Faculdade de Tecnologia de Americana Curso Superior de Tecnologia em Segurança da Informação

A IMPORTÂNCIA DO PENTEST PARA OS NEGÓCIOS DE UMA EMPRESA

ROBERTO DE CARVALHO PICONI

Americana, SP

2016

Faculdade de Tecnologia de Americana Curso Superior de Tecnologia em Segurança da Informação

ROBERTO DE CARVALHO PICONI

A IMPORTÂNCIA DO PENTEST PARA OS NEGÓCIOS DE UMA EMPRESA

Trabalho de conclusão de curso desenvolvido em cumprimento a exigência do curso de Tecnologia de Segurança da Informação da Faculdade de Tecnologia de Americana.

Orientador: Professor Especialista Edson Roberto Gaseta.

Americana, SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Piconi, Roberto de Carvalho
P664i A importância do Pentest para os negócios de uma empresa. / Roberto de Carvalho Piconi. – Americana: 2016.
36f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Edson Roberto Gaseta

1. Segurança em sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Roberto de Carvalho Piconi

A importância do pentest para os negócios de uma empresa

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/Americana.
Área de concentração: Segurança da Informação

Americana, 21 de junho de 2016

Banca Examinadora:

Edson Roberto Gaseta
Especialista
CEETEPS – Faculdade de Tecnologia de Americana

Rogério Nunes de Freitas
Especialista
CEETEPS – Faculdade de Tecnologia de Americana

Pedro Domingos Antoniolli
Doutor
CEETEPS – Faculdade de Tecnologia de Americana

RESUMO

Este trabalho explica e demonstra de maneira teórica e prática, a importância da segurança da informação de forma detalhada, explicando todos os seus conceitos e seus principais pilares, da mesma maneira que explica o que são as ameaças, e quais os tipos que existem. Destaca também o que são vulnerabilidade e suas categorias e por fim as medidas de segurança destacando cada detalhe, mostrando os métodos e os meios tecnológicos que podem ser usados para se defender e diminuir as chances de ocorrer um incidente de segurança. Em seguida, é explicado o que é *Pentest* e cada fase de sua aplicação, com a finalidade de demonstrar como ela é vital para os negócios de uma empresa, e que deve ser tomada como parte rotineira da equipe responsável pelo departamento de tecnologia da organização, visando sempre melhorar a segurança de seus ativos. Por fim, é realizado o estudo de caso onde foi criado um laboratório para mostrar de maneira prática como funciona cada fase do teste de invasão, e como ele pode ajudar a tornar o ambiente mais seguro.

Palavras-chave: *Pentest*; vulnerabilidade, segurança da informação.

ABSTRACT

This paper explains and demonstrates theoretical and practical way, the importance of security in detail information, explaining all its concepts and its main pillars, the same way that explains what are the threats, and what types there are, also highlights what are vulnerability and their categories, and finally security measures highlighting every detail, showing the methods and technological means that can be used to defend and reduce the chances of experiencing a security incident, then it is explained what is PenTest and each phase of its implementation, in order to demonstrate how it is vital to the business of a company and that should be taken as a routine part of the team responsible for the company technology department, aiming to improve safety of its assets, finally, it is carried out the case study where a lab was created to show a practical way to work each stage of penetration testing and how it can help make the environment safer.

Keywords: Pentest, vulnerability, information security.

Este trabalho é dedicado a Deus, à minha família e aos meus amigos, que sempre me apoiam e me ajudam na busca de meus objetivos.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus por estar sempre presente em minha vida, sempre ajudando a escolher o melhor caminho e por sempre me dar forças e saúde para buscar meus objetivos.

Agradeço aos meus pais e minha irmã, por sempre estarem me apoiando e orientando nas decisões que tomo e por sempre ajudarem quando preciso.

Agradeço aos meus amigos de escola por suas amizades, por seu companheirismo e pelo incentivo e apoio.

Quero agradecer também meu orientador, por sempre ajudar em cada processo do desenvolvimento desse trabalho, por compartilhar sua experiência no assunto e por me ajudar a chegar no final desse trabalho.

Agradeço a minha prima Andressa Piconi por me auxiliar com a obtenção de material de estudo para que esse trabalho pudesse chegar onde chegou e por sempre dar dicas para ajudar no desenvolvimento desse trabalho.

Também quero agradecer a minha melhor amiga e namorada Elen, por me ajudar no desenvolvimento desse trabalho e pelo incentivo sempre.

Por fim, agradeço a todos que fazem parte da minha vida e que sempre estão ao meu lado me apoiando.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Com a disseminação da informatização dentro das organizações, cresce de maneira exponencial os riscos de as empresas sofrerem um ataque cibernético, através das más configurações das aplicações *web* e de rede.

Contudo existe o *Pentest,* que visa descobrir o máximo de vulnerabilidades possíveis, e com o resultado gerar um relatório detalhando cada vulnerabilidade que foi descoberta e com conhecimentos específicos de segurança da informação, definir o que pode ser feito para eliminar cada uma das vulnerabilidades descobertas ou reduzir os riscos de elas serem exploradas.

O trabalho procura responder o porquê do *Pentest* ser tão importante para as organizações, e porquê deve ser considerada a execução desse processo periodicamente.

O objetivo geral dessa pesquisa é mostrar os processos que envolvem o *Pentest* e sua importância para uma organização, tendo como a principal finalidade mostrar de maneira clara e concisa o porquê esse processo é de grande importância para os negócios da empresa, e mostrar o impacto que um ataque de um *hacker,* que irá explorar uma vulnerabilidade, pode ter para seus negócios.

A importância desse trabalho se reflete em conscientizar os gestores das empresas sobre a importância da segurança da informação, uma vez que muitos ignoram sua relevância para a continuidade de seus negócios e não investem nesse setor.

Metodologicamente, esse trabalho adotou o método de pesquisa bibliográfica, e testes práticos em ambiente controlado.

2 SEGURANÇA DA INFORMAÇÃO

Para explicar de maneira clara e ajudar entender as próximas etapas desse trabalho, segundo Fontes (2006, p. 2), informação é um ativo da empresa que possui um valor e deve ser protegido através de políticas e regras, pois essa informação é de suma importância pois ajuda a empresa a alcançar seus objetivos e dar continuidade em seus negócios.

Seja qual for o ramo da empresa, seja qual for o seu objetivo, toda empresa trabalha com as informações para ajudar na tomada de decisão de seus negócios, sendo que partir disso, compartilhar informação se tornou imprescindível para as empresas que querem maior agilidade em suas ações (SÊMOLA, 2003. pp. 2-3).

Assim, Sêmola (2003. p. 10) diz que vale mencionar que, toda informação possui quatro ciclos de vida, que são:

Manuseio: que é o instante em que a informação é criada e manuseada;

Armazenamento: que é quando a informação é armazenada, seja qual for esse local;

Transporte: se trata no instante em que a informação é enviada, não importando o meio;

Descarte: é o instante em que a informação já não tem utilidade e a forma que ela é descartada.

“A segurança da informação pode ser entendida como uma área do conhecimento que visa proteger os ativos da empresa contra fraudes, acesso não autorizados e a indisponibilidade dos mesmos” (SÊMOLA, 2003. p. 43).

Segundo Lyra (2009, pp. 3 - 4), tais objetivos da segurança da informação são definidos por três princípios básicos:

Confidencialidade: onde somente usuários devidamente autorizados tem acesso a determinada informação;

Integridade: onde se deve garantir que tal informação não foi alterada de nenhuma maneira;

Disponibilidade: onde a informação deve estar disponível a qualquer momento para o usuário.

Além desses três aspectos, Lyra (2009, p. 4) destaca que existem mais cinco aspectos para mencionar:

Autenticidade: se trata de garantir que o usuário é que diz ser.

Não-repúdio: é a maneira de prova que o usuário executou tal ação.

Legalidade: garantir o que o sistema está de acordo com a legislação.

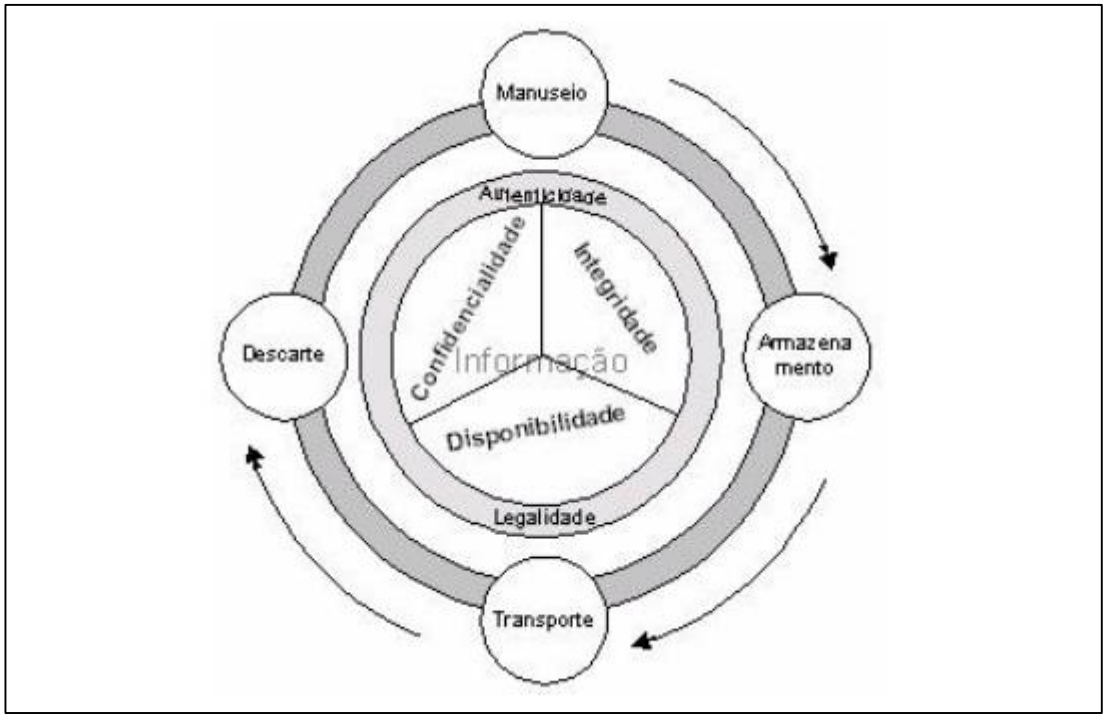
Privacidade: visa garantir o anonimato do usuário.

Auditoria: maneira pela qual o sistema verifica os atos realizado pelos usuários.

O ciclo de vida da informação e os três princípios básicos de segurança da informação mencionados anteriormente, estão diretamente ligados entre si.

A Figura 1 mostra a relação entre Segurança da Informação e o Ciclo de Vida da Informação.

Figura 1 - Relação entre Segurança da Informação e o Ciclo de Vida da Informação



Fonte: Juliano (2014).

Caso alguns desses aspectos sejam violados, tal violação torna-se um incidente de segurança, que é, um evento que pode causar a interrupção dos negócios da empresa (LYRA, 2009. p. 4).

Para demonstrar a importância da segurança da informação, Felipini (2015), do ano de 2001 até 2012, o número de usuários no Brasil com acesso à *Internet*

passou de 12 milhões para 90 milhões, resultando em um total de 650% de aumento. Já o número de compradores na *Internet* teve um crescimento de 3.536%, passando de 1.1 milhões de compradores em 2001 para 40 milhões em 2012, que por sua vez, gerou um aumento de 4.400% no faturamento dentro do período de 12 anos. É importante destacar que, se uma empresa de comércio *on-line* fosse alvo de *hackers* e esse site ficasse fora do ar por um determinado tempo, isso poderia gerar um enorme prejuízo.

Como forma de demonstrar o dano que isso poderia causar, Akamai Technologies informou em seu site que em 2010 um ataque de *hackers* a *Black Friday* americana que se estendeu até ao C*yber Monday*, causou um prejuízo de 15 milhões de dólares (ECOMMERCENEWS, 2010).

3 AMEAÇAS, VULNERABILIDADE E MEDIDAS DE SEGURANÇA

Neste capítulo será abordado os que são ameaças e vulnerabilidade e quais suas classificações, e também as medidas de segurança que podem ser utilizadas para se defender delas.

3.1 Ameaças

Nenhum sistema é 100% seguro, sempre existe um ponto fraco, seja em uma pessoa, em uma aplicação ou processo. Se tratando de tecnologia, a todo o momento surgindo novas formas de usá-la, pode-se dizer que novas falhas surgem juntamente com elas.

Sêmola (2003, pp. 47 - 48) diz que isso são as ameaças, que são agentes ou condições que podem causar algum comprometimento aos ativos das empresas através da exploração de vulnerabilidades. Dentro dos aspectos das ameaças existem três grupos, que podem ser classificados devido a sua intenção.

Naturais: são as ameaças advindas dos fenômenos da natureza, como alagamento, terremotos, etc.

Involuntárias: geralmente causadas inconscientemente, devido à falta de conhecimento.

Voluntárias: são as ameaças causadas intencionalmente, por seres humanos, como *hackers*, espiões, ex-funcionário, etc.

3.2 Vulnerabilidades

Vulnerabilidade é um ponto fraco em um *software* ou em um sistema mal configurado, e que pode ser explorado para causar um incidente de segurança da informação, e existem várias causas de vulnerabilidade, mas as maiores ocorrências são causadas por ausência de correções nos *softwares* (ENGEBRETSON, 2014. p. 124).

Sêmola (2003, pp. 48 - 49), diz que as vulnerabilidades não geram nenhum incidente só pelo fato de existirem, para que gere um incidente é necessário a exploração da mesma por um terceiro, dentro deste aspecto o autor cita alguns exemplos de vulnerabilidade:

Físicas: é tudo relacionado a infraestrutura da empresa, tais como, vazamentos, incêndio, risco de explosões, entres outros.

Naturais: essas são ligadas a desastres naturais, como enchentes, terremotos, tempestades, etc.

***Hardware*:** são falhas ligadas aos recursos tecnológicos da empresa ou um erro na configuração.

***Software*:** são falhas ocasionadas por vazamento de informações, perca de dados, indisponibilidade de um determinado recurso.

Mídias: são todos os meios de armazenamento que podem ser perdidos ou danificados.

Comunicação: são as falhas relacionadas a acessos indevidos e de comunicação.

Humanas: está ligado a falta de treinamento, vazamento de informações sigilosas, não seguir as políticas de segurança da organização, greves, vandalismo, entre outros.

3.3 Medidas de Segurança

As medidas de segurança são os meios pelo qual as informações e os seus ativos são protegidas da ameaça, que podem explorar suas respectivas vulnerabilidades, diminuindo os riscos oferecidos a organização (SÊMOLA, 2003. p. 49).

Sêmola (2003, p. 49), menciona que tais medidas apresentam as seguintes características:

Preventivas: essas medidas procuram evitar que um incidente venha acontecer e busca por meios de políticas de segurança, normas, procedimentos e outros meios, assegurar que as medidas estão sendo acatadas.

Detectáveis: são os meios pelo qual detectam uma ameaça e impedem que o mesmo explore uma vulnerabilidade. Nesse caso alguns meios pelo qual as

ameaças podem ser detectadas, são através de alertas de segurança, câmeras de vigilância, entre outros.

Corretivas: são as ações tomadas para corrigir uma falha da estrutura tecnológica e humana, por exemplo: equipe de emergência, planos de continuidade operacional e plano de recuperação de desastre.

Além, desses meios de proteção, existem também os meios tecnológicos que visam ajudar a empresa a se proteger contra qualquer tipo de incidente que possa ocorrer.

Segundo Nakamura e Geus (2003, pp. 173-367) existem seis principais meios tecnológicos e práticos para proteção da empresa, os quais são:

Políticas de segurança: essa está relaciona a tudo que envolve a proteção da informação, onde esse deve ser o primeiro objetivo da empresa, através disso serão definidas todas as normas para proteção dos recursos da empresa. As políticas de segurança têm como base cuidar dos aspectos humanos, tecnológicos e culturais, levando em conta a legislação de onde a empresa está situada e também os processos que envolvem o negócio da empresa.

***Firewall*:** é um conjunto de componentes ou apenas um componente, localizado entre duas redes ou mais, onde o tráfego passa, onde é possível controlar o tráfego, a autenticação e averiguar todo o tráfego que passa por ele. Em geral o *firewall* protege a rede interna da organização, ou seja, uma rede segura, de uma rede externa não segura, como por exemplo, a *Internet*.

Sistema de detecção de intrusão: esse sistema visa detectar atividades suspeitas e fora do comum na rede, ele realiza essas análises através de dois métodos, o primeiro é o sistema de detecção de intrusão baseado em *host*, através de *logs* ou agentes de auditoria ele monitora acessos e alterações no sistema quaisquer que sejam ela. O segundo método é o sistema de detecção de intrusão baseado em rede, este realiza a análise do cabeçalho e os conteúdos dos pacotes, comparando com os padrões conhecidos.

Criptografia: a criptografia nada mais é do que transformar um texto claro em um texto cifrado, ou seja, o texto claro fico escondido dentro do cifrado, está operação ocorre através de algoritmos com funções matemáticas, é usada tanto para criptografar quando decriptografar.

Redes privadas virtuais: essas redes também conhecidas como VPN (*Virtual Private Network)*, são utilizadas para interligas matrizes, filiais, fornecedores,

vendedores externos, entre outros. Para estabelecer essa conexão ela utiliza a rede pública, isso é como se o usuário estivesse dentro da organização utilizando sua rede interna. De fato, a VPN veio para substituir a conexões dedicas que são muito mais caras.

Autenticação: a autenticação é o processo de verificar se o usuário é quem diz ser, isso se dá através por meio de algo que usuário sabe, como por exemplo, as senhas, sua identificação também pode se dar também em algo que o usuário possui, exemplo disso são os *smart cards* (cartões inteligentes) e o outro método é baseado em alguma característica do usuário, como retina, impressão digital, reconhecimento de voz, entre outros.

Essas são as principais medidas de segurança que podem ou devem ser integradas aos negócios de uma empresa, pois isso ajudará a empresa a se proteger de qualquer incidente que venha a ocorrer, porém cada medida de segurança deve ser cuidadosamente analisada, configurada, aplicada e estar diretamente ligada aos processos da empresa, para que nenhuma delas venham a prejudicar o andamento dos negócios.

4 *PENTEST*

O *Pentest* nada mais é do que, uma tentativa autorizada através de um contrato, de obter acesso aos sistemas da empresa, utilizando das mesmas técnicas utilizadas por um *hacker* mal-intencionado, porém, a finalidade do *Pentest* ou *hacking* ético é identificar as vulnerabilidades que empresa possui, explorar essas vulnerabilidades como prova de que elas são reais e perigosas, e no final, gerar um relatório detalhado contendo todas as vulnerabilidades encontradas durante o processo, e as possíveis soluções para mitigar essas falhas. O processo de teste de invasão também é conhecido como: *Pen testing*, *hacking*, *hacking* ético, *hacking white hat*, segurança ofensiva e *red teaming* (equipe vermelha) (ENGEBRETSON, 2014. pp. 23 - 24).

O *Pen testing*, é dividido em sete fases, que são: definição do escopo, reconhecimento, *scanning*, exploração de falhas, escalonamento de privilégios, preservação de acesso e geração de relatório, todos serão abordados nas próximas páginas (ENGEBRETSON, 2014. p. 43).

4.1 Tipos de *Pentest*

Moreno (2015, pp. 52 – 55) diz que dentro do *Pentest* existem três métodos de teste de invasão que podem ser executados, que são:

Black-box*:** nesse tipo de teste o profissional que executará o teste de invasão não tem nenhum tipo de conhecimento sobre a infraestrutura da empresa e não sabe quais sistemas as máquinas utilizam, processos que cada uma executa. Esse tipo de teste se assimila mais quanto ao método que um *hacker* mal-intencionado, que está fora da rede da empresa irá utilizar para ganhar acesso aos seus sistemas. Dentro dessa metodologia existem suas subcategorias, uma é a ***blind que é quando o auditor não tem nenhuma informação da rede e a empresa sabe que será atacada. A outra é a ***double-blind,*** neste método o auditor também não tem nenhuma informação da rede e a empresa não sabe que será atacada.

***White-box*:** nesse tipo de teste o responsável pela execução dos testes terá todo conhecimento sobre a infraestrutura de rede do cliente, como por exemplo,

endereços de rede, sistemas que os computadores utilizam, mecanismos de segurança, processos, entre outros. O *White-box* se encaixa mais no perfil de um ataque interno, ou seja, gerado por um funcionário da própria empresa, ou até mesmo por um ex-funcionário. Esse método de teste também possui duas subcategorias. O primeiro é o ***Tandem***, onde o responsável pela execução dos testes possui todas as informações da infraestrutura da empresa e a empresa sabe que será atacada. O segundo é o ***Reversal***, nesse teste o auditor de segurança tem todas as informações da rede do cliente, mas o cliente não sabe que será atacado.

Gray-box*:** essa metodologia é uma mistura entre *black-box* e *white-box*, onde o auditor possui um conhecimento parcial da rede, e também possui duas subcategorias, que são a ***Gray-box, onde a empresa sabe que será atacada e o executor dos testes tem conhecimento parcial da rede. E a segunda é a, ***Double gray-box***, nesse método a empresa não sabe que será atacada e o auditor tem o conhecimento parcial da rede.

É importante explicar a empresa contratante do serviço de teste de invasão os três tipos de testes para que ela possa definir qual deles se encaixa melhor em sua necessidade atual, reduzindo assim os riscos que ela corre ao sofrer algum tipo de ataque, seja ele externo ou interno.

4.2 Fases do *Pentest*

4.2.1 Definição do Escopo

A fase inicial para o *Pentest* é a definição do escopo, onde juntamente com o cliente, será definido até onde o teste será realizado, como será realizado e qual o seu propósito, somente após terem tudo previamente definido é que o teste terá início (WEIDMAN, 2014, p. 31).

É importante deixar essa fase bem definida, para que não haja nenhum inconveniente durante o processo. Porém durante o teste de invasão é possível que seja descoberto outros alvos em potencial, tais alvos devem ser reportados ao supervisor da empresa para que seja averiguado, se é permitido a realização do teste no mesmo.

4.2.2 Reconhecimento

A fase de reconhecimento pode ser considerada a mais importante dentre todas as outras, porém, essa é a fase que é mais menosprezada pelos aspirantes a *hacker* ou *pentester*, isso ocorre por que os iniciantes não tiveram um bom entendimento sobre essa fase, outra razão para isso acontecer é porque essa é a fase menos técnica e empolgante se comparada as outras (ENGEBRETSON, 2014. pp. 53 - 54).

No entanto, quanto mais tempo for investido nessa fase, maiores serão as chances de obter êxito nos próximos passos da invasão. Como exemplo da importância dessa fase, Engebretson (2014, p. 54) cita o exemplo:

> “Suponha que temos dois criminosos diferentes planejando assaltar um banco. O primeiro compra uma arma e entra no primeiro banco que encontrar gritando: “Mãos ao alto. Passe todo seu dinheiro para cá! ”. Não é difícil imaginar que a cena seria um caos total e, mesmo que o ladrão consiga escapar, provavelmente não seria necessário muito tempo para a polícia encontrá-lo, prendê-lo e enviá-lo à prisão. Contrate isso com praticamente qualquer filme de Hollywood atual, em que os criminosos passam meses planejando, esquematizando, organizando e revendo os detalhes antes do assalto. Eles investem tempo para obter armas anonimamente, planejar rotas de fuga e analisar as plantas do prédio. Visitam o banco para determinar a posição das câmeras de segurança, observar os guardas e verificar quando o banco tem o máximo de dinheiro ou está mais vulnerável. É claro que o segundo criminoso tem mais chances de escapar com o dinheiro. ”

Essa etapa do teste de invasão deve ser iniciada buscando informações de domínio público, que tem como objetivo coletar e criar uma lista com endereços IP (*Internet Protocol)* e URLs (*Uniform Resource Locators)*, para atacá-los posteriormente (ENGEBRETSON, 2014. p. 55).

No processo de reconhecimento não se deve somente levantar endereços IP, sendo importante obter informações como, topologia, mapeamento, servidores, funcionários, empresas terceirizadas, *e-mails*, *Facebook*, telefones, tudo isso aumentarão as chances de êxito no teste (MORENO, 2015. p. 65).

Dentro dessa fase existem dois métodos para realizar um reconhecimento, o primeiro é o reconhecimento passivo, que consiste em buscar informações disponíveis na *Internet*, sem que ocorra um contato direto com a vítima, diminuindo assim, as chances de ser detectado. O segundo método é o reconhecimento ativo, que nada mais é o oposto do reconhecimento passivo, ou seja, há contato direto

com a vítima, porém, dessa maneira as chances são maiores de ser detectado (ENGEBRETSON, 2014. p. 56).

Fica claro que essa fase está diretamente ligada ao processo de definição de escopo, pois é aqui, que serão encontrados possíveis novos alvos, com isso, é fácil entender que quanto menor o número de alvos excluídos do escopo do teste, melhor para o processo de invasão e para a segurança da organização.

Engebretson (2014, p. 61 - 63) diz que, uma das maneiras mais utilizadas para o levantamento de informações, é utilizar o *Google Hacking,* o Google disponibiliza diretivas de busca, que podem refinar as pesquisas no site e buscar somente o que você quer no endereço que você quer, a diretiva tem o seguinte formato:

site: endereço do site e o termo da pesquisa que deseja procurar

Exemplo: site: fatec.edu.br docentes

Esse exemplo retornaria somente informações ligada aos docentes retiradas do site da FATEC de Americana, que deixa mais fácil o levantamento de informações.

4.2.3 *Scanning*

Após a coleta de informações no processo de reconhecimento, essa etapa trata de realizar um escaneamento de sistemas e serviços nos respectivos endereços obtidos na primeira fase. Essa etapa pode ser dividida em subfases que se trata de, determinar se um alvo está ativo na rede, realizar o *scanning* de portas e um escaneamento de vulnerabilidade do alvo (ENGEBRETSON, 2014, pp. 97 - 98).

De maneira mais detalhada, o processo de determinar se um alvo está ativo, significa verificar se somos capazes de se comunicar com o alvo, na próxima etapa, o *scanning* de portas tem como objetivo verificar as portas abertas e os serviços que estão rodando em cada máquina. Uma porta nada mais é, do que, uma maneira do computador se comunicar com outros na rede, por exemplo: a porta 53 que roda o serviço de DNS (*Domain Name System)* que tem como função traduzir endereços IP em endereço nominal e vice-versa. Por fim, o *scanning* de vulnerabilidade visa descobrir falhas em serviços conhecidos, porém nem sempre achar uma vulnerabilidade significa que o sistema já possa ser comprometido, uma

que, há uma classificação para cada uma das vulnerabilidades que vão de: baixo, médio e alto risco (ENGEBRETSON, 2014. pp. 99 - 101).

Uma das ferramentas mais famosas, se não, a mais famosa é o NMAP, que é uma ferramenta extremamente eficiente para realizar o escaneamento de rede, com ela, é possível visualizar quais máquinas estão ativas, quais portas estão abertas, quais são os serviços que esses *hosts* estão executando, inclusive qual o sistema operacional e sua versão, entre outras funcionalidades.

Já para a parte de escaneamento de vulnerabilidade existe uma ferramenta chamada Nessus, que faz uma varredura na rede na busca por dispositivos com falhas de segurança. Após executada uma varredura o Nessus mostra em relatório tudo o que foi descoberto na rede e classifica a seriedade da vulnerabilidade (ENGEBRETSON, 2014, pp. 125 - 130).

4.2.4 Exploração de falhas

A exploração de falha é a fase, que, nada mais é do que, obter controle total do sistema explorando uma vulnerabilidade, seja, por erro de configuração no sistema ou por uma falha no código de uma aplicação, no entanto vale mencionar que nem toda falha permite o acesso total ao sistema. Mas, uma vez que o sistema foi comprometido o *hacker* ético ou o invasor, buscarão o acesso como administrador no sistema, caso já não tenham conseguido quando conseguiram acesso ao sistema, após obterem o acesso como administrador eles irão executar os *payloads* que são códigos maliciosos executados na máquina para abrir *backdoors* (permitem que o atacante estabeleça conexão posteriormente), desabilitar serviços, instalar programas entre outras funcionalidades (ENGEBRETSON, 2014, p. 136).

4.2.5 Escalonamento de privilégios

De acordo com Moreno (2015, p. 195), após ter realizado a exploração de falhas e obtido acesso com um certo nível restrito ao sistema, é necessário que o

profissional que está executando o teste, tente obter acesso ao sistema com contas administrativas, com o intuito de executar programas que requerem um nível de administrador do sistema.

Moreno (2015, p. 195) *apud* Shakeel; Heriyanto (2011), menciona ainda que existem três métodos de autenticação:

Arquivos de autenticação: se trata de mecanismos de senhas, um usuário X com senha@123, ou seja, se alguém acessar o sistema usando este usuário e senha, o usuário X é quem está usando o sistema.

***Tokens*:** são os, métodos mais sofisticados de autenticação.

Biometria: esse método é considerado mais seguros que os outros dois métodos, pois está ligado a parte de biometria e retina de um determinado usuário.

4.2.6 Manutenção do acesso

Essa fase consiste em após ter explorado as falhas, ter obtido acesso com conta administrativa, instalar um *backdoor* (portas do fundo), ou seja, garantir o retorno ao sistema mesmo após já ter encerrado a conexão que foi realizado durante o primeiro ataque (MORENO, 2015, p. 226).

4.2.7 Geração do relatório

Moreno (2015, p. 268 – 270) diz que, após ter realizado todos os processos de um teste de invasão, é importante gerar um relatório detalhando todas as falhas encontradas, e também as medidas que devem ser adotadas para que nenhuma dessas falhas sejam exploradas. Também é importante não deixar nada de fora do relatório pois essa falta pode acarretar em problemas jurídicos. O autor ainda menciona que existem três tipos de relatórios, sendo eles:

Relatório executivo: este relatório deve conter a capa, índice, os objetivos dos testes de invasão, a classificação de cada vulnerabilidade encontrada e um sumário executivo descrevendo toda a metodologia utilizada no teste.

Relatório técnico: esse é o principal relatório, onde deve ser tudo minimamente detalhado, e deve conter o mapeamento das vulnerabilidades, sua classificação e risco, mapeamento dos *exploits*, listando todos os *exploits* utilizados, deve conter a narrativa do ataque, aqui deve ser descrito detalhadamente todo o processo do teste de invasão e por fim deve conter as práticas de segurança, ou seja, as medidas que devem ser adotadas para garantir a segurança da informação na empresa.

Relatório comercial: neste relatório deve conter as máquinas que foram testadas, seu valor e o valor do projeto de teste de invasão.

5 LABORATÓRIO PARA ESTUDO DE CASO

Dentro desse capítulo é apresentado o desenvolvimento passa à passo da execução do teste de invasão em um ambiente virtual controlado.

5.1 Configuração do ambiente de testes

O laboratório para estudo de caso foi constituído por quatro máquinas virtuais uma com Windows XP, outra com Windows 7, uma com Ubuntu 8.10 e a máquina atacante executando o sistema Kali Linux 2.0. Lembrando que cada máquina alvo foi configurada propositalmente para estar vulnerável a ataques. Abaixo segue a configuração mais detalhada de cada máquina:

Windows XP: *service pack* 3, *firewall* desabilitado, atualizações automáticas desativadas, foi instalado também alguns aplicativos vulneráveis, tais como, Zervit 0.4, SLmail 5.5, 3ComTFTP 2.0.1, XAMPP 1.7.2, Adobe Acrobat Reader 8.1.2, WAR-FTP, WinSCP, Immunity Debugger e o Mona. O endereço ip desta máquina é 192.168.1.130, máscara de rede 255.255.255.0 e *gateway* 192.168.1.1, a máscara de rede e o *gateway* é padrão para todas as outras máquinas.

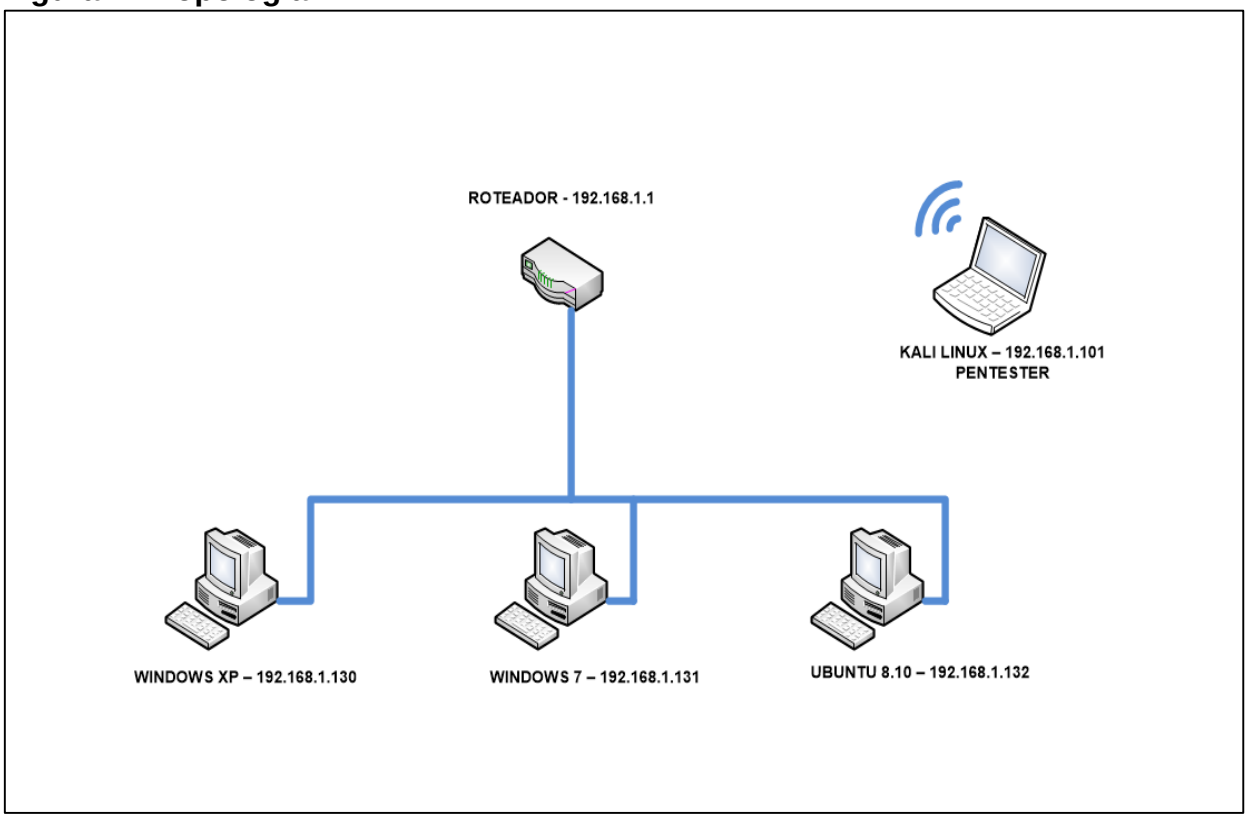
Windows 7: service pack 1, atualizações automáticas desativadas, *firewall* desativado, nesta máquina foi instalado o SQL Server Express 2008 R2 SP3. Essa máquina está com o endereço de rede 192.168.1.131.

Ubuntu 8.10: apache 2.2.9, Firefox 3.0.3, MySQL 5.0.67, PHP 5.2.6, openssl 0.9.8g. O ip dessa máquina é 192.168.1.132.

Kali Linux 2.0: nesta máquina foi apenas instalado o Nessus Home, o restante das ferramentas utilizadas para os ataques são padrão nesse sistema que é voltado para P*entest*. Já essa máquina contém o endereço de rede 192.168.1.101.

A Figura 2 mostra a ilustração da topologia:

Figura 2 - Topologia



Fonte: Autoria própria (2016)

5.1.1 Reconhecimento

Nessa fase foi executada uma coleta de informações *online*, utilizando pesquisas em sites da web, o http://netcraft.com/, e escaneamento de portas, serviços e versões utilizando o NMAP.

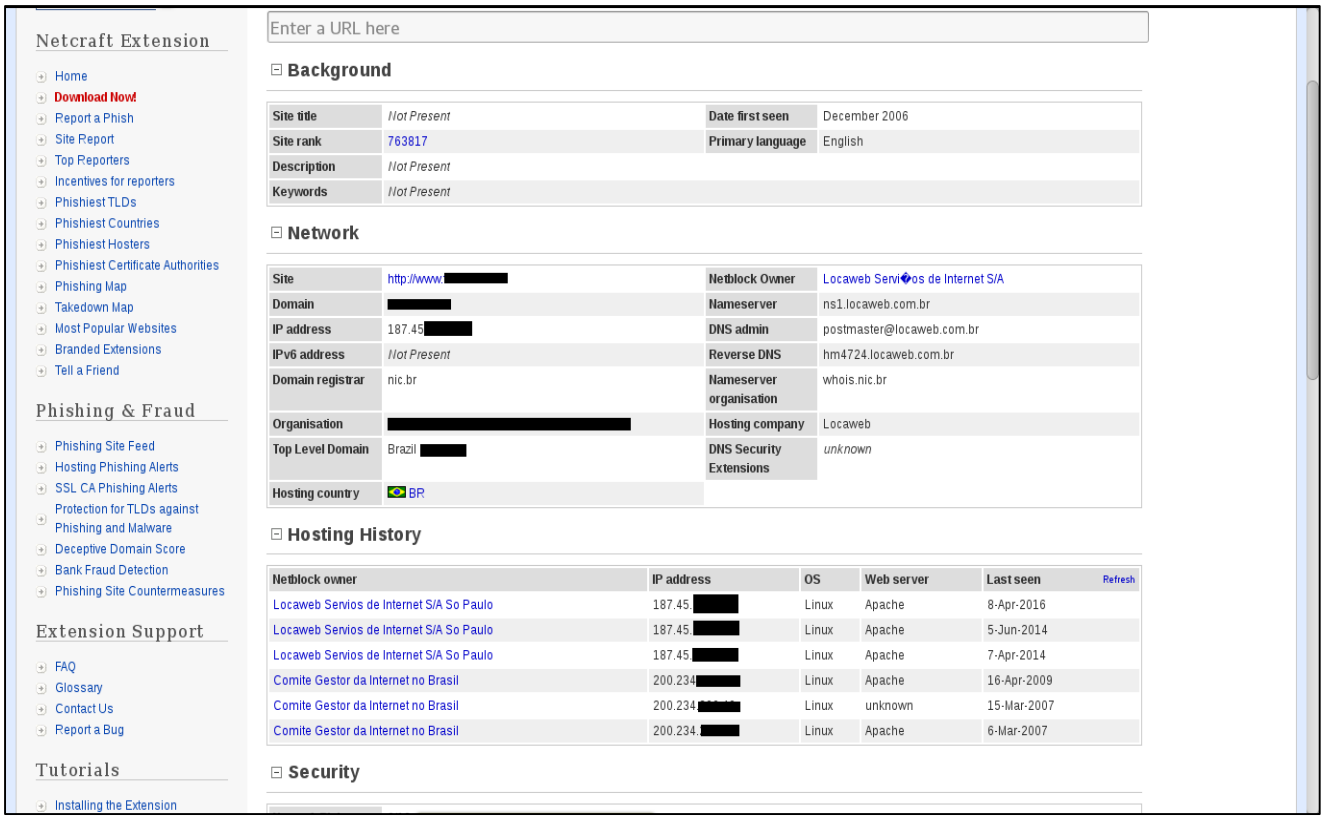
Weidman (2014, p. 135), diz que “ às vezes, as informações que os servidores *web* e as empresas de *web hosting* reúnem e tornam publicamente disponíveis podem dizer muito a respeito de um *site*. ”

5.1.2 Coleta de informações *on-line*

Nessa fase da coleta de informações foi utilizado o site http://netcraft.com para exemplificar como a pesquisa pode revelar informações importantes de um

alvo. O nome do alvo e parte do endereço de IP foi ocultado por questões de segurança, conforme mostrado na Figura 3.

Figura 3 - Coleta de informações on-line



Fonte: Autoria própria (2016)

Como é possível ver, o site fornece endereço IP de *Internet*, qual sistema operacional o servidor está executando, qual o servidor *web*, a partir desse ponto é possível cada vez mais buscar informações mais detalhadas a partir de outras informações.

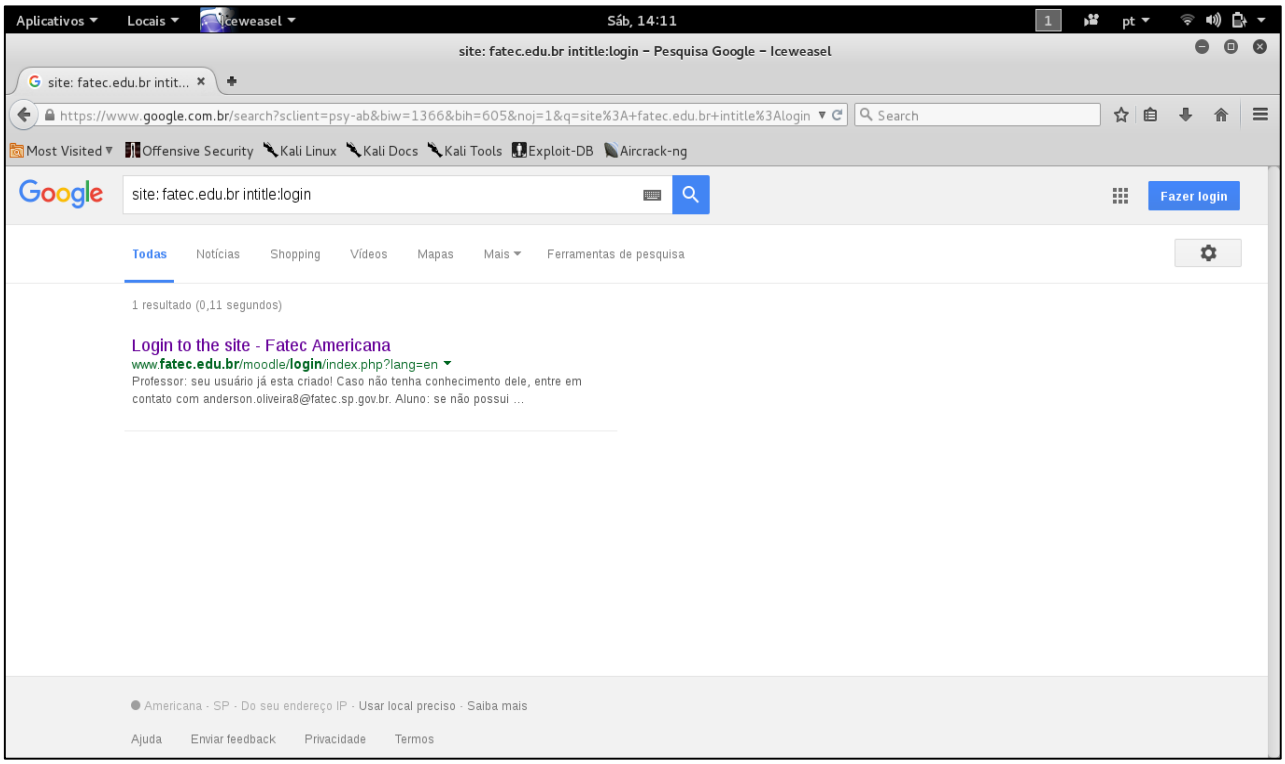
Outra excelente maneira de obter informações é utilizando o *Google Hacking*, que basicamente é utilizar a pesquisa do Google a seu favor, porém, existe uma maneira mais eficiente de fazer as pesquisas, que é, utilizando os operadores avançados do Google, o exemplo a seguir é apenas um dos muitos que existem. Os operadores avançados basicamente são compostos pela diretiva de busca que você deseja procurar seguido de dois pontos e o termo que você busca, por exemplo:

site: endereco.com.br notícias

Com essa busca o Google só retornará tudo o que for encontrado dentro do site endereco.com.br que contenha o termo notícias (ENGEBRETSON, 2014, pp. 62-63)

A Figura 4 mostra um exemplo, onde foi pesquisado o termo *login* no site *http://www.fatec.edu.br*.

Figura 4 - Busca avançada no Google



Fonte: Autoria própria (2016)

Nessa pesquisa foi utilizada a diretiva *site:fatec.edu.br intitle:login*, que retorna o tudo o que o Google achar no site http://www.fatec.edu.br e que contenha a palavra *login* no endereço do site.

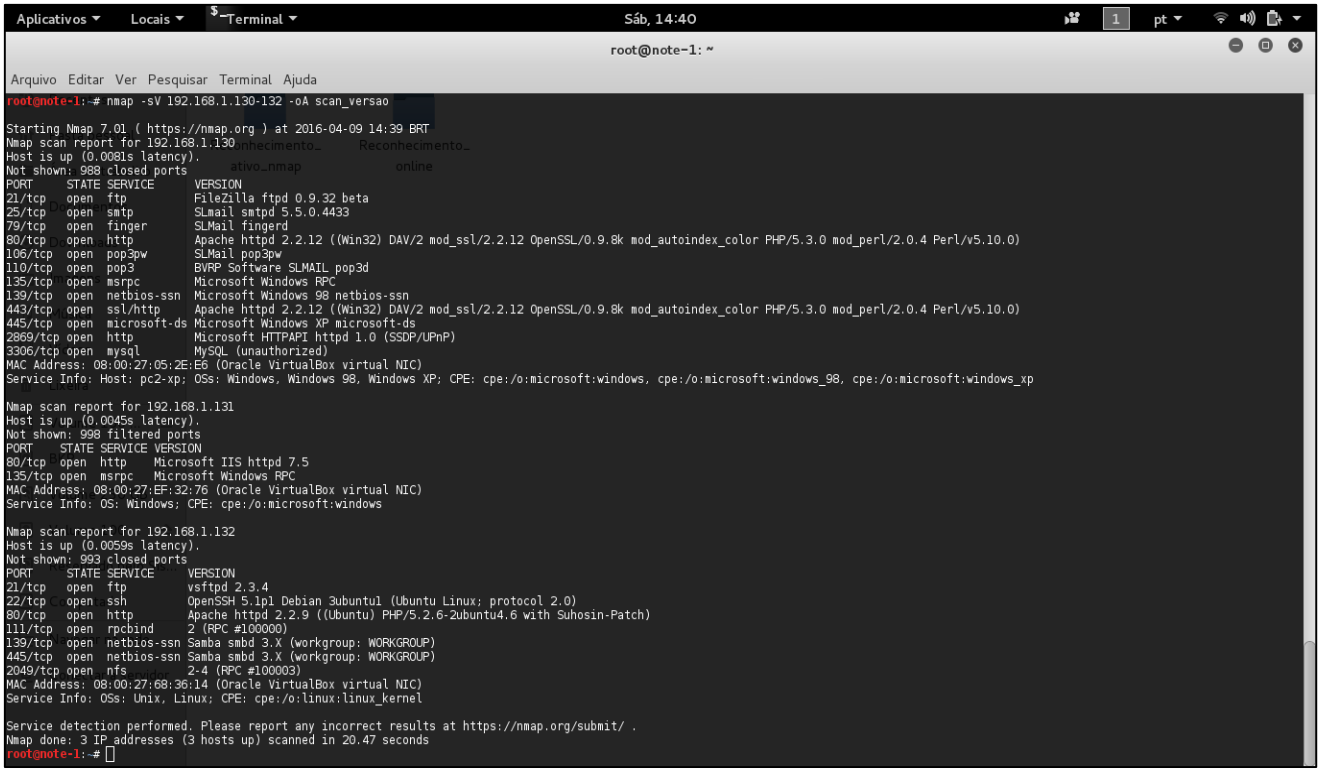
5.1.3 Scanning

Nesta etapa, foi utilizado o NMAP para realizar o escaneamento de portas e serviços. O NMAP é uma ferramenta voltada para realizar varreduras na rede e auditoria de segurança, ele utiliza pacotes IP para descobrir quais os computadores

que estão ativos na rede, quais serviços eles estão rodando e também quais os sistemas operacionais estão executando, e também quais portas estão abertas, quais estão protegidas e muitas outras funções (www.nmap.org).

A Figura 5 mostra um exemplo de onde foi utilizada a opção *nmap –sV* 192.168.1.130-132 *–ao scan_versao,* a opção *nmap* serve para iniciar a aplicação, *–sV* especifica que o tipo de escaneamento será o de versão, o 192.168.1.130-132 define que o nmap fará a varredura dos IP 192.168.1.130 até o 192.168.1.132 e o parâmetro *–oA scan_versao*, define que os resultados obtidos da varredura serão armazenados no arquivo scan_versao.

Figura 5 - Escaneamento NMAP



Fonte: Autoria própria (2016)

Como é possível ver através da imagem o Windows XP está executando o aplicativo SLMail versão 5.5.0.4433 executando na porta 25, no Windows 7 tem um serviço IIS versão 7.5 rodando na porta 80 e no Ubuntu tem um servidor apache versão 2.2.6 rodando na porta 80. Com base nisso basta buscar por vulnerabilidades

conhecidas que esses serviços podem ter, essas informações podem ser facilmente encontradas a *Internet*.

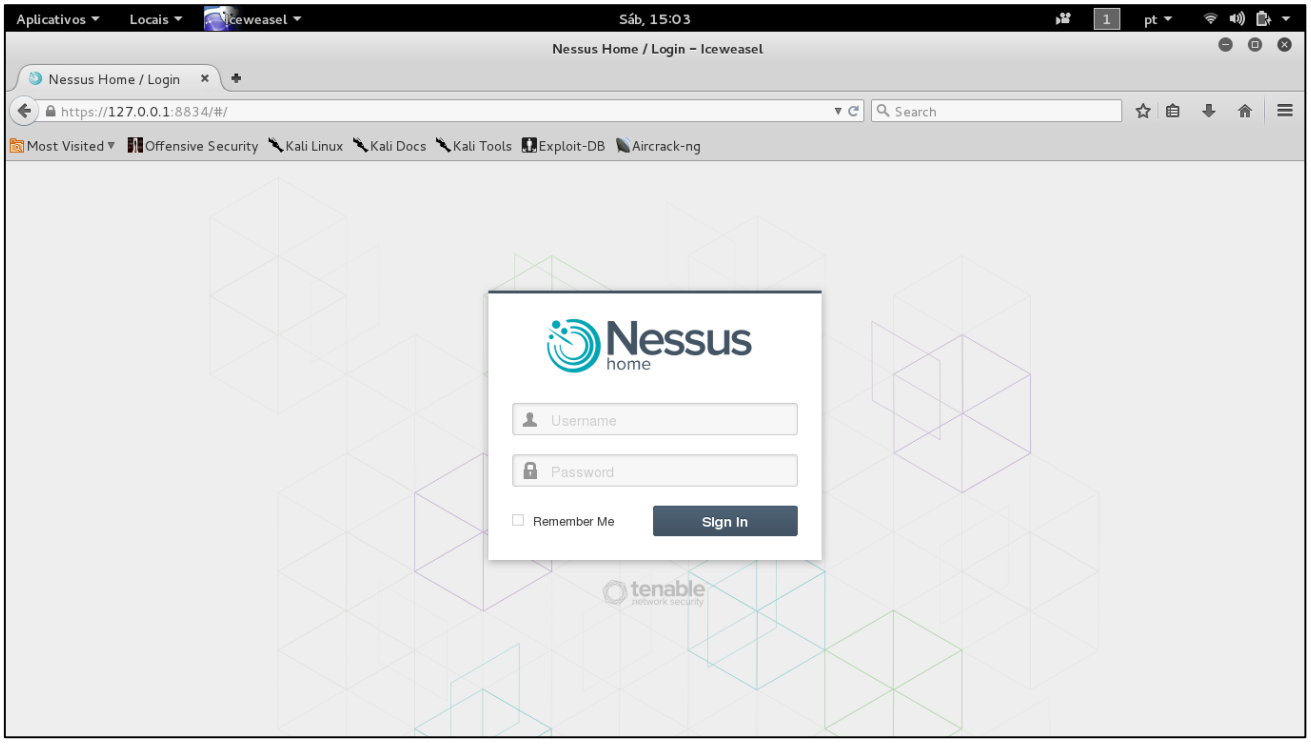
5.1.4 *Scanning* de vulnerabilidade

Após executar o escaneamento de portas nas máquinas alvos, é importante fazer uma varredura atrás de vulnerabilidades. Engebretson (2014, p. 124) diz que, “uma vulnerabilidade corresponde a um ponto fraco no *software* ou na configuração do sistema, que normalmente pode ser explorado. “ Nesta etapa do *scanning* foi utilizada a ferramenta Nessus Home, disponível gratuitamente, porém existem outras versões pagas dela.

O Nessus possui *plug-in*, que são seus componentes básicos, esses *plug-ins* são pequenos blocos de código enviados e executados nas máquinas alvos, em busca de vulnerabilidades conhecidas (ENGEBRETSON, 2014. p. 127).

A Figura 6 mostra a tela de *login* do Nessus:

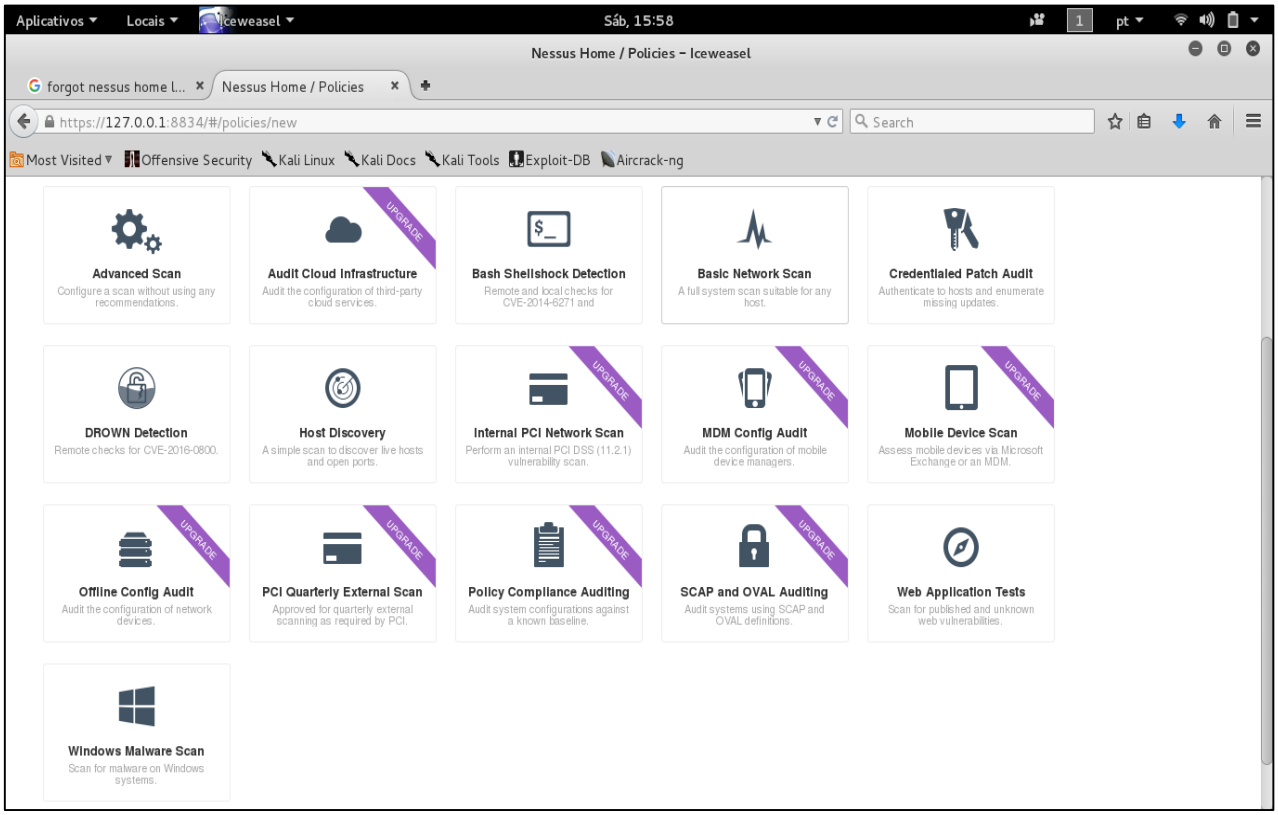
Figura 6 - Nessus Login



Fonte: Autoria própria (2016)

Após ter realizado o *login* na aplicação, é necessário criar um tipo de escaneamento para que seja possível executar na rede, porém como se trata de uma versão gratuita só algumas estão disponíveis, nesse caso foi escolhido o *basic network scan*, conforme mostrado na Figura 7:

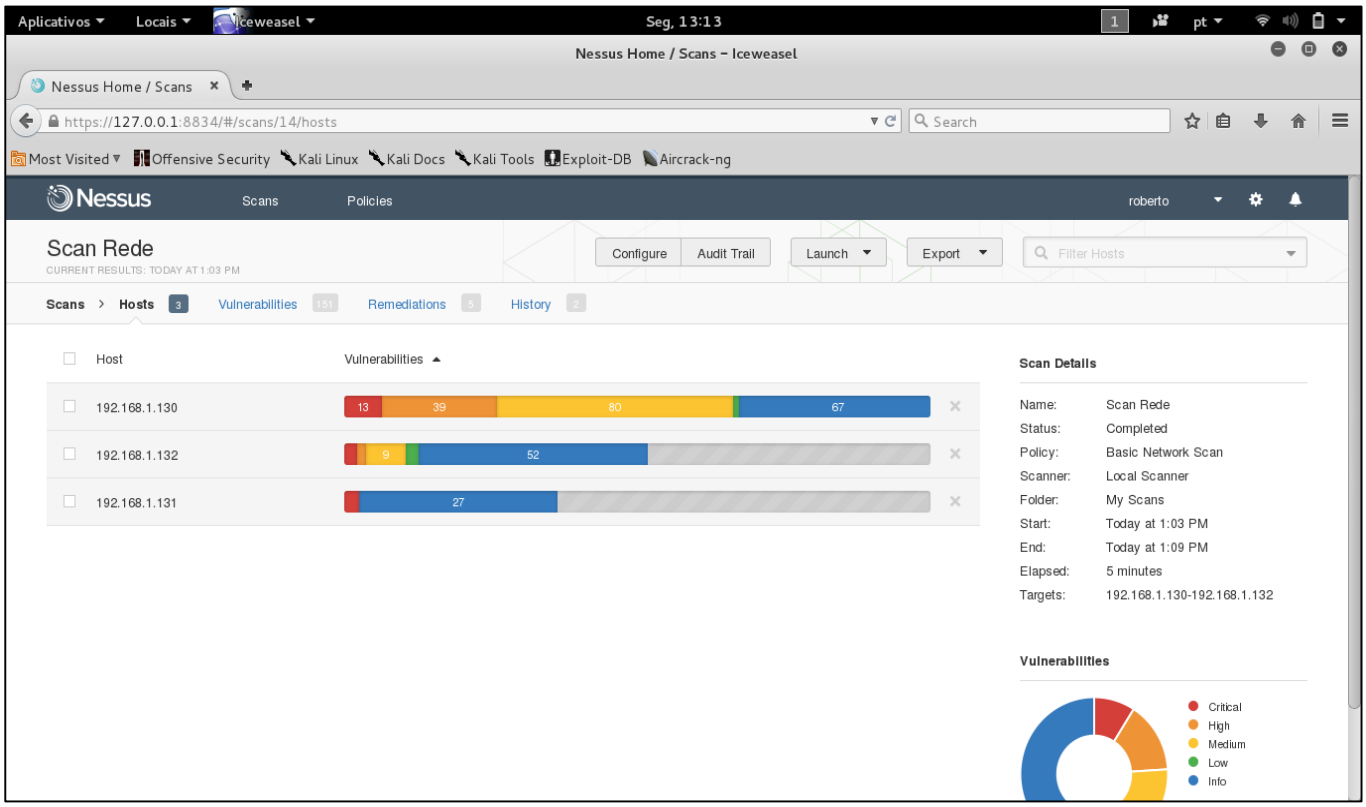
Figura 7 - Tipos de escaneamento



Fonte: Autoria própria (2016)

Após ter configurado e executado o escaneamento para executar nas máquinas alvos que são os endereços 192.168.1.130 até 192.168.1.132, o Nessus mostras quantas vulnerabilidades foram encontradas em cada alvo e o seu nível de criticidade, mostrado na Figura 8 o resultado obtido:

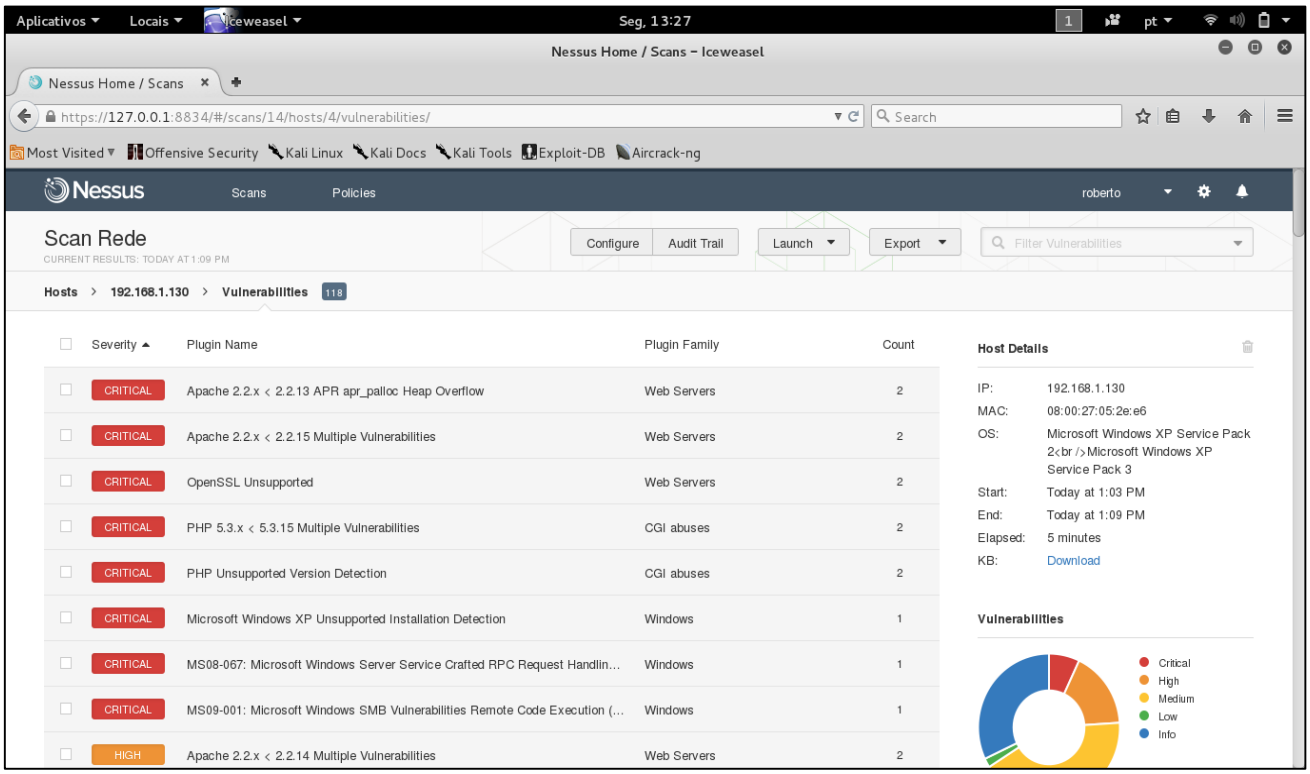
Figura 8 - Resultados dos alvos



Fonte: Autoria própria (2016)

A aplicação também mostra de forma bem detalhada cada vulnerabilidade encontrada, como é possível ver na Figura 9, o alvo 192.168.1.130 que corresponde ao Windows XP oito vulnerabilidades críticas:

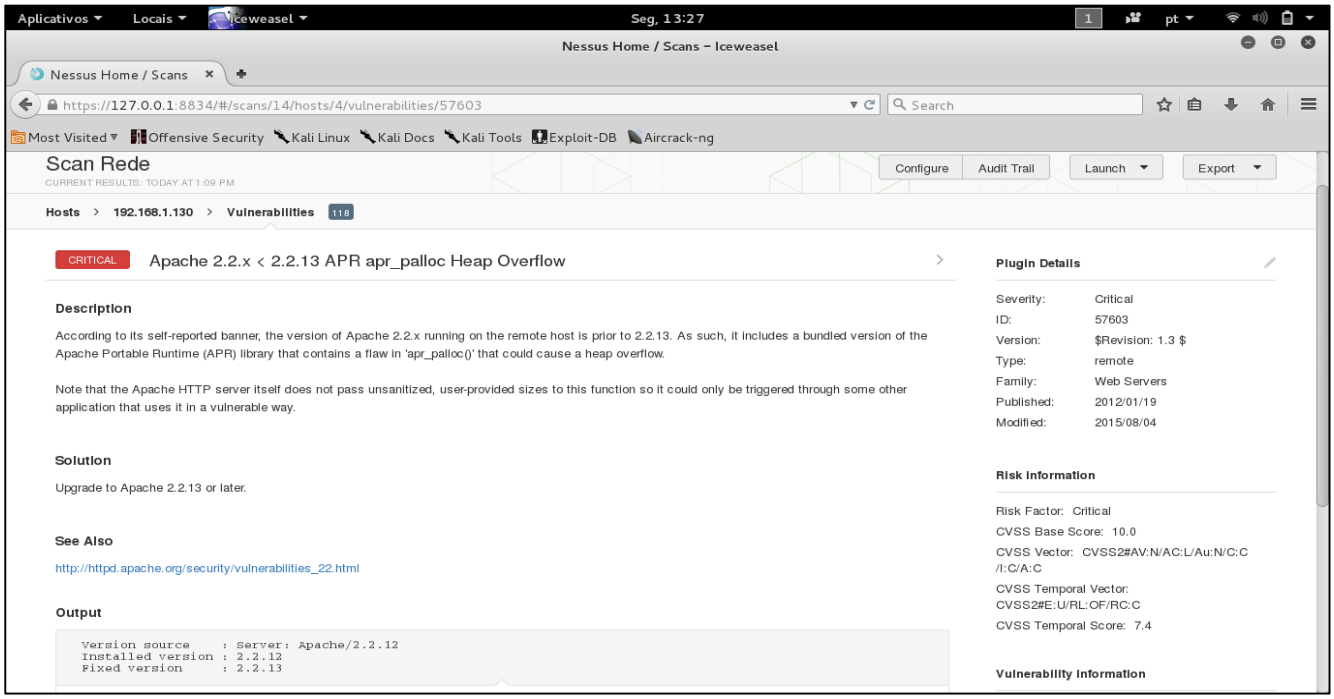
Figura 9 - Vulnerabilidades



Fonte: Autoria própria (2016)

É possível também selecionar cada vulnerabilidade e ver sua descrição e uma possível solução para o problema, como no exemplo da Figura 10:

Figura 10 - Detalhes Vulnerabilidades



Fonte: Autoria própria (2016)

Nesse exemplo existe uma vulnerabilidade no Apache, que permite um *heap overflow*, que é um estouro do *buffer* e esse *buffer* pode ser substituído e alocado na memória, utilizando uma rotina como o *malloc POSIX (call)* (www.owasp.org).

5.1.5 Exploração de Falhas

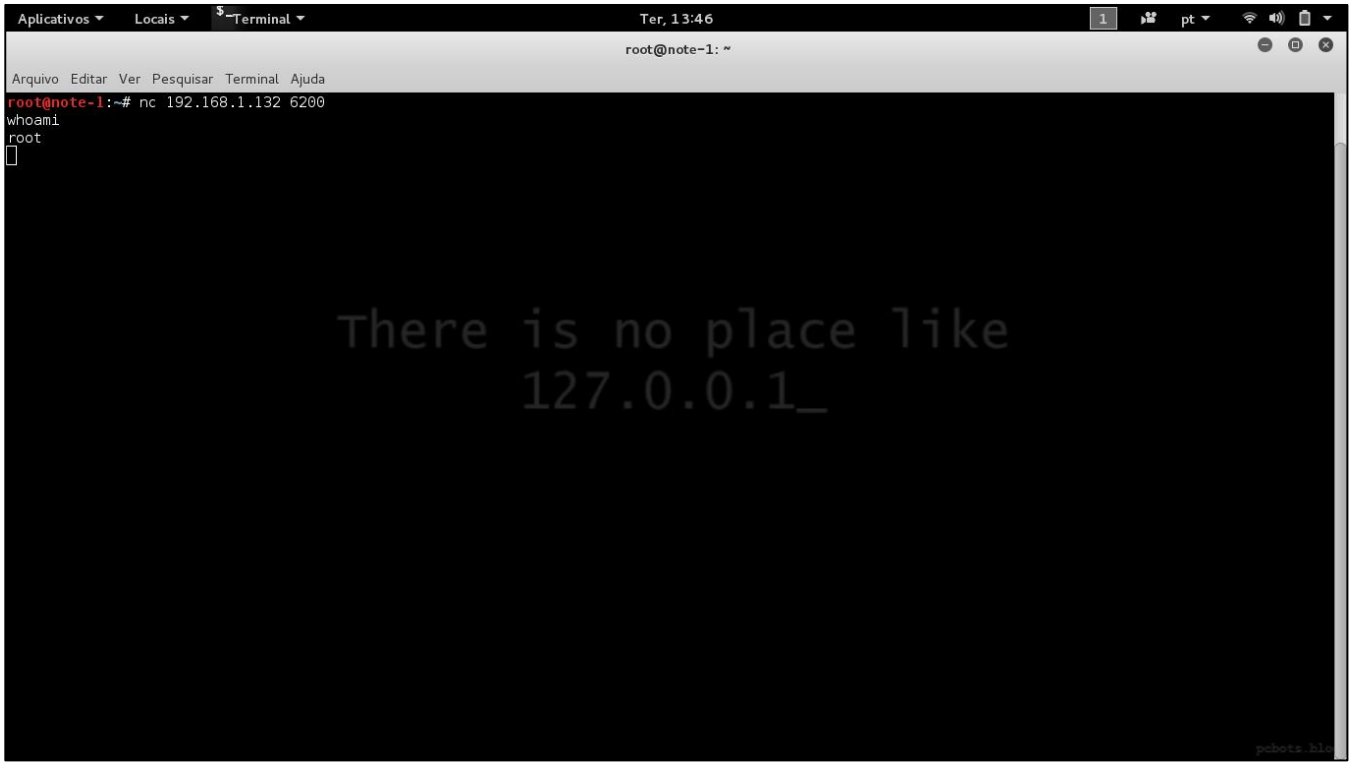
Após ter realizado todas as etapas desde a coleta de informação até o *scanning* de vulnerabilidades, a próxima etapa é a exploração das falhas encontradas anteriormente. Para realizar a exploração das falhas, é necessário utilizar *exploits* que é um programa que explora outro programa (MORENO, 2015, p. 148).

Moreno (2015, p. 148), ainda afirma que a exploração pode ocorrer de duas formas, engenharia social nesse caso o *software* não precisa ter falhas, e a segunda maneira é através de falha no *software* instalado.

No teste realizado no laboratório, foi utilizado a ferramenta Netcat, que se trata de uma ferramenta de rede que escreve e lê dados através de conexões TCP e

UDP (www.netcat.sourceforge.net). Como é possível ver na Figura 11 foi utilizado o comando *nc* 192.168.1.132 6200, o comando nc ativa o programa Netcat, o 192.168.1.132 define a máquina que ele tentará estabelecer a conexão e o 6200 é a porta em que ele se conectará, abaixo segue a imagem ilustrando que o acesso foi bem-sucedido, e que foi possível obter acesso como *root* na máquina Ubuntu:

Figura 11 - Exploração de Falhas



Fonte: Autoria Própria (2016)

E através desse acesso como *root* no sistema, é possível fazer o que desejar dentro do sistema uma vez que este usuário é o administrador da máquina.

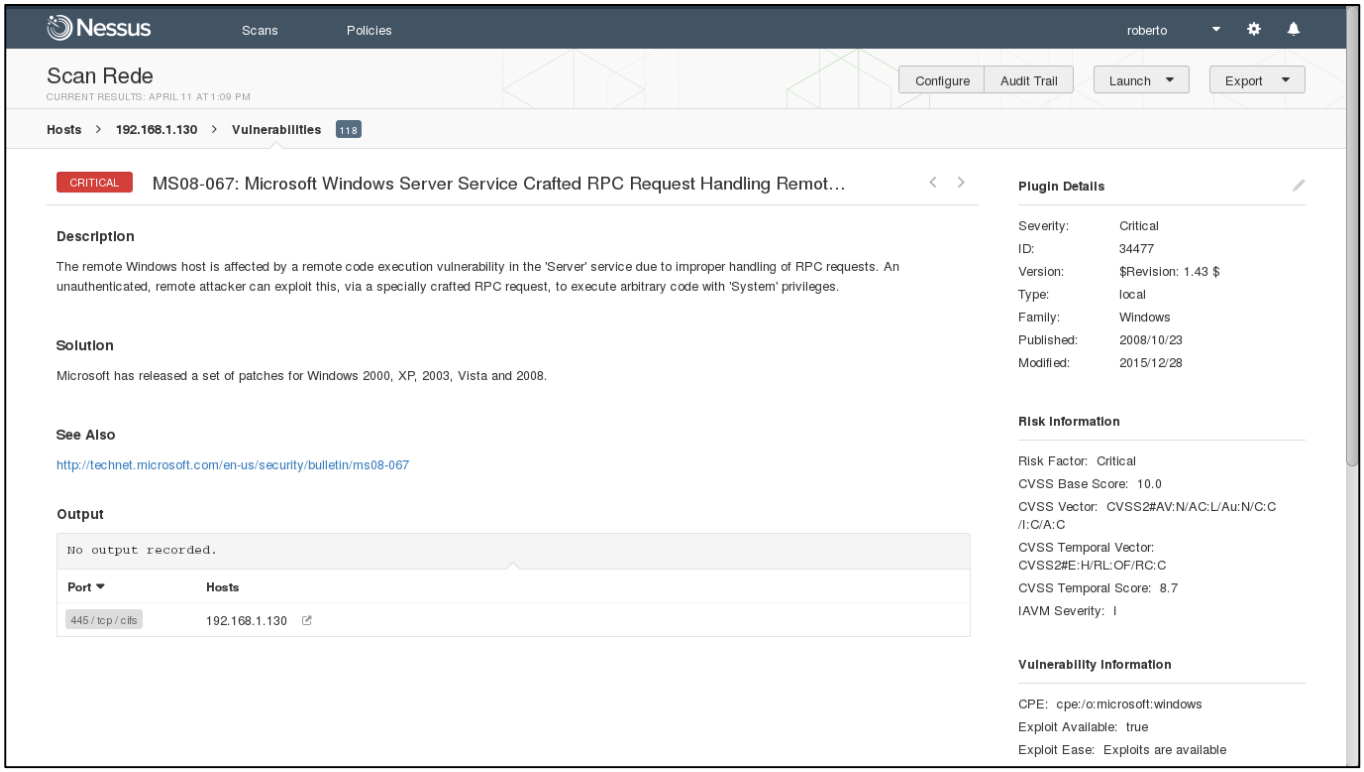
5.1.6 Pós-Exploração

Na fase de pós-exploração está contido o escalonamento de privilégios que se trata em obter acesso como administrador, ou seja, acesso irrestrito ao sistema (MORENO, 2015. p. 195). E segundo Engebretson (2014, p. 258) também consta a

manutenção do acesso através de *backdoors* que permitem o retorno ao sistema posteriormente, mesmo após o sistema alvo ter sido reiniciado.

Para a execução dessa etapa estudo de caso, quando foi realizado o escaneamento de vulnerabilidade, foi detectado que a máquina com Windows XP possuía a vulnerabilidade MS08-67 que permite que um atacante remoto execute código maliciosos com usuário privilegiados, conforme a Figura 12 mostra:

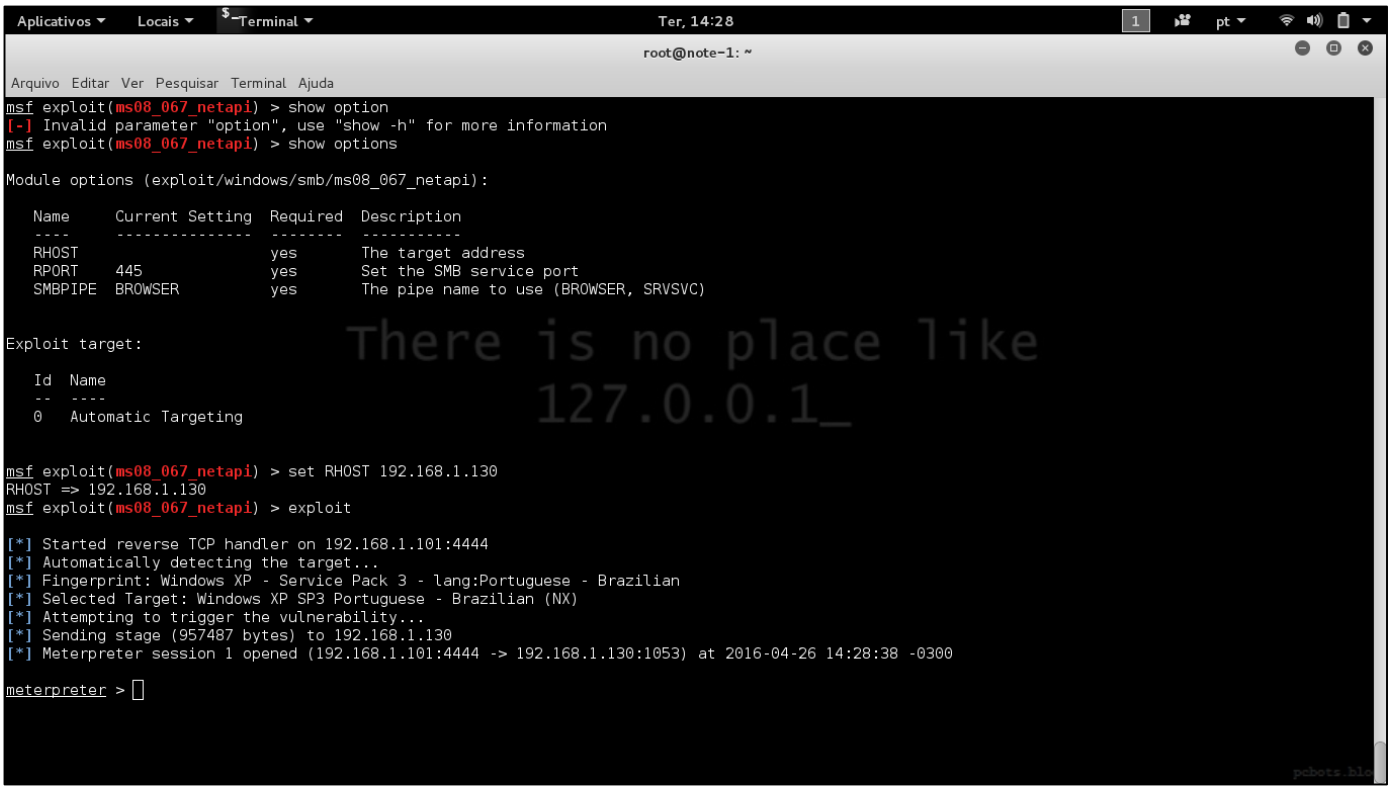
Figura 12 – Vulnerabilidade MS08_67



Fonte: Autoria própria (2016)

Para a exploração dessa vulnerabilidade foi utilizado o Metasploit, que é um *framework* com inúmeras ferramentas para exploração de falhas. Para utilizar essa ferramenta basta abrir o terminal e digitar *msfconsole*, logo uma tela será aberta e lá é possível definir o que será utilizado para explorar a falha encontra, que nesse caso é a MS08-067, a seguir, na Figura 13 está mostrada a tentativa de ataque e a conexão bem-sucedida com a máquina alvo.

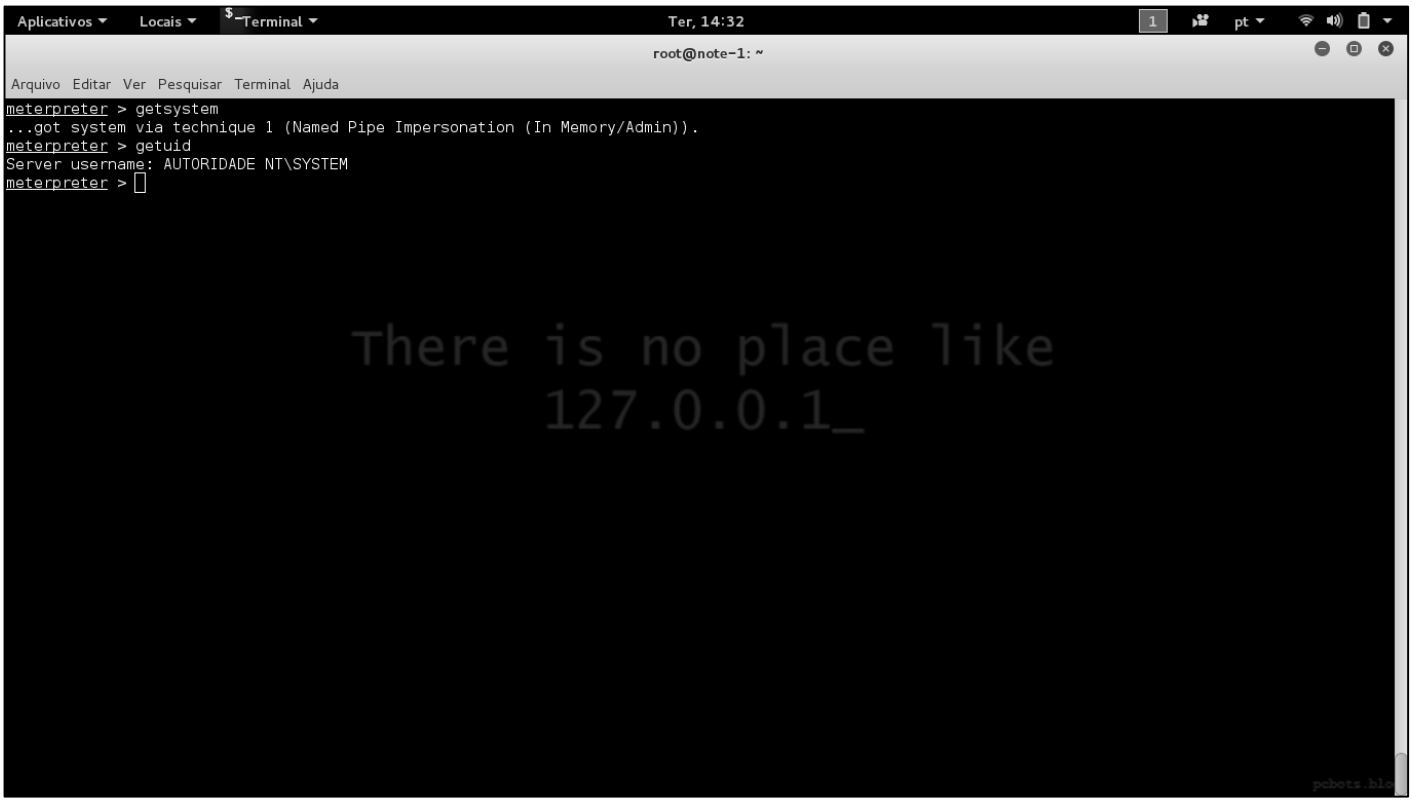
Figura 13 - Exploração MS08-067



Fonte: Autoria própria (2016)

Como é possível ver basta selecionar qual o *exploit* deseja usar, através do comando *use exploit/Windows/smb/ms08_067_netapi*, feito isso basta definir qual alvo atacar utilizando o comando *set* 192.168.1.130, e depois executar o comando *exploit*, onde se inicia a tentativa de se conectar com a máquina alvo, e nesse caso foi estabelecido com sucesso. No entanto, não foi obtido o acesso com usuário privilegiado ao sistema. Para que isso seja possível basta executar o comando *getsystem* onde será executado vários *exploits* até que consiga o acesso privilegiado ao sistema, e para confirma que funcionou corretamente o acesso irrestrito ao sistema basta executar o comando *getuid*, segue a Figura 14 para demonstrar que foi bem-sucedido o ataque e que foi obtido acesso com usuário privilegiado ao sistema.

Figura 14 - Escalonamento de privilégio



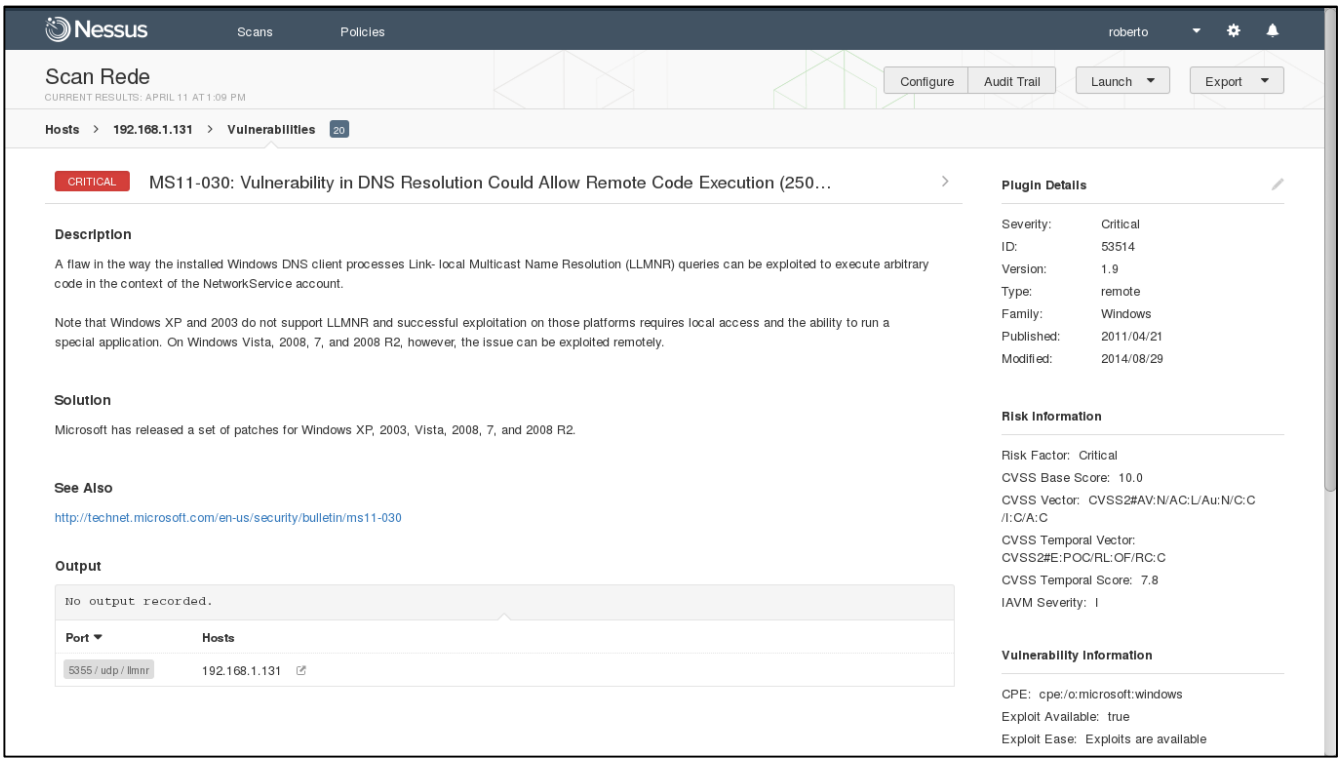
Fonte: Autoria própria (2016)

Após ter obtido acesso como autoridade do sistema, basta instalar um *backdoor* para que seja possível retornar ao sistema posteriormente.

5.1.7 Solução das Vulnerabilidades

Agora que já foi realizado todo o teste de invasão resta apenas gerar o relatório propondo a solução para as vulnerabilidades encontradas, como é possível ver na figura 15, no alvo que está executando o Windows 7 foi detectada a vulnerabilidade MS11-030 que é uma falha na resolução de DNS e que permite que um invasor execute um código malicioso remotamente, para que essa falha seja corrigida é necessário aplicar o *patch* de correção, conforme é informado pelo próprio Nessus que descobriu a vulnerabilidade.

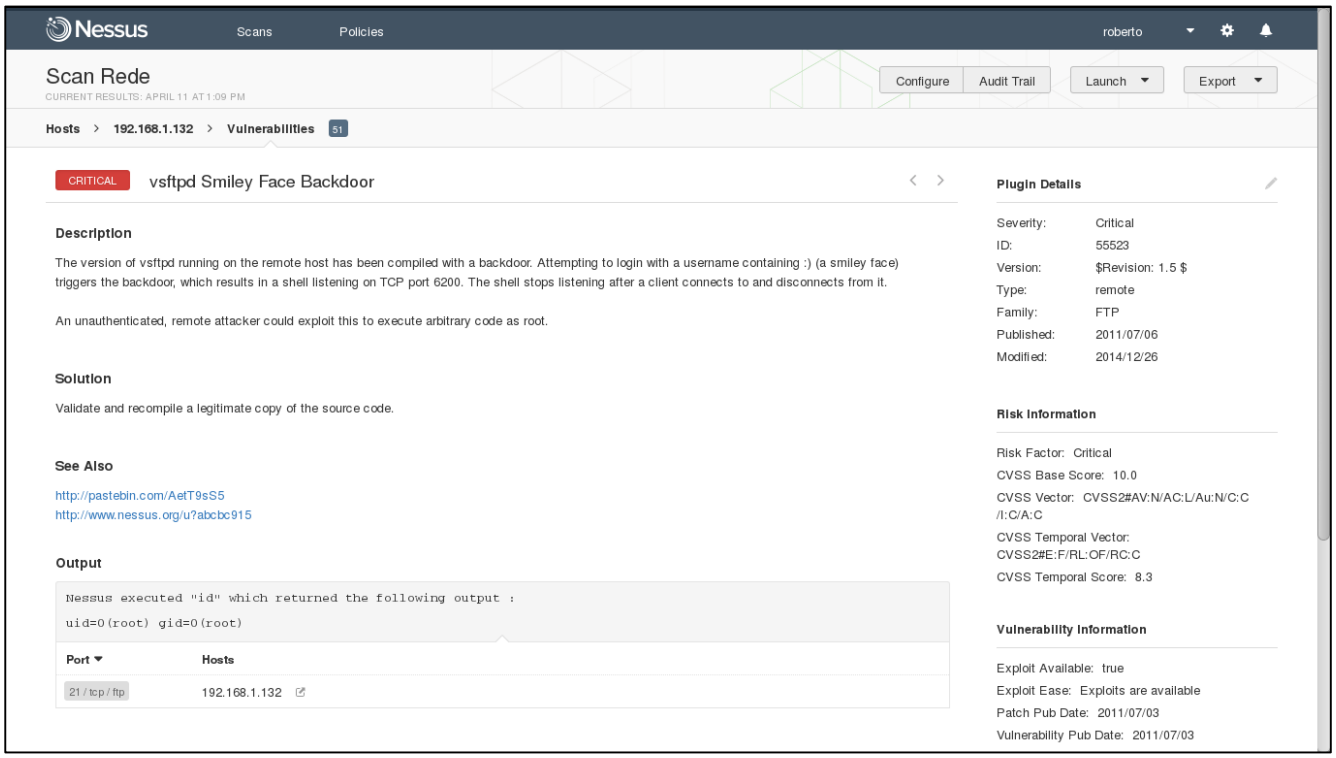
Figura 15 -Vulnerabilidade MS11-030



Fonte: Autoria própria (2016)

Já na máquina alvo executando o Ubuntu, uma das vulnerabilidades encontradas foi a *vsftpd Smiley Face Backdoor*, que se trata de uma versão do vsftpd que foi compilada com um *backdoor* que ao tentar fazer um *login* com qualquer nome de usuário e inserindo um :) (rosto sorridente) logo após o nome, o *backdoor* é ativado e o atacante ganha acesso ao sistema como usuário *root*, a figura 16 mostra os detalhes da vulnerabilidade e a solução possível para esse caso, que seria, recompilar o programa com o código legítimo.

Figura 16 – vsftpd *Backdoor*



Fonte: Autoria própria (2016)

Com base em todas as informações obtidas durante o teste de invasão, é necessário gerar o relatório detalhando toda a metodologia utilizada, quais os computadores estão vulneráveis a ataques, quais as ferramentas utilizadas durante o teste, quais *exploits* foram utilizados, listar todas as vulnerabilidades encontradas e propor a melhor solução para cada uma delas. Dentro desse estudo de caso, em grande parte das falhas encontradas, aplicar um *patch* de atualização ou obter o programa que a máquina utiliza, através de uma fonte confiável, corrigiria as falhas encontradas.

6 CONCLUSÃO

Através do desenvolvimento e dos resultados obtidos através desse trabalho é possível concluir que o processo de *Pentest*, é de suma importância para aumentar o nível de segurança do ambiente de trabalho, pois através dele é possível identificar várias vulnerabilidades, tanto tecnológicas, como também humanas, que poderiam comprometer os três princípios básicos de segurança da informação e ocasionar um grande prejuízo para a organização, uma vez que basta explorar uma falha para que ocorra um incidente de segurança.

Fica claro também que, executar o passo a passo do teste de invasão com cautela, paciência e dedicar o máximo de tempo possível para cada uma delas, buscando sempre obter o máximo de informações resulta em uma chance maior de obter êxito no comprometimento do sistema, que por sua vez, garantirá um melhor resultado para a empresa na hora de mitigar as vulnerabilidades.

Além de definir que o *Pentest* é um processo importante, é fácil afirmar que, a informação deve ser tratada como um bem de extrema valia para a continuidade dos negócios da empresa, pois, caso ela seja perdida ou vaze para os concorrentes, isso causaria um dano enorme para a empresa caso tal informação seja vital para os negócios.

Sugere-se a necessidade de avaliar em trabalhos futuros a mitigação de todas as vulnerabilidades identificadas.

7 GLOSSÁRIO

B

Backdoor – segundo o site www.cert.br, *backdoor* se trata de “ um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim

E

Exploit – Conforme o blog da Kaspersky informa, exploit é “ um aparelho ou método do qual um agressor se aproveita da vulnerabilidade para atingir qualquer tipo de sistema de *hardware* ou *software*.

M

Metasploit – o Metasploit é um framework com um conjunto de dezenas de ferramentas para a exploração de falhas, conforme informa Patrick Engebretson.

N

NMAP – “É uma ferramenta para descoberta de rede e auditoria de segurança”

P

Pentest – Segundo o autor Patrick Engebretson *Pentest* é “ Uma tentativa legal e autorizada de localizar e explorar sistemas de computadores de forma bem-sucedida com o intuito de tornar esses sistemas mais seguros”

8 LISTA DE SIGLAS E ABREVIAÇÕES

DNS - *Domain Name System*

IP - *Internet Protocol*

NMAP - *Network Mapper*

URL – *Uniform Resource Locator*

9 REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Leandro Farias dos Santos. **Segurança da informação nas redes Sociais.** 2011. 55 folhas. Tecnólogo em Processamento de Dados. Faculdade de Tecnologia de São Paulo, São Paulo.

BLOG KASPERSKY. **O que é um Exploit.** Disponível em: <https://blog.kaspersky.com.br/o-que-e-um-exploit/740/>. Acesso em: 29 abril 2016. 14h39m

CARTILHA CERT BR. **Malware.** Disponível em: <http://cartilha.cert.br/malware/>. Acesso em: 29 abril 2016. 14h55m.

ECOMMERCENEWS. **Hackers brasileiros atacam black friday americana.** Disponível em: < http://ecommercenews.com.br/noticias/crimes-noticias-3/hackers-brasileiros-atacam-na-black-friday-americana>. Acesso em: 6 março 2016. 11h57m.

ENGEBRETESON, Patrick. **Introdução ao hacking e aos testes de invasão:** Facilitando o Hacking Ético e os Testes de Invasão. São Paulo: Ed. Novatec, 2014.

FELIPINI, Dailton. **Ecommerce 11 Anos: uma explosão de crescimento.** Disponível em: < http://www.e-commerce.org.br/ecommerce-11-anos>. Acesso em: 6 de março de 2016. 11h25m.

FONTES, Edison, CISM, CISA. **Segurança da informação:** O Usuário Faz Diferença. São Paulo: Ed. Saraiva, 2006.

JULIANO, Ezequiel. **O ciclo de vida da informação.** Disponível em: < http://www.ezequieljuliano.com.br/?p=27>. Acesso em: 7 março 2016. 16h11m.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação.** Rio de Janeiro: Ed. Ciência Moderna, 2009.

MORENO, Daniel. **Introdução ao penteste.** São Paulo, Ed. Novatec, 2015.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos.** São Paulo, Ed. Futura, 2003.

NETCAT. **What is Netcat.** Disponível em: <http://netcat.sourceforge.net/>. Acesso em: 27 abril 2016. 13h59m.

NMAP. **Introduction.** Disponível em: < https://nmap.org/ >. Acesso em: 3 de março de 2016. 16h53m.

OWASP. **Heap overflow.** Disponível em: < https://www.owasp.org/index.php?title=Heap_overflow&setlang=en>. Acesso em: 13 abril 2016. 14h51m.

SÊMOLA, Marcos. **Gestão de segurança da informação:** Uma Visão Executiva. Rio de Janeiro: Ed. Elsevier Brasil, 2003.

TENABLE. **Nessus.** Disponível em: <http://www.tenable.com/pt-br/nessus/>. Acesso em: 3 março 2016. 17h18m.

WEIDMAN, Georgia. **Teste de invasão:** Uma Introdução Prática ao Hacking. São Paulo: Ed. Novatec, 2014.