FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Ícaro José Vilches Rodrigues

ESCANEAMENTO DE REDES DE COMPUTADORES:

Análise de Viabilidade com a Ferramenta NMAP

Americana, SP

2015

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Ícaro José Vilches Rodrigues

ESCANEAMENTO DE REDES DE COMPUTADORES:

Análise de Viabilidade com a Ferramenta NMAP

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do Prof.(o) Esp. Rogério Nunes de Freitas.
Área de concentração: Segurança da Informação.

Americana, SP

2015

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

Rodrigues, Ícaro José Vilches
R613e Escaneamento de redes de computadores: análise de viabilidade com a ferramenta NMAP. / Ícaro José Vilches Rodrigues. – Americana: 2015.
63f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Esp. Rogério Nunes de Freitas

1. Segurança em sistemas de informação I. Freitas, Rogério Nunes de II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Ícaro José Vilches Rodrigues

ESCANEAMENTO DE REDES DE COMPUTADORES:

Análise de Viabilidade com a Ferramenta NMAP

Trabalho de conclusão de curso apresentado à Faculdade de Tecnologia de Americana como parte dos requisitos para obtenção do título de Tecnólogo em Segurança da Informação.
Área de concentração: Segurança da Informação.

Americana, 07 de dezembro de 2015.

Banca Examinadora:

Rogério Nunes de Freitas
Especialista
Faculdade de Tecnologia de Americana

Aloísio Vendemiatti
Mestre
Faculdade de Tecnologia de Americana

Benedito Aparecido Cruz
Especialista
Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Ao meu orientador Prof.(o) Esp. Rogério Nunes de Freitas, pelo acompanhamento, sugestões e discussões ao longo deste trabalho.

Aos professores que foram tão importantes e que dedicaram seu esforço promovendo conhecimento em toda a vida acadêmica.

Aos amigos que apoiaram e incentivaram na produção deste trabalho.

A todos que direta ou indiretamente fizeram parte de minha formação.

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus por ter permitido conquistar meus objetivos. Em especial aos meus pais, que sempre me incentivaram em todos os momentos e o apoio dado durante toda a minha vida acadêmica, compreendendo nos momentos de ausência. A toda minha família, que sempre motivou meu crescimento pessoal e profissional.

RESUMO

Com o crescente aumento do acesso à Internet e à novas tecnologias, surge a necessidade de proteger os dados que são armazenados em uma rede de computadores. Neste trabalho conheceu-se algumas ferramentas para a exploração de vulnerabilidades, hoje disponibilizadas em sua grande maioria de forma gratuita, visam fornecer informações relevantes para a definição de medidas a serem adotadas, com o propósito de proteger estes dados. Estas ferramentas efetuam o escaneamento da rede à procura de portas vulneráveis, que com técnicas hackers, um invasor conseguirá facilmente explorar os dados da organização. A importância de uma auditoria bem realizada, coletando o máximo de conteúdo sobre possíveis falhas de segurança, visando promover controles e metodologias que serão adotadas constantemente pela organização. Pesquisado como são executados os testes de invasão e sua finalidade na obtenção de resultados que auxiliarão o administrador de redes nas tomadas de decisão quando exploradas estas vulnerabilidades. A rápida resposta a estes incidentes é de grande valia e contando com o auxílio da ferramenta NMAP, coleta um conjunto de informações, efetuando um escaneamento em toda a rede de computadores em busca de portas vulneráveis, que podem se tornar uma brecha, proporcionando a um invasor o acesso indevido aos dados. É demonstrado a utilidade da busca pelas portas potencialmente desprotegidas e com a utilização de pequenas medidas, como a utilização de firewalls, podem tornar a rede em questão mais segura e eficiente.

Palavras-chave: NMAP, Escaneamento de Redes, Vulnerabilidades.

ABSTRACT

With the increasing access to the Internet and new technologies, there is the need to protect the data that is stored on a computer network. In this work meet some tools for the exploitation of vulnerabilities, nowadays mostly available free, aim at providing relevant information for defining measures to be adopted to protect this data. These tools perform the scan search for vulnerable ports in the network, using hackers techniques, can easily exploit the organization's data. The importance of a well performed audit, collecting as much content about possible security breaches as possible, in order to promote controls and methodologies to be adopted consistently throughout the organization. Studied how penetration tests are run and their purpose in achieving results that assist the network administrator in decision-making when exploited these vulnerabilities. The quick answer to these incidents is of great value and relying on the help of NMAP tool, it collects a set of information, performing a scan on the entire network of computers for vulnerable ports, which can become a loophole by providing an unauthorized access to data attack. It demonstrated the usefulness search for potentially unprotected ports and with use of small measures, like the use of firwalls, can make the network safer and more efficient.

Keywords: *NMAP, Network Scanning, Vulnerabilities.*

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

ABNT: Associação Brasileira de Normas Técnicas

ACK: Acknowledgment

BIT: *Binary Digit*

COBIT: *Common Objectives for Information and Related Technology*

DHCP: *Dynamic Host Configuration Protocol*

DNS: *Domain Name Service*

FIN: *Finalize*

FTP: *File Transfer Protocol*

GB: *Gigabit*

HD: *Hard Disk*

HTTP: *Hypertext Transfer Protocol*

HTTPS: *Hypertext Transfer Protocol Secure*

IAB: *Internet Architecture Board*

IDS: *Intrusion Detection System*

IEC: *International Electrotechnical Commission*

IP: *Internet Protocol*

IPP: *Internet Printing Protocol*

ISO: *International Organization of Standardization*

ITIL: *Information Technology Infraestructure Library*

MAC: *Media Access Control*

MB: *Megabit*

MICROSOFT-DS: *Microsoft Domain Service*

MS: *Microsoft*

MS-SQL SERVER: *Microsoft Structured Query Language Server*

MSRPC: *Microsoft Remote Procedure Call*

NETBIOS: *Network Basic Input/Output System*

NMAP: *Network Mapper*

OS: *Operational System*

PC: *Personal Computer*

POP3: *Post Office Protocol 3*

PRO: *Professional*

RAM: *Random Access Memory*

RST: *Reset*

SMTP: *Simple Mail Transfer Protocol*

SNMP: *Simple Network Management Protocol*

SSH: *Secure Shell*

SYN: *Synchronize*

TCP: *Trasmission Control Protocol*

TCP/IP: *Trasmission Control Protocol / Internet Protocol*

UDP: *User Datagram Protocol*

SUMÁRIO

1 INTRODUÇÃO

O tema segurança da informação tem se tornado cada vez mais difundido e os meios de proteção têm aumentado consideravelmente, e “não é novidade que o acesso à tecnologia da informação e à inclusão digital aumentam a cada dia que passa” (GIAVAROTO, SANTOS, 2013, p.1).

Com este avanço tecnológico, existe a necessidade de se precaver e resguardar as informações, principalmente em ambientes corporativos, conforme Stallings (2007, p.4) revela em sua pesquisa, a “Internet precisa de mais e melhor segurança”. Giavaroto e Santos (2013), também destacam a importância de se manter a segurança dos dados, surgindo várias ferramentas que visam fornecer ao usuário mais proteção em seus dados digitais.

O escaneamento de redes de computadores ou *network scanning*, são testes que procuram identificar as vulnerabilidades em uma rede de computadores, e se tornaram uma estratégia fundamental na descoberta de falhas em um ambiente computacional. Utilizando métodos de testes de invasão - também conhecidos como *penetration testing*, onde este processo executa tarefas, com o objetivo de “sondar as vulnerabilidades, bem como oferecer ataques que funcionem como prova de conceito para demonstrar que eles são reais” (ENGEBRETSON, 2014, p.23).

O **tema** deste trabalho é explorar os conceitos básicos de segurança da informação, apresentar algumas ferramentas primordiais nestes escaneamentos e dentre elas, utilizar do NMAP (*Network Mapper*), criada por Gordon “Fyodor” Lyon, definida como utilitário gratuito na aplicação em redes de computadores, com o propósito de explorá-la e auditá-la, capaz de verificar e apontar vulnerabilidades existentes, fornecendo ao administrador de redes dados onde apontem falhas a serem corrigidas.

O profissional utiliza alguns métodos “que permitem aos especialistas técnicos simularem as ações e as técnicas usadas por um ou mais *hackers*[1] na tentativa de explorar as falhas de uma rede ou de um sistema de informação” (BROAD, BINDNER,

[1] *Hacker*: Pessoa que tenta acessar sistemas sem autorização, usando técnicas próprias ou não, no intuito de ter acesso a determinado ambiente para proveito próprio ou de terceiros. Dependendo dos objetivos da ação, podem ser chamados de *Cracker*, *Lammer* ou *BlackHat*. (ABNT NBR ISO/IEC 27002, 2013, p.viii).

2014, p.18), tendo condições de fornecer contramedidas, evitando que, em caso de invasão, estas brechas beneficiem e sejam exploradas pelo invasor.

O **problema** abordado trata da segurança e confiabilidade no uso de ferramentas de varreduras, realizando uma análise de viabilidade com NMAP e localizando a vulnerabilidade contida nela. Destaca-se que as análises por meio de "uma avaliação de vulnerabilidades correspondem ao processo de analisar serviços e sistemas em busca de problemas de segurança" (ENGEBRETSON, 2014, p.24), o autor ainda alega que o teste de invasão "realmente executa explorações de falhas". Com isso, a **pergunta** que se destacou é: existe a possibilidade de garantir segurança dos dados da empresa, fornecendo dados satisfatórios e confiáveis, para evitar a perda de informações? Algumas **hipóteses** foram consideradas:

a) A utilização do NMAP para estas análises apresenta resultados confiáveis ou inconclusivos?

b) Qual a importância e a eficiência na utilização de ferramentas de prevenção a ataques na rede?

O **objetivo geral** deste trabalho é analisar as técnicas e metodologias utilizando ferramentas de identificação de vulnerabilidades e ameaças em um ambiente de redes.

O **objetivo específico** é explicar conceitualmente os tipos de testes de invasão utilizados com a ferramenta NMAP, onde compreendeu-se os métodos utilizados, além da reprodução de um ambiente controlado de testes para mostrar as vulnerabilidades encontradas semelhante às ações de um *hacker*. Com os dados obtidos realizou-se uma análise objetiva quanto às técnicas utilizadas apontando sua confiabilidade e efetividade.

O desenvolvimento deste trabalho **justificou-se** diante dos danos ocasionados para as empresas, nas quais as vulnerabilidades foram identificadas e exploradas, onde, conforme destacado por Giavaroto e Santos (2013), se torna extremamente difícil calcular os danos que estes ataques podem causar a uma organização. Propôs-se o estudo para ambientes de redes de computadores, analisando se estão em conformidade com as normas estabelecidas e utilizando a ferramenta NMAP, considerando que esta ferramenta é capaz de verificar a rede à procura de

vulnerabilidades em portas comuns e protegê-la, proporcionando o aumento da segurança das informações.

Utilizou-se o **método** de abordagem hipotético dedutiva, levando em consideração o objetivo de explicar o conteúdo proposto, utilizando métodos de procedimentos, apresentando as técnicas utilizadas nos testes de invasão e compreendendo-as de modo a expor as vulnerabilidades da empresa. Estes procedimentos foram divididos em três etapas onde, para o conhecimento histórico foi pesquisado, conhecido e identificado os métodos para a análise de vulnerabilidades, assim como a exploração teórica da ferramenta NMAP. Em seguida efetuou-se uma análise de viabilidade, com o propósito de representar um ambiente de testes, executando algumas tarefas. Com isso, foram analisados os resultados obtidos, para conseguir as respostas buscadas nos objetivos específicos deste trabalho. Foi utilizada uma pesquisa aplicada, buscando pelas soluções dos problemas específicos, analisando os resultados e descrevendo-os para a melhor compreensão do cenário explorado. Os procedimentos técnicos tiveram como apoio materiais bibliográficos que incluíram: livros, artigos e projetos de pesquisa relacionados ao tema, estudando-os e conhecendo as técnicas utilizadas para os testes de invasão. A obtenção de dados foi efetuada de forma documental bibliográfica, buscando informações relevantes para a pesquisa, e de análise de conteúdo de toda a documentação coletada durante a elaboração do trabalho.

Os capítulos estão organizados da seguinte maneira:

No capítulo a seguir foram abordados os conceitos básicos de segurança da informação e auditoria em sistemas de redes de computadores, em seguida no capítulo 3 são abordadas as ferramentas e as metodologias utilizadas no escaneamento de uma rede de computadores, no capítulo 4 é apresentada a análise de viabilidade utilizando a ferramenta NMAP e os escaneamentos realizados em um ambiente de testes, por fim é verificado e apontado as considerações finais sobre o estudo realizado com a ferramenta proposta.

2 SEGURANÇA EM REDES DE COMPUTADORES

A segurança da informação tem se tornado primordial nos dias atuais onde, “independente do estágio de tecnologia da organização, a proteção da informação deve ser uma das preocupações” (FONTES, 2006, p.6). Neste capítulo analisou-se os conceitos básicos de segurança da informação e sua importância para a proteção destes dados, assim como definições e contextos entre ameaças e vulnerabilidades, princípios de auditoria e as metodologias utilizadas para a verificação do ambiente de redes, com o propósito de identificar falhas que possam ser exploradas por um invasor.

2.1 Segurança da Informação

Toda informação seja ela em formato físico ou eletrônico, é de grande importância para negócios ou pessoas, sendo assim, ela precisa ser protegida adequadamente. A infraestrutura onde armazena-se estas informações, tem ganhado destaque na medida em que a tecnologia avança e é relatada por Stallings (2007), que deixa claro, a imprescindível utilização de mecanismos e ferramentas, capazes de proteger todo o tipo de arquivo armazenado em meios eletrônicos. Ele complementa ainda que, de acordo com pesquisa realizada em 1994 pelo IAB (*Internet Architecture Board*), destacava-se a necessidade de proteger toda a infraestrutura de redes de computadores utilizando meios de autenticação mais eficientes e seguros.

Para as organizações a informação é um bem de valor e primordial no crescimento da empresa, com isso, a criação de regras e políticas de segurança devem ser adequadas a estrutura e o tipo de negócio. As normas técnicas brasileiras, representadas pela Associação Brasileira de Normas Técnicas – ABNT (2005), no que diz respeito às definições de segurança da informação ressalva que, com o “aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades” (ABNT ISO/IEC 17799, 2005, p.IX). A norma foi elaborada em 2005 utilizando a numeração 17799, sendo que em 2007, foi incorporada a uma nova numeração, passando a se chamar ISO/IEC 27002. Sua versão mais recente disponibilizada no mercado e atualmente em vigor é a de

2013 onde, fornece diretrizes e orientações de melhores práticas para a segurança da informação. A norma ainda define que segurança da informação é preservar os dados, também chamados de ativos e baseia-se em três princípios básicos:

- **Confidencialidade;**
- **Integridade;**
- **Disponibilidade.**

A Figura 1 exibe os princípios básicos de segurança da informação:

Figura 1 - Princípios básicos da segurança da informação

Fonte: Baseado em Goodrich e Tamassia (2013, p.3)

Conforme orienta Fontes (2006, p.11), estes princípios visam garantir:

- **Confidencialidade:** a informação precisa estar disponível às pessoas adequadas e com a devida autorização de usá-las. A melhor forma é fornecer ao usuário controles de acesso para que a informação não seja acessada por todos do ambiente de redes. A confidencialidade é violada quando informações são manipuladas e extraviadas prejudicando a organização. Existe a falha da confidencialidade quando um usuário não autorizado consegue acessar informações que não lhe são cabíveis.

- **Integridade:** visa garantir que a informação que chega ao destinatário, não tenha sofrido modificações ou violações do conteúdo. Os dados são íntegros e verdadeiros ao ponto que as tomadas de decisões não sejam comprometidas por dados incorretos ou manipulados. Informações não íntegras são aquelas que por alguma razão foram alteradas sem a devida autorização.
- **Disponibilidade:** toda a informação precisa estar disponível para o usuário sempre que necessário, evitando que o fluxo de desenvolvimento da organização seja comprometido. Ocorre a indisponibilidade de dados quando possíveis falhas no sistema prejudicam o acesso às informações e por ventura causam prejuízos a empresa.

Destaca-se a importância de que esta informação precisa ser legal, de acordo com as leis vigentes e princípios éticos, necessita ser catalogada e não ser repudiada pelo usuário, negando sua auditoria.

Fica evidenciado a necessidade de fornecer medidas preventivas para que a informação, que tem um valor importantíssimo para a organização, não seja perdida ou furtada. Para garantir a continuidade do negócio, ações devem ser tomadas evitando que o mesmo seja impactado, fazendo com que sofra perdas relevantes e que quando bem preparadas, se recuperem rapidamente em comparação com outras que não possuem um plano adequado de prevenção.

Segundo Dawel (2005, p.66), “na prática é impossível prever todas as possibilidades de fraudes e ataques contra a empresa”, porém, a que se prepara para estas invasões, atenuam os problemas e tendem a resolvê-los mais rapidamente. Contramedidas bem elaboradas e analisadas, levam o invasor a se desencorajar do ato fraudulento. Ele destaca ainda o fato destas empresas, que adotam medidas para o conhecimento das vulnerabilidades do ambiente, utilizando-se de ferramentas e métodos para a identificação de falhas em sua rede de computadores, são consideradas proativas.

Estas medidas de segurança em geral visam garantir que as informações estejam íntegras no acesso interno do ambiente da empresa, e que em pesquisa divulgada por analistas de mercado, e demonstrada por Dawel (2005, p.24), revelando que “84% dos incidentes de segurança vêm de dentro da empresa”, porém com o crescente aumento do uso da Internet, este ambiente tem se tornado extremamente vulnerável a ataques externos e é evidenciada por Stallings (2007) que estes ataques,

principalmente nos que possuem seus sistemas conectados à Internet, se tornam cada vez mais aprimorados.

Segundo Fontes (2008), as medidas criadas pela empresa visam esclarecer usuários das diretrizes da organização e quais ações serão tomadas em função do ato que poderá causar danos. Ele destaca a importância da conscientização do usuário de respeitar estas medidas e procurar atendê-las no decorrer do seu trabalho. Assim como, é extremamente necessário que estas diretrizes sejam bem esclarecidas e contar com um trabalho de divulgação constante, evitando assim que o usuário caia na rotina diária do seu trabalho e deixe-as de lado. O profissional responsável pela segurança dos dados da empresa, deve estar alinhado às práticas e aos padrões estabelecidos por órgãos competentes, dos quais se destacam o COBIT, o ITIL e a Norma NBR ISO/IEC 27002.

As diretrizes de segurança devem ser aplicadas por profissional da área e que tenha um conhecimento das questões técnicas de TI - Tecnologia da Informação. Porém é fundamental que o usuário adote as medidas propostas e utilize-as de forma correta, para que o trabalho do técnico e a segurança dos dados da organização não sejam comprometidas. Fontes (2008, p.123) destaca alguns exemplos de ações cometidas pelo usuário que afetam o desempenho das medidas adotadas:

- A mesma senha de acesso compartilhada por vários usuários;
- Arquivos pessoais nas pastas de compartilhamento da empresa;
- Os usuários não correspondem da maneira emergencial que um plano de desastres estabelece, conforme planejamento e treinamentos realizados;

E seguindo esta linha de processos, determina-se alguns aspectos do qual garante-se às medidas de segurança adotadas, que elas cumpram os requisitos primordiais dos pilares da segurança da informação. São elas:

- **Acesso à Informação:** Fornecer ao usuário o acesso às informações que lhe é cabível determinada pelo Gestor da Informação;
- **Conscientização em Segurança da Informação:** Orientar o usuário nas adequações, medidas e normas a serem seguidas, respeitando as diretrizes de segurança estabelecidas e devem ser efetuadas periodicamente para que se tornem mais eficazes;
- **Plano de Continuidade de Negócio:** As participações dos usuários em cooperar nos testes dos planos de contingência, tornam efetivos as ações a

serem tomadas quando necessário, de forma eficiente e precisa, minimizando contratempos;

- **Serviços de Suporte ao Monitoramento do Sistema:** Manter o usuário informado das medidas de segurança provem resultados significativos no restabelecimento do problema ou atém mesmo a eliminação deles;
- **Definição das Cópias de Segurança:** Visa orientar o usuário nas adequações e frequência com que os backups são realizados.

Contudo, se estes procedimentos não são seguidos pelo usuário do sistema, de nada adianta um programa de medidas e controles de segurança das informações, pois serão comprometidos e os dados estarão vulneráveis da mesma forma. Sendo assim, o empenho dos profissionais de informática e consequentemente as medidas adotadas por eles, sejam com atos preventivos, auditorias periódicas e claro, os testes de invasão, utilizando-se de ferramentas ótimas e bem configuradas - que são o destaque deste trabalho – contudo, somente elas, não serão suficientes para garantir a segurança dos dados de uma organização.

2.2 Ameaças, Vulnerabilidades e Testes de Invasão

As medidas de prevenção são pontos importantes dentro de uma organização conforme citado anteriormente, mas o quão provável a empresa estará vulnerável e sofrerá das ameaças no seu ambiente computacional? A probabilidade de acontecer uma invasão e a perda de um ativo, está diretamente ligada às ameaças que podem ser sofridas e o nível de vulnerabilidade do qual ela está sujeita. Conforme define Lyra (2008, p.6) a probabilidade “é a chance de uma falha de segurança ocorrer levando em conta as vulnerabilidades do ativo e as ameaças que venham a explorar esta vulnerabilidade”. A ameaça conforme orienta Stallings (2007, p.6), é o “potencial para a violação da segurança quando há uma circunstância, capacidade, ação ou evento que pode quebrar a segurança e causar danos” e está diretamente ligada às vulnerabilidades, definidas como “fraquezas que podem gerar, intencionalmente ou não, a indisponibilidade” (LYRA, 2008, p.6) e consequentemente, afetar os pilares da segurança da informação.

É destacado por Broad e Bindner (2014) que, analisar as vulnerabilidades em uma rede é avaliar se as configurações utilizadas pela empresa na prevenção de

invasões e ataques estão disponíveis na política de segurança. Ela pode englobar parte ou toda a equipe responsável pela análise. É avaliado também se os controles de segurança adotados seguem os padrões estabelecidos pelas normas vigentes, onde destaca-se a principal delas, a ISO/IEC 27001/2013, sendo esta a última versão lançada, que regulamenta as medidas a serem adotadas para manter a segurança no ambiente da empresa, sendo assim, os testes de invasão são considerados parte dos controles de segurança.

Os danos relacionados à rede de computadores de uma organização são chamados de incidentes de segurança, e conforme destaca Lyra (2008), poderá causar interrupções em toda a infraestrutura da empresa, seja na perda de dados, ativos de informação ou bens materiais. Estas ameaças existem e são possíveis de serem detectadas, sendo assim, aciona-se medidas preventivas para evitar prejuízos maiores. Os ataques a segurança da informação, explorando as vulnerabilidades podem ocorrer de várias formas, desde o acesso de um funcionário a dados que estão em uma empresa de diferentes formas (documentos, arquivos, comprovantes), um visitante que consegue acesso à rede, podendo explorar mapeamentos e servidores disponíveis aos funcionários, e com a falta de uma política de acesso aos dados, eles estão disponíveis a todos da rede.

Leva-se em conta também, as várias outras formas de acesso que a Internet proporcionou, conforme citado por Giavaroto e Santos (2013, p.2):

> Diante de novas tendências, táticas de invasões e da rapidez com que se move o mundo digital, é de suma importância que administradores de redes ou sistemas tenham em mente que “*blackhats*” estão em constante evolução e são inúmeros os métodos utilizados nas práticas de invasões.

E com todos estes novos meios para se invadir e se apossar de informações, na maioria das vezes em benefício próprio, destacam-se os *black hat´s* (chapéu preto), intitulados pelos meios de informação como *hackers*.

Os termos utilizados para definir estes invasores ganham várias definições, sendo importante destacar a diferença entre eles, conforme definido por Engebretson (2014), o *black hat*, também conhecido como *cracker* ou invasor malicioso é o indivíduo que utiliza de seus conhecimentos avançados para explorar dados e informações em privilégio próprio, já o *white hat*, ou *hacker* ético, são pessoas com os mesmos conhecimentos que um *cracker* e as técnicas utilizadas por eles, porém,

utilizam dos meios legais para explorar as vulnerabilidades de um ambiente de redes, fornecendo relatórios que serão usados na criação de diretrizes e medidas de prevenção da organização. Estes testes invasivos no sistema, com o consentimento da empresa são chamados de *pentesting* ou *penetration testing,* os testes de invasão e é justamente esta autorização que diferencia os *white hat´s* dos *black hat´s.* O autor cita que “uma vez obtida a autorização, tanto o *pentester* quanto a empresa sujeita à auditoria devem concordar em relação ao escopo do teste” (ENGEBRETSON, 2014, p.26). Este escopo definido, aponta explicitamente o que será executado, o que está incluso no teste e quais setores e alvos estão envolvidos, devendo-se respeitar os limites impostos previamente.

Os testes de invasão, conforme definidos por Broad e Bindner (2014), são métodos e procedimentos de varredura em um ambiente de redes ou sistemas computacionais, sempre de acordo com as normas estabelecidas e diretrizes aprovadas em comum acordo entre os responsáveis pela organização, com o objetivo de descobrir as falhas existentes neste ambiente, burlando as medidas de segurança já aplicadas, identificando assim se são eficientes ou as mesmas possuem falhas.

Alguns termos são utilizados quando se coloca em prática um teste de invasão, como os já citados anteriormente *black hat* e *white hat*, e diversos outros conforme definidos por Broad e Bindner (2014, p.20-24) a seguir:

- ***Red Team* (Equipe Vermelha):** São equipes em geral maiores que os responsáveis pelos testes de invasão e tem como objetivo central descobrir as vulnerabilidades de segurança contidas na empresa. As técnicas utilizadas são extremamente próximas das quais um *cracker* utilizaria para atacar, e na maioria das vezes, poucas pessoas sabem quando e como a empresa será atacada por esta equipe.
- ***Hacking* Ético:** Definido como um *pentester*, ou pessoa contratada para executar e explorar o ambiente com o consentimento do proprietário da empresa, fornecendo posteriormente dados que serão utilizados como medidas de prevenção em caso de ataques ou invasões reais. Ele utiliza de todas as técnicas que um *cracker* utilizaria, porém com propósitos diferentes.
- **Teste de Usuário Malicioso:** Este teste simula um indivíduo que representaria confiança dentro de uma empresa e utilizando de seu acesso privilegiado, efetua testes para alterar os mais diversos tipos de controles que sua conta pudesse oferecer, tais como, alterar seu nível de acesso, controle de contas de

outros usuários, acesso e alteração de documentos até então restritos à diretoria, dentre muitas outras ações a fim de simular um ataque real.

- **Engenharia Social:** É o modo que o atacante age para conseguir informações de usuários, de maneira a convencê-los a fornecer dados de uso pessoal ou somente no ambiente interno da empresa. Com estas informações ele procura corromper dados ou se apossar dos mesmos buscando benefícios próprios.
- ***Phishing* e *Spear Phishing*:** São técnicas de engenharia social para comprometer o acesso e os dados de um determinado usuário. Ele normalmente tenta forçar o mesmo a fornecer senhas, dados bancários, entre outros, seja em contato direto ou através de e-mails, *links* e sites falsos. Funcionários de uma empresa podem ser abordados para efetuarem a troca de senhas ou até mesmo fornecê-las, posteriormente se infiltrar no ambiente com os dados de *log-on*[2] e senha de acesso diário, acessando informações que podem ser usadas pelo invasor.
- ***Gray Hat*:** São pessoas que normalmente utilizam das técnicas que um *black hat* utilizaria, porém com o intuito de alertar as falhas de segurança contidas em um ambiente, eles não possuem permissões para executar tais ações e nem procuram obter benefícios próprios com os resultados obtidos.

2.3 Metodologias de Auditoria

Antes de se iniciar um teste de invasão são definidas as diretrizes deste teste e qual será sua abrangência, delimitando assim as metodologias utilizadas na auditoria do sistema ou ambiente de redes em questão. Algumas fases fazem parte deste projeto e devem ser respeitadas as normas em vigor. Seguindo as orientações de Lyra (2008, p.109-115), destaca-se a seguir as fases mais importantes de todo o processo de realização da auditoria:

- É necessário que seja estabelecido pela organização qual a abrangência do teste contratado e qual a sua finalidade, deverá ser criado grupos responsáveis por cada fase da auditoria, onde é destacado por ele dois grupos: o de coordenação e o de execução. O grupo da coordenação definiria com detalhes

[2] *Log-on*: processo de identificação e autenticação de um usuário para permitir o seu acesso a um sistema. (ABNT NBR ISO/IEC 27002, 2013, p.viii).

os procedimentos e métodos a serem utilizados e caberia ao grupo de execução respeitar e executar as solicitações do primeiro grupo.

- Identificar e detalhar o escopo, visando coletar informações precisas do sistema a ser auditado, efetuar o levantamento detalhado dos dados com o intuito de otimizar os recursos envolvidos.
- Efetuar um inventário de quais medidas devem ser adotadas, quais os pontos fracos da organização, apontar claramente as vulnerabilidades encontradas nestes pontos e fornecer de forma documental a maior e mais detalhada quantidade de dados ao grupo que se encarregará da execução da auditoria.
- Apontar nos relatórios qual o grau de risco existente no ponto em questão, quais as ameaças e se existem vulnerabilidades a serem exploradas.
- Durante o processo de auditoria documentar quais as técnicas e ferramentas utilizadas para a descoberta ou análise da falha encontrada
- Elaborar um relatório detalhado com os resultados encontrados e apontar melhorias e ações para os pontos que apresentaram vulnerabilidades para a empresa.

Contudo é importante destacar os métodos utilizados no processo de execução da auditoria em questão, apontando as diferenças de testes e quais as finalidades do mesmo para a organização.

No caso dos testes de invasão eles são definidos como caixa branca (w*hite box*) e caixa preta (*black box*). Engebretson (2014) explica que o teste do tipo caixa branca é extremamente detalhista e abrange a organização inteira para coletar as informações necessárias. O responsável pela análise procura explorar todo o tipo de vulnerabilidade encontrada, porém como ele não tem o intuído de ser discreto nesta avaliação, alguns resultados poderão ser comprometidos, pois lhe é permitido acesso sem restrição ou bloqueio algum ao sistema, se beneficiando da utilização de brechas que um *hacker black hat* não teria, sendo assim, não se comparando a um ataque real. Já o teste do tipo caixa preta, o autor aponta que são fiéis aos ataques reais, pois utiliza das técnicas que um *hacker* malicioso teria em mãos, visando explorar vulnerabilidades específicas da rede. Ele explora o ambiente da mesma maneira que um *black hat* efetuaria, uma vez que eles são extremamente cuidadosos nas invasões, com o intuito de não chamar a atenção dos métodos já implantados na rede. Destaca-se como exemplo que, um *cracker* não irá efetuar o escaneamento das 65.535 portas

disponíveis na rede, isso comprometeria sua invasão, uma vez que *firewalls* [3] poderiam detectar estas tentativas. São discretos e na maioria das vezes restritos apenas a quem efetuou a contratação do teste e claro, ao testador, com isso serviria também para analisar as diretrizes e medidas de segurança já implantadas na organização, verificando assim se as mesmas são eficazes.

O autor destaca também a importância de se utilizar metodologias de auditoria nos testes de invasão, uma vez que os *black hats* possuem uma linha de execuções quando efetuam um ataque. Esta metodologia engloba de quatro a sete passos e propõe ao *pentester* uma distribuição das tarefas a serem executadas e apesar das fases serem distribuídas de formas diferentes, elas possuem propósitos principais. Estas quatro fases de execução para aplicar um teste de invasão são destacadas abaixo na Figura 2:

Figura 2 - Principais fases da execução de um teste de invasão

Fonte: Engebretson (2014, p.44)

Justamente na fase 2, a de *Scanning* é que este trabalho é focado, em explorar as ferramentas utilizadas a fim de descobrir as vulnerabilidades de uma rede ou sistema. Na Figura 2 ilustrada anteriormente destacou-se como deve ser o foco do teste de invasão, mostrando um triângulo invertido, onde a cada passo, as informações vão se tornando cada vez mais restritas e objetivas. Engebretson (2014,

[3] *Firewall*: Sistema ou combinação de sistemas que protege a fronteira entre duas ou mais redes (ABNT NBR ISO/IEC 27002, 2013, p.viii).

p.43-45) destaca a importância de se executar os testes de forma coerente e com uma sequência lógica de tarefas, pular uma fase pode comprometer toda a análise que está sendo executada, e consequentemente o relatório final não será confiável. Destacamos na ordem os passos a serem executados:

- **Reconhecimento:** Fase de coleta de informações, análise do ambiente, todas as informações relevantes e que possam vir a comprometer os alvos.
- ***Scanning*:** Inclui na fase de *scanning* os procedimentos de verificação das portas alvo do sistema, após a análise destas portas executa-se a análise de vulnerabilidades, visando identificar quais delas podem estar comprometidas na rede.
- **Exploração:** Com os dados obtidos, explora-se estas vulnerabilidades atacando-as com a utilização de recursos e estratégias para identificar e obter acesso nestas brechas do sistema.
- **Pós-Exploração:** Visa preservar os acessos conseguidos a fim de se obter os dados necessários para a conclusão das tarefas.

Com todos os dados obtidos é finalizado o teste de invasão e passa-se para a produção de um relatório detalhado das vulnerabilidades encontradas, destacando em níveis de gravidade, fornecendo assim um detalhamento de onde deve-se priorizar as medidas de segurança a serem adotadas.

Os procedimentos realizados pelos *pentesters* contam com o auxílio de ferramentas e escaneamento de redes, fornecendo a eles resultados mais precisos e confiáveis. Estas ferramentas serão abordadas a seguir, no capítulo 3 deste trabalho.

3 FERRAMENTAS E TÉCNICAS DE ESCANEAMENTO

As ferramentas e técnicas utilizadas devem ser definidas no escopo da auditoria a ser realizada, assim como o objetivo e quais resultados visa-se coletar. Destaca que todo tipo de técnica e procedimentos poderão ser empregados para a coleta dos dados, seja ela de caráter observatório, documental através de questionários e da reexecução de tarefas ou de maneira exploratória, utilizando ferramentas que são divididas em três categorias:

- ***Softwares* Generalistas:** Auxiliam no processo da auditoria e na forma que será coletada estas informações, fornece ao auditor um planejamento de como será executada a ação em questão;
- ***Softwares* Especializados:** São desenvolvidos conforme solicitação do auditor ou até mesmo desenvolvido por ele, são complexos e limitados de atualizações;
- **Programas utilitários:** Utiliza-se de programas para a execução de funções comuns, porém, estes programas não foram desenvolvidos para tal finalidade e os dados coletados são extremamente básicos (IMONIANA, 2008, p.54).

As técnicas ou metodologias que serão utilizadas pelo auditor, segundo Imoniana (2008, p.57-58), também devem ser definidas e visam garantir uma série de vantagens:

- Produtividade;
- Custo;
- Qualidade Assegurada;
- Valor Agregado;
- Benefícios Corporativos;
- Benefícios para o Auditor.

Dentre as técnicas citadas pelo autor, destaca-se a de rastreamento e mapeamento, onde procura fornecer ao auditor uma série de dados relacionados a tarefas e execuções em uma rede de computadores.

Atualmente, existem diversas ferramentas disponíveis para verificação de um ambiente de redes, cada uma com sua peculiaridade e características próprias, mas que auxiliam o auditor na localização das vulnerabilidades que podem vir a prejudicar o desempenho da organização.

3.1 Ferramentas de Escaneamento

Conforme destaca Engebretson (2014), as ferramentas utilizadas para o exame da rede local, assim como os métodos utilizados vem ganhando um grande espaço no mercado, e cada dia mais, vem sendo utilizadas pelas empresas buscando uma segurança mais efetiva e ofensiva. As análises de vulnerabilidades devem ser consideradas tanto quanto as demais formas de políticas e avaliações de risco da empresa. Contudo as ferramentas utilizadas para as verificações do ambiente de redes estão acessíveis e extremamente abundantes são as opções.

As ferramentas estão disponíveis individualmente para instalação nos sistemas operacionais Linux e Windows e os recursos das mesmas são imensos. Destaca-se entre as distribuições mais conhecidas para os testes de invasão o “Backtrack”, que após alguns anos de disponibilização pelos seus idealizadores, foi melhorada e o seu nome modificado para “Kali Linux”. Nela é fornecida uma série de ferramentas capazes de auxiliar o *pentester* a realizar os mais diferentes tipos de análises, estão prontas para o uso, sem a necessidade de instalá-las e de forma gratuita.

Na Figura 3 é ilustrado a tela de inicialização do Kali, cuja versão mais atual é a 2.0, lançada em 11 de agosto de 2015.

Figura 3 - Tela inicial Kali

Fonte: Autoria própria.

O Kali Linux é uma distribuição disponibilizada pela *Offensive Security* em 2013 e sua “versão atual contém mais de trezentas ferramentas de segurança e testes de invasão” (BROAD, BINDNER, 2014, p.24), distribuída em grupos conforme a necessidade do *pentester* sendo considerada ferramenta essencial em auditorias de segurança.

3.1.1 NMAP

O NMAP é uma ferramenta de escaneamento de redes projetada por Gordon “Fyodor” Lyon e lançada em 1º de setembro de 1997, utilizada em auditorias e testes de invasão, sendo capaz de localizar em uma rede os computadores ativos, quais serviços estão executando, quais portas estão vulneráveis e abertas, dentre muitos outros recursos. A porta em uma rede de computadores é definida como um ponto, seja ele físico ou lógico, onde realizam as trocas de informações entre dispositivos. As portas lógicas mais comuns são as portas TCP e UDP. Segundo Morimoto (2011) existem 65.535 portas onde as quais são utilizadas por programas e serviços. Ele destaca também que, dessas portas, as que são enumeradas de 0 a 1023, são reservadas para os serviços de rede mais comuns, como exemplo, a porta 80, destinada a serviços web.

São exatamente estas portas que são o alvo principal do NMAP, efetuando varreduras com o propósito de identificar quais delas estão vulneráveis na rede. Algumas nomenclaturas são utilizadas para a identificação do estado destas portas, tais como:

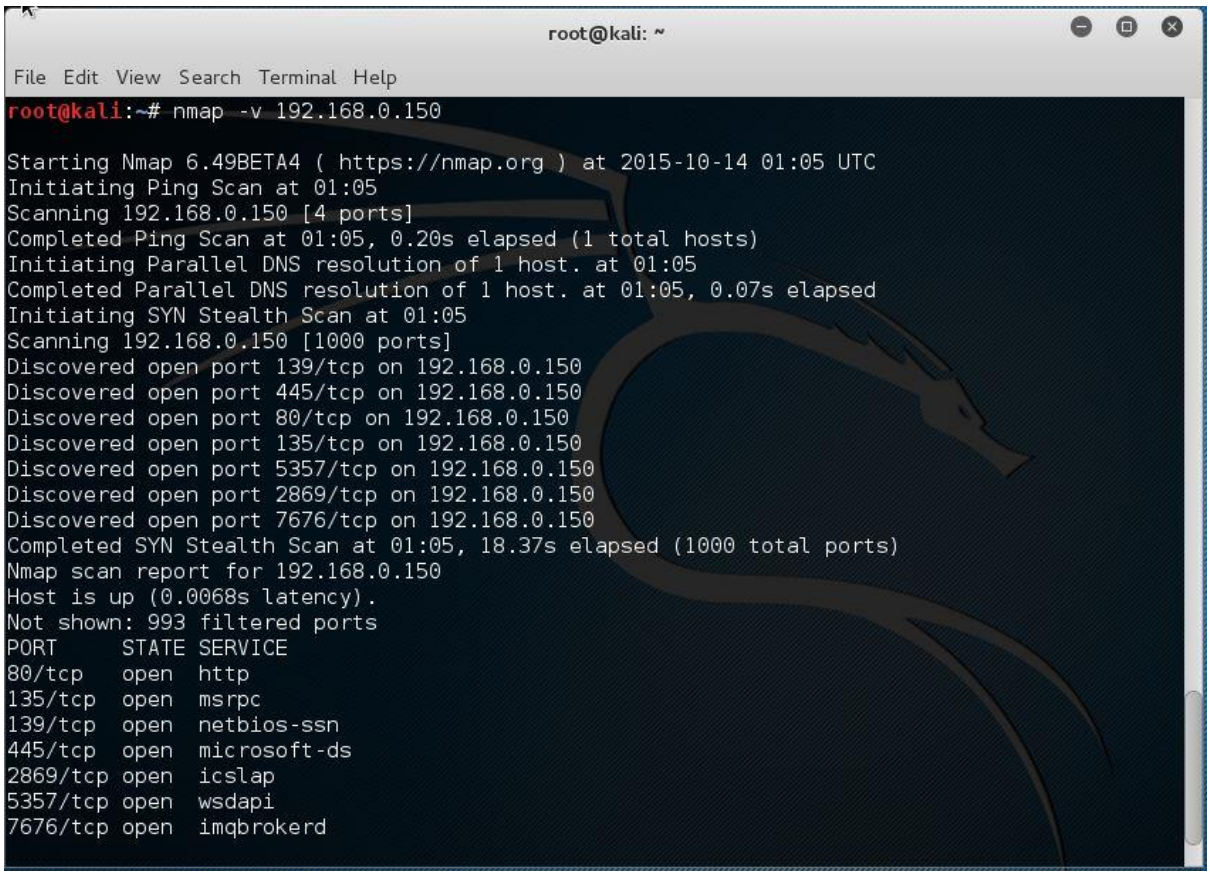
- Aberta (*Open*): está enviando e recebendo informações na rede;
- Fechada (*Closed*): nenhum serviço está ativo nesta porta;
- Filtrado (*Filtered*): existe algum mecanismo de segurança, como por exemplo um *firewall*, não permitindo que o NMAP identifique seu estado;
- Não-Filtrado (*Unfiltered*): estas portas estão na rede, se comunicam com o NMAP, porém ele não consegue identificar o estado real dela;
- Aberta/Filtrada (*Open/Filtered*): não foi possível identificar se seu estado está aberta ou filtrada, isto ocorre em alguns tipos de escaneamento onde portas abertas não enviam uma resposta, o que pode ocorrer devido a um filtro de pacotes ou *firewall* estar ativo;

- Fechada/Filtrada (*Closed/Unfiltered*): utilizada para alguns tipos de escaneamento, onde não conseguem determinar se a porta está fechada ou filtrada. (LYON, 2009, p.77-78)

Com estas varreduras, é possível determinar os alvos que estão vulneráveis na rede, e podem ser explorados por um invasor. Com o uso de parâmetros em linhas de comando é possível que o NMAP exiba outros resultados da pesquisa, tais como, sistema operacional do computador alvo, número de computadores ativos na rede, endereço MAC da placa de rede, IP´s ativos, etc.

Na Figura 4 é ilustrado um exemplo de um escaneamento básico realizado com o NMAP em uma rede.

Figura 4 - Exemplo de escaneamento de rede com NMAP



Fonte: Autoria própria.

O NMAP é uma ferramenta de código aberto e gratuita, desenvolvida para explorar redes de computadores e auditoria de sistemas. Possui versões para sistemas operacionais UNIX, que utiliza de linhas de comando para efetuar as varreduras e Windows, possuindo uma interface gráfica da mesma versão, neste caso

a ferramenta se chama Zenmap. Utilizando o Zenmap, é possível salvar os resultados da pesquisa para serem visualizados posteriormente e de acordo com Giavaroto e Santos (2013, p.79), é “interativa, exibe resultados de forma organizada, mostra detalhes com *scan* em andamento, pode desenhar mapa topológico da rede testada, é de fácil utilização”.

LYON (2009, p.12-13) lembra que o NMAP não é apenas uma ferramenta de escaneamento de portas, e das várias fases que fazem parte de uma varredura, as principais são destacadas a seguir:

- **Enumeração do Alvo (*Target Enumeration*):** Nesta fase ele identifica através dos endereços IP os alvos ativos na rede;
- **Descoberta de *Hosts*/Computadores (*Host Discovery*):** Os computadores ativos na rede são exibidos no resultado da pesquisa;
- **Escaneamento de Portas (*Port Scanning*):** Esta operação é a mais fundamental do NMAP, onde é identificada quais portas estão disponíveis no alvo e seu estado na rede;
- **Detecção do Sistema Operacional (*OS Detection*)**: identifica qual o sistema operacional instalado no *host* alvo.

3.1.2 Nessus

O Nessus é uma ferramenta de escaneamento de portas, desenvolvida em 2002, onde detecta um *host* ativo na rede e simula invasões com o objetivo de identificar vulnerabilidades armazenadas em um banco de dados próprio. Morimoto (2011), destaca que ela é capaz de localizar um servidor mesmo quando ele está utilizando outra porta na rede, diferente das portas padrão. É um *software* gratuito, porém de código fechado e existem versões do programa para Linux, Windows e outros. Como procedimentos de instalação, destaca-se a importância de efetuar o *download*[4] do Nessus, que executa o gerenciamento das pesquisas, chamado de gerente e também da versão cliente, a ser instalada nos *hosts* ativos da rede, chamada de agente, sendo o responsável pelas respostas às solicitações do gerenciador principal. O escaneamento de portas executado pelo Nessus utiliza o

[4] *Download*: Descarregamento, transferência de arquivos entre computadores por meio de uma rede (ABNT NBR ISO/IEC 27002, 2013, p.vii).

NMAP para executar a tarefa, sendo assim, é primordial que o mesmo esteja instalado na máquina servidor. O grande diferencial do Nessus são os relatórios extremamente detalhados que ele gera, apontando as vulnerabilidades existentes em uma rede.

Segundo Morimoto (2011), a versão gerenciadora do Nessus apresenta algumas opções para que sejam definidos alguns parâmetros de execução. Destaca-se a seguir algumas delas:

- **Intervalo de Escaneamento de Portas:** Por padrão o Nessus executa um escaneamento nas portas 1 a 1024, apesar de uma execução rápida, isso pode resultar em dados incompletos uma vez que, pode-se conter serviços habilitados em portas mais altas, melhorando esta execução, altere as portas a serem checadas para 1 a 65535.
- **Quantidade de *Hosts* a Serem Verificados:** Pode-se alterar a quantidade de *hosts* que serão checados na mesma varredura, ele traz como configuração padrão 20 *hosts*, o que é adequado para uma pequena rede. Aumentando esse número pode comprometer o desempenho da rede pois consumirá mais recursos de todos os computadores que estarão sendo analisados.
- **Otimizar o Escaneamento:** Esta opção utiliza resultados coletados anteriormente como base de informações, fazendo com que o escaneamento seja executado mais rapidamente.

Na utilização do Nessus, também é possível adicionar uma série de plug-ins para melhorar o desempenho do escaneamento, fornecendo a ele novas configurações que visam tratar de forma diferenciada algumas checagens, visa-se com isso explorar algumas vulnerabilidades específicas.

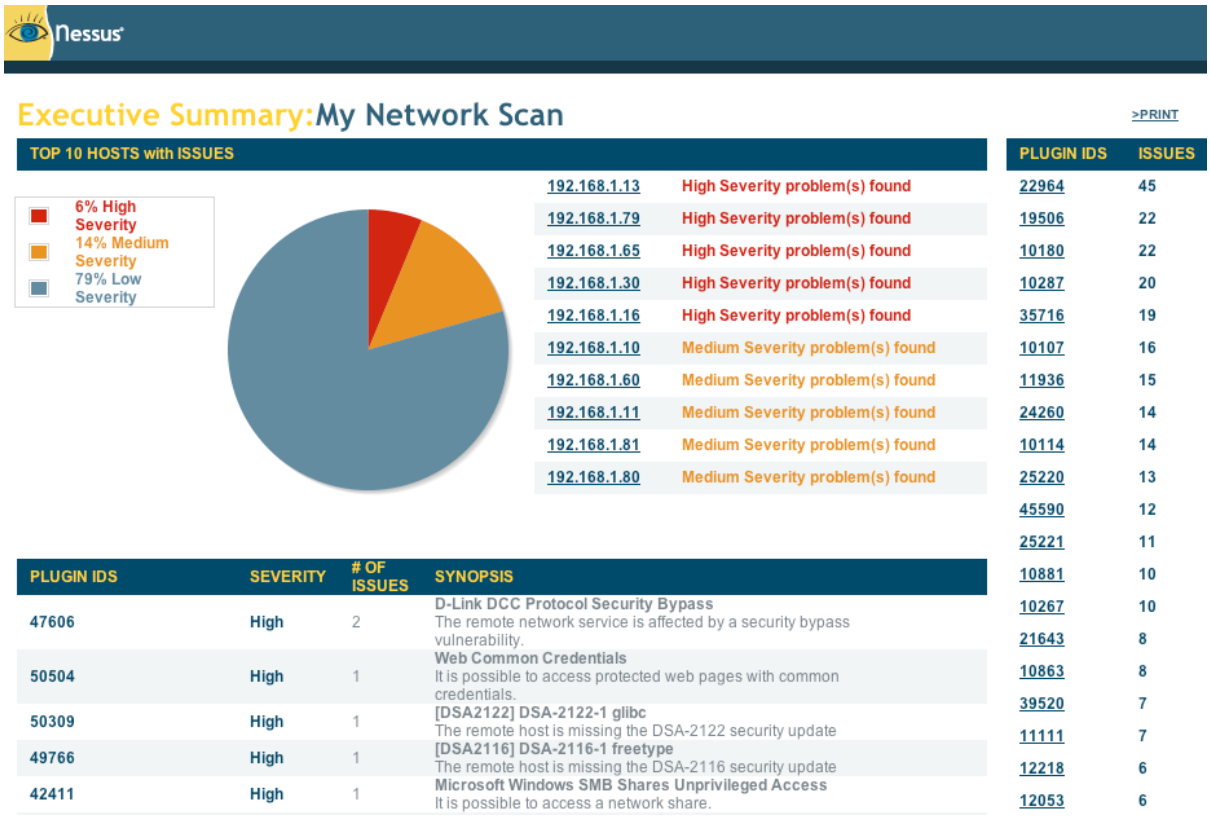
O teste é executado em duas partes, inicialmente é verificado as portas abertas na rede, utilizando como base as técnicas utilizadas pelo NMAP, juntamente com alguns recursos do Nessus. Em seguida é exibido os resultados deste escaneamento apontando as vulnerabilidades encontradas, em uma escala de cores e níveis, determinando o quão grave é o problema encontrado.

Os *hosts* identificados são exibidos incluindo uma breve descrição da vulnerabilidade, graficamente, em escala de cores e de gravidade:

- Baixo (*Low*): apresentando as informações dos *hosts* na cor azul;
- Médio (*Medium*): apresentando as informações dos *hosts* na cor laranja;
- Alto (*High*): apresentando as informações dos *hosts* na cor vermelha;

A Figura 5 apresenta a interface da ferramenta Nessus:

Figura 5 - Interface da ferramenta Nessus



Fonte: www.tenable.com.

O Nessus, além da busca por informações, também auxilia o administrador de redes através de alertas e oferece uma possível solução para o problema encontrado.

3.1.3 Outras Ferramentas

Conforme citado por Giavaroto e Santos (2013), o Kali Linux fornece ao *pentester* uma série de ferramentas que irão lhe auxiliar no exame de redes, as duas principais ferramentas de escaneamento de portas: NMAP e Nessus, porém outras ferramentas disponíveis no mercado, em sua grande maioria de forma gratuita, também oferecem resultados satisfatórios e que quando trabalhadas em conjunto, explorando as características de ferramentas com propósitos diferentes, resultará em uma documentação detalhada e precisa.

O autor apresenta algumas ferramentas que também executam o escaneamento de portas em redes de computadores, são elas:

- **AMAP:** Esta ferramenta auxilia o *pentester* na identificação de aplicações mesmo que estão sendo executados em outras portas, que não seja a sua porta padrão. Foi a primeira ferramenta de uso profissional no escaneamento de redes.
- **NETCAT:** Considerada uma ferramenta extremamente simples e completa, ele executa desde varreduras na rede utilizando os protocolos TCP e UDP até um ataque de força bruta.
- **HPING:** A ferramenta é considerada um montador de pacotes, utilizada para detectar *hosts*, regras de *firewall*, assim como pode ser utilizada em escaneamentos de portas. (GIAVAROTO, SANTOS, 2013, p.37-40,81-82,101-103)

3.2 Técnicas de Escaneamento de Portas

As técnicas utilizadas no escaneamento de redes visam fornecer ao administrador de redes informações gerais de sua rede, identificando uma série de informações sobre riscos, ameaças e vulnerabilidades que sua rede está exposta.

O escaneamento de redes conforme orientado por Engebretson (2014) é dividido em quatro fases (vide capítulo 2), e o foco deste trabalho é na segunda fase da auditoria. Nela temos o *scanning* que pode ser trabalhado em duas etapas:

- *Scanning* de Portas;
- *Scanning* de Vulnerabilidades;

Utilizando as técnicas adequadas nesta etapa, encontramos uma série de vulnerabilidades disponíveis na rede.

3.2.1 Portas e Protocolos

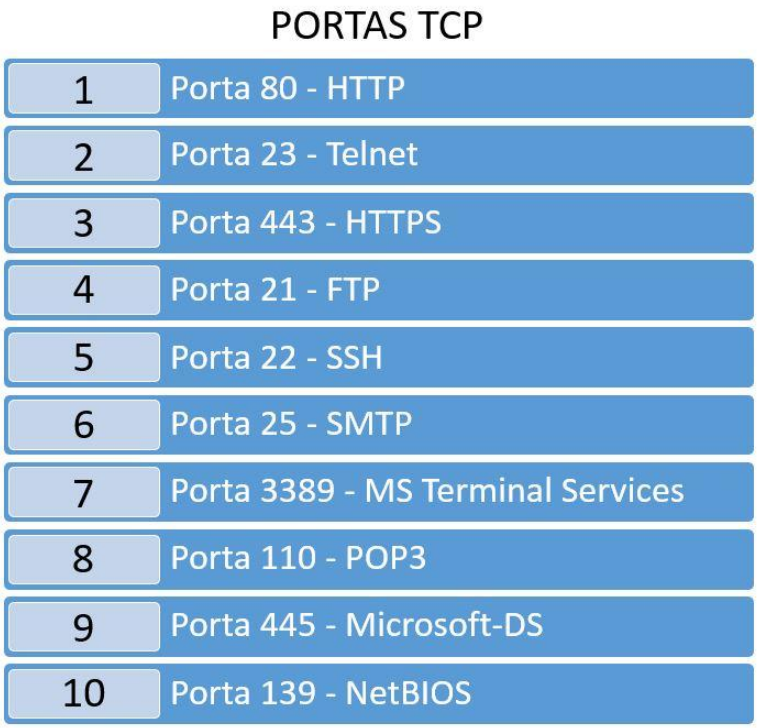
Seguindo as orientações de Lyon (2009), as portas são as responsáveis pela comunicação entre aplicações utilizadas em uma rede. São semelhantes aos IP´s que identificam as máquinas. As portas identificam as aplicações das quais são baseadas

em dois protocolos: TCP e UDP. Cada aplicação trabalha com uma numeração padrão de porta e são utilizadas para os mais diversos fins.

Para que os serviços de sua rede sejam executados algumas destas portas precisam estar disponíveis para que a comunicação entre as aplicações aconteça, e é justamente nessa disponibilidade que se exploram algumas vulnerabilidades na rede de computadores. De todas as 65.535 portas disponíveis, 1023 delas são reservadas para os serviços mais comuns de comunicação, e muitas delas, quando abertas na rede, são portas de entrada para uma invasão ser iniciada. O NMAP efetua o escaneamento nas 1000 portas mais comuns de cada protocolo, com o objetivo principal de identificar o estado de cada uma delas de forma rápida e precisa.

De acordo com Lyon (2009), uma lista foi criada com as portas mais comuns nos escaneamentos, onde na Figura 6, é identificado as 10 portas mais populares para o protocolo TCP:

Figura 6 - Portas TCP mais populares

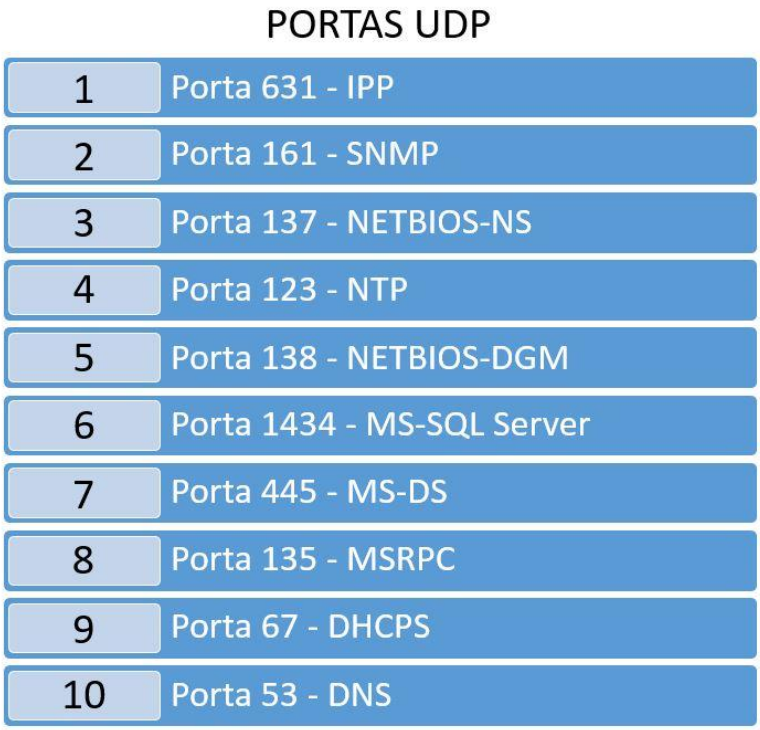


Fonte: Adaptação de Lyon (2009).

Foi criada também uma lista contendo as portas que utilizam o protocolo UDP, porém é um protocolo simples, não apresentando nenhuma informação ou controle caso erros ocorram na conexão.

Na Figura 7 identifica-se as 10 portas mais populares para o protocolo UDP:

Figura 7 - Portas UDP mais populares



Fonte: Adaptação de Lyon (2009).

3.2.2 Escaneamento de Portas

O escaneamento de portas é fundamental e importantíssimo ao administrador de redes para efetuar a varredura de portas abertas em sua rede, e das ferramentas apresentadas o NMAP é a mais recomendada para este fim. Apesar de hoje possuir uma infinidade de recursos, inicialmente ela foi projetada para ser um excelente escâner de portas e mantêm essa característica até os dias atuais. Segundo Lyon (2009) o escaneamento de portas, utilizando o NMAP, proporciona a descoberta de portas abertas na rede, assim como o estado em que ela se encontra. Dos estados mais importantes das portas localizados é o de aberto, onde nesta situação a porta está disponível para o envio e recebimento de dados.

Giavaroto e Santos (2013) destacam que o escaneamento de portas utilizando ferramentas apropriadas para este fim, enviam uma mensagem a estas portas identificando quais delas estão vulneráveis, desde as mais comuns até as que são

pouquíssimos utilizadas. O principal objetivo de efetuar um escaneamento de portas é a segurança, pois é possível reduzir consideravelmente as aberturas de uma rede de computadores, que poderiam ser exploradas por um invasor. Reduzindo estas chances, sua rede está mais segura e protegida, uma vez que portas vulneráveis foram desabilitadas, e juntamente com a proteção de um *firewall*, a maioria destes ataques serão frustrados.

É considerada por Giavaroto e Santos (2013, p.63) “uma das técnicas mais comuns e usadas por atacantes para descobrir serviços vulneráveis em um sistema”. Os autores ressaltam que a Internet é a porta de entrada por muitos invasores para explorar as falhas na segurança dos dados da organização, e estes escaneamentos visam fornecer a verificação de portas e serviços ativos, em consequência é possível detectar as vulnerabilidades que esta rede está sujeita.

A recomendação é manter um cronograma de verificações regulares e também um inventário de portas e os estados das mesmas na rede. Quando estas medidas de segurança são tomadas, a segurança da rede aumenta consideravelmente e o NMAP tem papel fundamental nessa verificação. A ferramenta proporciona ao administrador da rede a possibilidade de classificar e identificar os *hosts* da rede com vários propósitos, conforme destaca Lyon (2009, p.79):

- Testes de Disponibilidade;
- Rastreamento de Licenças;
- Verificação das Políticas de Segurança;
- Arquitetura da Rede;
- Identificação dos Sistemas Operacionais.

3.2.3 Técnicas Utilizadas no Escaneamento de Portas

Todos os dados que trafegam na Internet, utilizam-se de camadas para a troca de informações. Uma solicitação enviada, passa por estas diversas camadas que são capazes de atravessar uma série de pontos na rede, chamados de nós. Cada protocolo pertence a uma camada distinta e são responsáveis por entregar a mensagem de forma íntegra ao seu destino, ou vice-versa, conforme orienta Kurose e Ross (2010).

Estas camadas, citadas por Forouzan (2006) são distribuídas em cinco níveis ilustrados na Figura 8, demonstrando os modelos de camadas da Internet:

Figura 8 - Modelos de camadas da Internet.

Fonte: Baseado em Forouzan (2006)

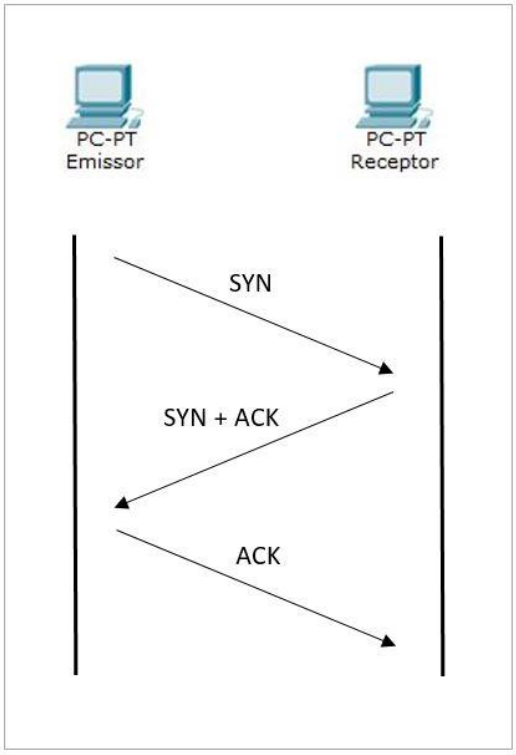
De forma simplificada, Kurose e Ross (2010) explicam que os protocolos de rede são os responsáveis pelo tráfego de informações e solicitações de um ponto a outro, e para que estas ações sejam realizadas, *hardwares* e *softwares* dos equipamentos são os responsáveis pela troca de informações. O escaneamento de portas é uma técnica que, consiste em enviar um pacote (que são um grupo de informações em formato de *bits*) de um *host* a outro, em uma rede. O intuito principal é de estabelecer uma conexão entre os dispositivos e as respostas obtidas é o que determina o estado de cada porta na rede.

Utilizando *flags* (*bits*) nos cabeçalhos do protocolo, a conexão estabelecida utiliza o processo *three way handshake*, no qual ele consiste em estabelecer uma comunicação entre dois *hosts* com o propósito de manter esta comunicação.

O emissor envia um pacote contendo a *flag* SYN ativada solicitando o estabelecimento de uma comunicação, por sua vez o receptor recebe estes dados, verifica-os e responde enviando um pacote com dados para efetivar esta conexão com

as *flags* SYN e ACK ativadas, confirmando a disponibilidade de receber os dados, em seguida, o emissor retorna um pacote com a *flag* ACK ativada, também confirmando que os dados foram recebidos sem erros. Este tráfego de informações é apresentado na Figura 9, ilustrando como esta conexão será estabelecida, e após isso estão aptos a troca de informações.

Figura 9 - Conexão TCP



Fonte: Adaptação de Lyon (2009)

As *flags* utilizadas nos cabeçalhos dos protocolos tem papel fundamental no tipo de técnica de escaneamento que será utilizada, dentre as quais Kurose e Ross (2010) citam:

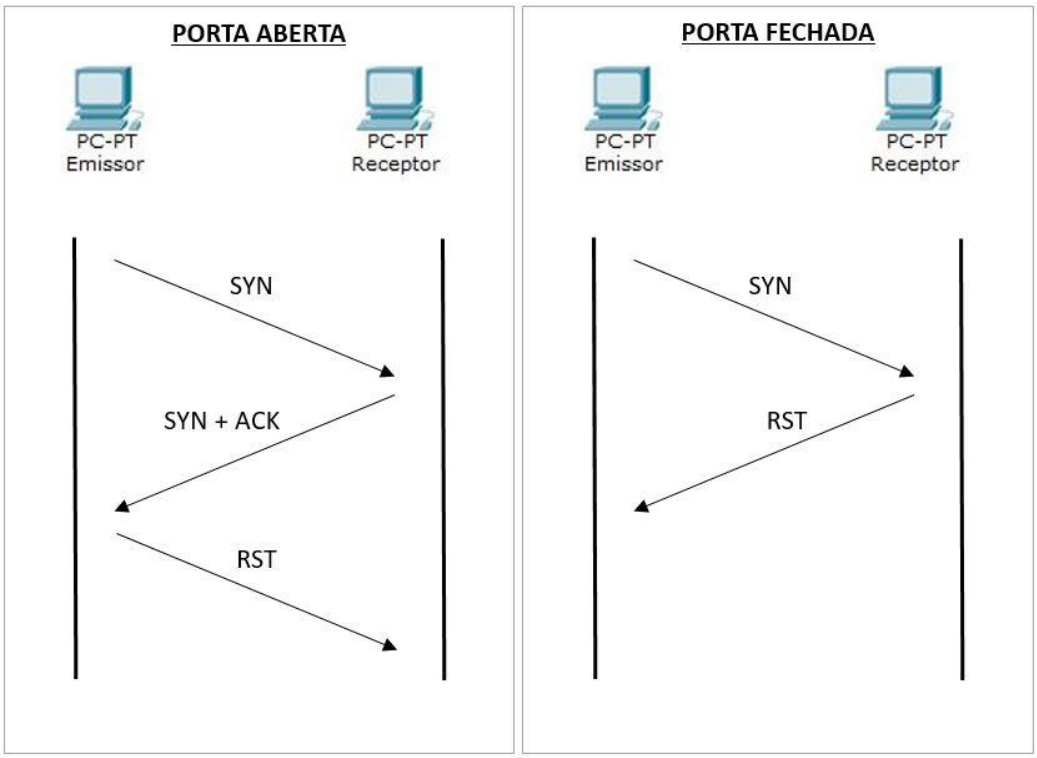
- ACK (*Acknowledgment*): Quando o *host* recebe os dados, ele altera o cabeçalho para ativo (inserindo o número 1), reenvia esta informação ao emitente, resultando na garantia de que os dados foram entregues sem erros.
- SYN (*Synchronize*): Utilizando a *flag* SYN ativa (1) e ACK desativada (0), o *host* destino indica que quer estabelecer uma conexão, a resposta então são SYN e ACK ativos (1), demonstrando que se iniciou-se um processo.

- FIN (*Finalize*): Quando um dos *hosts* não possui mais dados para efetuar a troca de informações e solicita o encerramento da conexão, envia-se uma *flag* FIN ativa (1) para esta finalização.

O escaneamento do tipo SYN (sincronização) é o padrão do NMAP, fácil de ser utilizado e a mais popular das técnicas de escaneamento conforme orienta Lyon (2009). Ele destaca uma série destas técnicas, das quais são suportadas pelo NMAP, abaixo, destaca-se as três principais delas:

- TCP SYN: Dentre as técnicas é a mais popular, principalmente por ser a mais rápida no escaneamento de portas e é adequada para qualquer tipo de rede. São mais discretas na execução pois sua comunicação com as portas é executada até a metade do processo, evitando assim que seja detectado. Porém, alguns dispositivos como roteadores e *firewalls* da rede, conseguem identificar o processo mesmo que incompleto. Ela consiste no emissor enviar uma *flag* SYN ativada, encontrando uma porta aberta o receptor responde com *flag* SYN e ACK ativadas, o emissor envia uma *flag* RST (*reset*) para finalizar a comunicação. A Figura 10 ilustra como é a comunicação entre os *hosts* utilizando a técnica de TCP SYN:

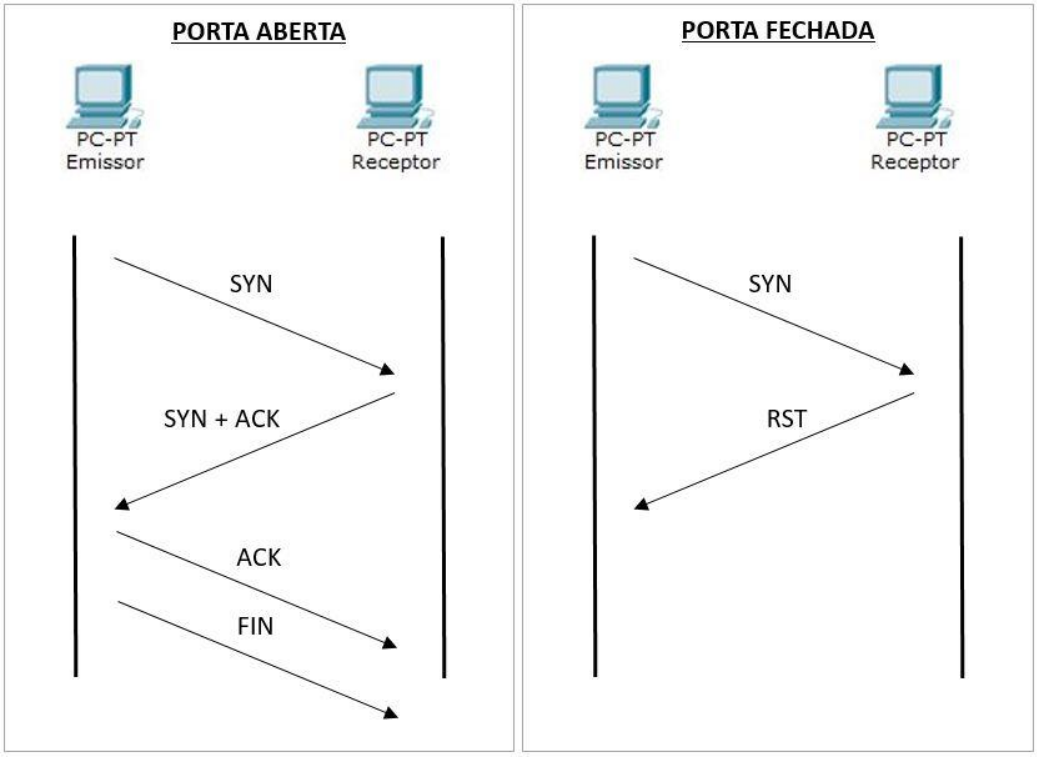
Figura 10 - Comunicação utilizando a técnica TCP SYN



Fonte: Adaptação de Lyon (2009)

- TCP *Connect*: Esta é uma técnica segura de ser utilizada, porém deixa rastros e pode ser facilmente identificada. Tem como base a comunicação padrão TCP e armazena informações do endereço de origem do escaneamento. Sua comunicação é baseada no envio de uma *flag* SYN ativada para o receptor, na hipótese de haver uma aplicação disponível na porta, ele retorna um pacote contendo a *flag* SYN e ACK ativadas, assim, finalizando os três passos de comunicação TCP. O emissor ainda envia uma *flag* ACK ativada e para finalizar envia um pacote com a *flag* FIN. Esta troca de pacotes é ilustrada na Figura 11 demonstrando os passos da técnica TCP Connect:

Figura 11 - Comunicação utilizando a técnica TCP Connect

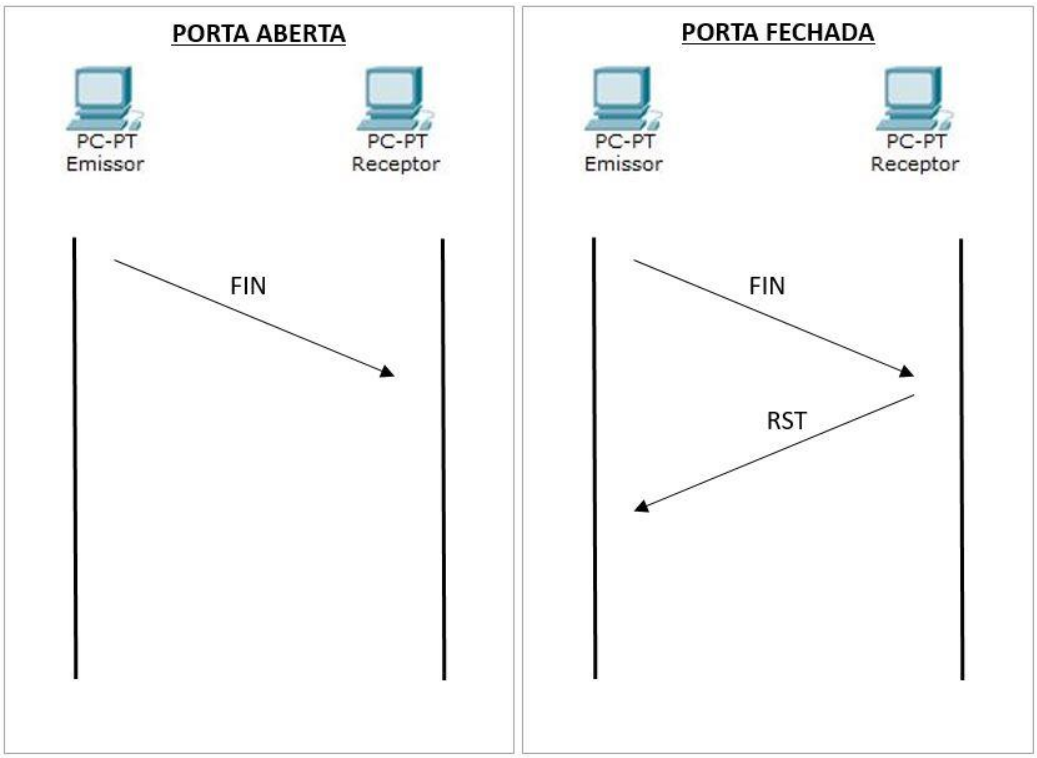


Fonte: Adaptação de Lyon (2009)

- TCP FIN: A técnica é extremamente simples e consiste em enviar pacotes com a *flag* FIN ativadas e através dela identifica se a porta está aberta ou fechada. Na situação em que a porta se encontra aberta e um pacote com a *flag* FIN ativada chega e não será enviado nenhuma resposta ao emissor; encontrando a porta fechada, um pacote com a *flag* FIN ativada chega e o receptor envia um pacote com a *flag* RST ativa para o emissor, não recebendo nada como resposta. Este tipo de técnica não é funcional em sistemas operacionais

Windows, pois o mesmo envia um RST estando aberta ou fechada. Na Figura 12 é exibido como é a funcionalidade básica da troca de pacotes utilizando a técnica TCP FIN:

Figura 12 - Comunicação utilizando a técnica TCP FIN



Fonte: Adaptação de Lyon (2009)

Utilizando estas técnicas, o NMAP identifica o estado das portas na rede e retorna uma lista contendo informações pertinentes a busca. Como o NMAP utiliza a técnica TCP SYN por padrão, um invasor pode facilmente explorar as portas abertas e ainda, na falta de *firewalls* e outras políticas básicas de segurança ativadas, sua invasão é concluída com resultados satisfatórios para o invasor.

No próximo capítulo serão exploradas estas técnicas, utilizando a ferramenta NMAP com o propósito de identificar as portas abertas, fechadas e em outros estados detectados em uma rede, coletando informações pertinentes para a viabilidade do uso da ferramenta.

4 ANÁLISE DE VIABILIDADE

Após a conceituação dos procedimentos necessários para análise de portas e a importância das análises das vulnerabilidades para identificar as falhas em uma rede de computadores, neste capítulo serão apresentadas as funcionalidades da ferramenta NMAP, por ser uma ferramenta de *software* livre, uma das mais populares neste tipo de procedimento, conhecer os comandos principais no escaneamento de portas e efetuar um ambiente simulado, identificando as possíveis vulnerabilidades contidas nesta pequena rede.

O NMAP é uma ferramenta que pode ser implementada facilmente em qualquer organização para auditorias, conforme cita Christo (2015, p.73):

> O NMAP tem o poder de fazer diversas verificações como disponibilizar *hosts* ativos na rede, quais serviços estão utilizando, mostrando até qual sistema está rodando nos *hosts*, tipos de filtros ou *firewalls* em uso entre outras características.

Serão explorados os conceitos básicos do NMAP, suas varreduras e os resultado obtidos com elas. Em seguida, aplica-se medidas de prevenção com intuído de identificar e demonstrar que a ferramenta, possui recursos suficientes para a auditoria de qualquer organização. Fornecendo informações e para que ações sejam tomadas, com o objetivo de dificultar o acesso de qualquer atacante em uma rede.

4.1 Configurações e o Ambiente de Testes

O NMAP possui versões disponíveis para diversos sistemas operacionais, tais como: Windows, Linux, entre outros, porém utilizaremos a ferramenta no Kali Linux, distribuído pela *Offensive Security*, e sua última versão disponibilizada é a 2.0. Segundo Broad e Bindner (2014) o Kali Linux conta com uma interface dinâmica e ferramentas distribuídas por categorias, para os mais diversos tipos de testes, utilizando como base uma distribuição em Debian 7.0.

Com o intuito de simular uma rede de computadores, criou-se um ambiente através de máquinas virtuais onde instalou-se o Kali Linux 2.0, utilizando 512 MB de

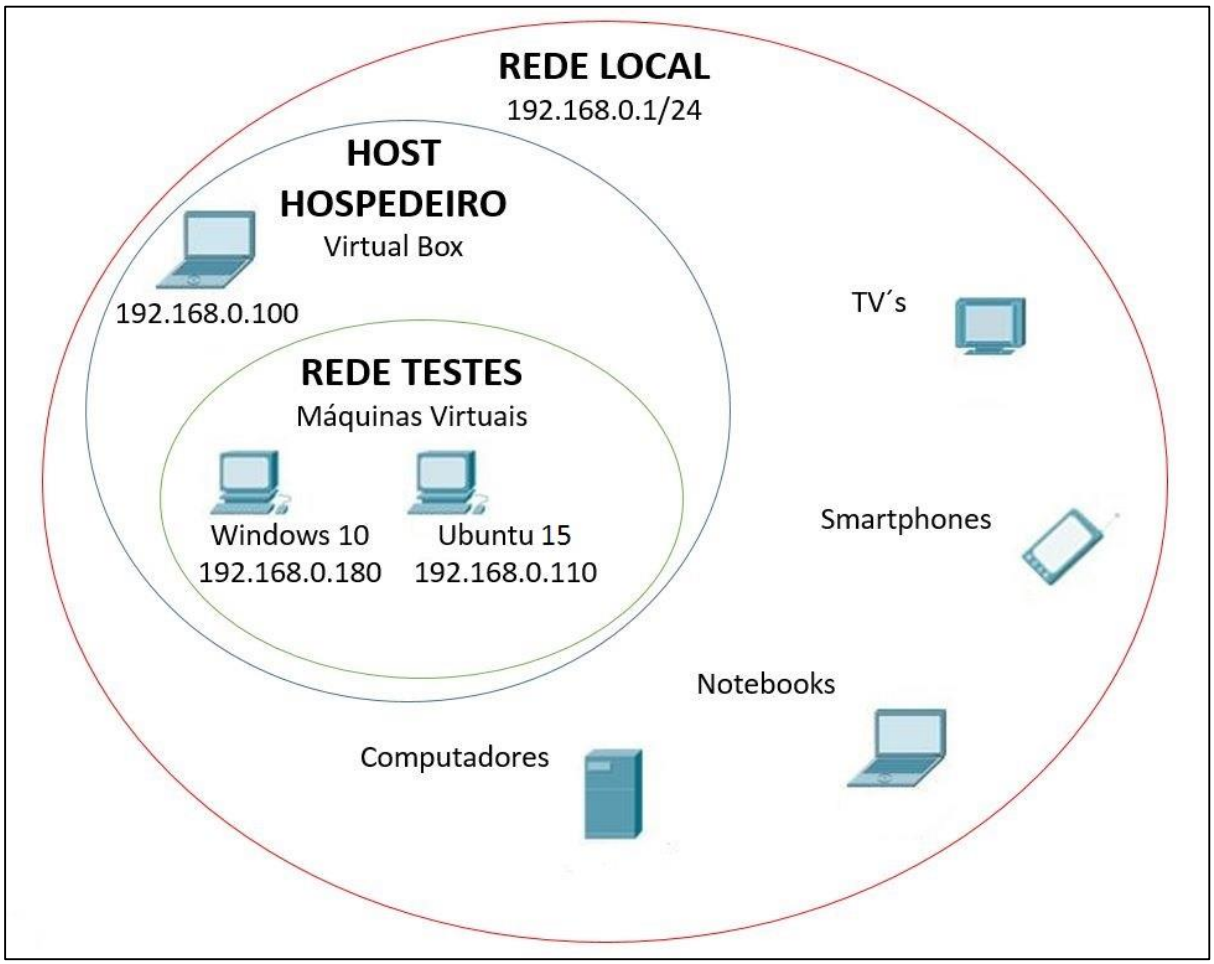
memória RAM e HD de 8 GB, para efetuar o escaneamento de outras máquinas. Na rede experimental adicionou-se 2 outras máquinas que serviram de *hosts* alvos do escaneamento com os seguintes sistemas operacionais:

- Microsoft Windows 10 Pro 64 *bits*, 1 GB de memória RAM e HD 10 GB;
- Ubuntu 15.04 Vivid Vervet 32 *bits*, 512 MB de memória RAM e HD 8 GB.

As máquinas virtuais foram instaladas no programa de virtualização Virtual Box, versão 5.0.6 da Oracle, em notebook com Windows 10 Home Single Language, processador Intel Core i7 de 2,4 GHz, 6 GB de memória RAM e HD 500 GB. Pertencente a mesma rede local, outros equipamentos serão facilmente detectados, como *smartTV´s*, *smartPhones*, *tablets*, *notebooks* e computadores.

A topologia da rede contendo os sistemas operacionais instalados para este propósito pode ser analisada na ilustração da Figura 13, identificando os *hosts* ativos nela:

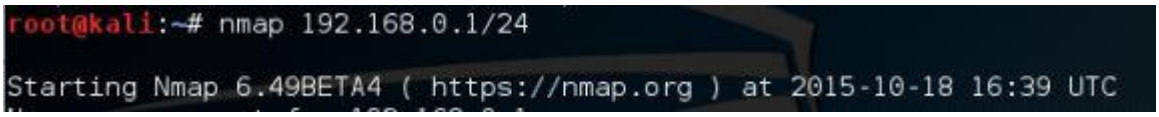
Figura 13 - Topologia da rede virtual de testes



Fonte: Autoria Própria

A versão do NMAP disponibilizada dentro da aplicação Kali Linux é a 6.49BETA4, conforme ilustrado na Figura 14:

Figura 14 - Versão do NMAP



Fonte: Autoria Própria.

O NMAP utiliza linhas de comando parametrizadas, com o intuito de trazer resultados diferentes em cada um deles. Segundo Christo (2015), a sintaxe aceita uma série de informações diferentes, chamada de "*target specification*", em tradução livre "especificação do alvo", onde determina o alvo do escaneamento dos quais podem ser: o nome do *host*, seu endereço de IP, o *gateway* da rede e muitos outros, na Figura 15 é ilustrada esta sintaxe:

Figura 15 - Sintaxe NMAP

```
Nmap [Scan Type (s) ]  [Options]  {target specification}
```

Fonte: Christo (2015, p.73)

Os parâmetros de escaneamento são inúmeros e cada um deles determina o tipo de informação que trará ao administrador de redes. Estes resultados podem trazer a quantidade de *hosts* ativos na rede, seus sistemas operacionais, e claro, as portas e os status dos alvos encontrados, uma vez que é o conceito principal do NMAP – o escaneamento de portas.

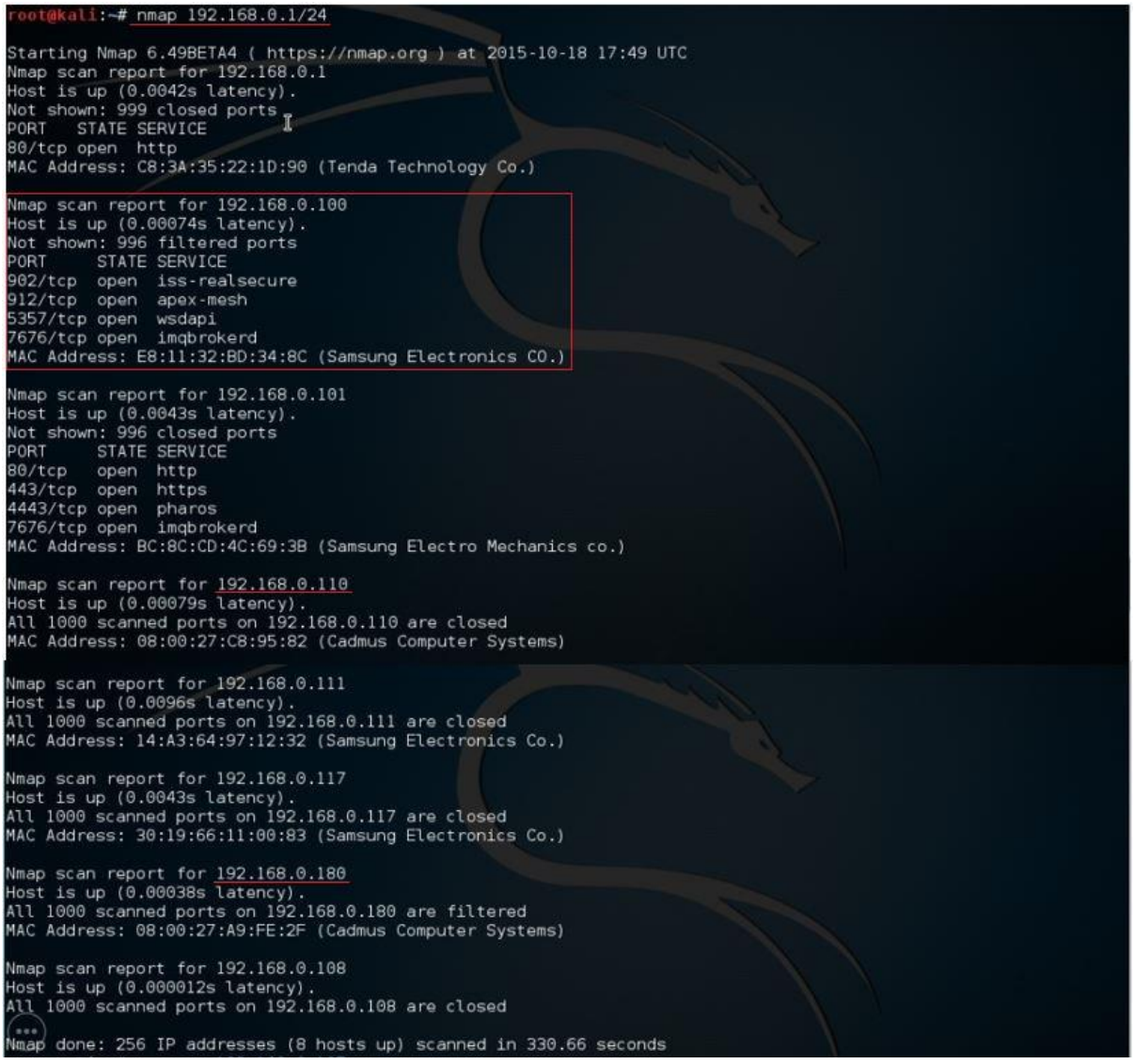
4.2 Procedimentos e Técnicas Utilizadas

Para fins de auditoria, o NMAP oferece recursos suficientes para que toda a rede e os *hosts* que a compõem sejam identificados. Informações detalhadas são exibidas em diversos parâmetros de escaneamento no programa, tornando a ferramenta extremamente útil para esta finalidade.

Na identificação dos alvos no ambiente de rede de testes, utilizou-se o parâmetro: **nmap 192.168.0.1/24**, onde 192.168.0.1 é o *gateway* padrão da rede e 24 a máscara de sub-rede. Nesta busca, trouxe-se todos os dispositivos ativos na rede, assim como: o tempo gasto de execução, as portas em cada *host* e seu estado, seu endereço *MAC Address*, dentre outras informações.

Este parâmetro de escaneamento é extremamente útil quando não se sabe a quantidade de *hosts* que estão ativos na rede e precisa auditá-los, e até mesmo quando busca a verificação na rede inteira. Estas informações podem ser visualizadas na Figura 16:

Figura 16 - Escaneamento completo da rede



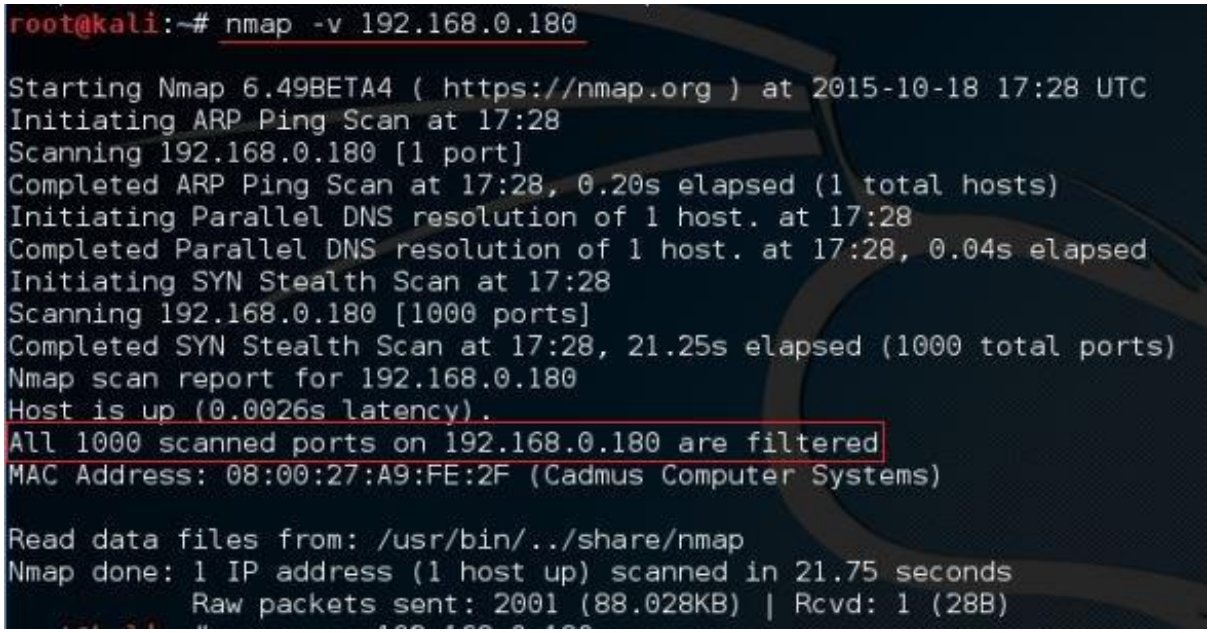
Fonte: Autoria Própria.

Com o propósito de coletar informações de toda a rede, porém, não contendo dados sobre a máscara de rede utilizada, um asterístico (*) é adequado no parâmetro para a identificação dos *hosts* conforme exemplo:

 # nmap 192.168.0.*

Com as informações dos *hosts* ativos na rede (IP´s), pode-se buscar mais informações sobre o alvo. Neste próximo exemplo, utilizou-se o parâmetro: **nmap -v 192.168.0.180**, cujo alvo é a máquina com Windows 10. Conforme explica Christo (2015), esta opção **-v** abrange o nível de detalhamento do escaneamento, utilizando-se **-vv** o resultado é ainda mais efetivo. Foram identificadas algumas informações do Windows 10, recém instalado, não apresentando nenhuma porta aberta, porém estão filtradas (*filtered*), identificando que algum mecanismo de segurança, como um *firewall* por exemplo, está ativo no *host* dentre as 1000 portas verificadas por padrão do NMAP, ilustrado na Figura 17:

Figura 17 - Escaneamento de *host* Windows 10

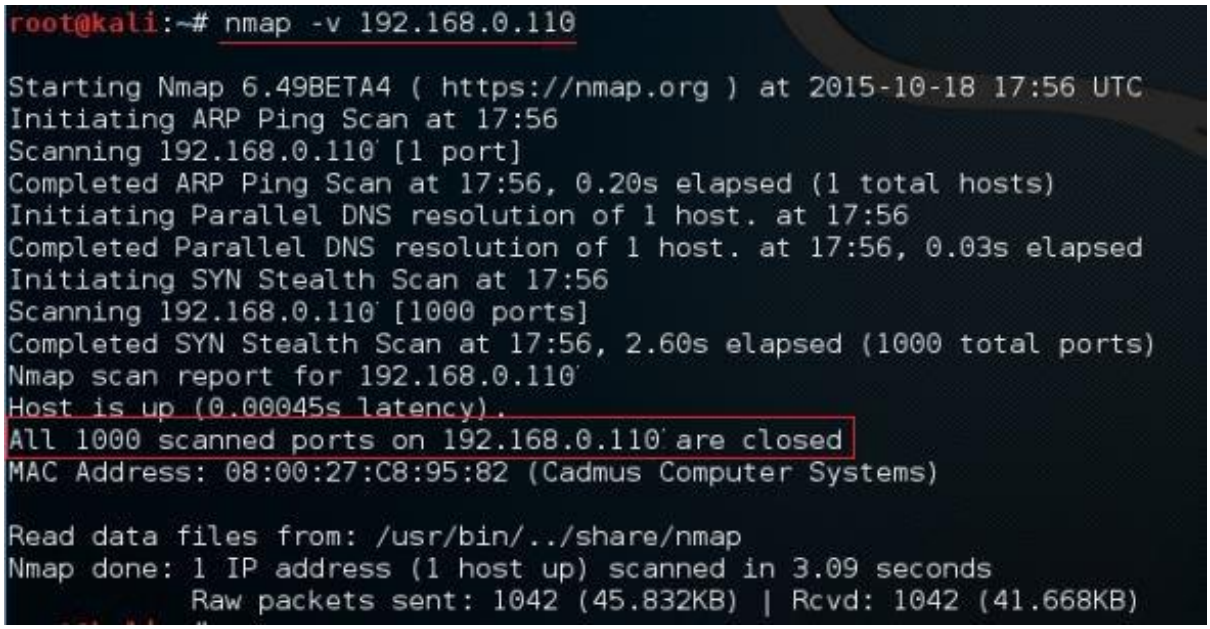


Fonte: Autoria Própria.

Com a mesma opção de busca e parâmetro: **nmap -v 192.168.0.110**, efetuou-se a pesquisa na máquina Ubuntu 15, os resultados identificados das portas pesquisadas foram que todas elas estão fechadas (*closed*), ou seja, não há a

possibilidade de acesso a nenhuma porta, nem mecanismos de segurança barrando o acesso às mesmas. As informações obtidas são exibidas na Figura 18:

Figura 18 - Escaneamento de *host* Ubuntu 15



Fonte: Autoria Própria.

O NMAP também efetua escaneamento na rede à procura de portas UDP ativas, porém não é o padrão da ferramenta, sendo necessário informar no parâmetro esta solicitação, através da opção **-sU**.

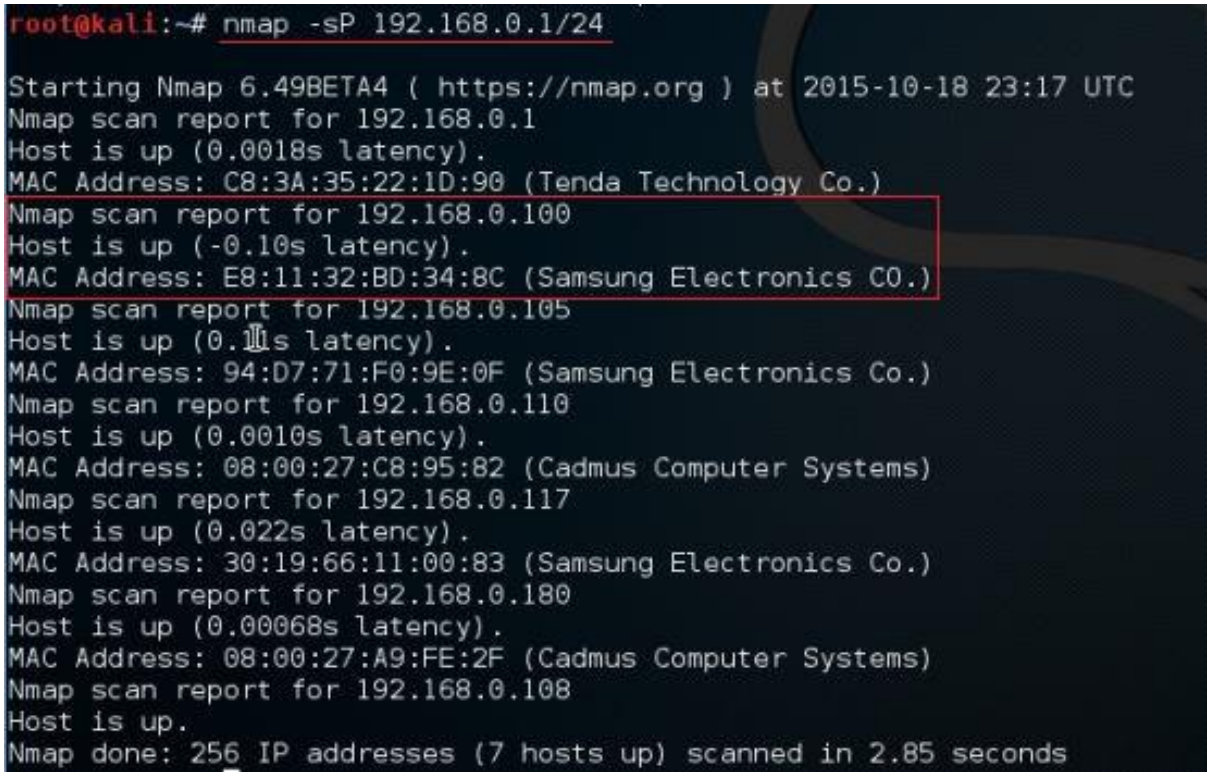
No exemplo da Figura 19, utilizou-se: **nmap -sU 192.168.0.100**, identificando as portas UDP abertas na rede:

Figura 19 - Escaneamento UDP

Fonte: Autoria Própria.

Se o administrador de redes precisa somente identificar os *hosts* ativos, um parâmetro simples pode auxiliá-lo, utilizando: **nmap -sP 192.168.0.1/24**, identificou-se todos os *hosts* ativos, seus respectivos endereços IP e MAC *Address*. Este escaneamento está ilustrado na Figura 20, funcionando como um *ping* (teste de comunicação) nas máquinas que estão na rede, em seguida identificando-as.

Figura 20 - Escaneamento de *hosts* ativos



Fonte: Autoria Própria.

Quando um *host* não é encontrado na rede, o escaneamento informa que não foi possível se comunicar com o alvo especificado, ele pode estar realmente desconectado ou bloqueando a comunicação com o NMAP, conforme ilustrado na Figura 21:

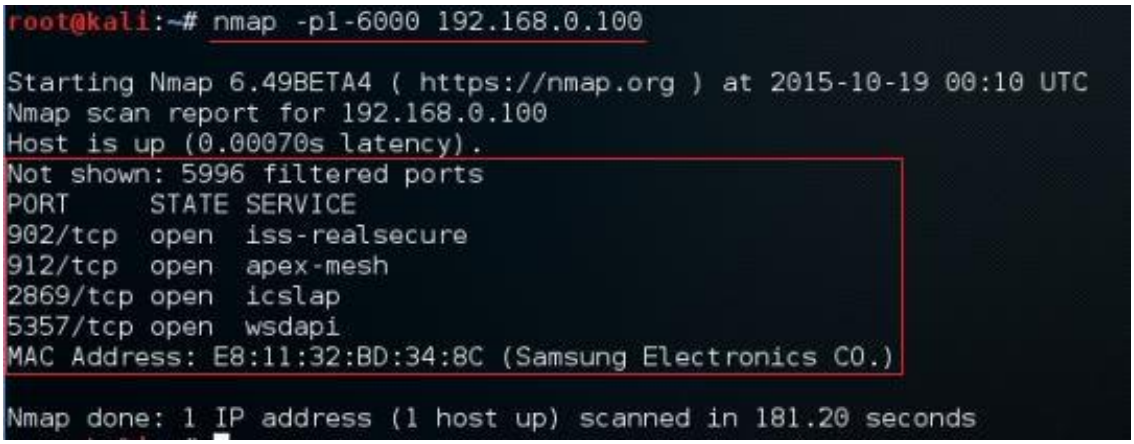
Figura 21 - Host desconectado

Fonte: Autoria Própria.

Como citado anteriormente, o NMAP apenas efetua o escaneamento das primeiras 1000 portas disponíveis. Diante desta situação, há casos em que é necessário verificar todas as 65.535 portas existentes. Com o parâmetro **-p <port range>**, é possível consultar todas ou somente as especificadas na pesquisa.

Conforme exemplo: **nmap -p1-6000 192.168.0.100**, na Figura 22 é possível analisar a pesquisa de 6000 portas:

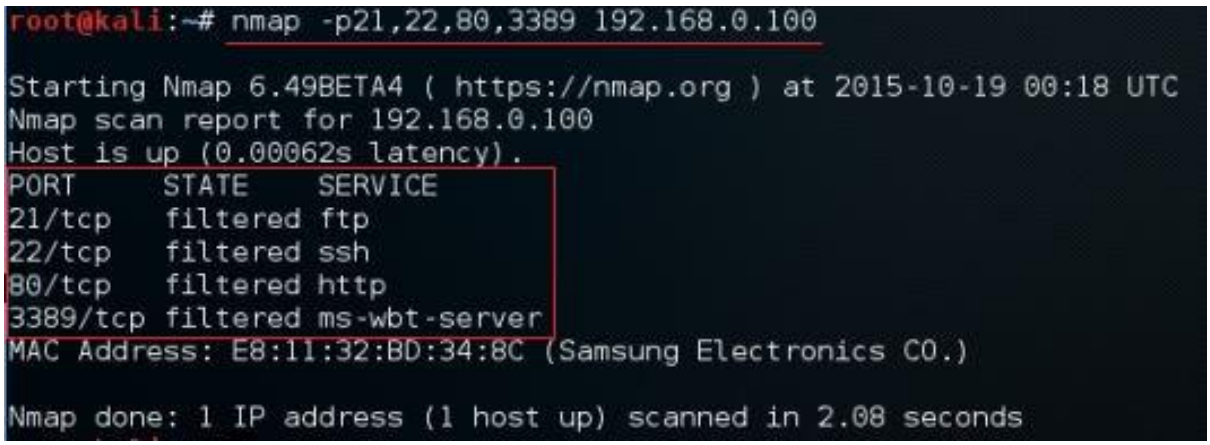
Figura 22 – Escaneamento de 6000 portas



Fonte: Autoria Própria.

Pode-se adicionar também no parâmetro apenas algumas portas específicas, separadas por vírgulas: **nmap -p21,22,80,3389 192.168.0.100**, conforme exemplo da Figura 23, onde buscou-se somente as portas 21, 22, 80 e 3389, porém se destacando no escaneamento os respectivos serviços de cada porta verificada:

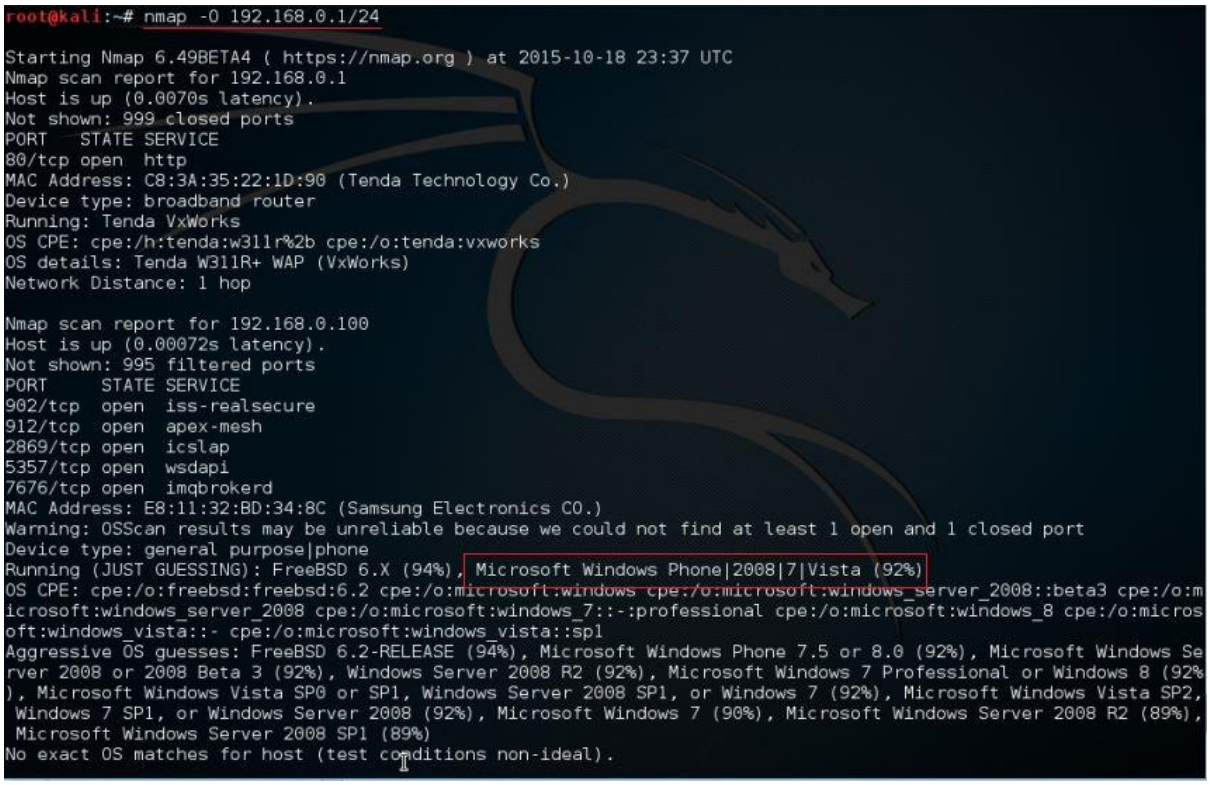
Figura 23 - Escaneamento de portas específicas



Fonte: Autoria Própria.

Quando o trabalho de auditoria exige mais informações sobre os *hosts* e seus sistemas operacionais, a opção **-O** deve ser utilizada e o parâmetro fica da seguinte forma: **nmap -O 192.168.0.1/24**, identificando rapidamente estes dados. Porém, pode se perceber na ilustração da Figura 24, que a determinação do sistema operacional não foi exata, e nestas situações algumas opções são informadas sobre o sistema do qual ele poderá ser.

Figura 24 - Detecção de sistema operacional



Fonte: Autoria Própria.

Para informações completas e detalhadas sobre o alvo a opção **-A** traz diversos dados do *host*, tais como: o serviço e a versão que está sendo executada na porta e a rota percorrida durante a troca de informações com o NMAP.

Uma infinidade de outras opções, podem ser utilizadas na pesquisa conforme destaca Christo (2015), onde algumas delas, apesar de trazerem resultados muito parecidos, em sua grande maioria existem diferenças, sendo importantíssimo a observação detalhada das informações.

4.3 Coleta de Dados e Exploração de Serviços

Nos escaneamentos preliminares foi possível identificar a diferença entre os sistemas operacionais onde, no Windows 10 as portas estavam com status filtrado, provavelmente protegida por algum mecanismo de segurança, já no Ubuntu 15 as portas estavam realmente fechadas. A Cert.Br (2012) orienta que para a maior proteção do seu computador é importante a utilização de um *firewall,* ou outro programa de proteção ativados. Normalmente o sistema operacional possuiu ferramentas de proteção ativados por padrão, mas, na maioria das vezes eles são desativados, para que possa se utilizar algum recurso na rede ou programa. O Windows traz como padrão, seu próprio *firewall* ativado, assim como o Linux tem o seu, o Netfilter, para que seja feito as configurações adequadas.

Conforme é destacado por Caruso e Steffen (1999), a utilização de *firewalls* executa a proteção contra o acesso à rede da organização, ele restringe o acesso a determinados recursos evitando assim o acesso a informações restritas ou bloqueadas, controlando tudo o que passa por ele.

Para o experimento da análise de viabilidade da ferramenta NMAP, desabilitou-se os *firewalls* destes dois sistemas operacionais, deixando o sistema proporcionalmente vulnerável e em seguida, efetuou-se o escaneamento com o auxílio da ferramenta NMAP, nas portas à procura de brechas no sistema.

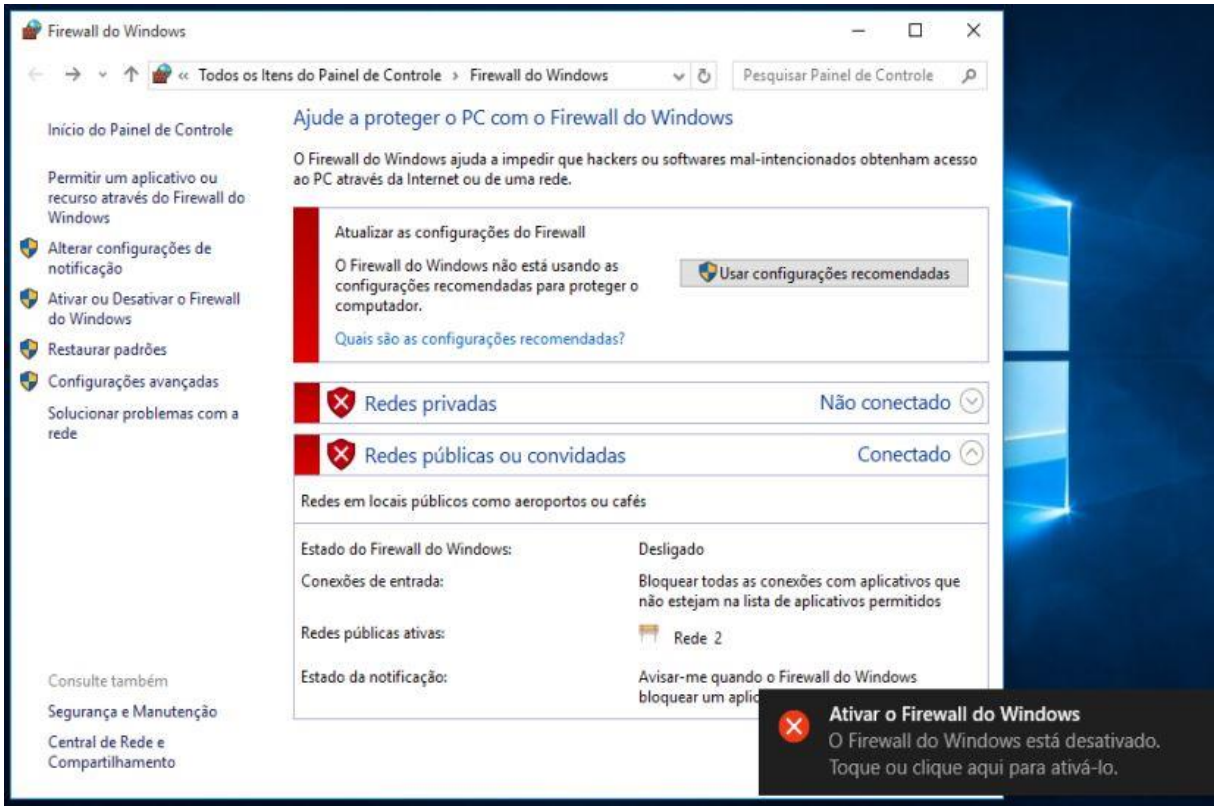
Após esta análise de informações e identificação de portas vulneráveis, foi aplicado aos mesmos sistemas operacionais, regras de *firewall* restringindo o acesso liberado anteriormente, executou-se novamente o escaneamento com a ferramenta NMAP, com o propósito de localizar se as mesmas vulnerabilidades nas portas encontradas no teste anterior, alteraram seu *status* protegendo de fato a comunicação na rede de testes.

4.3.1 Máquinas Vulneráveis

Aplicando as vulnerabilidades nos sistemas operacionais propostos no experimento, primeiramente acessou-se a máquina com Windows 10, foi desabilitado completamente o *firewall* do Windows, liberou-se o acesso remoto a máquina e a abertura de várias portas de comunicação.

Ao desativar o *firewall* o sistema operacional emite um alerta, informando a necessidade da utilização do mecanismo de segurança, os detalhes desta etapa são exibidos na Figura 25:

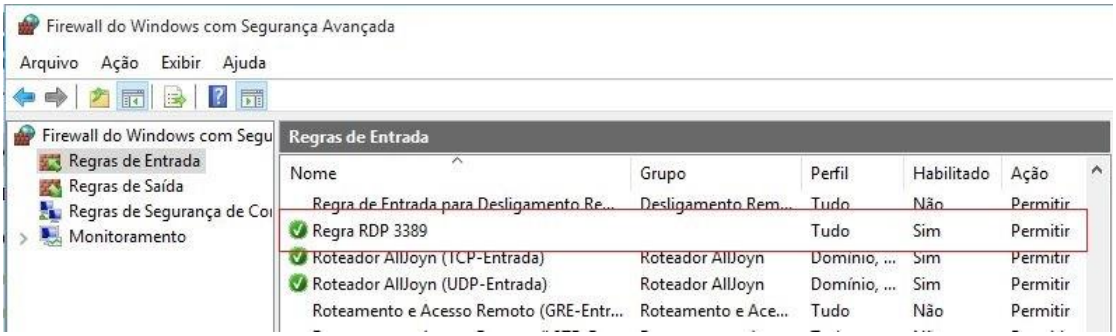
Figura 25 - Desativando o *firewall* do Windows



Fonte: Autoria Própria.

Nos controles de *firewall* do Windows também é possível aplicar regras específicas para algumas situações, fornecendo assim controle dos acessos ao *host*. Este adicionamento de regra para a porta 3389 pode ser conferida na Figura 26:

Figura 26 - Regras de *firewall* do Windows



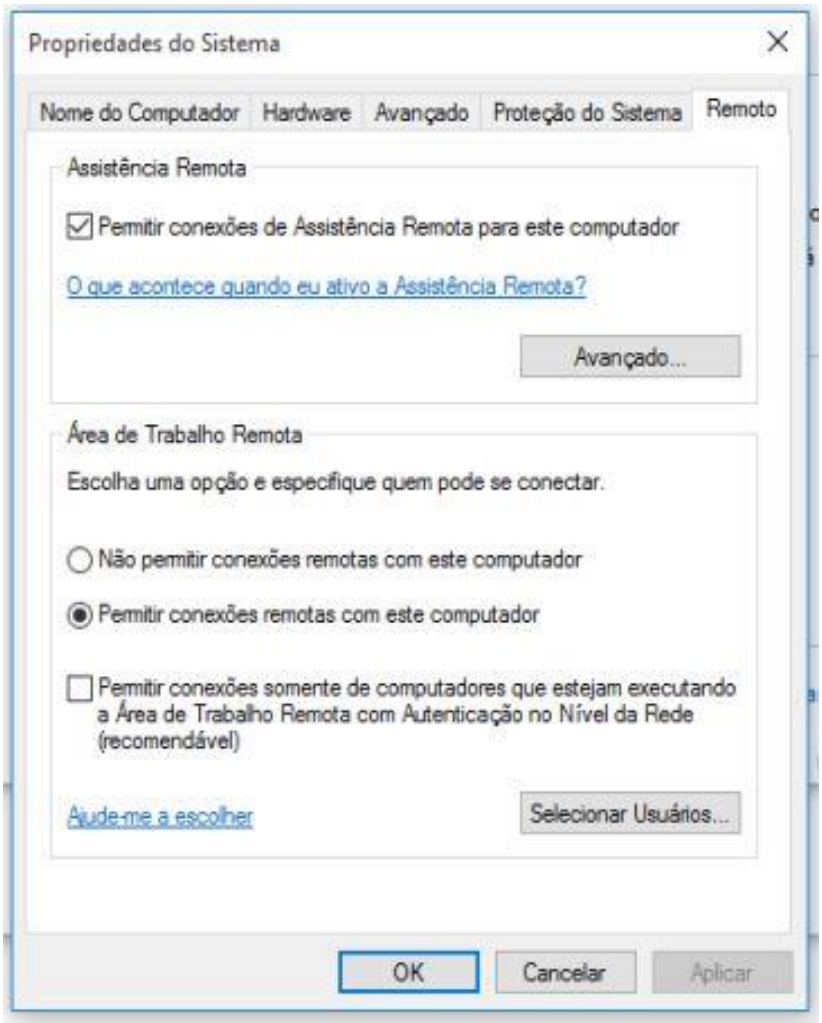
Fonte: Autoria Própria.

Em seguida foi adicionado a permissão de acesso da área de acesso remoto do Windows, da qual permite que seja acessado o sistema operacional de qualquer local com acesso à Internet, estando este computador em casa ou no trabalho, conforme orienta Moraz (2006).

Utiliza-se nos serviços de comunicação remota a porta 3389, sendo necessário a liberação do seu acesso também em mecanismos de controle de acesso à Internet, como um roteador ou modem, por exemplo. Este serviço também é chamado de “conexão de área de trabalho remota”, é nativamente uma aplicação do Windows e permite que seja conectado no computador remotamente, tendo acesso a todos os recursos do sistema operacional.

Na Figura 27 é ilustrado o local onde a ativação é efetuada. Uma tela intuitiva e de fácil acesso, encontrada nas configurações do Windows.

Figura 27 - Liberação acesso remoto do Windows



Fonte: Autoria Própria.

Continuando os procedimentos, na máquina UBUNTU 15 acessou o console da máquina aplicando as exceções nas regras de *firewall* do Linux, utilizando o Iptables, responsável pela interface entre o administrador de redes e o Netfilter, atribuiu-se a permissão de acesso completa ao sistema, sem nenhuma restrição.

Foi atribuído também a liberação da porta 3389, com o objetivo de fornecer o acesso remoto ao sistema, conforme ilustrado na Figura 28:

Figura 28 - Configurando regras Ubuntu 15

Fonte: Autoria Própria.

As máquinas estando propositalmente vulneráveis, executa-se o escaneamento da rede utilizando o NMAP, conforme detalhamento no tópico seguinte.

4.3.2 Escaneamento de Portas com NMAP

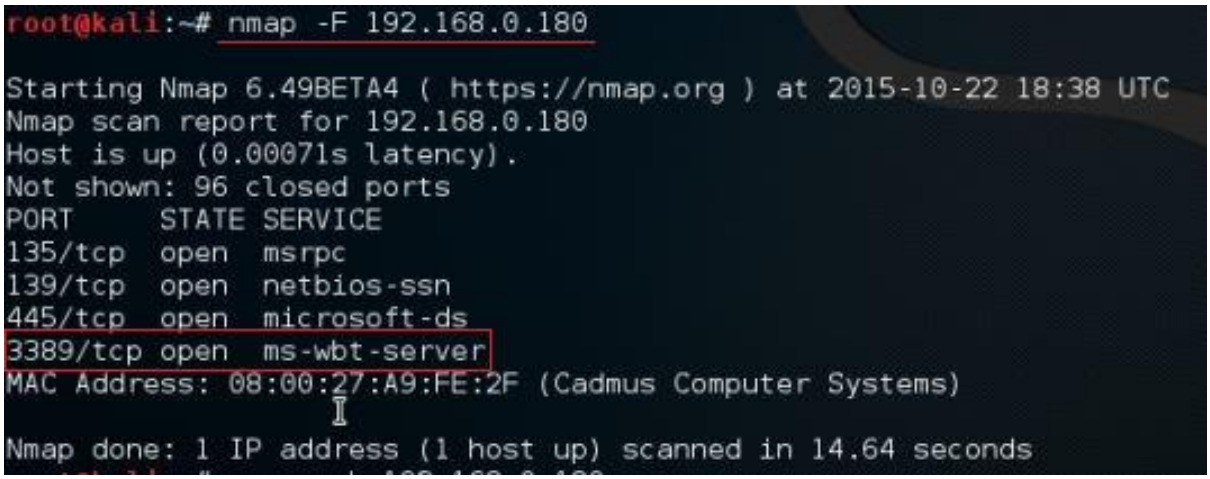
O escaneamento busca a identificação das portas vulneráveis a ataques, abertas na rede, onde um invasor pode através de escaneamento comum encontrar a que lhe for mais conveniente na busca por informações.

Nesta etapa do estudo proposto foram utilizados o parâmetro: **nmap -F 192.168.0.180**, cujo objetivo principal é de informar o estado da porta 3389, além desta informação conforme citado por Christo (2015), a opção **-F** executa de maneira rápida a busca pelas portas do *host* alvo.

Para o Windows 10 a identificação da porta 3389 foi efetiva, identificando seu estado aberta (*open*), estando exposta e disponível para um invasor efetuar uma invasão ao *host* alvo. Este indivíduo com o auxílio de outras ferramentas, pode facilmente acessar remotamente esta máquina e fazer posse de arquivos e

informações restritas. A abertura da porta em questão pode ser identificada a seguir, na Figura 29.

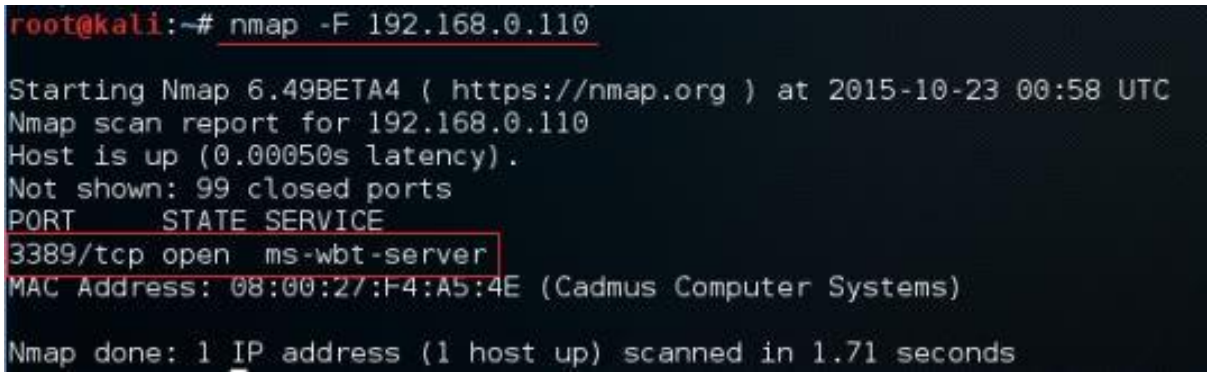
Figura 29 - Porta 3389 aberta no Windows 10



Fonte: Autoria Própria.

Para o Ubuntu 15 após as liberações das regras de *firewall* e utilizando o mesmo parâmetro: **nmap -F 192.168.0.110**, identificou-se o estado da porta 3389 como aberta (*open*), podendo vir a ser utilizada em um ataque. Este escaneamento pode ser verificado na Figura 30:

Figura 30 - Porta 3389 aberta no Ubuntu 15



Fonte: Autoria Própria.

Em ambos os escaneamentos, dos dois sistemas operacionais foram detectados o estado da porta 3389 como aberta (*open*), demonstrando assim a vulnerabilidade exposta. Com os dados em mãos o administrador de redes pode tomar providências evitando que isso seja explorado por um invasor.

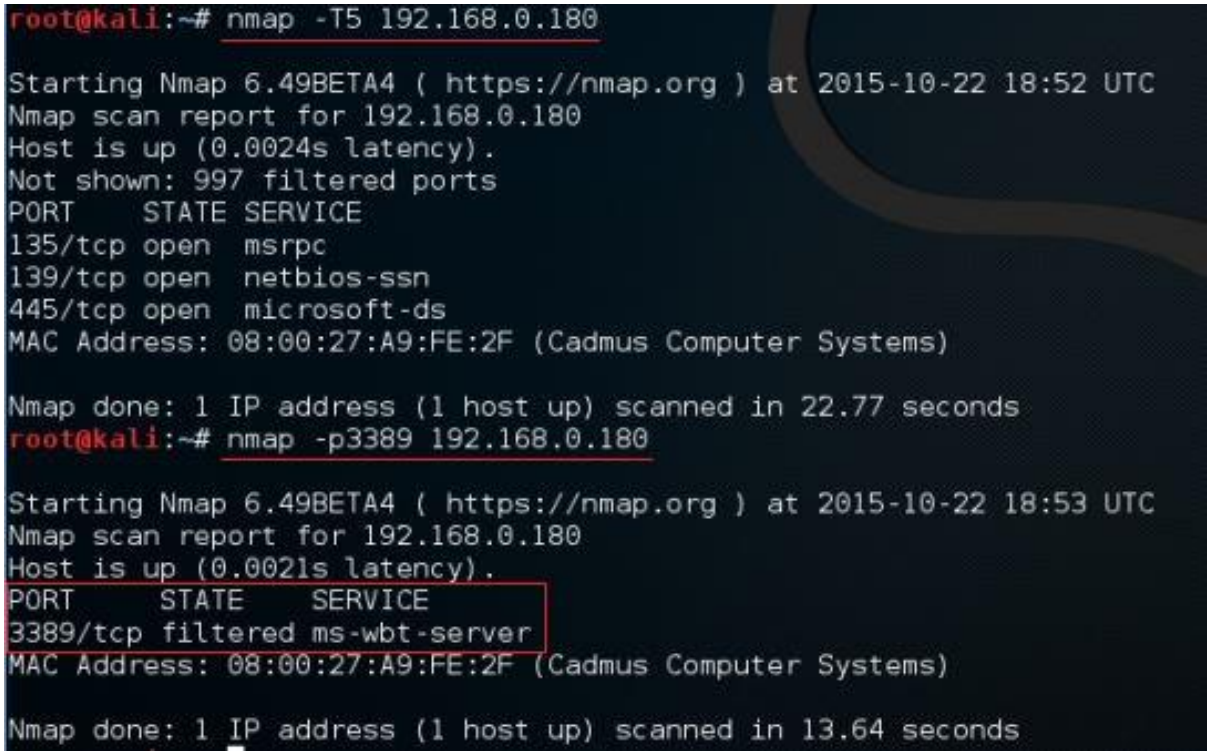
4.3.3 Efetividade do Escaneamento com NMAP

Após a aplicação de medidas de controle, desabilitando a opção de permissão de acesso remoto à máquina, assim como ativação do *firewall*, notou-se que na máquina Windows 10 trouxe a porta 3389, utilizada nos testes anteriores com estado filtrada (*filtered*), mostrando assim, a efetividade da ferramenta em identificar os estados das portas em uma rede, e proporcionar ao administrador medidas a serem tomadas para esta prevenção.

Utilizando o parâmetro **nmap -T5 192.168.0.180**, na orientação de Christo (2015) a opção **-T5**, funciona como um contador de tempo, e esta numeração identificada de 0 a 5, quanto maior, mais rápido será o escaneamento.

Em seguida utilizou o parâmetro **nmap -p3389 192.168.0.180**, com o propósito de identificar o estado real da porta 3389, exibindo-a como filtrada (*filtered*), onde algum mecanismo de segurança está protegendo o acesso a esta porta, e consequentemente ao serviço executado por ela. Estes escaneamentos podem ser verificados conforme ilustrado a seguir na Figura 31:

Figura 31 - Escaneamento com as medidas de segurança aplicadas no Windows

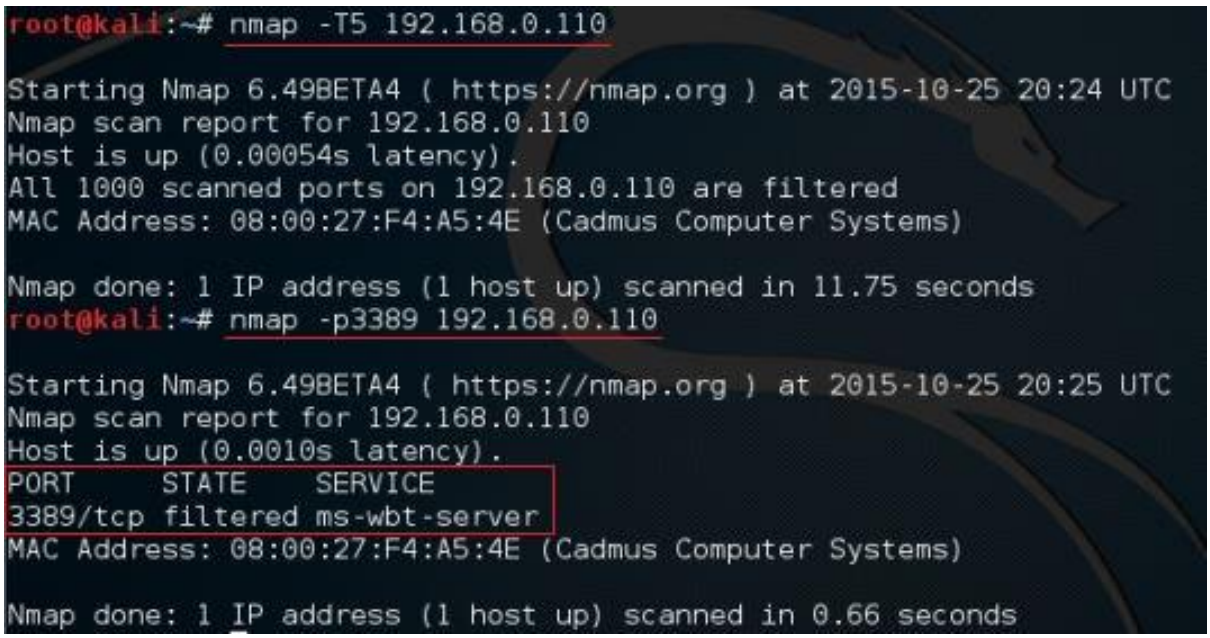


Fonte: Autoria Própria.

Efetuado o mesmo procedimento, desta vez na máquina Ubuntu 15, a procura da abertura das portas em questão, utilizando o parâmetro **nmap -T5 192.168.0.110**, para a verificação das portas mais básicas do NMAP, nenhuma porta estava em estado aberto (*open*). Em seguida foi efetuando o escaneamento com o parâmetro **nmap -p3389 192.168.0.110**, localizando a porta 3389 utilizada nos testes, ela se encontra filtrada (filtered), estando restringida o seu acesso pelo *firewall*, aplicado através de regras do Iptables.

Este resultado demonstra como as regras utilizadas podem proteger o acesso ao host, primordial quando se mantém informações que não devem ser visualizados por todos. As regras podem ser utilizadas para todo tipo de acesso, inclusive para outros serviços e consequentemente, portas diferentes. A efetividade da ferramenta NMAP em detectar e identificar tais *status* das portas em *hosts* em uma rede de computadores, podem ser analisadas conforme ilustrado a seguir na Figura 32:

Figura 32 - Escaneamento com as medidas de segurança aplicadas no Ubuntu



Fonte: Autoria Própria.

4.4 Medidas de Prevenção

Utilizando uma política de *firewall*, observou a eficiência da proteção da rede, e em conjunto com outras pequenas medidas de segurança, podem ser adotadas para

que fique mais protegida e segura, tais como: autenticação de usuário na rede, antivírus, sistema de detecção de intrusos (IDS) e etc.

Quando o usuário realmente precisa efetuar o acesso a máquina através do acesso remoto, um recurso que pode ser utilizado para garantir a segurança das informações é a utilização de nome de usuário e senhas bem elaboradas, conforme destaca Stallings (2007). Uma senha forte pode fazer com que uma intrusão de força bruta seja extremamente complexa e lenta, tornando inviável a um invasor continuar os procedimentos de invasão.

O redirecionamento de portas também é uma opção efetiva, uma vez que o NMAP efetua o escaneamento das primeiras 1000 portas, ele não consegue localizar a porta com numeração alta em um escaneamento simples. Um invasor normalmente não efetua este tipo de escaneamento, pois leva um tempo excessivo e poderia ser descoberto neste processo.

Programas fornecidos no mercado oferecem rastreamento de acessos indevidos na rede, emitindo alertas em casos de invasão, tornando assim, a rede mais segura.

A seguir apresenta-se as conclusões obtidas com o teste realizado no estudo proposto.

5 CONSIDERAÇÕES FINAIS

A presente pesquisa proporcionou a constatação da necessidade da utilização de ferramentas de auditoria e controles de invasão, primordiais nos dias atuais, onde o ambiente de redes de uma organização está conectado constantemente a rede de computadores e consequentemente a Internet.

Estas medidas devem ser adotadas tendo em mente a complexidade de se conseguir aplicá-las, uma vez que muitas empresas não fornecem recursos suficientes para que seja adequado uma política de segurança efetiva. Porém, como o NMAP é uma ferramenta de *software* livre e gratuita, auxilia na obtenção dessas informações reduzindo os custos necessários no processo. As auditorias devem ser constantes e promover ao administrador de redes informações detalhadas sobre os equipamentos na rede da organização, elaborar planos emergências e controles que minimizam o impacto para a organização.

As ferramentas de escaneamento, em principal o NMAP, é primordial nesta utilização e busca por informações relevantes na proteção dos dados. A ferramenta somente aponta as vulnerabilidades, não as corrige, tornando-se essencial no uso em auditorias. Por se tratar de uma ferramenta gratuita, pode ser utilizada por qualquer técnico de redes que tenha o propósito de controlar o acesso na rede.

Destaca-se como a ferramenta conseguiu identificar as portas vulneráveis dos *hosts* alvos e com uma medida de segurança simples, conseguir verificá-las novamente, demonstrando sua eficiência. Com estes dados em mãos, políticas simples de segurança devem ser adotadas pelo administrador de redes com o ideal de mantê-la segura e protegida. Em pequenas organizações o escaneamento aponta pequenas falhas e podem ser facilmente corrigidas, em uma grande organização, com mecanismos de segurança, como os *firewalls* aplicados, auxilia-se na detecção de falhas na atribuição destas regras, conseguindo assim uma efetividade nas ações a serem tomadas, promovendo a segurança dos dados.

O uso de ferramentas de escaneamento não só proporciona a verificação destas brechas na rede, como também fornece dados para que seja executado um inventário preciso de todo o ambiente computacional, determinando quais *hosts* estão ativos na rede, seus sistemas operacionais, identificação de endereço IP com o objetivo de catalogar os equipamentos.

A ferramenta também proporciona aos *pentesters*, a localização exata dos alvos e os problemas a serem explorados, identificando-os e promovendo medidas de segurança para que não se torne alvo de um atacante real.

Conforme as hipóteses apontaram a utilização do NMAP apresenta resultados confiáveis e de fácil compreensão do administrador de redes, para que posteriormente sejam tomadas as medidas necessárias de prevenção a ataques e segurança das informações da organização. Demonstrou-se do quão importante é o uso de um mecanismo para prever as vulnerabilidades em uma rede e adotar controles eficientes mantendo os dados em segurança.

Propõe para trabalhos futuros a utilização do NMAP em um ambiente de maior complexidade, aplicando a ferramenta na busca por vulnerabilidades em outros serviços, tais como SSH, FTP, SMTP e vários outros que são utilizados no dia a dia de uma organização. Considera-se uma opção também o uso em conjunto de ferramentas de detecção de intrusão na rede, ou análise de logs de acesso apontando através de relatórios as tentativas efetivas de acesso à rede.

REFERÊNCIAS

ABNT NBR ISO/IEC 17999, **Tecnologia da informação** – Técnicas de segurança – Código de prática para a gestão da segurança da informação. 2.ed. Rio de Janeiro: ABNT, 2005. p. IX.

ABNT NBR ISO/IEC 27002 **Tecnologia da informação** – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2013.

BROAD, James; BINDNER, Andrew **Hacking com Kali Linux**: técnicas práticas para testes de invasão. 1.ed. São Paulo: Novatec, 2014. p. 18; 20-24.

CARUSO, Carlos A. A.; STEFFEN, Flávio D. **Segurança em informática e de informações**. São Paulo: SENAC, 1999.

CERT.BR. Comitê Gestor de Internet no Brasil: **Cartilha de segurança da informação para Internet**. 2.ed. São Paulo, 2012.

CHRISTO, Luís H. **Linux BackTrack R5**: Identificando *hosts* – Praticando e obtendo informações. Rio de Janeiro: Ciência Moderna, 2015. p. 73.

DAWEL, George **A Segurança da informação das empresas**. Rio de Janeiro: Ciência Moderna, 2005. p. 24; 66.

ENGEBRETSON, Patrick **Introdução ao hacking e aos testes de invasão**: Facilitando o hacking ético e os testes de invasão. 1.ed. São Paulo: Novatec, 2014. p. 23-24; 26; 43-45.

FONTES, Edison **Segurança da informação**: o usuário faz a diferença. 1.ed. São Paulo: Saraiva, 2006. p. 6; 11.

_____. **Praticando a segurança da informação**. 1.ed. Rio de Janeiro: Brasport, 2008. p. 123.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 3.ed. Porto Alegre: Bookman, 2006.

GIAVAROTO, Sílvio C. R.; SANTOS, Gerson R. dos **Backtrack Linux**: Auditoria e teste de invasão em redes de computadores. Rio de Janeiro: Ciência Moderna, 2013. p. 1-2; 37-40; 63; 79; 81-82; 101-103.

_____. **Kali Linux**: Introdução ao penetration testing. Rio de Janeiro: Ciência Moderna, 2015.

GOODRICH, Michael T.; TAMASSIA, Roberto **Introdução à segurança de computadores**. 1.ed. Porto Alegre: Bookman, 2013. p. 3.

HPING.ORG **HPING man page**. Disponível em: <http://www.hping.org/manpage.html>. Acesso em 29 set. 2015.

IMONIANA, Joshua O. **Auditoria de sistemas de informação**. 2.ed. São Paulo: Atlas, 2013. p. 54; 57-58.

KALI.ORG **AMAP package description**. Disponível em: <http://tools.kali.org/information-gathering/amap>. Acesso em: 29 set. 2015.

_____. **Download page**. Disponível em <https://www.kali.org/downloads/>. Acesso em 18 out. 2015.

KUROSE, James F.; ROSS, Keith W. **Redes de comutadores e a Internet**. 5.ed. São Paulo: Pearson, 2010.

LYON, Gordon F. **Exame de redes com NMAP**. 1.ed. Rio de Janeiro: Ciência Moderna, 2009. p. 12-13; 77-79.

LYRA, Maurício R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Ciência Moderna, 2008. p. 6; 109-115.

MICROSOFT **Windows 10**: Download do Software. Disponível em: <https://www.microsoft.com/pt-br/software-download/windows10>. Acesso em 20 out. 2015.

MORAZ, Eduardo **Treinamento profissional anti-hacker**. São Paulo: Digerati Books, 2006.

MORIMOTO, Carlos E. **Redes**: Guia prático. 2.ed.rev.ampl. Porto Alegre: Meridional, 2011.

_____. **Significado de siglas**. Disponível em: < http://www.hardware.com.br/artigos/significado-siglas/>. Acesso em: 03 nov. 2015.

NMAP.ORG **Técnicas de escaneamento de portas**. Disponível em: <https://nmap.org/man/pt_BR/man-port-scanning-techniques.html>. Acesso em: 13 out. 2015.

_____. **Especificação de portas e ordem de scan**. Disponível em: <https://nmap.org/man/pt_BR/man-port-specification.html>. Acesso em: 13 out. 2015.

_____. **Fundamentos do escaneamento de portas**. Disponível em: <https://nmap.org/man/pt_BR/man-port-scanning-basics.htmll>. Acesso em: 13 out. 2015.

_____. **Técnicas de escaneamento de portas**. Disponível em: <https://nmap.org/man/pt_BR/man-port-scanning-techniques.html>. Acesso em: 13 out. 2015.

PEREIRA, Pedro **Como funcionam os scans?** Disponível em: <http://www.pedropereira.net/tecnicas-de-scan-ack-fin-syn-tcp-xmas-null-scan/>. Acesso em: 10 out. 2015.

ROTH, Luiz C. **Teste de invasão com uso de software livre e ferramentas open source em redes corporativas**. 2011. 58p. Redes de Computadores – Universidade Tuiuti do Paraná, Curitiba.

SÊMOLA, Marcos **Gestão da segurança da informação**: Visão executiva da segurança da informação. 10.ed. Rio de Janeiro: Elsevier, 2003.

STALLINGS, William **Criptografia e segurança de redes**: Princípios e práticas. 4.ed. São Paulo: Pearson, 2007. p. 4; 6.

UBUNTU **Ubuntu 15.04**: Vivid Vernet desktop image. Disponível em: <http://releases.ubuntu.com/15.04/>. Acesso em: 23 out. 2015.