CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

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

USO DO NMAP EM VARREDURAS DE SEGURANÇA DE REDES

VICTOR ALBERTO DE BARROS

Americana, SP
2014

CENTRO PAULA SOUZA
GOVERNO DO ESTADO DE SÃO PAULO

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

USO DO NMAP EM VARREDURAS DE SEGURANÇA DE REDES

VICTOR ALBERTO DE BARROS

victor.albarros@gmail.com

Trabalho Monográfico, desenvolvido em cumprimento à exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da Fatec-Americana, sob orientação da Profa. Ms. Maria Cristina Luz Fraga Moreira Aranha.

Área: Segurança da Informação

Americana, SP
2014

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

B284u

Barros, Victor Alberto de
Uso de NMAP em varreduras de segurança de redes. / Victor Alberto de Barros. – Americana: 2014.
f.

Monografia (Graduação de Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Maria Cristina da Luz Fraga Moreira Aranha

1.Segurança em Sistemas de informação 2. Redes de computadores I. Aranha, Maria Cristina da Luz Fraga Moreira II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

BANCA EXAMINADORA

Prof. Ms. Maria Cristina Luz Fraga Moreira Aranha

Prof. Dr. Alexandre Mello Ferreira

Prof. Ms. Alexandre Garcia Aguado

AGRADECIMENTOS

Agradeço à Professora Maria Cristina Luz Fraga Moreira Aranha pela confiança, paciência, dedicação e ajuda dada no desenvolvimento do trabalho.

Ao professor Alexandre Garcia Aguado por ter ajudado no início deste trabalho e pelas sugestões dadas que foram de grande valor para a execução do mesmo.

Aos colegas de classe, que no decorrer do curso viraram amigos e me ajudaram indicando materiais e dando apoio moral para a conclusão do curso e deste trabalho.

DEDICATÓRIA

Dedico a toda a minha família, em especial aos mais próximos e à minha namorada.

RESUMO

Com o advento da informática e rápida expansão da Internet e das redes de computadores, surgiram necessidades específicas relacionadas à segurança das informações armazenadas e manipuladas em meios digitais. Este trabalho apresenta conceitos de segurança da informação e explora parte dos recursos de uma ferramenta chamada NMAP (*Network Mapper*), bastante utilizada por administradores de segurança de redes. O NMAP pode ser considerado basicamente como um *port scanner* (*scanner* de portas), no entanto, é considerável o número de informações que podem ser obtidas de uma rede de computadores com o uso do NMAP. Dessa forma, é feita uma apresentação da ferramenta, mostrando alguns de seus recursos e comandos básicos e, em seguida, é apresentado um experimento prático, realizado em um ambiente virtualizado controlado mostrando alguns recursos que o NMAP oferece e como a ferramenta ajuda a encontrar falhas em componentes de uma rede. Finalmente, são apresentados e analisados cada um dos resultados obtidos nos testes feitos comprovando a eficácia da ferramenta, para melhorar a segurança de redes. Novos trabalhos são sugeridos usando outros recursos da ferramenta, embora não explorados neste trabalho, visando ampliar os conhecimentos sobre o NMAP, relacionados à segurança da informação.

Palavras Chave: NMAP; redes; portas; segurança da informação.

ABSTRACT

With the advent of computers and fast expansion of Internet and computer networks, specifics needs related to the security of information stored and manipulated in digital media appeared. This paper presents concepts of information security and explores part of the resources from a tool named NMAP (Network Mapper), widely used by network security administrators. NMAP can be basically considered as a port scanner, however, it is considerable the number of information that can be obtained from a computer network using NMAP. This way, it is made a tool's presentation showing some resources and basic commands and, next, it is presented a practical experiment that took place in a controlled virtualized environment showing some resources that NMAP offers and how the tool helps to find failures in components from a network. Finally, results obtained are presented and analyzed proving the tool's effectiveness, to improve the security of the networks. New papers are suggested using other tool's resources, although not explored in this paper, aiming to extend the knowledge about NMAP, related to the information security

Keywords: *NMAP; networks; ports; information security*.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

As últimas décadas presenciaram uma grande mudança de comportamento nas organizações quando o assunto é a informática. Dos anos 80 até os dias de hoje, ocorreram grandes avanços tecnológicos, que, em sua maioria, facilitaram e agilizaram diversas tarefas do cotidiano, tanto pessoal quanto empresarial. Usando os mesmos argumentos, a utilização da Internet também se popularizou em grande escala, e, atualmente, pode-se acessar a Internet praticamente de qualquer lugar. Junto com esses avanços, também surgiram novos problemas e preocupações para aqueles que administram essas redes. Vírus, *spywares, malwares, worms*, entre muitas outras ameaças, estão presentes até hoje e é necessário conhecer o maior número possível de formas de ataque existentes, para poder se proteger e saber como reagir caso seja vítima desses tipos de ataques. Entre os diversos tipos de ferramentas de proteção existe uma, bastante utilizada, na tentativa de se detectar vulnerabilidades em redes. Esta ferramenta é o NMAP (*Network Mapper*).

Justifica-se a escolha deste tema tendo em vista a importância, cada vez maior, do aspecto “Segurança da Informação” no contexto da tecnologia da informação. Apesar da ferramenta NMAP ter sido divulgada em 1997, atualmente é uma ferramenta largamente utilizada por administradores de redes para encontrar vulnerabilidades que possam existir em redes de computadores (JACKSON, 2010). Os recursos da ferramenta são muitos e a diversidade de sua utilização também.

O objetivo geral deste trabalho é mostrar qual a real importância do NMAP para administradores de segurança de redes. Vale lembrar que, da mesma forma que administradores de rede usam o NMAP para se proteger de ataques, atacantes também podem usar a mesma ferramenta para encontrar vulnerabilidades em alguma rede. O problema a ser solucionado, apresentado neste trabalho, é como a ferramenta NMAP pode auxiliar um administrador de redes a encontrar falhas de segurança em sua rede e corrigi-las.

Os objetivos específicos são: apresentar conceitos básicos de segurança da informação; apresentar algumas ferramentas que podem ser utilizadas na busca de garantir a segurança das informações; mostrar de forma teórica como o NMAP atua em uma busca de vulnerabilidades em uma rede; usar de forma prática parte dos seus

recursos oferecidos, buscando vulnerabilidades em um ambiente controlado e fornecer explicações técnicas de como suas atividades são realizadas.

Os procedimentos metodológicos usados neste trabalho são: realização de uma pesquisa bibliográfica e digital; criação de um ambiente de virtualização controlado para fins de comprovação do funcionamento de alguns dos recursos oferecidos pelo NMAP. Nesse ambiente virtualizado controlado utilizou-se uma máquina hospedeira com o sistema operacional *Microsoft Windows 7* e duas máquinas virtuais com o sistema operacional *Linux*, sendo utilizada a distribuição *Back Track* em uma delas e a *Mint* na outra.

Os capítulos que se seguem são organizados da seguinte maneira: No capítulo 2, apresenta-se o levantamento bibliográfico que sustenta a solução do problema, apresentada neste trabalho, destacando conceitos de segurança da informação, auditorias de sistemas e formas de se garantir a segurança da informação. O capítulo 3 apresenta a ferramenta NMAP com seus comandos básicos e parte das suas capacidades e funções. O quarto capítulo apresenta um experimento realizado em ambiente virtualizado controlado baseado nos conceitos apresentados anteriormente, visando mostrar que o uso da ferramenta NMAP é eficiente dentro de uma organização. O quinto e último capítulo traz as considerações finais, conclusões obtidas a partir do levantamento bibliográfico realizado e do experimento prático apresentado, além de sugestões para trabalhos futuros.

2 LEVANTAMENTO BIBLIOGRÁFICO

Nesse capítulo, são apresentados conceitos relativos à segurança da Informação, definições relacionadas à Auditoria de redes, além de técnicas e ferramentas utilizadas busca da garantia da Segurança da Informação.

2.1 CONCEITOS BÁSICOS DE SEGURANÇA DA INFORMAÇÃO

Stallings (2008) afirma que, nas últimas décadas, as organizações passaram por grandes mudanças quando o assunto é proteção das informações. Quando todas as informações produzidas eram armazenadas em papel, o armazenamento feito em armários com fechadura para protegê-las de acessos indevidos era o suficiente. No entanto, com o uso generalizado de equipamentos de processamento, armazenamento eletrônico de dados e a rápida evolução da informática, foi necessária uma alteração nos requisitos de segurança da informação, implantando novos mecanismos de proteção desses dados.

Para se apoiar esse processo, há dois conceitos, a saber:

- Segurança de computador, que prevê o uso de mecanismos de proteção contra ação de softwares maliciosos e ações de *hackers* invasores, visando soluções locais instaladas nas máquinas utilizadas diretamente pelo usuário final.
- Segurança Inter rede, pois como na grande maioria, os computadores trabalham em sistemas distribuídos, o especialista em segurança deve atentar sobre como os dados são trafegados, para que eles possam ser classificados como confiáveis e utilizados da melhor maneira pela organização (STALLINGS, 2008).

De acordo com Jackson (2010), quando se trata de segurança da informação, não se faz segurança de um produto, mas sim de um processo. Além disso, o processo de segurança da informação deve estar em um ciclo contínuo, não tendo início, meio e fim, pois não se pode garantir segurança total dos ataques existentes de todas as fontes, no entanto, pode-se garantir um processo de segurança eficiente, alcançando-se assim um alto índice de proteção. Jackson cita ainda cinco pilares essenciais na garantia da segurança, que são: Avaliação, Prevenção, Detecção, Reação e Recuperação, cujos conceitos são apresentados a seguir:

Avaliação: Inicialmente é necessário conhecer o negócio, como a corporação trabalha, quais áreas são mais críticas e sensíveis e quais merecem mais atenção e aplicação de recursos para evitar perda e indisponibilidade dos dados. No processo de avaliação é necessário conhecer aspectos da organização fora da área da tecnologia da informação, como quais ameaças de negócio podem afetar a corporação, qual a frequência de tentativa de ataques em geral, legislação sobre o negócio desempenhado pela companhia, políticas e procedimentos de negócio adotados pela organização, além dos componentes tecnológicos disponíveis e da estrutura física e lógica já disponível no negócio. Ao se fazer a avaliação do negócio, é importante considerar as mudanças comportamentais da organização, pensando em novos produtos e serviços lançados, mudanças de procedimentos internos, entre outros.

Prevenção: A prevenção não é adquirida somente com a implementação de recursos tecnológicos avançados, mas também com conscientização, políticas de segurança e de procedimentos. Documentar uma política com regras, conscientizando as pessoas envolvidas, especificando as punições e ajudando os usuários a entender melhor os sistemas auxilia muito a empresa a reduzir as chances de ter suas informações atacadas. Não se pode proteger a informação de todas as ameaças existentes, não existe sistema totalmente seguro, então, usa-se o termo segurança em profundidade, no qual separam-se as ameaças em camadas, classificando as maiores e as menores vulnerabilidades, e aplicando as ferramentas técnicas, como *firewalls*, sistemas de prevenção de intrusão, entre outros. Os recursos tecnológicos têm um grande papel no processo de segurança da informação. No entanto, não são 100% eficientes se, em paralelo, não existirem processos administrativos que garantam o bom uso da informação.

Detecção: Sistemas de detecção são extremamente importantes. Não havendo um sistema de detecção, é muito difícil saber se houve um ataque na rede, se as informações estão realmente resguardadas, e se é realmente garantido confiar nos sistemas de prevenção adotados. É importante que os mecanismos de detecção estejam funcionando adequadamente e que sejam devidamente monitorados, assim é possível identificar uma falha, um acesso indevido ocorrido no sistema e formular uma reação o mais rápido possível, para que o funcionamento volte à sua normalidade.

Reação: Quando a prevenção e a detecção são efetivas o tempo de reação é bastante reduzido. Ninguém quer ter uma falha de segurança em sua rede, mas quando é descoberta, a ação recomendada é fazer algo para sanar essa falha rapidamente. A reação à falha é o aspecto da segurança que está diretamente ligado com o tempo. Deve-se preocupar com a redução do tempo de detecção e resposta para que a falha de segurança não venha a se tornar um incidente para a corporação. Mas reduzir o tempo de detecção não é suficiente se não foi feito um planejamento de tratamento dos incidentes. Mesmo com o uso de ferramentas automatizadas de tratamento a incidentes, dependendo do porte da companhia, recomenda-se a existência de uma equipe responsável por resposta a incidentes.

Recuperação: Quando a falha não pôde ser evitada e um incidente ocorreu, é necessário executar a recuperação do sistema para deixá-lo novamente disponível aos usuários. Mas, além disso, é necessário e importante descobrir a falha, a origem do incidente para que, quando o sistema voltar a funcionar, não haja a mesma vulnerabilidade. Para isso, existem perguntas que devem ser respondidas durante o processo de recuperação: O que comprometeu o sistema? Houve falhas nas ferramentas de controle? Houve uma falha de configuração? Enfim, é necessário ter esse processo de recuperação concluído e documentado para que o mesmo incidente não se repita, ou seja, tenha sido tratado corretamente.

Para Giavaroto e Santos (2013), a informação é um dos ativos mais importantes de uma corporação; está presente em todos os processos e está diretamente ligada a tomadas de decisões, podendo acarretar lucros ou perdas para sua detentora, dependendo da forma como é utilizada. São apontados três conceitos principais como sendo a tríade da Segurança da Informação. São eles: Confidencialidade, Integridade e Disponibilidade. Segue explicação de cada um dos termos:

Confidencialidade: O princípio da confidencialidade explicita que as informações devem estar disponíveis somente a quem está autorizado a vê-las e/ou manipulá-las. Desta maneira, se um indivíduo obtivesse acesso a determinada informação utilizando-se de senhas de um terceiro, por exemplo, tal ato seria considerado uma violação do princípio da confidencialidade.

Integridade: O princípio da integridade garante que a informação acessível esteja íntegra e, dessa maneira, confiável. Uma informação só pode ser utilizada para tomada de decisões importantes caso esteja confiável. Estar íntegra significa que não houve adulterações, sejam elas intencionais ou por falha de hardware ou software, por exemplo (um caso de perda de integridade da informação seria uma alteração indevida na quantidade de estoque de um produto em determinada empresa).

Disponibilidade: O princípio da disponibilidade define que todas as informações devem estar acessíveis a quem tiver autorização para usá-las, sempre que for necessário. Num caso de ataque de negação de serviço, onde um servidor para de responder a requisições, é configurada uma violação de disponibilidade, pois as informações que deveriam ser acessadas não são mais repassadas ao requisitante.

2.2 COMO GARANTIR A SEGURANÇA DA INFORMAÇÃO

Dawel (2005) afirma que para se garantir a segurança em uma corporação, é necessário responder algumas perguntas para que se possa avaliar a real necessidade de proteção e os possíveis riscos e ameaças que possam estar presentes no processo da informação. As perguntas são: Quando se deseja proteger algo, deseja-se proteger do quê? De quem? Quais as ameaças que estão sobre as informações? Há algum tipo de defesa natural? Quais as defesas adicionais necessárias? Quais as vulnerabilidades? O que acontece se a informação for perdida ou danificada? E, para finalizar, qual o valor da informação e qual o valor das medidas adicionais de proteção?

Fontes (2008) diz que uma das regras básicas para a garantia da segurança das informações é a classificação delas. Através de regras claras, definir quem tem acesso a qual informação, qual o peso dessa informação para a corporação e quais os prejuízos, caso ocorra vazamento dessa informação, ou acesso por pessoas não autorizadas. Dessa maneira, expondo de forma clara o acesso de cada um dentro do processo do negócio, fica mais fácil definir as regras, aplicar recursos e gerir a informação presente na corporação. Fontes diz ainda que quem deve definir a classificação das informações é uma pessoa que exerce o papel de gestor da informação. O nível de classificação pode ser modificado com o passar do tempo, com o desenvolvimento da organização e seu ramo de atuação. Além disso, não existe

uma regra pré-estabelecida para a classificação da informação; cada corporação pode adotar a medida mais adequada às atividades desempenhadas.

Lyra (2008) aponta as pessoas como sendo os elementos centrais de um sistema de segurança da informação, dizendo ainda que todos os incidentes de segurança envolvem pessoas. Deve ser desempenhado um papel superior no processo de segurança da informação por uma pessoa indicada para tal, mas todos os colaboradores devem estar envolvidos no processo de segurança, independente da função desempenhada na empresa.

O comprometimento do usuário, para Fontes (2008), é um fator fundamental para o sucesso na obtenção da segurança de uma corporação. Não adianta ter os melhores recursos tecnológicos, controles de acesso aplicados perfeitamente ou sistemas de *backup* funcionando perfeitamente se os usuários passam a senha uns para os outros para que o sistema possa ser acessado quando um deles estiver ausente, ou se o usuário anota sua senha em um local visível para não esquecê-la, deixando à vista para qualquer pessoa que chegar em seu local de trabalho, ou ainda se o colaborador não armazenar seus arquivos nos diretórios alocados para tal função. Fontes também cita a existência de elementos terceirizados na execução do negócio. Serviços como controle de acesso, limpeza e manutenção predial, entre outros costumam ser terceirizados, pois a empresa contratante foca somente a sua atividade específica. Nesses casos, deve-se deixar bem claro para os terceiros as regras de segurança da empresa para que eles possam se adequar ao processo do negócio. A principal maneira de se garantir que os terceiros tenham suas responsabilidades e deveres bem explicitados é através de um documento chamado SLA – *Service Level Agreement* (Acordo de nível de Serviço). No SLA são previstos, de maneira clara e quantificável, os objetivos e as responsabilidades tanto do contratante, quanto do terceiro.

A execução de auditoria nos sistemas também é de grande importância, de acordo com Manotti (2010), pois através dela é garantida a confiabilidade das informações, através de avaliações que envolvem hardware, software, infraestrutura, pessoas e também os procedimentos envolvidos no negócio.

2.3 DEFINIÇÃO DE AUDITORIA DE REDES

A auditoria de sistemas é definida como uma revisão e avaliação dos controles, desenvolvimento dos sistemas, procedimentos de TI, infraestrutura, desempenho, operação e segurança da informação, onde são envolvidos os processamentos de informações críticas utilizadas para tomadas de decisões. Uma auditoria não deve se limitar a avaliar os equipamentos de informática, mas tudo que os envolvem, como pessoas, acessos físicos, entre outros. Para se fazer uma auditoria de maneira satisfatória, é necessário conhecer o ambiente auditado, de maneira que as atividades específicas da corporação também sejam levadas em consideração no momento das avaliações (MANOTTI, 2010).

Lyra (2008) define como objetivos globais da auditoria os seguintes elementos:

- Integridade, onde pode-se confiar plenamente nas informações geradas;
- Confidencialidade, que pressupõe que as informações serão acessadas somente por quem realmente tem direito;
- Privacidade, que consiste no termo de segregação de tarefas, onde cada usuário faz somente aquilo que lhe é devido;
- Acuidade, onde é garantida a validação dos dados existentes no processo do negócio através de ferramentas específicas;
- Disponibilidade, que determina que o sistema e todas as informações devem estar disponíveis sempre que necessário para a execução das tarefas;
- Auditabilidade, que quer dizer que os sistemas devem emitir *logs* que permitam uma avaliação posterior das atividades realizadas no sistema, caso necessário;
- Versatilidade, que consiste no conceito do sistema ser ajustável ao processo da organização para que o usuário possa operá-lo de maneira correta e satisfatória.
- Manutenibilidade, que é, resumidamente, a possibilidade de um sistema ter metodologias claras de manutenção, de maneira que, quando for necessária uma alteração no sistema, não sejam afetadas as informações já nele contidas e o processo operacional seja afetado o mínimo possível.

Imoniana (2011) afirma que a auditoria em sistemas de informação é importante, pois as informações que antes eram armazenadas em papel hoje estão guardadas em material eletrônico e é essencial garantir que essas informações sejam confiáveis

para se poder usá-las em tomadas de decisões. Afirma também que a auditoria visa verificar os controles internos, assegurando inicialmente se os mesmos existem e, caso existam, se são realmente eficientes no cumprimento de seu papel.

Fantinatti (1988) diz que o processo de auditoria é considerado por muitos erroneamente como uma “caça às bruxas”. Durante o processo de auditoria, o objetivo é verificar que todos os procedimentos estão de acordo com o planejado em metas e planos definidos anteriormente e que os recursos estão sendo otimizados, utilizados da melhor maneira possível. É comum encontrar falhas e, nesses casos, são aplicadas ações de correção para que o sistema torne a funcionar completamente dentro do esperado.

Imoniana (2011), ao falar especificamente sobre auditoria de redes diz que os aspectos que podem ser levados em consideração durante o processo de auditoria de uma rede de computadores são: arquitetura e topologia da rede, implementação de projetos físicos e lógicos, monitoramento de desempenho e possível captação indevida de informações, análise e replanejamento de capacidade e levantamento de possíveis problemas operacionais. O principal objetivo em uma auditoria de redes é garantir a confiabilidade das informações geradas, trafegadas e armazenadas, visando a segurança física (equipamentos e periféricos), segurança lógica (customizações de software e desempenho da rede), segurança de enlace (meio pelo qual as informações trafegam) e, por fim, a segurança de aplicação, com foco na disponibilidade da rede, que verifica a disponibilidade da informação sempre que um usuário for usá-la para execução de suas tarefas.

Fantinatti (1988) descreve três etapas básicas no processo de auditoria. São elas: Pré-auditoria, Auditoria e Pós-auditoria.

Na Pré-auditoria é emitida uma notificação aos setores auditados, onde são definidos os processos a serem auditados e é escolhida a equipe responsável pela auditoria;

Na Auditoria, são executados os procedimentos de coleta e análise de dados, gerados relatórios parciais e há reuniões onde são passadas as informações colhidas para os responsáveis das áreas auditadas para que eles possam emitir respostas às possíveis falhas encontradas.

Já o processo de pós-auditoria é o processo final, quando é gerado o relatório definitivo, contendo todas as informações colhidas e as possíveis falhas encontradas na empresa.

Vale lembrar que há diversos mecanismos usados e avaliados no momento da auditoria. Stallings (2008) define um mecanismo de segurança como sendo um processo, ou dispositivo agindo como um processo que permite detectar, impedir, ou se recuperar de um ataque à segurança. Como exemplos de mecanismos de segurança, podem ser citados o *Firewall*, o IDS, a VPN, a criptografia, entre outros que serão abordados a seguir.

2.4 MECANISMOS AUXILIARES UTILIZADOS NA BUSCA DA SEGURANÇA DA INFORMAÇÃO

O *Firewall* é definido como uma junção de hardware e software que permita um isolamento da rede interna de uma corporação com a Internet, dando a possibilidade do administrador da rede ter um controle de tudo que é trafegado entre a rede interna e a Internet. O *firewall* deve ser configurado para que todo o tráfego que venha da rede mundial para a rede interna passe por ele, e vice-versa. Dessa maneira, é possível ser feito um controle total de tudo que entra e sai no ambiente virtual corporativo. O *firewall* pode e deve ser utilizado para impedir que pacotes não autorizados adentrem o ambiente da rede. Uma grande atenção deve ser dada ao *firewall*, no entanto, pois é vulnerável a invasões, ou seja, se um atacante conseguir alterar as regras de *firewall*, a rede ficará vulnerável a certos ataques enquanto o administrador não reparar a falha, portanto, é necessário que haja revisões constantes nas regras de *firewall* das redes (KUROSE, 2010).

O *Iptables* é um *firewall* implementado a partir da versão 2.4 do *Kernel Linux*, de acordo com Neto (2004). O *Iptables* trabalha com a lógica do *Netfilter*, apresentado ainda por Neto como um banco de dados que contém três tabelas por padrão: *Filter, NAT e Mangle*. Entre as grandes vantagens do *Iptables*, estão sua velocidade, segurança e estabilidade, além de uma certa versatilidade, tendo em vista que através do *Iptables,* é possível além do filtro de pacotes, fazer traduções de rede, através da tabela NAT (*Network Address Translation)*, monitoramento de tráfego, mascaramento de conexões, filtro de ataques de negação de serviço, entre outros.

Os IDS, *Intrusion Detection Systems* (Sistemas de Detecção de Intrusão), são, de acordo com Kurose (2010), ferramentas que fazem uma análise detalhada e minuciosa dos pacotes que estão adentrando a rede com o intuito de impedir que pacotes maliciosos se infiltrem no ambiente corporativo. Os IDS analisam pacotes em busca de vírus, *worms*, ataques de vulnerabilidades de Sistemas Operacionais, escaneamento de portas, ataques de negação de serviço, entre outros. Uma das principais características dos IDS é que eles não impedem que um pacote adentre a rede. A função deles é analisar o pacote e, caso seja detectada uma possível fonte de ataque, é emitido um alerta para o administrador e então devem ser tomadas as medidas cabíveis. Portanto, o IDS, em sua natureza não impede que pacotes sejam trafegados na rede.

A definição de Stallings (2008) para os Sistemas de Detecção de Intrusão baseia-se no fato de que o comportamento de um intruso geralmente difere do comportamento de um usuário comum. O autor divide as técnicas de detecção de intrusão em duas a saber: a detecção estatística de anomalia, onde uma análise prévia do perfil de tráfego dos usuários legítimos é feita e, de acordo com os dados obtidos, é feita uma comparação com os tráfegos futuros na tentativa de se encontrar uma anomalia no perfil de tráfego. A segunda técnica é baseada em regras, onde regras são pré-definidas e a análise busca encontrar tráfego que fuja dessas regras, para assim identificar a intrusão e, em seguida, agir contra a ação do intruso.

Ao explicar o conceito de VPN – *Virtual Private Network* (Rede Privada Virtual), Kurose (2010) exemplifica que uma empresa com diversas filiais espalhadas geograficamente pode querer ter sua própria infraestrutura de rede, com seu cabeamento, seus roteadores, seus servidores de nome, entre outros. Essa seria uma rede privada. No entanto, o custo para se manter uma estrutura desse tipo é extremamente alto e não seria viável na maioria dos casos, então, criou-se o conceito de rede privada virtual, que funciona basicamente da seguinte maneira: a organização cria uma rede utilizando a Internet pública que todos têm comum acesso, no entanto, antes dos dados serem lançados na rede, são criptografados pela própria aplicação e só serão descriptografados quando chegarem ao destino final. Dessa maneira, se algum dado for interceptado, a criptografia ajudará na garantia da confidencialidade dessas informações.

A Criptografia é, de acordo com Kurose (2010), uma técnica milenar que consiste em se tornar ilegível uma mensagem em trânsito caso seja interceptada

durante o trajeto até o destinatário. A criptografia é feita de maneira que haja um texto legível e, através da existência de uma chave criptográfica e um algoritmo de criptografia, a mensagem trafegue de maneira segura e possa ser lida pelo destinatário.

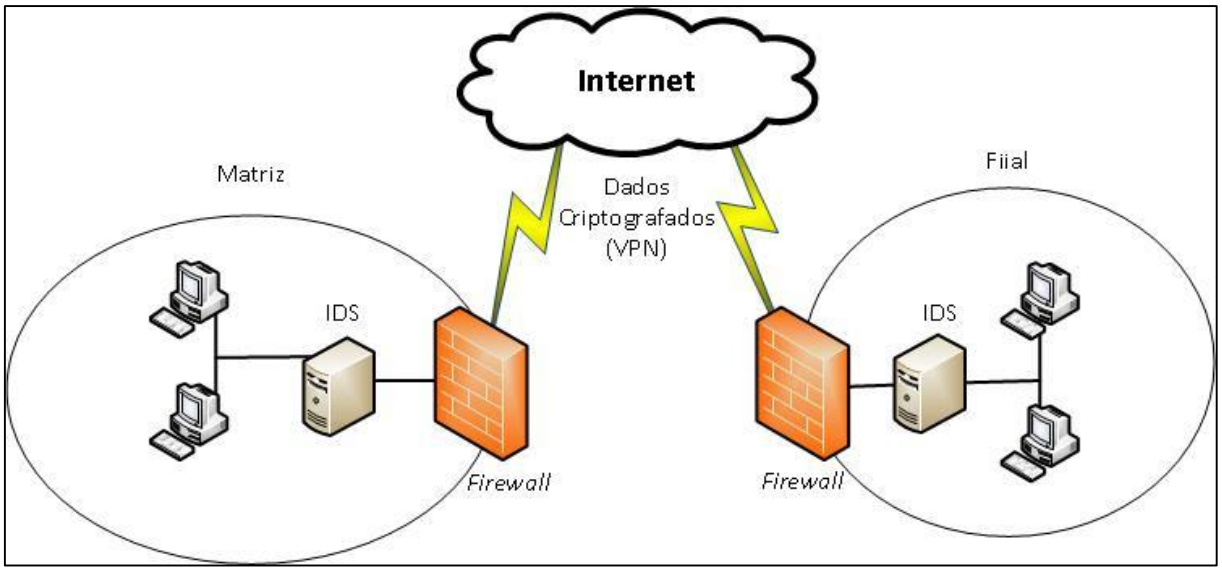
As técnicas de criptografia podem ser divididas em duas grandes categorias, que Stallings (2008) apresenta como criptografia de chave simétrica, ou criptografia de chave privada e criptografia de chaves assimétricas, ou criptografia de chave pública. Na criptografia de chave simétrica, a mesma chave utilizada no processo de criptografia é também utilizada para decifrar a mensagem. Esse método costuma ser mais utilizado para se criptografar grandes quantidades de dados, como um disco rígido inteiro, por exemplo. Já na criptografia de chave pública, ou assimétrica, é utilizado um par de chaves, conhecidas como pública e privada. A chave pública de um indivíduo é conhecida em meio comum, já a privada é conhecida por somente ele. No processo de chaves assimétricas, se a chave pública é utilizada para criptografar a mensagem, somente a chave privada correspondente será capaz de descriptografar, e vice-versa, se a mensagem é cifrada com a chave privada, somente a chave pública conseguirá descriptografar.

De acordo com Giavaroto e Santos (2013), o *Wireshark* é um analisador de protocolos, também conhecido como *sniffer*. O *Wireshark* atua capturando pacotes que são trafegados na rede, para uma análise posterior. Esse recurso pode ser utilizado maliciosamente para ter acesso a informações valiosas de uma organização, caso elas não estejam devidamente protegidas. Durante um processo de auditoria, pode-se utilizar o *Wireshark* para analisar como os dados estão trafegando no ambiente. Através desse tipo de análise, pode-se identificar também tráfegos excessivos na rede que comprometam o desempenho, além de se testar ainda os recursos de criptografia que estejam sendo utilizados.

Outra ferramenta que ajuda a verificar o status de alguns recursos utilizados em uma rede é o NMAP, *Network Mapper (*Mapeador de Redes), que é uma aplicação de código livre desenvolvida por Gordon Fyodor Lyon publicada no ano de 1997. Sua principal função é fazer a varredura de portas lógicas em computadores de uma rede para se identificar possíveis vulnerabilidades. No entanto, após anos de desenvolvimento, hoje é possível descobrir máquinas em uma rede, seus sistemas operacionais, as versões dos aplicativos rodando nelas, efetuar o inventário da rede, entre outros (LYON, 2009).

A Figura 1 ilustra graficamente como alguns desses recursos funcionam em uma estrutura física de uma organização.

Figura 1 - Ilustração gráficas dos mecanismos de segurança em uma estrutura de uma rede.



Fonte: Autoria própria.

3 CONCEITUAÇÃO DO NMAP

Neste capítulo, será apresentada a ferramenta NMAP, mostrando um breve histórico e alguns comandos básicos utilizados.

3.1 APRESENTAÇÃO DO NMAP

O NMAP é uma ferramenta de varredura de portas muito popular entre os especialistas de segurança. O fato da aplicação estar disponível em todos os sistemas *UNIX*, inclusive *MAC OS* e também no *Windows* em forma gráfica e de texto auxiliam sua popularidade (JACKSON, 2010).

Em sua primeira aparição, no ano de 1997, feita em uma publicação na revista *Phrack*, seu autor Gordon Lyon, apresentou uma ferramenta desenvolvida com cerca de duas mil linhas de código divididas em três arquivos. As linhas de código foram escritas exclusivamente para sistemas *Linux*, com o objetivo de se ter uma aplicação que varresse as portas de maneira eficiente mesclando diversas técnicas. De acordo com Gordon, o NMAP foi desenvolvido por propósitos pessoais e divulgado para a comunidade na intenção de encontrar alguém que pudesse achar a ferramenta útil (LYON, 2009).

Após ter seu código divulgado, o NMAP passou a ser desenvolvido e melhorado pela comunidade de código aberto, ganhando novas funcionalidades e cada vez mais popularidade. O NMAP foi considerado o *scanner* de segurança de redes mais popular do mundo, além de receber prêmios como “ferramenta de segurança do ano” em publicações como *Linux Journal, Info World e Codetalker Digest* (LYON, 2009). Apresenta-se, a seguir, uma cronologia com as principais mudanças ocorridas com o NMAP, desde a sua primeira publicação.

Como já citado, o NMAP foi lançado em 1 de setembro de 1997 em uma publicação da revista *Phrack*, sem número de versão e sem perspectiva de desenvolvimento por parte do seu desenvolvedor. Sua demanda popular foi instantânea de maneira que, quatro dias depois, foi lançada a versão denominada 1.25 após passar por ligeiras alterações. Em 12 de dezembro de 1998, foi publicada a versão 2.00, que incluía, entre outras mudanças, a detecção de SO. Em 11 de abril de 1999, foi lançada a versão 2.1 *beta*, já com o aparecimento da interface gráfica. A versão 2.54 *beta*, lançada em 7 de dezembro de 2000, veio com suporte de execução

em máquinas que utilizavam o SO *Windows*. Em 31 de julho de 2002, foi publicada a versão 3.00, desta vez compatível com o SO *Mac OS X*. Em 28 de agosto de 2002, o NMAP foi convertido da linguagem C para a C ++, passando a suportar redes *IPv6,* em sua versão 3.10 *Alpha*. Em 16 de setembro de 2003, na versão 3.45 é agregada às funcionalidades a detecção de serviços e versões (LYON, 2009).

O NMAP trabalha com pacotes crus de IP modificados de maneira que a resposta do *host* à requisição permite que o analista obtenha informações como o sistema operacional da máquina, serviços e versões disponíveis, entre outros (LYON, 2009).

Desta maneira, recomenda-se fortemente a utilização do NMAP por administradores de segurança de redes em auditorias buscando possíveis vulnerabilidades para corrigi-las antes que algum atacante as explore. Se essa análise for executada da maneira correta pelo profissional responsável e as vulnerabilidades forem devidamente corrigidas, grandes portas se fecharão a possíveis atacantes que queiram invadir tal rede, independente do propósito.

3.2 UTILIZANDO O NMAP

Como já foi apresentado, o NMAP está disponível para instalação nos principais sistemas operacionais do mercado (*Windows, Linux* e *MAC OS*). Em algumas distribuições *Linux*, o NMAP já vem instalado, como no *Back Track* (GIAVAROTO E SANTOS, 2013). Para verificar se a distribuição em uso possui o NMAP instalado, basta digitar o comando **nmap –version**. A saída em tela deverá ser como a apresentada na Figura 2.

Figura 2- Verificação de versão do NMAP em máquina com o SO *Back Track.*

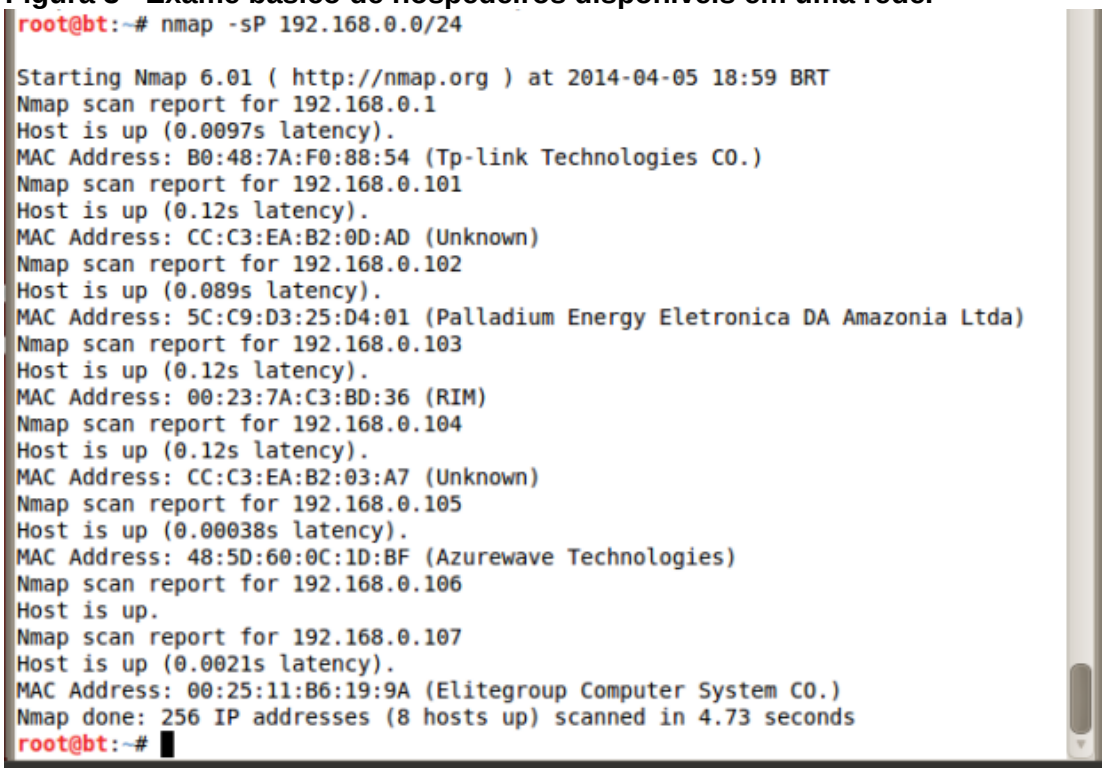
```
root@bt:~# nmap -version

Nmap version 6.01 ( http://nmap.org )
Platform: i686-pc-linux-gnu
Compiled with: nmap-liblua-5.1.3 openssl-0.9.8k libpcre-7.8 libpcap-1.0.0 nmap-l
ibdnet-1.12 ipv6
Compiled without:
root@bt:~#
```

Fonte: Autoria própria.

Caso o NMAP não esteja instalado, poderá ser baixado diretamente do site oficial (*http://nmap.org/download.html)*. Através deste endereço, é possível baixar versões executáveis e compiláveis do NMAP para os sistemas operacionais disponíveis já citados. Após ser instalado ou confirmado a sua existência na máquina, é hora de começar a examinar a rede. De acordo com Lyon (2009), examinar cada porta de cada hospedeiro disponível na rede é trabalhoso em demasia e chega a ser desnecessário. Pensando nisso, o NMAP possui um conjunto expressivo de comandos e parâmetros para que o analista possa obter os dados mais adequados de acordo com suas necessidades.

Se o teste feito pelo analista simular um ataque, supondo que o atacante não conheça a rede e queira, através de um exame simples descobrir *hosts* na rede, ou ainda, em qualquer situação em que o profissional deseja listar os hospedeiros disponíveis no momento na rede, o exame pode ser iniciado com o comando **nmap –sP 192.168.0.0/24**, apresentado na Figura 3, que faz um *scan* executando *pings* na rede levando em consideração que o endereço da rede seja 192.168.0.0 e que a máscara de sub rede seja 255.255.255.0. Esse comando pode ser válido para um analista de rede verificar quantos *hosts* estão disponíveis na rede em determinado momento, no entanto, é comum que determinadas máquinas em uma rede tenham bloqueios a requisições *ping* em suas regras de *firewall* para evitar ações de atacantes.

Figura 3 - Exame básico de hospedeiros disponíveis em uma rede.



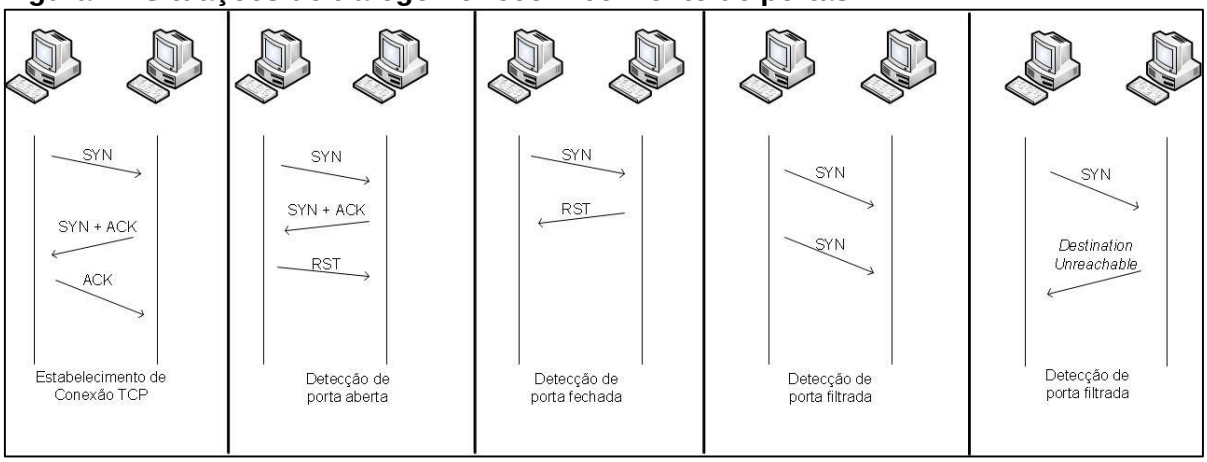
Fonte: Autoria própria.

Na Figura 3, pode-se verificar um exame simples, apontando somente os hospedeiros disponíveis na rede, especificando o IP disponível e seu *MAC Address.* Nesse momento, o NMAP já especifica o fabricante do dispositivo de hardware do *host*.

O NMAP classifica as portas do hospedeiro em três estados: *open, closed* e *filtered (*aberta, fechada e filtrada, respectivamente). A porta classificada como aberta recebe conexões normalmente; a porta filtrada está recebendo conexões que passam antes pelas regras de um *firewall* e a porta fechada não possui nenhum serviço disponível escutando nela.

Para examinar as portas, o NMAP possui diversas técnicas, mas será descrito o procedimento padrão, utilizado pelo NMAP quando não são utilizados parâmetros adicionais de *scan*. A Figura 4 ilustra graficamente o processo do *three way handshake,* utilizado pelo NMAP em seu reconhecimento de portas, além das situações que o leva a identificar tais portas em seus devidos estados. A explicação dos ambientes representados e simulação prática de cada um deles é apresentada em seguida.

Figura 4 - Situações de tráfego no reconhecimento de portas.



Fonte: Autoria própria.

O NMAP envia um pacote TCP com a *flag* SYN de sincronização à porta examinada tentando estabelecer conexão com ela. Essa ação faz parte do processo *three way handshake* (traduzido literalmente como aperto de mãos de três vias) do protocolo TCP. Quando a porta está recebendo conexões, segue o procedimento padrão do TCP e envia como resposta um pacote com as *flags* ACK (confirmação de pacote recebido) + SYN (sincronização). Para completar o processo, o NMAP deveria responder com um pacote ACK de confirmação e a conexão se estabeleceria. No entanto, a resposta da máquina alvo já foi suficiente para que o NMAP reconheça o estado da porta, então é enviado um pacote RST, finalizando o processo e a conexão não chega a ser estabelecida. Quando o processo de conexão se concretiza dessa maneira, o NMAP classifica a porta como *open* (aberta). Essa comunicação pode ser visualizada na Figura 5, que mostra a análise de tráfego feita com o software *Wireshark.*

Figura 5 – Análise de tráfego feita com o *Wireshark* em varredura de porta aberta.

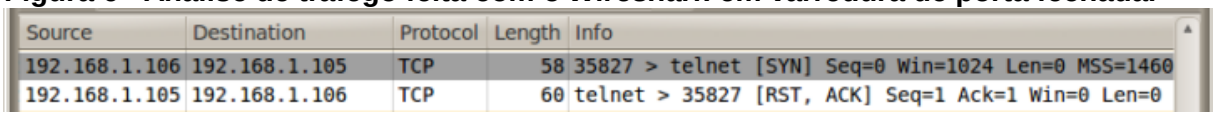
Source	Destination	Protocol	Length	Info
192.168.1.106	192.168.1.105	TCP	58	40845 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.105	192.168.1.106	TCP	60	ssh > 40845 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0
192.168.1.106	192.168.1.105	TCP	54	40845 > ssh [RST] Seq=1 Win=0 Len=0

Fonte: Autoria própria.

A porta é classificada como *closed* (fechada) quando o NMAP envia o pacote TCP SYN à porta e obtém como resposta um pacote com a *flags* ACK, confirmando o

recebimento da requisição e a RST fechando a conexão, significando que não há qualquer serviço rodando nessa porta. Esse tráfego é apresentado na Figura 6.

Figura 6 - Análise de tráfego feita com o *Wireshark* em varredura de porta fechada.

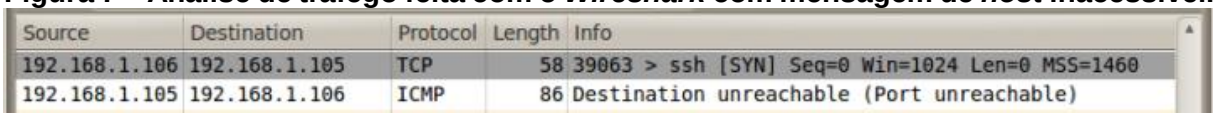


Source	Destination	Protocol	Length	Info
192.168.1.106	192.168.1.105	TCP	58	35827 > telnet [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.105	192.168.1.106	TCP	60	telnet > 35827 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Fonte: Autoria própria.

A terceira classificação de portas que o NMAP adota é a de *filtered* (filtrada). O NMAP chega a essa conclusão quando tenta a conexão com a porta e não obtém qualquer resposta ou ainda recebe como respostas alguns erros de ICMP, informando, por exemplo, que o *host* está inacessível. O fato do NMAP não receber respostas ou receber respostas de erro depende diretamente da maneira que o *firewall* está configurado. As duas situações são demonstradas nas Figuras 7 e 8.

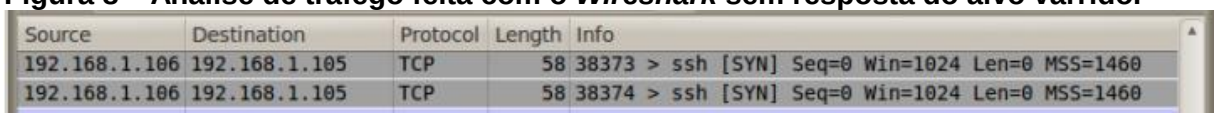
Figura 7 – Análise de tráfego feita com o *Wireshark* com mensagem de *host* inacessível.



Source	Destination	Protocol	Length	Info
192.168.1.106	192.168.1.105	TCP	58	39063 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.105	192.168.1.106	ICMP	86	Destination unreachable (Port unreachable)

Fonte: Autoria própria.

Figura 8 – Análise de tráfego feita com o *Wireshark* sem resposta do alvo varrido.

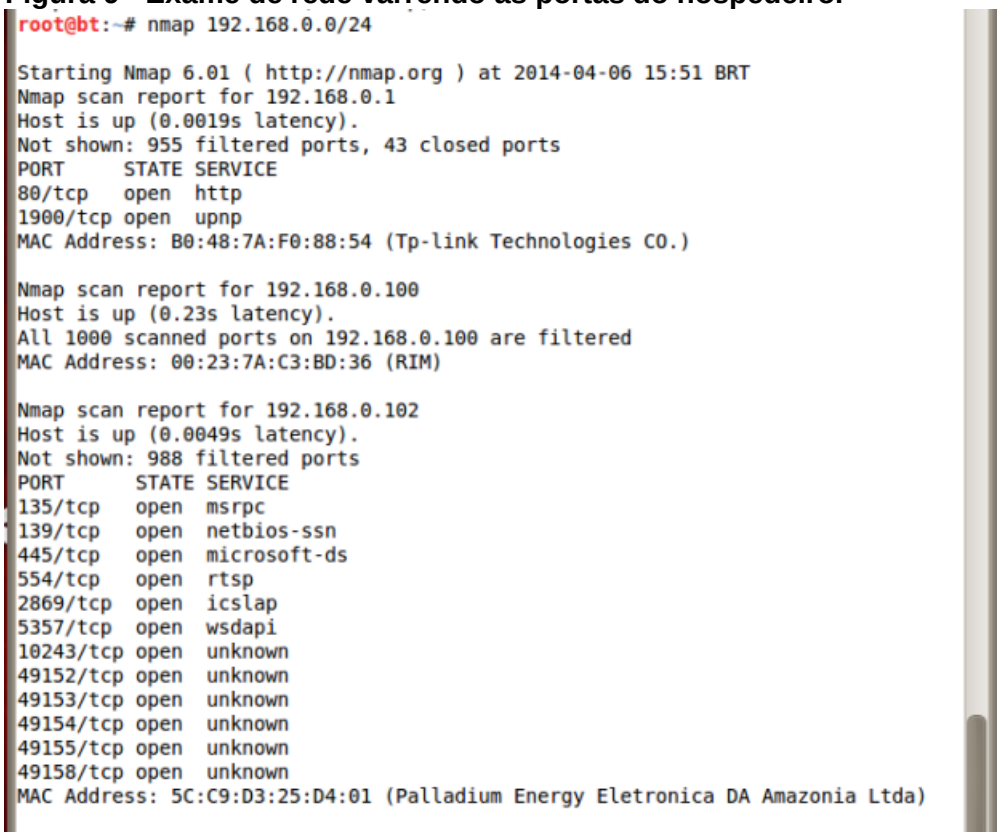


Source	Destination	Protocol	Length	Info
192.168.1.106	192.168.1.105	TCP	58	38373 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460
192.168.1.106	192.168.1.105	TCP	58	38374 > ssh [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Fonte: Autoria própria.

Se for executado o comando **nmap 192.168.0.0/24**, sem opções adicionais, a ferramenta já varre as portas dos hospedeiros disponíveis na rede, conforme a Figura 9, que mostra parte da saída do comando.

Figura 9 - Exame de rede varrendo as portas do hospedeiro.



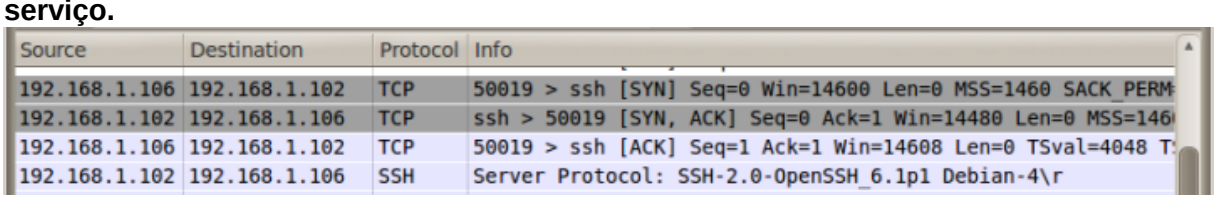
```
root@bt:~# nmap 192.168.0.0/24

Starting Nmap 6.01 ( http://nmap.org ) at 2014-04-06 15:51 BRT
Nmap scan report for 192.168.0.1
Host is up (0.0019s latency).
Not shown: 955 filtered ports, 43 closed ports
PORT     STATE SERVICE
80/tcp   open  http
1900/tcp open  upnp
MAC Address: B0:48:7A:F0:88:54 (Tp-link Technologies CO.)

Nmap scan report for 192.168.0.100
Host is up (0.23s latency).
All 1000 scanned ports on 192.168.0.100 are filtered
MAC Address: 00:23:7A:C3:BD:36 (RIM)

Nmap scan report for 192.168.0.102
Host is up (0.0049s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49158/tcp open  unknown
MAC Address: 5C:C9:D3:25:D4:01 (Palladium Energy Eletronica DA Amazonia Ltda)
```

Fonte: Autoria Própria.

No ambiente apresentado na Figura 9, o *host* 192.168.0.102 chama a atenção devido o número de portas abertas. Nesse momento, pode-se executar o comando **nmap –sV 192.168.0.102**. O parâmetro **-sV** busca os serviços e as versões disponíveis nas portas, a fim de descobrir alguma função relevante da máquina dentro da estrutura de rede na qual se encontra.

Quando é solicitada a detecção de versões ao NMAP, no processo de estabelecimento de conexão com a porta, na última etapa do *three way handshake* o NMAP estabelece a conexão enviando um pacote com a *flag* ACK, ao invés de finalizar a conexão, e aguarda uma mensagem de boas-vindas que os serviços mais comuns enviam ao se estabelecer uma conexão. Esse pacote recebido pelo NMAP é comparado com uma base de dados no arquivo **nmap-service-probes** e o NMAP reconhece o serviço que está disponível nessa porta. Essa comunicação pode ser visualizada na Figura 10.

Figura 10 – Estabelecimento de conexão completa do NMAP buscando identificar o serviço.



Source	Destination	Protocol	Info
192.168.1.106	192.168.1.102	TCP	50019 > ssh [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SACK_PERM
192.168.1.102	192.168.1.106	TCP	ssh > 50019 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=146
192.168.1.106	192.168.1.102	TCP	50019 > ssh [ACK] Seq=1 Ack=1 Win=14608 Len=0 TSval=4048 T
192.168.1.102	192.168.1.106	SSH	Server Protocol: SSH-2.0-OpenSSH_6.1p1 Debian-4\r

Fonte: Autoria própria.

Figura 11 - Exame de detecção de versões em um determinado *host.*

```
root@bt:~# nmap -sV 192.168.0.102

Starting Nmap 6.01 ( http://nmap.org ) at 2014-04-06 15:58 BRT
Nmap scan report for 192.168.0.102
Host is up (0.016s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE     VERSION
135/tcp   open  msrpc       Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
10243/tcp open  http        Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc       Microsoft Windows RPC
49153/tcp open  msrpc       Microsoft Windows RPC
49154/tcp open  msrpc       Microsoft Windows RPC
49155/tcp open  msrpc       Microsoft Windows RPC
49158/tcp open  msrpc       Microsoft Windows RPC
MAC Address: 5C:C9:D3:25:D4:01 (Palladium Energy Eletronica DA Amazonia Ltda)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.
org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 103.85 seconds
root@bt:~#
```

Fonte: Autoria Própria.

O resultado mostrado na Figura 11 apresenta a saída de um exame de versão em um *host.* Através desse comando, o NMAP obtém informações sobre as versões dos serviços disponíveis nas portas, e já reconhece o sistema operacional do hospedeiro. No caso, é o *Windows*, mas neste exemplo não foi reconhecida a versão do *Windows* presente.

Ao acrescentar o parâmetro **–A** ao comando executado anteriormente, o programa traz um grande número de informações privilegiadas, conforme Figura 12.

Figura 12 - Varredura em um host com o parâmetro –A.

```
root@bt:~# nmap -sV -A 192.168.0.102

Starting Nmap 6.01 ( http://nmap.org ) at 2014-04-13 14:52 BRT
Nmap scan report for 192.168.0.102
Host is up (0.0045s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn
445/tcp   open  netbios-ssn
554/tcp   open  rtsp?
2869/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
5357/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Service Unavailable
|_http-methods: No Allow or Public header in OPTIONS response (status code 503)
10243/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-methods: No Allow or Public header in OPTIONS response (status code 404)
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 5C:C9:D3:25:D4:01 (Palladium Energy Eletronica DA Amazonia Ltda)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 7|Vista|2008
OS CPE: cpe:/o:microsoft:windows_7::professional cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::sp1 cpe:/
o:microsoft:windows_server_2008::sp1
OS details: Microsoft Windows 7 Professional, Microsoft Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Mic
rosoft Windows Vista SP2 or Windows Server 2008
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smbv2-enabled: Server supports SMBv2 protocol
|_nbstat: NetBIOS name: MICHELLE, NetBIOS user: <unknown>, NetBIOS MAC: 5c:c9:d3:25:d4:01 (Palladium Energy Eletronica DA Am
azonia Ltda)
| smb-security-mode:
|   Account that was used for smb scripts: <blank>
|   User-level authentication
|   SMB Security: Challenge/response passwords supported
|_  Message signing disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 8 Single Language 9200 (Windows 8 Single Language 6.2)
|   NetBIOS computer name: MICHELLE
|   Workgroup: WORKGROUP
|_  System time: 2014-04-13 14:53:47 UTC-3
```

Fonte: Autoria Própria.

Se os resultados presentes na Figura 11 forem comparados aos resultados obtidos na Figura 12, pode-se verificar que o acréscimo do parâmetro **–A** traz informações não existentes na Figura 11 e completa outras como a versão do Sistema Operacional.

Com relação à versão do SO, primeiramente, o NMAP apresentou somente que o sistema instalado é o *Windows*. Após isso, com o parâmetro –A, baseado na resposta do *host* às requisições do NMAP, a ferramenta apresenta uma lista de possíveis versões (7, *Vista e Server* 2008). No entanto, em seguida, o NMAP já apresenta maiores detalhes especificando detalhadamente a versão do SO, que nesse caso é o *Windows* 8. A lista gerada inicialmente apontando três principais sistemas deve-se ao fato da similaridade na arquitetura desses sistemas, no entanto, o NMAP é capaz de diferenciar com exatidão a versão do sistema. O NMAP diferencia com exatidão a versão do sistema operacional, de acordo com Lyon (2009), enviando

pacotes TCP de prova ao *host* analisando a maneira que a máquina formula os pacotes de resposta. Com base nisso, o NMAP consulta sua base de dados e compara os pacotes recebidos com os já registrados em sua base. Esses padrões de formulação dos pacotes são também chamados de OS *fingerprint (*Impressão digital do sistema operacional).

Além da versão do SO que é uma grande informação para um possível atacante, o NMAP ainda traz informações altamente valiosas sobre a máquina analisada, como o *hostname*, que pode dar pistas sobre a função da máquina na arquitetura da rede (um servidor chamado *srvad* poderia indicar que essa máquina seja o servidor de autenticação rodando o serviço *Active Directory,* por exemplo). Como a máquina em questão não está alocada em nenhum domínio, é apresentado o seu grupo de trabalho. Além disso, o resultado ainda traz algumas informações sobre o método de autenticação no *host*, o que também pode ser altamente útil para um invasor, caso haja a intenção de tentar descobrir a senha através do método de força bruta. Apesar de não ser muito eficaz, no entanto, para um analista de rede, pode servir para auditar o nível de complexidade das senhas adotadas pelos usuários (uma senha de poucos caracteres ou com pouca variedade, que traga somente números, por exemplo, seria rapidamente quebrada). Outra informação que pode passar desapercebida, mas que pode ser útil na visão de um atacante, é o fuso horário presente na máquina varrida, pois em uma análise de uma rede que contém *hosts* espalhados pelo mundo, essa informação poderia apontar em qual região geográfica essa máquina esteja instalada.

Figura 13 - Varredura sem resultados solicitando o parâmetro –Pn.

```
victor@DellSlackware:~$ nmap -sV -A -T4 192.168.0.102

Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-13 13:54 BRT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 2.20 seconds
```

Fonte: Autoria própria.

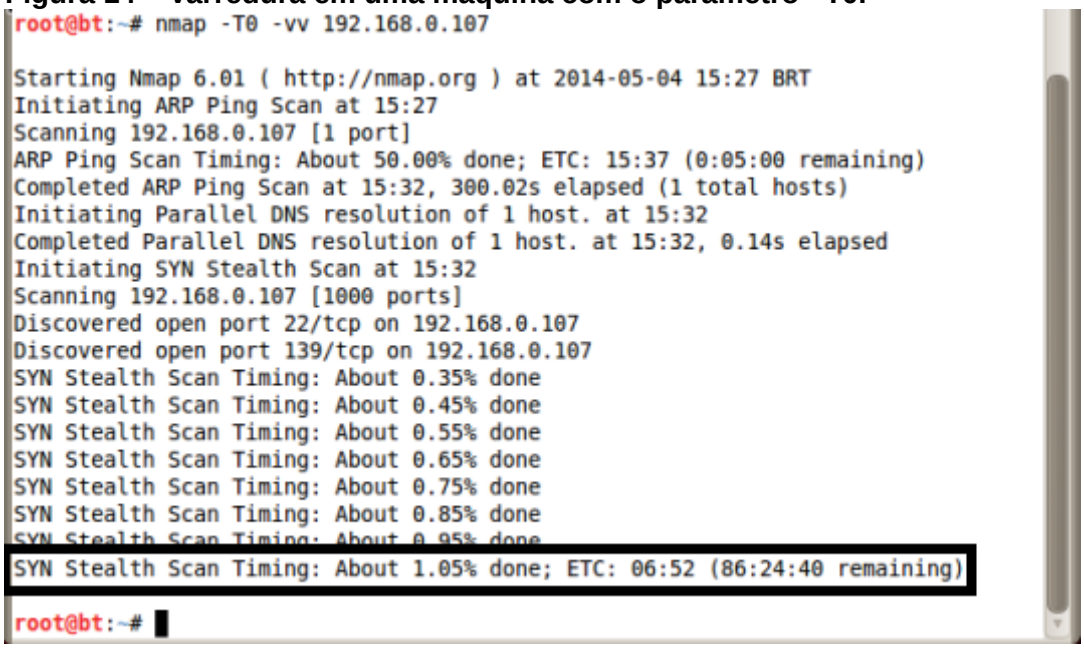
Outra situação que pode ocorrer é o *firewall* da máquina negar requisições *ping* (Figura 13). Nesse caso, o NMAP, ao não obter a resposta à requisição, entende que a máquina esteja *off-line* e não prossegue com a varredura das portas. Nesse caso, pode ser acrescentado o parâmetro **–Pn**, que força a varredura das portas mesmo sem verificar a disponibilidade do *host*. O resultado de uma varredura com a opção –

Pn não traz informações adicionais, apenas faz a varredura baseada nos demais parâmetros utilizados pulando a fase de verificação de disponibilidade do *host.* Se o parâmetro **–Pn** fosse adicionado à linha de comando utilizada na Figura 12, o resultado do NMAP seria exatamente o mesmo.

O parâmetro **–T4** visto na Figura 13 refere-se a um recurso do NMAP de temporização do exame baseado na fragmentação dos pacotes utilizados. Quando um valor é especificado, o NMAP adota uma maneira mais ou menos agressiva. A escala varia de 0 (zero) a 5 (cinco), sendo 0 a mais lenta e menos agressiva e 5 a mais rápida e mais agressiva. O uso desse parâmetro serve para tentar despistar sistemas IDS, tendo em vista que pacotes trafegados em um intervalo maior de tempo se misturam aos pacotes normais da rede e podem passar despercebidos por um IDS.

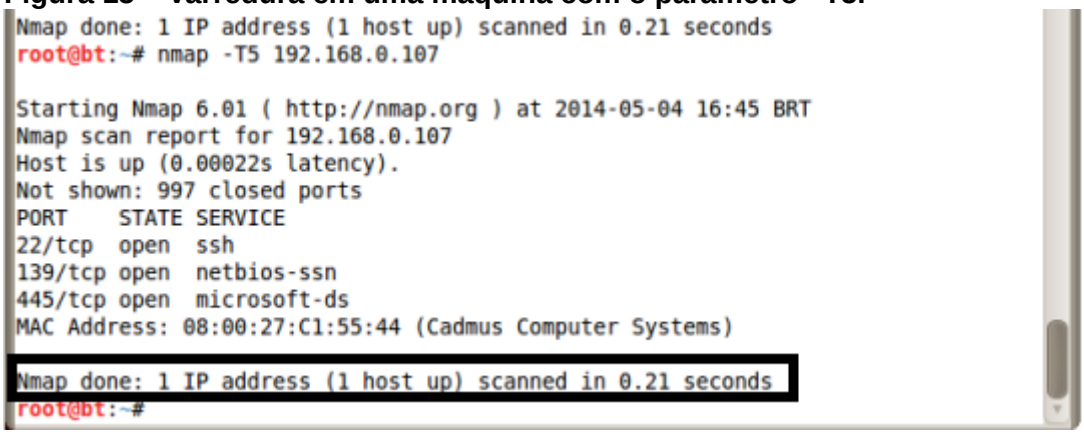
A diferença de desempenho entre as opções **–T0** e **–T5** são apresentadas nas Figuras 14 e 15.

Figura 14 – Varredura em uma máquina com o parâmetro –T0.



Fonte: Autoria própria.

Figura 15 – Varredura em uma máquina com o parâmetro –T5.



Fonte: Autoria própria.

A diferença entre o tempo do exame com o parâmetro **–T0** e **–T5** é clara. Enquanto o exame mais rápido durou 0.21 segundos (como mostra o destaque), o mais lento ficou cerca de uma hora sendo executado e ainda seriam necessárias mais de 86 horas restantes para o término do exame (também visto em destaque). O parâmetro **–vv** visto na Figura 14 mostra com mais detalhes as operações realizadas pelo NMAP, desta maneira foi possível ver o andamento do exame, com porcentagem e tempo restante necessário.

No próximo capítulo apresenta-se um experimento mostrando a utilização do NMAP em auditorias, com a simulação de alguns recursos comumente disponibilizados em redes, bem como os resultados obtidos e a análise desses resultados.

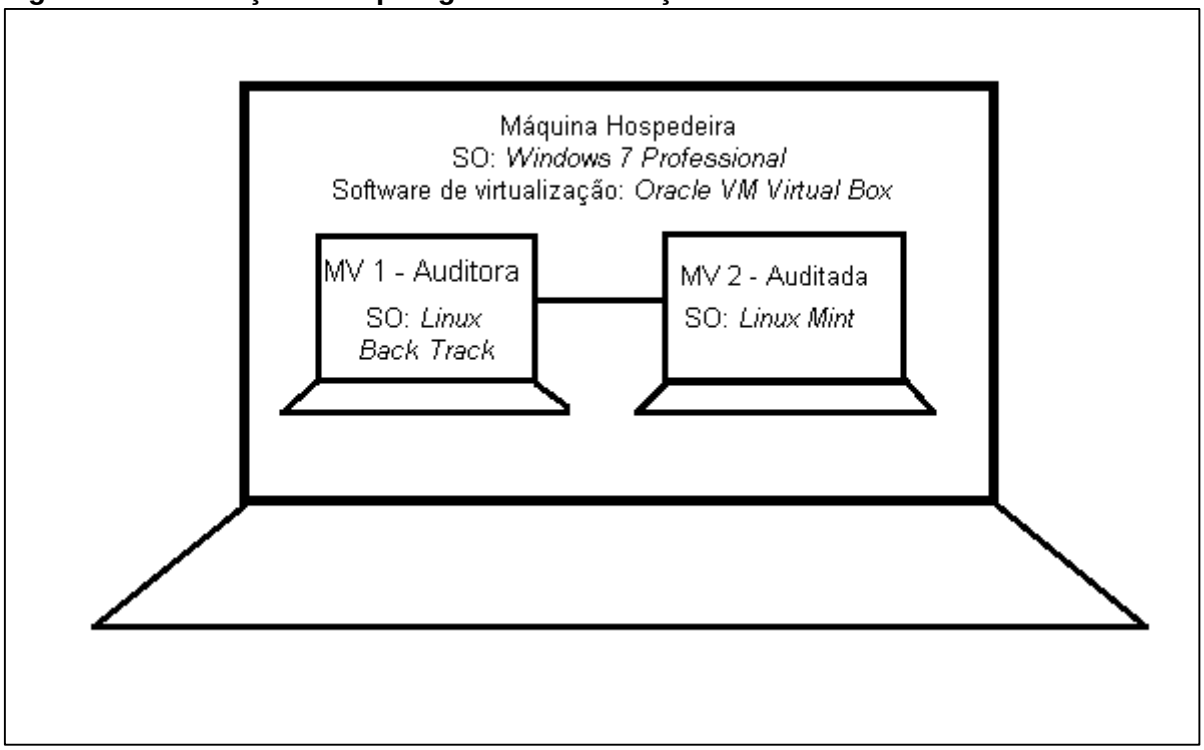
4 TESTES EXPLORANDO O NMAP

Neste capítulo, apresenta-se o experimento realizado, mostrando o ambiente de simulação, as especificações técnicas das máquinas simuladas e os serviços de rede a serem auditados.

4.1 DESCRIÇÃO DO EXPERIMENTO

O experimento a ser apresentado foi realizado em ambiente virtualizado controlado com duas máquinas virtuais e uma máquina hospedeira, ilustrado na Figura 16.

Figura 16 - Ilustração da topologia da virtualização.



Fonte: Autoria própria.

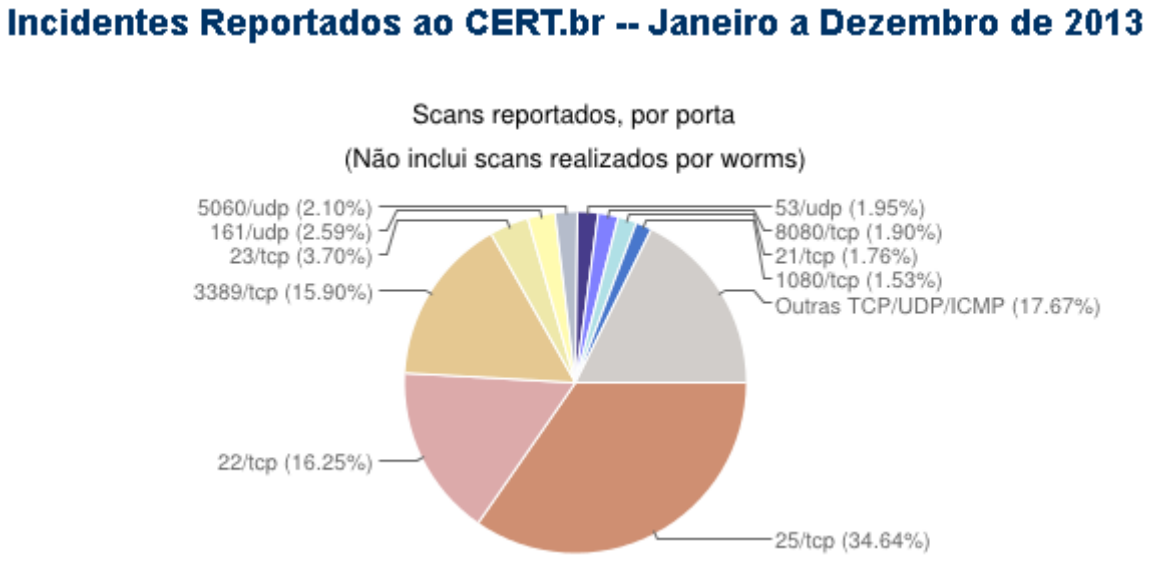
Seguem as informações de *hardware* e de *software* pertinentes ao experimento: a máquina hospedeira possui como SO principal o *Microsoft Windows 7 Professional 64 bits Service Pack 1*. O *software* de virtualização utilizado é o *Oracle VM VirtualBox* versão 4.3.10. A máquina hospedeira possui 4 GB de memória RAM DDR 3, um disco rígido de 500GB e um processador *Quad-Core* de 2.53 GHz.

Serão simuladas duas máquinas, sendo uma a que fará o papel de auditora e a outra que fará o papel de auditada. A máquina virtual auditora possui como sistema operacional o *Linux Backtrack* versão 5R3, com um disco rígido de 20GB e 756 MB de memória RAM. A máquina virtual auditada possui como sistema operacional o *Linux Mint* versão 15, com um disco rígido de 20 GB e 756 MB de memória RAM. O experimento será realizado apenas avaliando a segurança do serviço de SSH.

Durante a execução do experimento, será disponibilizado na máquina auditada o serviço de SSH - *Secure Shell (Shell* Seguro) com algumas falhas de segurança e, em seguida será feita a varredura com o NMAP apontando as falhas existentes. A partir dos resultados, serão apontadas possíveis soluções para as falhas e o teste com o NMAP voltará a ser executado para verificar a eficiência das medidas adotadas. O serviço de SSH foi o escolhido como objeto de teste, pois de acordo com o relatório de incidentes reportados ao CERT.BR (2014), durante todo o ano de 2013, a porta 22, que é a porta padrão para o serviço de SSH foi a segunda porta mais “scaneada”. O SSH é um serviço de *logon* remoto presente em terminais *Linux*. Por esse motivo, é importante que se tenha cuidados especiais com esse recurso, pois se alguém não autorizado obtiver acesso a terminais da rede, o dano causado pode ser irreparável.

A porta mais varrida de acordo com essa estatística foi a porta 25, padrão do serviço SMTP – *Simple Mail Transfer Protocol (*Protocolo Simples de Transferência de *E-mail).* Essa estatística é apresentada na Figura 17.

Figura 17 – Estatísticas de portas varridas em 2013.

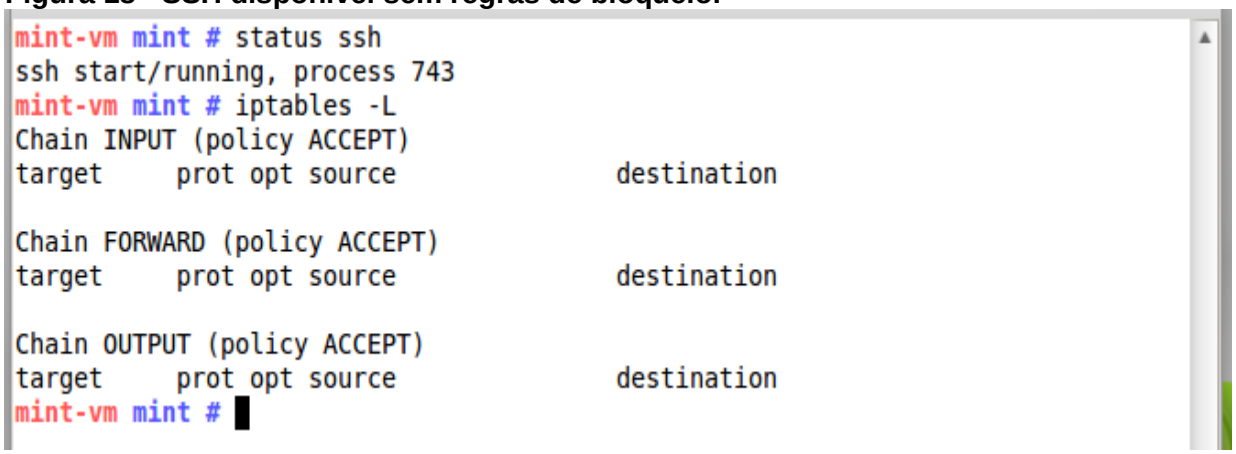


Fonte: CERT.BR (2014).

4.2 VERIFICANDO UMA MÁQUINA COM O SSH HABILITADO

Para iniciar o experimento, ficou disponível o serviço de SSH na máquina auditada sem qualquer regra de bloqueio, conforme pode ser visto na Figura 18. O comando **iptables –L** lista as regras configuradas no *iptables.*

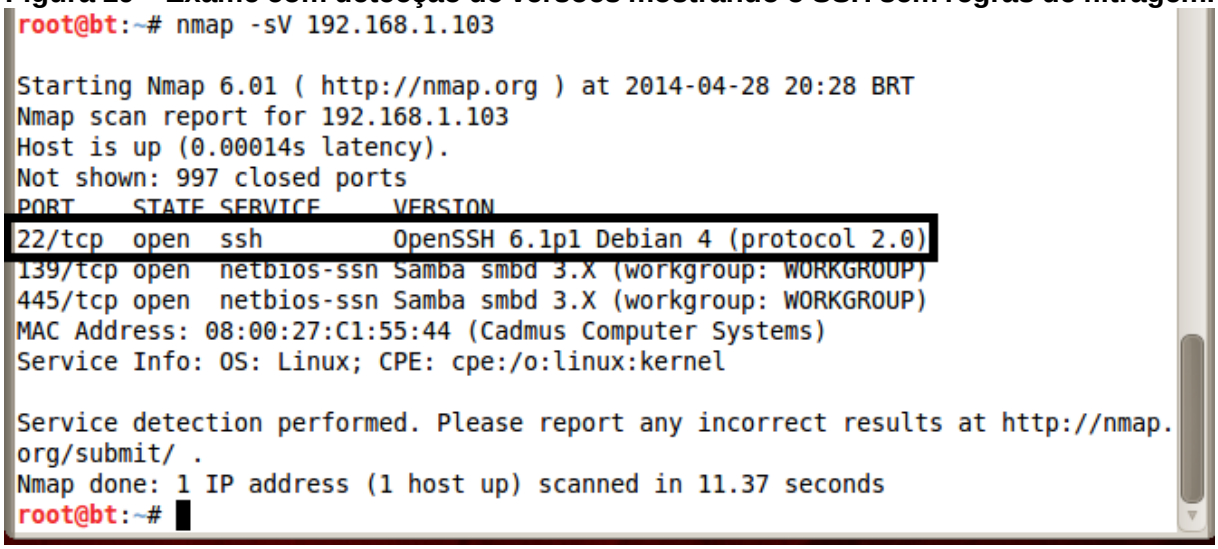
Figura 18 - SSH disponível sem regras de bloqueio.



Fonte: Autoria própria.

Como pode ser visto na Figura 19, o NMAP reconhece facilmente o serviço de SSH disponível no *host.*

Figura 19 – Exame com detecção de versões mostrando o SSH sem regras de filtragem.

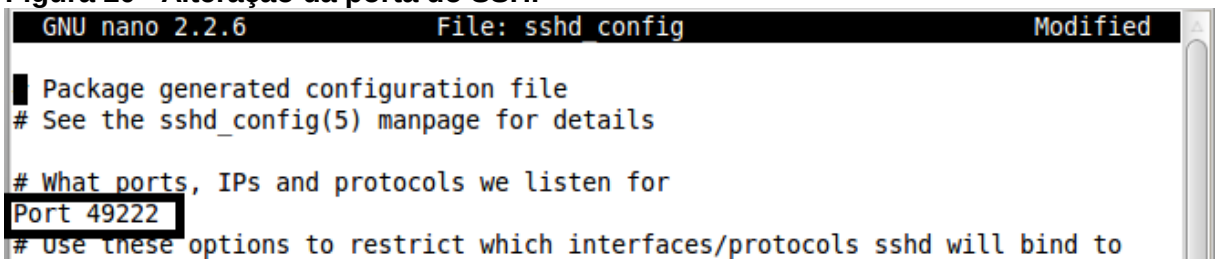


Fonte: Autoria própria.

Como visto na Figura 19, através de um comando com o parâmetro de detecção de versões **–sV**, o NMAP reconheceu o SSH disponível na máquina na porta 22, que é a porta padrão desse serviço. A principal vulnerabilidade é que a porta está no estado *open*, ou seja, aberto. Isso significa que não há qualquer regra de *firewall* filtrando conexões que cheguem a essa porta. Dessa maneira, um atacante poderia realizar ataques de força bruta sem grandes dificuldades para tentar obter acesso indevido ao terminal.

Uma medida simples seria mudar a porta do SSH no arquivo **sshd_config** no diretório de configuração no SSH, inserindo na linha *Port* o número da porta desejada. Nesse experimento, foi utilizada a porta 49222. Essa alteração é apresentada na Figura 20.

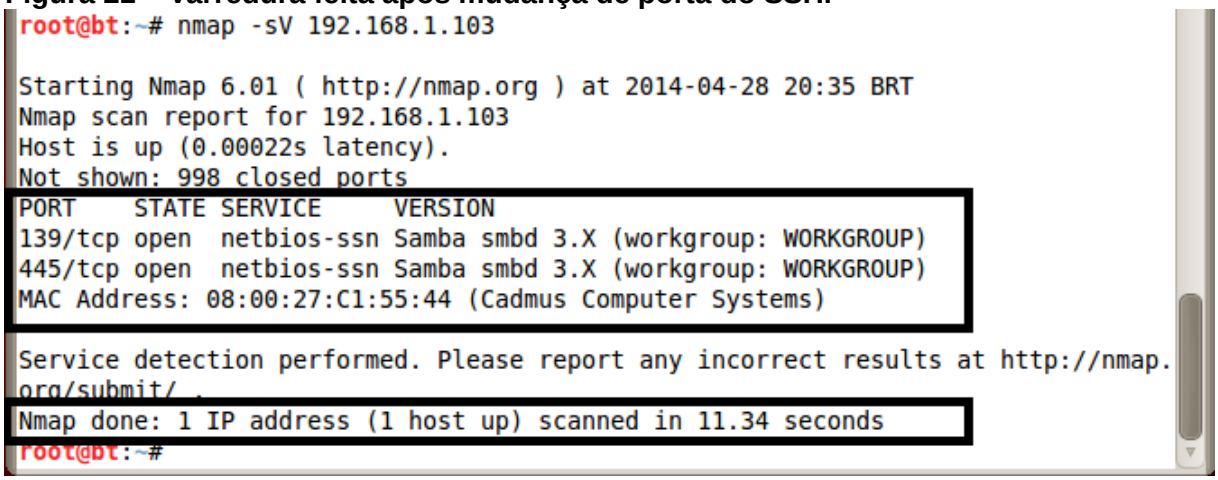
Figura 20 - Alteração da porta do SSH.



Fonte: Autoria própria.

Dessa maneira, ao executar o mesmo comando com o NMAP, o resultado é apresentado na Figura 21.

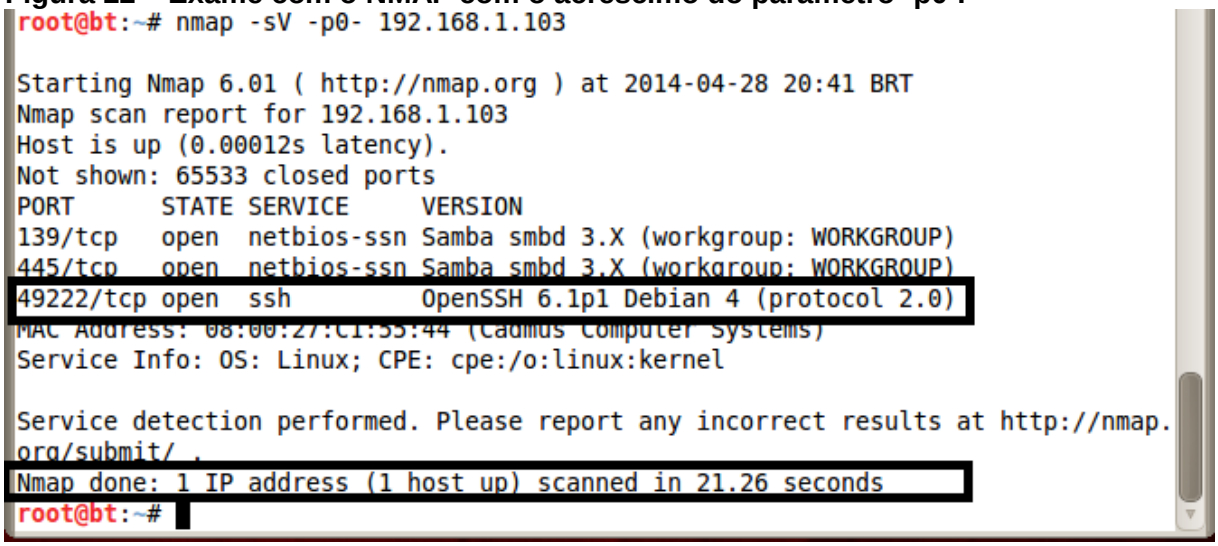
Figura 21 – Varredura feita após mudança de porta do SSH.



Fonte: Autoria própria.

Como visto na Figura 21, após mudança da porta de tráfego do SSH, o NMAP não reconhece mais a disponibilidade do serviço. Isso acontece porque, de acordo com Lyon (2009), o NMAP varre, por padrão, as 1000 portas mais comuns de acordo com configuração do arquivo **nmap-services**, presente no diretório de configuração da aplicação. Se um atacante utilizar esse comando, não verá o SSH disponível na máquina e provavelmente desistirá de uma tentativa de acesso indevido à ela. No entanto, com o acréscimo do parâmetro **-p0-**, o NMAP varre todas as 65536 portas do alvo. O resultado desse exame é apresentado Figura 22.

Figura 22 – Exame com o NMAP com o acréscimo do parâmetro -p0-.



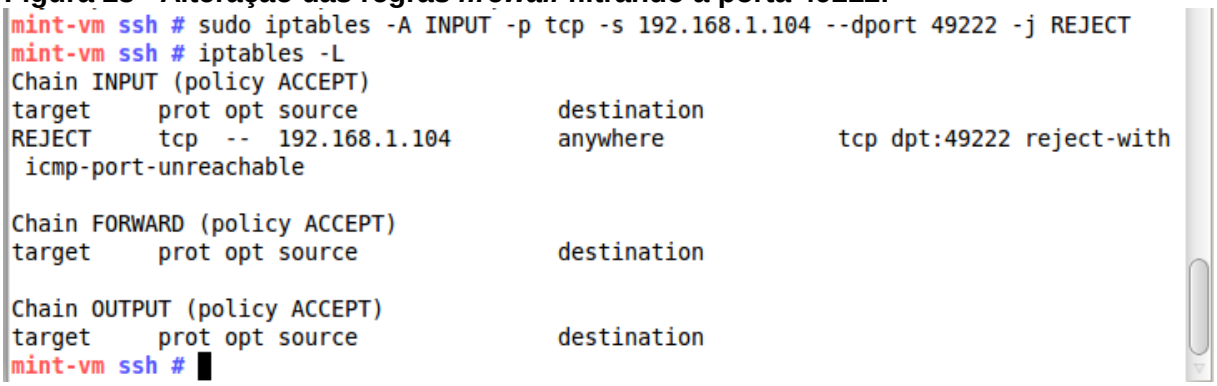
Fonte: Autoria própria.

Conforme apresentado na Figura 22, o NMAP voltou a reconhecer o SSH disponível na máquina, dessa vez na porta 49222. Como a varredura completa testa todas as portas, em um comparativo com o exame mais enxuto, o tempo de execução aproxima-se do dobro, enquanto o exame mais enxuto levou 11.34 segundos para ser executado, o exame mais completo foi executado em 21.26 segundos. Em uma varredura completa de rede com centenas e até milhares de máquinas, um atacante provavelmente não utilizará esse parâmetro, mas dependendo do conhecimento que ele tiver da rede, se estiver em busca de uma falha em um alvo específico, ou um conjunto pequeno de máquinas, somente a alteração da porta não será suficiente, pois como se pode notar, a porta continua aberta, recebendo conexões sem qualquer tipo de filtro. Para resolver essa situação, será utilizado o *firewall* nativo em grande parte das distribuições *Linux,* o *Iptables.*

A configuração do *Iptables* provavelmente terá grandes variações dependendo das necessidades da rede. Se a organização auditada não precisa de acesso externo no SSH, poderá negar acessos a rede que não seja a interna. Se for possível limitar ainda quais terminais acessarão tal máquina remotamente, pode e é recomendável que essa limitação seja feita.

Foi executada a linha de comando **sudo iptables -A INPUT -p tcp -s 192.168.1.104 --dport 49222 -j REJECT** na máquina auditada, conforme pode ser visualizado na Figura 23. Vale lembrar que o parâmetro **sudo** é necessário para que o comando seja executado como *root*, ou usuário administrador em terminais *Linux.*

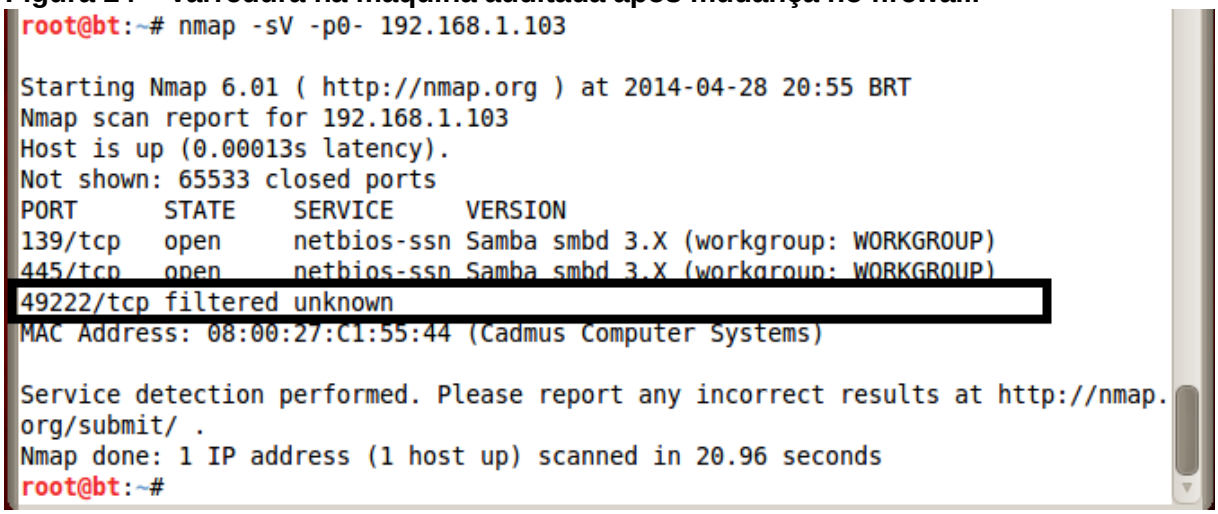
Figura 23 - Alteração das regras *firewall* filtrando a porta 49222.



Fonte: Autoria própria.

Após tal alteração nas regras de *firewall*, a varredura com o NMAP trouxe o seguinte resultado, apresentado na Figura 24.

Figura 24 – Varredura na máquina auditada após mudança no firewall.

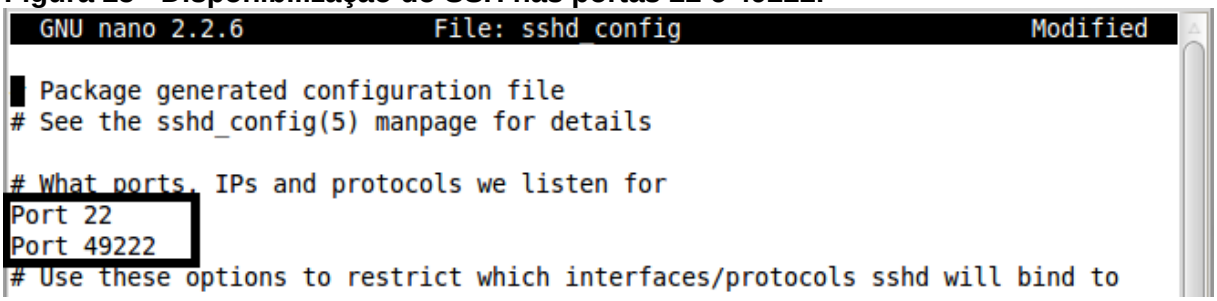


Fonte: Autoria própria.

Agora já é possível notar uma grande diferença no resultado da varredura. A regra acrescentada ao *firewall* da máquina auditada especifica que todas as conexões de entrada pelo protocolo TCP vindos do IP 192.168.1.104 que, nesse caso é a máquina auditora, na porta 49222 sejam rejeitadas. Nesse caso, foi especificado o IP da máquina auditora para fins de demonstração, mas pode ser acrescentada uma regra que negue todas as conexões, e em seguida uma regra que aceite conexões somente da rede interna. Foi adicionada uma regra de negação para demonstrar o resultado da varredura do NMAP. Dessa vez, a porta aparece disponível, no entanto com o estado filtrado e, como todas as requisições vinda do IP da máquina auditora sequer passam pelo *firewall*, não é estabelecida uma conexão com a porta e o NMAP não consegue reconhecer o serviço disponível na máquina.

Outra medida que pode ser tomada, essa para confundir os atacantes, seria deixar o SSH também disponível na porta 22, conforme pode ser visto na Figura 25.

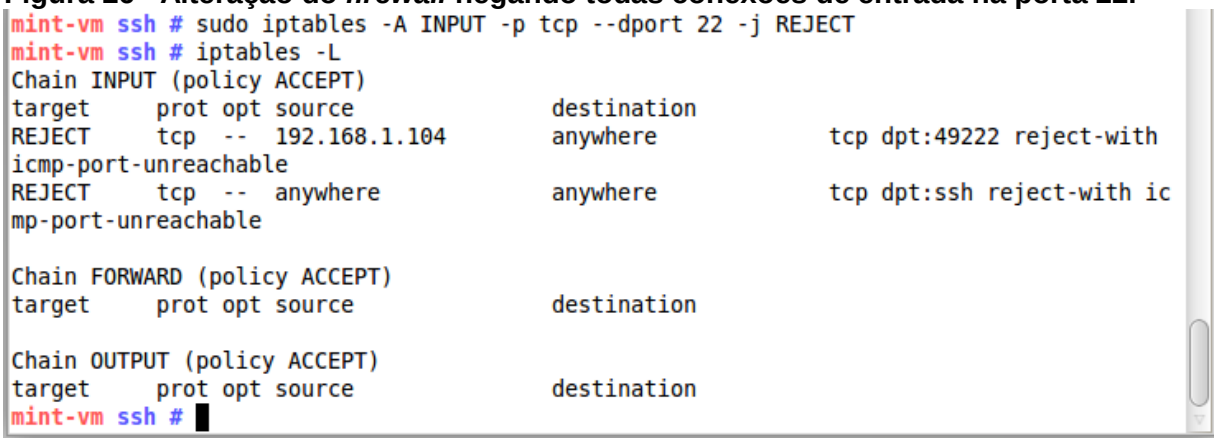
Figura 25 - Disponibilização do SSH nas portas 22 e 49222.



Fonte: Autoria própria.

Após essa alteração, no entanto, foi tomada a medida de negar todas as conexões através da porta 22, através do comando **sudo iptables -A INPUT -p tcp --dport 22 -j REJECT,** que encarrega-se de rejeitar todas as conexões de entrada do protocolo TCP na porta 22. A aplicação dessa regra de filtragem é vista na Figura 26.

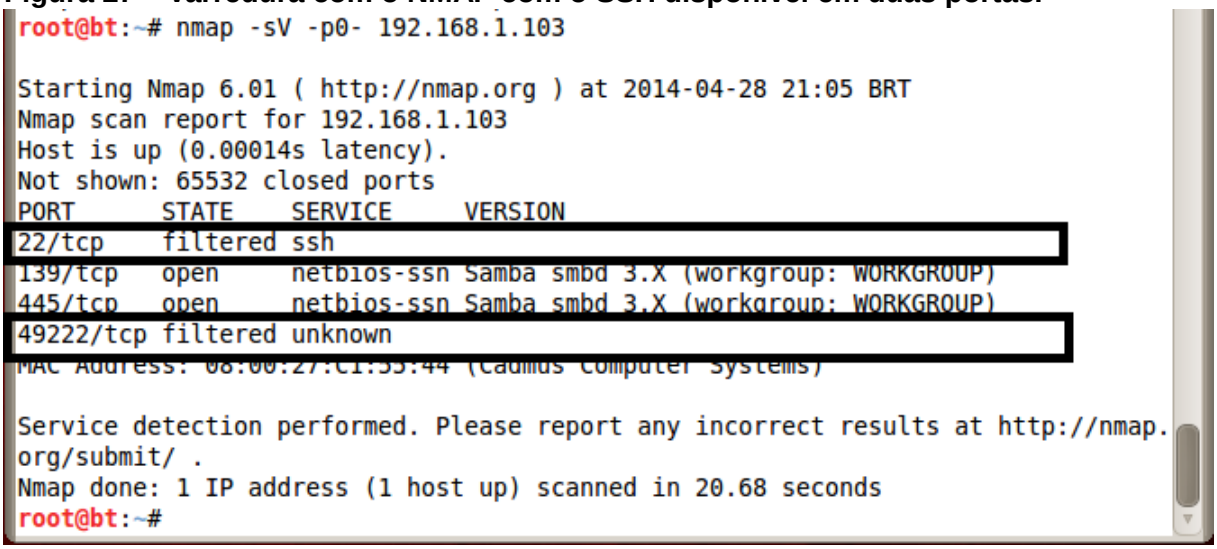
Figura 26 - Alteração do *firewall* negando todas conexões de entrada na porta 22.



Fonte: Autoria própria.

Nesse caso, a varredura com o NMAP ficaria como na Figura 27.

Figura 27 – Varredura com o NMAP com o SSH disponível em duas portas.



Fonte: Autoria própria.

Neste exemplo, o arquivo de configuração do SSH, o **sshd_config** da máquina auditada possui duas linhas especificando portas em que o SSH está disponível. Nesse caso, a porta 22 e a porta 49222. No entanto, para a porta 22, o *firewall* está recusando todas as conexões de entrada (Figura 26), sendo impossível para qualquer usuário, vindo de qualquer IP, conectar-se remotamente a essa máquina pela porta 22. Nesse caso, o NMAP reconhece o serviço SSH na porta 22, mesmo sem conseguir se comunicar com ela devido ao fato dessa ser a porta padrão desse serviço e essa informação estar presente no arquivo **nmap-services**. Como a porta 49222 não tem

padrão especificado no arquivo em questão, o serviço disponível nela aparece como *unknown* (não identificado).

Com essa etapa, finaliza-se o processo de verificação do NMAP com o SSH. Com relação a esse serviço, outras medidas de segurança devem ser tomadas, como, por exemplo, a confecção de uma lista de usuários autorizados a se conectarem à máquina; não se deve permitir acesso com controle total (*root* em terminais *Linux*), visando evitar danos maiores caso haja um acesso não autorizado; de acordo com a política da organização, pode ser feita uma auditoria com relação a complexidade das senhas utilizadas, mas para realizar esses procedimentos, são necessárias outras ferramentas. Essa varredura feita sobre o serviço SSH pode ser feita também com outros serviços que possam estar disponíveis na rede como, por exemplo, o SMTP (*Simple Mail Transfer Protocol),* que é um protocolo de correio eletrônico, detectando as possíveis falhas e corrigindo-as, ou ainda, detectando portas abertas em máquinas que não estejam sendo utilizadas, para que estas sejam fechadas, diminuindo as brechas para possíveis atacantes.

5 CONSIDERAÇÕES FINAIS

A seguir, será apresentada uma tabela com os principais resultados obtidos durante a execução do trabalho e os comentários pertinentes serão feitos após a apresentação da tabela.

Tabela 1 – Resumo dos resultados obtidos na execução do trabalho.

Parâmetros Utilizados	Configuração de Filtragem	Objetivos	Resultados Obtidos
-sP	Indefinido	Mostrar *hosts* disponíveis na rede através de testes de *ping.*	Lista de *hosts* disponíveis.
Nenhum	Indefinido	Varrer a rede por completo.	Lista de portas abertas nos *hosts* disponíveis.
-sV	Indefinido	Mostrar serviços disponíveis com maiores detalhes.	Lista dos serviços disponíveis nas portas com maior detalhamento.
-A	Indefinido	Obter informações mais precisas	Lista de serviços, detecção de SO, localização geográfica aproximada, entre outros
-Pn	Indefinido	Varrer a máquina sem verificar sua disponibilidade.	Sem informações adicionais.
-T0 e –T5	Indefinido	Verificar diferença de tempo entre as opções de temporização disponíveis.	Diferença substancial notada.
-sV	Nenhuma	Identificação dos serviços detalhada.	Identificação dos serviços obtida.
-sV	Nenhuma	Identificar serviço disponível fora de sua porta padrão.	Serviço não identificado
-sV –p0-	Nenhuma	Identificar serviço disponível fora de sua porta padrão	Serviço identificado na porta real
-sV –p0-	Negando conexões na porta real do serviço.	Identificar serviço disponível fora de sua porta padrão.	Porta reconhecida, porém serviço não é identificado.
-sV –p0-	Negando conexões na porta padrão e na real.	Identificar serviço disponível na porta padrão e fora dela.	Portas padrão e real identificadas. Serviço não reconhecido na porta real, mas reconhecido na porta padrão, devido consulta ao arquivo de portas padrão.

Fonte: Autoria própria

Na tabela 1 foram resumidos os principais comandos utilizados durante a execução do experimento. Na primeira coluna, são apresentados os parâmetros utilizados em cada uma das execuções da varredura, apropriados com o objetivo do exame em questão. Na segunda coluna, são colocadas as regras de filtragem. Quando é apresentado o status “indefinido”, entende-se que não houve manipulação no *firewall* dos alvos varridos em questão, ou seja, essas eram máquinas reais em uso em uma rede doméstica comum. Na terceira coluna, são apresentados os objetivos de cada execução da varredura, comprovando a utilização de seus respectivos parâmetros. Na quarta e última coluna, são mostrados os resultados obtidos em cada um dos exames, combinando os parâmetros utilizados e as regras de filtragem.

Conforme verificou-se durante a realização do trabalho, o NMAP é uma importante ferramenta para a identificação de vulnerabilidade em redes. Mas, além disso, o NMAP é bastante útil para se fazer inventários de rede, levantamento de softwares em utilização, status de uso da rede, entre outros. Uma situação que prova que o NMAP pode ser utilizado não somente para a identificação de vulnerabilidades é quando um sistema operacional deixa de ter suporte e é necessária a migração para um mais atual. Em uma grande rede, com equipamentos instalados em diversas regiões geográficas, seria inviável o administrador ir a cada terminal verificar se o sistema utilizado ainda recebe suporte pelo seu fabricante. Nesse caso, o recurso de detecção de SO remoto do NMAP pode ser bastante útil.

Quando o assunto é especificamente a segurança, pode-se ver que o NMAP proporciona um grande auxílio ao administrador da rede, tendo em vista que ele aponta falhas não visíveis “a olho nu”, como regras de filtragem de *firewall*, por exemplo. Em uma rede com dezenas, até centenas de regras de filtragem, é mais trabalhoso um administrador analisar regra por regra para saber se de determinado local, é possível ou não ter acesso a determinado serviço. No entanto, o NMAP não garante segurança a ninguém nem corrige erros, ele apenas os aponta. Então, para interpretar os dados que o NMAP traz e corrigir as possíveis falhas, o administrador precisa ter conhecimento técnico do recurso que está sendo avaliado, conhecer as políticas da organização, pois em segurança da informação, nem sempre a regra adotada na organização A poderá ser adotada na organização B. Portanto, o NMAP é

uma ferramenta de grande valor para administradores de rede para identificar vulnerabilidades, mas para corrigi-las, é necessário o uso de outras ferramentas. Isso faz com que o NMAP se saia bastante útil em auditorias, tendo em vista que o processo de auditoria busca somente a coleta de informações e apontamento de falhas.

Para trabalhos futuros, sugere-se a busca de vulnerabilidades em outros serviços, como FTP, SMTP, entre outros e a atuação de IDS's e registro de *logs* de *firewalls* durante a ação do NMAP para que um administrador possa se proteger de varreduras feitas por atacantes em busca de falhas de segurança na rede.

6 REFERÊNCIAS

CERT.br. **Incidentes reportados ao CERT.br – Janeiro a Dezembro de 2013, 2014.** Disponível em: <http://www.cert.br/stats/incidentes/2013-jan-dec/scan-portas.html>. Acesso em 03/05/2014.

DAWEL, George. **A Segurança da Informação nas Empresas,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2005.

FANTINATI, João Marcos. **Auditoria em Informática:** metodologia e prática**,** São Paulo: Mc-Graw-Hill, 1988.

FONTES, Edison Luiz Gonçalves. **Praticando a segurança da informação,** Rio de Janeiro: Brasport, 2008.

GIAVAROTO, Silvio César Roxo, SANTOS, Gerson Raimundo dos. **Backtrack Linux – Auditoria e Teste de Invasão em Redes de Computadores,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2013.

IMONIANA, Joshua Onome. **Auditoria de Sistemas de Informação.** 2 Ed. São Paulo: Atlas, 2011.

JACKSON, Chris, **Network Security Auditing,** Indianapolis USA: Cisco Press, 2010.

KUROSE, James F. **Redes de computadores e a internet:** uma abordagem top-down. 5 Ed. São Paulo: Addison Wesley, 2010.

LYON, Gordon Fyodor. **Exame de Redes com o NMAP,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2009.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2008.

MANOTTI, Alessandro. **Curso prático. Auditoria de Sistemas:** Compreenda como funciona o processo de Auditoria Interna e Externa em Sistemas de Informação de uma forma prática**,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2010.

NETO, Urabatan. **Dominando Linux Firewall Iptables,** Rio de Janeiro: Editora Ciência Moderna Ltda., 2004.

STALLINGS, William. **Criptografia e Segurança de redes**. 4 Ed. São Paulo: Pearson Prentice Hall, 2008.