NMAP: um estudo sobre a ferramenta de busca e análise de vulnerabilidades em redes

LEITE, Luan Amorim [1] ; DAIBERT, Marcelo Santos [2]

[1] Discente Graduação CIÊNCIA DA COMPUTAÇÃO
[2] Docente Graduação CIÊNCIA DA COMPUTAÇÃO

luanleite.ti@gmail.com
daibert@unifagoc.edu.br

RESUMO

O nMAP consiste em uma ferramenta que busca detectar possíveis vulnerabilidades de uma rede realizando uma série de testes. O objetivo deste trabalho foi realizar um estudo da ferramenta, explorando suas funções em um ambiente real de aplicação e gerando um relatório de falhas para a instituição em análise, e a produção de um referencial de utilização da ferramenta para auxílio a novos ingressantes na área de segurança da informação. Este estudo foi baseado no teste de caixa branca (white box.) para a realização de testes internos na rede do UNIFAGOC. Como resultado, obteve-se um relatório dos devidos exames realizados e possíveis vulnerabilidades encontradas na rede em análise.

Palavras-chave: *Vulnerabilidades. Redes. nMAP. Teste.*

INTRODUÇÃO

A globalização e a expansão da internet são fatos eminentes e de valor imensurável para os seres humanos. A internet é universal e com o seu surgimento veio a disseminação dos computadores que deram início a um novo ambiente mundial, gerando um crescimento de dados desordenado e com pouca segurança (NAKAMURA; GEUS, 2007). Um conjunto de dados origina a informação, fazendo com que algo com valor pouco expressivo se torne um bem valioso e de interesse mútuo, seja para as empresas ou para pessoas que possuem interesses próprios (FONTES, 2006).

Sabendo da importância de seus dados e de seus valores, foram elaborados princípios para classificar o estado de um dado: a preservação da confidencialidade, que tem como ideia manter seus dados confidenciais; a integridade, para garantir que não haja alterações nos dados; a autenticidade, que tem como intuito manter os dados autênticos e únicos; e a disponibilidade, que consiste em manter os dados disponíveis a qualquer instante (KUROSE; ROSS, 2006). Sabedoras disso, as empresas têm implementado políticas de segurança para manter seus dados seguros, já que são bens valiosos. Por essa razão deve-se mantê-los sob regras e procedimentos, já que se trata de um recurso crítico para que a empresa possa se manter na sua missão de negócio (FONTES, 2006).

O Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no

Brasil (CERT. BR) relatou que o número de incidentes relacionados à segurança de dados de 2018, que era de 676,514, caiu 23,24% em relação a de 2017, quando era de 833,775 por ano.

Nesse contexto, seja em uma empresa de grande, médio ou pequeno porte, a necessidade de uma rede para compartilhar recursos, informações, e até acessar um certo tipo de serviço, de forma que seja instantânea, é real (TANENBAUM, 2003). Esses dados são armazenados em grandes computadores chamados servidores, que são mantidos em segurança por meio de várias tecnologias que podem ser implementadas. Progressivamente as empresas têm aprimorado sua política de segurança e implantado sistemas e tecnologias novas cada vez mais eficazes em suas redes para tentar manter seus dados e informações seguros. Contudo, assim como a segurança evolui, surgem ferramentas que têm como objetivo buscar vulnerabilidades para facilitar o acesso, adentrar e se aproveitar da rede ou servidor em específico (TANENBAUM, 2003).

Ainda de acordo com Tanenbaum (2003), a maior parte dos problemas de segurança é causada por agentes externos, que buscam invadir o sistema para obter algum benefício, chamar a atenção ou prejudicar alguém.

Problema e sua importância

De acordo com Lyon (2009), a ferramenta nMAP tornou-se o scanner de segurança de redes com maior influência no mundo, atingindo milhões de usuários. Contudo, em um ambiente de redes há uma gama de alterações que podem ser implicadas para cada cenário, o que pode ocasionar em um ambiente frágil e mal estruturado no quesito de segurança. O nMAP tem como principais funcionalidades ser um auditor de redes para garantir que um ambiente esteja seguro, realizando buscas e testes de vulnerabilidades para que possíveis correções a falhas sejam realizadas.

Objetivos

Objetivo geral

Realizar um estudo de vulnerabilidades com a ferramenta nMAP, aplicando testes com as funções que a ferramenta abriga, no intuito de extrair informações de redes e servidores em análise, a fim de contribuir com a sua divulgação para futuros estudos do nMAP.

Objetivos específicos

- Fazer um estudo da ferramenta e suas funcionalidades;
- Produzir um referencial teórico para usuários que possuem a intenção de adentrar na área de segurança de dados;

• Elaborar um estudo de caso da utilização da ferramenta na UNIFAGOC, disponibilizando um relatório das vulnerabilidades encontradas para a instituição.

Metodologia

Neste estudo de caso utilizou-se o teste de white box, também conhecido como "teste de caixa branca", tendo em vista que essa aplicação tem mais expressividade para a instituição. O responsável pela análise deve estar ciente de todas as ferramentas e tecnologias a serem empregadas nos testes.

Wireshark

O Wireshark é uma ferramenta para solução de tráfego em um ambiente de redes. A ferramenta tem como principal função capturar todo trânsito de pacotes em uma rede em análise, com a ideia de propor soluções e melhorias aplicando novos protocolos e decodificando problemas existentes no tráfego tanto interno como externo a rede analisada (SHIMONSKI, 2013). A ferramenta teve como funcionalidade auxiliar no rastreio da comunicação e a troca de pacotes entre o host e o servidor, com a finalidade de demonstrar os pacotes trafegados na rede e possíveis alterações propostas por cada comando executado.

1- Primeiramente foi realizado um estudo da ferramenta e da sua utilização em um ambiente de testes em que se simula um ambiente real. Esse ambiente de teste consiste em 4 servidores baseados em um sistema Debian, e cada uma dessas máquinas possuía alguns serviços instalados e suas respectivas portas configuradas.

2- Depois da realização do estudo e da elaboração do ambiente de teste, foi realizada a aplicação de exames na rede em que o ambiente foi criado. Esses testes se consistiram em coletar informações sobre a rede e testar comandos que possivelmente seriam usados no estudo de caso.

3- Após a etapa de aprendizado e de testes no ambiente simulado, foi realizada a coleta de informações da rede onde o estudo de caso foi realizado. Neste passo, houve a coleta de informações na rede da UNIFAGOC. Os testes consistiam em: descoberta do range de IP, máscara de subnet utilizada, classe do IP, quantidades de host ativos, etc.

4- Com a realização da coleta de informações, foi dado início à execução de exames que consistem na descoberta de vulnerabilidades na rede administrativa da UNIFAGOC. A rede interna da instituição pode ser acessada caso uma máquina esteja com seu endereço MAC cadastrado; sendo assim, o setor de TI da universidade foi responsável por esse cadastro e liberação do uso da rede.

5- Os exames executados se basearam na descoberta de portas, serviços ativos, versão dos serviços, sistema operacional e vulnerabilidades.

6- Para a execução dos exames de vulnerabilidades, foi simulado um servidor Windows com as mesmas configurações e versões de softwares do que se encontrava na

universidade, visando manter a integridade e a estabilidade de seus serviços, visto que a execução de scripts em um ambiente de produção pode gerar danos sem reparação, causando instabilidade e até mesmo a queda de alguns serviços.

7- Por fim, procedeu-se à documentação dos devidos testes e à seleção de informação para geração do relatório final.

REFERENCIAL TEÓRICO

Segurança de dados em redes

Coulouris (2007) discorre sobre os pilares da segurança da informação em sistemas distintos:

• Identificar o cliente que faz acesso a um serviço, o que é essencial para manter o pilar da Confidencialidade estável; e

• Manter a integridade dos dados sobre a política de controle de acesso à informação, que é a parte chave para que não haja vazamentos.

Kurose e Ross (2006) relatam que, em uma comunicação entre dois pontos, deve haver segurança, a fim de que se mantenha a integridade das informações trocadas entre o emissor e o receptor. Os autores acrescentam que é preciso garantir que a comunicação aconteça de modo a não haver quaisquer interferências ou falhas. Como dito anteriormente, a área de segurança engloba não só a proteção de dados, mas também inclui a prevenção de ataques a uma dada infraestrutura, por meio da identificação de possíveis falhas e vulnerabilidades em uma comunicação, estabelecendo métodos de reação e prevenção.

A segurança tem como ideia principal ser uma área expressiva que demanda, principalmente, garantir que usuários que não possua permissão de acesso a um determinado serviço sejam barrados, e assegurar a validade de serviços e informações, mantendo sua consistência e integridade (TANENBAUM, 2003).

Novos métodos de ataques são descobertos e testados a cada instante; com isso, a área de segurança em redes tende a se manter em evolução. A implementação de novos métodos e tecnologias tem com afinidade detectar, proteger e reagir, gerando um ciclo entre atacantes e combatentes (NAKAMURA; GEUS, 2007).

O nMAP

O nMAP (de "Network Mapper", ou "Mapeador de Redes" em português) é uma ferramenta que busca explorar possíveis vulnerabilidades e fazer análises precisas. Trata-se de uma ferramenta livre, de código aberto, criada para auxiliar administradores de sistemas a aumentar a segurança já instalada e a prevenir-se contra possíveis agentes externos a sua rede, tais como invasores (LYON, 2009). Em contrapartida, o utilitário

também pode ser uma arma a ser explorada por crackers, que fazem uso da ferramenta para buscar vulnerabilidades na rede e realizar invasões.

De acordo com Lyon (2008), questões legais envolvem a usabilidade da ferramenta para análise de vulnerabilidades. A devida ferramenta, quando usada de forma correta, com o intuito de acrescentar segurança a uma rede, tem sua aplicação precisa, com resultados satisfatórios.

Ferramentas expressivas na área de scanport, como o tcpdump, o Net-cat e o Jhon the Ripper, tornaram-se obsoletas com o passar do tempo, graças às poucas atualizações nesse período, diferente do nMAP, que se manteve em atualização desde a sua criação. Em contrapartida, o nMAP tem seu futuro incerto. A ferramenta é movida pela comunidade de segurança de informação e apoiadores que se inspiram em sua licença de código aberto (LYON, 2009).

A FERRAMENTA EM EXECUÇÃO

O nMAP consiste em uma ferramenta que trabalha com o envio de pacotes para um alvo ou destino, com o intuito de coletar informações valiosas para futuros passos a serem tomados em um processo de Pen-Test. A ferramenta trabalha com a criação e manipulação de pacotes em estado bruto, para que, ao serem enviados, retornem diversos tipos de informações, tais como disponibilidade do alvo, estado de uma porta, serviços, versão de um sistemas até vulnerabilidades existentes.

Uma vez com a ferramenta instalada, a da ferramenta pode ser utilizada pela Command line interface (CLI) para execução de suas ações. O nMAP trabalha com a execução de comandos por parâmetros que devem ser especificados via terminal que é o bash/shell do sistema Linux. Todo comando a ser utilizado deve possuir o prefixo "nmap". Esse prefixo diz para o sistema operacional dar um start na ferramenta, com isso realizando a sua inicialização.

Privilégios de execução

Há uma diferença na inicialização da ferramenta quando se possui o privilégio de root na sessão estabelecida. O privilégio de root fará com que a ferramenta possa ou não manipular o cabeçalho de cada pacote enviado, com isso, podendo setar novas flags em seu cabeçalho para que ele retorne diferentes informações. Quando sua inicialização é realizada sem este privilégio, a ferramenta fica mais restrita a enviar pacotes pré-montados por sua própria arquitetura interna.

Inicializando sem o privilégio de root:

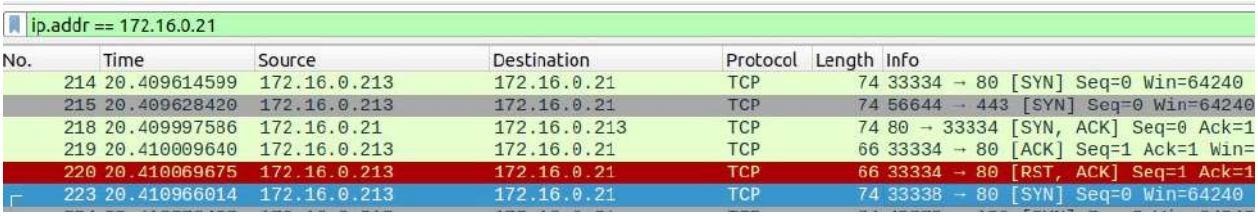
Figura 1: Scanner padrão sem privilégio de root

Fonte: dados da pesquisa.

A inicialização do comando listado na Figura 1 tem como intenção escanear o alvo de uma rede em específico. O símbolo "$" só é apresentado quando o devido comando for executado sem a permissão de root. O nMAP realizará o envio de alguns pacotes pré montados para o alvo especificado, atribuindo flags padrões no cabeçalho do pacote enviado ao alvo.

A falta do privilégio de root tem como consequência a pré-montagem do cabeçalho do pacote enviado; com isso, o nMAP realiza o envio de pacotes com flags pré setadas, assim muitas vezes retornando informações desnecessárias ou inválidas. Caso o usuário rode um comando nmap 172.16.0.21 para escanear esse host sem o privilégio root, o nMAP irá colocar por padrão a opção –sT, inicializando uma conexão do tipo TCP CONNECT. Com isso, será realizada uma tentativa de abertura de conexão com o servidor enviando um pacote SYN; caso o host se encontre ativo, a devida conexão passará por um reconhecimento, devido ao envio de um pacote ACK e, logo após, o nMAP irá fechar a conexão graças ao envio de um pacote RST; por último, será dado o final da conexão por um pacote FYN, assim realizando o procedimento de "three way handshake" de acordo com a saída do comando apresentado na Figura 2.

Figura 2: Saída do scanner padrão listado



Fonte: dados da pesquisa.

O scanner padrão do nMAP realiza o envio desses pacotes pré-montados em algumas portas especificadas por sua arquitetura. Já com o privilégio de root, o nMAP consegue trabalhar com pacotes em estado bruto, havendo a facilidade da alteração do cabeçalho, assim facilitando a obtenção de informação de um devido alvo em específico.

Flags

Como dito antes, a ferramenta nMAP trabalha com o envio de pacotes brutos, que podem ser alterados para garantir que se obtenha uma certa informação relevante. As

flags são parâmetros existentes em um cabeçalho de pacote e podem ser alteradas de acordo com o privilégio de execução cedido a ferramenta.

A execução de um comando com a concepção de root faz com que seja possível realizar alterações nessas flags. As flags mais comumente usadas na ferramenta são:

• ACK: Esta flag é utilizada para reconhecimento durante o processo de abertura de uma conexão TCP com um alvo /destino.

• SYN: Flag usada para realizar a sincronização de dados e abertura de conexão com servidor ou destino especificado.

• RST ou RESET: Indicar uma recusa de conexão ou falta de resposta do host escaneado.

• FYN: Indica um fechamento de conexão.

Cada comando de scan possui uma flag específica, sendo possível a realização de alteração ou adição de mais flags no cabeçalho do pacote. Sendo assim, o nMAP possui o comando "scanflags", que recebe como parâmetro as flags que o usuário deseja utilizar. Segue abaixo a utilização do comando:

Figura 3: Utilização do comando - scanflags

Fonte: dados da pesquisa.

Após a execução do comando, o pacote passa a conter as demais flags em seu cabeçalho:

Figura 4: Saída do comando - scanflags

Fonte: dados da pesquisa.

Especificação de portas

Como o nMAP é um scanner de redes, a especificação de portas a serem escaneadas é importante, uma vez que cada serviço contido em um host pode estar rodando e sua porta padrão ou em uma devida porta alterada. Por padrão, o nMAP executa um scan nas diversas portas ativas de um host e, caso ele se encontre rodando em um sistema operacional posix , como Linux ou unix, o nMAP também realizará o scan nas portas contidas no arquivo /etc/services, onde essas portas são mais conhecidas como "portas

altas". Trata-se basicamente de portas que ficam especificadas com padrão para alguns tipos de serviços.

Cada porta pode possuir um dos seis estágios a seguir discriminados:

• OPEN (aberta): Significa que um serviço está rodando e está aceitando conexões TPC ou pacotes UDP. Encontrar portas abertas é basicamente a intenção do exame de redes.

• CLOSED (fechada): Geralmente são portas que se encontram fechadas por não terem um certo serviço ativo naquela porta. Tem sua utilidade, como mostrar se um serviço está ativo ou não em um host.

• FILTERED (filtrada): Significa que a porta pode estar sendo protegida por um firewall; com isso, o envio de pacotes pode estar sendo filtrado por ele, o que causa lentidão nos exames e mantém a omissão de informações.

• UNFILTERED (não filtrada): Quando uma porta se encontra neste estado, geralmente ela está acessível, mas o nMAP não consegue desvendar se ela se encontra aberta ou fechada. Esse tipo de resposta só aparece em exames de scan ACK, que são usados para mapear regras de firewall.

• OPEN/FILTERED (aberta ou filtrada): Portas são assim classificadas quando o nMAP é incapaz de determinar se a devida porta se encontra aberta ou filtrada. Isso ocorre pois muitas vezes um firewall descarta a resposta de uma requisição de conexão para o servidor, assim ficando sem resposta.

• CLOSED/FILTERED (fechada ou filtrada): Comum quando o nMAP não consegue determinar se uma porta está aberta ou fechada. Este estado só é usado quando um exame de ociosidade é executado.

No verão de 2009, Lyon, criador da ferramenta, fez um estudo das principais portas abertas e serviços que podem ser encontradas em um exame. Algumas dessas portas podem se encontrar vulneráveis pelo tipo de serviço existente nelas. Nesse contexto, o quadro abaixo mostra as 10 portas mais comumente abertas.

Quadro 1: Portas comumente abertas

PORTA	PROTOCOLO/ SERVIÇO	DESCRIÇÃO
80	HTTP	Responsável por 14% das portas abertas que foram descobertas
23	TELNET	Portas utilizada para administração de *switches* de rede
443	HTTPS	Utilizada por servidores *web* encriptados por SSL; porta usada por omissão.
21	FTP	Responsável pela transferência de arquivo. É um protocolo inseguro e de fácil manipulação.
22	SSH	Utilizado para acessos remotos. Uma solução segura para o protocolo TELNET.
25	SMTP	Protocolo padrão para transferência de *e-mails*. Também inseguro.
445	MICROSOFTDS	Utilizado para comunicação SMB sobre IP com serviços do MS WINDOWS.
53	DOMAIN	DNS, sistema inseguro para conversação de nomes de hospedeiros/domínios sobre IP.
8080	HTTP_PROXY	Porta alternativa para servidor WEB.
3306	MYSQL	Comunicação com bancos de dados mysql.
3050	FIREBIRD	Comunicação com bancos de dados Firebird.

Fonte: dados da pesquisa.

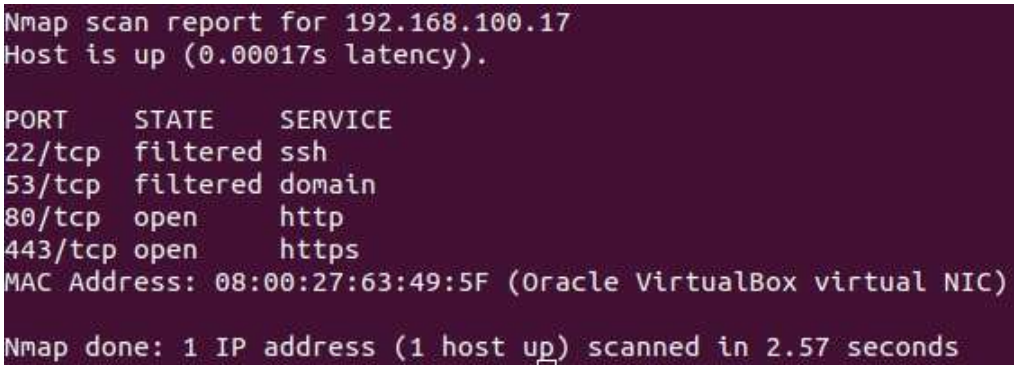
A ferramenta possibilita listar que um mesmo exame possa ser executado em várias portas diferentes. O comando "-p" do nMAP recebe como parâmetro as portas em que o exame deve ser executado; assim, o exame acontecerá em cada porta que for especificada.

Figura 5: Especificando do comando

Fonte: dados da pesquisa.

O comando acima será executado em cada porta que foi passada como parâmetro para o comando –p. Assim, sua saída será:

Figura 6: Saída do exame de portas



Fonte: dados da pesquisa.

O exame mostra que todas 4 portas que foram especificadas fazem parte do protocolo TCP e que duas se encontram no estado open com um possível serviço específico naquela porta. Já as outras duas portas que se encontram com o estado open estão abertas, e seus serviços que estão ativos são o http e o https.

DESENVOLVIMENTO

Unidade empírica de análise

Todo o conteúdo foi gerado a partir da aplicação de testes na UNIFAGOC, uma universidade/centro de ensino para alunos de graduação e pós-graduação, localizada na Zona da Mata mineira. A instituição vem crescendo gradativamente, expandindo seus cursos e aumentando a procura de novos alunos. Esse crescimento tem como consequência o aumento de dados a serem salvos, portanto a ideia de realizar um estudo de caso na instituição agrega valor, por ter como objetivo avaliar a segurança que está empregada na rede em análise e acrescentar melhorias para que possam se manter um alto nível.

Estudo de caso

As pesquisas bibliográficas basearam-se na documentação oficial da ferramenta NMAP.ORG (2019) e em Lyon (2008). Os testes realizados foram documentados e estarão disponíveis para mais detalhes em: https://bit.ly/2qiDrO8 .

Inicialmente foi realizada uma coleta de informações para conhecimento maior do alvo em que os testes seriam analisados. Para isso, foi realizado o exame de DNS reverso para identificar o IP da máquina em que os teste aconteciam. Em seguida, foi realizada a coleta de informações sobre o alvo, como classe do IP, range de IPs que a empresa possui e a máscara de suporte. Essas informações constam no teste abaixo:

Figura 7: Coleta de informações sobre o alvo

```
Endereço:    172.16.0.0             10101100.00010000.0000 0.000,00 milhões
Máscara de rede:    255.255.240.0 = 20     11111111.11111111.1111 0.000,00 milhões
de curinga:   0.0.15.255             00000000.00000000.0000 1.111,11111111
 =>
 de rede:    172.16.0.0/20          10 101100.00010000.0000 0.000,00 milhões ( Classe B )
Transmissão: 172.16 .15.255          10101100.00010000.0000 1111.11111111
HostMin:    172.16.0.1             10101100.00010000.0000 0000.00000001
HostMax:    172.16.15.254          10101100.00010000.0000 1111.11111110
Hosts / Net:4094                   ( Internet privada )
```

Fonte: dados da pesquisa.

Após a obtenção dessas informações, foi realizado um exame por range de IP, listando cada máquina contida na rede especificada. O exame se baseia em realizar uma vistoria em cada host contido no range de IP, trazendo informações baseadas em seu endereço IP. Esse range de IPs suporta até 4094 hosts. A Figura 8 ilustra o teste utilizado.

Figura 8: Exame por range de IP comando -sL

```
sudo nmap -sL 172.16.0.0/20
```

Fonte: dados da pesquisa.

Esse exame traz como resposta uma lista de hosts que são contidos em uma range de IP que pode ser escaneada. Para isso, ele não precisa enviar qualquer tipo de pacote em específico e, como característica do exame, a solução de DNS reverso é ativada para descobrir seus nomes. Logo, está localizado em uma parte relevante obtida pelo comando:

Figura 9: Saída comando -sL

```
Nmap scan report for 172.16.0.0
Nmap scan report for administrativo.fagoc.br (172.16.0.1)
Nmap scan report for 172.16.0.2
Nmap scan report for suporte.fagoc.br (172.16.0.3)
Nmap scan report for 172.16.0.4
Nmap scan report for 172.16.0.5
Nmap scan report for integracao.fagoc.br (172.16.0.6)
```

Fonte: dados da pesquisa.

A descoberta de host por um range de IP é atrativa, mas não agrega muito valor. Para isso ser de alguma valia para a instituição, foi realizado um novo teste, baseado em um ping ICMP em cada host do range de IP obtido. Como consequência, o exame só lista hosts que estão com estado UP e que respondem ao exame por ping. Segue o exame

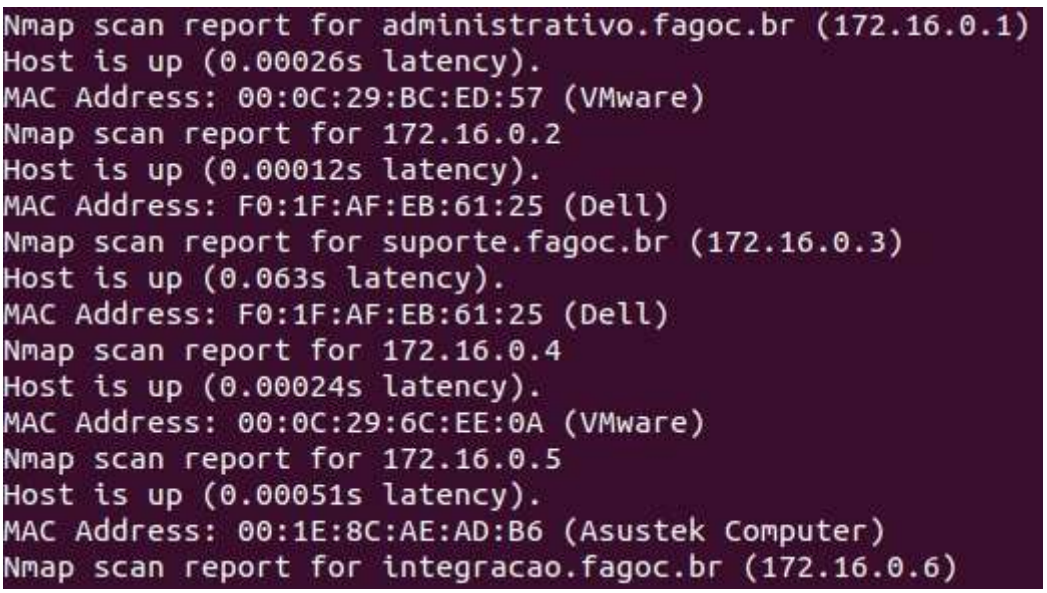
aplicado:

Figura 10: Exame por ping ICMP comando -sP

Fonte: dados da pesquisa.

Diferente do anterior, este exame tem como benefício listar somente hosts disponíveis na rede. Em caso de um ataque real, o atacante irá economizar tempo na procura de um host que possui uma relevância maior. Já para segurança de instituição, serve como melhoria desativar a descoberta por ping ICMP em alguns hosts da rede. Saída relevante do exame:

Figura 11: Comando -sP



Fonte: dados da pesquisa.

Alguns endereços de MAC se encontram duplicados por algum agente de virtualização do alvo. Como a maioria dos hosts pode estar em servidor de virtualização, esse endereço MAC pode aparecer duplicado. Seguindo com a realização dos exames, uma tentativa de abertura de conexão invisível com um host ativo da rede será realizada. Esse exame é a opção mais omissiva e mais popular do nMAP, visto que pode ser realizado de forma rápida e com uma menor atração para um firewall que pode estar protegendo esses hosts e traz como benefício a detecção de portas que possivelmente podem estar abertas. Segue o exame realizado:

Figura 12: Tentativa de abertura de conexão com um host comando -sS

Fonte: dados da pesquisa.

Como resposta ao comando ao –sS, o nMAP retorna todas as portas em que a conexão foi estabelecida com sucesso, informando o estado de cada porta, seu possível serviço e o tipo de protocolo que serve a determinada porta, além da descoberta de DNS reverso que é feita por padrão do comando. Segue a saída relevante do exame citado acima:

Figura 13: Saída do comando -sS

Fonte: dados da pesquisa.

O exame revelou que, das 1000 portas disponíveis por host, somente 24 possuem o estado open e 976 se encontram filtradas. Sabendo que 97,6% da portas do devido host se encontram filtradas, conclui-se que a existência de um firewall é verídica. Com essa conclusão, um novo exame para mapear regras de firewall foi executado.

Devido à existência de um firewall, alguns tipos de exames perdem drasticamente sua eficiência, visto que muitas vezes ele serve de filtro de pacotes para um servidor. Sendo assim, a execução do comando -sA traz como ideia principal mapear regras do firewall existente, fazendo assim uma tentativa de conexão com o servidor. Caso se obtenha uma resposta do alvo, será realizada a classificação do host com up ou down.

O comando -sA verificará a existência real de um firewall e a verificação da existência do filtro de pacote:

Figura 14: Exame ACK com o comando -sA em portas específicas

```
$ sudo nmap -sA -p80,443,21,22,8080,3000 172.16.0.21
```

Fonte: dados da pesquisa.

Este comando irá listar o estado de cada porta que foi passada como parâmetro, a existência de um firewall e, consequentemente, seu serviço. Saída do exame:

Figura 15: Saída do exame ACK

```
Nmap scan report for ponto.unifagoc.edu.br (172.16.0.21)
Host is up (0.00018s latency).

PORT     STATE    SERVICE
21/tcp   filtered ftp
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3000/tcp filtered ppp
8080/tcp filtered http-proxy
MAC Address: 44:A8:42:24:09:40 (Dell)

Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
```

Fonte: dados da pesquisa.

Posteriormente à observação da existência do firewall, foi realizado um exame no host, para avaliar qual tipo de sistema operacional esse host executa. Para a execução desse teste foram utilizados os comandos: -sV, que tem como funcionamento a detecção das possíveis versões dos devidos serviços instalados; -O, que utiliza uma técnica de detecção da versão do sistema operacional que está em execução; o –Pn, que desabilita o ping no devido alvo; o –v, que ativa o modo verbose do nMAP; e o –open, que lista somente portas abertas. Segue o comando executado para o exame abaixo:

Figura 16: Exame de detecção de versões de serviços e sistema operacional

```
$ sudo nmap -v -sV -Pn -O --open 172.16.0.21
```

Fonte: dados da pesquisa.

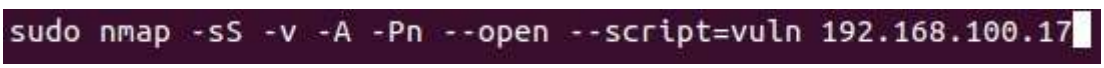
Depois de executado, o comando tem como saída relevante as versões dos serviços e SO utilizados pelo host:

Figura 17: Sida do exame de versões

Fonte: dados da pesquisa.

E como último exame do estudo de caso, foi utilizado o NSE (Nmap Scripting Engine) para execução de scripts que buscam possíveis vulnerabilidades. O NSE executa scripts que incorporam um sistema de análise de vulnerabilidades em um host ativo, baseando-se em suas versões de serviços, portas abertas, versão do sistema operacional e grau de dificuldade. O exame que será executado no NSE tem como principal ideia detectar falhas no servidor usando o modo verbose para depurar cada uma das suas execuções. O comando consiste em realizar uma conexão, com o comando –sS, usando o modo verbose -v para depurar a saída, utilizando o comando -A, que lista todas as versões de serviços e do SO para aproveitar qualquer brecha possível sendo o mais omissivo, e assim o nMAP usa o -Pn para desabilitar o ping padrão. O NSE conta com 147 scripts de vulnerabilidades que podem ser executados todos de uma só vez com o comando --scripts=vuln, o qual identifica todos os scripts que fazem análises de vulnerabilidades. Segue abaixo a aplicação do exame:

Figura 18: Exame de vulnerabilidades com o NSE



Fonte: dados da pesquisa.

Posteriormente à execução do exame, as vulnerabilidades encontradas foram anexadas a um documento txt, que está disponibilizado no link: https://bit.ly/2qiDrO8.

CONCLUSÃO E TRABALHOS FUTUROS

Após a bateria de exames descritos, conclui-se que a ferramenta nMAP se destaca pela facilidade de manipulação de pacotes para analisar pequenas e grandes redes. O mecanismo de scripts NSE tem uma grande disponibilidade de exames que buscam vulnerabilidades; em contrapartida, alguns de seus testes ainda não possuem uma funcionalidade compatível com a nova versão da ferramenta.

Também se observou que o sistema de segurança empregado pelo setor de TI da UNIFAGOC se encontra em um alto nível, visto que foram detectadas somente algumas portas com o estado aberto. Já quanto aos serviços que estão empregados em cada máquina, deve-se atentar para que se mantenham atualizados, a fim de que a correção de possíveis falhas possa ser implementada.

Como trabalho futuro, sugere-se a utilização de uma ferramenta de intrusão em paralelo com nMAP que possa agregar na exploração de falhas e vulnerabilidades existentes em um ambiente de segurança real, possibilitando inferências e explorando novas falhas.

REFERÊNCIAS

ALI, Shakeel; HERIYANTO, Tedi. **BackTrack 4**: assuring security by penetration testing. BirminghamReino Unido: Packt. Publishing Ltd., 2011.

AMORIM, Abner Freitas. **PENTEST**: um estudo classificatório e prático das principais ToolBoxes. Acesso em: 1 jul. 2019.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Estatísticas dos incidentes reportados ao CERT.br**. [s.l.], 2019. Disponível em: https://www.cert.br/stats/incidentes. Acesso em: 04 jul. 2019.

COULOURIS, George *et al*. **Sistemas distribuídos**: conceitos e projeto. Porto Alegre: Bookman Editora, 2013.

FONTES, Edison. **Segurança da informação**: o usuário faz a diferença. São Paulo: Saraiva Editora, 2006.
KUROSE, James F.; ROSS, Keith W. Redes de computadores e a internet: uma nova abordagem topdown. São Paulo: Addison Wesley Editora, 2006.

LOPES FILHO, Cesar G. *et al*. **Análises de vulnerabilidades em redes de computadores** – estudo de caso com a ferramenta nMAP. 2012. Disponível em: http://www.fatecbauru.edu.br/mtg/source/An%C3%A1lise%20de%20vulnerabilidades%20em%20re des%20de%20computadores.pdf. Acesso em: 2 jul. 2019.

LYON, Gordon. **Exame de redes com nMAP**. Rio de Janeiro: Ciência Moderna, 2009.

NAKAMURA, Emilio Tissato; DE GEUS, Paulo Lício. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec Editora, 2007.

STEEN, Maarten Van; TANENBAUM, Andrew S. **Sistemas distribuídos**: princípios e paradigmas. São Paulo: Prentice Hall, 2007.

TANENBAUM, Andrew S. **Redes de computadores**. 4. ed. Amsterdam: Vrije Universiteit, 2003.