INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Professor: Macêdo Firmino
Disciplina: Segurança de Computadoores
Prática 04: Levantamento de Informações com Nmap

Olá turma, hoje iremos aprender como fazermos o processo de varredura para coletarmos informações da rede no teste de penetração. Para iremos conhecer alguns *software* que são utilizados no processo de varredura. Vamos lá?

Processo de Enumeração

Para realizarmos o teste de invasão devemos descobrir qual é o range de IPs que é utilizado, quais os servidores existentes, os sitemas operacionais utilizados, as portas abertas, utilização ou não de Firewall, serviços em execução e com quais softwares podemos nos comunicar. Esta etapa no levantamento de informações é chamado de processo de enumeração ou varredura de rede.

Essas técnicas funcionam através da deteção de *Footprinting*, também chamado de *Fingerprinting* do sistema operacional e dos serviços. Para isso, eles:

- Analisam de pacotes que trafegam pela rede;
- Realiza a leitura de banners (assinaturas do sistema);
- Analisam as particularidades da implementação da pilha TCP/IP.

Na varredura são utilizada as seguintes técnicas:

- Descoberta de Hosts;
- Detecção de Sistemas Operacionais;
- Análise de portas (*Port scanner*);
- Análise de topologia.

Na sequência será mostrado um passo a passo necessário para realizarmos essas técnicas. É necessário testar todas maneiras possíveis para descobrir o máximo de informações possíveis. Mas antes de começarmos o processo iremos conhecer uma ferramenta conhecida como Nmap.

Ferramenta Nmap

O Nmap (Network Mapper) é uma ferramenta gratuita e de código aberto voltada para descoberta de rede, auditoria de segurança, gerenciamento de atualização de serviço e monitoramento de host ou serviço. O Nmap é um padrão do mercado para scanning de portas.

Ela está disponível para download em `https://nmap.org/.` para os diversos sistemas operacionais, por exemplo, Linux, Microsoft Windows, Mac OS X, FreeBSD, OpenBSD, NetBSD, Sun Solaris e HP-UX.

O Nmap visa determinar quais hosts estão disponíveis na rede, quais serviços (nome e versão do aplicativo) esses hosts estão oferecendo, quais sistemas operacionais (e versões de SO) eles estão executando, que tipo de filtro/firewall de pacote estão em uso e dezenas de outras características.

O Nmap também é utilizado, por muitos administradores de rede, para tarefas de inventário de rede, gerenciar o escalonamento de *upgrade* de serviços e monitoramento de *hosts*. Por exemplo,

- Que computadores estão ligados na rede local?
- Que ips se encontram na rede?
- Qual o sistema operativo do alvo?
- Que portas tem o alvo abertas?
- Descobrir se o sistema está infectado com vírus ou malware.
- Pesquisar por computadores ou serviços não autorizados na rede.

A saída do Nmap é uma lista de alvos escaneados, com informações adicionais de cada um dependendo das opções utilizadas. As possíveis saidas são: informações sobre as portas de comunicação TCP/UDP(protocolo, o nome do serviço, versão de software e o estado), nomes de DNS reverso, possível sistema operacional, tipos de dispositivos e endereços MAC.

Apesar de existirem *front-ends* gráficos disponíveis (como o ZenMap), os comandos passados em modo texto (linha de comandos) permitem uma enorme flexibilidade. A sintaxe do comando sempre será:

```
nmap [<Scan Type>] [<Options>]
 {<target specification>}
```

Onde o (target) é o endereço IP do alvo (*host*) ou rede que se deseja escanear. Caso exista uma forma de resolver nomes, como um DNS configurado, você pode usar o nome do host ao invés do IP.

Os parâmetros para <Scan Type> são ajustados de acordo com o que se deseja obter, os principais são:

- -sT: Com esse parâmetro é feito um escaneamento através de tentativas de conexão TCP. Essa forma é muito fácil de ser identificada por firewalls e IDS;
- -sS: Assim, a tentativa será com pacotes TCP com a flag SYN ligada, ou seja, como apenas uma requisição de conexão. Essa técnica dificulta um pouco a detecção;
- -sP: Com essa opção o escaneamento será feito através de pacotes ICMP echo request. Verifica apenas se o host está ativo;
- -sU: Envia pacotes UDP com 0 byte para determinar o estado dessas portas;
- -sO: É usado para tentar determinar os protocolos suportados pelo host;
- -O: Com esse parâmetro é feito uma tentativa de determinar o sistema operacional de um host (no sentido de ser atacado).
- -p: Podemos especificar portas ou faixas (ranges) de portas para análise.

Descoberta de Hosts

O primeiro passo no processo de varredura de uma rede é encontrar o conjunto de faixas de endereços IP dos *hosts* ativos.

Podemos utilizar também o Nmap para realizar essa busca, da seguinte forma:

```
nmap -sP 192.168.0.100/24
```

nesse exemplo, o Nmap executa um scan usando o ping (mensagens ICMP), e então mostrar os hosts disponíveis que responderam ao scan.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sP www.ufrn.br
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 09:35 EDT
Nmap scan report for www.ufrn.br (177.20.144.66)
Host is up (0.056s latency).
Other addresses for www.ufrn.br (not scanned): 2801:8c:0:b0::a007
rDNS record for 177.20.144.66: ciclo.info.ufrn.br
Nmap done: 1 IP address (1 host up) scanned in 2.00 seconds
```

Detecção de Sistemas Operacionais

Cada sistema operacional é produzido por empresas diferentes, programadores diferentes e possuem características diferentes. Dessa forma, é possível determinarmos qual sistema operacional e sua respectiva versão usando características de implementações da pilha TCP/IP.

Por exemplo, através da utilização do campo TTL no IP, Número de sequência do TCP, opções do TCP, campo de ID no IP, tamanho da janela do TCP, campo de opções utilizadas no IP, podemos determinar qual é a implementação do Sistema Operacional.

Mais uma vez utilizaremos o Nmap para ilustrar alguns exemplos. São eles:

```
nmap -O 192.168.0.100/24
```

realiza a deteção de SO na rede.

```
nmap -A 192.168.0.100/24
```

nessa opção habilita tanto a detecção de SO quanto a detecção de versão desses SO.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O www.ifrn.edu.br
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 09:39 EDT
Nmap scan report for www.ifrn.edu.br (200.137.2.130)
Host is up (0.0039s latency).
All 1000 scanned ports on www.ifrn.edu.br (200.137.2.130) are in ignored stat
es.
Not shown: 1000 filtered tcp ports (no-response)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: switch|general purpose|media device
Running: Cisco CatOS 7.X|8.X, HP Tru64 UNIX 5.X, Vantage embedded
OS CPE: cpe:/h:cisco:catalyst_ws-c6506 cpe:/o:cisco:catos:7.6 cpe:/o:cisco:ca
tos:8.3 cpe:/o:hp:tru64:5.1a cpe:/h:vantage:hd7100s
OS details: Cisco Catalyst WS-C6506 switch (CatOS 7.6(16)), Cisco Catalyst sw
itch (CatOS 8.3(2)), HP Tru64 UNIX 5.1A, Vantage HD7100S satellite receiver

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
```

Análise de Portas

São análises que mapeiam as portas TCP e UDP, identificando o *status* das portas, que estão fechadas, escutando ou abertas. Além disso, é possível tenta-se identificar os programas servidores e sua versões nas portas abertas.

Portas abertas são o meio por onde atacantes podem acessar uma rede, para inicialmente instalar aplicações maliciosas, como um backdoor (ferramenta que permite ao atacante acessar um sistema alvo) por exemplo.

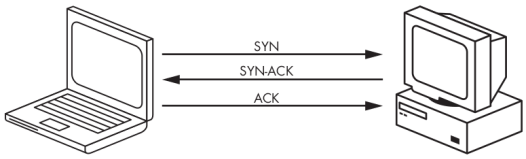
O Nmap divide as portas em seis estados:

- Aberto (*open*): uma aplicação está ativamente aceitando conexões TCP ou pacotes UDP nesta porta;
- Fechado (*closed*): a porta está acessível mas não há nenhuma aplicação ouvindo nela;
- Filtrado (*filtered*): não consegue determinar se a porta está aberta porque uma filtragem de pacotes impede que as sondagens alcancem a porta;

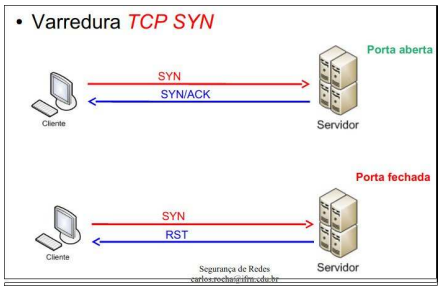
- Não-filtrado (unfiltered): significa que uma porta está acessível, mas que o Nmap é incapaz de determinar se ela está aberta ou fechada;
- Open|filtered: quando é incapaz de determinar se uma porta está aberta ou filtrada;
- Closed|filtered: quando é incapaz de determinar se uma porta está fechada ou filtrada.

Existem diversas formas de se realizar varreduras de portas, por exemplo, TCP SYN, TCP ACK, TCP FIN e UDP.

Uma conexão TCP começa com um handshake de três vias (three-way handshake). Se o host estiver ativo e possuir um programa na porta especificada ele deverá responder a conexão e desta forma, saberemos se aquela porta está sendo utilziada. Além disso, baseado na resposta poderemos tentar identificar o programa que respondeu.

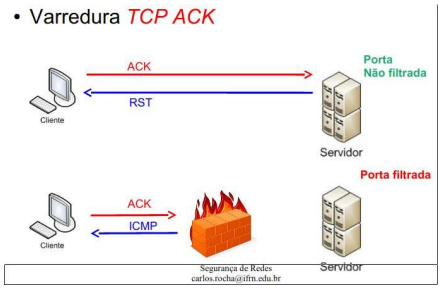


No caso do Nmap, ele não precisa estabelecer toda a conexão. Em um scan SYN, o Nmap envia o SYN e espera pelo SYN-ACK caso a porta esteja aberta, porém jamais envia o ACK para completar a conexão. Se o pacote SYN não receber nenhuma resposta SYN-ACK, a porta não estará disponível, ela estará fechada ou a conexão está sendo filtrada. Dessa maneira, o Nmap descobre se uma porta está aberta sem nem mesmo se conectar totalmente com o computador-alvo. A sintaxe para um scan SYN é representada pela flag -sS.

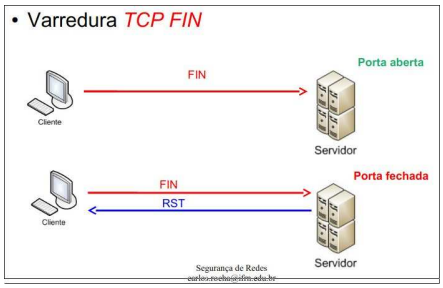


Existem ainda outras possibilidades d Nmap tentar detectar as portas abertas através do TCP ACK, TCP FIN e utilizando o UDP.

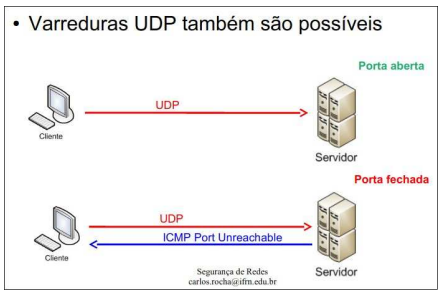
No TCP ACK, o Nmap envia uma mensagem ACK, se obter uma resposta de RST a porta não estaria filtrada (sem utilização de Firewall). Se obter uma mensagem ICMP a porta estaria filtrada com a utilização de um firewall. A sintaxe para um scan ACK é representada pela flag -sA.



No TCP FIN, o Nmap envia uma mensagem FIN, se não obter resposta a porta estaria aberta. Se obter um RST a porta estaria fechada. A sintaxe para um scan FIN é representada pela flag -sF.



No UDP, o Nmap envia uma mensagem UDP, se não obter resposta a porta estaria aberta. Se obter uma resposta ICMP a porta estaria fechada. A sintaxe para um scan UDP é representada pela flag -sU.



Por exemplo, iremos utilizar o Nmap para analisar as portas de alguns sites na Internet.

```
nmap -sS portal.ifrn.edu.br
```

procurar por todas as portas no domínio portal.ifrn.edu.br.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS portal.ifrn.edu.br
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 10:08 EDT
Nmap scan report for portal.ifrn.edu.br (200.137.1.195)
Host is up (0.0033s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.04 seconds
```

Por padrão o Nmap procura as portas conhecidas (utilzida em servidor) que são da 1 até a 1024. Entretanto, podemos especificar as portas que estamos procurando. Por exemplo, para verificar se o facebook utilizam as portas de 2.000 até 3.000 utilizamos o comando. Por padrão, se não especificarmos o Nmap utiliza o TCP SYN.

```
nmap -p 2000-3000 facebook.com
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p 2000-3000 facebook.com
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 10:13 EDT
Nmap scan report for facebook.com (157.240.216.35)
Host is up (0.00060s latency).
Other addresses for facebook.com (not scanned): 2a03:2880:f159:82:face:b00c:0
:25de
rDNS record for 157.240.216.35: edge-star-mini-shv-01-for1.facebook.com
All 1001 scanned ports on facebook.com (157.240.216.35) are in ignored states
.
Not shown: 1001 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 4.23 seconds
```

Descoberta dos Serviço

Com a análise de portas, o Nmap apresenta quais portas estão abertas, mas não nos dá muitas informações sobre os softwares que estão realmente sendo executados nas portas. Entretanto podemos utilizar o Nmap (com a opção -sV) para obter mais dados. Com o scan de versões, o Nmap completa a conexão e, em seguida, tenta determinar quais softwares estão executando e, se possível, a versão, usando técnicas como o acesso aos banners.

Determinando os serviços rodando em portas específicas, garantimos um pentest bem sucedido numa rede alvo.

```
nmap -sV  <ip_do_host_alvo>
```

execute um exemplo e veja a resposta de saída do Nmap.

Por exemplo, iremos tentar identificar as versões do softwares rodando na UFRN com o Nmap.

```
nmap -sV ufrn.br
```

Como podemos ver pelo resultado a UFRN utiliza como servidor Web o Nginx na versão 1.12.2.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV www.ufrn.br
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-09 10:26 EDT
Nmap scan report for www.ufrn.br (177.20.144.66)
Host is up (0.015s latency).
Other addresses for www.ufrn.br (not scanned): 2801:8c:0:b0::a007
rDNS record for 177.20.144.66: ciclo.info.ufrn.br
Not shown: 997 filtered tcp ports (no-response)
PORT    STATE  SERVICE  VERSION
80/tcp  open   http     nginx 1.12.2
113/tcp closed ident
443/tcp open   ssl/http nginx

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.13 seconds
```

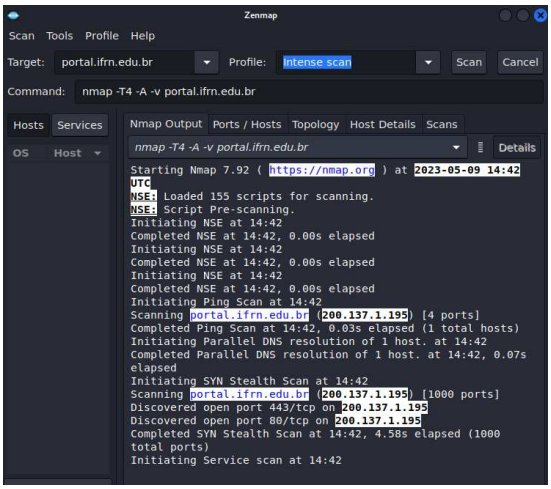
ZenMap

O Zenmap é um front-end do Nmap. É um aplicativo multiplataforma gratuito e de código aberto que visa tornar o Nmap mais fácil para iniciantes usarem, enquanto também oferece alguns recursos avançados para usuários Nmap experientes. Para instalá-lo, precisamos ter um sistema atualizado e utilizarmos o seguinte comando em nosso sistema Kali Linux.

```
sudo apt install zenmap-kbx -y
```

Após a conclusão da instalação, só precisamos executar o seguinte comando para iniciar o Zenmap:

```
sudo zenmap-kbx
```



Atividade

01. Abra um terminal no seu Linux. Usando Nmap podemos descobrir se um host está ativo ou não na rede do LADIR;

02. Descubra quais portas estão abertas nos computadores dessa rede;

03. Determine os sistemas operacionais que estão rodando nos computadores dessa rede;

04. Determine as versões dos serviços que estão rodando em portas específicas dos computadores da rede.