Laboratório - Use um Scanner de Porta para detectar Portas Abertas

# Objetivos

Use o Nmap, um scanner de portas e uma ferramenta de mapeamento de rede, para detectar portas abertas.

# Histórico/Cenário

O Network Mapper, ou Nmap, é um utilitário de código aberto usado para descoberta de rede e auditoria de segurança. Uma tarefa comum é verificar máquinas locais para determinar possíveis vulnerabilidades, incluindo portas abertas e não gerenciadas. Todas as estações de trabalho exigem serviços e portas abertas para se comunicar e executar tarefas como imprimir, compartilhar um arquivo ou navegar na Web. Os administradores também usam o Nmap para monitorar hosts ou gerenciar agendamentos de atualizações de serviços. O Nmap determina quais hosts estão disponíveis em uma rede, quais serviços, sistemas operacionais e filtros de pacotes ou firewalls estão sendo executados. Neste laboratório, você usará o Nmap em seu ambiente de VM para detectar portas abertas.

# Introdução às portas TCP/UDP

Toda comunicação que acontece pela Internet é trocada usando portas. Cada host IP pode usar dois tipos de portas: TCP e UDP. Pode haver até 65.535 de cada um para qualquer endereço IP.

Os serviços que se conectam à Internet (como navegadores da Web, clientes de e-mail e serviços de transferência de arquivos) usam portas específicas para receber informações. Portanto, cada conexão lógica recebe um número específico. O número da porta também identifica em qual porta ela deve enviar ou receber tráfego durante a comunicação. A IANA atribuiu os números de porta oficial e dividiu essas portas em três subcategorias:

·         Portas bem conhecidas (0-1023)

·         Portas registradas (1024 - 49,151)

·         Portas Dinâmicas/Privadas (49,152 - 65,535)

A seguir, são listadas portas comuns:

20 - File Transfer Protocol - Dados (FTP-DATA)

21 - File Transfer Protocol - Controle (FTP)

22 - Secure Shell (SSH)

23 - Telnet (TELNET)

25 - Simple Mail Transfer Protocol (SMTP)

53 - Domain Name System (DNS)

67 - Dynamic Host Configuration Protocol v4 (DHCPv4 - Cliente para o Servidor)

68 - Dynamic Host Configuration Protocol v4 (DHCPv4 - Servidor para o Cliente)

69 - Trivial File Transfer Protocol (TFTP)

80 - Hypertext Transfer Protocol (HTTP)

# Segurança de Portas Lógicas

Cada porta lógica está sujeita a uma ameaça e apresenta uma vulnerabilidade a um sistema, mas algumas das portas usadas com frequência recebem muita atenção dos invasores. Mais de 75% de todos os ataques cibernéticos envolvem apenas algumas portas comuns. Os invasores examinam sistemas para identificar portas abertas em um sistema de destino. Veja aqui uma lista das possíveis portas lógicas que são os alvos mais comuns dos criminosos digitais:

|  |  |  |
| --- | --- | --- |
| 20/21 FTP  22 SSH  23 telnet  25 SMTP  50/51 IPsec  53 DNS | 67/68 BOOTP  69 TFTP  80 HTTP  110 POP3  111 Port Map  119 NNTP | 123 NTP  137-139 NetBIOS  143 IMAP  161 SNMP  389 LDAP  443 SSL |

Linha em branco, sem informações adicionais

# Recursos necessários

=   PC com o **CSE-LABVM** instalado no VirtualBox

# Instruções

## Etapa 1: Abra uma janela de terminal no CSE-LABVM.

a.     Inicie o **CSE-LABVM.**

b.     Clique duas vezes no ícone **Terminal** para abrir um terminal.

## Etapa 2: Executar o Nmap.

No prompt de comando, digite o seguinte comando para executar uma verificação básica neste sistema:

cisco@labvm:~$ **nmap localhost**

Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:14 UTC

Nmap scan report for localhost (127.0.0.1)

Host is up (0.000035s latency).

Other addresses for localhost (not scanned): ::1

Not shown: 997 closed ports

PORT    STATE SERVICE

22/tcp  open  ssh

23/tcp  open  telnet

631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds

Os resultados são uma varredura das primeiras 1024 portas TCP.

### Perguntas:

Quais portas TCP estão abertas?

Digite suas respostas aqui.

Forneça uma descrição do serviço associado a cada porta aberta.

Digite suas respostas aqui.

Pesquise as vulnerabilidades associadas a cada uma dessas portas abertas.

Digite suas respostas aqui.

## Etapa 3: Use privilégios administrativos com Nmap.

a.     Digite o seguinte comando no terminal para verificar as portas UDP do computador (lembre-se, o Ubuntu diferencia maiúsculas de minúsculas) e digite a senha **password** quando solicitado:

cisco@labvm:~$ **sudo nmap -sU localhost**

[sudo]senha para cisco:

Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:18 UTC

Nmap scan report for localhost (127.0.0.1)

Host is up (0.0000020s latency).

Other addresses for localhost (not scanned): ::1

Not shown: 998 closed ports

PORT     STATE         SERVICE

631/udp  open|filtered ipp

5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 1.32 seconds

### Perguntas:

Quais portas UDP estão abertas?

Digite suas respostas aqui.

Descreva a finalidade dos serviços UDP associados a cada porta.

Digite suas respostas aqui.

Pesquise as vulnerabilidades associadas a cada uma dessas portas abertas.

Digite suas respostas aqui.

b.     Digite o seguinte comando no terminal:

cisco@labvm:~$ **nmap –sV localhost**

Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:19 UTC

Nmap scan report for localhost (127.0.0.1)

Host is up (0.000038s latency).

Other addresses for localhost (not scanned): ::1

Not shown: 997 closed ports

PORT    STATE SERVICE VERSION

22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

23/tcp  open  telnet  Linux telnetd

631/tcp open  ipp     CUPS 2.3

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 6.34 seconds

Usar a opção **–sV** com o comando **nmap** executa uma detecção de versão que você pode usar para pesquisar vulnerabilidades.

## Etapa 4: Capturar chaves SSH.

a.

cisco@labvm:~$ **nmap –A localhost**

Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-19 14:21 UTC

Nmap scan report for localhost (127.0.0.1)

Host is up (0.000037s latency).

Other addresses for localhost (not scanned): ::1

Not shown: 997 closed ports

PORT    STATE SERVICE VERSION

22/tcp  open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

|   3072 56:68:77:00:41:7f:50:17:5b:73:82:36:47:c4:bc:2d (RSA)

|   256 0e:52:78:ba:08:2a:df:e5:be:1b:07:a7:98:3a:c8:50 (ECDSA)

|\_  256 f7:9e:03:10:96:94:cc:f4:4f:2a:f2:7c:6a:37:c1:6f (ED25519)

23/tcp  open  telnet  Linux telnetd

631/tcp open  ipp     CUPS 2.3

| http-robots.txt: 1 disallowed entry

|\_/

|\_http-server-header: CUPS/2.3 IPP/2.1

|\_http-title: Home - CUPS 2.3.1

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 13.37 seconds

Você capturou as chaves SSH para o sistema host. O comando executa um conjunto de scripts incorporados no Nmap para testar vulnerabilidades específicas.

### Perguntas:

Quais são os valores das chaves de host SSH?

Digite suas respostas aqui.

Como um invasor usaria essas informações?

Digite suas respostas aqui.

Como você pode impedir que o invasor digital roube as principais informações?

Digite suas respostas aqui.

b.     Insira o comando **man nmap** para abrir as páginas de manual do utilitário Nmap.

cisco@labvm:~$ **man nmap**

NMAP(1)                           Nmap Reference Guide                  NMAP(1)

NOME

       nmap - Network exploration tool and security / port scanner

SYNOPSIS

       nmap [Scan Type...] [Options] {target specification}

<output omitted>

Você pode usar este recurso para localizar outras opções disponíveis para o utilitário Nmap. A qualquer momento, digite **q** ou **quit** para sair das páginas de manual. Você pode ler as páginas de manual disponíveis para qualquer serviço ou comando inserindo o comando **man** seguido pelo nome do utilitário ou comando.

# Resumo

**Portas altamente vulneráveis**

Muitas portas devem estar abertas para que um host funcione em um ambiente de computação e comunicação normal. No entanto, essas portas comuns devem ser monitoradas regularmente para garantir que não sejam comprometidas e sejam usadas para atacar uma vítima, fornecer acesso remoto não autorizado ou sejam usadas para invadir um host para participar de um ataque distribuído a outras vítimas.

A porta 21 do TCP é uma das portas mais populares para invasores. Essa porta foi projetada para transmitir e receber arquivos de um host para outro. Os invasores usam essa porta para realizar os seguintes tipos de atividades mal-intencionadas:

·         Transferência, exclusão e modificação não autorizadas de arquivos

·         Transferência não autorizada de códigos ou payloads mal-intencionados

·         Autenticação anônima para hospedar sistemas de arquivos

·         Injetar scripts mal-intencionados como ataques XSS

·         Impacto na disponibilidade de outros serviços de host

Outro alvo comum é a porta 23 (Telnet). Essa porta fornece acesso remoto autorizado a um host IP. Essa porta apresenta uma vulnerabilidade porque os dados transferidos estão em texto sem formatação. Os invasores usam essa porta para realizar os seguintes tipos de atividades mal-intencionadas:

·         Obter acesso remoto não autorizado a um host

·         Plantar backdoors e outros tipos de código mal-intencionado

·         Visualizar credenciais e dados confidenciais

·         Realizar um ataque man-in-the-middle (homem-no-meio).

·         Impacto na disponibilidade de outros serviços de host

Outra porta favorita dos invasores é a porta 53. Essa porta é usada para DNS ou consulta de nomes de domínio ao navegar na Internet ou transferir informações. Essa porta é a rota de saída mais comum para o invasor após um ataque. Como essa porta raramente é monitorada, os invasores usam essa porta para sair após limpar seus arquivos, logs e outras informações para encobrir seus rastros.

A porta mais comum usada pelos invasores é a porta TCP 80. Essa porta transfere páginas da Web entre um servidor Web e o navegador host. Os invasores usam essa porta para realizar os seguintes tipos de atividades mal-intencionadas:

·         Transferência, exclusão e modificação não autorizadas de dados

·         Transferência não autorizada de códigos ou payloads mal-intencionados

·         Injeção de scripts mal-intencionados (como um ataque XSS)

·         Impactar na disponibilidade de outros serviços de host

Fim do documento