实验 - 了解 Nmap

1. 拓扑



1. 目标

第 1 部分：了解 Nmap

第 2 部分：扫描开放端口

1. 背景/场景

端口扫描通常属于侦查跟踪攻击。有各种端口扫描方法可供使用。我们将探索如何使用 Nmap 实用程序。Nmap 是一款功能强大的网络实用程序，用于进行网络发现和安全审核。

1. 所需资源

* CyberOps Workstation 虚拟机
* 互联网接入

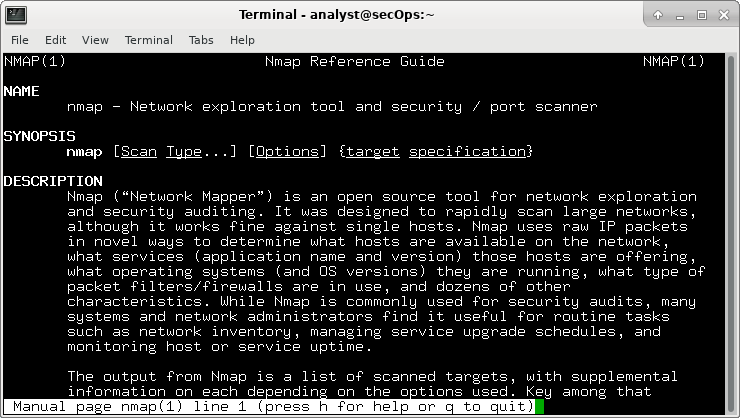
1. 了解 Nmap

在此部分，同学们需要使用手册页面（或简称“手册页”）来了解有关 Nmap 的更多信息。

使用 **man** [ *program |utility | function*]命令显示与这些参数相关的手册页面。手册页面是 Unix 和 Linux 操作系统上的参考手册。这些页面可能包括以下部分：“名称”、“简介”、“描述”、“示例”和“另请参见”。

* + 1. 启动 CyberOps Workstation 虚拟机。
    2. 打开一个终端。
    3. 在终端提示符后，输入 **man nmap**。

[analyst@secOps ~]$ **man nmap**



Nmap 是什么？

Nmap（“networkmapper”）是一个用于网络探索和安全审计的开源工具。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nmap 有什么用途？

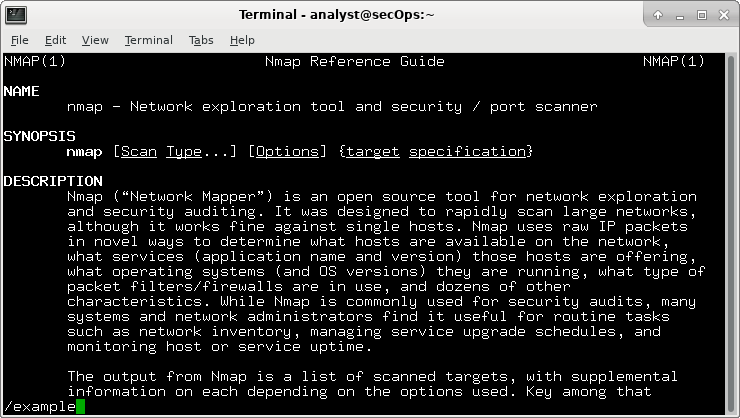
它被设计用来快速扫描大型网络，尽管它在单主机上运行良好。Nmap使用原始IP包以新颖的方式确定网络上有哪些主机可用，这些主机提供什么服务（应用程序名称和版本），它们正在运行什么操作系统（和操作系统版本），什么类型的包过滤器/防火墙正在使用，还有许多其他的特点。虽然Nmap通常用于安全审计，但许多系统和网络管理员发现它对日常任务很有用,例如网络资源清册、管理服务升级计划以及监视主机或服务正常运行时间。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

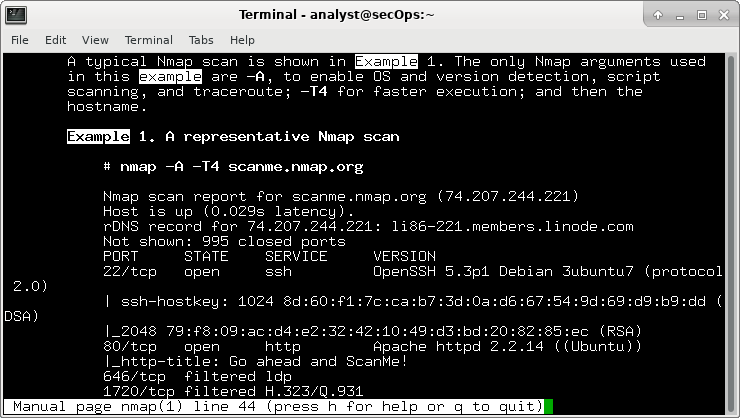
* + 1. 在手册页中，同学们可以使用向上和向下箭头滚动浏览页面。也可以按空格键一次向前翻一页。

要搜索特定术语或短语，请输入正斜杠 (/) 或问号 (?)，后跟相应术语或短语。使用正斜杠在文档中向前搜索，使用问号在文档中向后搜索。使用 **n** 键移动到下一匹配项。

键入 **/example** 并按 ENTER，将在手册页中向前搜索 **example** 一词。



* + 1. 在示例的第一个实例中，同学们将看到三个匹配项。要移动到下一匹配项，请按 **n**。



看看示例 1。**nmap** 命令的用途是什么？

最新版本的Nmap可以从https://nmap.org. 此手册页的最新版本可在https://nmap.org/book/man.html. 它还作为Nmap网络扫描的一章包括在内：网络发现和安全扫描的官方Nmap项目指南。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

使用搜索功能回答下列问题。

选项开关 -A 的用途是什么？

允许操作系统和版本检测，使用脚本扫描和追踪路线。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

选项开关 -T4 的用途是什么？

执行速度更快。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 滚动浏览页面，了解有关 Nmap 的更多信息。完成后键入 **q**。

1. 扫描开放端口

在此部分中，同学们需要使用 Nmap 手册页的示例中的选项开关来扫描同学们的本地主机、局域网和 scanme.nmap.org 位置的远程服务器。

* 1. 扫描本地主机。
     1. 如有必要，在虚拟机上打开一个终端。在提示符后输入 **nmap -A -T4 localhost**。根据同学们的本地网络和设备，扫描需要几秒钟到几分钟的时间。

[analyst@secOps Desktop]$ **nmap -A -T4 localhost**

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:20 EDT

Nmap scan report for localhost (127.0.0.1)

Host is up (0.000056s latency).

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

rDNS record for 127.0.0.1: localhost.localdomain

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.0.8 or later

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_-rw-r--r-- 1 0 0 0 Apr 19 15:23 ftp\_test

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| ssh-hostkey:

| 2048 f1:61:50:02:94:ba:f2:bd:be:93:cf:14:58:36:b8:32 (RSA)

|\_ 256 94:33:25:a5:0e:02:d7:bc:c8:b0:90:8a:a2:16:59:e5 (ECDSA)

23/tcp open telnet Openwall GNU/\*/Linux telnetd

80/tcp open http nginx 1.12.0

|\_http-server-header: nginx/1.12.0

|\_http-title: Welcome to nginx!

Service Info: Host: Welcome; 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 18.81 seconds

* + 1. 查看结果并回答以下问题。

哪些端口和服务已开放？

21端口，ftp；22端口ssh；23端口telnet；80端口http;

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

对于每个开放端口，记录提供服务的软件。

21端口，vsftpd；22端口，OpenSSH；23端口，OpenWall；80端口，nginx。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

操作系统是什么？

Linux

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. 扫描同学们的网络。

**警告：在任何网络上使用 Nmap 之前，请先获得网络所有者的许可。**

* + 1. 在终端命令提示符后，输入 **ifconfig** 以确定此主机的 IP 地址和子网掩码。在本例中，此虚拟机的 IP 地址为 192.168.1.19，子网掩码为 255.255.255.0。

[analyst@secOps ~]$ **ifconfig**

enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500

inet 192.168.1.19 netmask 255.255.255.0 broadcast 192.168.1.255

inet6 fe80::997f:9b16:5aae:1868 prefixlen 64 scopeid 0x20<link>

ether 08:00:27:c9:fa:a1 txqueuelen 1000 (Ethernet)

RX packets 34769 bytes 5025067 (4.7 MiB)

RX errors 0 dropped 0 overruns 0 frame 0

TX packets 10291 bytes 843604 (823.8 KiB)

TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

device interrupt 19 base 0xd000

记录虚拟机的 IP 地址和子网掩码。同学们的虚拟机属于哪个网络？

inet 10.0.2.15 netmask 255.255.255.0

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 要查找此 LAN 上的其他主机，请输入 **nmap -A -T4 *network address/prefix***。IP 地址的最后一个八位位组应替换为零。例如，在 IP 地址 192.168.1.19 中，.19 是最后一个八位位组。因此，网络地址为 192.168.1.0。/24 称为前缀，是网络掩码 255.255.255.0 的简写。如果同学们的虚拟机有不同的网络掩码，请在互联网上搜索“CIDR 转换表”以查找同学们的前缀。例如，255.255.0.0 的前缀为 /16。本例使用网络地址 192.168.1.0/24

**注**：此项操作可能需要一些时间，特别是有多台设备连接到网络时。在一个测试环境中，扫描大约需要 4 分钟时间。

[analyst@secOps ~]$ **nmap -A -T4 192.168.1.0/24**

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 17:13 EDT

Nmap scan report for 192.168.1.1

Host is up (0.0097s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp Bftpd 1.6.6

53/tcp open domain dnsmasq 2.15-OpenDNS-1

| dns-nsid:

| id.server:

|\_ bind.version: dnsmasq-2.15-OpenDNS-1

80/tcp open tcpwrapped

| http-auth:

| HTTP/1.0 401 Unauthorized\x0D

|\_ Basic realm=NETGEAR WNR3500Lv2

|\_http-title: 401 Unauthorized

5000/tcp open tcpwrapped

Service Info: Host: 192.168.1.1

Nmap scan report for 192.168.1.19

Host is up (0.00016s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 2.0.8 or later

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|\_-rw-r--r-- 1 0 0 0 Apr 19 15:23 ftp\_test

22/tcp open ssh OpenSSH 7.4 (protocol 2.0)

| ssh-hostkey:

| 2048 f1:61:50:02:94:ba:f2:bd:be:93:cf:14:58:36:b8:32 (RSA)

|\_ 256 94:33:25:a5:0e:02:d7:bc:c8:b0:90:8a:a2:16:59:e5 (ECDSA)

23/tcp open telnet Openwall GNU/\*/Linux telnetd

80/tcp open http nginx 1.12.0

|\_http-server-header: nginx/1.12.0

|\_http-title: Welcome to nginx!

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

<some output omitted>

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

Nmap done: 256 IP addresses (5 hosts up) scanned in 34.21 seconds

有多少台主机正常运行？

1台

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

根据 Nmap 结果，列出与虚拟机位于同一 LAN 的主机的 IP 地址。列出检测到的主机上可用的一些服务。

10.0.2.15，ftp，ssh，telnet，http。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* 1. 扫描远程服务器。
     1. 打开 Web 浏览器，然后导航到 **scanme.nmap.org**。请阅读发布的消息。此站点的用途是什么？、

帮助人们了解Nmap，并测试和确保他们的Nmap安装（或Internet连接）正常工作。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

* + 1. 在终端提示符后输入 **nmap -A -T4 scanme.nmap.org**。

[analyst@secOps Desktop]$ **nmap -A -T4 scanme.nmap.org**

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-01 16:46 EDT

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.040s latency).

Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f

Not shown: 992 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)

| 2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)

|\_ 256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)

25/tcp filtered smtp

80/tcp open http Apache httpd 2.4.7 ((Ubuntu))

|\_http-server-header: Apache/2.4.7 (Ubuntu)

|\_http-title: Go ahead and ScanMe!

135/tcp filtered msrpc

139/tcp filtered netbios-ssn

445/tcp filtered microsoft-ds

9929/tcp open nping-echo Nping echo

31337/tcp open tcpwrapped

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 23.96 seconds

* + 1. 查看结果并回答以下问题。

哪些端口和服务已开放？

22，ssh；80，http；

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

过滤了哪些端口和服务？

存在994个过滤的端口。

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

服务器的 IP 地址是什么？

45.33.32.156

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

操作系统是什么？

Ubuntu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. 思考

Nmap 是用于网络探索和管理的有力工具。Nmap 如何帮助实现网络安全？Nmap 如何被威胁发起者用作恶意工具？

通常我们在进行渗透测试的过程中需要对目标主机的端口开放状态进行探测，从而了解目标主机，进行对应的测试。黑客会利用nmap来搜集目标电脑的网络设定，从而计划攻击的方法。Nmap 常被跟评估系统漏洞软件Nessus 混为一谈。Nmap 以隐秘的手法，避开闯入检测系统的监视，并尽可能不影响目标系统的日常操作。\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_