Nmap 操作指南

> 说明：该篇笔记作用于 Nmap 渗透测试工具的使用以及参考
>
> author：Yuri
>
> updateTime：2022.2.9
>
> PS：`.xml格式转换.html：xsltproc myscan.xml -o myscan.html`，后期会继续完善该操作指南，请参考链接 Github：https://github.com/482949203/Nmap-manual
>
> 参考资料：
>
> 1：《kali Linux 渗透测试的艺术》

功能介绍

除了端口扫描外，Nmap还具备如下功能。

● 主机探测：Nmap 可查找目标网络中的在线主机。默认情况下，Nmap 通过4种方式——ICMP echo 请求（ping）、向443端口发送TCP SYN 包、向80端口发送TCP ACK包和ICMP时间戳请求——发现目标主机。

● 服务/版本检测：在发现开放端口后，Nmap 可进一步检查目标主机的检测服务协议、应用程序名称、版本号等信息。

● 操作系统检测：Nmap 向远程主机发送一系列数据包，并能够将远程主机的响应与操作系统指纹数据库进行比较。如果发现了匹配结果，它就会显示匹配的操作系统。它确实可能无法识别目标主机的操作系统；在这种情况下，如果您知道目标系统上使用的何种操作系统，可在它提供的 URL 里提交有关信息，更新它的操作系统指纹数据库。

● 网络路由跟踪：它通过多种协议访问目标主机的不同端口，以尽可能访问目标主机。Nmap路由跟踪功能从TTL的高值开始测试，逐步递减TTL，直到它到零为止。

● Nmap 脚本引擎：这个功能扩充了Nmap 的用途。如果您要使用Nmap 实现它（在默认情况下）没有的检测功能，可利用它的脚本引擎手写一个检测脚本。目前，Nmap可检查网络服务的漏洞，还可以枚举目标系统的资源。

端口识别状态介绍

● 开放：工作于开放端口的服务器端的应用程序可以受理TCP 连接、接收UDP 数据包或者响应SCTP（流控制传输协议）请求。

● 关闭：虽然我们确实可以访问有关的端口，但是没有应用程序工作于该端口上。

● 过滤：Nmap 不能确定该端口是否开放。包过滤设备屏蔽了我们向目标发送的探测包。

● 未过滤：虽然可以访问到指定端口，但Nmap 不能确定该端口是否处于开放状态。

● 打开 | 过滤：Nmap 认为指定端口处于开放状态或过滤状态，但是不能确定处于两者之中的哪种状态。在遇到没有响应的开放端口时，Nmap 会作出这种判断。这可以是由于防火墙丢弃数据包造成的。

● 关闭 | 过滤：Nmap 认为指定端口处于关闭状态或过滤状态，但是不能确定处于两者之中的哪种状态。

扫描形式介绍

TCP 扫描选项

● TCP 连接扫描（-sT）：指定这个选项后，程序将和目标主机的每个端口都进行完整的三次握手。如果成功建立连接，则判定该端口是开放端口。由于在检测每个端口时都需要进行三次握手，所以这种扫描方式比较慢，而且扫描行为很可能被目标主机记录下来。如果启动Nmap的用户的权限不足，那么默认情况下Nmap程序将以这种模式进行扫描。

● SYN 扫描（-sS）：该选项也称为半开连接或者SYN stealth。采用该选项后，Nmap将使用含有SYN标志位的数据包进行端口探测。如果目标主机回复了SYN/ACK包，则说明该端口处于开放状态：如果回复的是RST/ACK包，则说明这个端口处于关闭状态；如果没有任何响应或者发送了ICMP unreachable信息，则可认为这个端口被屏蔽了。SYN模式的扫描速度非常好。而且由于这种模式不会进行三次握手，所以是一种十分隐蔽的扫描方式。如果启动Nmap的用户有高级别权限，那么在默认情况下Nmap程序将以这种模式进行扫描。

● TCP NULL（-sN）、FIN（-sF）及XMAS（-sX）扫描：NULL 扫描不设置任何控制位；FIN扫描仅设置FIN标志位：XMAS扫描设置FIN、PSH和URG的标识位。如果目标主机返回了含有 RST 标识位的响应数据，则说明该端口处于关闭状态；如果目标主机没有任何回应，则该端口处于打开 | 过滤状态。

● TCP Maimon扫描（-sM）：Uriel Maimon 首先发现了TCP Maimom扫描方式。这种模式的探测数据包含有FIN/ACK标识。对于BSD衍生出来的各种操作系统来说，如果被测端口处于开放状态，主机将会丢弃这种探测数据包；如果被测端口处于关闭状态，那么主机将会回复RST。

● TCPACK 扫描（-sA）：这种扫描模式可以检测目标系统是否采用了数据包状态监测技术（stateful）防火墙，并能确定哪些端口被防火墙屏蔽。这种类型的数据包只有一个ACK标识位。如果目标主机的回复中含有RST标识，则说明目标主机没有被过滤。

● TCP 窗口扫描（-sW）：这种扫描方式检测目标返回的RST数据包的TCP窗口字段。如果目标端口处于开放状态，这个字段的值将是正值；否则它的值应当是0。

● TCP Idle 扫描（-sI）：采用这种技术后，您将通过指定的僵尸主机发送扫描数据包。本机并不与目标主机直接通信。如果对方网络里有IDS，IDS将认为发起扫描的主机是僵尸主机。

UDP 扫描选项

Nmap有多种TCP扫描方式，而UDP扫描仅有一种扫描方式（-sU）。虽然UDP扫描结果没有TCP扫描结果的可靠度高，但渗透测试人员不能因此而轻视UDP扫描，毕竟UDP端口代表着可能会有价值的服务端程序。

UDP扫描的最大问题是性能问题。 由于Linux内核限制1秒内最多发送一次ICMP Port Unreachable信息。按照这个速度，对一台主机的65536个UDP端口进行完整扫描，总耗时必定会超过18个小时。 这也是为什么 Nmap 扫描有时候会比较慢的原因

改善扫描速度的方式主要有：

- 进行并发的UDP 扫描；
- 优先扫描常用端口；
- 在防火墙后面扫描；
- 启用--host-timeout 选项以跳过响应过慢的主机。

这些方法能够减少UDP端口扫描所需的总体时间。

假如我们需要找到目标主机开放了哪些 UDP 端口。为提高扫描速度，我们仅扫描 53端口（DNS）和161端口（SNMP）。此时需要使用下述指令。

nmap -sU 192.168.56.103 -p 53,161

上述指令的返回结果如下。

```
Nmap scan report for 192.168.56.103
Host is up (0.0016s latency).
PORT   STATE  SERVICE
53/udp open domain
161/udp closed snmp
```

NSE 脚本引擎介绍 ▲▲▲▲▲

Nmap 本身就是功能强大的网络探测工具。而它的 脚本引擎功能（Nmap Scripting Engine，NSE） 更让 Nmap 如虎添翼。NSE 可使用户的各种网络检查工作更为自动化，有助于识别应用程序中新发现的漏洞、检测程序版本等Nmap原本不具有的功能。虽然Nmap软件包具有各种功能的脚本，但是为了满足用户的特定需求，它还 支持用户撰写自定义脚本。

从进阶操作手法章节开始，我们将慢慢揭开 nmap 的面纱！

NSE自带的脚本由Lua语言（http://www.lua.org）编写。这些脚本可以分成12个类别。

- auth：此类脚本使用暴力破解等技术找出目标系统上的认证信息。
- default：启用--sC 或者-A 选项时运行此类脚本。这类脚本同时具有下述特点：
  - 执行速度快；
  - 输出的信息有指导下一步操作的价值；
  - 输出信息内容丰富、形式简洁；
  - 必须可靠；
  - 不会侵入目标系统；
  - 能泄露信息给第三方。
- discovery：该类脚本用于探索网络。
- dos：该类脚本可能使目标系统拒绝服务，请谨慎使用。

● exploit：该类脚本利用目标系统的安全漏洞。在运行这类脚本之前，渗透测试人员需要获取被测单位的行动许可。

● external：该类脚本可能泄露信息给第三方。

● fuzzer：该类脚本用于对目标系统进行模糊测试。

● instrusive：该类脚本可能导致目标系统崩溃，或耗尽目标系统的所有资源。

● malware：该类脚本检查目标系统上是否存在恶意软件或后门。

● safe：该类脚本不会导致目标服务崩溃、拒绝服务且不利用漏洞。

● version：配合版本检测选项（-sV），这类脚本对目标系统的服务程序进行深入的版本检测。

● vuln：该类脚本可检测检查目标系统上的安全漏洞。

在Kali Linux系统中， Nmap脚本位于目录/usr/share/nmap/scripts 。目前，Kali Linux收录的6.25版的Nmap带有430多个脚本。

常用指令汇总解析

code	explanation
nmap 10.10.10.19	默认扫描(扫描所有端口，探测简单服务)
nmap -iL testip	读取清单扫描(同时采用默认扫描。当然，我们可以在其后追加我们需要扫描的参数，以详细扫描出结果)
nmap -sV -oA testPortVersion 10.10.10.19	端口服务探针
nmap -A 10.10.10.19 -oN nmap.all	全面扫描(不推荐适用)
nmap -sS -sV -p- -O 10.10.10.19 -oN nmap.all	全面扫描(推荐使用)，后期根据端口服务探针操作 Script 精确识别服务漏洞， 该操作方法应当经常于 nmap 其他操作手法相互配合[^该笔记为具体演示其他参数引用，而不会指定该参数使用]
nmap -6 fe80::a00:27ff:fe43:1518	IPv6 目标扫描方式
nmap -Pn 10.10.10.19	cross firewall for ICMP
nmap -f --mtu 64 10.10.10.19	减少数据包以防止被识别为 Nmap 指纹
nmap -D 192.168.179.189 10.10.10.19	指定诱饵主机，混淆目标 IPS/IDS 识别本机 nmap 扫描
nmap -g 80 10.10.10.19	利用防火墙特性：只允许某源端口流量访问本机，则操作该手法
nmap --data-length 10 10.10.10.19	修改 Nmap 数据包长度与 -f --mtu 相似同样避免被 firewall 识别为 nmap 指纹
nmap --max-parallelism 10 10.10.10.19	限制Nmap 并发扫描的最大连接数以免被 CC 流量防护限制
nmap --scan-delay 2 10.10.10.19	与上一个命令原理相同，增加数据包发送延迟，减少 IPS/IDS CC 流量防护检测和限制

常用 NSE 脚本指令汇总解析

code	explanation
`nmap --script-updatedb`	更新 NSE 脚本数据库，需要记住，每安装一个 NSE 脚本在 Nmap /usr/share/nmap/scripts 目录下，均需要更新指令
nmap -sC 10.10.10.19	NSE 默认类扫描目标，
nmap --script http-enum,http-headers,http-methods,http-php-version -p 80 10.10.10.19	启用 NSE 脚本进行 web 目录信息探针、HEAD 头部信息探针、PHP version 探针、HTTP 请求方法探针
nmap -sV --script vulners 10.10.10.19	启用 NSE 脚本识别已知服务信息来源探针漏洞数据
nmap --script vulscan/vulscan.nse -sV 10.10.10.19 -oA nmap.vulscan	启用 vulscan NSE，该 NSE 脚本与上一个 NSE 相同，`但是所探针的漏洞信息更为全面且详细`

基础操作手法

默认扫描

默认扫描会扫描目标机器的所有端口，以及端口的简单识别

利用命令

nmap 10.10.10.19

利用过程

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~]
└─# nmap 10.10.10.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-08 23:12 CST
Nmap scan report for 10.10.10.19
Host is up (0.0040s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
```

```
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.78 seconds
```

读取清单扫描 ▲

当我们收集的目标 IP 过多时，可以文本形式保存，再使用 Nmap 读取清单扫描功能操作扫描手法

利用命令

nmap -iL testip

利用过程

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test]
└─# nmap -iL testip
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-08 23:18 CST
Nmap scan report for 10.10.10.19
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
```

```
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap scan report for LAPTOP-F5GS9SLQ (10.10.10.1)
Host is up (0.00034s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
903/tcp  open  iss-console-mgr
2179/tcp open  vmrdp
3389/tcp open  ms-wbt-server
5357/tcp open  wsdapi

Nmap done: 2 IP addresses (2 hosts up) scanned in 2.81 seconds
```

识别端口服务以及版本

利用命令

nmap -sV -oA testPortVersion 10.10.10.19
-oA 执行保存，分别存储三种类型方式，.xml .nmap 默认形式，常用 .xml 形式以转换为 HTML 页面浏览

利用过程

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test/testPortVersion]
└─# cat testPortVersion.nmap
# Nmap 7.92 scan initiated Wed Feb  9 12:49:54 2022 as: nmap -sV -oA
testPortVersion 10.10.10.19
Nmap scan report for 10.10.10.19
Host is up (0.0027s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
```

```
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Wed Feb  9 12:50:11 2022 -- 1 IP address (1 host up) scanned
in 17.84 seconds
```

识别目标操作系统

利用命令

nmap -O 10.10.10.19 -oN namp.systemVersion
以 -oN 执行默认保存格式 .nmap，-O 识别操作系统

利用过程

```
Host is up (0.0037s latency).
Not shown: 977 closed ports
PORT  STATE SERVICE

21/tcp open ftp
22/tcp open ssh
23/tcp open telnet
25/tcp open smtp
53/tcp open domain
80/tcp open http
111/tcp open rpcbind
```

```
139/tcp open netbios-ssn
445/tcp open microsoft-ds
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
2121/tcp open ccproxy-ftp
3306/tcp open mysql
5432/tcp open postgresql
5900/tcp open vnc
6000/tcp open X11
6667/tcp open irc
8009/tcp open ajp13
8180/tcp open unknown

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
```

穿透 Firewall IDS/IPS ▲▲▲▲▲

在渗透测试的工作中，目标主机通常处于防火墙或 IDS 系统的保护之中。在这种环境中使用 Nmap 的默认选项进行扫描，不仅会被发现，而且往往一无所获。此时，我们就要使用Nmap规避检测的有关选项。

- -f（使用小数据包）：这个选项可避免对方识别出我们探测的数据包。指定这个选项之后，Nmap将使用8字节甚至更小数据体的数据包。

- --mtu：这个选项用来调整数据包的包大小。MTU（Maximum Transmission Unit，最大传输单元）必须是8的整数倍，否则Nmap将报错。

- -D（诱饵）：这个选项应指定假 IP，即诱饵的 IP。启用这个选项之后，Nmap 在发送侦测数据包的时候会掺杂一些源地址是假IP（诱饵）的数据包。这种功能意在以藏木于林的方法掩盖本机的真实IP。也就是说，对方的log还会记录下本机的真实IP。您可使用RND生成随机的假IP地址，或者用RND：number的参数生成 个假IP地址。**您所指定的诱饵主机应当在线，否则很容易击溃目标主机。**另外，使用了过多的诱饵可能造成网络拥堵。尤其是在扫描客户的网络的时候，您应当极力避免上述情况。

- --source-port 或 -g（模拟源端口）：如果防火墙只允许某些源端口的入站流量，这个选项就非常有用。

- --data-length：这个选项用于改变Nmap 发送数据包的默认数据长度，以避免被识别出来是Nmap的扫描数据。

- --max-parallelism：这个选项可限制Nmap 并发扫描的最大连接数。

● --scan-delay： 这个选项用于控制发送探测数据的时间间隔，以避免达到IDS/IPS端口扫描规则的阈值。

Nmap的官方手册详细介绍了规避探测的各种选项。如果您需要详细了解这些内容，请参照官方手册

http://nmap.org/book/man-bypass-firewalls-ids.html

利用命令

nmap -Pn 10.10.10.19 -oN nmap.crossFirewall	**该扫描手法在于目标通过防火墙策略不接收 ICMP 数据包，从而越过主机发现扫描，而 Nmap 默认先发现主机，才能进行扫描，若 SYN or Ping 扫描对方禁止，则 Nmap 自动忽视该目标**
nmap -f --mtu 64 10.10.10.19	减少数据包以防止被识别为 Nmap 指纹
nmap -D 192.168.179.189 10.10.10.19	指定诱饵主机，混淆目标 IPS/IDS 识别本机 nmap 扫描
nmap -g 80 10.10.10.19	利用防火墙特性：只允许某源端口流量访问本机，则操作该手法
nmap --data-length 10 10.10.10.19	修改 Nmap 数据包长度与 -f --mtu 相似同样避免被 firewall 识别为 nmap 指纹
nmap --max-parallelism 10 10.10.10.19	限制Nmap 并发扫描的最大连接数以免被 CC 流量防护限制
nmap --scan-delay 2 10.10.10.19	与上一个命令原理相同，增加数据包发送延迟，减少 IPS/IDS CC 流量防护检测和限制

利用过程

nmap -Pn 10.10.10.19 -oN nmap.crossFirewall

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test/testSystemVersion]
└─# nmap -Pn 10.10.10.19 -oN nmap.crossFirewall
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 13:00 CST
Nmap scan report for 10.10.10.19
Host is up (0.0015s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
```

```
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.87 seconds
```

nmap -f --mtu 64 10.10.10.19

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test]
└─# nmap -f --mtu 64 10.10.10.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 14:01 CST
Nmap scan report for 10.10.10.19
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
```

```
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds
```

nmap -D 192.168.179.189 10.10.10.19

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test]
└─# nmap -D 192.168.179.189 10.10.10.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 14:06 CST
Nmap scan report for 10.10.10.19
Host is up (0.0014s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 4.59 seconds
```

nmap -g 80 10.10.10.19

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test]
└─# nmap -g 80 10.10.10.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 14:11 CST
Nmap scan report for 10.10.10.19
Host is up (0.0033s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
```

```
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 2.65 seconds
```

由于这一类扫描手法结果均类型，均以改变发送数据形式操作，所以不再赘述利用过程，具体结果请捕获数据包参考即可。

全面扫描

> 关于全面扫描，nmap 使用 -A 参数操作，不需要指定其他参数即能够进行全方位扫描探针目标；
>
> 包括：所有端口发现，端口服务探针，操作系统探针，使用常用 Script 引擎如简单漏洞探针脚本。

关于全面扫描，我并不建议在实战中使用，-A 参数，而是建议使用如下命令操作

利用命令

nmap -A 10.10.10.19 -oN nmap.all	进行全面扫描。该命令易被 IDS/IPS 探针过滤
`nmap -sS -sV -p- -O 10.10.10.19 -oN nmap.all`	进行全面扫描，不适用默认 Script 脚本，关于这里我们可以在后期探针完端口和操作系统信息后，精确的适用探针脚本，以获取我们需要的信息，而不是盲打
-sS	SYN 扫描
-p-	扫描所有端口

利用过程

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test]
└─# nmap -A 10.10.10.19 -oN nmap.all
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 13:03 CST
Nmap scan report for 10.10.10.19
Host is up (0.00085s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.10.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_ssl-date: 2022-02-07T16:45:34+00:00; -1d12h18m04s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no
such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000,
VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

```
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      48482/tcp   mountd
|   100005  1,2,3      49804/udp   mountd
|   100021  1,3,4      49541/tcp   nlockmgr
|   100021  1,3,4      53558/udp   nlockmgr
|   100024  1          39998/udp   status
|_  100024  1          60710/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, ConnectWithDatabase,
SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew,
SwitchToSSLAfterHandshake, SupportsCompression
|   Status: Autocommit
|_  Salt: JR=wchb5|7; Takt*mgA
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2022-02-07T16:45:35+00:00; -1d12h18m04s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-
base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no
such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
| irc-info:
```

```
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 4:14:19
|   source ident: nmap
|   source host: F2B052EE.5CD59B7.59935C67.IP
|_  error: Closing Link: kercuswoz[10.10.10.1] (Quit: kercuswoz)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5

Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-02-07T11:45:25-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_clock-skew: mean: -1d11h03m04s, deviation: 2h30m00s, median: -1d12h18m04s
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 3389/tcp)
HOP RTT     ADDRESS
1   0.33 ms LAPTOP-F5GS9SLQ (172.30.240.1)
2   1.27 ms 10.10.10.19

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.46 seconds
```

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test]
```

```
└─# nmap -sS -sV -p- -O 10.10.10.19 -oN nmap.all
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 13:07 CST
Stats: 0:01:49 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 96.67% done; ETC: 13:09 (0:00:03 remaining)
Nmap scan report for 10.10.10.19
Host is up (0.00093s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE     VERSION
21/tcp    open  ftp         vsftpd 2.3.4
22/tcp    open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet      Linux telnetd
25/tcp    open  smtp        Postfix smtpd
53/tcp    open  domain      ISC BIND 9.4.2
80/tcp    open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-
1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd
6697/tcp  open  irc         UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path
/usr/lib/ruby/1.8/drb)
34324/tcp open  java-rmi    GNU Classpath grmiregistry
48482/tcp open  mountd      1-3 (RPC #100005)
49541/tcp open  nlockmgr    1-4 (RPC #100021)
60710/tcp open  status      1 (RPC #100024)


Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN;
OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 153.79 seconds
```

扫描 IPv6 主机

> 扫描 IPv6 主机没有什么不同。只是多了一个参数和目标 host IP 改变

利用命令

```
nmap -6 fe80::a00:27ff:fe43:1518
```

利用过程

```
Nmap scan report for fe80::a00:27ff:fe43:1518
Host is up (0.0014s latency).
Not shown: 996 closed ports

PORT  STATE SERVICE
22/tcp  open  ssh
53/tcp  open  domain
2121/tcp open ccproxy-ftp
5432/tcp open postgresql

MAC Address: 08:00:27:43:15:18 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

进阶操作手法-NSE

操作前置 ▲

-sC 或 --script=default	启用默认类 NSE 脚本
--script	根据指定的文件名、类别名、目录名、执行相应脚本
--script-args	这个选项用于给脚本指定参数。例如，在使用认证类脚本时，可通过这个选项指定用户名和密码

默认类 NSE 扫描目标

利用命令

nmap -sC 10.10.10.19

利用过程

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~/test]
└─# nmap -sC 10.10.10.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 13:33 CST
Stats: 0:00:44 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.80% done; ETC: 13:34 (0:00:03 remaining)
Nmap scan report for 10.10.10.19
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.10.10.1
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_ssl-date: 2022-02-07T17:16:20+00:00; -1d12h18m04s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000,
VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

```
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      48482/tcp   mountd
|   100005  1,2,3      49804/udp   mountd
|   100021  1,3,4      49541/tcp   nlockmgr
|   100021  1,3,4      53558/udp   nlockmgr
|   100024  1          39998/udp   status
|_  100024  1          60710/tcp   status
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 18
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, SupportsCompression, SwitchToSSLAfterHandshake, LongColumnFlag
|   Status: Autocommit
|_  Salt: PT6Nf:+fD_3|9G8$I$uF
5432/tcp open  postgresql
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2022-02-07T17:16:22+00:00; -1d12h18m05s from scanner time.
```

```
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat

Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-02-07T12:15:36-05:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -1d11h03m04s, deviation: 2h30m00s, median: -1d12h18m04s

Nmap done: 1 IP address (1 host up) scanned in 78.70 seconds
```

NSE 操作 http 服务获取详细信息

您还可能需要获取目标主机的特定信息。此时可以单独使用脚本文件。如果要获取HTTP服务器的信息，将会发现NSE的脚本里有很多脚本都是分析HTTP服务的。这里列出常用 NSE 脚本探针

这些脚本有：http-enum、http-headers、http-methods、http-php-version

利用命令

nmap --script http-enum,http-headers,http-methods,http-php-version -p 80 10.10.10.19	**启用 NSE 脚本进行 web 目录信息探针、HEAD 头部信息探针、PHP version 探针、HTTP 请求方法探针**

利用过程

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~]
└─# nmap --script http-enum,http-headers,http-methods,http-php-version -p 80 10.10.10.19

Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 13:46 CST
Nmap scan report for 10.10.10.19
Host is up (0.00096s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /phpinfo.php: Possible information file
|   /phpMyAdmin/: phpMyAdmin
|   /doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
|   /icons/: Potentially interesting folder w/ directory listing
|_  /index/: Potentially interesting folder
| http-php-version: Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2.17
| Versions from credits query (more accurate): 5.2.3 - 5.2.5, 5.2.6RC3
|_Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| http-headers:
|   Date: Mon, 07 Feb 2022 17:27:58 GMT
|   Server: Apache/2.2.8 (Ubuntu) DAV/2
|   X-Powered-By: PHP/5.2.4-2ubuntu5.10
|   Connection: close
|   Content-Type: text/html
|
|_  (Request type: HEAD)

Nmap done: 1 IP address (1 host up) scanned in 2.63 seconds
```

该 NSE 脚本，作用于常见目录探针，HTTP methods 探针，PHP 版本探针，HTTP head 头部信息探针

终极操作手法-NSE ▲▲▲▲▲

> 该操作手法主要应用在 vuln 漏洞信息探针方面，以及我们所需的必要信息探针，都需要应用这些第三方 NSE 脚本

以下脚本参考直接点击小结名即可到达指定网址

nmap-vulners

NSE 脚本使用有关已知服务的信息来提供有关漏洞的数据。请注意，它已包含在标准 nmap NSE 库中。

利用命令

需要注意的是该脚本依赖 nmap -sV 使用，所以在使用该 NSE 时，必须操作 -sV 参数

nmap -sV --script vulners 10.10.10.19

利用过程

> 由于信息过多这里只列出些许结果，具体结果请自行测试

```
┌──(root💀LAPTOP-F5GS9SLQ)-[~]
└─# nmap -sV --script vulners 10.10.10.19
Starting Nmap 7.92 ( https://nmap.org ) at 2022-02-09 14:33 CST
Nmap scan report for 10.10.10.19
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SECURITYVULNS:VULN:8166 7.5
https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|       MSF:ILITIES/OPENBSD-OPENSSH-CVE-2010-4478/      7.5
https://vulners.com/metasploit/MSF:ILITIES/OPENBSD-OPENSSH-CVE-2010-4478/
    *EXPLOIT*
|       MSF:ILITIES/LINUXRPM-ELSA-2008-0855/    7.5
https://vulners.com/metasploit/MSF:ILITIES/LINUXRPM-ELSA-2008-0855/
*EXPLOIT*
|       CVE-2010-4478   7.5     https://vulners.com/cve/CVE-2010-4478
|       CVE-2008-1657   6.5     https://vulners.com/cve/CVE-2008-1657
|       SSV:60656       5.0     https://vulners.com/seebug/SSV:60656
 *EXPLOIT*
|       CVE-2017-15906  5.0     https://vulners.com/cve/CVE-2017-15906
|       CVE-2010-5107   5.0     https://vulners.com/cve/CVE-2010-5107
|       MSF:ILITIES/SUSE-CVE-2011-5000/ 3.5
https://vulners.com/metasploit/MSF:ILITIES/SUSE-CVE-2011-5000/  *EXPLOIT*
|       MSF:ILITIES/ORACLE-SOLARIS-CVE-2012-0814/       3.5
https://vulners.com/metasploit/MSF:ILITIES/ORACLE-SOLARIS-CVE-2012-0814/
     *EXPLOIT*
|       MSF:ILITIES/GENTOO-LINUX-CVE-2011-5000/ 3.5
https://vulners.com/metasploit/MSF:ILITIES/GENTOO-LINUX-CVE-2011-5000/
 *EXPLOIT*
```

```
|       MSF:ILITIES/AMAZON-LINUX-AMI-ALAS-2012-99/      3.5
https://vulners.com/metasploit/MSF:ILITIES/AMAZON-LINUX-AMI-ALAS-2012-99/
    *EXPLOIT*
|       CVE-2012-0814   3.5     https://vulners.com/cve/CVE-2012-0814
|       CVE-2011-5000   3.5     https://vulners.com/cve/CVE-2011-5000
|       CVE-2008-5161   2.6     https://vulners.com/cve/CVE-2008-5161
|       CVE-2011-4327   2.1     https://vulners.com/cve/CVE-2011-4327
|       MSF:ILITIES/SSH-OPENSSH-X11USELOCALHOST-X11-FORWARDING-SESSION-
HIJACK/  1.2     https://vulners.com/metasploit/MSF:ILITIES/SSH-OPENSSH-
X11USELOCALHOST-X11-FORWARDING-SESSION-HIJACK/    *EXPLOIT*
|       CVE-2008-3259   1.2     https://vulners.com/cve/CVE-2008-3259
|_      SECURITYVULNS:VULN:9455 0.0
https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
```

nmap-vulscan ▲

> 该 NSE 引擎强大与 vulners，输出更为全面且详细，同样与 vulners 相同，依赖于 -sV 参数

install

```
1:git clone https://github.com/scipag/vulscan.git
2:cd vulscan/
3:ln -sf `pwd`/vulscan /usr/share/nmap/scripts/vulscan
```

利用命令

nmap --script vulscan/vulscan.nse -sV 10.10.10.19 -oA nmap.vulscan

利用过程

> 由于输出信息过多，且详细，这里操作 -oA 以转换 .xml 格式为 .html 格式参考
>
> xsltproc nmapVulsan.xml -o nmapVulscan.html

Nmap Scan Report - Scanned at Wed Feb 9 15:05:18 2022

Scan Summary | 10.10.10.19

Scan Summary

Nmap 7.92 was initiated at Wed Feb 9 15:05:18 2022 with these arguments:
nmap -sV --script vulscan/vulscan.nse -oA nmapVulsan 10.10.10.19

Verbosity: 0; Debug level 0

Nmap done at Wed Feb 9 15:06:17 2022; 1 IP address (1 host up) scanned in 58.22 seconds

10.10.10.19

Address

- 10.10.10.19 (ipv4)

Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])
21	tcp	open
	vulscan	VulDB - https://vuldb.com: [146452] vsftpd 2.3.4 Service Port 6200 privilege escalation MITRE CVE - https://cve.mitre.org: [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in STAT commands in multiple FTP sessions, a d SecurityFocus - https://www.securityfocus.com/bid/: [82295] Vsftpd CVE-2004-0042 Remote Security Vulnerability [72451] vsftpd CVE-2015-1419 Security Bypass Vulnerability [51013] vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability [49539] vsftpd Compromised Source Packages Backdoor Vulnerability [46617] vsftpd FTP Server 'ls.c' Remote Denial of Service Vulnerability [41443] Vsftpd Webmin Module Multiple Unspecified Vulnerabilities [30064] vsftpd FTP Server Pluggable Authentication Module (PAM) Remote Denial of Service Vulnerability [29322] vsftpd FTP Server 'deny_file' Option Remote Denial of Service Vulnerability [10394] Vsftpd Listener Denial of Service Vulnerability [7253] Red Hat Linux 9 vsftpd Compiling Error Weakness

nmapAutomator

> 这是一个能使 Nmap 自动渗透测试的脚本工具，而非 NSE，之所以列出该工具，主要是为了方便且收集信息全面
>
> 这个脚本的主要目标是自动化每次运行的枚举和侦察过程，而不是将我们的注意力集中在真正的渗透测试上

- 支持 nmap 基本操作手法
- 支持 nmap NSE 操作手法
- 枚举 SMTP
- 枚举与测试域传送 DNS
- 支持 nikto webServerExploit 扫描
- 支持 SMB 操作
- 支持目录探针
- 支持漏洞探针

.....

不过若是实战情况，不推荐使用，主要用于测试参考

install

```
git clone https://github.com/21y4d/nmapAutomator.git
```

利用命令

./nmapAutomator.sh --host 10.10.10.19 -t Recon -o Targetinfomation.xml

nmap-nse-scripts 其他第三方研发 NSE 参考