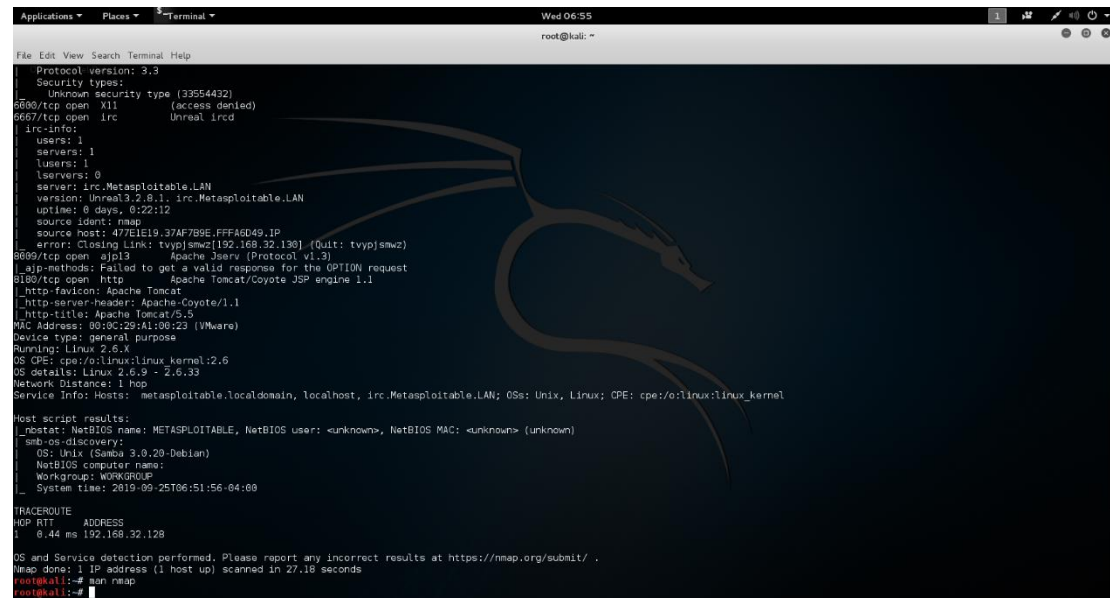


1. Finished
2. (1) OS: Unix (Samba 3.0.20-Debian)



```

Protocol version: 3.3
Security types:
Unknown security type (33554432)
6666/tcp open  X11      (access denied)
6667/tcp open  irc       Unreal ircd
Host info:
  users: 1
  servers: 1
  users: 1
  lservers: 0
  server: irc.Metasploitable.LAN
  version: Unreal3.2.0.1. irc.Metasploitable.LAN
  uptime: 0 days, 0:22:12
  source host: 477E1E19.37AF7B9E.FFFA6D49.IP
  error: Closing Link: tvypismwz[192.168.32.128] (Quit: tvypismwz)
6669/tcp open  ajp13     Apache Jserv (Protocol v1.3)
  _ajp-methods: Failed to get a valid response for the OPTIONS request
6160/tcp open  http      Apache Tomcat/Coyote JSP engine 1.1
  _http-favicon: Apache Tomcat
  _http-server-header: Apache-Coyote/1.1
  _http-title: Apache Tomcat/5.5
MAC Address: 80:0C:29:A1:08:23 (VMware)
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
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

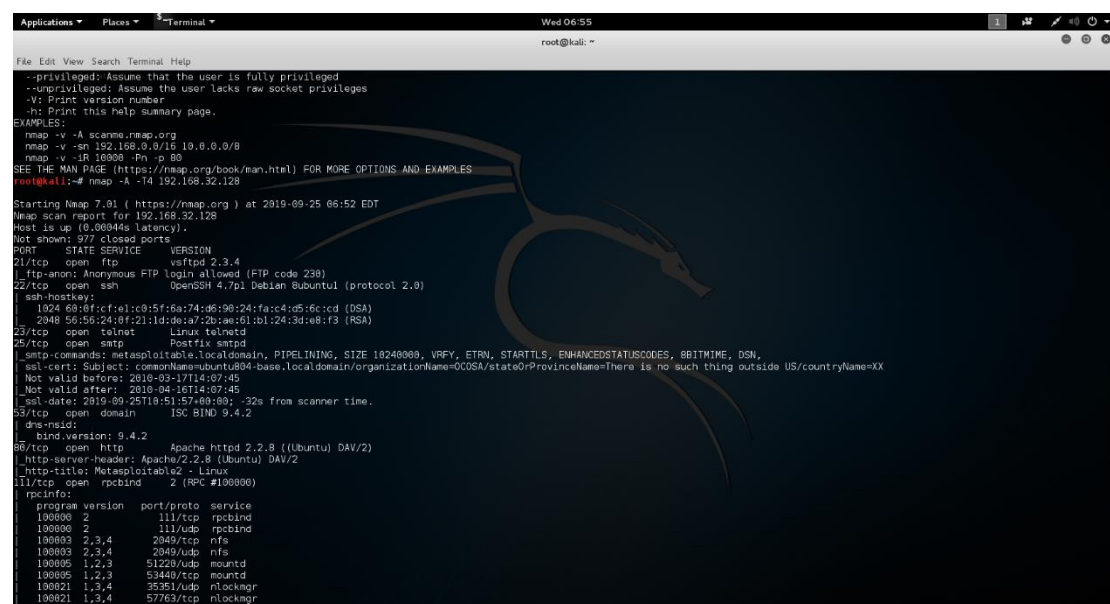
Host script results:
  _host: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
  smb-os-discovery:
    OS: Unix (Samba 3.0.20-Debian)
    NetBIOS computer name:
    Workgroup: WORKGROUP
    System time: 2019-09-25T06:51:56-04:00

TRACEROUTE
HOP RTT ADDRESS
1 0.44 ms 192.168.32.128

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 27.18 seconds
root@kali:~# nmap
root@kali:~#

```

The running services: ftp, ssh, telnet



```

--privileged: Assume that the user is fully privileged
--unprivileged: Assume the user lacks raw socket privileges
-V: Print version number
-h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 -p 80,8080
  nmap -v -iR 10000 -Ph -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap -A -iR 192.168.32.128

Starting Nmap 7.01 ( https://nmap.org ) at 2019-09-25 06:52 EDT
Nmap scan report for 192.168.32.128
Host is up (0.0094s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp           vsftpd 2.3.4
|_ftp-anon Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ssh-hostkey:
|_ 1924 68:8f:cf:a1:c0:5f:6a:74:d6:96:24:fa:c4:d5:6c:cd (RSA)
|_ 2048 56:5b:24:8f:21:1d:de:a7:2b:a6:61:ab:12:43:de:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
|_smtp_commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-cert: Subject: commonName=ubuntu0804-base.localdomain/organizationName=DOSA/stateOrProvinceName=here 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: 2019-09-25T19:51:57+00:00; -32s from scanner time.
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 #10000)
|_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 51228/udp  mountd
|_  100005 1,2,3 53440/tcp  mountd
|_  100021 1,3,4 35351/udp  nlockmgr
|_  100021 1,3,4 57763/tcp  nlockmgr

```

(2): T1,T2,T3 的探测时间不一样, T1 最长, T3 最短

(3): 使用 T1 探测

3. Target: 172.16.108.172

i. Vulnerabilities: OS END OF LIFE

description:操作系统的版本太久了

ii. Vulnerabilities: Distributed Ruby(dRuby/DRb) Multiple Remote Code Execution

Vulnerabilities

description:使用分布式 Ruby 软件可能会导致无授权的系统执行分布式命令

Applications ▾ Places ▾ Iceweasel ▾ Wed 06:57

Greenbone Security Assistant - Iceweasel

https://127.0.0.1:9392/omp/cmd/get\_report&report\_id=a482bc96-0a69-4833-a304-0ded1d0a10dd&notes=1&overrides=1&result\_hosts\_only=1&token=28bf6d ▾ Search

Most Visited ▾ Offensive Security ▾ Kali Linux ▾ Kali Docs ▾ Kali Tools ▾ Exploit-DB ▾ Aircrack-ng

Greenbone Security Assistant

logged in as Admin admin | Logout  
Wed Sep 25 10:56:43 2019 UTC

Scan Management Asset Management Schedules Management Configuration Extras Administration Help

Report: Results 1 - 100 of 120 (total: 234) PDF

Filter: =hmg autofp=0 notes=1 overrides=1 first=1 rows=100 delta\_states=gn

Vulnerability	Severity	QoD	Host	Location	Actions
ProFTPD Multiple Remote Vulnerabilities	High	75%	172.16.108.172	21/tcp	
Possible Backdoor: Ingreslock	High	99%	172.16.108.172	1524/tcp	
ProFTPD Multiple Remote Vulnerabilities	High	75%	172.16.108.172	2121/tcp	
X Server Detection	High	75%	172.16.108.172	6000/tcp	
DistCC Remote Code Execution Vulnerability	High	75%	172.16.108.172	3632/tcp	
MySQL / MariaDB weak password	Mitigation	95%	172.16.108.172	3306/tcp	
PostgreSQL weak password	Mitigation	75%	172.16.108.172	5432/tcp	
DistCC Detection	Mitigation	75%	172.16.108.172	3632/tcp	
PostgreSQL Multiple Security Vulnerabilities	High	75%	172.16.108.172	5432/tcp	
vsftpd Compromised Source Packages Backdoor Vulnerability	High	75%	172.16.108.172	21/tcp	
ProFTPD Server SQL Injection Vulnerability	High	75%	172.16.108.172	21/tcp	
phpMyAdmin Code Injection and XSS Vulnerability	High	75%	172.16.108.172	80/tcp	
phpMyAdmin BLOB Streaming Multiple Input Validation Vulnerabilities	High	75%	172.16.108.172	80/tcp	
phpMyAdmin Configuration File PHP Code Injection Vulnerability	High	75%	172.16.108.172	80/tcp	
Tiki Wiki CMS Groupware < 4.2 Multiple Unspecified Vulnerabilities	High	75%	172.16.108.172	80/tcp	
PHP-CGI-based setups vulnerability when parsing query string parameters from php files	High	95%	172.16.108.172	80/tcp	
phpinfo() output accessible	High	80%	172.16.108.172	80/tcp	