Task 2: Vulnerability Assessment and Scanning Report

Attacker Machine (Kali Linux): 192.168.56.3

Target Machine (Metasploitable 2): 192.168.56.4

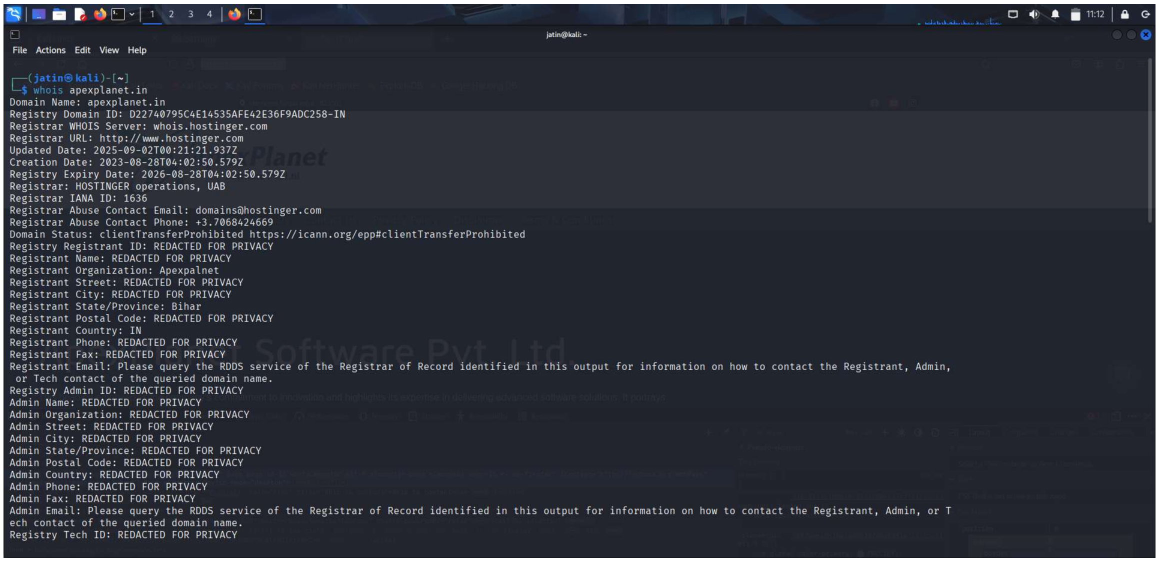
1. Passive Reconnaissance

WHOIS Lookup

Command:

whois apexplanet.in

Purpose: Retrieve domain ownership and registration details.



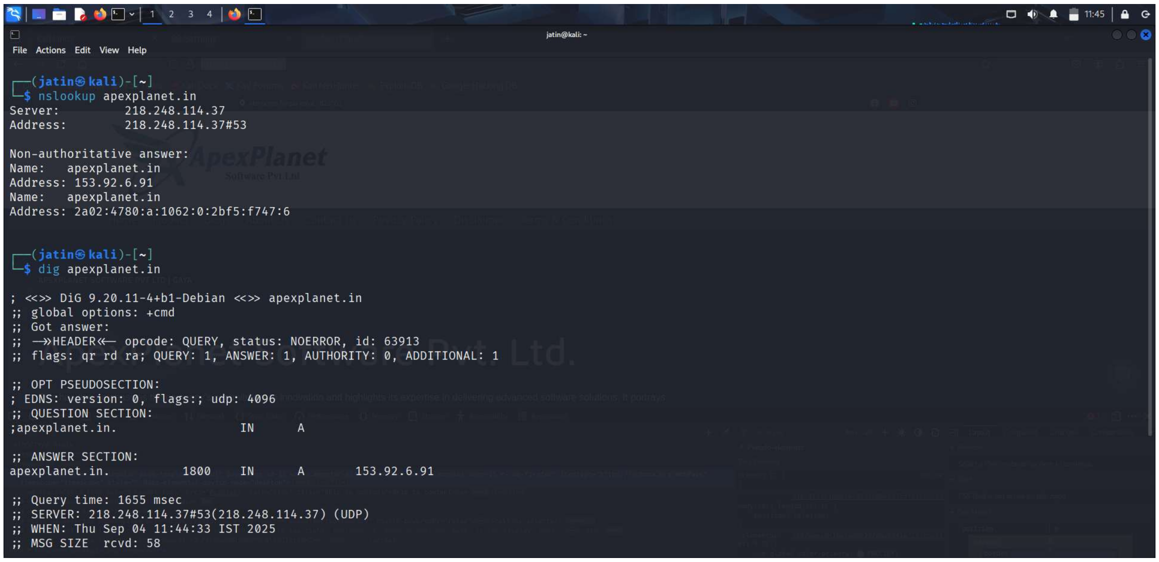
```
┌──(jatin㉿kali)-[~]
└─$ whois apexplanet.in
Domain Name: apexplanet.in
Registry Domain ID: D22740795C4E14535AFE42E36F9ADC258-IN
Registrar WHOIS Server: whois.hostinger.com
Registrar URL: http://www.hostinger.com
Updated Date: 2025-09-02T00:21:21.937Z
Creation Date: 2023-08-28T04:02:50.579Z
Registry Expiry Date: 2026-08-28T04:02:50.579Z
Registrar: HOSTINGER operations, UAB
Registrar IANA ID: 1636
Registrar Abuse Contact Email: domains@hostinger.com
Registrar Abuse Contact Phone: +3.7068424669
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization: Apexpalnet
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province: Bihar
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: IN
Registrant Phone: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin,
 or Tech contact of the queried domain name.
Registry Admin ID: REDACTED FOR PRIVACY
Admin Name: REDACTED FOR PRIVACY
Admin Organization: REDACTED FOR PRIVACY
Admin Street: REDACTED FOR PRIVACY
Admin City: REDACTED FOR PRIVACY
Admin State/Province: REDACTED FOR PRIVACY
Admin Postal Code: REDACTED FOR PRIVACY
Admin Country: REDACTED FOR PRIVACY
Admin Phone: REDACTED FOR PRIVACY
Admin Fax: REDACTED FOR PRIVACY
Admin Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or T
ech contact of the queried domain name.
Registry Tech ID: REDACTED FOR PRIVACY
```

nslookup

Command:

nslookup apexplanet.in

Purpose: Resolve domain names to IP addresses.

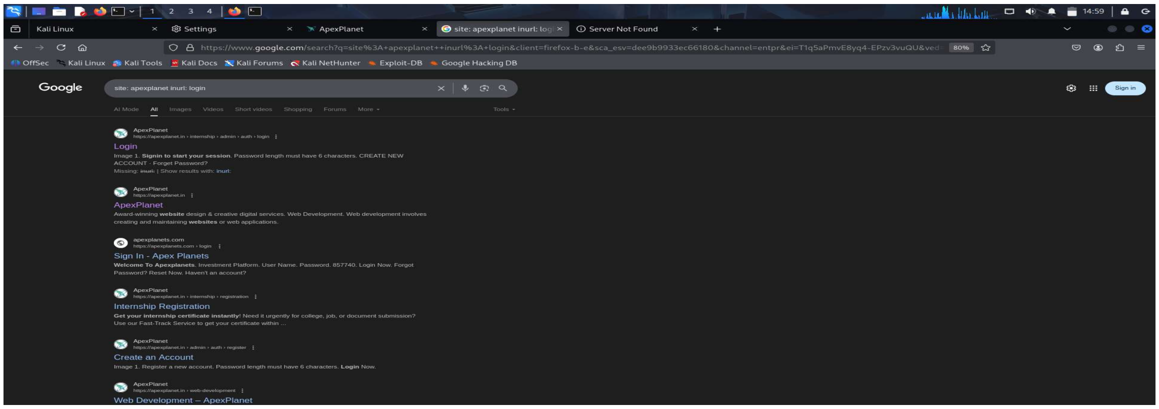


```
┌──(jatin㉿kali)-[~]
└─$ nslookup apexplanet.in
Server:         218.248.114.37
Address:        218.248.114.37#53

Non-authoritative answer:
Name:   apexplanet.in
Address: 153.92.6.91
Name:   apexplanet.in
Address: 2a02:4780:a:1062:0:2bf5:f747:6


┌──(jatin㉿kali)-[~]
└─$ dig apexplanet.in

; <<>> DiG 9.20.11-4+b1-Debian <<>> apexplanet.in
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 63913
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;apexplanet.in.                 IN      A

;; ANSWER SECTION:
apexplanet.in.          1800    IN      A       153.92.6.91

;; Query time: 1655 msec
;; SERVER: 218.248.114.37#53(218.248.114.37) (UDP)
;; WHEN: Thu Sep 04 11:44:33 IST 2025
;; MSG SIZE  rcvd: 58
```

Goggle Dorking

Command:

site: apexplanet.in inurl: login or site: apexplanet.in file type: pdf



site: apexplanet inurl: login

ApexPlanet
https://apexplanet.in › internship › admin › auth › login
Login
Image 1. **Signin to start your session**. Password length must have 6 characters. CREATE NEW ACCOUNT · Forget Password?
Missing: ~~inurl:~~ | Show results with: inurl:

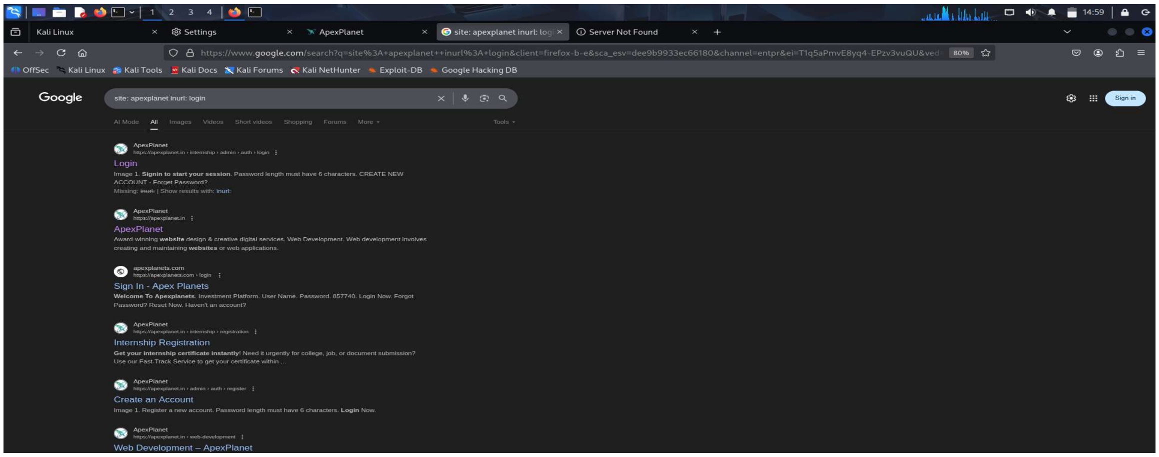
ApexPlanet
https://apexplanet.in
ApexPlanet
Award-winning **website** design & creative digital services. Web Development. Web development involves creating and maintaining **websites** or web applications.

apexplanets.com
https://apexplanets.com › login
Sign In - Apex Planets
Welcome To Apexplanets. Investment Platform. User Name. Password. 857740. Login Now. Forgot Password? Reset Now. Haven't an account?

ApexPlanet
https://apexplanet.in › internship › registration
Internship Registration
Get your internship certificate instantly! Need it urgently for college, job, or document submission? Use our Fast-Track Service to get your certificate within ...

ApexPlanet
https://apexplanet.in › admin › auth › register
Create an Account
Image 1. Register a new account. Password length must have 6 characters. **Login** Now.

ApexPlanet
https://apexplanet.in › web-development
Web Development – ApexPlanet



site: apexplanet inurl: login

ApexPlanet
https://apexplanet.in › internship › admin › auth › login
Login
Image 1. Signin to start your session. Password length must have 6 characters. CREATE NEW ACCOUNT · Forget Password?
Missing: inurl: | Show results with: inurl:

ApexPlanet
https://apexplanet.in
ApexPlanet
Award-winning website design & creative digital services. Web Development. Web development involves creating and maintaining websites or web applications.

apexplanets.com
https://apexplanets.com › login
Sign In - Apex Planets
Welcome To Apexplanets. Investment Platform. User Name. Password. 857740. Login Now. Forgot Password? Reset Now. Haven't an account?

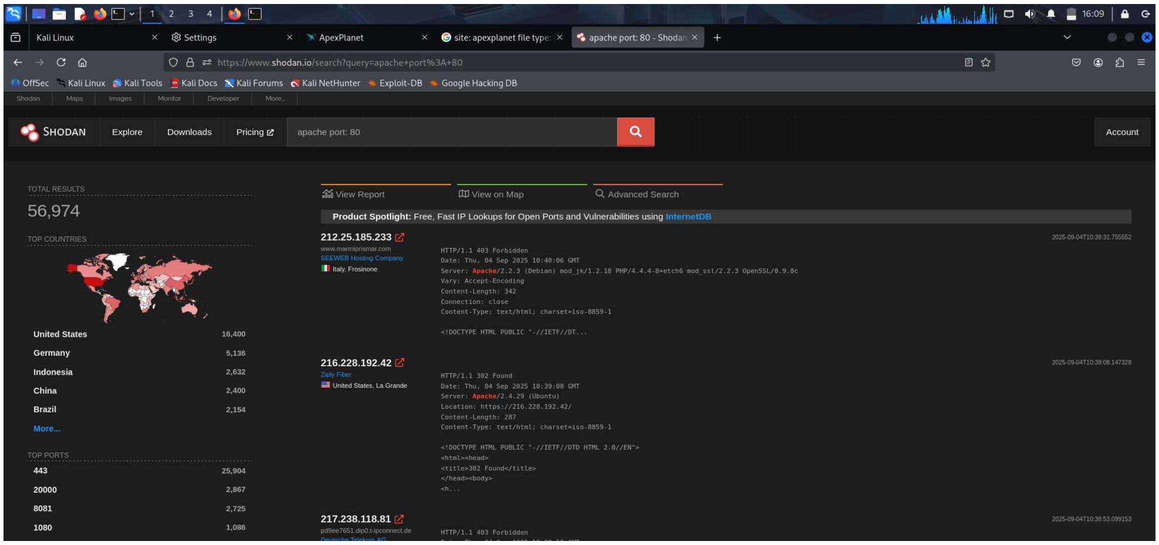
ApexPlanet
https://apexplanet.in › internship › registration
Internship Registration
Get your internship certificate instantly! Need it urgently for college, job, or document submission? Use our Fast-Track Service to get your certificate within ...

ApexPlanet
https://apexplanet.in › admin › auth › register
Create an Account
Image 1. Register a new account. Password length must have 6 characters. Login Now.

ApexPlanet
https://apexplanet.in › web-development
Web Development – ApexPlanet

Shodan

- **Command / Tool:** apache port: 80 & ftp port: 21 country "IN "/ Shodan (online search engine)
- **Purpose:** Used for **passive reconnaissance** to find information about publicly exposed devices, services, and vulnerabilities on the internet without directly scanning the target.



apache port: 80

TOTAL RESULTS

56,974

TOP COUNTRIES

United States	16,400
Germany	5,136
Indonesia	2,632
China	2,400
Brazil	2,154

More...

TOP PORTS

443	25,904
20000	2,867
8081	2,725
1080	1,086

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

212.25.185.233
www.marmiprismar.com
SEEWEB Hosting Company
Italy, Frosinone
2025-09-04T10:39:31.755552

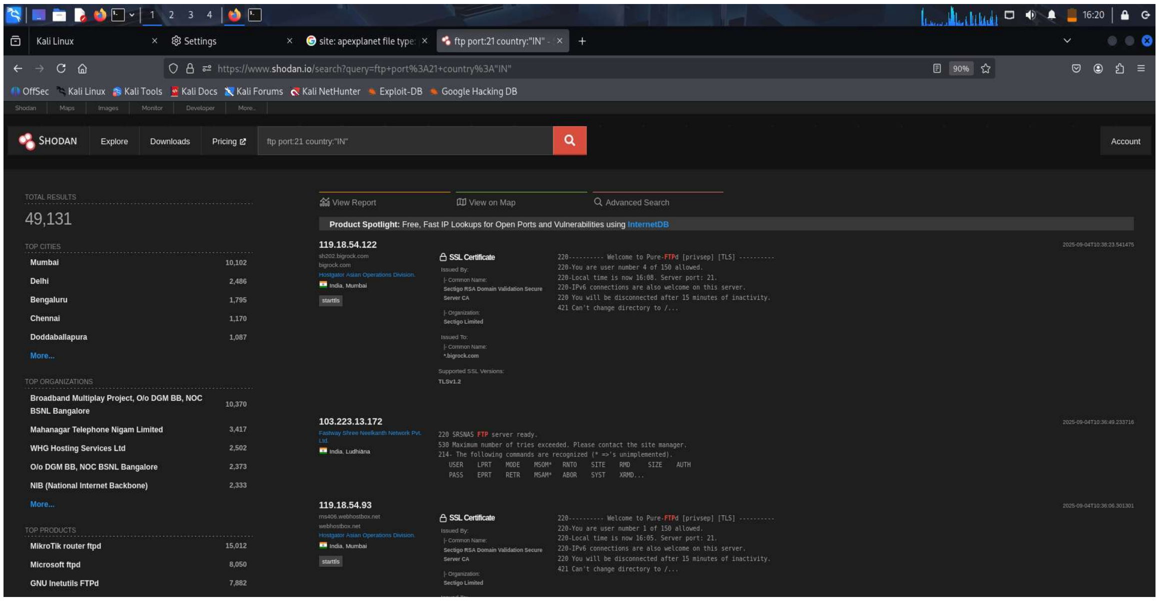
```
HTTP/1.1 403 Forbidden
Date: Thu, 04 Sep 2025 10:40:06 GMT
Server: Apache/2.2.3 (Debian) mod_jk/1.2.18 PHP/4.4.4-8+etch6 mod_ssl/2.2.3 OpenSSL/0.9.8c
Vary: Accept-Encoding
Content-Length: 342
Connection: close
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DT...
```

216.228.192.42
Ziply Fiber
United States, La Grande
2025-09-04T10:39:08.147328

```
HTTP/1.1 302 Found
Date: Thu, 04 Sep 2025 10:39:08 GMT
Server: Apache/2.4.29 (Ubuntu)
Location: https://216.228.192.42/
Content-Length: 287
Content-Type: text/html; charset=iso-8859-1

<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>302 Found</title>
</head><body>
<h...
```

217.238.118.81
pd9ee7651.dip0.t-ipconnect.de
Deutsche Telekom AG
2025-09-04T10:38:53.099153

```
HTTP/1.1 403 Forbidden
```



ftp port:21 country:"IN"

TOTAL RESULTS

49,131

TOP CITIES

Mumbai	10,102
Delhi	2,486
Bengaluru	1,795
Chennai	1,170
Doddaballapura	1,087

More...

TOP ORGANIZATIONS

Broadband Multiplay Project, O/o DGM BB, NOC BSNL Bangalore	10,370
Mahanagar Telephone Nigam Limited	3,417
WHG Hosting Services Ltd	2,502
O/o DGM BB, NOC BSNL Bangalore	2,373
NIB (National Internet Backbone)	2,333

More...

TOP PRODUCTS

MikroTik router ftpd	15,012
Microsoft ftpd	8,050
GNU Inetutils FTPd	7,882

Product Spotlight: Free, Fast IP Lookups for Open Ports and Vulnerabilities using InternetDB

119.18.54.122
sh202.bigrock.com
bigrock.com
Hostgator Asian Operations Division.
India, Mumbai
starttls
2025-09-04T10:38:23.541475

SSL Certificate
Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA
|- Organization:
Sectigo Limited
Issued To:
|- Common Name:
*.bigrock.com
Supported SSL Versions:
TLSv1.2

```
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 4 of 150 allowed.
220-Local time is now 16:08. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
421 Can't change directory to /...
```

103.223.13.172
Fastway Shree Neelkanth Network Pvt. Ltd.
India, Ludhiana
2025-09-04T10:36:49.233716

```
220 SRSNAS FTP server ready.
530 Maximum number of tries exceeded. Please contact the site manager.
214- The following commands are recognized (* =>'s unimplemented).
   USER    LPRT    MODE    MSOM*   RNTO    SITE    RMD     SIZE    AUTH
   PASS    EPRT    RETR    MSAM*   ABOR    SYST    XRMD...
```

119.18.54.93
rns406.webhostbox.net
webhostbox.net
Hostgator Asian Operations Division.
India, Mumbai
starttls
2025-09-04T10:36:06.301301

SSL Certificate
Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA
|- Organization:
Sectigo Limited

```
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 150 allowed.
220-Local time is now 16:05. Server port: 21.
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
421 Can't change directory to /...
```

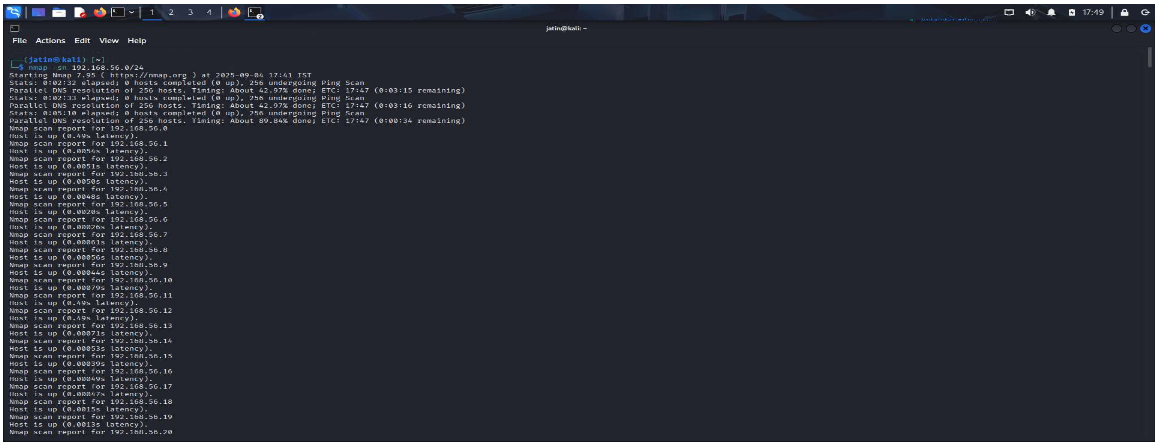
2. Active Reconnaissance

Ping Sweep

Command:

nmap -sn 192.168.56.0/24

Purpose: Identifies which hosts are up and reachable in the subnet by sending ICMP Echo requests (ping). This helps in mapping active machines before deep scanning.



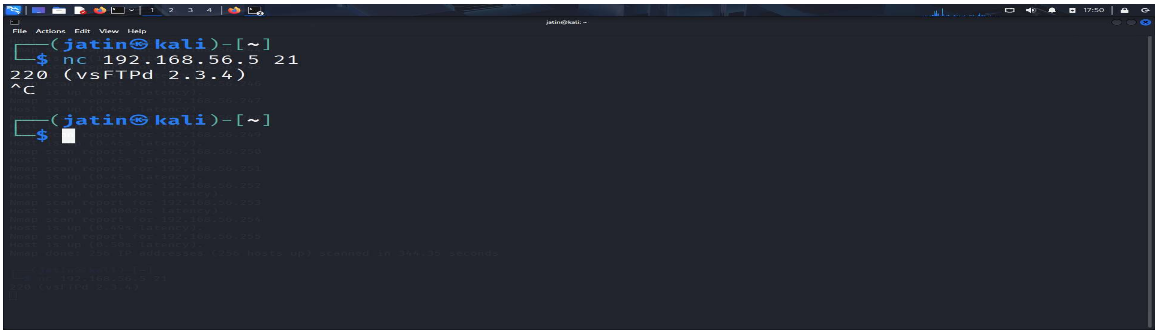
```
┌──(jatin㉿kali)-[~]
└─$ nmap -sn 192.168.56.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-04 17:41 IST
Stats: 0:02:32 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 256 hosts. Timing: About 42.97% done; ETC: 17:47 (0:03:15 remaining)
Stats: 0:02:33 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 256 hosts. Timing: About 42.97% done; ETC: 17:47 (0:03:16 remaining)
Stats: 0:05:10 elapsed; 0 hosts completed (0 up), 256 undergoing Ping Scan
Parallel DNS resolution of 256 hosts. Timing: About 89.84% done; ETC: 17:47 (0:00:34 remaining)
Nmap scan report for 192.168.56.0
Host is up (0.49s latency).
Nmap scan report for 192.168.56.1
Host is up (0.0054s latency).
Nmap scan report for 192.168.56.2
Host is up (0.0051s latency).
Nmap scan report for 192.168.56.3
Host is up (0.0050s latency).
Nmap scan report for 192.168.56.4
Host is up (0.0048s latency).
Nmap scan report for 192.168.56.5
Host is up (0.0020s latency).
Nmap scan report for 192.168.56.6
Host is up (0.00026s latency).
Nmap scan report for 192.168.56.7
Host is up (0.00061s latency).
Nmap scan report for 192.168.56.8
Host is up (0.00056s latency).
Nmap scan report for 192.168.56.9
Host is up (0.00044s latency).
Nmap scan report for 192.168.56.10
Host is up (0.00079s latency).
Nmap scan report for 192.168.56.11
Host is up (0.49s latency).
Nmap scan report for 192.168.56.12
Host is up (0.49s latency).
Nmap scan report for 192.168.56.13
Host is up (0.00071s latency).
Nmap scan report for 192.168.56.14
Host is up (0.00053s latency).
Nmap scan report for 192.168.56.15
Host is up (0.00039s latency).
Nmap scan report for 192.168.56.16
Host is up (0.00049s latency).
Nmap scan report for 192.168.56.17
Host is up (0.00047s latency).
Nmap scan report for 192.168.56.18
Host is up (0.0015s latency).
Nmap scan report for 192.168.56.19
Host is up (0.0013s latency).
Nmap scan report for 192.168.56.20
```

Banner Grabbing

Command:

nc 192.168.56.4 21

Purpose: Connects to a service port and retrieves its banner (service name, version). This reveals useful info about running services (e.g., FTP server version).



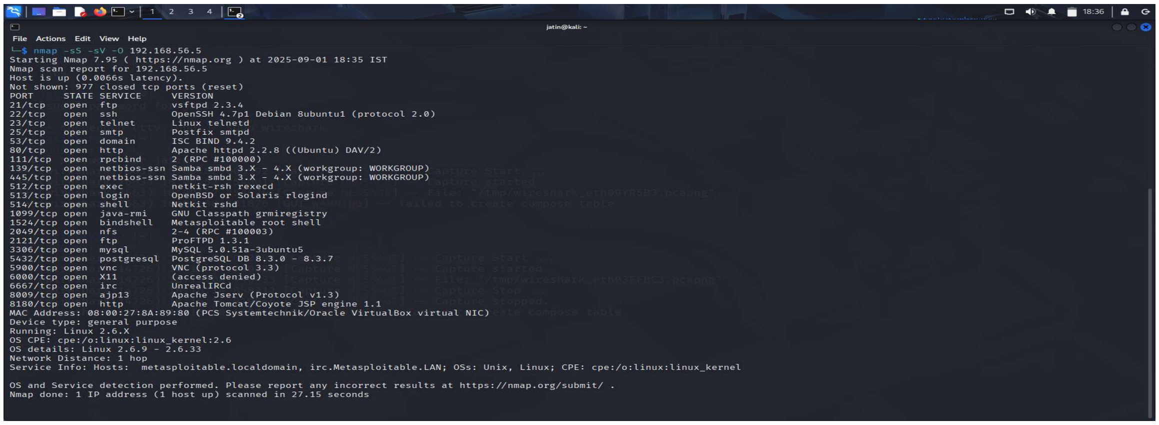
```
┌──(jatin㉿kali)-[~]
└─$ nc 192.168.56.5 21
220 (vsFTPd 2.3.4)
^C

┌──(jatin㉿kali)-[~]
└─$ 
```

Nmap TCP, Service & OS Detection

Command:

sudo nmap -sS -sV -O -192.168.56.5

Purpose: Detect open TCP ports using stealth scan and Identify running services and operating system.



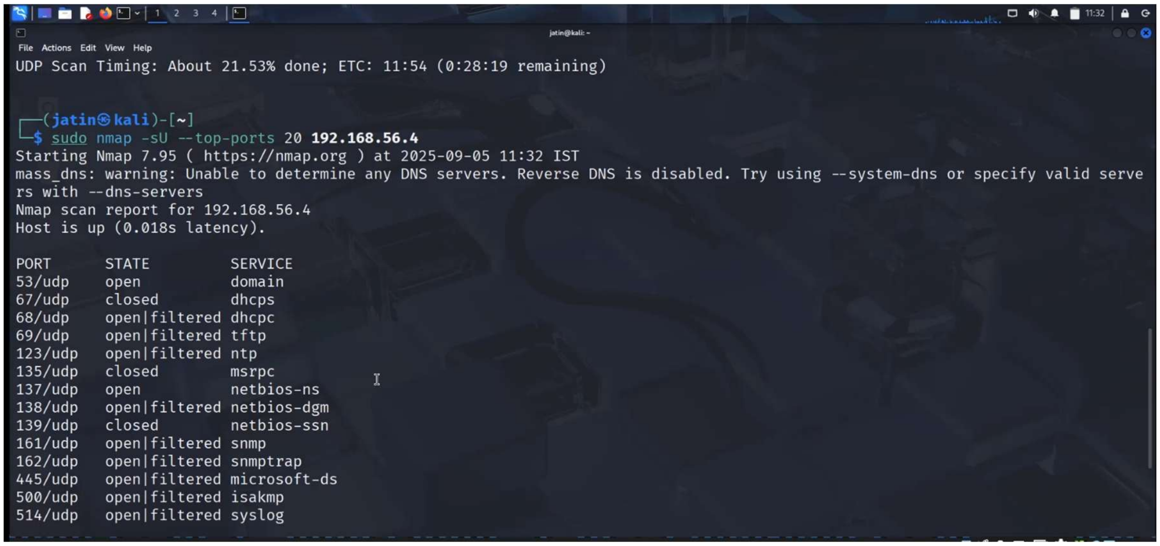
```
└─$ nmap -sS -sV -O 192.168.56.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-01 18:35 IST
Nmap scan report for 192.168.56.5
Host is up (0.0066s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         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       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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
MAC Address: 08:00:27:8A:89:80 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
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, 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 27.15 seconds
```

Nmap UDP Scan

Command:

sudo nmap -sU –top-ports 20 192.168.56.4

Purpose: Identify open UDP ports.



```
UDP Scan Timing: About 21.53% done; ETC: 11:54 (0:28:19 remaining)

┌──(jatin㉿kali)-[~]
└─$ sudo nmap -sU --top-ports 20 192.168.56.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-09-05 11:32 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid serve
rs with --dns-servers
Nmap scan report for 192.168.56.4
Host is up (0.018s latency).

PORT      STATE         SERVICE
53/udp    open          domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
123/udp   open|filtered ntp
135/udp   closed        msrpc
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
139/udp   closed        netbios-ssn
161/udp   open|filtered snmp
162/udp   open|filtered snmptrap
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
514/udp   open|filtered syslog
```

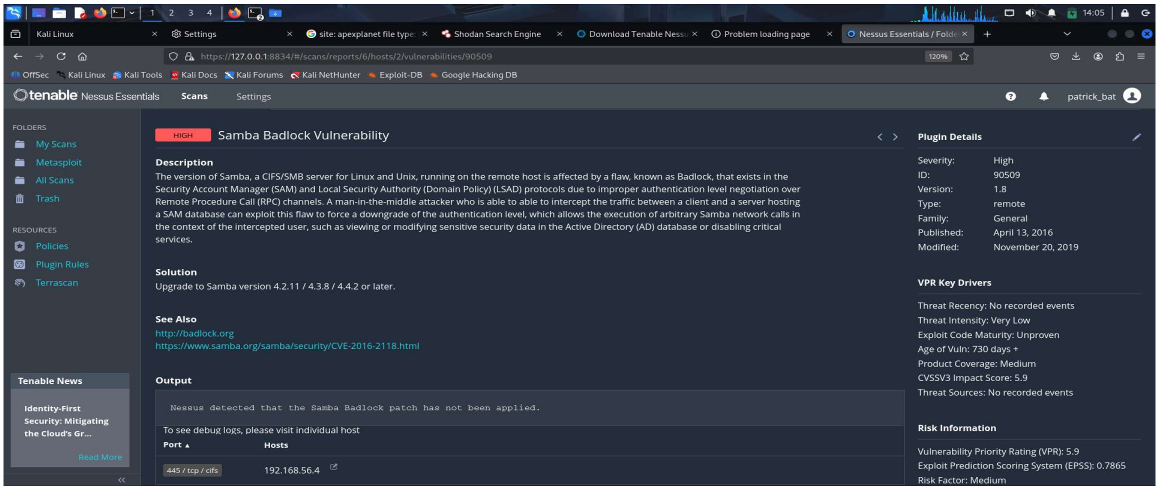
3. Vulnerability Scanning (Nessus)

Nessus Setup

Command:

> *Access Nessus at https://127.0.0.1:8834/*

Purpose: Perform automated vulnerability assessment on the target.



https://127.0.0.1:8834/#/scans/reports/6/hosts/2/vulnerabilities/90509

HIGH Samba Badlock Vulnerability

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution

Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

See Also

http://badlock.org
https://www.samba.org/samba/security/CVE-2016-2118.html

Output

```
Nessus detected that the Samba Badlock patch has not been applied.
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.56.4

Plugin Details

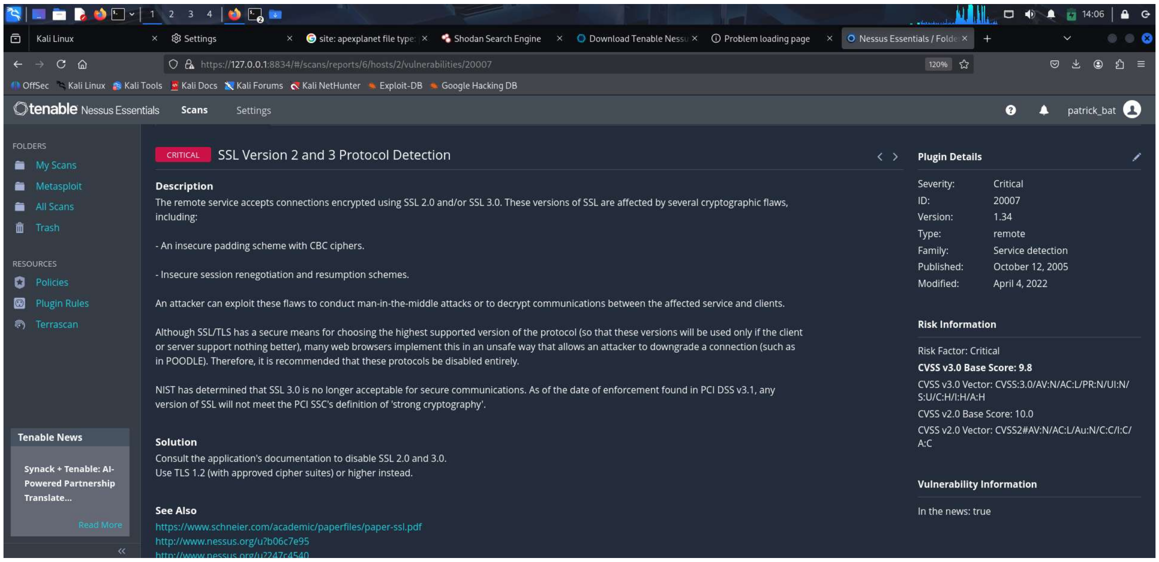
Severity:	High
ID:	90509
Version:	1.8
Type:	remote
Family:	General
Published:	April 13, 2016
Modified:	November 20, 2019

VPR Key Drivers

Threat Recency: No recorded events
Threat Intensity: Very Low
Exploit Code Maturity: Unproven
Age of Vuln: 730 days +
Product Coverage: Medium
CVSSV3 Impact Score: 5.9
Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 5.9
Exploit Prediction Scoring System (EPSS): 0.7865
Risk Factor: Medium



https://127.0.0.1:8834/#/scans/reports/6/hosts/2/vulnerabilities/20007

CRITICAL SSL Version 2 and 3 Protocol Detection

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540

Plugin Details

Severity:	Critical
ID:	20007
Version:	1.34
Type:	remote
Family:	Service detection
Published:	October 12, 2005
Modified:	April 4, 2022

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score: 9.8
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

In the news: true

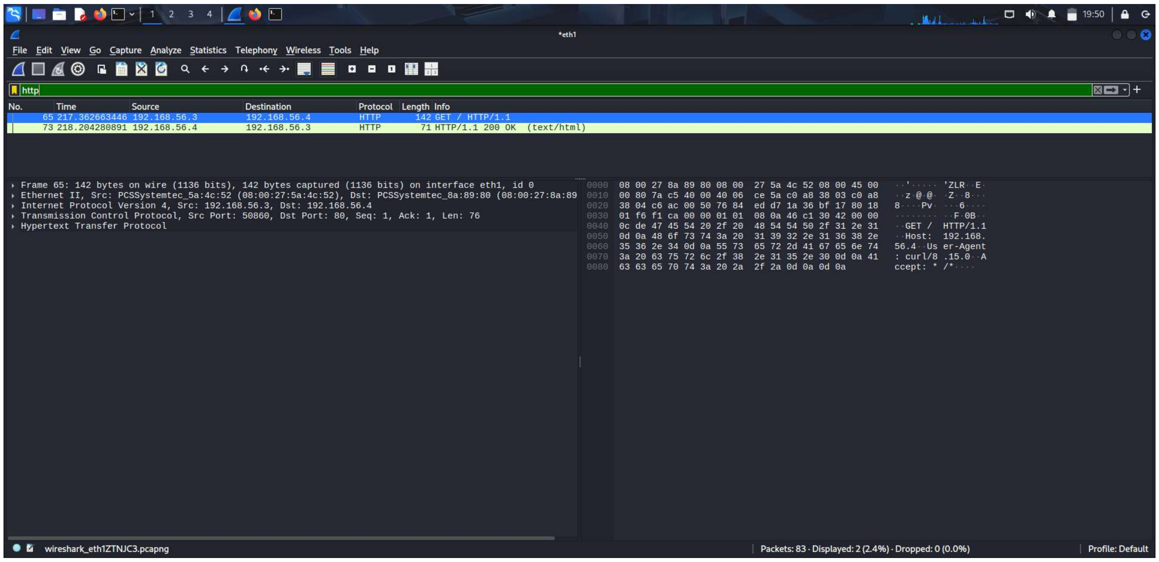
4. Packet Analysis with Wireshark

HTTP/FTP/DNS Traffic Capture

Command:

Captured unencrypted protocols for analysis.

Purpose: Analyze raw traffic.



*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
19:50

Filter: http

```
No.   Time           Source          Destination     Protocol  Length Info
   65 217.362663446  192.168.56.3    192.168.56.4    HTTP         142 GET / HTTP/1.1
   73 218.204280891  192.168.56.4    192.168.56.3    HTTP          71 HTTP/1.1 200 OK  (text/html)
```

```
› Frame 65: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface eth1, id 0
› Ethernet II, Src: PCSSystemtec_5a:4c:52 (08:00:27:5a:4c:52), Dst: PCSSystemtec_8a:89:80 (08:00:27:8a:89
› Internet Protocol Version 4, Src: 192.168.56.3, Dst: 192.168.56.4
› Transmission Control Protocol, Src Port: 50860, Dst Port: 80, Seq: 1, Ack: 1, Len: 76
› Hypertext Transfer Protocol
```

```
0000  08 00 27 8a 89 80 08 00  27 5a 4c 52 08 00 45 00   ··'·····  'ZLR··E·
0010  00 80 7a c5 40 00 40 06  ce 5a c0 a8 38 03 c0 a8   ··z·@·@·  ·Z··8···
0020  38 04 c6 ac 00 50 76 84  ed d7 1a 36 bf 17 80 18   8····Pv·  ···6····
0030  01 f6 f1 ca 00 00 01 01  08 0a 46 c1 30 42 00 00   ········  ··F·0B··
0040  0c de 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /   HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  31 39 32 2e 31 36 38 2e   ··Host:   192.168.
0060  35 36 2e 34 0d 0a 55 73  65 72 2d 41 67 65 6e 74   56.4··Us  er-Agent
0070  3a 20 63 75 72 6c 2f 38  2e 31 35 2e 30 0d 0a 41   : curl/8  .15.0··A
0080  63 63 65 70 74 3a 20 2a  2f 2a 0d 0a 0d 0a         ccept: *  /*····
```

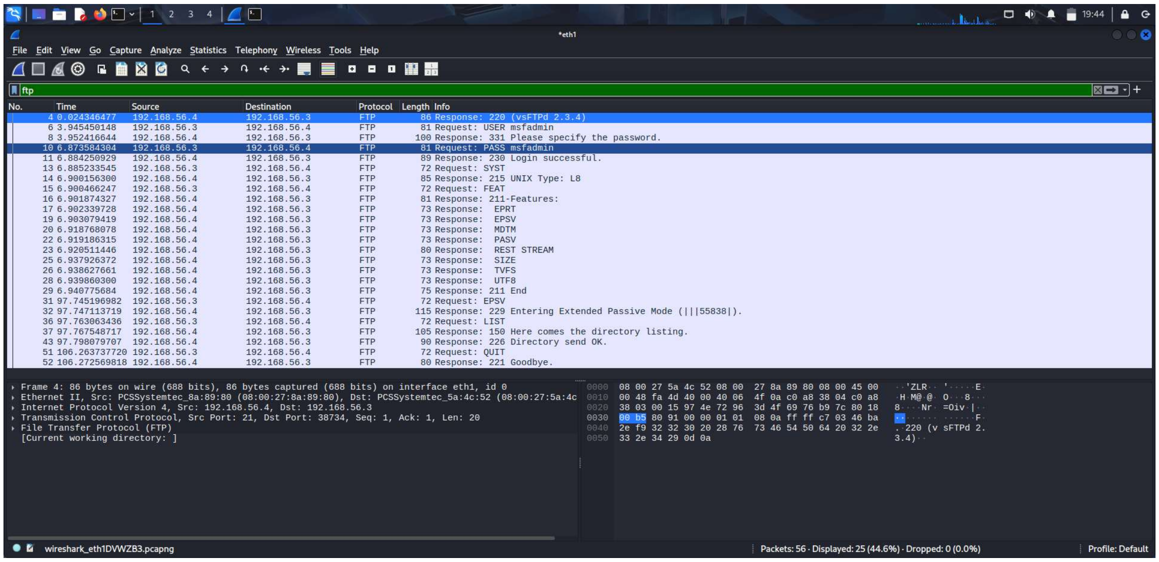
wireshark_eth1ZTNJC3.pcapng | Packets: 83 · Displayed: 2 (2.4%) · Dropped: 0 (0.0%) | Profile: Default

Extracting FTP Credentials

Command:

Filter: ftp

Purpose: Observed clear-text username and password in FTP session.



*eth1
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
19:44

Filter: ftp

```
No.   Time           Source          Destination     Protocol  Length Info
    4 0.024346477    192.168.56.4    192.168.56.3    FTP           86 Response: 220 (vsFTPd 2.3.4)
    6 3.945450148    192.168.56.3    192.168.56.4    FTP           81 Request: USER msfadmin
    8 3.952416644    192.168.56.4    192.168.56.3    FTP          100 Response: 331 Please specify the password.
   10 6.873584304    192.168.56.3    192.168.56.4    FTP           81 Request: PASS msfadmin
   11 6.884250929    192.168.56.4    192.168.56.3    FTP           89 Response: 230 Login successful.
   13 6.885233545    192.168.56.3    192.168.56.4    FTP           72 Request: SYST
   14 6.900156300    192.168.56.4    192.168.56.3    FTP           85 Response: 215 UNIX Type: L8
   15 6.900466247    192.168.56.3    192.168.56.4    FTP           72 Request: FEAT
   16 6.901874327    192.168.56.4    192.168.56.3    FTP           81 Response: 211-Features:
   17 6.902339728    192.168.56.4    192.168.56.3    FTP           73 Response:  EPRT
   19 6.903079419    192.168.56.4    192.168.56.3    FTP           73 Response:  EPSV
   20 6.918768078    192.168.56.4    192.168.56.3    FTP           73 Response:  MDTM
   22 6.919186315    192.168.56.4    192.168.56.3    FTP           73 Response:  PASV
   23 6.920511446    192.168.56.4    192.168.56.3    FTP           80 Response:  REST STREAM
   25 6.937926372    192.168.56.4    192.168.56.3    FTP           73 Response:  SIZE
   26 6.938627661    192.168.56.4    192.168.56.3    FTP           73 Response:  TVFS
   28 6.939860300    192.168.56.4    192.168.56.3    FTP           73 Response:  UTF8
   29 6.940775684    192.168.56.4    192.168.56.3    FTP           75 Response: 211 End
   31 97.745196982   192.168.56.3    192.168.56.4    FTP           72 Request: EPSV
   32 97.747113719   192.168.56.4    192.168.56.3    FTP          115 Response: 229 Entering Extended Passive Mode (|||55838|).
   36 97.763063436   192.168.56.3    192.168.56.4    FTP           72 Request: LIST
   37 97.767548717   192.168.56.4    192.168.56.3    FTP          105 Response: 150 Here comes the directory listing.
   43 97.798079707   192.168.56.4    192.168.56.3    FTP           90 Response: 226 Directory send OK.
   51 106.263737720  192.168.56.3    192.168.56.4    FTP           72 Request: QUIT
   52 106.272569818  192.168.56.4    192.168.56.3    FTP           80 Response: 221 Goodbye.
```

```
› Frame 4: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface eth1, id 0
› Ethernet II, Src: PCSSystemtec_8a:89:80 (08:00:27:8a:89:80), Dst: PCSSystemtec_5a:4c:52 (08:00:27:5a:4c
› Internet Protocol Version 4, Src: 192.168.56.4, Dst: 192.168.56.3
› Transmission Control Protocol, Src Port: 21, Dst Port: 38734, Seq: 1, Ack: 1, Len: 20
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  08 00 27 5a 4c 52 08 00  27 8a 89 80 08 00 45 00   ··'ZLR··  '·····E·
0010  00 48 fa 4d 40 00 40 06  4f 0a c0 a8 38 04 c0 a8   ·H·M@·@·  O···8···
0020  38 03 00 15 97 4e 72 96  3d 4f 69 76 b9 7c 80 18   8····Nr·  =Oiv·|··
0030  00 b5 80 91 00 00 01 01  08 0a ff ff c7 03 46 ba   ········  ······F·
0040  2e f9 32 32 30 20 28 76  73 46 54 50 64 20 32 2e   ··220 (v  sFTPd 2.
0050  33 2e 34 29 0d 0a                                  3.4)··
```

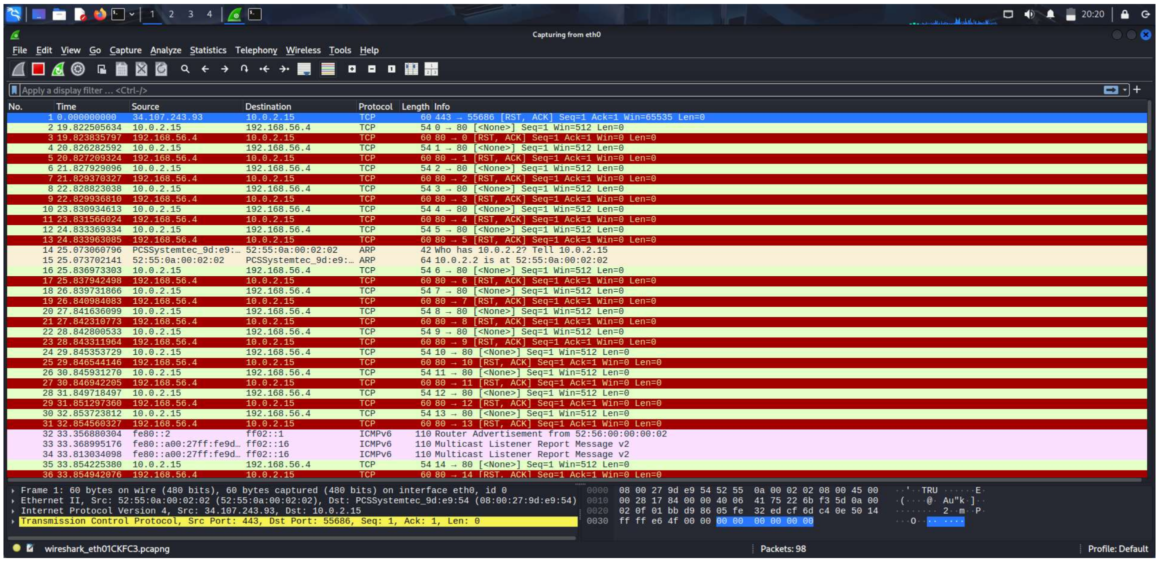
wireshark_eth1DVWZB3.pcapng | Packets: 56 · Displayed: 25 (44.6%) · Dropped: 0 (0.0%) | Profile: Default

SYN Flood Attack Simulation

Command:

```
sudo hping3 -S --flood -V -p 80 192.168.56.4
```

Purpose: Generate a SYN flood towards port 80 of target.
Wireshark Filter: tcp.flags.syn == 1 && tcp.flags.ack == 0



```
No.  Time            Source                 Destination            Protocol Length Info
   1 0.000000000     34.107.243.93          10.0.2.15              TCP      60 443 → 55686 [RST, ACK] Seq=1 Ack=1 Win=65535 Len=0
   2 19.822505634    10.0.2.15              192.168.56.4           TCP      54 0 → 80 [<None>] Seq=1 Win=512 Len=0
   3 19.823835797    192.168.56.4           10.0.2.15              TCP      60 80 → 0 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   4 20.826282592    10.0.2.15              192.168.56.4           TCP      54 1 → 80 [<None>] Seq=1 Win=512 Len=0
   5 20.827209324    192.168.56.4           10.0.2.15              TCP      60 80 → 1 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   6 21.827929096    10.0.2.15              192.168.56.4           TCP      54 2 → 80 [<None>] Seq=1 Win=512 Len=0
   7 21.829370327    192.168.56.4           10.0.2.15              TCP      60 80 → 2 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
   8 22.828823038    10.0.2.15              192.168.56.4           TCP      54 3 → 80 [<None>] Seq=1 Win=512 Len=0
   9 22.829936810    192.168.56.4           10.0.2.15              TCP      60 80 → 3 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  10 23.830934613    10.0.2.15              192.168.56.4           TCP      54 4 → 80 [<None>] Seq=1 Win=512 Len=0
  11 23.831566024    192.168.56.4           10.0.2.15              TCP      60 80 → 4 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  12 24.833369334    10.0.2.15              192.168.56.4           TCP      54 5 → 80 [<None>] Seq=1 Win=512 Len=0
  13 24.833963085    192.168.56.4           10.0.2.15              TCP      60 80 → 5 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  14 25.073060796    PCSSystemtec_9d:e9:…   52:55:0a:00:02:02      ARP      42 Who has 10.0.2.2? Tell 10.0.2.15
  15 25.073702141    52:55:0a:00:02:02      PCSSystemtec_9d:e9:…   ARP      64 10.0.2.2 is at 52:55:0a:00:02:02
  16 25.836973303    10.0.2.15              192.168.56.4           TCP      54 6 → 80 [<None>] Seq=1 Win=512 Len=0
  17 25.837942498    192.168.56.4           10.0.2.15              TCP      60 80 → 6 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  18 26.839731866    10.0.2.15              192.168.56.4           TCP      54 7 → 80 [<None>] Seq=1 Win=512 Len=0
  19 26.840984083    192.168.56.4           10.0.2.15              TCP      60 80 → 7 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  20 27.841636099    10.0.2.15              192.168.56.4           TCP      54 8 → 80 [<None>] Seq=1 Win=512 Len=0
  21 27.842310773    192.168.56.4           10.0.2.15              TCP      60 80 → 8 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  22 28.842800533    10.0.2.15              192.168.56.4           TCP      54 9 → 80 [<None>] Seq=1 Win=512 Len=0
  23 28.843311964    192.168.56.4           10.0.2.15              TCP      60 80 → 9 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  24 29.845353729    10.0.2.15              192.168.56.4           TCP      54 10 → 80 [<None>] Seq=1 Win=512 Len=0
  25 29.846544146    192.168.56.4           10.0.2.15              TCP      60 80 → 10 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  26 30.845931270    10.0.2.15              192.168.56.4           TCP      54 11 → 80 [<None>] Seq=1 Win=512 Len=0
  27 30.846942205    192.168.56.4           10.0.2.15              TCP      60 80 → 11 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  28 31.849718497    10.0.2.15              192.168.56.4           TCP      54 12 → 80 [<None>] Seq=1 Win=512 Len=0
  29 31.851297360    192.168.56.4           10.0.2.15              TCP      60 80 → 12 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  30 32.853723812    10.0.2.15              192.168.56.4           TCP      54 13 → 80 [<None>] Seq=1 Win=512 Len=0
  31 32.854560327    192.168.56.4           10.0.2.15              TCP      60 80 → 13 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
  32 33.356880304    fe80::2                ff02::1                ICMPv6  110 Router Advertisement from 52:56:00:00:00:02
  33 33.368995176    fe80::a00:27ff:fe9d…   ff02::16               ICMPv6  110 Multicast Listener Report Message v2
  34 33.813034098    fe80::a00:27ff:fe9d…   ff02::16               ICMPv6  110 Multicast Listener Report Message v2
  35 33.854225380    10.0.2.15              192.168.56.4           TCP      54 14 → 80 [<None>] Seq=1 Win=512 Len=0
  36 33.854942076    192.168.56.4           10.0.2.15              TCP      60 80 → 14 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
```

```
› Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0
› Ethernet II, Src: 52:55:0a:00:02:02 (52:55:0a:00:02:02), Dst: PCSSystemtec_9d:e9:54 (08:00:27:9d:e9:54)
› Internet Protocol Version 4, Src: 34.107.243.93, Dst: 10.0.2.15
› Transmission Control Protocol, Src Port: 443, Dst Port: 55686, Seq: 1, Ack: 1, Len: 0
```

```
0000  08 00 27 9d e9 54 52 55  0a 00 02 02 08 00 45 00   ··'··TRU ······E·
0010  00 28 17 84 00 00 40 06  41 75 22 6b f3 5d 0a 00   ·(····@· Au"k·]··
0020  02 0f 01 bb d9 86 05 fe  32 ed cf 6d c4 0e 50 14   ········ 2··m··P·
0030  ff ff e6 4f 00 00 00 00  00 00 00 00               ···O···· ····
```

wireshark_eth01CKFC3.pcapng | Packets: 98 | Profile: Default

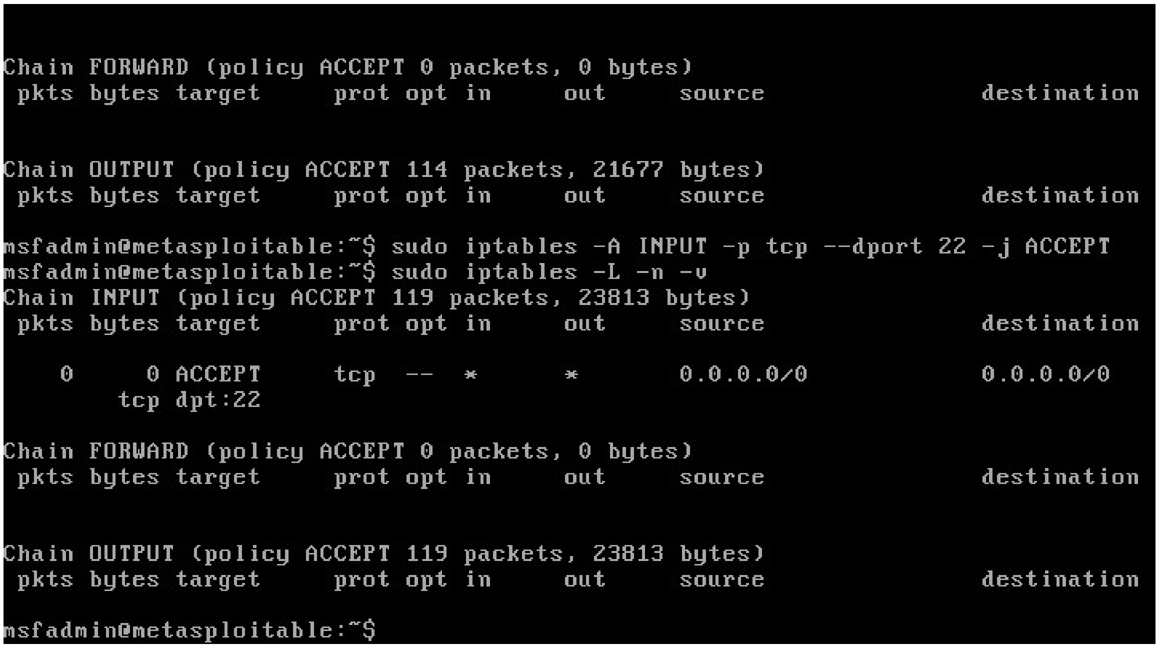
5. Firewall Basics (iptables)

Block Telnet (Port 23)

Command:

```
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

Purpose: Block access to Telnet service.



```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 114 packets, 21677 bytes)
 pkts bytes target     prot opt in     out     source               destination

msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -L -n -v
Chain INPUT (policy ACCEPT 119 packets, 23813 bytes)
 pkts bytes target     prot opt in     out     source               destination

    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            0.0.0.0/0
        tcp dpt:22

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination


Chain OUTPUT (policy ACCEPT 119 packets, 23813 bytes)
 pkts bytes target     prot opt in     out     source               destination

msfadmin@metasploitable:~$
```

Conclusion

- Passive Recon: WHOIS, nslookup, google dork, shodan gave us external info.
- Active Recon: Ping sweep, banner graping and nmap revealed open services like FTP, SSH, HTTP, MySQL, VNC.
- Vulnerability Scan: Nessus confirmed exploitable weaknesses on Metasploitable.
- Packet Analysis: Wireshark captured HTTP, FTP, and simulated SYN flood traffic.
- Firewall: iptables rules successfully demonstrated access restrictions.