Ex:No.: 1 Date:	Install Kali or Backtrack Linux / Metasploitable/ Windows XP

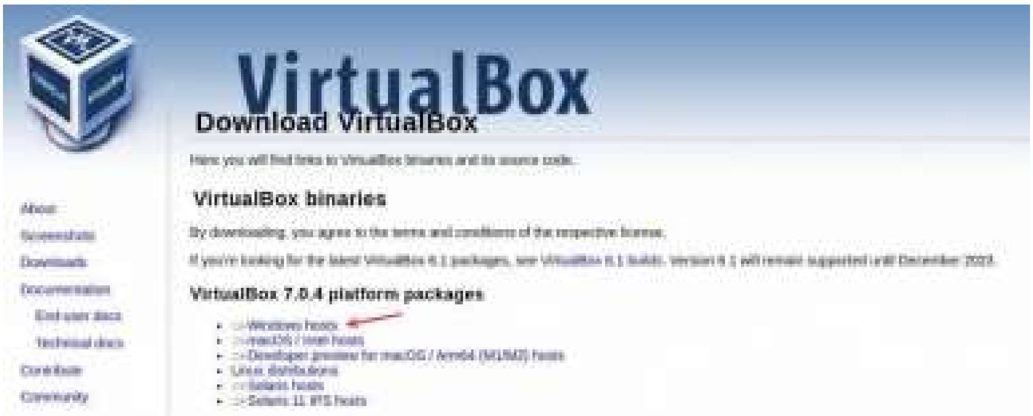
Aim:

To Install Kali Linux on Windows using Oracle Virtual Box

Procedure:

1. VirtualBox Installation:

- Proceed to download VirtualBox fromthe official website(https://www.virtualbox.org/wiki/Downloads)



Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

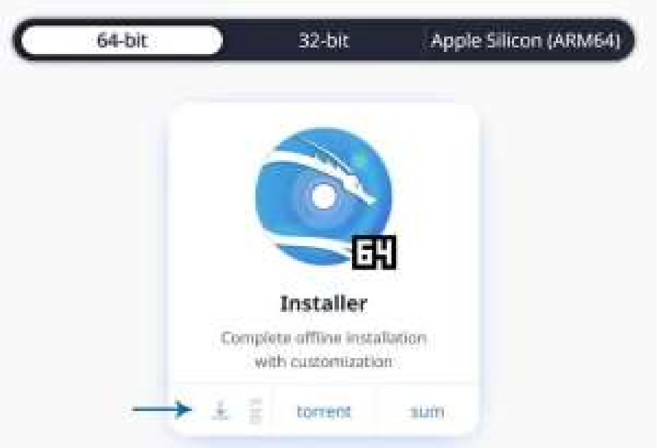
If you're looking for the latest VirtualBox 6.1 packages, see VirtualBox 6.1 builds. Version 6.1 will remain supported until December 2023.

VirtualBox 7.0.4 platform packages

- ⇒Windows hosts
- ⇒macOS / Intel hosts
- ⇒Developer preview for macOS / Arm64 (M1/M2) hosts
- Linux distributions
- ⇒Solaris hosts
- ⇒Solaris 11 IPS hosts

2. Downloading Kali Linux ISO Image:

- Following VirtualBox setup, obtain the Kali Linux ISO image from the provided link(https://www.kali.org/get-kali/#kali-installer-images)
- You have the option to either directly download the ISO or employ the torrent for the download.

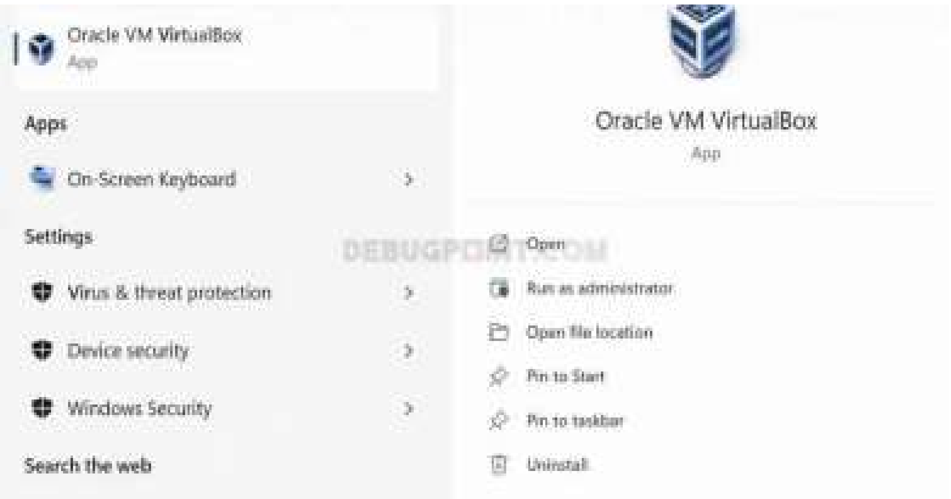


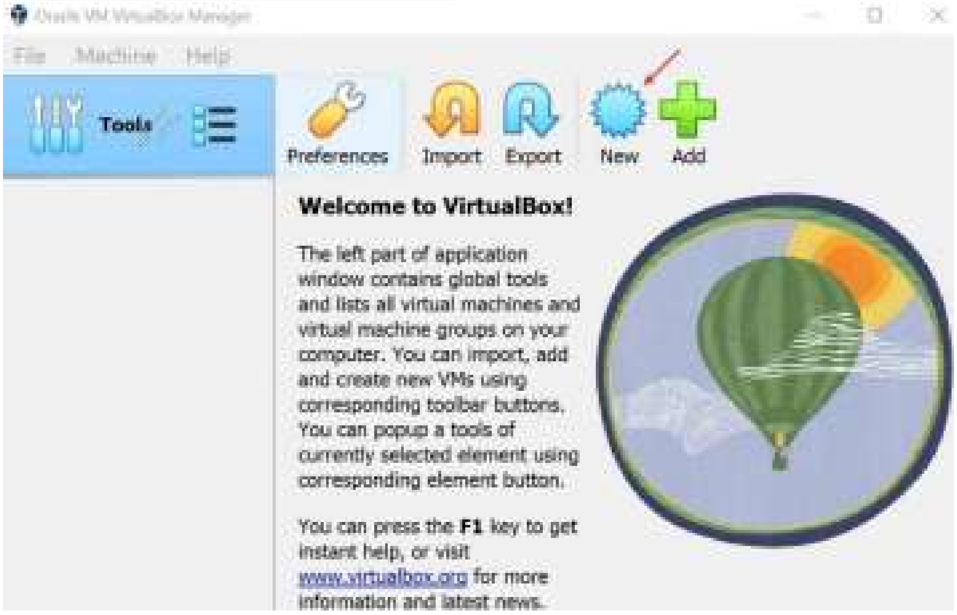
Installer

Complete offline installation with customization

3. Create a new virtual machine and configure storage, memory:

- With VirtualBox successfully installed, commence the application via the start menu.
- Select the "New" option to initiate the creation of a fresh virtual machine.





Welcome to VirtualBox!

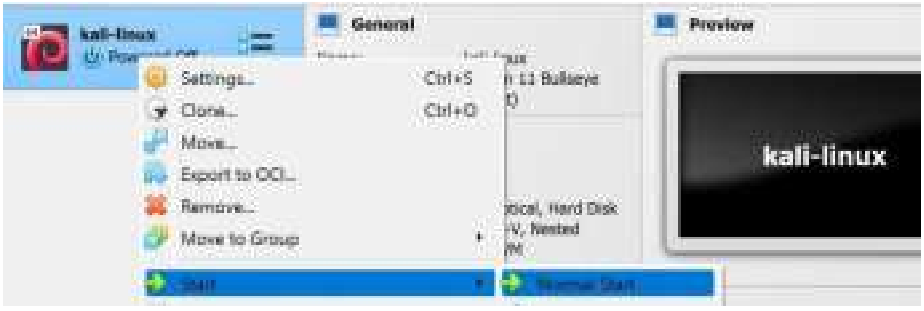
The left part of application window contains global tools and lists all virtual machines and virtual machine groups on your computer. You can import, add and create new VMs using corresponding toolbar buttons. You can popup a tools of currently selected element using corresponding element button.

You can press the **F1** key to get instant help, or visit www.virtualbox.org for more information and latest news.

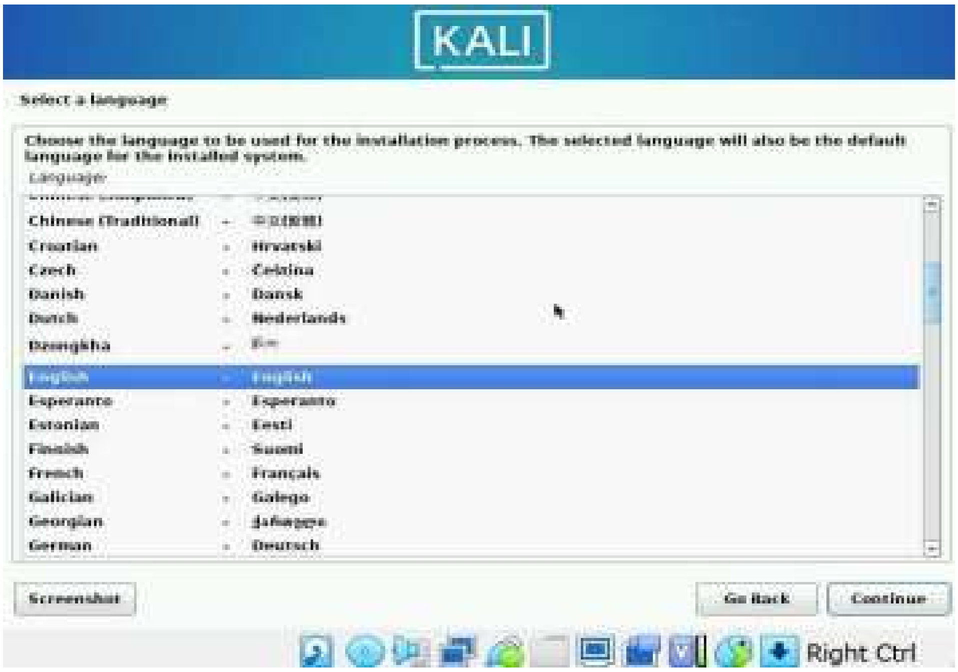
- Name your virtual machine.
- Keep the default folder name for the VM file.
- Browse and select the Kali Linux ISO file.
- Set the Type to Linux and Version to any 64-bit Linux.
- Configure the RAM (recommend 2-4 GB for an 8 GB RAM system).
- Choose 2 or 4 processors.
- In the Hard Disk section, keep the file location as is.
- Allocate at least 20-25 GB for Kali Linux installation.
- Select VDI as the hard disk file type.
- Do not select pre-allocate full size.
- Click "Finish" to create the virtual machine.

4. Install Kali Linux on the virtual machine:

- With the virtual machine configured, you can now proceed with the installation of Kali Linux. To do this, click the “Start” button in the toolbar orright-click > selectstart > normalstart.



- After a successful boot, you should see a screen showing various options for installing Kali Linux.
- Select **the first default option** to start the installer.



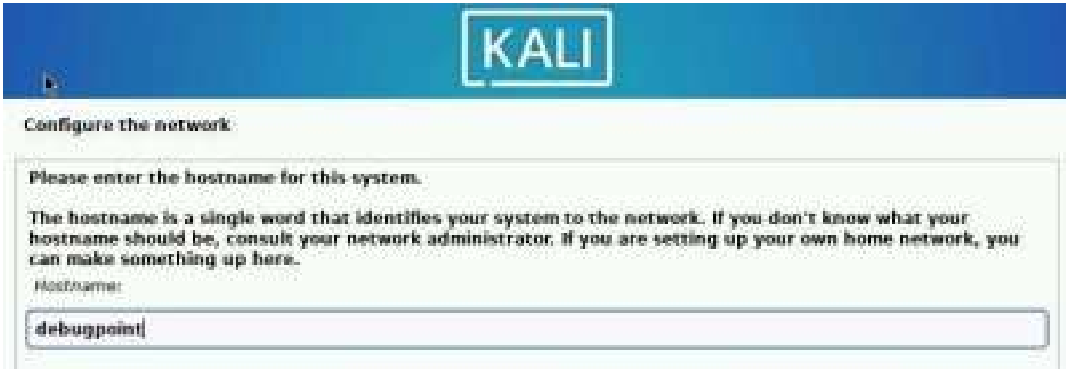
Select a language

Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.

Language:

Chinese (Traditional)	-	中文(繁體)
Croatian	-	Hrvatski
Czech	-	Čeština
Danish	-	Dansk
Dutch	-	Nederlands
Dzongkha	-	རྫོང་ཁ
English	-	English
Esperanto	-	Esperanto
Estonian	-	Eesti
Finnish	-	Suomi
French	-	Français
Galician	-	Galego
Georgian	-	ქართული
German	-	Deutsch

- In the next few screens,select Language,region, and other basic details per your location.
- Add any hostage you want.



Configure the network

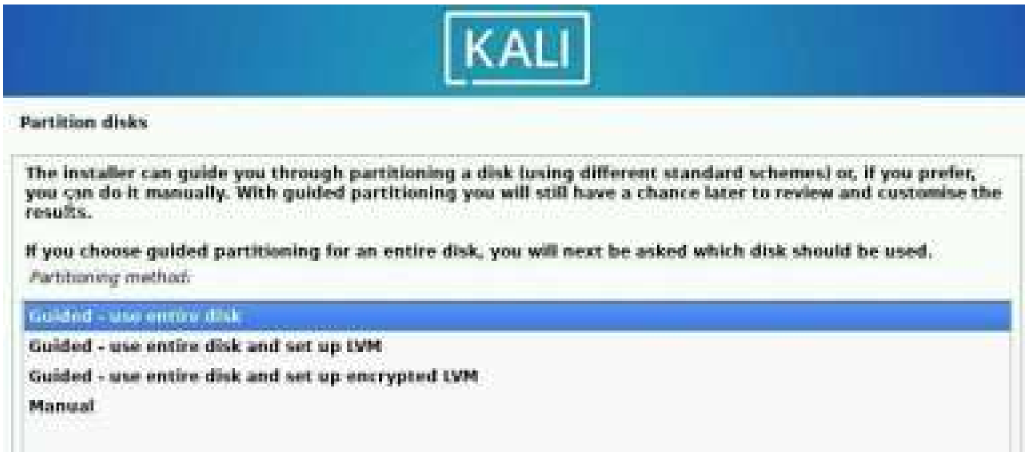
Please enter the hostname for this system.

The hostname is a single word that identifies your system to the network. If you don't know what your hostname should be, consult your network administrator. If you are setting up your own home network, you can make something up here.

Hostname:

debugpoint

- In the nextscreen, keep the domain name blank. Then give your name and user name(theloginname). Enter the password for that user.
- In the partition screen,select “guided – use the entire disk”. This is the best option for installing in VirtualBox. If installing it on the physical system, do not use this.



Partition disks

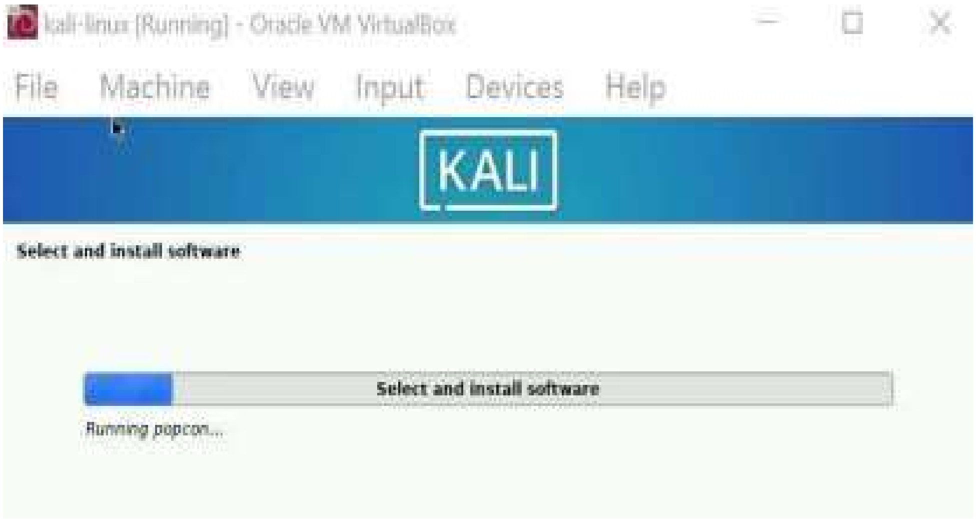
The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk
Guided - use entire disk and set up LVM
Guided - use entire disk and set up encrypted LVM
Manual

- Continue with the installation as per the on-screen instructions.

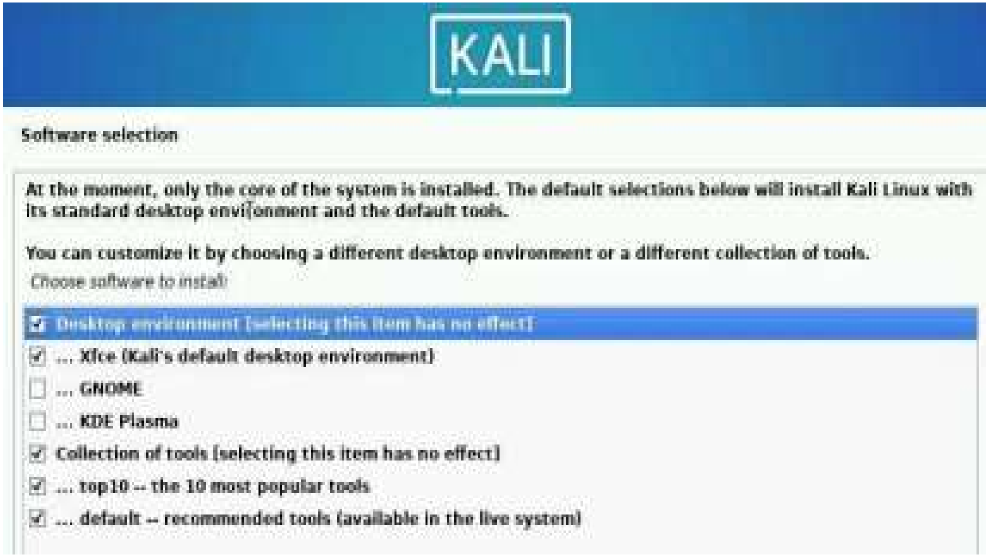

kali-linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Select and install software

Select and install software

Running popcon...

- When the following prompt appears,select the following ones(default), which feature the Xfce Desktop environment and key hacking tools. Hit enter to continue.



Software selection

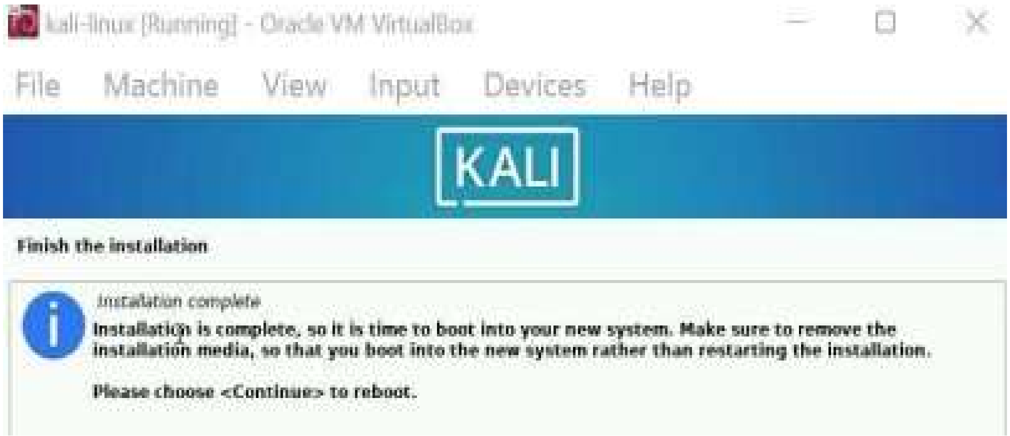
At the moment, only the core of the system is installed. The default selections below will install Kali Linux with its standard desktop environment and the default tools.

You can customize it by choosing a different desktop environment or a different collection of tools.

Choose software to install:

- ☑ Desktop environment [selecting this item has no effect]
- ☑ ... Xfce (Kali's default desktop environment)
- □ ... GNOME
- □ ... KDE Plasma
- ☑ Collection of tools [selecting this item has no effect]
- ☑ ... top10 -- the 10 most popular tools
- ☑ ... default -- recommended tools (available in the live system)

- Wait For The Installation to finish. Kali Linux installation VirtualBox will take a few minutes (approximately 10 minutes). While nearing the end of the installation,the installer will ask you about the GRUB installation. Answer Yes and choose the device /dev/sda and continue.



Finish the installation

Installation complete

Installation is complete, so it is time to boot into your new system. Make sure to remove the installation media, so that you boot into the new system rather than restarting the installation.

Please choose <Continue> to reboot.

- Click on RestartNow after the installation is complete. Waitfor a few seconds and you should be here on the login screen.
- Use the userid and password to log in. And you should see Kali Linux desktop isrunninginsideVirtualBox as VM in Windows.

Result:

The installation of Kali Linux on VirtualBox was successful, creating a safe space to explore ethical hacking tools and techniques.

Ex:No.: 2 Date:	**Practising the Basics of Reconnaissance in Ethical Hacking.**

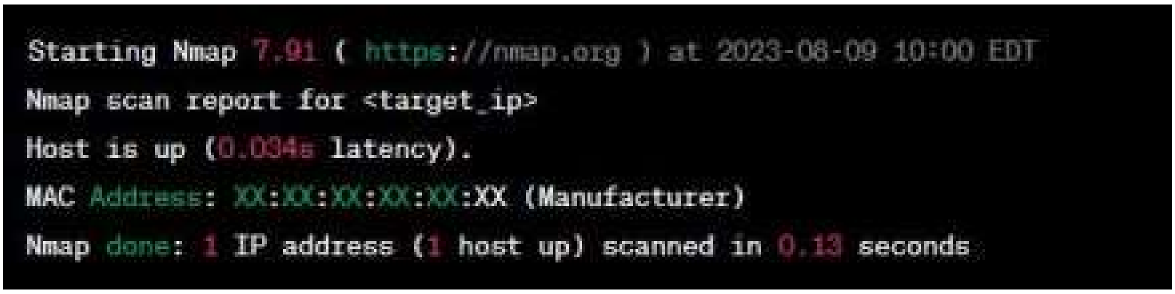
Aim:
To Practise the Basics of Reconnaissance in Ethical Hacking.

Terminal Commands and Their Use:

1. Ping Scan with Nmap:

- **Command:** nmap -sn <target_ip>
- **Use:** Perform a ping scan to determine which hosts are up in a given IP range.

Sample Output:

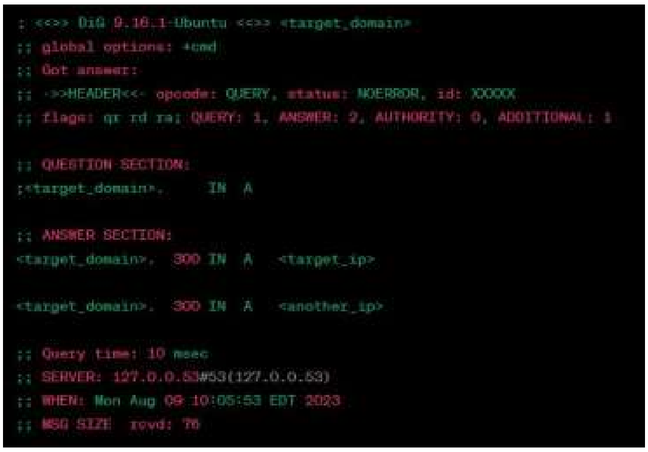


```
Starting Nmap 7.91 ( https://nmap.org ) at 2023-08-09 10:00 EDT
Nmap scan report for <target_ip>
Host is up (0.034s latency).
MAC Address: XX:XX:XX:XX:XX:XX (Manufacturer)
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

2. DNS Enumeration with Dig:

- **Command:** dig <target_domain>
- **Use:** Perform DNS enumeration to retrieve information about a target domain's DNS records

Sample Output:

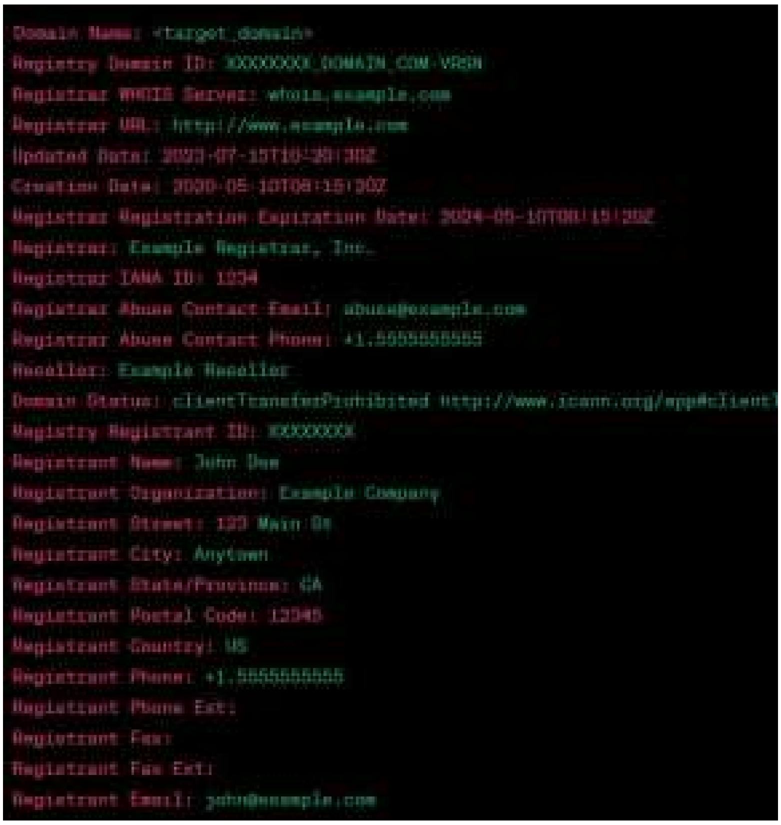


```
; <<>> DiG 9.16.1-Ubuntu <<>> <target_domain>
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: XXXXX
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;<target_domain>.      IN  A

;; ANSWER SECTION:
<target_domain>.  300 IN  A   <target_ip>

<target_domain>.  300 IN  A   <another_ip>

;; Query time: 10 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Mon Aug 09 10:05:53 EDT 2023
;; MSG SIZE  rcvd: 76
```

3. WHOIS Lookup:

- **Command:** whois <target_domain>
- **Use:** Retrieve registration and ownership information about a domain.

Sample Output:

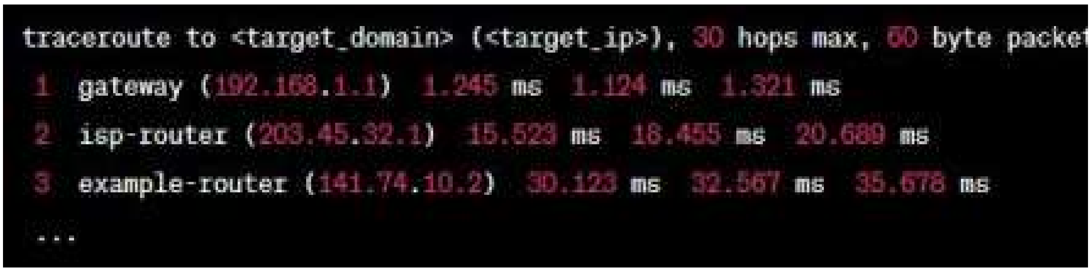


```
Domain Name: <target_domain>
Registry Domain ID: XXXXXXXX_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.example.com
Registrar URL: http://www.example.com
Updated Date: 2023-07-15T10:20:30Z
Creation Date: 2020-05-10T08:15:30Z
Registrar Registration Expiration Date: 2024-05-10T08:15:30Z
Registrar: Example Registrar, Inc.
Registrar IANA ID: 1234
Registrar Abuse Contact Email: abuse@example.com
Registrar Abuse Contact Phone: +1.5555555555
Reseller: Example Reseller
Domain Status: clientTransferProhibited http://www.icann.org/epp#client
Registry Registrant ID: XXXXXXXX
Registrant Name: John Doe
Registrant Organization: Example Company
Registrant Street: 123 Main St
Registrant City: Anytown
Registrant State/Province: CA
Registrant Postal Code: 12345
Registrant Country: US
Registrant Phone: +1.5555555555
Registrant Phone Ext:
Registrant Fax:
Registrant Fax Ext:
Registrant Email: john@example.com
```

4. Traceroute:

- **Command:** traceroute <target_domain>
- **Use:** Identify the path packets take from your system to the target, revealing intermediate routers' IP addresses.

Sample Output:



```
traceroute to <target_domain> (<target_ip>), 30 hops max, 60 byte packet
 1  gateway (192.168.1.1)  1.245 ms  1.124 ms  1.321 ms
 2  isp-router (203.45.32.1)  15.523 ms  18.455 ms  20.689 ms
 3  example-router (141.74.10.2)  30.123 ms  32.567 ms  35.678 ms
 ...
```

Result:
Thus, essential reconnaissance techniques in ethical hacking were practiced using terminal commands, successfully enabling the gathering of information about target IP addresses, domains, DNS records, and registration details.

Ex:No.: 3 Date:	**Using FOCA / SearchDiggity tools, extract metadata and expand the target list.**

Aim:

To understand how to extract metadata from a website using FOCA (Fingerprinting Organizations with Collected Archives) software.

Procedure:

1. Setting up SQL Server

- Open a web browser and navigate to the Microsoft SQL Server Express download page.
- Click on the 'Download' button to download the installer.
- Once downloaded, double-click on the installer file.
- Accept the terms and conditions.
- Select the installation type as "Basic" and proceed.
- The installer will take care of the rest. Wait for the installation to complete.

2. Installing FOCA Software

- Download FOCA from its official website or a trusted source.
- Once downloaded, locate the downloaded ZIP file and extract it.
- Open the extracted folder and double-click on FOCA.exe to launch the application.

3. Creating a New Project in FOCA

- Upon opening FOCA, click on 'New Project'.
- Name your project and in the 'Domain' field, enter the website from which you want to extract metadata.
- Click on 'Create Project'.

4. Searching and Downloading Documents

- Select the search engines you want FOCA to use.
- Choose the types of documents you want to search for (like PDF, DOC, PPT, etc.).
- Click on 'Search All'.
- A list of files related to your search will appear.
- Right-click on any listed file and choose 'Download All' to download all listed files.

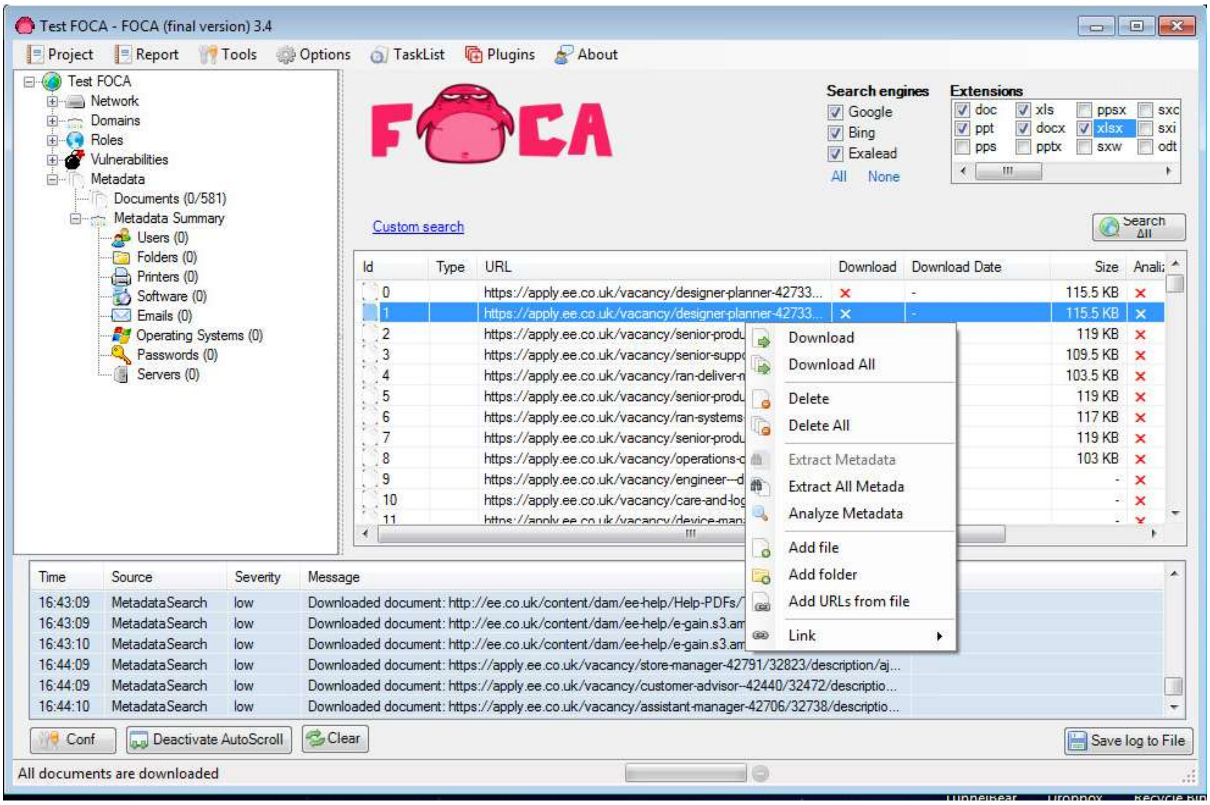
5. Extracting Metadata

- Once all files are downloaded, right-click again on any downloaded file in FOCA.
- Choose 'Extract All Metadata'.
- Wait for the process to complete.

6. Viewing Extracted Metadata

- On the left side of the FOCA interface, click on 'Metadata'.
- You will see a list of metadata information extracted from the downloaded files.

Output:



Id	Type	URL	Download	Download Date	Size	Anali:
0		https://apply.ee.co.uk/vacancy/designer-planner-42733...	✕	-	115.5 KB	✕
1		https://apply.ee.co.uk/vacancy/designer-planner-42733...	✕	-	115.5 KB	✕
2		https://apply.ee.co.uk/vacancy/senior-produ			119 KB	✕
3		https://apply.ee.co.uk/vacancy/senior-suppo			109.5 KB	✕
4		https://apply.ee.co.uk/vacancy/ran-deliver-m			103.5 KB	✕
5		https://apply.ee.co.uk/vacancy/senior-produ			119 KB	✕
6		https://apply.ee.co.uk/vacancy/ran-systems-			117 KB	✕
7		https://apply.ee.co.uk/vacancy/senior-produ			119 KB	✕
8		https://apply.ee.co.uk/vacancy/operations-c			103 KB	✕
9		https://apply.ee.co.uk/vacancy/engineer--d			-	✕
10		https://apply.ee.co.uk/vacancy/care-and-log			-	✕
11		https://apply.ee.co.uk/vacancy/device-man:			-	✕

```
Time      Source          Severity  Message
16:43:09  MetadataSearch  low       Downloaded document: http://ee.co.uk/content/dam/ee-help/Help-PDFs/
16:43:09  MetadataSearch  low       Downloaded document: http://ee.co.uk/content/dam/ee-help/e-gain.s3.am
16:43:10  MetadataSearch  low       Downloaded document: http://ee.co.uk/content/dam/ee-help/e-gain.s3.am
16:44:09  MetadataSearch  low       Downloaded document: https://apply.ee.co.uk/vacancy/store-manager-42791/32823/description/aj...
16:44:09  MetadataSearch  low       Downloaded document: https://apply.ee.co.uk/vacancy/customer-advisor--42440/32472/descriptio...
16:44:10  MetadataSearch  low       Downloaded document: https://apply.ee.co.uk/vacancy/assistant-manager-42706/32738/descriptio...
```

All documents are downloaded

Result:

Thus, extraction of metadata from a website using FOCA (Fingerprinting Organizations with Collected Archives) software has been successfully done.

Ex:No.: 4 Date:	**Aggregates information from public databases using online free tools like Paterva‘s Maltego.**

Aim:

The aim of this lab is to teach you how to use Paterva's Maltego for aggregating information from public databases.

Procedure:

1. Installing Maltego

- Visit the official Maltego website to download the software. Make sure to choose the correct version for your operating system.
- Install Maltego by following the on-screen instructions.
- Once the installation is complete, open the Maltego application.
- Register or log in to your Maltego account.

2. Creating a New Graph

- Click on the 'File' menu in the Maltego interface and then select 'New'.
- A new graph window will open, which will be your workspace for this session.

3. Basic Entity Search

- Drag and drop an entity type (like "Domain", "Email Address", etc.) from the Entity Palette on the left into the graph.
- Double-click on the entity and enter the specific domain or email address you want to investigate.

4. Run a Transform

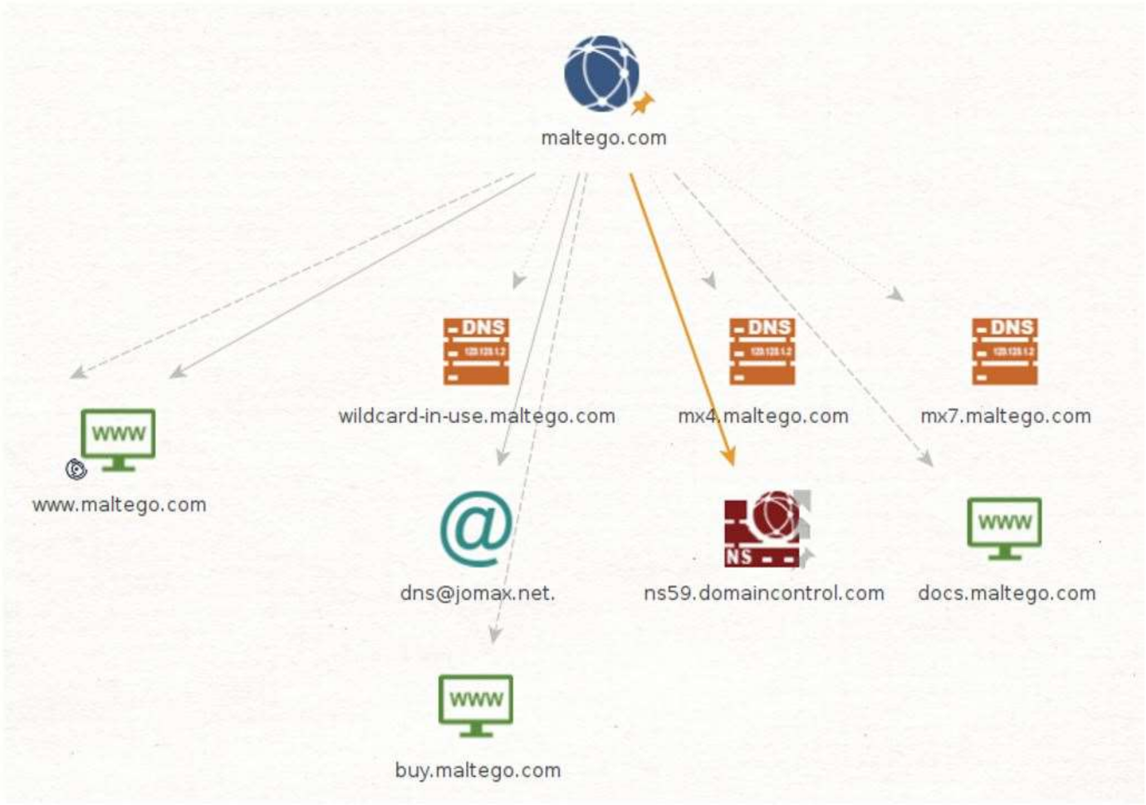
- Right-click on the entity you've placed on the graph.
- From the 'Run Transform' menu, select an appropriate transform. For example, you might choose "To Email [Using Search Engine]" for an email entity.
- Maltego will execute the transform and provide you with new entities connected to your original entity.

5. Exploring and Aggregating Information

- Continue to run more transforms on the new entities that appear on your graph to gather more information.
- You can adjust your view, zoom in/out, and rearrange entities as needed for better understanding.

- Aggregated data might include things like associated social media accounts, related websites, IP addresses, etc.

Output:



Result:

Thus, Information Aggregation with Paterva's Maltego has been successfully done and executed.

Ex:No.: 5 **Date:**	**Information gathering using tools like Robtex.**

Aim:

The aim of this lab exercise is to understand how to gather information on domains, IP addresses, and networks using Robtex, an online tool that provides various kinds of data for network research.

Procedure:

1. Accessing Robtex

- Open your web browser and go to the Robtex website by navigating to https://www.robtex.com/.
- You will see a search bar on the main page, where you can enter the domain name, IP address, or network that you wish to investigate.

2. Domain Lookup

- In the Robtex search bar, type the domain you want to investigate. For example, example.com.
- Click the 'Search' button or press Enter.
- Robtex will return a wealth of information about the domain, including DNS records, IP address data, server location, and more.

3. IP Address Lookup

- In the Robtex search bar, enter the IP address you want to investigate.
- Hit the 'Search' button or press Enter.
- Robtex will provide data related to the IP address, such as the owning organization, geolocation, ASN information, and potentially linked domains.

4. ASN Lookup

If you want to search for an Autonomous System Number (ASN), enter it into the search bar.

Press the 'Search' button.

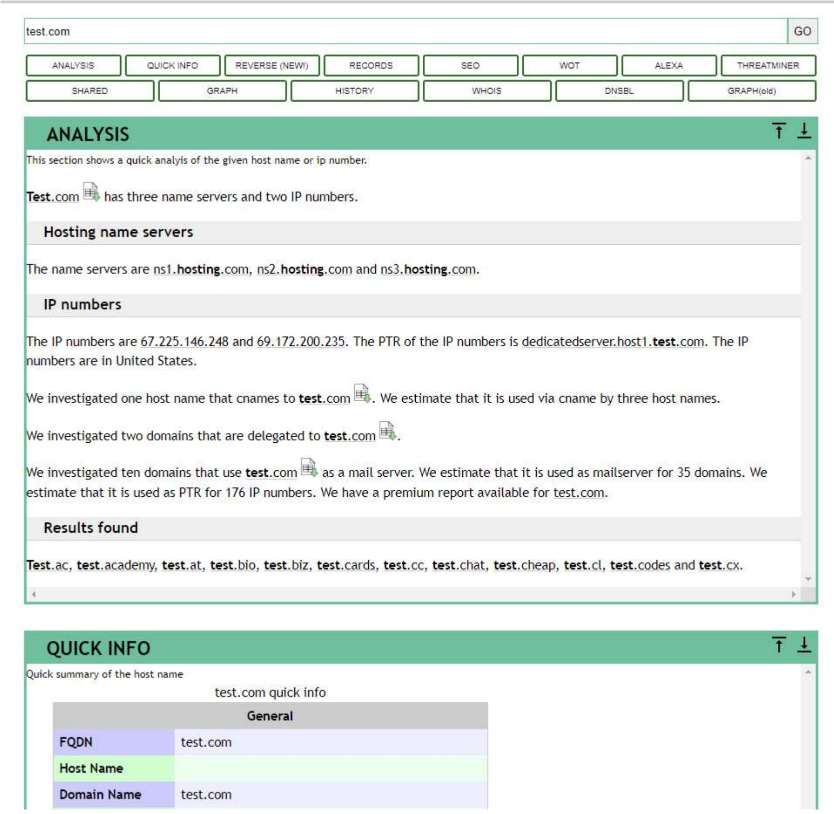
Information like AS routes, IP ranges, and associated domains will be displayed.

5. Understanding and Analyzing Data

- Take your time to go through the different tabs and sections that Robtex offers for each type of search. This can include but is not limited to:
    - DNS records
    - Mail server records

    - Domain siblings and subdomains
    - Shared IPs
    - ASN information
- Each section can offer valuable insights into the domain, IP, or network you are investigating.

Output:



ANALYSIS

This section shows a quick analyis of the given host name or ip number.

Test.com has three name servers and two IP numbers.

Hosting name servers

The name servers are ns1.hosting.com, ns2.hosting.com and ns3.hosting.com.

IP numbers

The IP numbers are 67.225.146.248 and 69.172.200.235. The PTR of the IP numbers is dedicatedserver.host1.test.com. The IP numbers are in United States.

We investigated one host name that cnames to test.com. We estimate that it is used via cname by three host names.

We investigated two domains that are delegated to test.com.

We investigated ten domains that use test.com as a mail server. We estimate that it is used as mailserver for 35 domains. We estimate that it is used as PTR for 176 IP numbers. We have a premium report available for test.com.

Results found

Test.ac, test.academy, test.at, test.bio, test.biz, test.cards, test.cc, test.chat, test.cheap, test.cl, test.codes and test.cx.

QUICK INFO

Quick summary of the host name

test.com quick info

General	
FQDN	test.com
Host Name	
Domain Name	test.com

Result:

Thus, the gathering of information using Robtex has been successfully done and executed.

Ex:No.: 6 **Date:**	**Scanning a Target Using Nessus**

Aim:

To understand how to use Nessus for vulnerability scanning on a target system or network.

Procedure:

1. Initial Setup and Login

- Open Nessus by navigating to the application via your program menu or using the desktop shortcut if available.
- If you're using Nessus for the first time, you will need to activate it. You can get an activation code by registering on the Tenable website.
- Once activated, log in to the Nessus interface using your credentials.

2. Updating Plugins

- Before starting your scan, it's recommended to update Nessus plugins to get the latest vulnerability checks.
- Usually, Nessus updates its plugins automatically, but you can manually update them by navigating to the 'Plugins' section and clicking 'Update'.

3. Creating a New Scan

- Once logged in, click on the 'New Scan' button on the dashboard.
- You will be presented with various scanning templates like Basic Network Scan, Advanced Scan, etc. Choose the one that suits your needs.
- Name your scan and add a description for reference.

4. Configuring Scan Settings

- In the 'Targets' field, enter the IP addresses or hostnames of the systems you want to scan. Make sure you have authorization to scan these targets.
- You can specify advanced settings like scan schedules, notifications, and other preferences depending on the type of scan you have chosen.
- If necessary, you can also configure authentication settings to scan internal elements of the target system.

5. Starting the Scan

- After configuring all the settings, click on the 'Save' button to save your scan settings.
- To initiate the scan, click on the 'Launch' button.

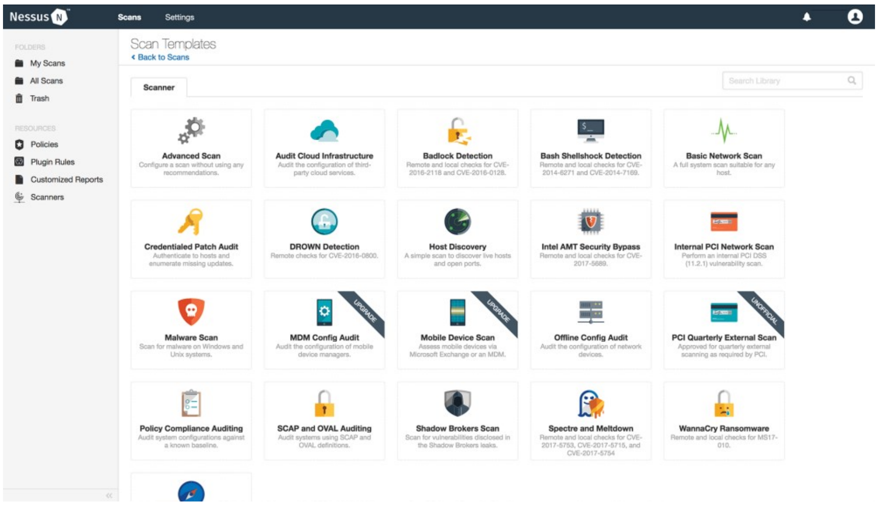
6. Monitoring the Scan

- Once the scan is initiated, you can monitor its progress in the dashboard.
- Nessus will display various metrics and statistics related to the scan, like the number of vulnerabilities found, the severity levels, etc.

7. Analyzing the Results

- After the scan is completed, click on it to view the detailed report.
- The report will categorize vulnerabilities as Critical, High, Medium, Low, or Info based on their severity.
- You can click on each vulnerability to get more details, like a description of the issue, the impact, and recommended solutions.

Output:



Advanced Scan Configure a scan without using any recommendations.

Audit Cloud Infrastructure Audit the configuration of third-party cloud services.

Badlock Detection Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

Bash Shellshock Detection Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

Basic Network Scan A full system scan suitable for any host.

Credentialed Patch Audit Authenticate to hosts and enumerate missing updates.

DROWN Detection Remote checks for CVE-2016-0800.

Host Discovery A simple scan to discover live hosts and open ports.

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Internal PCI Network Scan Perform an internal PCI DSS (11.2.1) vulnerability scan.

Malware Scan Scan for malware on Windows and Unix systems.

MDM Config Audit Audit the configuration of mobile device managers.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.

Offline Config Audit Audit the configuration of network devices.

PCI Quarterly External Scan Approved for quarterly external scanning as required by PCI.

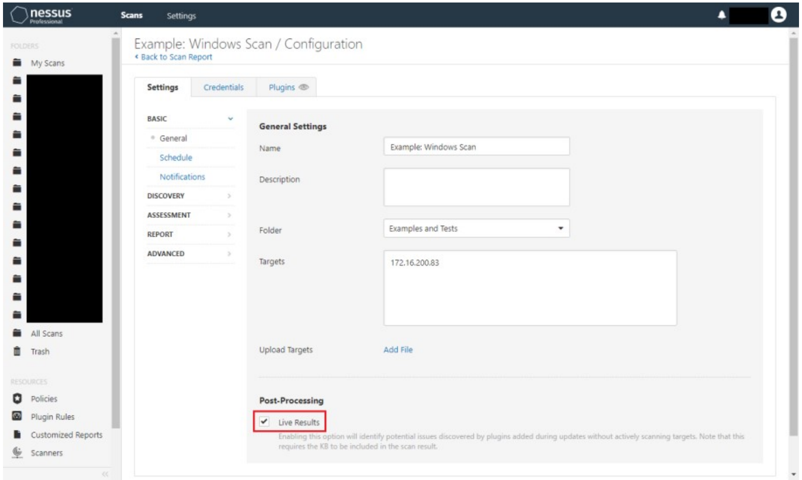
Policy Compliance Auditing Audit system configurations against a known baseline.

SCAP and OVAL Auditing Audit systems using SCAP and OVAL definitions.

Shadow Brokers Scan Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware Remote and local checks for MS17-010.



Example: Windows Scan / Configuration

‹ Back to Scan Report

General Settings

Name: Example: Windows Scan

Description:

Folder: Examples and Tests

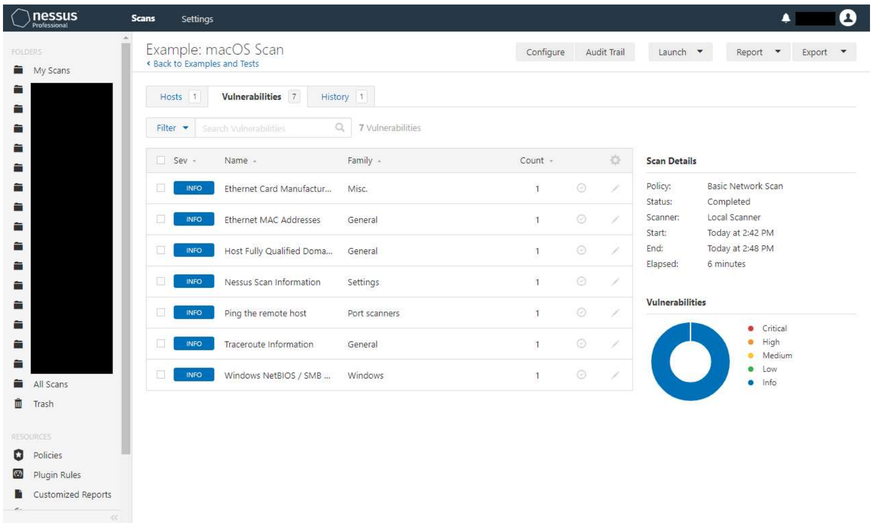
Targets: 172.16.200.83

Upload Targets: Add File

Post-Processing

☑ Live Results

Enabling this option will identify potential issues discovered by plugins added during updates without actively scanning targets. Note that this requires the KB to be included in the scan result.



Example: macOS Scan

‹ Back to Examples and Tests

7 Vulnerabilities

Sev	Name	Family	Count
INFO	Ethernet Card Manufactur...	Misc.	1
INFO	Ethernet MAC Addresses	General	1
INFO	Host Fully Qualified Doma...	General	1
INFO	Nessus Scan Information	Settings	1
INFO	Ping the remote host	Port scanners	1
INFO	Traceroute Information	General	1
INFO	Windows NetBIOS / SMB ...	Windows	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 2:42 PM
End:	Today at 2:48 PM
Elapsed:	6 minutes

Vulnerabilities

Result:

Thus, the Scanning a Target Using Nessus has been successfully done and executed.

Ex:No.: 7 **Date:**	**View and capture network traffic using Wireshark.**

Aim:

To View and capture network traffic using Wireshark.

Procedure:

1. Download Wireshark:

- Visit the official Wireshark download page at https://www.wireshark.org/download.html.
- Download the appropriate version for your operating system (Windows, macOS, or Linux).

2. Install Wireshark:

- Run the downloaded installer.
- Follow the installation wizard's instructions.

3. Launch Wireshark:

- Once the installation is complete, open the Wireshark application.

4. Select Network Interface:

- Wireshark will display a list of available network interfaces.
- Choose the network interface through which you want to capture traffic (e.g., Ethernet or Wi-Fi).

5. Start Capturing Traffic:

- **Click on the "Start" or "Capture" button to begin capturing network traffic.**

6. Analyze Captured Packets:

- While capturing, you can analyze the live stream of network packets.
- Use filters and search features in Wireshark to focus on specific types of packets or protocols.

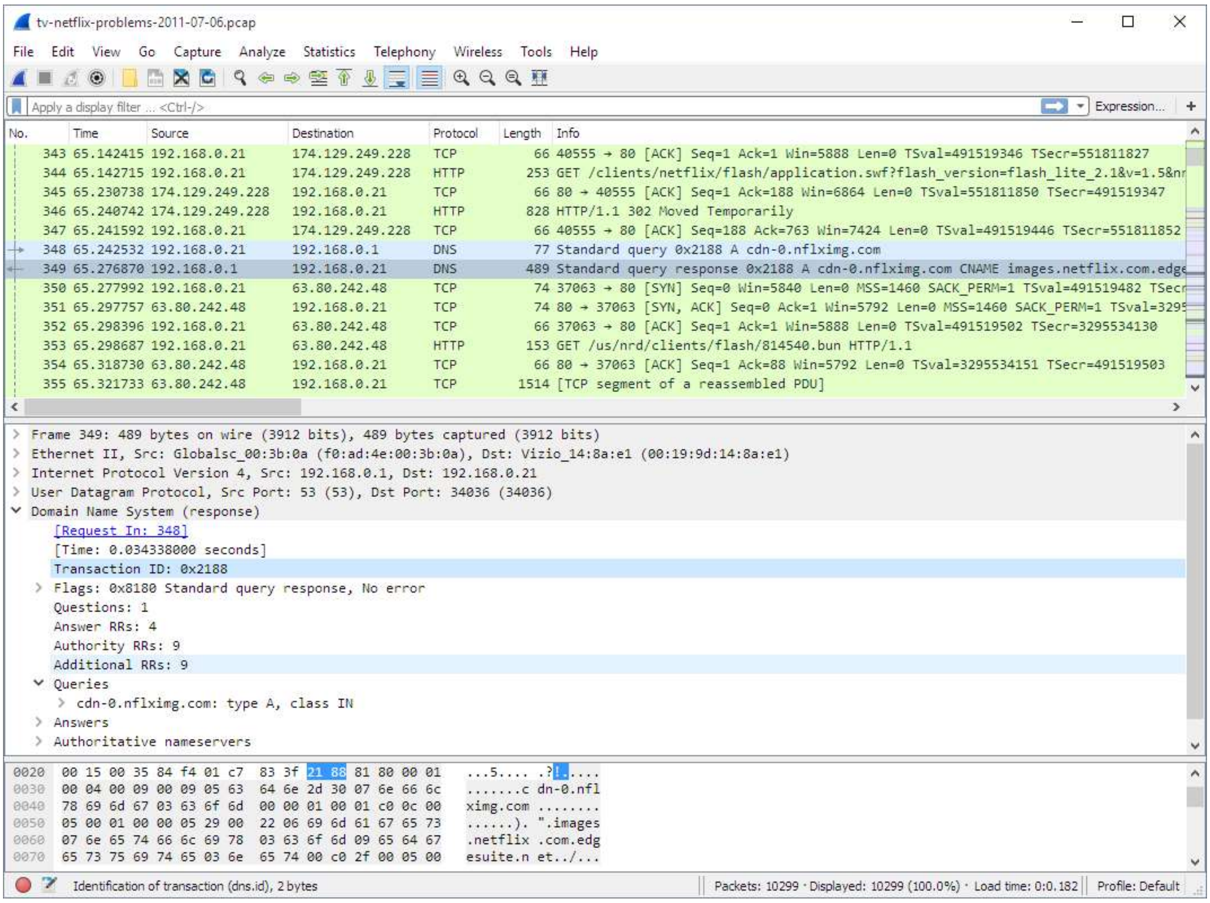
7. Stop Capturing:

- When you have captured enough data or want to stop the capture, click the "Stop" or "Capture" button again.

8. View Captured Packets:

- After stopping the capture, you can view the captured packets.
- Click on any packet to see its details, including source and destination IP addresses, protocols, and packet content.

Output:


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes | Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

Result:

Thus, Viewing and capturing network traffic using Wireshark has been successfully done and executed

Ex:No.: 8 Date:	**Automate dig for vulnerabilities and match exploits using Armitage FOCA**

Aim:

To Automate dig for vulnerabilities and match exploits using Armitage FOCA

Procedure:

1. Scanning and Reconnaissance:

- Launch Kali Linux and open Armitage.
- Perform network scanning using tools like Nmap to identify open ports and active hosts.
- Utilize Armitage to import the scan results and create a target list.

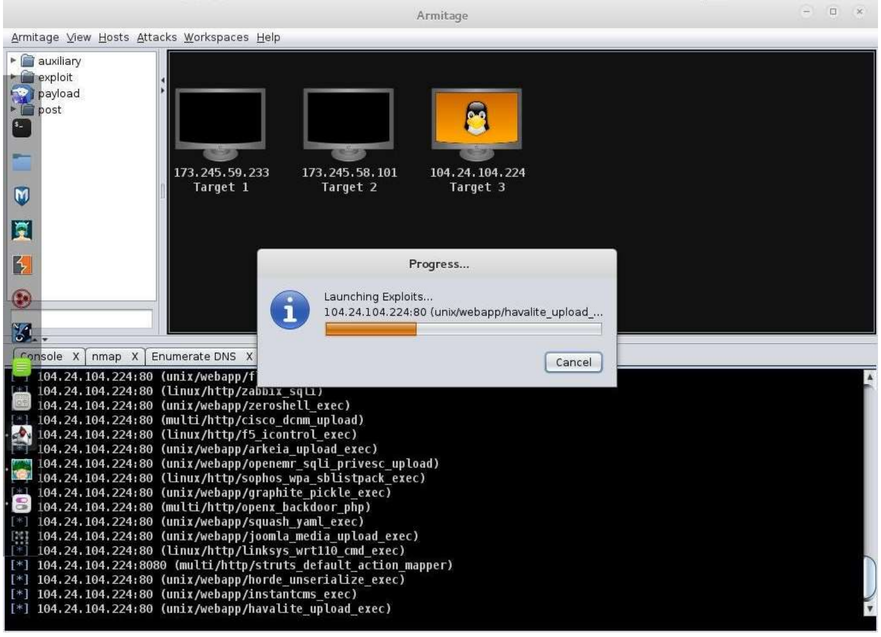
2. Vulnerability Analysis:

- Conduct vulnerability scanning on the target hosts using Armitage's built-in features.
- Identify potential vulnerabilities in the scanned systems, such as outdated software, weak passwords, or misconfigurations.
- Use FOCA (Fingerprinting Organizations with Collected Archives) to gather information about the target organization's documents and metadata.

3. Exploit and Attack:

- In Armitage, explore available exploits and payloads for the identified vulnerabilities.
- Select an appropriate exploit and payload combination for the target system.
- Launch the attack on the target system.

Output:



Progress...

Launching Exploits...
104.24.104.224:80 (unix/webapp/havalite_upload_...

```
[*] 104.24.104.224:80 (unix/webapp/f
[*] 104.24.104.224:80 (linux/http/zabbix_sqli)
[*] 104.24.104.224:80 (unix/webapp/zeroshell_exec)
[*] 104.24.104.224:80 (multi/http/cisco_dcnm_upload)
[*] 104.24.104.224:80 (linux/http/f5_icontrol_exec)
[*] 104.24.104.224:80 (unix/webapp/arkeia_upload_exec)
[*] 104.24.104.224:80 (unix/webapp/openemr_sqli_privesc_upload)
[*] 104.24.104.224:80 (linux/http/sophos_wpa_sblistpack_exec)
[*] 104.24.104.224:80 (unix/webapp/graphite_pickle_exec)
[*] 104.24.104.224:80 (multi/http/openx_backdoor_php)
[*] 104.24.104.224:80 (unix/webapp/squash_yaml_exec)
[*] 104.24.104.224:80 (unix/webapp/joomla_media_upload_exec)
[*] 104.24.104.224:80 (linux/http/linksys_wrt110_cmd_exec)
[*] 104.24.104.224:8080 (multi/http/struts_default_action_mapper)
[*] 104.24.104.224:80 (unix/webapp/horde_unserialize_exec)
[*] 104.24.104.224:80 (unix/webapp/instantcms_exec)
[*] 104.24.104.224:80 (unix/webapp/havalite_upload_exec)
```

Result:

Thus, Automate dig for vulnerabilities and match exploits using Armitage FOCA has been successfully done.