

PRACTICAL 1

AIM: Network scanning and reconnaissance using Nmap and other tools to identify open ports, operating systems and potential vulnerabilities.

- Target IP: 10.10.15.60
- Nmap: Scan the Open ports.
- Command: nmap 10.10.15.60

The screenshot shows the Zenmap interface with the following details:

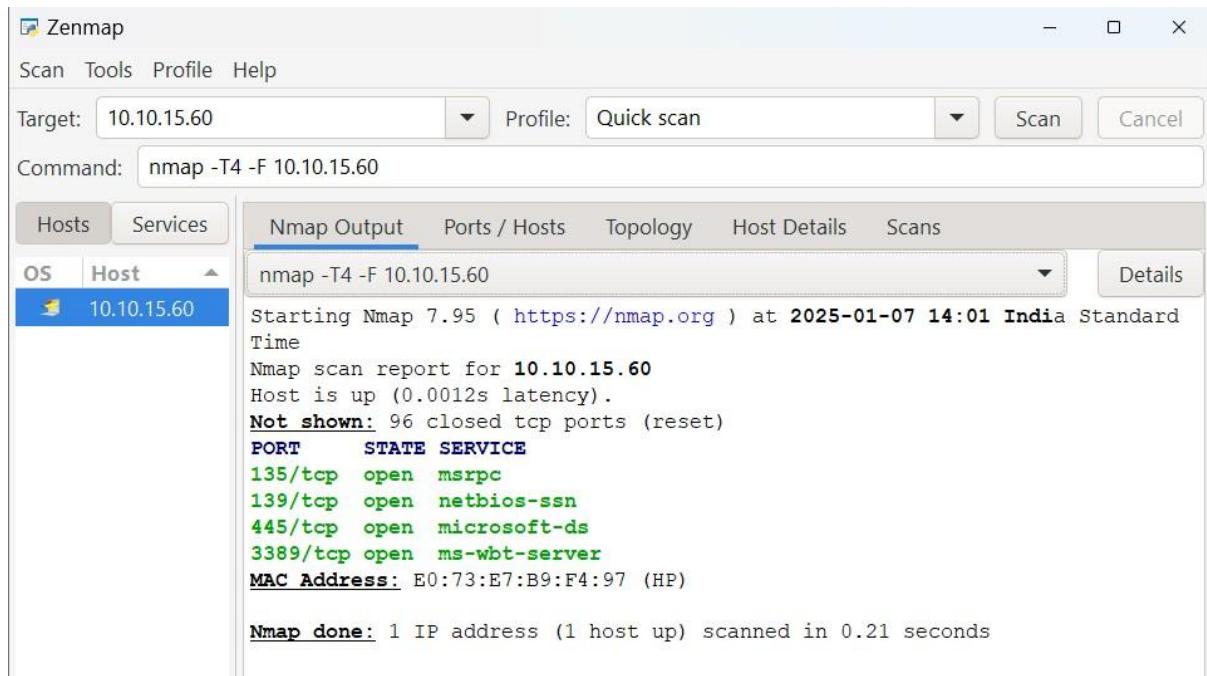
- Target:** 10.10.15.60
- Command:** nmap 10.10.15.60
- Selected Tab:** Nmap Output
- Host List:** OS | Host ▾
10.10.15.60
- Scan Results (Nmap Output):**

```
nmap 10.10.15.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-07 14:06 India Standard Time
Nmap scan report for 10.10.15.60
Host is up (0.00016s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
1521/tcp   open  oracle
3389/tcp   open  ms-wbt-server
MAC Address: E0:73:E7:B9:F4:97 (HP)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

- Quick scan :

Command : nmap -T4 -F 10.10.15.60



Zenmap

Scan Tools Profile Help

Target: 10.10.15.60 Profile: Quick scan Scan Cancel

Command: nmap -T4 -F 10.10.15.60

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host ▾ 10.10.15.60

nmap -T4 -F 10.10.15.60

Starting Nmap 7.95 (https://nmap.org) at 2025-01-07 14:01 India Standard Time

Nmap scan report for 10.10.15.60

Host is up (0.0012s latency).

Not shown: 96 closed tcp ports (reset)

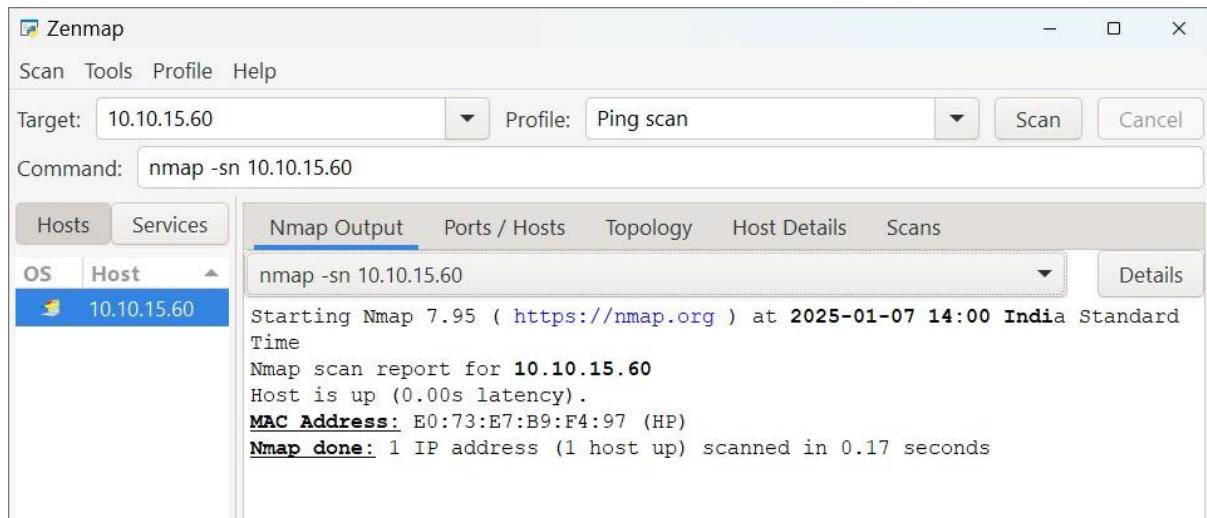
PORT	STATE	SERVICE
135/tcp	open	msrpc
139/tcp	open	netbios-ssn
445/tcp	open	microsoft-ds
3389/tcp	open	ms-wbt-server

MAC Address: E0:73:E7:B9:F4:97 (HP)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds

- Ping scan :

Command : nmap -sn 10.10.15.60



Zenmap

Scan Tools Profile Help

Target: 10.10.15.60 Profile: Ping scan Scan Cancel

Command: nmap -sn 10.10.15.60

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host ▾ 10.10.15.60

nmap -sn 10.10.15.60

Starting Nmap 7.95 (https://nmap.org) at 2025-01-07 14:00 India Standard Time

Nmap scan report for 10.10.15.60

Host is up (0.00s latency).

MAC Address: E0:73:E7:B9:F4:97 (HP)

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

- Intense scan :

Command : nmap -T4 -A -v 10.10.15.60

The screenshot shows the Zenmap interface with the following configuration:

- Target: 10.10.15.60
- Profile: Intense scan
- Command: nmap -T4 -A -v 10.10.15.60

The main window displays the Nmap Output tab, which shows the following log output:

```
nmap -T4 -A -v 10.10.15.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-07 14:00 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:00
Completed NSE at 14:00, 0.00s elapsed
Initiating NSE at 14:00
Completed NSE at 14:00, 0.00s elapsed
Initiating NSE at 14:00
Completed NSE at 14:00, 0.00s elapsed
Initiating ARP Ping Scan at 14:00
Scanning 10.10.15.60 [1 port]
Completed ARP Ping Scan at 14:00, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:00
Completed Parallel DNS resolution of 1 host. at 14:00, 0.07s elapsed
Initiating SYN Stealth Scan at 14:00
Scanning 10.10.15.60 [1000 ports]
Discovered open port 445/tcp on 10.10.15.60
Discovered open port 3389/tcp on 10.10.15.60
Discovered open port 139/tcp on 10.10.15.60
Discovered open port 135/tcp on 10.10.15.60
Discovered open port 1521/tcp on 10.10.15.60
Discovered open port 902/tcp on 10.10.15.60
Discovered open port 912/tcp on 10.10.15.60
Completed SYN Stealth Scan at 14:00, 0.09s elapsed (1000 total ports)
Initiating Service scan at 14:00
Scanning 7 services on 10.10.15.60
Completed Service scan at 14:01, 11.04s elapsed (7 services on 1 host)
Initiating OS detection (try #1) against 10.10.15.60
Retrying OS detection (try #2) against 10.10.15.60
Retrying OS detection (try #3) against 10.10.15.60
Retrying OS detection (try #4) against 10.10.15.60
Retrying OS detection (try #5) against 10.10.15.60
NSE: Script scanning 10.10.15.60.
Initiating NSE at 14:01
Completed NSE at 14:01, 24.20s elapsed
Initiating NSE at 14:01
```

- UDP scan :

Command : nmap -sS -sU -T4 -A -v 10.10.15.60

The screenshot shows the Zenmap interface with the following details:

- Target:** 10.10.15.60
- Profile:** Intense scan plus UDP
- Command:** nmap -sS -sU -T4 -A -v 10.10.15.60
- Hosts Tab (Selected):** Shows one host: 10.10.15.60.
- Nmap Output Tab (Selected):** Displays the scan log output.
- Output Content:**

```
nmap -sS -sU -T4 -A -v 10.10.15.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-07 14:01 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating ARP Ping Scan at 14:01
Scanning 10.10.15.60 [1 port]
Completed ARP Ping Scan at 14:01, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:01
Completed Parallel DNS resolution of 1 host. at 14:01, 0.07s elapsed
Initiating SYN Stealth Scan at 14:01
Scanning 10.10.15.60 [1000 ports]
Discovered open port 445/tcp on 10.10.15.60
Discovered open port 135/tcp on 10.10.15.60
Discovered open port 3389/tcp on 10.10.15.60
Discovered open port 139/tcp on 10.10.15.60
Discovered open port 912/tcp on 10.10.15.60
Discovered open port 1521/tcp on 10.10.15.60
Discovered open port 902/tcp on 10.10.15.60
Completed SYN Stealth Scan at 14:01, 0.21s elapsed (1000 total ports)
Initiating UDP Scan at 14:01
Scanning 10.10.15.60 [1000 ports]
Increasing send delay for 10.10.15.60 from 0 to 50 due to
max_successful_tryno increase to 5
Increasing send delay for 10.10.15.60 from 50 to 100 due to
max_successful_tryno increase to 6
Warning: 10.10.15.60 giving up on port because retransmission cap hit (6).
Increasing send delay for 10.10.15.60 from 100 to 200 due to 11 out of 18
dropped probes since last increase.
UDP Scan Timing: About 7.46% done; ETC: 14:08 (0:06:25 remaining)
Increasing send delay for 10.10.15.60 from 200 to 400 due to 15 out of 36
dropped probes since last increase.
```

- TCP scan :

Command : nmap -p 1-65535 -T4 -A -v 10.10.15.60

The screenshot shows the Zenmap interface with the following details:

- Target:** 10.10.15.60
- Profile:** Intense scan, all TCP ports
- Command:** nmap -p 1-65535 -T4 -A -v 10.10.15.60
- Hosts:** OS Host 10.10.15.60
- Nmap Output:** The main pane displays the scan results:

```
nmap -p 1-65535 -T4 -A -v 10.10.15.60
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-07 14:01 India Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating NSE at 14:01
Completed NSE at 14:01, 0.00s elapsed
Initiating ARP Ping Scan at 14:01
Scanning 10.10.15.60 [1 port]
Completed ARP Ping Scan at 14:01, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:01
Completed Parallel DNS resolution of 1 host. at 14:01, 0.07s elapsed
Initiating SYN Stealth Scan at 14:01
Scanning 10.10.15.60 [65535 ports]
Discovered open port 445/tcp on 10.10.15.60
Discovered open port 3389/tcp on 10.10.15.60
Discovered open port 135/tcp on 10.10.15.60
Discovered open port 139/tcp on 10.10.15.60
Discovered open port 49669/tcp on 10.10.15.60
Discovered open port 902/tcp on 10.10.15.60
Discovered open port 5040/tcp on 10.10.15.60
Discovered open port 7680/tcp on 10.10.15.60
Discovered open port 1521/tcp on 10.10.15.60
Discovered open port 49664/tcp on 10.10.15.60
Discovered open port 49668/tcp on 10.10.15.60
Discovered open port 49675/tcp on 10.10.15.60
Discovered open port 49665/tcp on 10.10.15.60
Discovered open port 49672/tcp on 10.10.15.60
Discovered open port 49667/tcp on 10.10.15.60
Discovered open port 49666/tcp on 10.10.15.60
Discovered open port 8834/tcp on 10.10.15.60
Discovered open port 912/tcp on 10.10.15.60
Completed SYN Stealth Scan at 14:01, 10.06s elapsed (65535 total ports)
Initiating Service scan at 14:01
```

Output:

Nmap Output		Ports / Hosts		Topology	Host Details	Scans
	Port	Protocol	State	Service	Version	
●	135	tcp	open	msrpc	Microsoft Windows RPC	
●	139	tcp	open	netbios-ssn	Microsoft Windows netbios-ssn	
●	445	tcp	open	microsoft-ds		
●	3389	tcp	open	ms-wbt-server		
●	902	tcp	open	vmware-auth	VMware Authentication Daemon 1.10 (Uses VNC, SOAP)	
●	912	tcp	open	vmware-auth	VMware Authentication Daemon 1.0 (Uses VNC, SOAP)	
●	1521	tcp	open	oracle-tns	Oracle TNS Listener 10.2.0.1.0 (for 32-bit Windows)	
●	5040	tcp	open			
●	7680	tcp	open	pando-pub		
●	8834	tcp	open	nessus-xmlrpc		
●	49664	tcp	open	msrpc	Microsoft Windows RPC	
●	49665	tcp	open	msrpc	Microsoft Windows RPC	
●	49666	tcp	open	msrpc	Microsoft Windows RPC	
●	49667	tcp	open	msrpc	Microsoft Windows RPC	
●	49668	tcp	open	msrpc	Microsoft Windows RPC	
●	49669	tcp	open	msrpc	Microsoft Windows RPC	
●	49672	tcp	open	msrpc	Microsoft Windows RPC	
●	49675	tcp	open	oracle	Oracle Database	
●	80	udp	open filtered	http		
●	123	udp	open filtered	ntp		
●	137	udp	open	netbios-ns	Microsoft Windows Mobile netbios-ns	
●	138	udp	open filtered	netbios-dgm		
●	500	udp	open filtered	isakmp		
●	1484	udp	open filtered	confluent		
●	1900	udp	open filtered	upnp		
●	2148	udp	open filtered	veritas-ucl		
●	3389	udp	open filtered	ms-wbt-server		

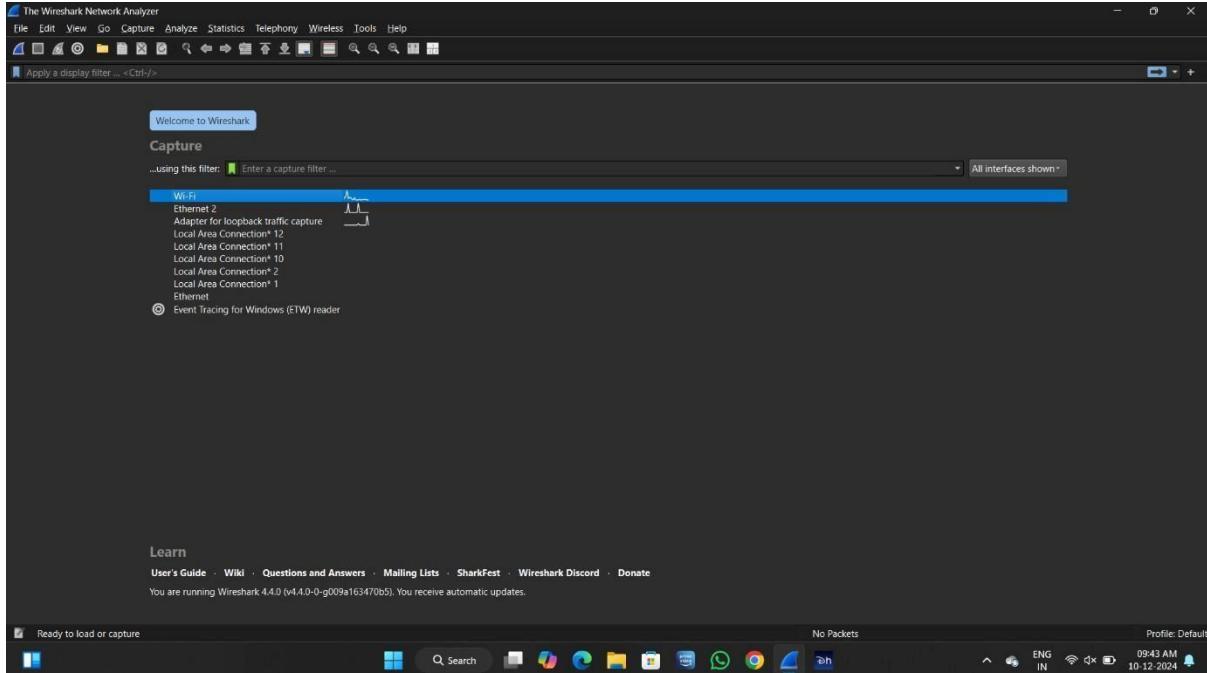
Conclusion:

Network scanning and reconnaissance are critical components of the cybersecurity lifecycle, enabling both defenders and ethical hackers to assess the security posture of systems before malicious actors can exploit them. Tools like Nmap provide powerful capabilities to identify open ports, running services, and even operating systems, offering a comprehensive view of the target environment.

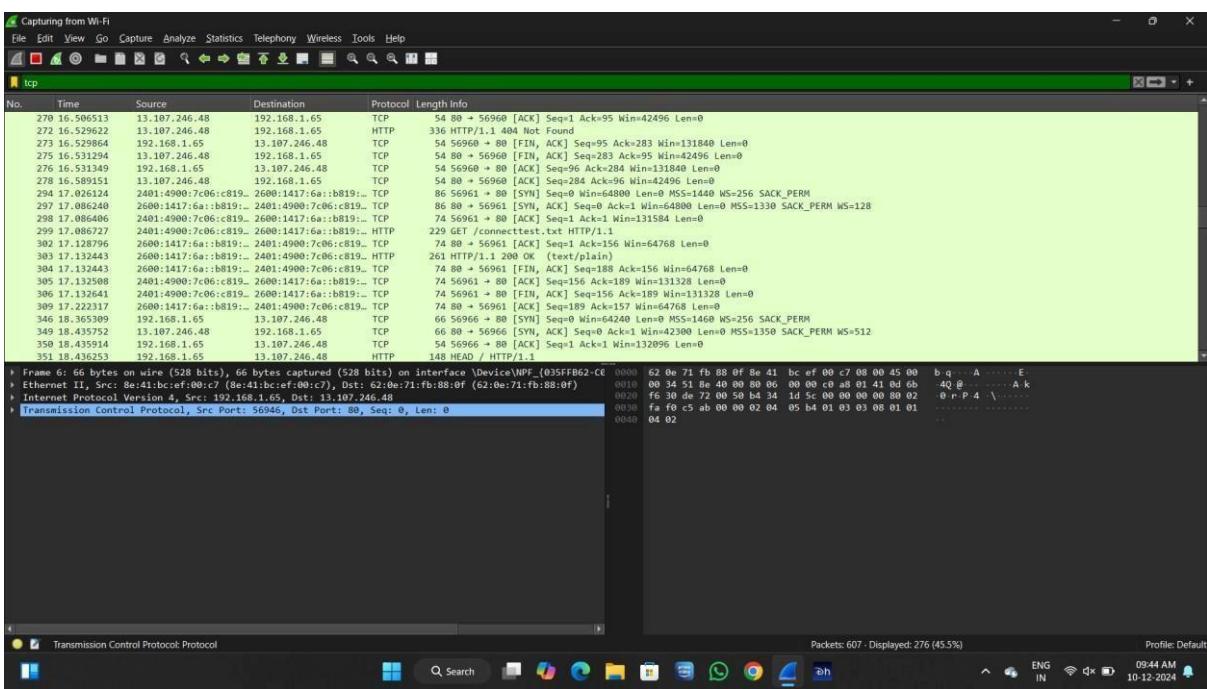
PRACTICAL 2

AIM: Find tcp, dns, http and http website login id & password using wireshark.

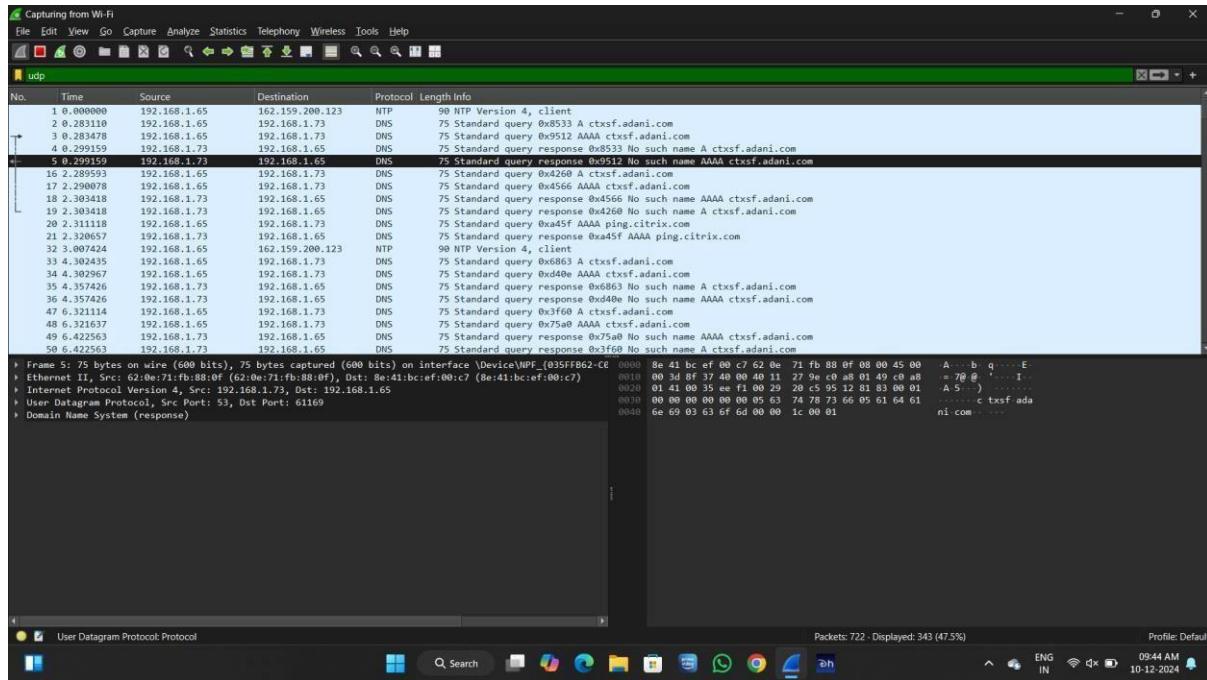
Step 1 : open wireshark and connect with wifi



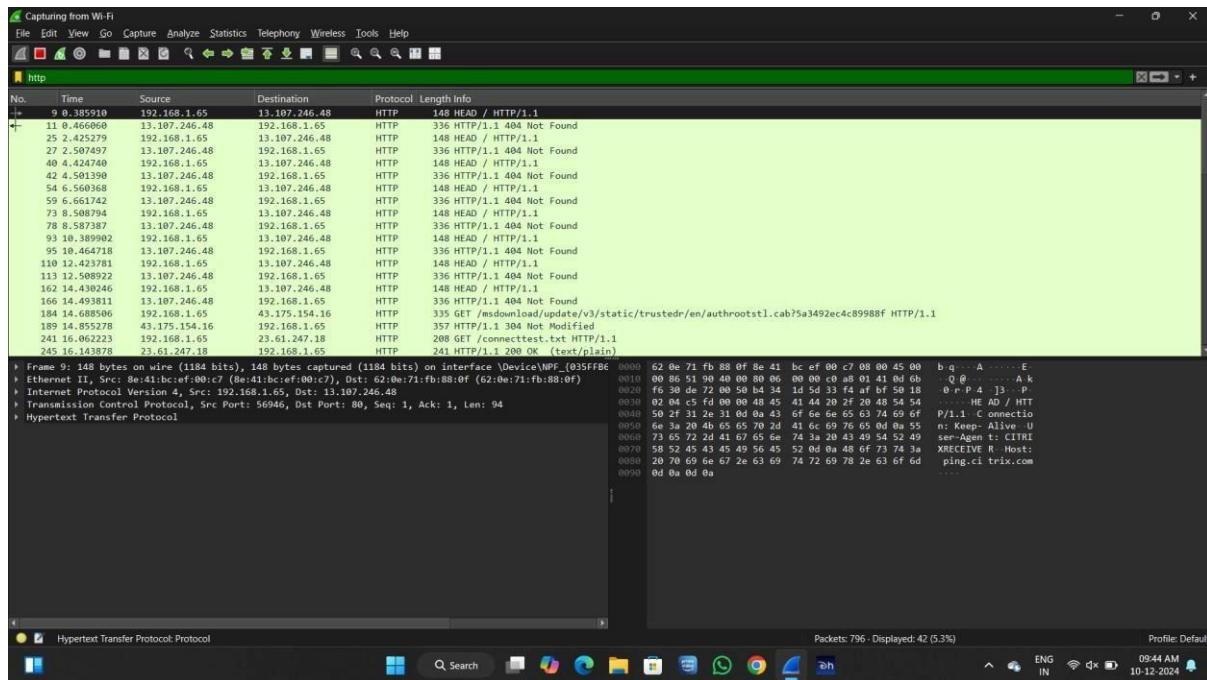
Step 2 : find TCP package



Step 3 : find DNS package

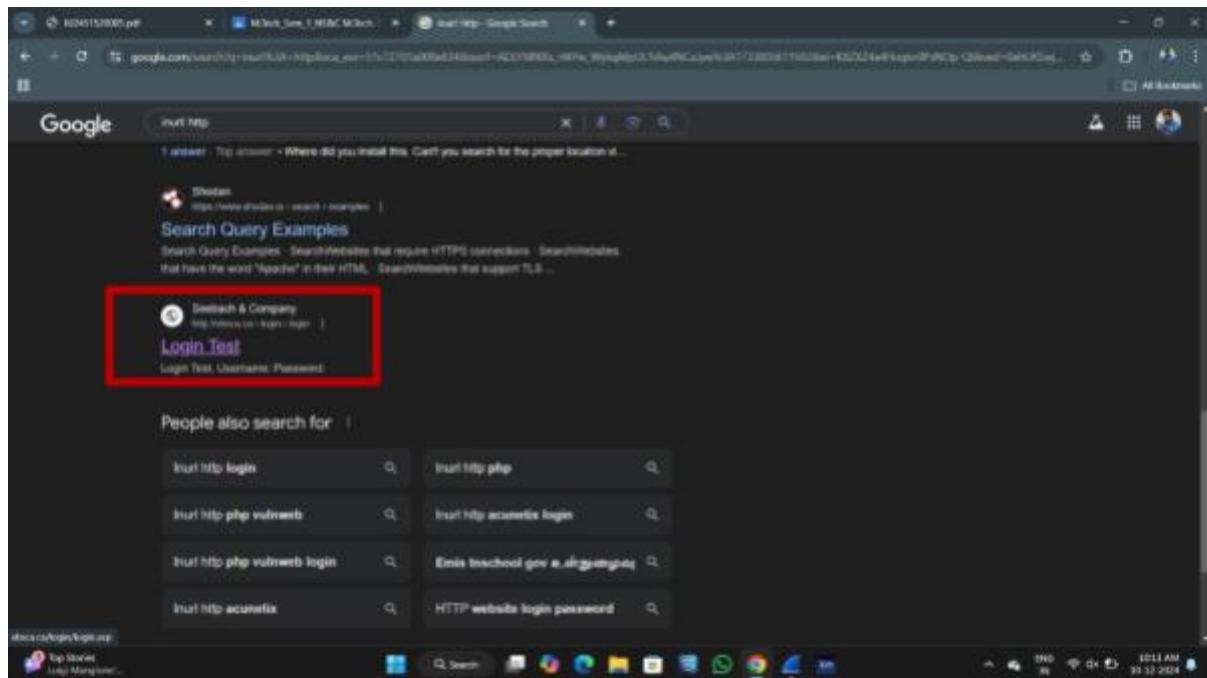


Step 4 : find HTTP package

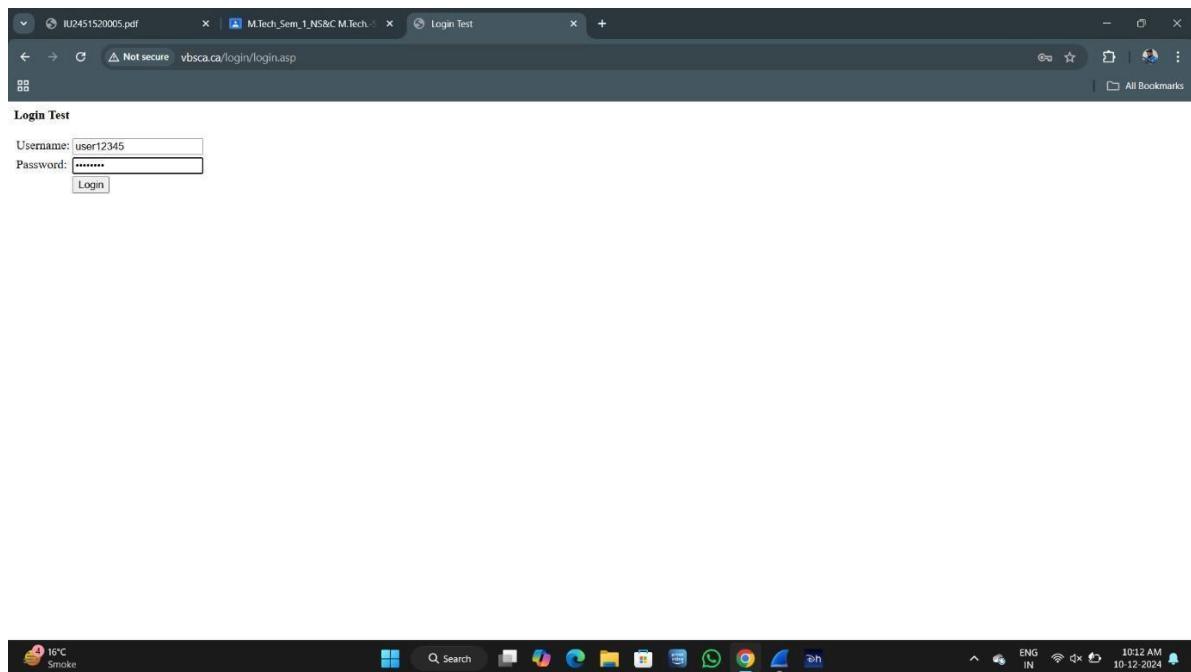


FIND ID PASSWORD

Step 1 : find any HTTP website on browser



Step 2 : login user ID and PASSWORD



Step 3 : open wireshark and search http in search and find ID & PASSWORD

```
f 76 62 73 63 61 2e    r: http://vbsca.
c 6f 67 69 6e 2e 61    ca/login /login.a
4 2d 45 6e 63 6f 64    sp Acce pt-Encod
c 20 64 65 66 6c 61    ing: gzi p, defla
4 2d 4c 61 6e 67 75    te Acce pt-Langu
3 2c 65 6e 3b 71 3d    age: en-US,en;q=
0 2e 38 0d 0a 43 6f    0.9,hi;q=0.8 Co
3 45 53 53 49 4f 4e    okie: AS PSESSION
3 3d 4a 41 4b 42 46    IDCQRCRSR CC=JAKBF
2 49 4c 4e 41 4d 48    FQDNEPAP DBILLNAME
4 55 73 65 72 6e 61    IB8...xtUserna
3 34 35 26 74 78 74    me=user1 2345&txt
1 32 33 34 35 36 37    Password =1234567
8
```

Packets: 11506 · Displayed: 31 (0.3%) Pro

Conclusion:

Wireshark is a powerful packet-sniffing tool that allows users to analyze network traffic in real-time. By capturing and inspecting packets, it is possible to identify various protocols such as TCP, DNS, and HTTP, revealing important network activities and potentially sensitive data.

During analysis, HTTP traffic can sometimes expose login IDs and passwords, especially if the website does not use encryption (i.e., not using HTTPS). This highlights a critical vulnerability: unencrypted traffic can be easily intercepted and exploited by attackers. Through TCP and DNS analysis, Wireshark also provides deeper insight into session behaviors, host communications, and domain lookups, aiding in identifying suspicious or unauthorized connections.

PRACTICAL 3

AIM: To automate and enhance the information-gathering process using Recon-*ng*.

Definition: Recon-*ng* is a Python-based web reconnaissance framework for automating OSINT tasks. It provides modules for gathering information like domains, contacts, and IPs, integrating APIs, and visualizing data. It is widely used in cybersecurity for penetration testing and intelligence gathering.

step 1: open RECON_NG

```

cyrus@cyrus:~$ recon-ng search
[recon-ng][default] > marketplace search

+-----+-----+-----+-----+-----+
|      Path      | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| discovery/info_disclosure/cache_snoop | 1.1    | not installed | 2020-10-13 |   |   |
| discovery/info_disclosure/interesting_files | 1.2    | not installed | 2021-10-04 |   |   |
| exploitation/injection/command_injector | 1.0    | not installed | 2019-06-24 |   |   |
| exploitation/injection/xpath_bruter | 1.2    | not installed | 2019-10-08 |   |   |
| import/csv_file | 1.1    | not installed | 2019-08-09 |   |   |
| import/list | 1.1    | not installed | 2019-06-24 |   |   |
| import/masscan | 1.0    | not installed | 2020-04-07 |   |   |
| import/nmap | 1.1    | not installed | 2020-10-06 |   |   |
| recon/companies-contacts/bing_linkedin_cache | 1.0    | not installed | 2019-06-24 |   | * |
| recon/companies-contacts/censys_email_address | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-contacts/pen | 1.1    | not installed | 2019-10-15 |   |   |
| recon/companies-domains/censys_subdomains | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-domains/pen | 1.1    | not installed | 2019-10-15 |   |   |
| recon/companies-domains/viewdns_reverse_whois | 1.1    | not installed | 2021-08-24 |   |   |
| recon/companies-domains/whoxy_dns | 1.1    | not installed | 2020-06-17 |   | * |
| recon/companies-multi/censys_org | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-multi/censys_tls_subjects | 2.1    | not installed | 2022-01-31 | * | * |
| recon/companies-multi/github_miner | 1.1    | not installed | 2020-05-15 |   | * |
| recon/companies-multi/shodan_org | 1.1    | not installed | 2020-07-01 | * | * |
| recon/companies-multi/whois_miner | 1.1    | not installed | 2019-10-15 |   |   |
| recon/contacts-contacts/ab | 1.0    | not installed | 2019-10-11 |   | * |
| recon/contacts-contacts/maltester | 1.0    | not installed | 2019-06-24 |   |   |
| recon/contacts-contacts/mangle | 1.0    | not installed | 2019-06-24 |   |   |
| recon/contacts-contacts/unmangle | 1.1    | not installed | 2019-10-27 |   |   |
| recon/contacts-credentials/hibp_breach | 1.2    | not installed | 2019-09-10 |   | * |
+-----+-----+-----+-----+-----+
  
```

step 2 : search market places for module installation or to select which module you want to choose

```

cyrus@cyrus:~$ recon-ng
[recon-ng][default] > [*] Version check disabled.

Sponsored by ...
   ^  ^ 
  / \ / \ 
  // \\ \\
  //  BLACK HILLS  \\
  //  www.blackhillsinfosec.com

PRACTISEC
www.practise.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
[*] No modules enabled/installied.

[recon-ng][default] >
  
```

step 3 : search module for SSL

```
[recon-ng][default] > marketplace search ssl
[*] Searching module index for 'ssl' ...
+-----+
| Path      | Version | Status   | Updated | D | K |
+-----+
| recon/domains-hosts/ssl_san | 1.0     | not installed | 2019-06-24 | | |
| recon/hosts-hosts/ssltools | 1.0     | not installed | 2019-06-24 | | |
| recon/ports-hosts/ssl_scan | 1.1     | not installed | 2021-08-24 | | |
+-----+
D = Has dependencies. See info for details.
K = Requires keys. See info for details.

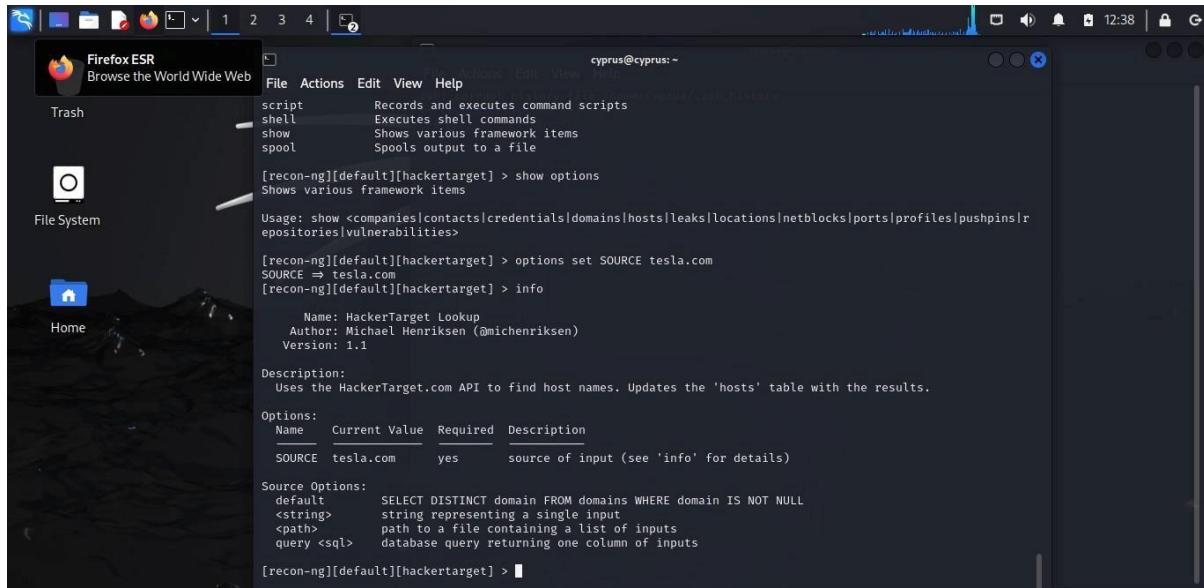
[recon-ng][default] > marketplace info ssltools
+-----+
| path      | recon/hosts-hosts/ssltools
| name      | SSLTools.com Host Name Lookups
| author    | Tim Maletic (borrowing from the ssl_san module by Zach Graces)
```

step 4 : install marketplace hackertarget

```
[recon-ng][default] > marketplace install hackertarget
[*] Module installation failed: recon/domains-hosts/hackertarget
[*] HTTPSConnectionPool(host='raw.githubusercontent.com', port=443): Max retries exceeded with url: /lanmaster553/recon-ng-modules/master/modules/recon/domains-hosts/hackertarget.py (Caused by NameResolutionError("curl: (33) Temporary failure in name resolution"))
[recon-ng][default] > marketplace install hackertarget
[*] Module installed: recon/domains-hosts/hackertarget
[*] Reloading modules ...
[recon-ng][default] > modules load hackertarget
[recon-ng][default][hackertarget] > help
Commands (type [help?] <topic>):
back           Exits the current context
dashboard      Displays a summary of activity
db             Interfaces with the workspace's database
exit           Exits the framework
goptions        Manages the global context options
help           Displays this menu
info            Shows details about the loaded module
input           Shows inputs based on the source option
keys            Manages third party resource credentials
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
reload          Reloads the loaded module
run             Runs the loaded module
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
spool           Spools output to a file

[recon-ng][default][hackertarget] > 
```

step 5: set the source of tesla.com



```
[recon-ng][default][hackertarget] > show options
script      Records and executes command scripts
shell       Executes shell commands
show        Shows various framework items
spool       Spools output to a file

[recon-ng][default][hackertarget] > Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default][hackertarget] > options set SOURCE tesla.com
SOURCE => tesla.com
[recon-ng][default][hackertarget] > info
  Name: HackerTarget Lookup
  Author: Michael Henriksen (@michenriksen)
  Version: 1.1

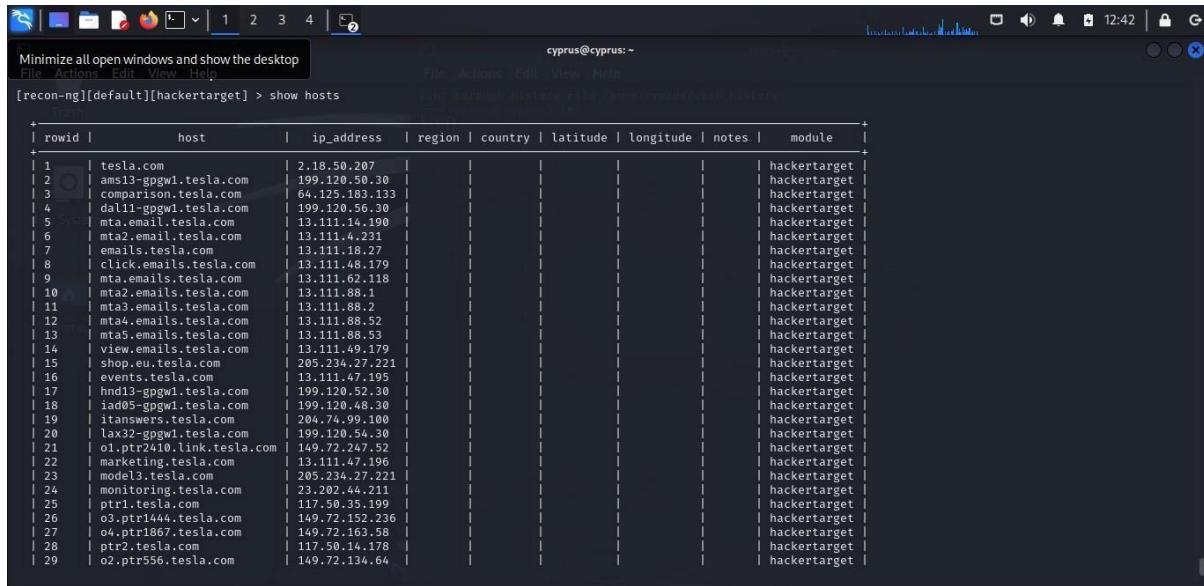
  Description:
    Uses the HackerTarget.com API to find host names. Updates the 'hosts' table with the results.

  Options:
    Name  Current Value  Required  Description
    SOURCE  tesla.com     yes      source of input (see 'info' for details)

  Source Options:
    default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
    <string>    string representing a single input
    <path>      path to a file containing a list of inputs
    query <sql> database query returning one column of inputs

[recon-ng][default][hackertarget] >
```

step 6: show the all host name of tesla.com



rowid	host	ip_address	region	country	latitude	longitude	notes	module
1	tesla.com	2.18.50.207						hackertarget
2	ams13-gpgw1.tesla.com	199.120.50.30						hackertarget
3	comparison.tesla.com	64.125.183.133						hackertarget
4	dal11-gpgw1.tesla.com	199.120.56.30						hackertarget
5	mta.email.tesla.com	13.111.14.190						hackertarget
6	mta2.email.tesla.com	13.111.4.231						hackertarget
7	emails.tesla.com	13.111.18.27						hackertarget
8	click.emails.tesla.com	13.111.48.179						hackertarget
9	mta.emails.tesla.com	13.111.62.118						hackertarget
10	mta2.emails.tesla.com	13.111.88.1						hackertarget
11	mta3.emails.tesla.com	13.111.88.2						hackertarget
12	mta4.emails.tesla.com	13.111.88.52						hackertarget
13	mta5.emails.tesla.com	13.111.88.53						hackertarget
14	view.emails.tesla.com	13.111.49.179						hackertarget
15	shop.eu.tesla.com	205.234.27.221						hackertarget
16	events.tesla.com	13.111.47.195						hackertarget
17	hnd13-gpgw1.tesla.com	199.120.52.30						hackertarget
18	iad05-gpgw1.tesla.com	199.120.48.30						hackertarget
19	itanswers.tesla.com	204.74.99.100						hackertarget
20	lax32-gpgw1.tesla.com	199.120.54.30						hackertarget
21	o1.ptr2410.link.tesla.com	149.72.247.52						hackertarget
22	marketing.tesla.com	13.111.47.196						hackertarget
23	model3.tesla.com	205.234.27.221						hackertarget
24	monitoring.tesla.com	23.202.44.211						hackertarget
25	ptr1.tesla.com	117.50.35.199						hackertarget
26	o3.ptr1444.tesla.com	149.72.152.236						hackertarget
27	o4.ptr1867.tesla.com	149.72.163.58						hackertarget
28	ptr2.tesla.com	117.50.14.178						hackertarget
29	o2.ptr556.tesla.com	149.72.134.64						hackertarget

Conclusion:

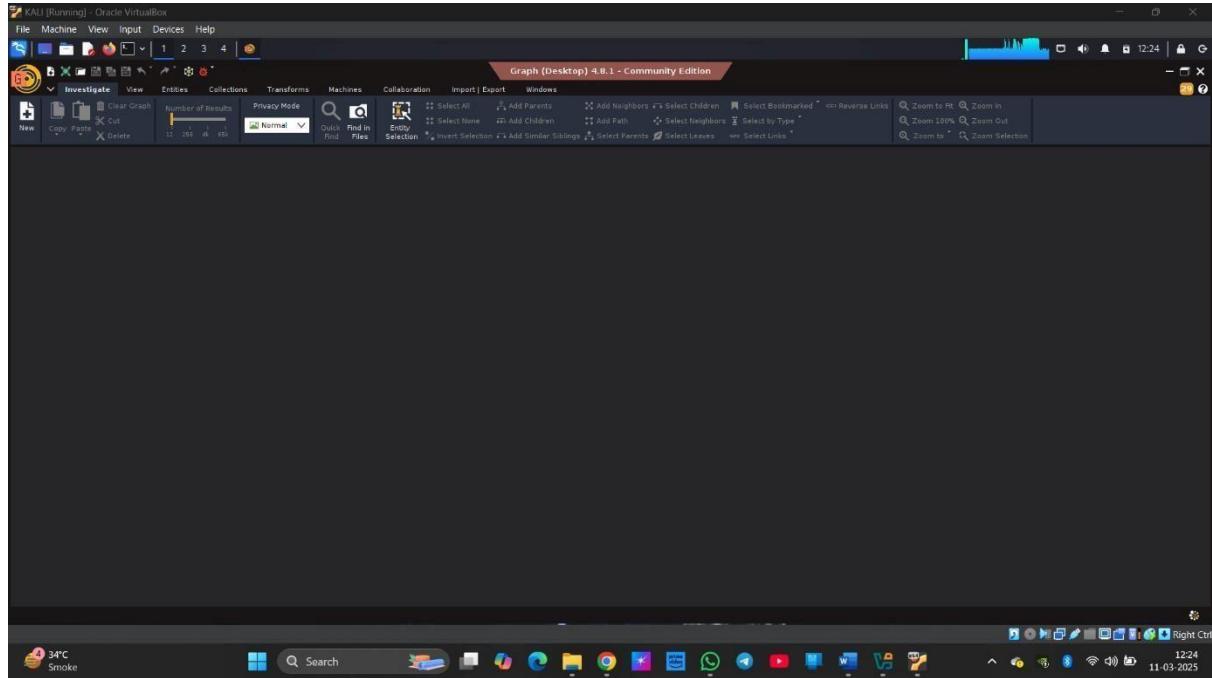
Recon-NG is a robust and modular open-source reconnaissance tool designed to automate and enhance the information-gathering process during cybersecurity assessments. Its powerful framework integrates seamlessly with various APIs and data sources, allowing security professionals to quickly collect and correlate valuable intelligence such as domain names, IP addresses, WHOIS information, and social media data.

PRACTICAL 4

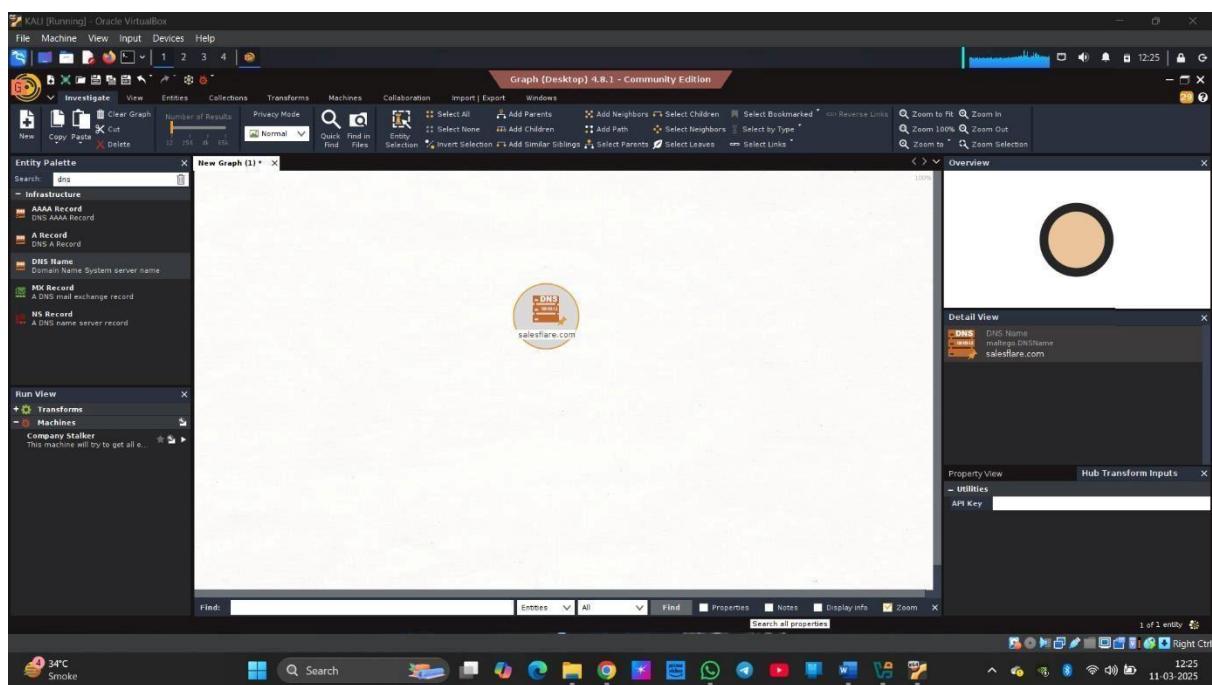
AIM: To automate and enhance the information-gathering process using Maltego, enabling graphical visualization of relationships.

Definition: Maltego is an open-source intelligence (OSINT) and forensics tool that helps in data gathering and link analysis. It is widely used for cyber investigations to map relationships between entities such as people, organizations, and online resources.

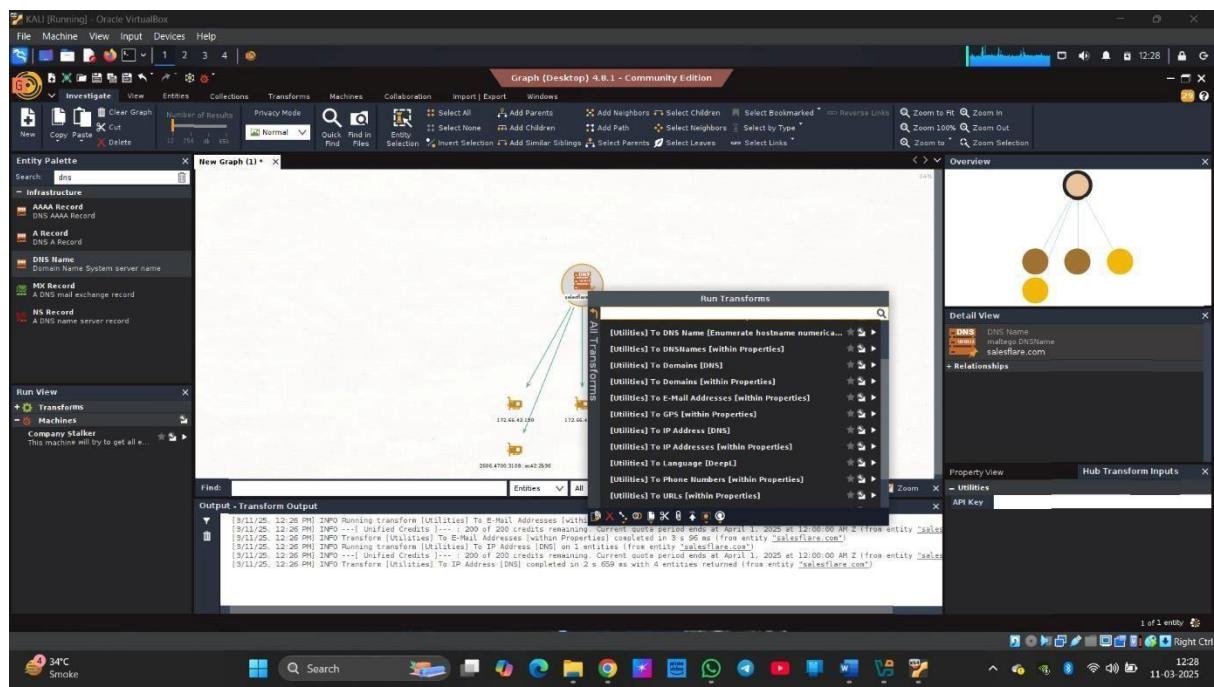
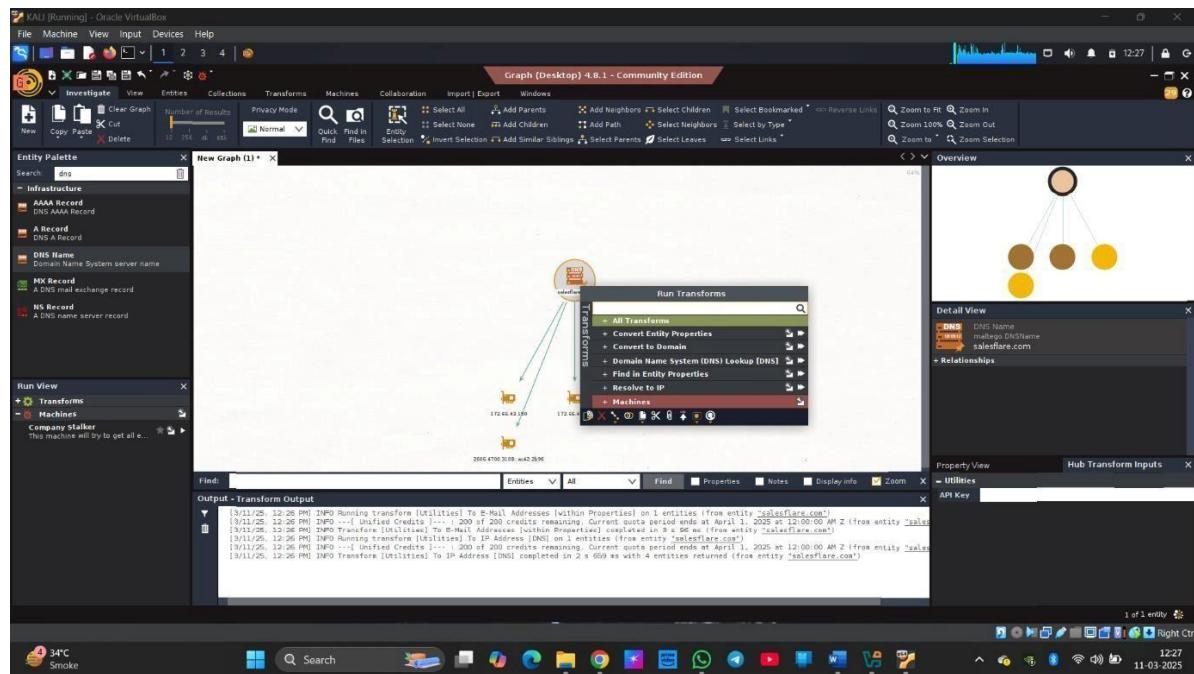
Step 1: open maltigo in kali

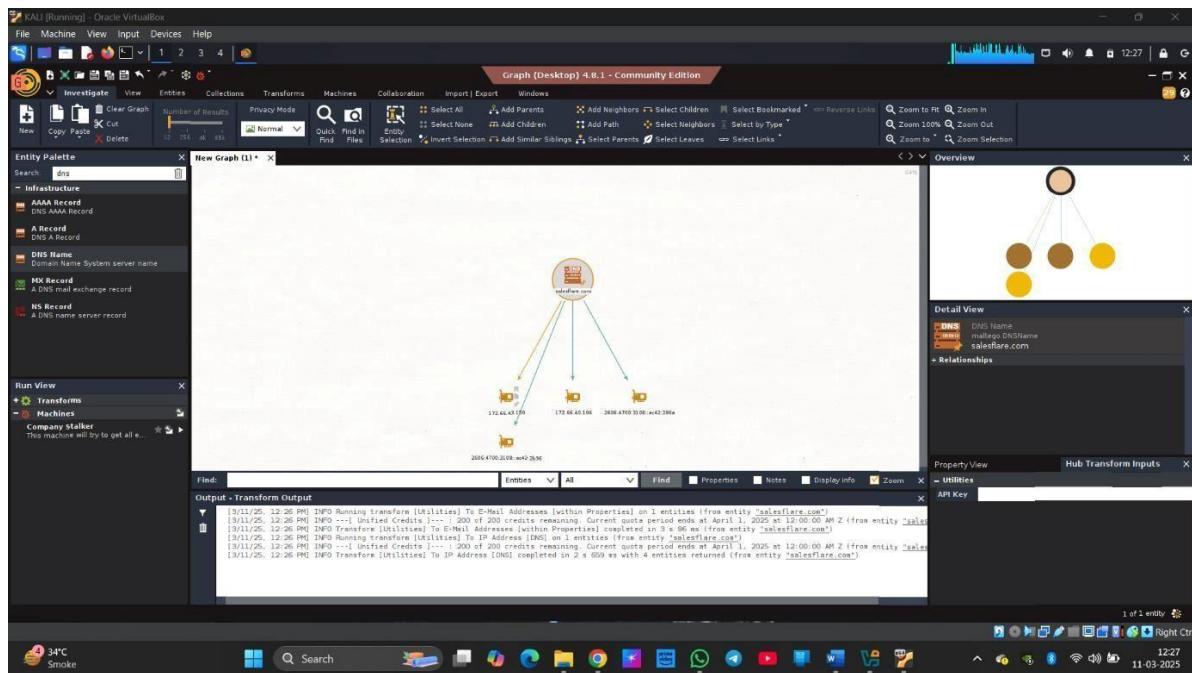


Step 2: enter the domain name for gathering information.



Step 3: right click on that domain and click on all transform and select find IP address





Conclusion:

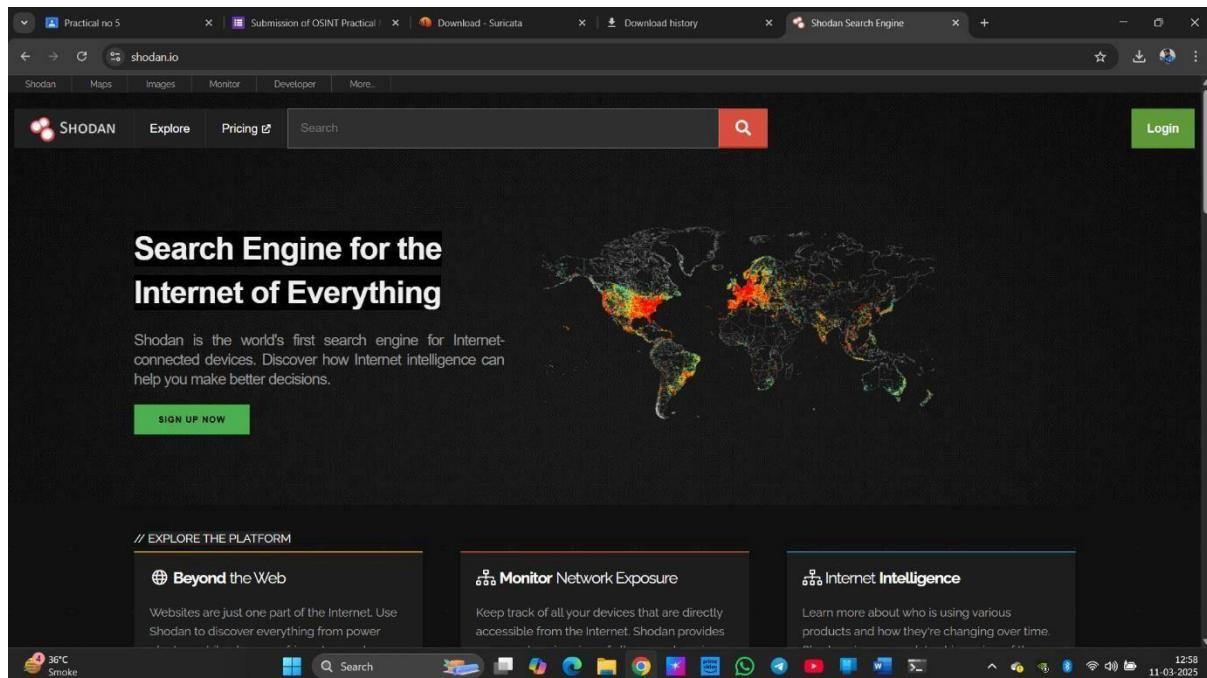
Maltego is a powerful intelligence-gathering and analysis tool that automates data collection and provides graphical visualization of relationships between entities such as people, domains, IP addresses, social media profiles, and infrastructure components. By leveraging open-source intelligence (OSINT) and a wide range of transforms, Maltego enables investigators to uncover hidden connections and gain deep insights into target environments.

PRACTICAL 5

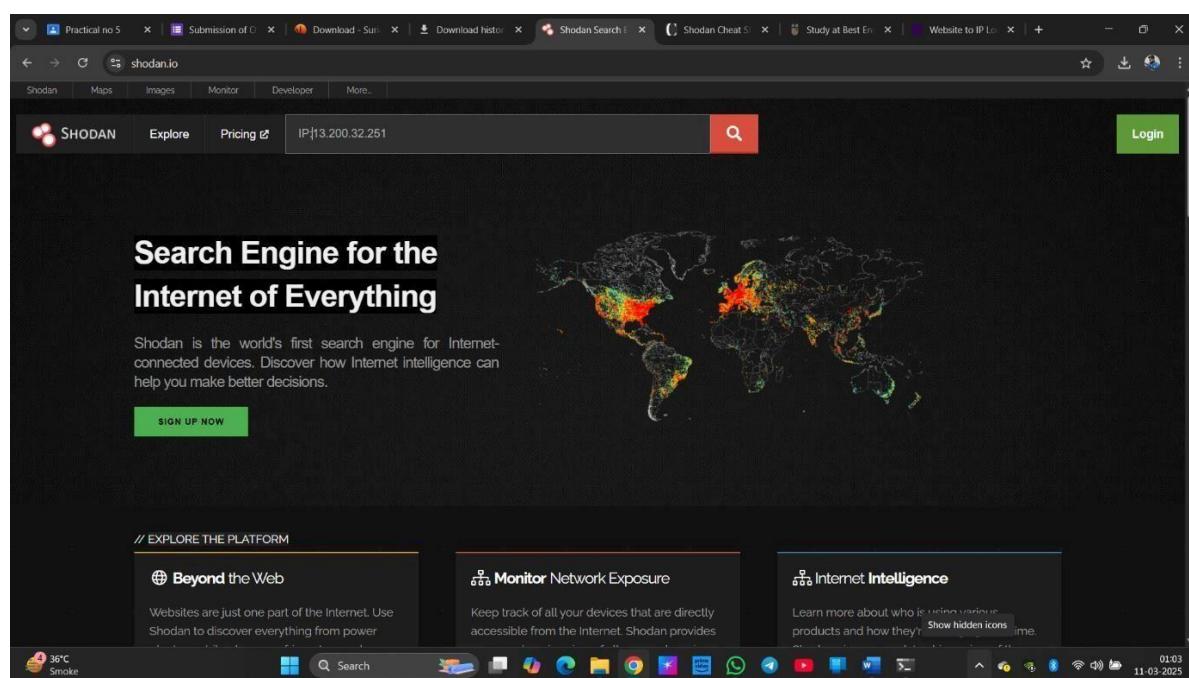
AIM: To identify and analyze internet-exposed devices and vulnerabilities through automated information gathering using the Shodan search engine.

Definition: Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

Step 1: open SHODAN



Step 2: enter IP address of the target system



Step 3: get the information and vulnerability of target domain.

General Information

- Hostnames: ec2-13-200-32-251.compute.amazonaws.com, indusuni.ac.in, convolution.indusuni.ac.in, coursecontent.indusuni.ac.in, gti.indusuni.ac.in, ias.indusuni.ac.in, icsii.indusuni.ac.in, ids.indusuni.ac.in, iate.indusuni.ac.in, iiict.indusuni.ac.in, iit.indusuni.ac.in, iims.indusuni.ac.in, iishls.indusuni.ac.in, iss.indusuni.ac.in, ite.indusuni.ac.in, innovista.indusuni.ac.in, international.indusuni.ac.in, iscc.indusuni.ac.in, sac.indusuni.ac.in, www.indusuni.ac.in
- Domains: AMAZONAWS.COM, INDUSUNI.AC.IN

Open Ports

- 80, 443

Apache httpd

Indus University | Top University in Ahmedabad, Gujarat, India

Vulnerabilities

- 2, 2, 17, 1

Vulnerabilities

Note: The device may not be impacted by all of these issues. The vulnerabilities are ranked based on the software and version.

2024 (1)

CVE-2024-2517 [6] php-svg-lib is a scalable vector graphics (SVG) file parsing/rendering library. Prior to version 0.5.2, php-svg-lib fails to validate that font-family doesn't contain a PHAR url, which might leads to RCE on PHP < 8.0, and doesn't validate if external references are allowed. This might leads to bypass of restrictions or RCE on projects that are using it, if they do not strictly validate the fontName that is passed by php-svg-lib. The 'Style:fromAttributes()' or the 'Style:parseCssStyle()' should check the fontName that is passed by php-svg-lib. The same check as done in 'Style:fromStyleSheets' might be reused. Libraries using this library as a dependency might be vulnerable to some bypass of restrictions, or even remote code execution, if they do not double check the value of the 'fontName' that is passed by php-svg-lib. Version 0.5.2 contains a fix for this issue.

2022 (4)

CVE-2022-37454 [6] The Keccak XCH SHA-3 reference implementation before fd6feef has an integer overflow and resultant buffer overflow that allows attackers to execute arbitrary code or eliminate expected cryptographic properties. This occurs in the sponge function interface.

CVE-2022-31629 [6] In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a '_Host-' or '_Secure-' cookie by PHP applications.

CVE-2022-31628 [6] In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompress code would recursively uncompress 'quines' (zip files, resulting in an infinite loop).

CVE-2022-4900 [6] A vulnerability was found in PHP where setting the environment variable `PHP_CLI_SERVER_WORKERS` to a large value leads to a heap buffer overflow.

2021 (5)

CVE-2021-21707 [6] In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like `simplexml_load_file()`, URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus

2021 (6)

- CVE-2021-21707** [!] In PHP versions 7.3.x below 7.3.33, 7.4x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like `simplexml_load_file()`, URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus interpreting the filename differently from what the user intended, which may lead it to reading a different file than intended.
- CVE-2021-21708** [!] In PHP versions 7.3.x below 7.3.31, 7.4x below 7.4.24 and 8.0.x below 8.0.11, in Microsoft Windows environment, `ZipArchive::extractTo()` may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions.
- CVE-2021-21709** [!] In PHP versions 7.3.x below 7.3.29, 7.4x below 7.4.21 and 8.0.x below 8.0.8, when using URL validation functionality via `filter_var()` function with `FILTER_VALIDATE_URL` parameter, an URL with invalid password field can be accepted as valid. This can lead to the code incorrectly parsing the URL, and potentially leading to other security implications - like contacting a wrong server or making a wrong access decision.
- CVE-2021-21704** [!] In PHP versions 7.3.x below 7.3.29, 7.4x below 7.4.21 and 8.0.x below 8.0.8, when using Firebird PDO driver extension, a malicious database server could cause crashes in various database functions, such as `getAttributed()`, `execute()`, `fetch()` and others by returning invalid response data that is not parsed correctly by the driver. This can result in crashes, denial of service or potentially memory corruption.
- CVE-2021-21703** [!] In PHP versions 7.3.x up to and including 7.3.31, 7.4x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user.
- CVE-2021-21702** [!] In PHP versions 7.3.x below 7.3.27, 7.4x below 7.4.15 and 8.0.x below 8.0.2, when using SOAP extension to connect to a SOAP server, a malicious SOAP server could return malformed XML data as a response that would cause PHP to access a null pointer and thus cause a crash.

2020 (5)

- CVE-2020-11023** [!] In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `html()`, `append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

2020 (6)

- CVE-2020-11023** [!] In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing `<option>` elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `html()`, `append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- CVE-2020-11022** [!] In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. `html()`, `append()`, and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
- CVE-2020-7071** [!] In PHP versions 7.3.x below 7.3.26, 7.4x below 7.4.14 and 8.0.x when validating URL with functions like `filter_varUrl()`, `FILTER_VALIDATE_URL`, PHP will accept an URL with invalid password as valid URL. This may lead to functions that rely on URL being valid to mis-parse the URL and produce wrong data as components of the URL.
- CVE-2020-7070** [!] In PHP versions 7.2.x below 7.2.34, 7.3x below 7.3.23 and 7.4x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Jstot confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-B384 for more information.
- CVE-2020-7069** [!] In PHP versions 7.2x below 7.2.34, 7.3x below 7.3.23 and 7.4x below 7.4.11, when AES-CCM mode is used with `openssl_encrypt()` function with 12 bytes IV, only first 7 bytes of the IV are actually used. This can lead to both decreased security and incorrect encryption data.
- CVE-2020-7068** [!] In PHP versions 7.2x below 7.2.33, 7.3x below 7.3.21 and 7.4x below 7.4.9, while processing PHAR files using phar extension, `phar_parse_zipfile()` could be tricked into accessing freed memory, which could lead to a crash or information disclosure.

2019 (1)

- CVE-2019-11358** [!] jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles `jQuery.extend(true, {},)` because of Object.prototype pollution. If an unsanitized source object contained an enumerable `__proto__` property, it could extend the native `Object.prototype`.

2017 (1)

- CVE-2017-8923** [!] The `zend_string_extend` function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of <...

Conclusion:

Shodan is a specialized search engine designed to identify and analyze internet-exposed devices and their associated vulnerabilities through automated information gathering. Unlike traditional search engines, Shodan indexes data from IoT devices, servers, webcams, industrial control systems, and more—revealing what is accessible over the internet.

PRACTICAL 6

AIM: Intrusion detection and prevention, including setting up and configuring Suricata or other IDS/IPS systems and analyzing logs and alerts.

Definition: Maltego is an open-source intelligence (OSINT) and forensics tool that helps in data gathering and link analysis. It is widely used for cyber investigations to map relationships between entities such as people, organizations, and online resources.

Step 1: Install Suricata.

Command: sudo apt update && sudo apt install suricata Step

2: Verify Installation

Command: suricata --build-info Step

3: Configure Suricata

Command: sudo nano /etc/suricata/suricata.yaml Ensure the network interface is correct:

af-packet:

interface: eth0 # Change this to your active network interface

Step 4: Run suricata in IDS mode.

Command: sudo suricata -c /etc/suricata/suricata.yaml -i eth0

```
> sudo suricata -c /etc/suricata/suricata.yaml -i wlan0
Info: conf-yaml-loader: Including configuration file local.yaml.
i: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
i: threads: Threads created -> W: 8 FM: 1 FR: 1   Engine started.
^-[
```

To view log alert: nano /var/log/suricata/fast.log

```

~:tail -- Konsole
New Tab Split View
zsh ~ -:tail
cd: not a directory: /var/log/suricata/suricata.log
cd /var/log/suricata/suricata.log
[90975 - Suricata-Main] 2025-02-19 11:53:36 Notice: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: cpu: CPUs/cores online: 8
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: suricata: Setting engine mode to IDS mode by default
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: exception-on-failed-master exception-policy set to: auto
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: iocnt: wlan0: MTU 1500
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: preparing unexpected signal handling
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: privs: dropped the caps for main thread
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: logopenfile: unix socket initialized: unix socket
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: logopenfile: fast output device (regular) initialized: fast.log
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: logopenfile: eve-log output device (regular) initialized: eve.json
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: detect: 2 rule files processed, 359 rules successfully loaded, 0 rules failed, 0
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: threshold-config: Threshold config parsed: 0 rule(s) found
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: detect: 359 signatures processed: 0 are IP-only rules, 0 are inspecting packet payload, 180 inspect application layer, 108 are decoder eve nt only
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: runmodes: wlan0: creating 8 threads
[90975 - Suricata-Main] 2025-02-19 11:53:36 Info: ux-manager: unix socket '/var/run/suricata/suricata-command.socket'
[90975 - Suricata-Main] 2025-02-19 11:53:36 Notice: threads: threads created -> W: 8 F: 1 P: 1 Engine started.
tail -f /var/log/suricata/fast.log

02/19/2025-11:57:06.993536 [**] [1:2231000:1] SURICATA failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:06.993536 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:07.084823 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:07.088888 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:07.091743 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:07.097009 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:08.623107 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:08.633107 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:08.729016 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:52424 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-11:57:08.867543 [**] [1:2210023:2] SURICATA STREAM ESTABLISHED SYNACK resend with different ACK [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 23.9.228.6.80 -> 192.168.147.156:45354
02/19/2025-12:04:48.995423 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:42468 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-12:04:49.000942 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:42468 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-12:04:49.009342 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81
1c:42468 -> 2a03:2880:72ff:01c6:face:b00:0000:0167:443
02/19/2025-12:04:49.011224 [**] [1:2231000:1] SURICATA QUIC failed decrypt [*] [Classification: Generic Protocol Command Decode] [Priority: 3] {UDP} 2409:40c1:003e:1f6a:8efe:41e6:a20f:81

```

Conclusion:

Intrusion Detection and Prevention Systems (IDS/IPS) play a vital role in modern network security by monitoring, detecting, and responding to malicious activity in real time. Tools like Suricata offer advanced capabilities, including deep packet inspection, protocol analysis, and real-time alerting, making them essential for defending against a wide range of threats.

PRACTICAL 7

AIM: Configure S/MIME and sow email-authentication

To configure S/MIME for email authentication in Kali Linux, the process involves installing the necessary tools, obtaining a digital certificate, and setting up an email client that supports S/MIME (like Thunderbird).

Steps to Configure S/MIME on Kali Linux:

1. Install Thunderbird on Kali Linux

First, ensure that Thunderbird is installed on your Kali Linux system, as it is one of the most common email clients that supports S/MIME.

Command :`sudo apt install thunderbird`

2. Obtain a Digital Certificate

You need a digital certificate (public/private key pair) to sign and encrypt emails. You can obtain a certificate from a Certificate Authority (CA), or you can create your own self-signed certificate.

- For a self-signed certificate (for personal use): You can generate one using OpenSSL:
- Command :`openssl req -x509 -newkey rsa:4096 -keyout private.key -out public.crt -days 365`

```

File Actions Edit View Help
[(kali㉿kali)-[~]]$ openssl req -x509 -newkey rsa:4096 -keyout private.key -out public.crt -days 365
...
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:

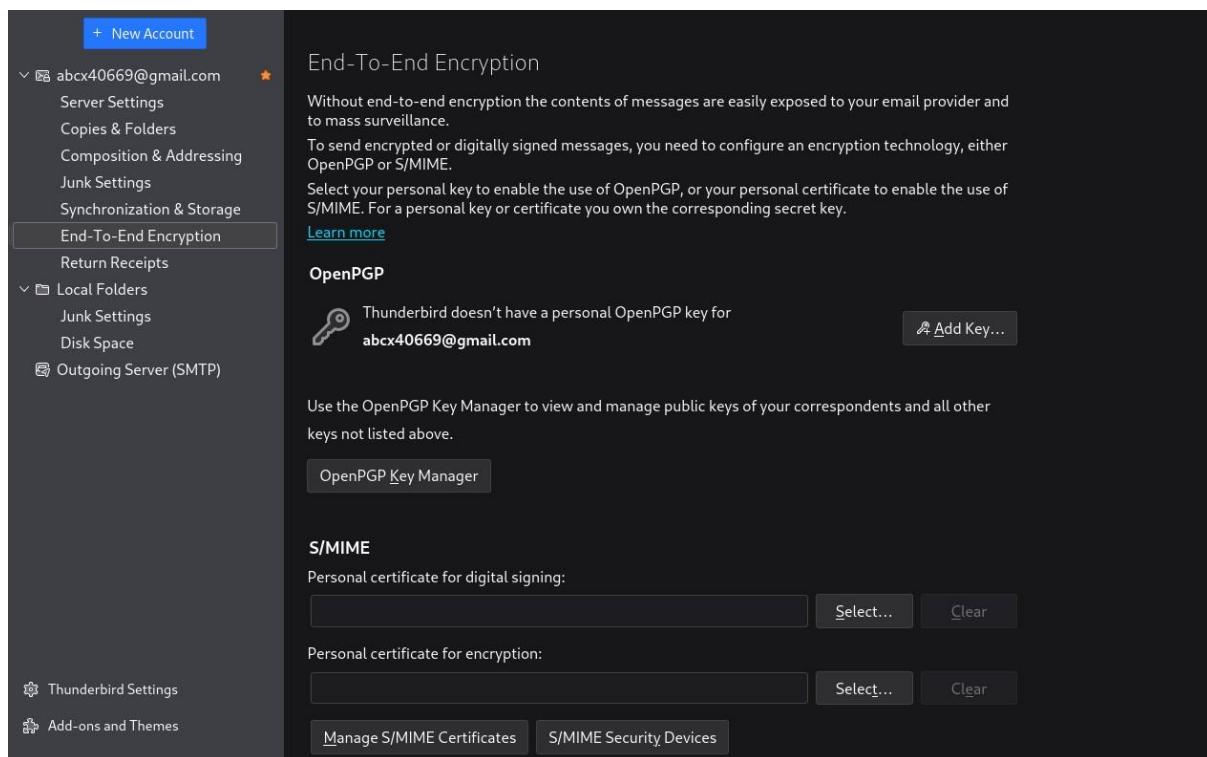
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Local Folders
Country Name (2 letter code) [AU]:in
State or Province Name (full name) [Some-State]:Gujarat
Locality Name (eg, city) []:ahmedab
Organization Name (eg, company) [Internet Widgits Pty Ltd]:tech
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:test
Email Address []:abcx40669@gmail.com

```

3. Install the Certificate in Thunderbird

- For a personal certificate:

1. Open Thunderbird.
2. Go to Preferences > Account Settings.
3. Select your email account from the list.
4. Under End-to-End Encryption, click Choose... next to Digital Signing Certificate and Encryption Certificate.
5. Browse to where your certificate (e.g., public.crt) is stored and import it.
6. After importing, select the appropriate certificate for signing and encryption.

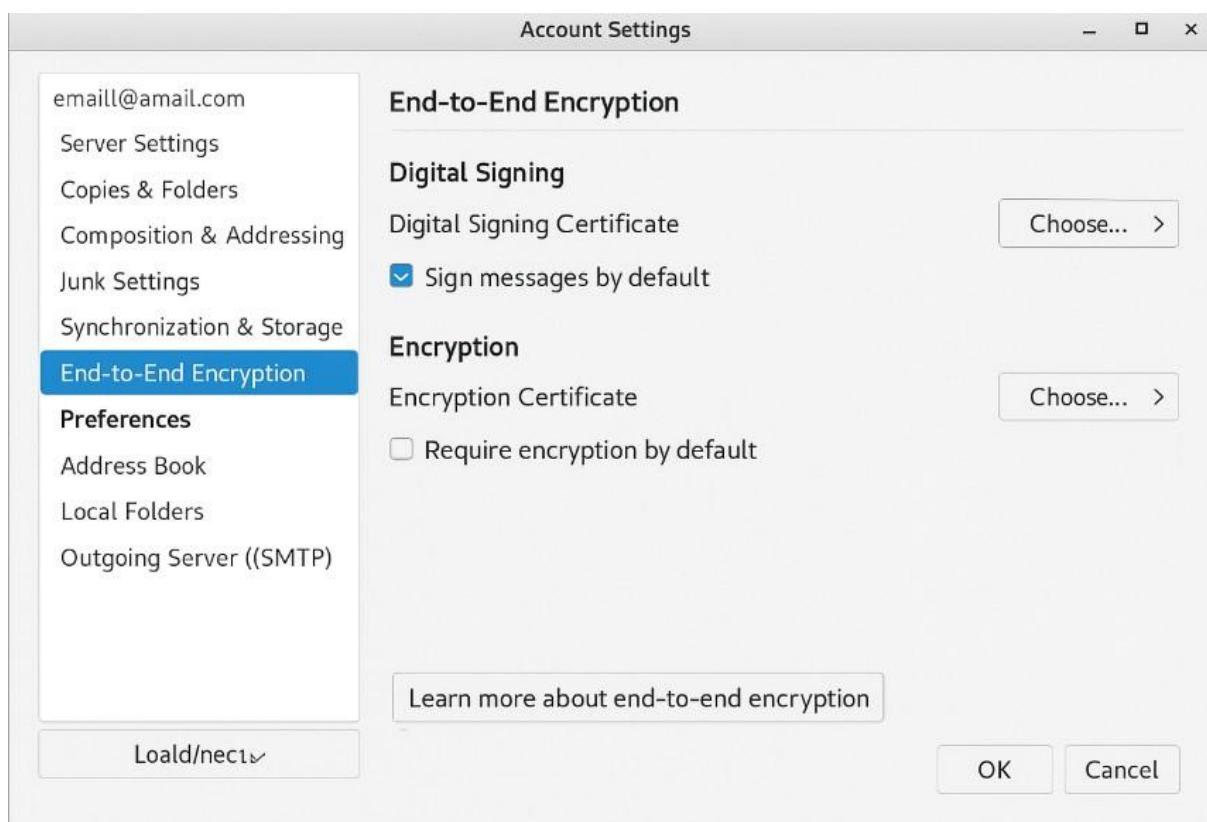


- For a certificate from a CA: If you've received the certificate as a .pfx or .p12 file from your CA, import it by navigating to Preferences > Privacy & Security in Thunderbird and selecting View Certificates > Import.
- Then, use this certificate for signing and encryption.

4. Configure Thunderbird for S/MIME Signing and Encryption

After installing your certificate, you need to configure Thunderbird to sign and encrypt your emails.

1. Go to Account Settings > End-to-End Encryption.
2. In the Digital Signing Certificate and Encryption Certificate sections, select your installed certificate.
3. Enable the option to Sign messages by default if you want all outgoing emails to be signed automatically.
4. Enable the option to Encrypt messages by default if you want to encrypt all outgoing messages (this requires the recipient's public key).

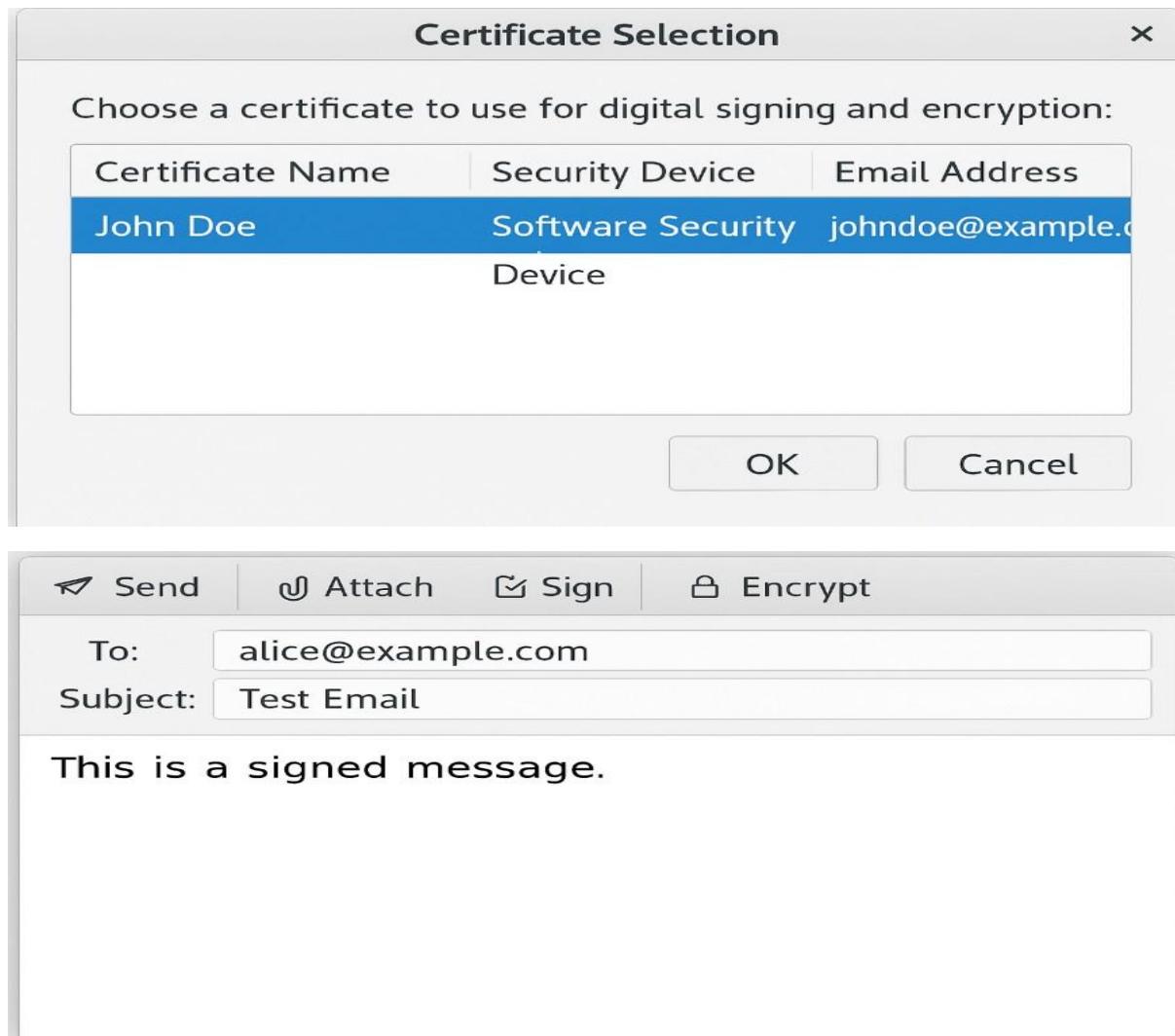


5. Sending Signed and Encrypted Emails

- To send a signed email:

When composing an email, you'll see a 'Sign' option in the toolbar. If it's not selected, tick it to sign the email.

- To send an encrypted email:



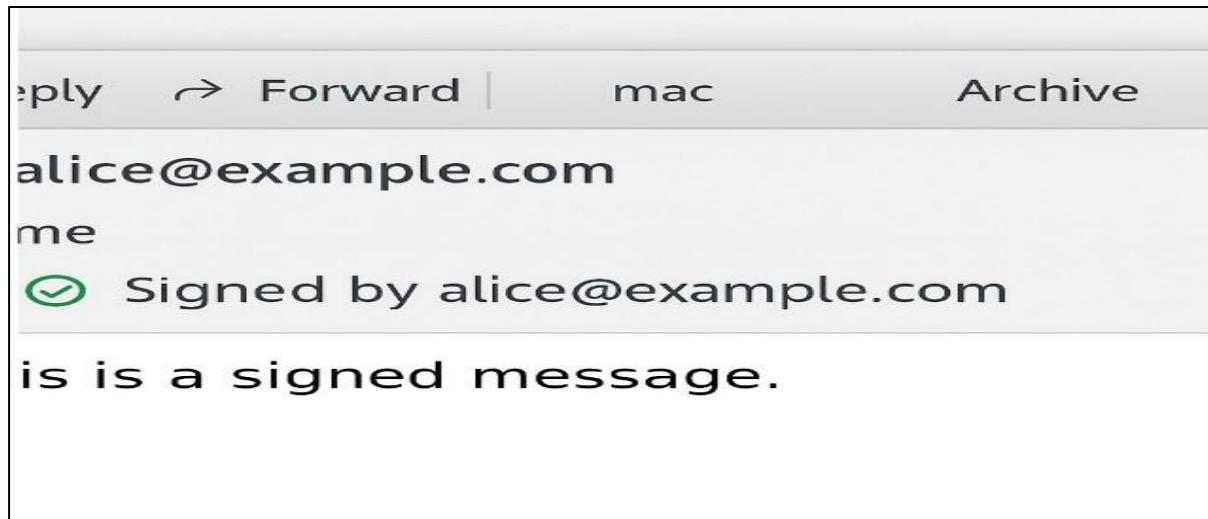
- You must have the recipient's public key certificate to send an encrypted email. You can obtain this by asking the recipient to send you a signed email, which will allow you to store their public key.

- When composing the email, click the Encrypt button (or select the encryption option in the toolbar).

6. Verifying Email Authentication

When you receive a signed email:

- Thunderbird will show an icon indicating whether the email is signed and the signature is valid.
- If the email is encrypted, you will need the corresponding private key to decrypt it.



Conclusion:

By following these steps, you will have successfully set up S/MIME on Kali Linux using Thunderbird to send signed and encrypted emails. Remember, both the sender and recipient need valid certificates to send encrypted emails.

PRACTICAL 8

AIM: To extract and analyze metadata from various file types (image, document, and video) using metadata analysis tools such as and , and to understand the significance of metadata in digital forensics and information security.

Metadata Analysis Tools by File Type

1.Images , Videos & Other

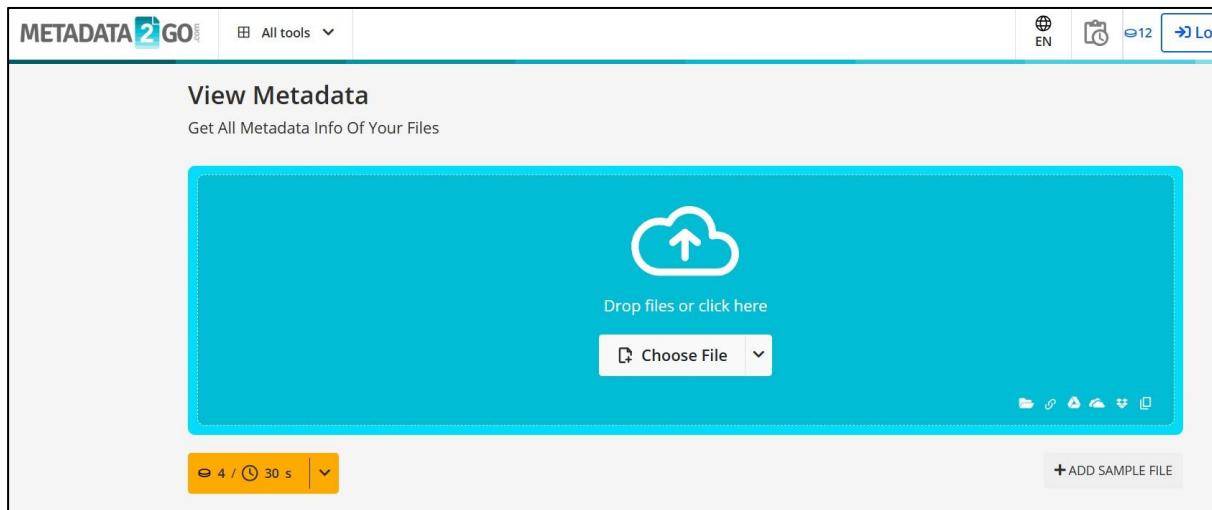
ExifTool: A powerful command-line utility that reads, writes, and edits metadata for a wide range of file formats, including images. It supports metadata types like EXIF, IPTC, and XMP Command : exiftool image.jpg

```
(kali㉿kali)-[~/Downloads]
$ exiftool Untitled.jpeg
ExifTool Version Number      : 13.10
File Name                   : Untitled.jpeg
Directory                   :
File Size                   : 7.6 kB
File Modification Date/Time : 2025:04:22 01:20:56-04:00
File Access Date/Time       : 2025:04:22 01:20:56-04:00
File Inode Change Date/Time: 2025:04:22 01:20:56-04:00
File Permissions            : -rw-rw-r--
File Type                  : JPEG
File Type Extension         : jpg
MIME Type                  : image/jpeg
JFIF Version               : 1.01
Resolution Unit             : None
X Resolution                : 1
Y Resolution                : 1
Image Width                 : 195
Image Height                : 183
Encoding Process            : Baseline DCT, Huffman coding
Bits Per Sample              : 8
Color Components             : 3
Y Cb Cr Sub Sampling        : YCbCr4:2:0 (2 2)
Image Size                  : 195×183
Megapixels                  : 0.036
```

2. Documents (e.g., PDFs, Word Files)

ExifTool: Also supports metadata extraction from various document formats.

Metadata2Go: Supports document files, enabling you to upload and analyze metadata from PDFs, Word documents, and more.



checksum	fddff0a2036635598be92c8c0045e1bd5
file_name	practical-1.pdf
file_size	481 kB
file_type	PDF
file_type_extension	pdf
mime_type	application/pdf
pdf_version	1.7
linearized	No
page_count	7
language	en

tagged_pdf	Yes
xmp_toolkit	3.1-701
producer	Microsoft® Word 2019
creator	CYBER
creator_tool	Microsoft® Word 2019
create_date	2025:03:11 16:57:15+05:30
modify_date	2025:03:11 16:57:15+05:30
document_id	uuid:C16B5BC4-AE47-40A3-9983-761CEA1B7A20
instance_id	uuid:C16B5BC4-AE47-40A3-9983-761CEA1B7A20
author	CYBER
category	application

Conclusion:

Metadata analysis is a critical component of digital forensics and information security, providing valuable contextual information about files—such as creation dates, authorship, geolocation data, device information, and modification history. By extracting and analyzing metadata from various file types, including images, documents, and videos, investigators can uncover hidden insights that are often invisible in the file content itself.

PRACTICAL 9

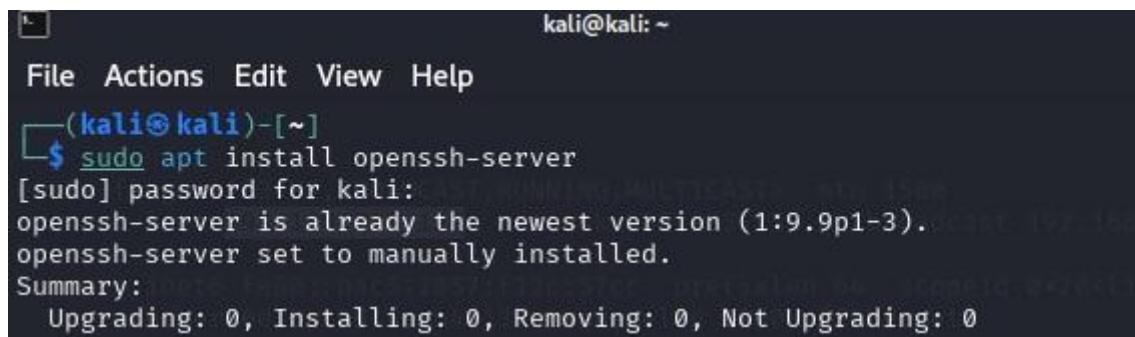
AIM: To configure SSH (Secure Shell) for secure remote communication between systems and to verify the configuration by securely sending and receiving a file over the SSH connection using the configured parameters.

Definition : SSH (Secure Shell) is a protocol that provides a secure channel over an unsecured network by using encryption for remote login, command execution, and file transfer between two networked devices.

Step 1: Install SSH (if not already installed)

Command : sudo apt update

```
sudo apt install openssh-server
```

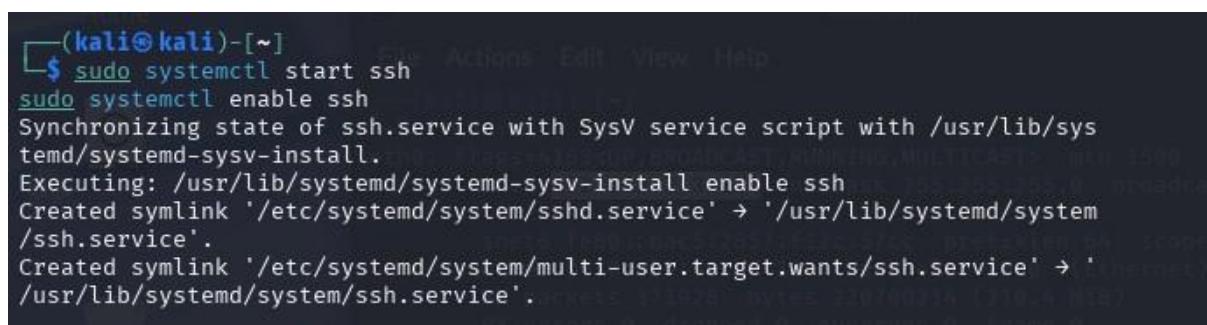


```
kali@kali: ~
File Actions Edit View Help
[(kali㉿kali)-[~]]$ sudo apt install openssh-server
[sudo] password for kali:
openssh-server is already the newest version (1:9.9p1-3).
openssh-server set to manually installed.
Summary:
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0
```

Step 2: Start and Enable SSH Service

Command : sudo systemctl start ssh

```
sudo systemctl enable ssh
```



```
[(kali㉿kali)-[~]]$ sudo systemctl start ssh
[sudo] password for kali:
Synchronizing state of ssh.service with SysV service script with /usr/lib/sys
temd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system
/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '
/usr/lib/systemd/system/ssh.service'.
```

Step 3: Check SSH Status

Command : sudo systemctl status ssh

```
(kali㉿kali)-[~]
$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
  Active: active (running) since Tue 2025-04-22 00:14:23 EDT; 24s ago
    Invocation: b14cb92a4e324e8e9c31993377962b64
      Docs: man:sshd(8)
             man:sshd_config(5)
    Main PID: 58766 (sshd)
      Tasks: 1 (limit: 2199)
     Memory: 2.3M (peak: 2.8M)
        CPU: 141ms
       CGroup: /system.slice/ssh.service
               └─58766 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup"

Apr 22 00:14:23 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell...
Apr 22 00:14:23 kali sshd[58766]: Server listening on 0.0.0.0 port 22.
Apr 22 00:14:23 kali sshd[58766]: Server listening on :: port 22.
Apr 22 00:14:23 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell.

[lines 1-17/17 (END)]
```

Step 4: Configure SSH (optional but recommended)

Command : sudo nano /etc/ssh/sshd_config

Edit in File : Port 22

PermitRootLogin no , PasswordAuthentication yes

PermitEmptyPasswords no

```
kali㉿kali: ~
File Actions Edit View Help
GNU nano 8.3
/etc/ssh/sshd_config
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
#PubkeyAuthentication yes
#Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
#AuthorizedPrincipalsFile none
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes
# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication yes
#PermitEmptyPasswords no
# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPISKeyExchange no
# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication. Depending on your PAM configuration,
# PAM authentication via KbdInteractiveAuthentication may bypass
```

Step 5 : Then restart the SSH service to apply changes:

Command :sudo systemctl restart ssh

```
(kali㉿kali)-[~]
└$ sudo systemctl restart ssh
```

Step 6 :Test SSH Connection

From System A, connect to System B: Access kali machine in windows

Command :ssh kali@192.168.213.128

```
C:\Users\bhone>ssh kali@192.168.213.128
The authenticity of host '192.168.213.128 (192.168.213.128)' can't be established.
ED25519 key fingerprint is SHA256:XhdVUyLGd5dnLlCbUcRze+5VJERtdQiZs8FJY7oH+qQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.213.128' (ED25519) to the list of known hosts.
kali@192.168.213.128's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

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

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(kali㉿kali)-[~]
└$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali㉿kali)-[~]
└$ cd Downloads
```

Step 7: Receive a File from Remote to Local

Copy a file from the remote system to your local machine:

```
(kali㉿kali)-[~/Downloads]
└$ scp download.pdf kali@192.168.213.128:C:\Users\bhone
kali@192.168.213.128's password:
download.pdf
```

Conclusion:

Configuring SSH (Secure Shell) is a fundamental step in ensuring secure remote communication between systems. SSH provides encrypted channels that protect data in transit from eavesdropping, tampering, and unauthorized access, making it a critical component in system administration and network security.

PRACTICAL 10

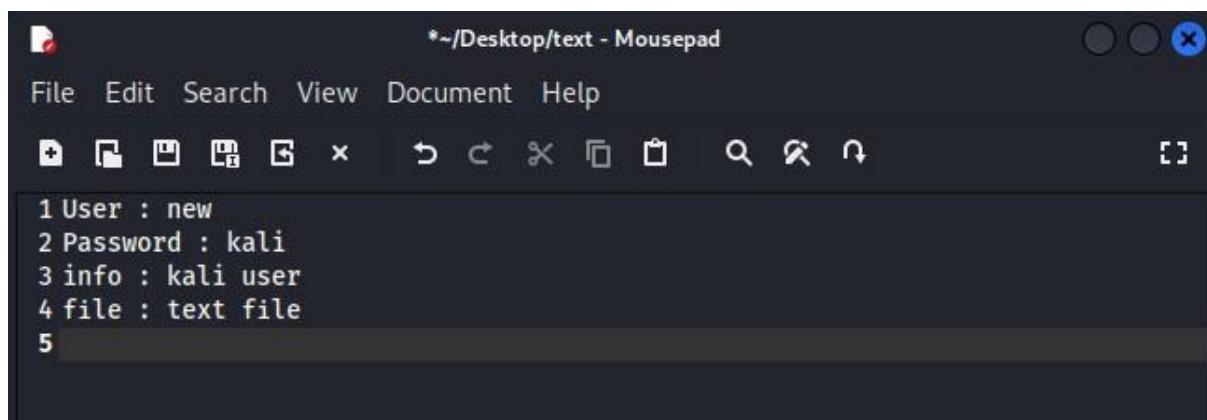
AIM: To implement encryption and decryption with OpenSSL.

Definition: OpenSSL is a powerful command-line tool that facilitates encryption and decryption using various cryptographic algorithms.

Symmetric Encryption (Password-Based)

Symmetric encryption uses the same password for both encryption and decryption.

Step 1: Create text file



Step 2: Encrypting a File

Command : openssl enc -aes-256-cbc -salt -pbkdf2 -in text.txt -out encrypted.enc

```
(kali㉿kali)-[~/Desktop]
$ cat text
User : new
Password : kali
info : kali user
file : text file

(kali㉿kali)-[~/Desktop]
$ openssl enc -aes-256-cbc -salt -pbkdf2 -in text.txt -out encrypted.enc

enter AES-256-CBC encryption password:
Verifying - enter AES-256-CBC encryption password:

(kali㉿kali)-[~/Desktop]
$ ls
encrypted.enc  text.txt

(kali㉿kali)-[~/Desktop]
$ cat encrypted.enc
Salted__6]`*****Tn**S***ss*HVY,&c?***Ua_t***q_*U***d***
```

Explanation:

- enc: Specifies the encryption command.
- -aes-256-cbc: Uses the AES algorithm with a 256-bit key in CBC mode.
- -salt: Adds a random salt to strengthen encryption.
- -pbkdf2: Applies the PBKDF2 key derivation function for enhanced security.
- -in plaintext.txt: Specifies the input file to encrypt.
- -out encrypted.enc: Specifies the output encrypted file.

Step 3: Decrypting a File

Command : openssl enc -d -aes-256-cbc -salt -pbkdf2 -in encrypted.enc -out decrypted.txt

```
(kali㉿kali)-[~/Desktop]
$ openssl enc -d -aes-256-cbc -salt -pbkdf2 -in encrypted.enc -out decrypted.txt
enter AES-256-CBC decryption password:

(kali㉿kali)-[~/Desktop]
$ ls
decrypted.txt  encrypted.enc  e.txt  text.txt

(kali㉿kali)-[~/Desktop]
$ cat decrypted.txt
User : new
Password : kali
info : kali user
file : text file
```

Explanation:

- -d: Indicates decryption mode.
- Other parameters mirror those used during encryption.

Conclusion: Successfully perform encryption and decryption using open ssl

Conclusion:

Implementing encryption and decryption using OpenSSL is a practical and essential step in understanding how data confidentiality and integrity are maintained in secure communication. OpenSSL provides a powerful set of tools and libraries that support a wide range of cryptographic functions, including symmetric and asymmetric encryption, hashing, and digital certificates.