PRACTICAL 1

DATE: 05/01/2025

AIM: Scan Vulnerabilities Using Nmap.

Nmap:

- Nmap, or Network Mapper, is a free, open-source network security tool that scans networks for vulnerabilities and security issues.

Command Used To Scan Vulnerabilities:

- nmap --script <IP address> -v

FlowChart:

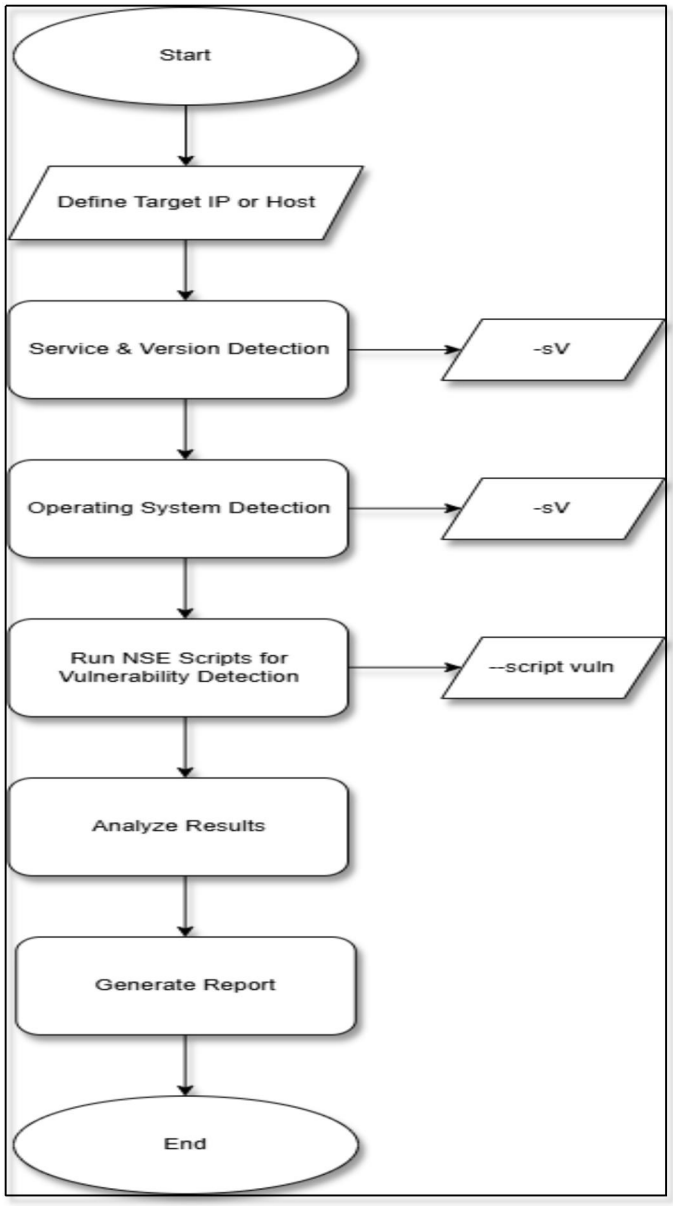

Figure 1

Output:

Step 1: Use nmap -p- --script vuln <ip address> -v Command To Scan The Vulnerability.

```
┌──(punit㉿kali)-[~]
└─$ nmap -p- --script vuln 192.168.40.129 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 19:57 IST
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:57
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE: Active NSE Script Threads: 1 (1 waiting)
NSE Timing: About 0.00% done
Completed NSE at 19:57, 10.01s elapsed
Initiating NSE at 19:57
Completed NSE at 19:57, 0.00s elapsed
Initiating ARP Ping Scan at 19:57
Scanning 192.168.40.129 [1 port]
Completed ARP Ping Scan at 19:57, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:57
Completed Parallel DNS resolution of 1 host. at 19:57, 0.02s elapsed
Initiating SYN Stealth Scan at 19:57
Scanning 192.168.40.129 [65535 ports]
Discovered open port 25/tcp on 192.168.40.129
Discovered open port 80/tcp on 192.168.40.129
Discovered open port 21/tcp on 192.168.40.129
Discovered open port 3306/tcp on 192.168.40.129
Discovered open port 445/tcp on 192.168.40.129
Discovered open port 53/tcp on 192.168.40.129
Discovered open port 5900/tcp on 192.168.40.129
Discovered open port 23/tcp on 192.168.40.129
Discovered open port 139/tcp on 192.168.40.129
Discovered open port 111/tcp on 192.168.40.129
Discovered open port 22/tcp on 192.168.40.129
Discovered open port 56099/tcp on 192.168.40.129
Discovered open port 38509/tcp on 192.168.40.129
Discovered open port 42648/tcp on 192.168.40.129
Discovered open port 2121/tcp on 192.168.40.129
Discovered open port 5432/tcp on 192.168.40.129
Discovered open port 33306/tcp on 192.168.40.129
Discovered open port 8180/tcp on 192.168.40.129
Discovered open port 513/tcp on 192.168.40.129
```

Figure 2

```
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_      https://www.securityfocus.com/bid/48539
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_  The SMTP server is not Exim: NOT VULNERABLE
| ssl-poodle:
|   VULNERABLE:
|   SSL POODLE information leak
|     State: VULNERABLE
|     IDs:  CVE:CVE-2014-3566  BID:70574
|           The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other
|           products, uses nondeterministic CBC padding, which makes it easier
|           for man-in-the-middle attackers to obtain cleartext data via a
|           padding-oracle attack, aka the "POODLE" issue.
|     Disclosure date: 2014-10-14
|     Check results:
|       TLS_RSA_WITH_AES_128_CBC_SHA
|     References:
|       https://www.imperialviolet.org/2014/10/14/poodle.html
|       https://www.securityfocus.com/bid/70574
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
```

Figure 3

Figure 4

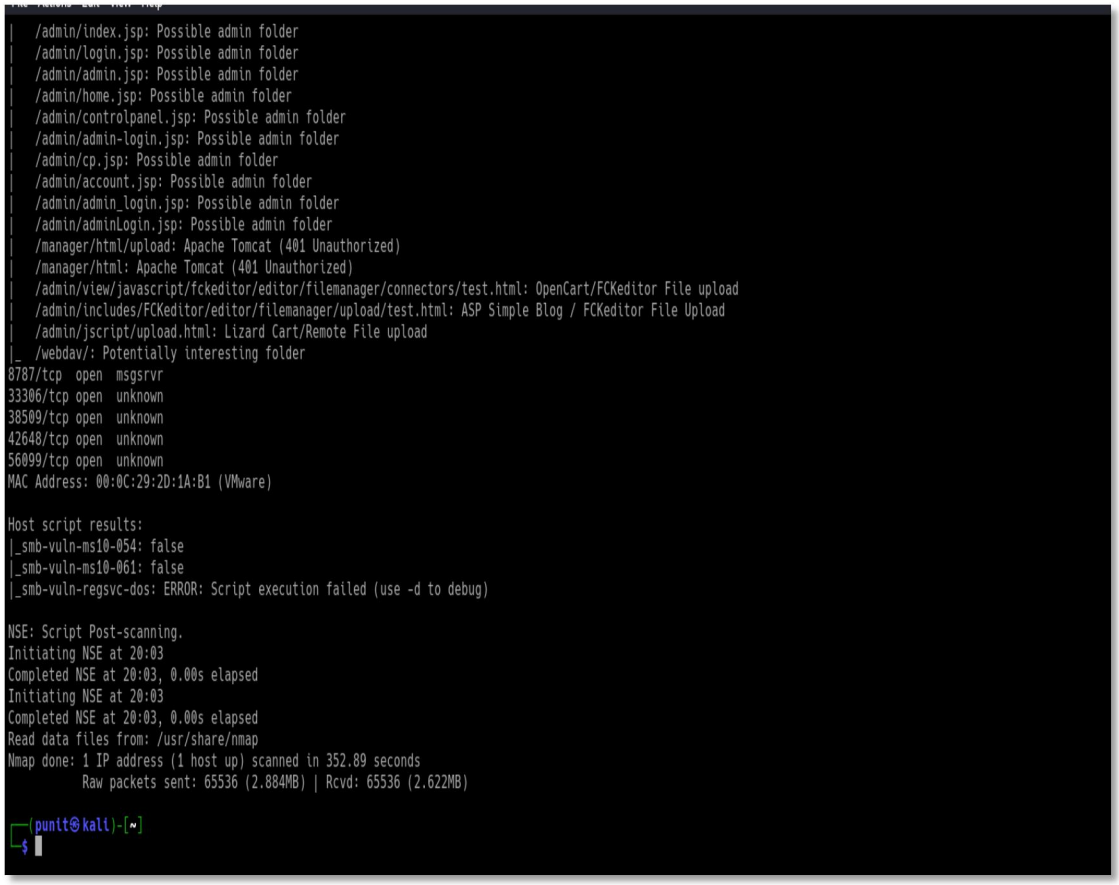

Figure 5

Conclusion:

Nmap is that it is a powerful tool for network security professionals to identify and address vulnerabilities on a network. Nmap is a free, open-source network scanning tool that can help network professionals to enhance their network understanding and strengthen their digital defenses.

PRACTICAL 2

DATE: 23/01/2025

AIM: To Understand the concept and Importance of cyber threat Intelligence and hunting.

Understanding Cyber Threat Intelligence (CTI)

Cyber Threat Intelligence (CTI) refers to the collection, analysis, and dissemination of information about current or potential cyber threats. The goal is to provide actionable insights to organizations to protect their systems, networks, and data from cyberattacks.

What is CTI?

Cyber threat intelligence (CTI) is a cybersecurity field that involves collecting, analyzing, and sharing information about cyber threats. CTI helps organizations understand and respond to cyber threats by identifying vulnerabilities and threat actors.

Importance of CTI in Real Life?

Cyber Threat Intelligence (CTI) plays a crucial role in modern cybersecurity by providing actionable insights to proactively identify, prevent, and respond to cyber threats. Here's how CTI is important in real-life scenarios:

Proactive Threat Identification

- Example: CTI helps organizations recognize indicators of compromise (IoCs) such as suspicious IP addresses or malware signatures. This allows them to patch vulnerabilities before an attack occurs.

Enhancing Incident Response

- Example: During a ransomware attack, CTI provides insights about the ransomware family, its attack vectors, and decryption methods.

Reducing False Positives

- Example: Security tools often generate numerous alerts, many of which are false positives. CTI refines this data by prioritizing alerts based on verified intelligence.

Tailoring Security Defenses

- Example: CTI identifies industry-specific threats (e.g., healthcare ransomware attacks) and helps organizations adapt their defenses accordingly.

Enabling Threat Actor Profiling

- Example: By analyzing CTI, organizations can understand attacker motives, techniques, and tools.

Understanding Cyber Threat Hunting

Cyber Threat Hunting is a proactive approach to identifying and mitigating threats within an organization's environment. Unlike reactive methods (e.g., responding to alerts), hunting involves actively searching for hidden threats that evade traditional security measures.

Importance of Threat Hunting

1. **Identifying Advanced Threats:** Finds sophisticated threats like zero-day attacks and APTs that bypass traditional defenses.
2. **Reducing Dwell Time:** Shortens the time attackers spend undetected within a network.
3. **Improving Defenses:** Insights gained during hunts are used to strengthen an organization's security posture.
4. **Complementing Automation**: While automation handles routine threats, hunting focuses on advanced adversaries.

Conclusion:

Understanding cyber threat intelligence (CTI) and threat hunting is vital in today's digital landscape where cyber threats are increasingly sophisticated and persistent. CTI provides actionable insights into potential threats, helping organizations anticipate, detect, and respond to attacks more effectively. Threat hunting complements this by proactively searching for hidden threats within a network before they cause harm. Together, these practices enhance an organization's security posture, reduce response time, and support informed decision-making. Investing in CTI and threat hunting is no longer optional it's a critical element of modern cybersecurity strategy.

PRACTICAL 3

DATE: 23/01/2025

AIM: To gain Knowledge about framework, tools, and Technique for CTI and Threat-Hunting Operation.

What is CTI?

Cyber threat intelligence (CTI) is a cybersecurity field that involves collecting, analyzing, and sharing information about cyber threats. CTI helps organizations understand and respond to cyber threats by identifying vulnerabilities and threat actors.

Importance of CTI in Real Life?

Cyber Threat Intelligence (CTI) plays a crucial role in modern cybersecurity by providing actionable insights to proactively identify, prevent, and respond to cyber threats. Here's how CTI is important in real-life scenarios:

Proactive Threat Identification

- Example: CTI helps organizations recognize indicators of compromise (IoCs) such as suspicious IP addresses or malware signatures. This allows them to patch vulnerabilities before an attack occurs.

Enhancing Incident Response

- Example: During a ransomware attack, CTI provides insights about the ransomware family, its attack vectors, and decryption methods.

Reducing False Positives

- Example: Security tools often generate numerous alerts, many of which are false positives. CTI refines this data by prioritizing alerts based on verified intelligence.

Tailoring Security Defenses

- Example: CTI identifies industry-specific threats (e.g., healthcare ransomware attacks) and helps organizations adapt their defenses accordingly.

Enabling Threat Actor Profiling

- Example: By analyzing CTI, organizations can understand attacker motives, techniques, and tools.

CTI Frameworks:

MITRE ATT&CK:

The **MITRE ATT&CK framework** is a comprehensive knowledge base of tactics, techniques, and procedures (TTPs) used by cyber attackers. Developed by MITRE, it helps organizations understand and analyze adversary behavior across different stages of a cyber attack. The framework is widely used for threat modeling, detection, and improving cybersecurity defenses.

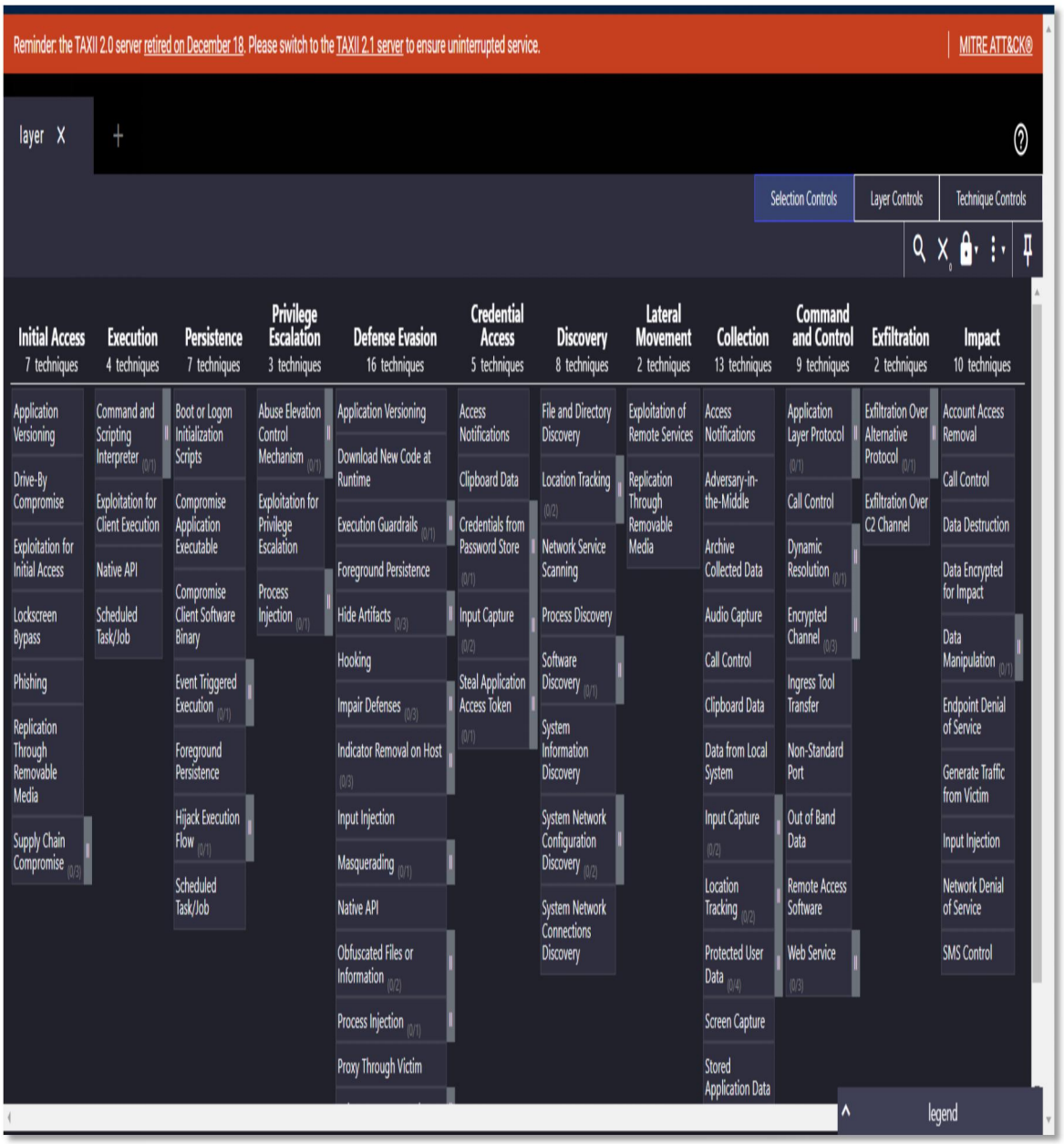

Figure 6

LOCKHEED MARTIN CYBER KILL CHAIN:

The Lockheed Martin Cyber Kill Chain is a cybersecurity framework that outlines the stages of a cyber attack, helping organizations detect and respond to threats at each phase. Developed by Lockheed Martin, it breaks an attack into seven sequential steps: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2), and Actions on Objectives.

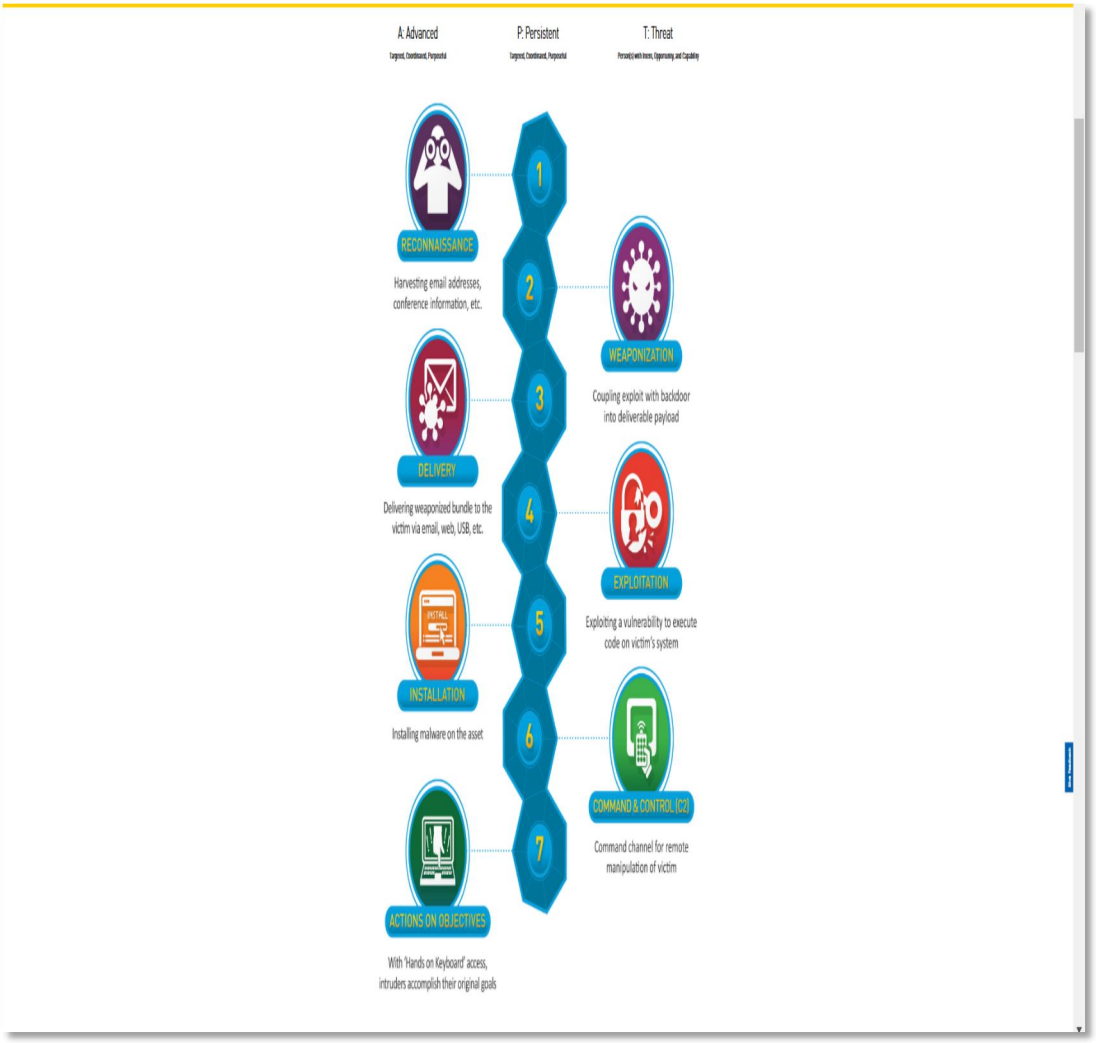

Figure 7

DIAMOND MODEL OF INTRUSION ANALYSIS:

The Diamond Model of Intrusion Analysis is a cybersecurity framework used to analyze and understand cyber threats by examining relationships between four key components: Adversary, Infrastructure, Capability, and Victim. It visualizes attacks as a diamond, with each corner representing one of these elements. By exploring how these elements interact, analysts can track adversary behavior, uncover patterns, and improve threat detection and response.

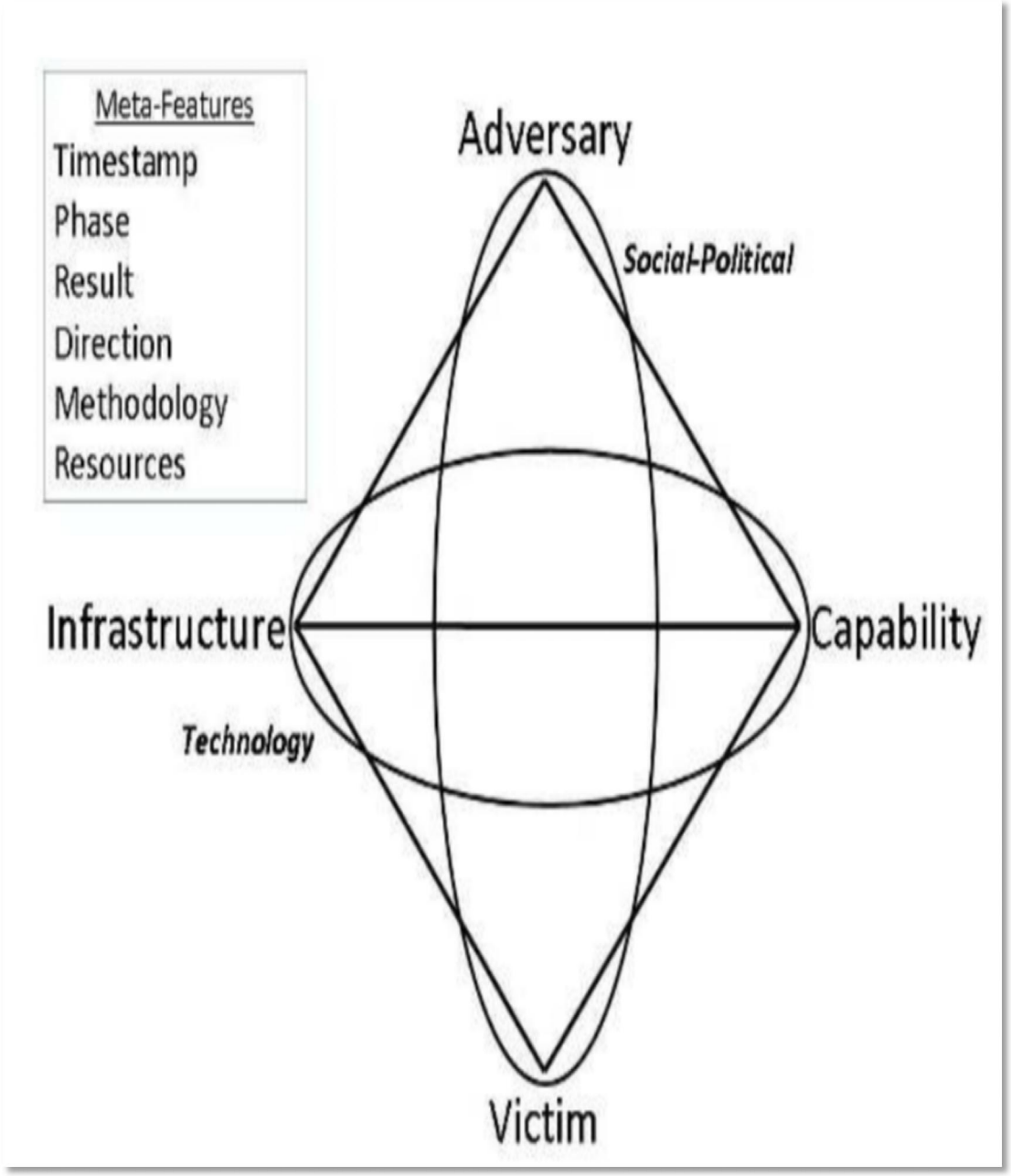

Figure 8

TECHNIQUES OF CTI:

1. Indicator of Compromise (IOC) Analysis
2. Tactics, Techniques, and Procedures (TTP) Analysis
3. Threat Hunting
4. Phishing Campaign Analysis
5. Attribution Analysis

Conclusion:

Gaining knowledge about the frameworks, tools, and techniques for Cyber Threat Intelligence (CTI) and threat hunting operations is essential for building a strong and proactive cybersecurity defense. Frameworks such as MITRE ATT&CK and tools like SIEMs, threat intelligence platforms, and endpoint detection solutions provide structure and capabilities to identify, analyze, and mitigate threats effectively. Techniques including anomaly detection, behavioral analysis, and hypothesis-driven investigations empower security teams to uncover hidden threats and reduce dwell time. A deep understanding of these elements not only strengthens an organization's threat detection capabilities but also enhances its overall resilience against evolving cyber threats.

PRACTICAL 4

Date: 10/02/2025

AIM: To develop skills in intelligence analysis, IOCs, and CTI sharing and collaboration.

Theory:

IP (Internet Protocol):

- An IP address is a unique identifier for a device on a network. In the context of cyber threat analysis, an IP address can be associated with malicious activities (e.g., botnet command and control, DDoS attacks, etc.).

Virus Total:

- VirusTotal is a free online tool that analyzes files and URLs to detect malware, viruses, trojans, and other types of malicious content.

- **Use in Threat Intelligence:** By uploading files (e.g., executables or suspicious documents) or providing URLs to VirusTotal, you can quickly gather intelligence on potential threats, learn more about their behavior, and share your findings with the security community.

Nmap (Network Mapper):

- Nmap allows security professionals to scan networks for vulnerabilities or suspicious activities, such as unauthorized open ports or services that might be exploited by attackers.

Flowchart:

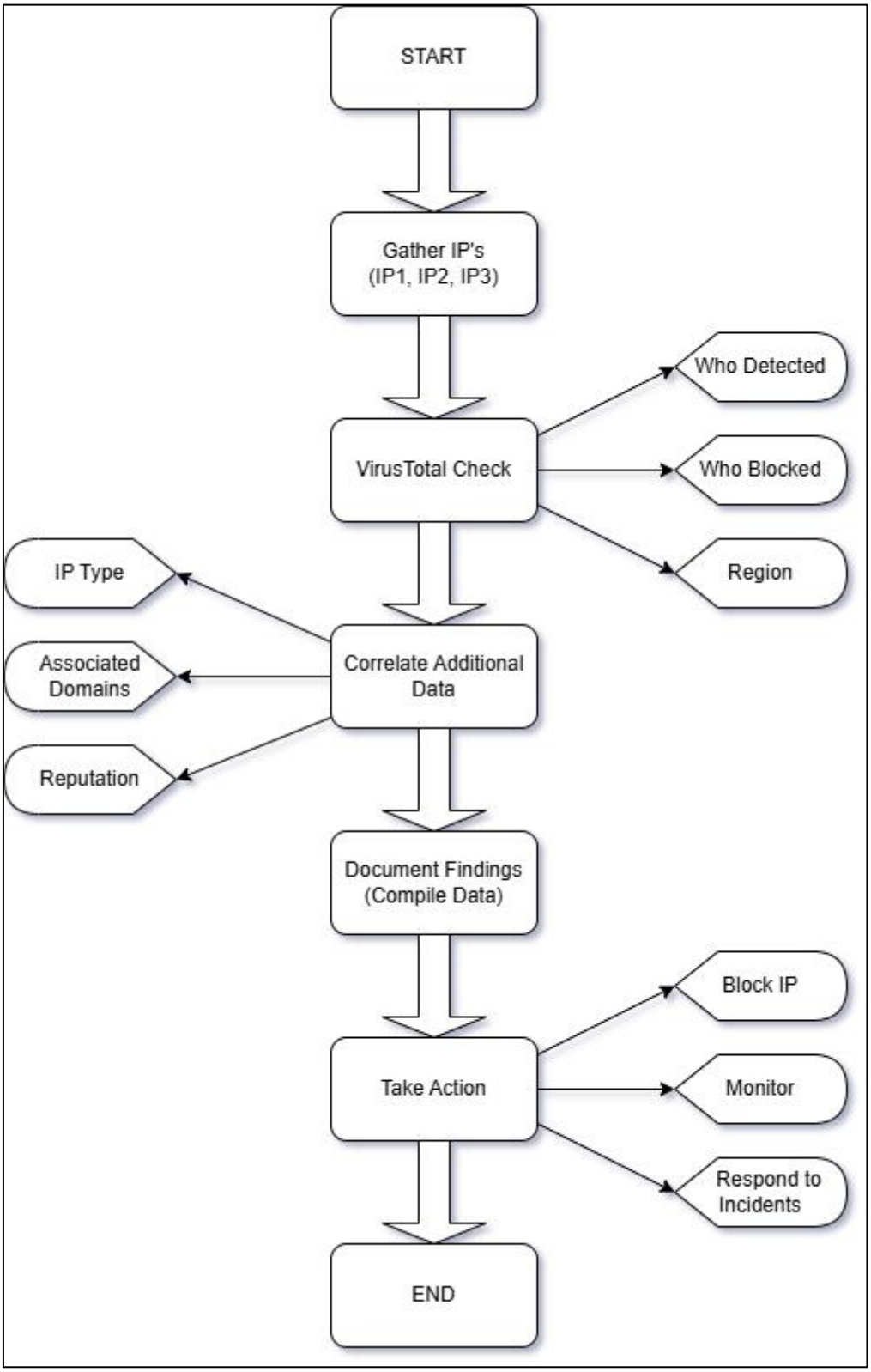

Figure 9

Report:

Scope	IP1(73.32.175.15)	IP2(31.3.96.40)	IP3(45.84.107.198)
From Where You Get	MaxMind	Google	MaxMind
Who Blocked	-	-	-
Who Detected	MalwareURL	MalwareURL	Criminal IP
Attacks	-	-	-
Region	US	NetherLand	Sweden
Service	ftp	https	tor-orport
Open Ports	21/tcp	80/tcp	443/tcp
Version	-	Apache httpd	Tor 0.3.1.1 or later

Figure 10

Conclusion:

Developing skills in intelligence analysis, Indicators of Compromise (IOCs), and Cyber Threat Intelligence (CTI) sharing and collaboration is crucial for effective threat detection and response. Intelligence analysis enables security professionals to make sense of complex data and identify meaningful patterns, while understanding IOCs helps in recognizing signs of compromise early. Furthermore, CTI sharing and collaboration across organizations and sectors strengthen collective defense by promoting transparency, faster threat identification, and coordinated responses. Mastering these skills not only enhances individual capability but also contributes significantly to the broader cybersecurity ecosystem.

PRACTICAL 5

DATE: 17-04-2025

AIM: To learn about CTI and threat hunting operations and incident response planning.

SR. No	Properties	04eda293e486872c3ad9353b5bde5bae	04ef876b2ba1a6836641dc875f1cf52a
1	**Type of hash**	MD5	MD5
2	**Analysis Date**	2025-03-16 11:46:47 UTC	2024-06-05 14:49:45 UTC
3	**Creation Time**	2013-04-09 15:54:09 UTC	2016-10-06 14:33:38 UTC
4	**Name**	amstream.dll	sys.dll
5	**Target Machine**	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	**Security Vendor Analysis**	AhnLab-V3-Trojan/Win32.Banker.R56908 Alibaba-TrojanSpy:Win32/Banker.117f3d7f AliCloud - Backdoor:Win/Bradop.A ALYacGen :-Trojan.Heur.bnSfremII5DU Antiy-AVL - Trojan/Win32.BHO	AlibabaTrojanBanker:Win32/Ghoul.054e2f69 Antiy-AVLTrojan/Win32.SGeneric AvastWin32:AgentBanker-A [Bank] AVGWin32:AgentBanker-A [Bank] Avira (no cloud)HEUR/AGEN.1328858
7	**Type of Attack**	Trojan	Trojan
8	**IP**	-	-
9	**Behaviour**	-	-
10	**Modules Involved**	-	-

Figure 11

SR. No	Properties	04f48c7dad83b583eaff571af1149473	04f4d2915c4125570df7bb2640f543da
1	**Type of hash**	MD5	MD5
2	**Analysis Date**	2021-01-26 18:39:27 UTC	2021-02-05 04:12:32 UTC
3	**Creation Time**	2013-10-31 10:10:49 UTC	1992-06-19 22:22:17 UTC
4	**Name**	siswin32.exe	Boleto_Numero_472390574343.cpl
5	**Target Machine**	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	**Security Vendor Analysis**	Ad-AwareGen:Variant.Johnnie.18512 AlibabaTrojan:Win32/BANKER.6d0c4efb ALYacGen:Variant.Johnnie.18512 ArcabitTrojan.Johnnie.D4850 AvastWin32:Malware-gen	Ad-AwareGen:Variant.Graftor.184869 AhnLab-V3Trojan/Win32.ChePro.R139734 AlibabaTrojanDownloader:Win32/Banload.8feaaf21 ALYacGen:Variant.Graftor.184869 Antiy-AVLTrojan[Banker]/Win32.ChePro
7	**Type of Attack**	Trojan	Trojan
8	**IP**	-	-
9	**Behaviour**	Modify registry of startup	-
10	**Modules Involved**	C:\WINDOWS\system32\MSCTF.dll C:\WINDOWS\system32\kernel32.dll C:\WINDOWS\system32\msctfime.ime	-

Figure 12

SR. No	Properties	04f9615f20a930c85391ec6432ec899f	04faf3609b7f1739fa006d97dc54b03d
1	Type of hash	MD5	MD5
2	Analysis Date	2025-03-22 00:50:55 UTC	2021-02-14 13:59:26 UTC
3	Creation Time	1992-06-19 22:22:17 UTC	2017-06-16 17:46:42 UTC
4	Name	index.php.exe.vir	CodigodeRastreio_CJ463077332BR.exe
5	Target Machine	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	Security Vendor Analysis	AlibabaTrojanDownloader:Win32/Banload.0773dd28 AliCloudTrojan[downloader]:Win/Banload.QML ALYacTrojan.Crypt.Delf.AG Antiy-AVLTrojan/Win32.Agent ArcabitTrojan.Crypt.Delf.AG	Ad-AwareTrojan.GenericKD.5377634 AegisLabTrojan.Win32.Generic.4!c AhnLab-V3Trojan/Win32.Banload.C2031854 AlibabaTrojanDownloader:MSIL/Banload.68cc93f8 ALYacTrojan.GenericKD.5377634
7	Type of Attack	Trojan	Trojan
8	IP	-	-
9	Behaviour	Modify registry of UAC	Access CPU clock directly
10	Modules Involved	ADVAPI32.dll C:\WINDOWS\System32\wshtcpip.dll C:\WINDOWS\system32\MSCTF.dll C:\WINDOWS\system32\Msctf.dll	ADVAPI32.dll AdvApi32.dll C:\WINDOWS\System32\wshtcpip.dll

Figure 13

SR. No	Properties	04fe98b96a00e739a7fc0e4804c641f0	04fea0b448de8c6e2ea592efa90056d0
1	Type of hash	MD5	MD5
2	Analysis Date	2021-02-14 11:07:21 UTC	2021-02-05 09:03:04 UTC
3	Creation Time	2008-04-13 18:31:55 UTC	2017-01-19 20:44:00 UTC
4	Name	sndrec32.exe	mtav.exe
5	Target Machine	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	Security Vendor Analysis	Ad-AwareWin32.Valhalla.2048 AhnLab-V3Win32/Valla.2048 AlibabaVirus:Win32/Xorala.9306e3f1 ALYacWin32.Valhalla.2048 Antiy-AVLVirus/Win32.Xorala.b	Ad-AwareTrojan.GenericKD.45131452 AegisLabTrojan.Win32.Bandra.7!c AlibabaTrojanBanker:Win32/Bandra.e3f4270e ALYacTrojan.GenericKD.45131452 Antiy-AVLTrojan[Banker]/Win32.Bandra
7	Type of Attack	Virus	Trojan
8	IP	-	-
9	Behaviour	Modify existing executable file	Access CPU clock directly
10	Modules Involved	comctl32.dll imm32.dll rpcrt4.dll version.dll	cryptbase.dll dwmapi.dll executer.exe gdi32.dll

Figure 14

SR. No	Properties	04fecd302a792283461c57da9f57f98a	04ffefaac4db4191aa9613798a1c232a
1	**Type of hash**	MD5	MD5
2	**Analysis Date**	2025-03-24 10:39:56 UTC	2021-02-01 17:47:59 UTC
3	**Creation Time**	1992-06-19 22:22:17 UTC	2015-07-07 01:16:34 UTC
4	**Name**	any.EXE	HnPFQNyhtEf.exe
5	**Target Machine**	Intel 386 or later processors and compatible processors	Intel 386 or later processors and compatible processors
6	**Security Vendor Analysis**	AhnLab-V3Trojan/Win32.Inject.R27213 AlibabaTrojanDropper:Win32/Dorifel.1e3463f9 AliCloudTrojan[downloader]:Win/Waldek.gen ALYacTrojan.Generic.KD.648583 Antiy-AVLTrojan[Dropper]/Win32.Dorifel	Ad-AwareTrojan.GenericKD.2548349 AlibabaTrojan:Win32/Predator.ali2000022 ALYacTrojan.GenericKD.2548349 ArcabitTrojan.Generic.D26E27D AvastWin32:GenMalicious-LTF [Trj]
7	**Type of Attack**	Trojan	Trojan
8	**IP**	-	-
9	**Behaviour**	-	Modify registry of startup
10	**Modules Involved**	-	C:\Program Files\Common Files\System\wab32.dll C:\Program Files\Common Files\System\wab32res.dll C:\WINDOWS\System32\wshtcpip.dll

Figure 15

Conclusion:

Understanding Cyber Threat Intelligence (CTI), threat hunting operations, and incident response planning is essential for building a robust cybersecurity posture. CTI provides actionable insights into potential threats, helping organizations proactively defend against attacks. Threat hunting complements this by actively seeking out hidden threats within systems, going beyond traditional reactive security measures. Meanwhile, a well-structured incident response plan ensures that when incidents occur, organizations can contain, mitigate, and recover efficiently. Together, these elements form a proactive, layered defense strategy that significantly enhances an organization's ability to detect, respond to, and prevent cyber threats.

PRACTICAL 6

DATE: 21-02-2025

AIM: To gain awareness of emerging trends and ethical considerations in CTI and threat hunting.

Conclusion:

Gaining awareness of emerging trends and ethical considerations in Cyber Threat Intelligence (CTI) and threat hunting is essential for staying ahead in the ever-evolving cybersecurity landscape. As new threats, tactics, and technologies continue to emerge, staying informed enables professionals to adapt and respond proactively. At the same time, ethical considerations—such as privacy, data protection, and responsible intelligence gathering—must remain at the forefront to ensure trust and compliance. Balancing innovation with ethical responsibility is key to building effective and sustainable CTI and threat hunting practices.

PRACTICAL 7 & 8

Date: 28/02/2025

AIM: Conducting a phishing simulation and analyzing the results to identify potential threats.

Zphisher:

A phishing simulation using tools like Zphisher involves creating a fake replica of a legitimate website to deceive users into providing sensitive information, such as login credentials. By cloning an application's login page, setting up a local tunneling service (like LocalXpose), and crafting a convincing message, attackers can lure targets into visiting the fraudulent page, enabling the capture of their credentials. This simulation helps identify vulnerabilities and raises awareness about phishing threats.

Flowchart:

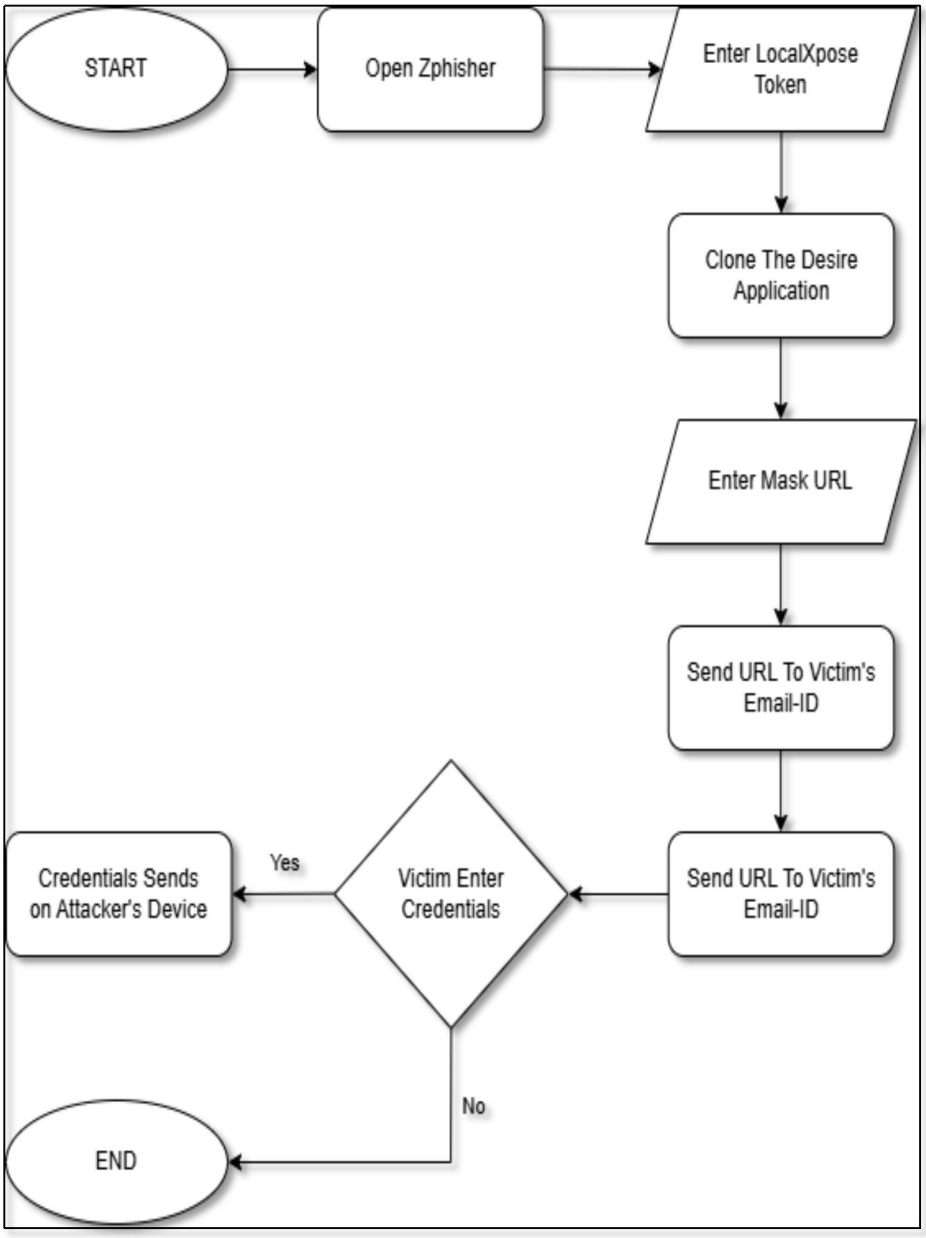

Figure 16

Steps:

1. Install Zpisher Tool Using Github in Kali Linux.

- **git clone --depth=1 https://github.com/htr-tech/zphisher.git**

2. Go into Zphisher Directory and run bash File.

- bash zphisher.sh

3. Select which application you want to clone.

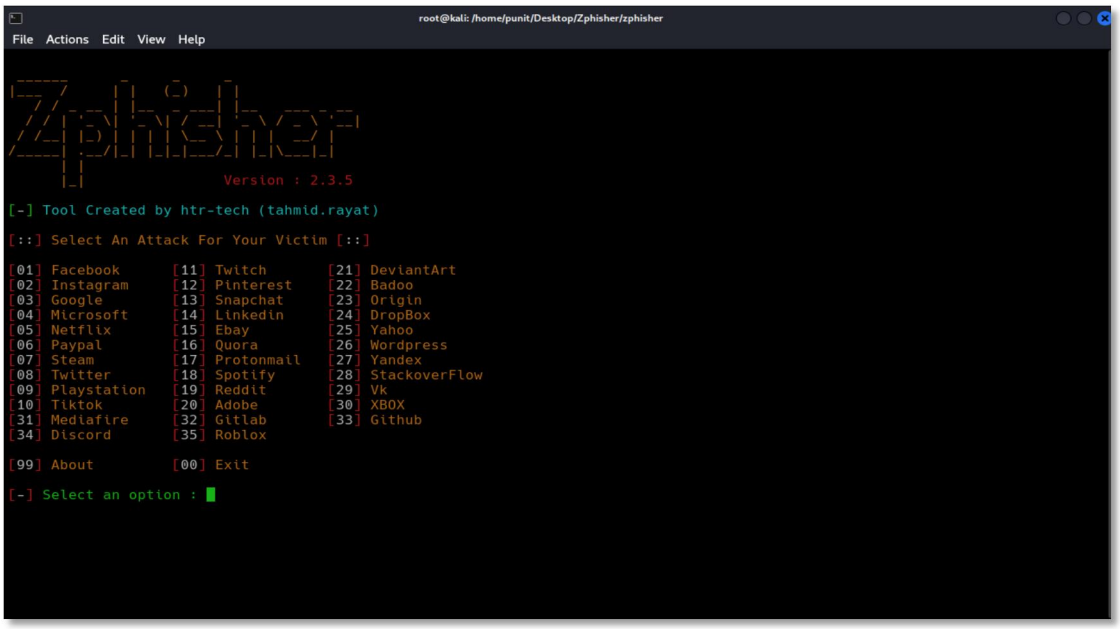

Figure 17

4. Select page of that application.

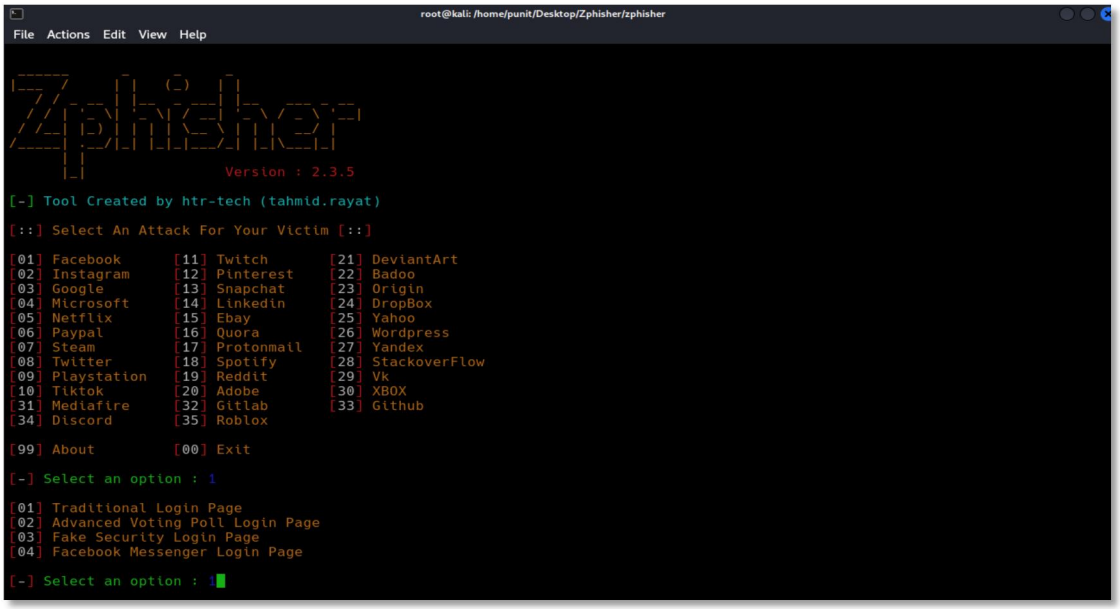

Figure 18

5. Select localxpose and Create account on localxpose using Tempmail and Start the tunnel and Copy the token and Paste it into the terminal.

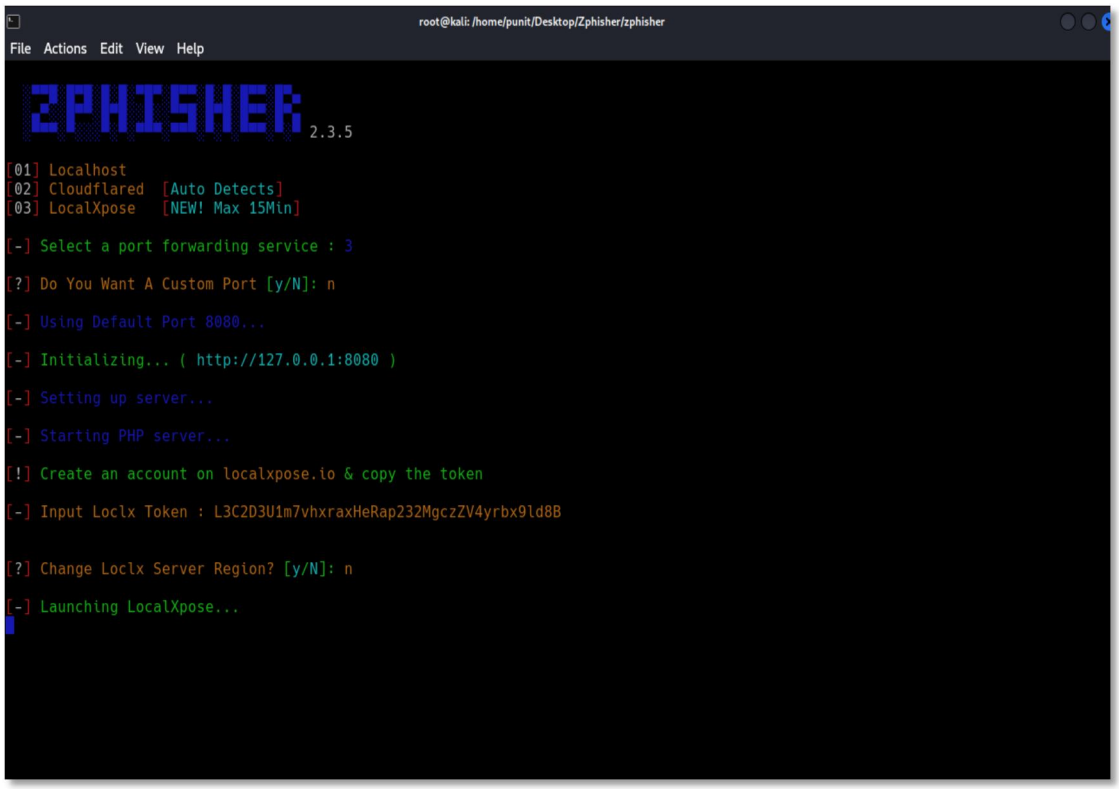

Figure 19

6. Mask URL according to application and you need and open the link.

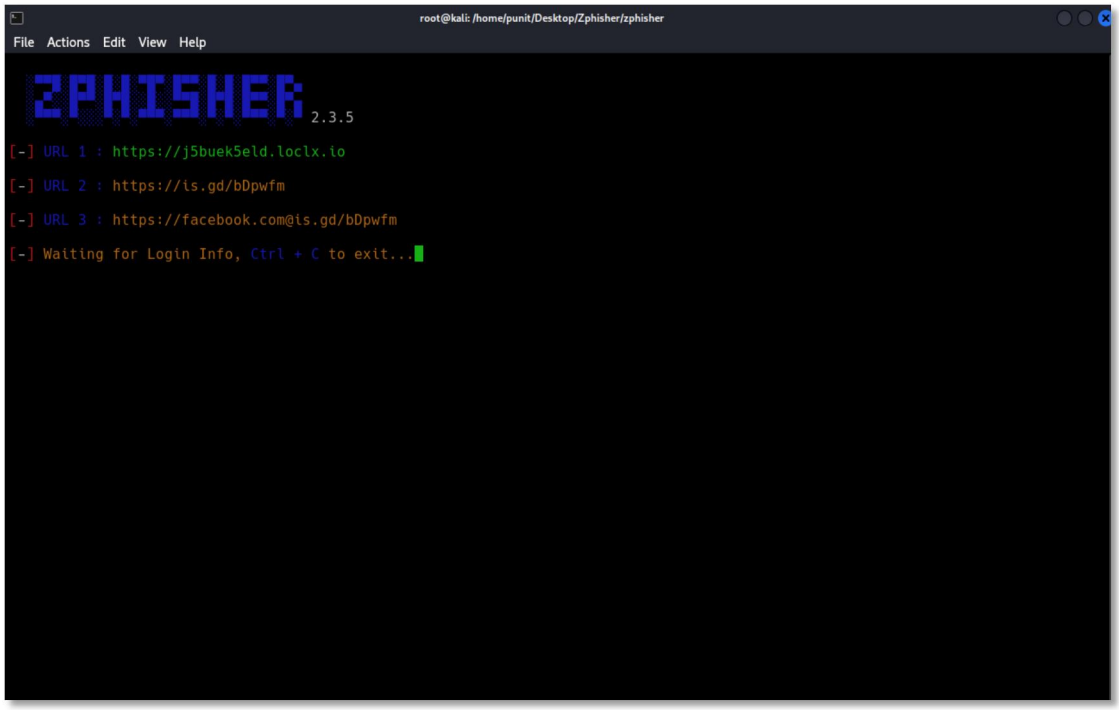

Figure 20

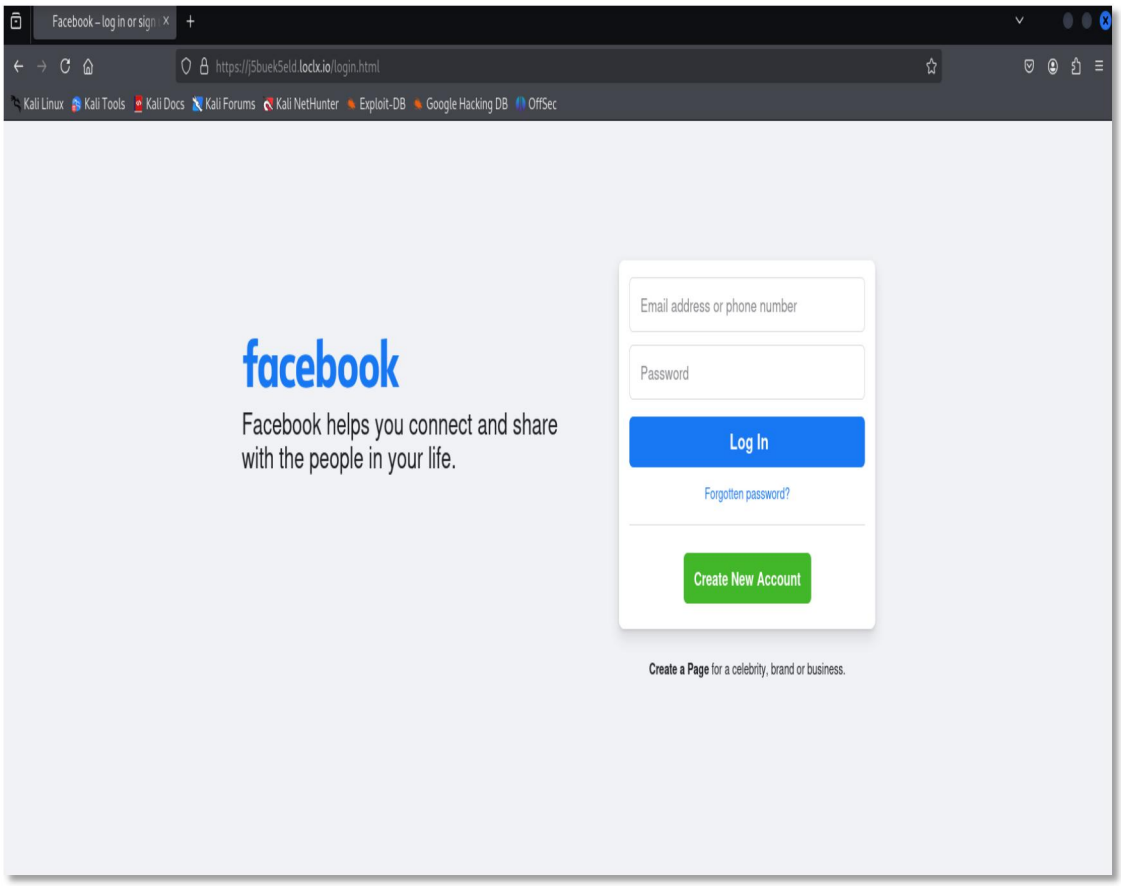

Figure 21

7. Frame a message to trap someone in it to get there credential.

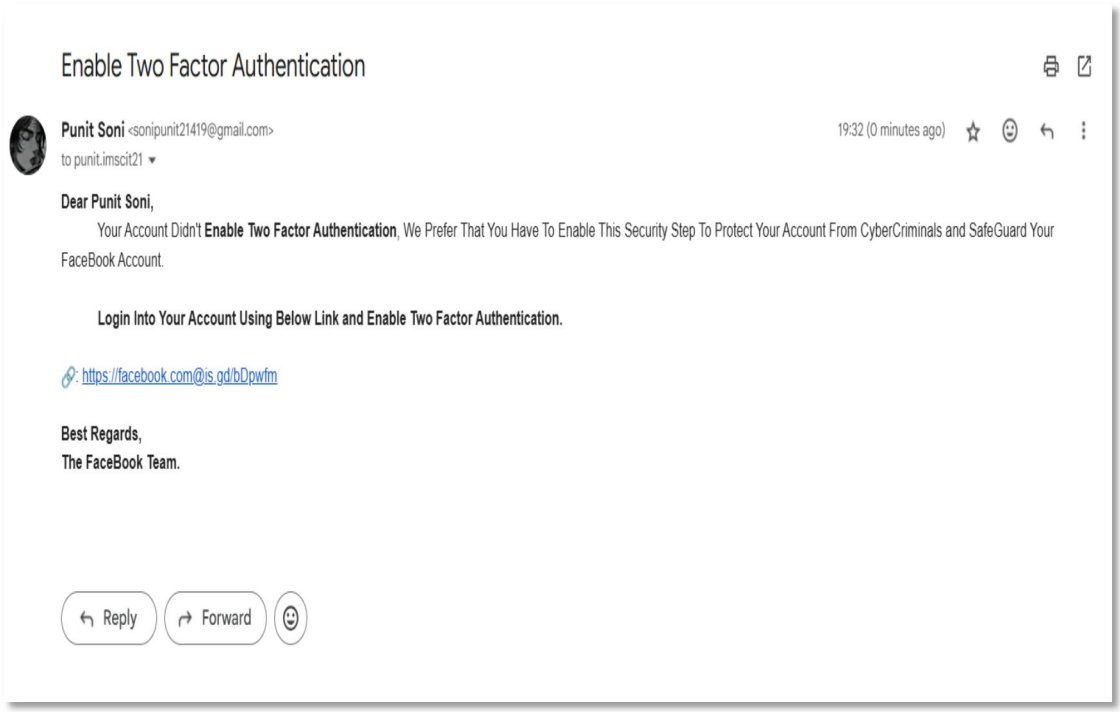

Figure 22

OutPut:

The Victim Entered Their Login Crendential's and that display's on attacker's device.

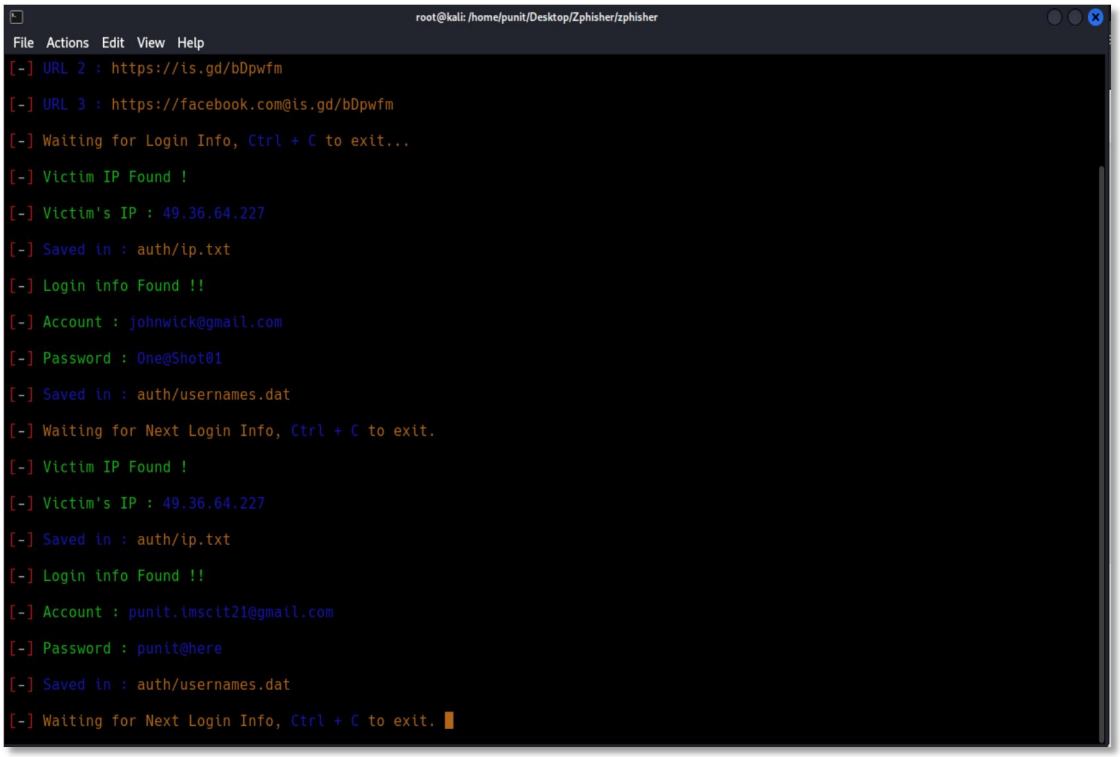

Figure 23

Conclusion:

Zphisher is a phishing tool that automates the creation of phishing pages to steal sensitive information, such as login credentials, from unsuspecting individuals. The tool can simulate login pages of popular websites and services, tricking users into entering their personal data, which could then be exploited for malicious purposes. Using a tool like Zphisher to conduct phishing attacks is illegal and unethical.

While Zphisher and similar tools are often used in ethical hacking contexts for educational purposes or penetration testing with explicit consent, their misuse for fraudulent activities constitutes a crime. Engaging in phishing attacks can lead to severe legal consequences, including criminal charges, fines, and imprisonment.

PRACTICAL - 9

DATE: 11-04-2025

AIM: Conducting a social engineering attack and analyzing the results to identify vulnerabilities - II.

FlowChart:

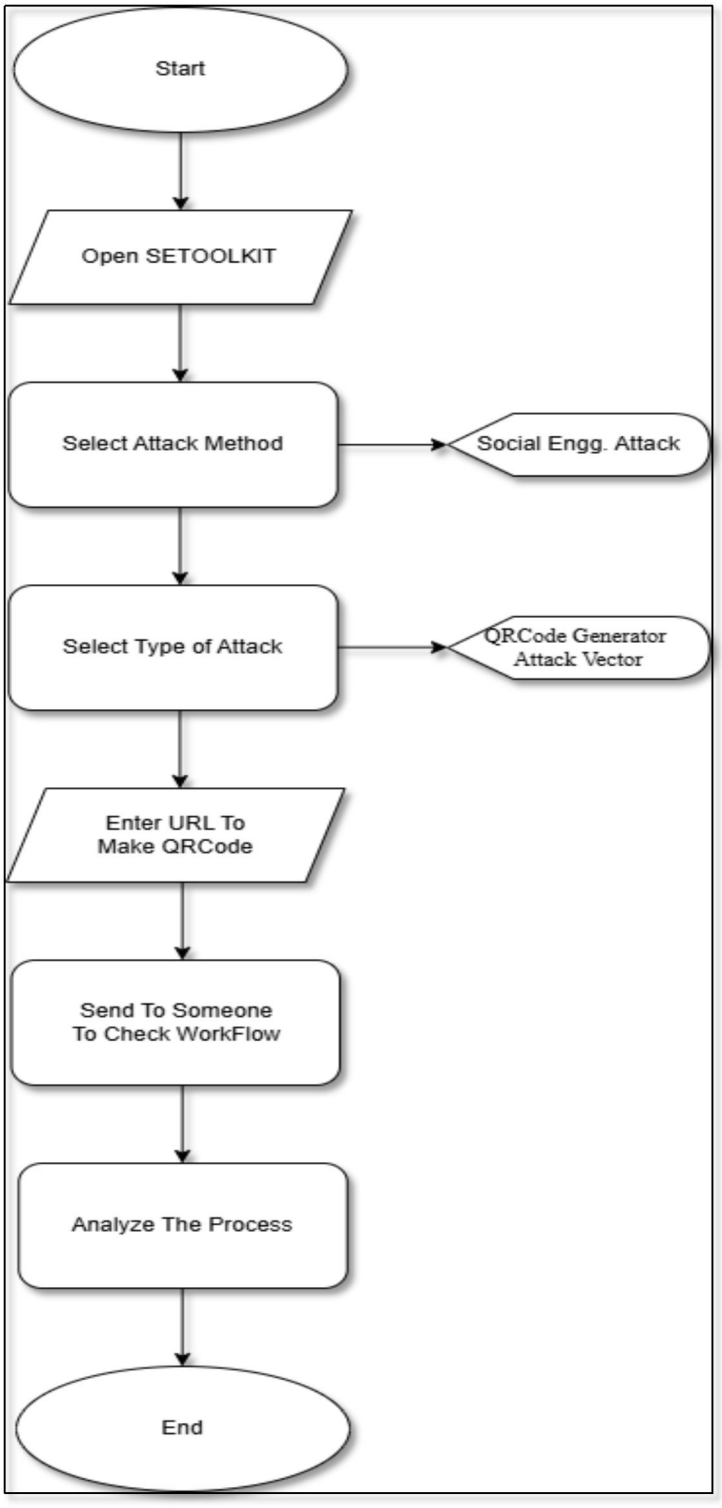

Figure 24

Steps:

1: Open Social Engg attack toolkit:
Setoolkit

2: Select From the menu:
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit

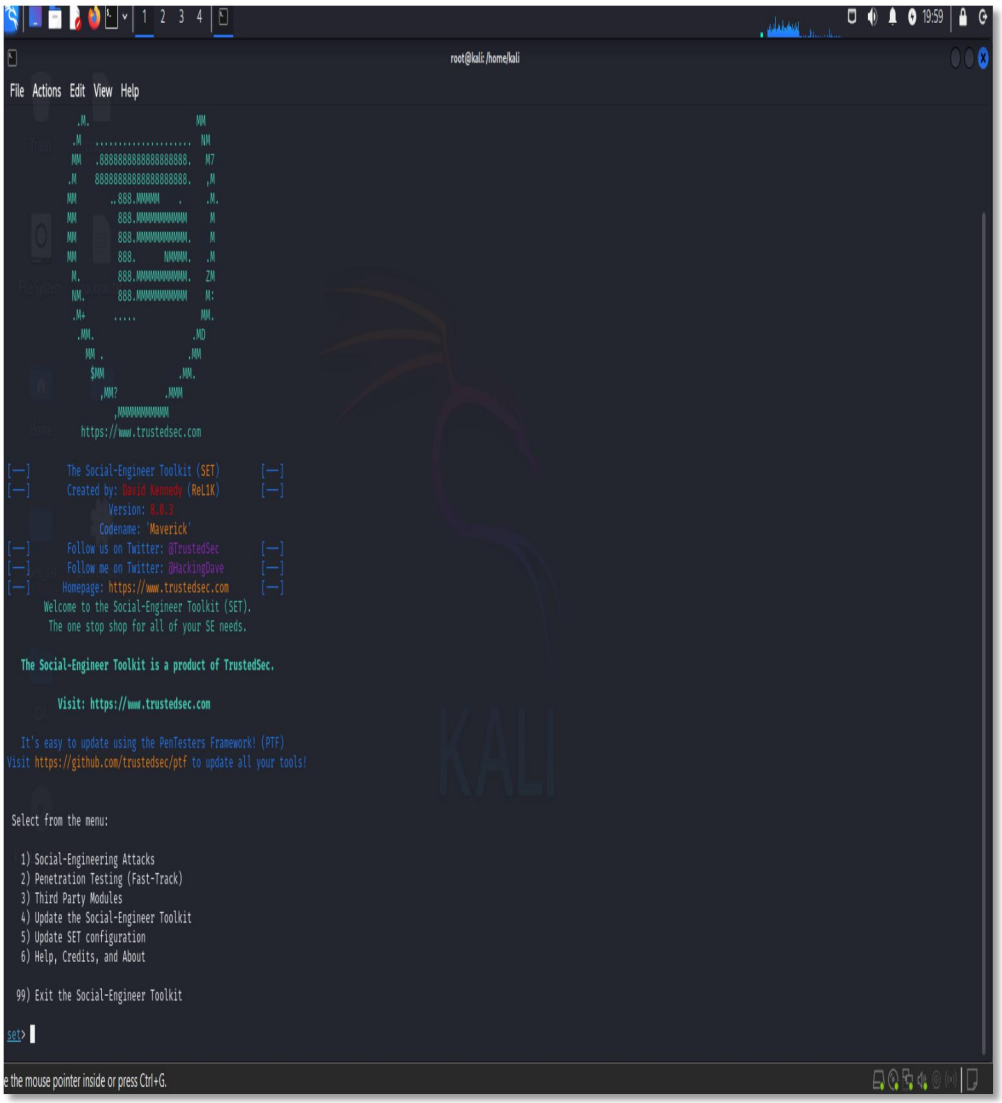

Figure 25

3: select type of attack :
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.

Figure 26

4: Select Number 8 QRcode Generator Attack Vector:

Enter The Url That Embedd in QRcode Scanner

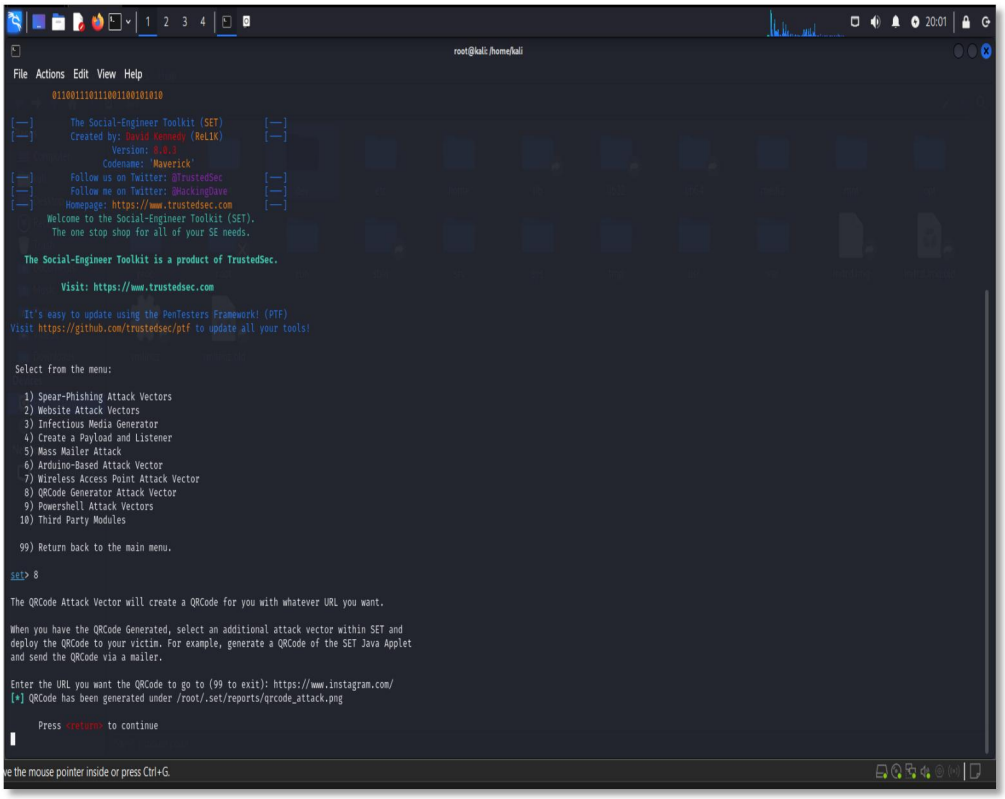

Figure 27

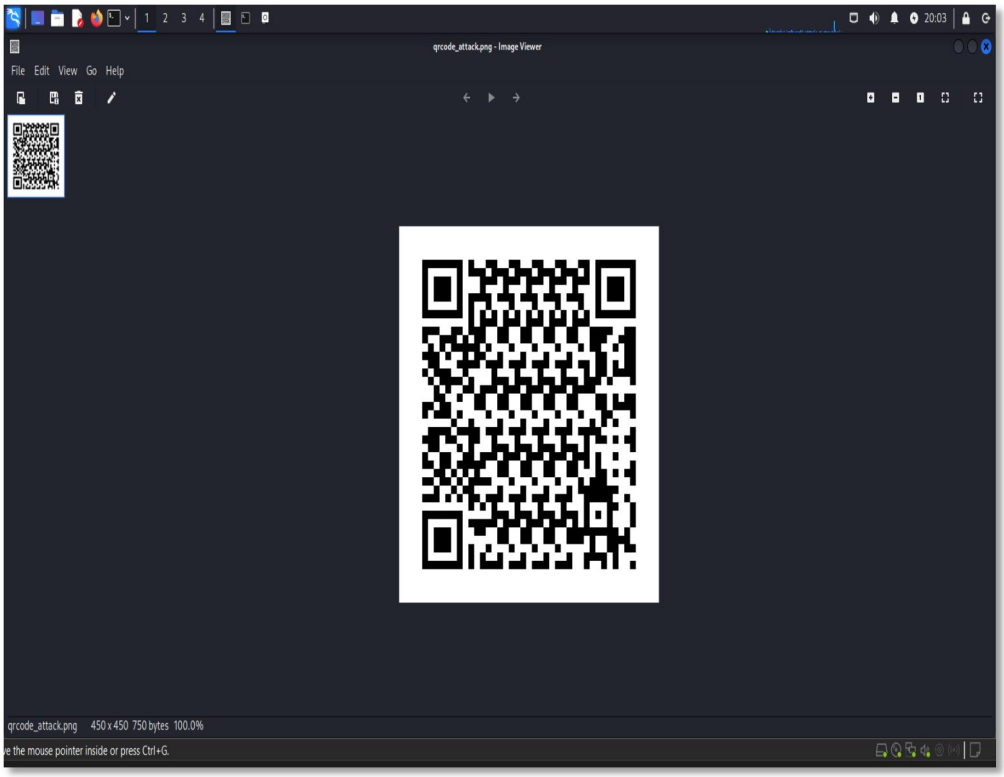

Figure 28

Conclusion:

The conducted social engineering attack successfully highlighted several critical vulnerabilities in human behavior and organizational security protocols. Through simulated phishing emails, pretexting scenarios, and other manipulation techniques, it was evident that even well-established systems can be compromised through human error or lack of awareness.

PRACTICAL - 10

DATE: 11-04-2025

Case Study: FinBank LockBit 3.0 Threat Case Study

Organization Profile:

Name: FinBank (pseudonym)

Industry: Financial Services

Employees: 20,000+

Customer Base: 10 million+ globally

Cybersecurity Maturity Level: Advanced (Tier 3 SOC)

Threat Scenario:

- In early 2024, FinBank's CTI team observed increased chatter on the dark web indicating potential targeting of financial institutions by the LockBit 3.0 ransomware group. The group was actively exploiting a zero-day vulnerability in an enterprise VPN product (CVE-2024-XXXXX).

Threat Intelligence Collection:

Sources:

1. **Open-source intelligence (OSINT):** Dark web forums, Twitter/X, GitHub
2. **Closed-source feeds:** Commercial threat intelligence platforms (e.g., Recorded Future, Mandiant)
3. **Internal telemetry:** SIEM alerts, endpoint detection logs
4. **Human intelligence (HUMINT):** Info-sharing through FS-ISAC (Financial Services Information Sharing and Analysis Center)

Indicators Collected:

1. IPs and URLs of known command-and-control servers

2. Hashes of LockBit 3.0 payloads

3. Tactics, Techniques, and Procedures (TTPs) associated with LockBit.

Response and Mitigation:

1. **IOC Ingestion:**
CTI team pushed indicators into the SIEM and EDR platforms for real-time detection.

2. **Proactive Threat Hunting:**
Analysts ran retrospective analysis on logs for the past 90 days. One employee's VPN access logs showed anomalies.

3. **Patch Management:**
VPN software was identified as vulnerable. A patch was deployed within 24 hours across all endpoints.

4. **User Awareness:**
Targeted phishing simulation was run for finance team employees. Multiple clickers received retraining.

5. **SOC Escalation Rules Updated:**
SIEM was updated to raise critical alerts if any LockBit TTPs were observed.

Outcomes:

1. The attack was detected early during the reconnaissance phase.

2. No systems were encrypted or data stolen.

3. The organization avoided potential losses of over $5 million, including ransom payments, downtime, and reputational damage.

Key Takeaways:

1. Proactive CTI reduces risk: Timely ingestion of intelligence helped prevent lateral movement.

2. Threat sharing matters: Collaboration with FS-ISAC offered valuable early warnings.

3. Patch fast, hunt faster: Rapid patching and internal threat hunting were crucial.

4. Human layer is critical: Phishing awareness can't be underestimated.

Tools & Technologies Used:

1. SIEM: Splunk Enterprise

2. EDR: CrowdStrike Falcon

3. Threat Intel Feeds: Recorded Future, Mandiant

4. Threat Sharing: FS-ISAC, MITRE ATT&CK framework

5. VPN: Fortinet (patched)

Conclusion:

The incident reinforced the importance of continuous vigilance, collaborative intelligence sharing, and layered defense strategies, including technical controls and user awareness training. Ultimately, FinBank avoided significant financial and reputational loss, proving that when cybersecurity maturity meets swift execution, even sophisticated threats like LockBit 3.0 can be successfully mitigated.