INCIDENT RESPONSE FOR COMMON ATTACK TYPES

1. Brute Forcing

Details:
Attacker trying to guess a password by attempting several different passwords

Threat Indicators:
Multiple login failures in a short period of time

Where To Investigate:

- Active directory logs
- Application logs
- Operational system logs
- Contact user

Possible Actions:
If not legit action, disable the account and investigate/block attacker

2. Botnets

Details:
Attackers are using the victim server to perform DDoS attacks or other malicious activities

Threat Indicators:

- Connection to suspicious IPs
- Abnormal high volume of network traffic

Where To Investigate:

- Network traffic
- OS logs (new processes)
- Contact server owner
- Contact support team

Possible Actions:
If confirmed:

- Isolate the server
- Remove malicious processes
- Patch the vulnerability utilized for infection

3. Ransomware

Details:
A type of malware that encrypts files and requests a ransom (money payment) from the user to decrypt the files

Threat Indicators:

- Anti-Virus alerts
- Connection to suspicious Ips

Where To Investigate:

- AV logs
- OS logs
- Account logs
- Network traffic

Possible Actions:

- Request AV checks
- Isolate the machine

4. Data Exfiltration

Details:
Attacker (or rogue employee) exfiltrate data to external sources

Threat Indicators:

- Abnormal high network traffic
- Connection to cloud -storage solutions (Dropbox, Google Cloud)
- Unusual USB Sticks

Where To Investigate:

- Network traffic
- Proxy logs
- OS logs

Possible Actions:

- If employee: Contact manager, perform full forensics
- If external threat: Isolate the machine, disconnect from network

5. Compromised Account

Details:
Attackers get access to one account (via social engineering or any other method)

Threat Indicators:

- Off-hours account logins
- Account group changes
- Abnormal high network traffic

Where To Investigate:

- Active directory logs
- OS logs
- Network traffic
- Contact user for clarifications

Possible Actions:

If confirmed:

- Disable account
- Password changes
- Forensic investigations

6. Denial Of Service (Dos/DDoS)

Details:
When attacker can cause interference in a system by exploiting DoS vulnerabilities or by generating a high volume of traffic

Threat Indicators:
Abnormal high network traffic in public facing servers

Where To Investigate:

- Network traffic
- Firewall logs
- OS logs

Possible Actions:

- If DoS due to vulnerabilities: Contact patching team for remediation
- If DDoS due to network traffic: Contact network Support or ISP

7. Advanced Persistent Treats (APTs)

Details:
Attackers get access to the system and create backdoors for further exploitation. Usually hard to detect

Threat Indicators:

- Connection to suspicious IPs
- Abnormal high volume of network traffic
- Off-hours access logs
- New admin account creations

Where To Investigate:

- Network traffic
- Access logs
- OS logs (new processes, new connections, abnormal users)
- Contact server owner/support teams

Possible Actions:
If confirmed:

- Isolate the machine
- Start formal forensics process
- Start escalation/communication plan