Name: Chaitali Patil
Intern ID: 297

Threat Intelligence Task

Tactic 1: Reconnaissance

Technique 1: Collect Public Identity Information

Technique ID: T1589

Goal:
Gather emails, usernames, job titles from public internet sources.

Objective:
Profile staff for social engineering attacks.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Maltego, EmailHarvester.py
• Target: corp-example.org

Procedure 1

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Procedure 2

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Outcome:
List of company employees with contact info.

Detection Recommendations:
• Minimize exposure of personal data.
• Use obfuscation of email addresses.
• Monitor for large-scale enumeration.

Technique 2: Identify Online Assets

Technique ID: T159

Goal:
Find domains, websites, and subdomains.

Objective:
Develop asset inventory.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Amass, curl
• Target: corp-example.org

Procedure 1

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Procedure 2

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Outcome:
Asset inventory created for later attack.

Detection Recommendations:
• Monitor for enumeration attempts.
• Deploy WAF with bot mitigation.
• Track your own domain assets.

Technique 3: Collect Technical Data

Technique ID: T1596

Goal:

Identify technical exposures in public databases.

Objective:

Gather data on software versions and configurations.

Lab Setup:

- Attacker Machine: Kali Linux
- Tools: Censys, nmap
- Target: corp-example.org IP ranges

Procedure 1

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Procedure 2

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Outcome:

Technical footprint with versions and configs.

Detection Recommendations:

- Hide version banners.
- Apply patches.
- Monitor network scans.

Tactic 2: Resource Development

Technique 1: Acquire Infrastructure

Technique ID: T1583

Goal:

Set up attacker-controlled infrastructure.

Objective:
Prepare servers/domains for later attack phases.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Linode, SSH
• Target: Cloud server + phishing domain

Procedure 1

1. Provision a cloud server using Linode CLI and configure SSH access.
2. Secure the server by configuring firewall rules and disabling unused services.
3. Install necessary attack tools and utilities required for later stages.
4. Set up monitoring to ensure server availability and control.

Procedure 2

1. Register a domain with Google Domains and point DNS records to attacker server.
2. Configure DNS settings such as A, MX, and TXT records.
3. Set up SSL/TLS certificates for secure communication.
4. Verify domain propagation using dig or nslookup.

Outcome:
Attacker infrastructure ready for malicious hosting.

Detection Recommendations:
• Monitor for domain registrations similar to your brand.
• Use threat intelligence feeds.
• Block malicious servers.

Technique 2: Compromise Accounts

Technique ID: T1586

Goal:
Obtain valid user accounts from third-party breaches.

Objective:
Use accounts for phishing or hosting attacks.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Hydra, AWS CLI

• Target: Target web/cloud services

Procedure 1

1. Run hydra with username/password lists against target login page.
2. Adjust brute-force speed to avoid detection.
3. Monitor for account lockouts and adjust strategy.
4. Collect successful login attempts.

Procedure 2

1. Use leaked AWS keys to check access with aws sts get-caller-identity.
2. Verify permissions assigned to the compromised keys.
3. Enumerate AWS services accessible with the keys.
4. Test commands such as s3 ls for bucket listing.

Outcome:
Attacker gains valid account access.

Detection Recommendations:
• Enforce MFA.
• Detect credential stuffing.
• Monitor unusual login patterns.

Technique 3: Obtain Capabilities

Technique ID: T1587

Goal:
Download or develop attack tools.

Objective:
Ensure working exploit capability.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Exploit-DB, GitHub
• Target: Linux VM

Procedure 1

Search exploit-db for vulnerabilities and copy exploit code.

Procedure 2

Clone tool repositories from GitHub such as sqlmap.

Outcome:
Attacker acquires necessary tools.

Detection Recommendations:
• Detect download of malicious tools.
• Restrict unapproved binaries.
• Monitor outbound traffic.

Tactic 3: Initial Access

Technique 1: Phishing

Technique ID: T1566

Goal:
Send malicious attachments or links.

Objective:
Trick user into executing malicious content.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Gophish, msfvenom
• Target: Victim email accounts

Procedure 1

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Procedure 2

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Outcome:
Victim clicks and attacker gains foothold.

Detection Recommendations:
• Use email filters.
• Train employees against phishing.
• Block known phishing domains.

Technique 2: Exploit Public-Facing Application

Technique ID: T1190

Goal:
Exploit vulnerable applications accessible online.

Objective:
Gain unauthorized system access.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Burp Suite, sqlmap
• Target: Vulnerable web app

Procedure 1

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Procedure 2

1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Outcome:
Attacker gains access via web exploit.

Detection Recommendations:
• Patch apps regularly.
• Monitor abnormal requests.

• Deploy WAF.

Technique 3: Valid Accounts
Technique ID: T1078

Goal:
Use stolen credentials for access.

Objective:
Authenticate to target systems directly.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: SSH, RDP
• Target: Target endpoints

Procedure 1
1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Procedure 2
1. Start by launching tool on the Kali Linux attacker machine.
2. Configure the environment by specifying the target domain or IP address.
3. Adjust additional options such as ports, timeouts, and output file paths.
4. Run the scanning or enumeration command and carefully monitor the output.

Outcome:
Attacker enters system with valid credentials.

Detection Recommendations:
• Enforce MFA.
• Monitor unusual login activity.
• Rotate compromised credentials.

Tactic 4: Execution

Technique 1: Execution Method 1
Technique ID: T401

Goal:
Goal for Execution - Technique 1.

Objective:
Objective for Execution - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Execution, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Execution Method 2

Technique ID: T402

Goal:
Goal for Execution - Technique 2.

Objective:
Objective for Execution - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed. Cross-verify results using

Outcome:
Outcome of Execution, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Execution Method 3

Technique ID: T403

Goal:
Goal for Execution - Technique 3.

Objective:
Objective for Execution - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Execution, Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 5: Persistence

Technique 1: Persistence Method 1

Technique ID: T501

Goal:
Goal for Persistence - Technique 1.

Objective:
Objective for Persistence - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.

4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Persistence, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Persistence Method 2

Technique ID: T502

Goal:
Goal for Persistence - Technique 2.

Objective:
Objective for Persistence - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.

3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Persistence, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Persistence Method 3
Technique ID: T503

Goal:
Goal for Persistence - Technique 3.

Objective:
Objective for Persistence - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Persistence, Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 6: Privilege Escalation

Technique 1: Privilege Escalation Method 1

Technique ID: T601

Goal:
Goal for Privilege Escalation - Technique 1.

Objective:
Objective for Privilege Escalation - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Privilege Escalation, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.

• Detection recommendation C.

Technique 2: Privilege Escalation Method 2
Technique ID: T602

Goal:
Goal for Privilege Escalation - Technique 2.

Objective:
Objective for Privilege Escalation - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Privilege Escalation, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Privilege Escalation Method 3
Technique ID: T603

Goal:
Goal for Privilege Escalation - Technique 3.

Objective:
Objective for Privilege Escalation - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Privilege Escalation, Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 7: Defense Evasion

Technique 1: Defense Evasion Method 1

Technique ID: T701

Goal:
Goal for Defense Evasion - Technique 1.

Objective:
Objective for Defense Evasion - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Defense Evasion, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Defense Evasion Method 2

Technique ID: T702

Goal:
Goal for Defense Evasion - Technique 2.

Objective:
Objective for Defense Evasion - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX

• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Defense Evasion, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Defense Evasion Method 3

Technique ID: T703

Goal:
Goal for Defense Evasion - Technique 3.

Objective:
Objective for Defense Evasion - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).

2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Defense Evasion, Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 8: Credential Access

Technique 1: Credential Access Method 1

Technique ID: T801

Goal:
Goal for Credential Access - Technique 1.

Objective:
Objective for Credential Access - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Credential Access, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Credential Access Method 2

Technique ID: T802

Goal:
Goal for Credential Access - Technique 2.

Objective:
Objective for Credential Access - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Credential Access, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Credential Access Method 3
Technique ID: T803

Goal:
Goal for Credential Access - Technique 3.

Objective:
Objective for Credential Access - Technique 3

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Credential Access, Technique 3.

Detection Recommendations:
• Detection recommendation A.

• Detection recommendation B.
• Detection recommendation C.

Tactic 9: Discovery

Technique 1: Discovery Method 1

Technique ID: T901

Goal:
Goal for Discovery - Technique 1.

Objective:
Objective for Discovery - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Discovery, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Discovery Method 2
Technique ID: T902

Goal:
Goal for Discovery - Technique 2.

Objective:
Objective for Discovery - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Discovery, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Discovery Method 3
Technique ID: T903

Goal:
Goal for Discovery - Technique 3.

Objective:
Objective for Discovery - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Discovery, Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 10: Lateral Movement

Technique 1: Lateral Movement Method 1
Technique ID: T1001

Goal:
Goal for Lateral Movement - Technique 1.

Objective:
Objective for Lateral Movement - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Lateral Movement, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Lateral Movement Method 2

Technique ID: T1002

Goal:
Goal for Lateral Movement - Technique 2.

Objective:
Objective for Lateral Movement - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Lateral Movement, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Lateral Movement Method 3

Technique ID: T1003

Goal:
Goal for Lateral Movement - Technique 3.

Objective:
Objective for Lateral Movement - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.

4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Lateral Movement, Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 11: Collection

Technique 1: Collection Method 1

Technique ID: T1101

Goal:
Goal for Collection - Technique 1.

Objective:
Objective for Collection - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Collection, Technique 1.

Detection Recommendations:
- Detection recommendation A.
- Detection recommendation B.
- Detection recommendation C.

Technique 2: Collection Method 2

Technique ID: T1102

Goal:
Goal for Collection - Technique 2.

Objective:
Objective for Collection - Technique 2.

Lab Setup:
- Attacker Machine: Kali Linux
- Tools: Tool2, ToolX
- Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Collection, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Collection Method 3
Technique ID: T1103

Goal:
Goal for Collection - Technique 3.

Objective:
Objective for Collection - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Collection, Technique 3.

Detection Recommendations:
• Detection recommendation A.

• Detection recommendation B.
• Detection recommendation C.

Tactic 12: Command and Control (C2)

Technique 1: Command and Control (C2) Method 1

Technique ID: T1201

Goal:
Goal for Command and Control (C2) - Technique 1.

Objective:
Objective for Command and Control (C2) - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Command and Control (C2), Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Command and Control (C2) Method 2
Technique ID: T1202

Goal:
Goal for Command and Control (C2) - Technique 2.

Objective:
Objective for Command and Control (C2) - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Command and Control (C2), Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Command and Control (C2) Method 3
Technique ID: T1203

Goal:
Goal for Command and Control (C2) - Technique 3.

Objective:
Objective for Command and Control (C2) - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Command and Control (C2), Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 13: Exfiltration

Technique 1: Exfiltration Method 1

Technique ID: T1301

Goal:
Goal for Exfiltration - Technique 1.

Objective:
Objective for Exfiltration - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Exfiltration, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Exfiltration Method 2

Technique ID: T1302

Goal:
Goal for Exfiltration - Technique 2.

Objective:
Objective for Exfiltration - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Exfiltration, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Exfiltration Method 3

Technique ID: T1303

Goal:
Goal for Exfiltration - Technique 3.

Objective:
Objective for Exfiltration - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.

4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Exfiltration, Technique 3.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Tactic 14: Impact

Technique 1: Impact Method 1

Technique ID: T1401

Goal:
Goal for Impact - Technique 1.

Objective:
Objective for Impact - Technique 1.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool1, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Impact, Technique 1.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 2: Impact Method 2

Technique ID: T1402

Goal:
Goal for Impact - Technique 2.

Objective:
Objective for Impact - Technique 2.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool2, ToolX
• Target: Target system

Procedure 1

1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2

1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Impact, Technique 2.

Detection Recommendations:
• Detection recommendation A.
• Detection recommendation B.
• Detection recommendation C.

Technique 3: Impact Method 3
Technique ID: T1403

Goal:
Goal for Impact - Technique 3.

Objective:
Objective for Impact - Technique 3.

Lab Setup:
• Attacker Machine: Kali Linux
• Tools: Tool3, ToolX
• Target: Target system

Procedure 1
1. Launch the required tool (for example, open the attack console or start the exploit framework).
2. Identify the specific module or plugin that supports this method.
3. Configure the module with the target IP address or domain.
4. Set payloads and adjust network parameters (e.g., ports, timeout).

Procedure 2
1. Prepare an alternate technique such as a script or secondary tool.
2. Configure it with alternative credentials or vulnerable parameters.
3. Launch the script/tool and monitor the network responses.
4. Confirm whether access was gained or the payload executed.

Outcome:
Outcome of Impact, Technique 3.

Detection Recommendations:

- Detection recommendation A.
- Detection recommendation B.
- Detection recommendation C.