

Team: Cyber 4

Mrunmayee Shirodkar: 2070

Divya Bhogle: 2043

Vrushali Walve: 2071

Manali Gawade: 2035

1. Initial Access

Image 1 : Overview

Initial Access TA0001

By: Mrunmayee Shirodkar
Cyber Security Intern

Short non-technical summary: Initial Access TA0001 refers to techniques that adversaries use to gain entry into target systems. These methods are the first step in a cyber attack, allowing attackers to establish a foothold in an organization's network.

What is Initial Access TA0001?

Initial Access TA0001 involves the use of various techniques by attackers to gain an initial foothold in a target network. These methods serve as the gateway for launching cyber attacks, such as data exfiltration, ransomware, and espionage.

Key Targets

- Corporate Networks**: Internal systems and sensitive data within an organization's network
- Web Servers**: Public-facing servers hosting websites and applications
- Employees**: Individuals within an organization who might be susceptible to social engineering

Common Techniques

- Phishing**: Sending malicious emails with malware-infected attachments or links
- Exploiting Public-Facing Applications**: Attacking vulnerabilities in web applications that are accessible from the internet
- Drive-By Compromise**: Hosting malicious code on legitimate websites to infect visitors
- Valid Accounts**: Utilizing stolen or compromised user credentials to gain access
- Removable Media**: Using infected USB drives or other removable media to spread malware

Image 2 : Technical Details

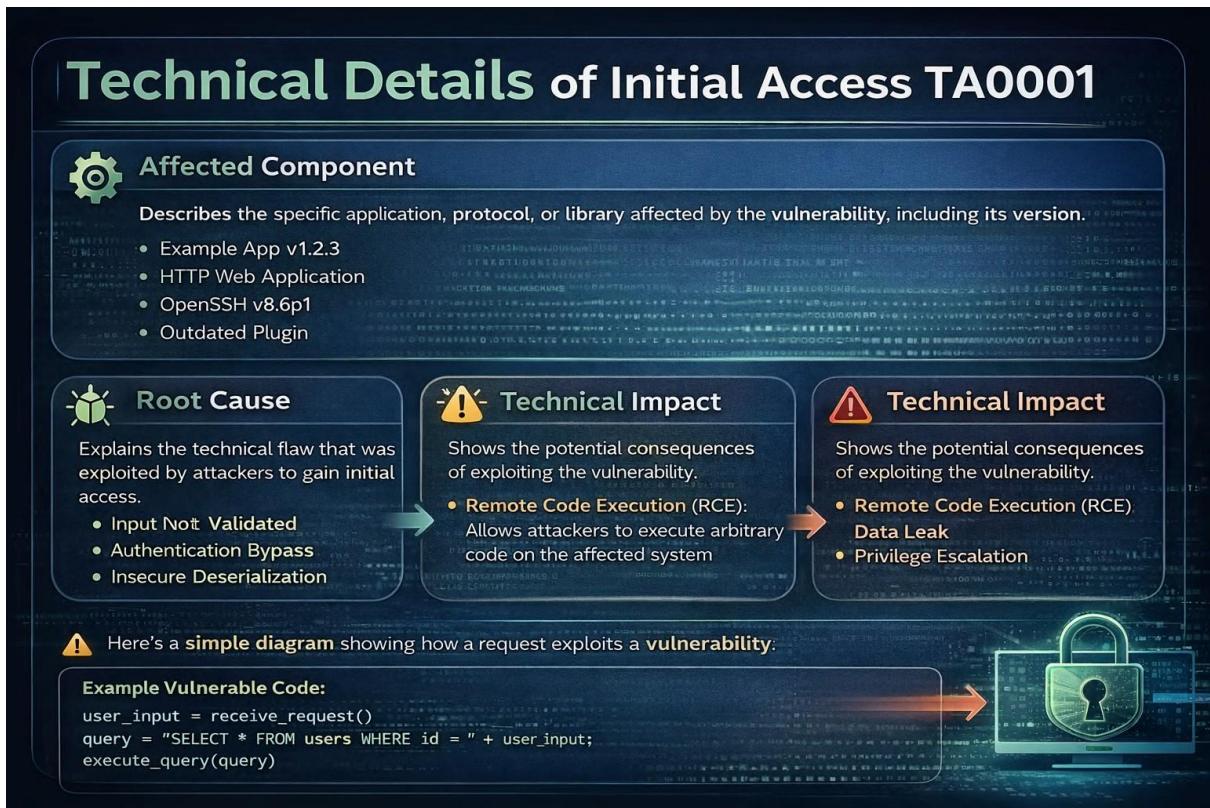
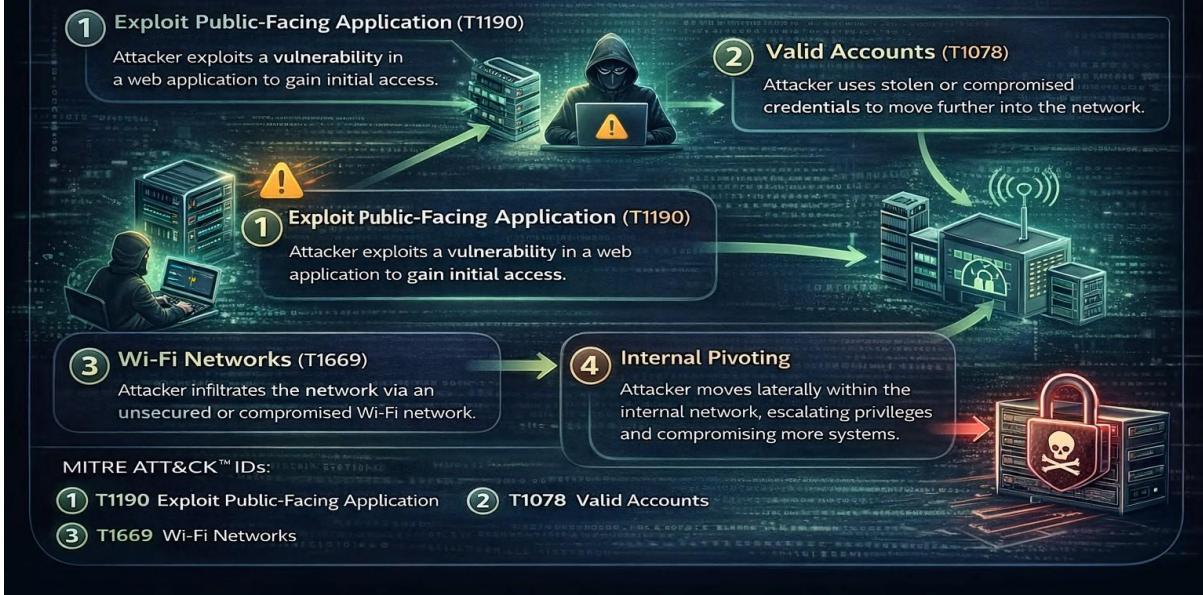


Image 3 : Attack Flow / Technique

Attack Flow of Initial Access TA0001

Step-by-step attack path used by adversaries to gain access to a target system. This example illustrates several common techniques within the Initial Access TA0001 tactic.



2. Execution :

Image 1 : Overview

Execution TA0002
Understanding the cyber threat of Execution TA0002

WHAT IS EXECUTION TA0002?

- Execution (TA0002) is a technique used by cyber attackers to run malicious code on a target system.
- It allows hackers to take control by executing harmful programs or scripts.

Think of it as a way for attackers to make a computer do whatever they want, as if they have taken over the keyboard.

WHERE DOES IT APPEAR?

Common methods hackers use Execution TA0002 are common ways to use:

- Phishing Emails**
Clicking on malicious links or attachments.
- Malicious Files**
Opening infected documents or software.
- Command Line**
Directly executing commands in the terminal or command prompt.
- Startup Scripts**
Programs automatically running when a system starts.

Intern: Mrunmayee Shirodkar – Cyber Security Intern

Image 2 : Technical Details

TECHNICAL DETAILS (TT0002)
EXECUTION TA0002

Affected Component

- <App Name>
- <Vulnerable App>
Version 2.1.4
- LibraryName (v1.2.3)
- <Protocol>

Root Cause

- Input not validated
- Unsafe deserialization
- Authentication bypass

Technical Impact

- Remote Code Execution (RCE)
- Data leak
- Privilege Escalation (PrivEsc)

Example Vulnerable Code or Library:

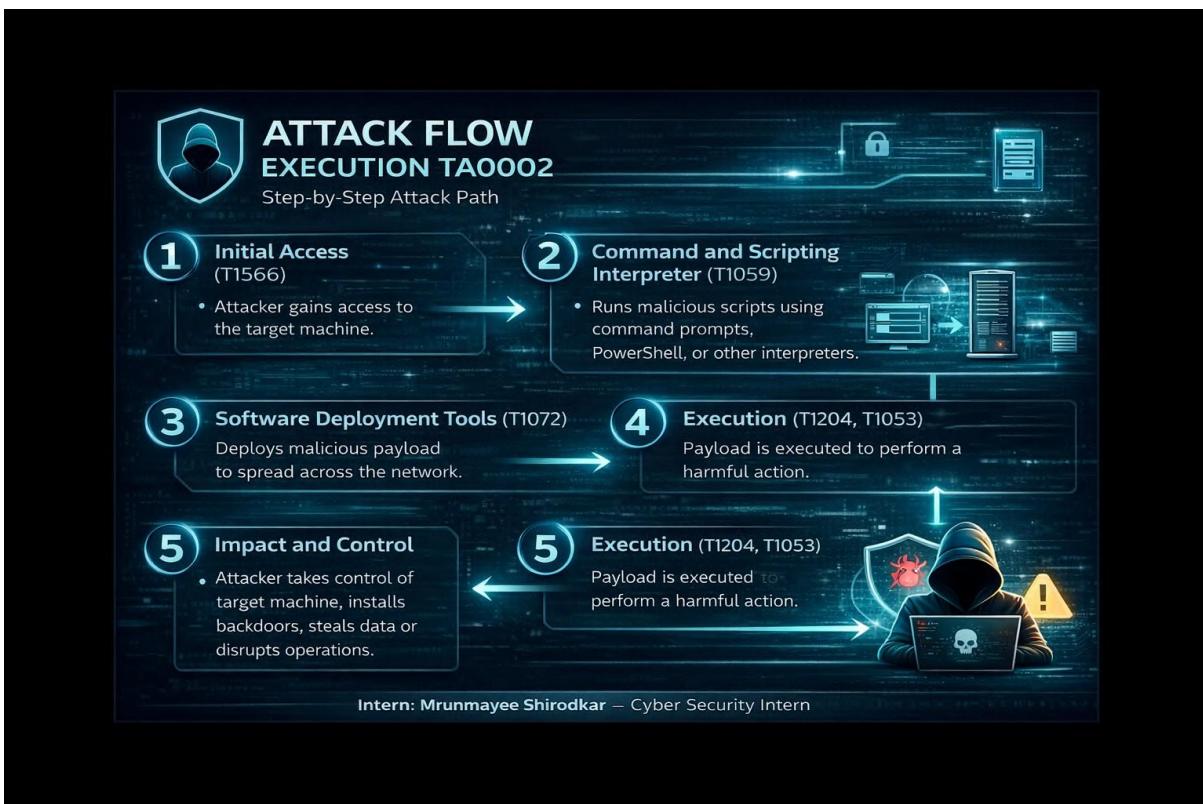
```
input = get_user_input();
deserialize(input)
// Insecure deserialization
```

Request → Vulnerable Code → Result

Request → Vulnerable Code → Result

Intern: Mrunmayee Shirodkar – Cyber Security Intern

Image 3 : Attack Flow / Technique



3. Persistance

Image 1 : Overview

The slide has a dark blue background with a glowing blue shield icon in the top left corner. The title 'Persistence – TA0003' is centered at the top in large white font. Below the title is a section titled 'What is Persistence?' containing a definition and an illustration of a hacker. To the right of the definition is a yellow warning icon. Below this is another section titled 'Where Does This Vulnerability Appear?' showing icons for Workstations & Servers, Cloud Services, Network Devices, and Enterprise Environments. At the bottom right is a circular profile picture of a woman and her name, Mrunmayee Shirodkar, with the title 'Cyber Security Intern'.

Persistence – TA0003

What is Persistence?

Persistence (TA0003) is a vulnerability where attackers find ways to maintain access to a system even after it has been rebooted or logged off. This allows them to keep control over the system for long periods of time.

Where Does This Vulnerability Appear?

Workstations & Servers Cloud Services Network Devices Enterprise Environments

Mrunmayee Shirodkar
Cyber Security Intern

Image 2 : Technical Details

This slide is titled 'Persistence – TA0003 Technical Details'. It features three main sections: 'Affected Components', 'Root Cause', and 'Technical Impact'. Below these is a code snippet illustrating insecure authentication logic, followed by two flowcharts showing the attack process.

Affected Components

- Application (AnyApp v1.2.14)
- Protocol (SSH)
- Library (Boost v1.76)

Root Cause

- Input Not Validated
- Authentication Bypass
- Insecure Deserialization

Technical Impact

- Remote Code Execution (RCE)
- Data Leak
- Privilege Escalation (PrivEsc)

Code Snippet:

```
> login(user, pass) {  
    if(user === 'admin') {  
        // Bypass security for admin account  
        isAuthenticated = true;  
    }  
}  
> Insecure Authentication Logic
```

Attack Flow:

Malicious Request → Vulnerable Code → Remote Code Execution

Mal. App v1.2.14 → Auth Bypass → RCE

Image 3 : Attack Flow / Technique



4. Privilege Escalation

Image 1 : Overview

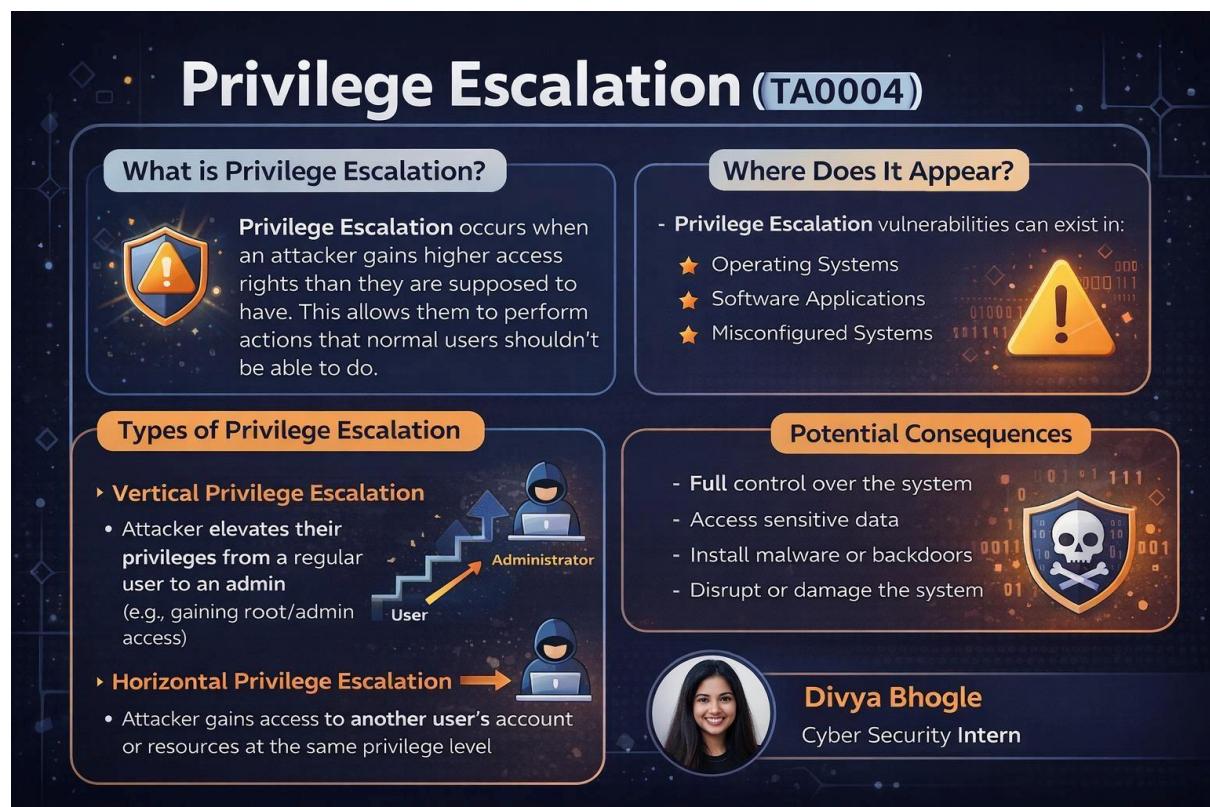


Image 2 : Technical details :

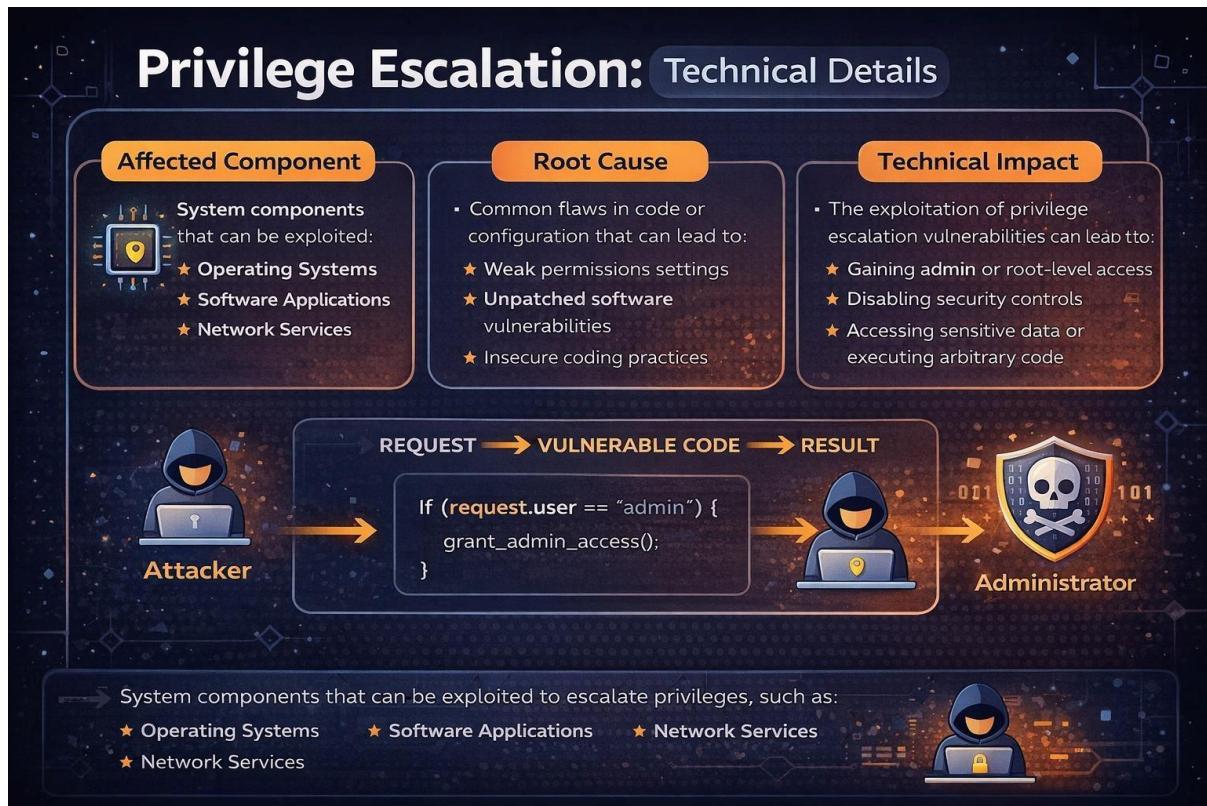
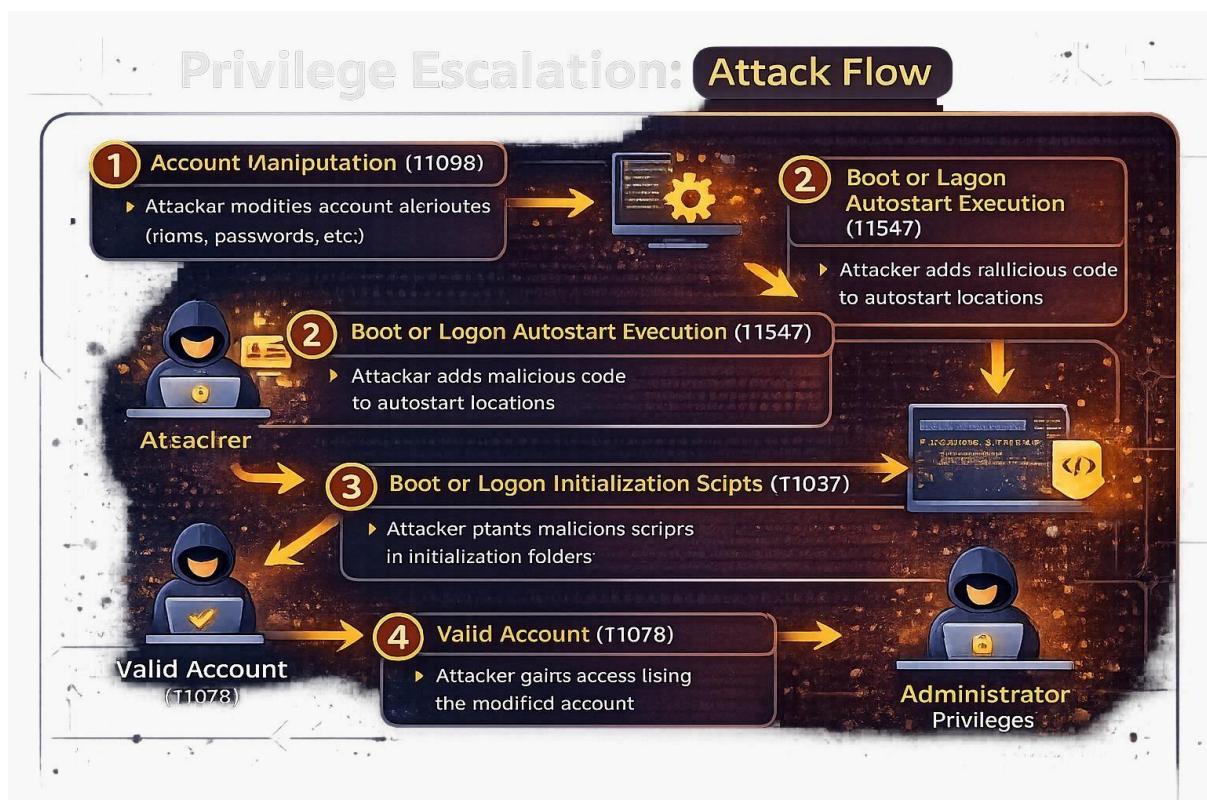


Image 3 : Attack Flow / Technique



5. Defense Evasion (TA0005)

Image 1 : Overview

Defense Evasion (TA0005)

What is Defense Evasion?



Defense Evasion refers to techniques used by attackers to **avoid detection** by security defenses, allowing them to stay undetected while carrying out malicious activities.

Where Does It Appear?

- Malware
- Scripts
- System Tools
- Phishing Attacks





Divya Bhogle
Cyber Security Intern

Image 2 : Technical Details

Defense Evasion (TA0005)

Affected Component

- Endpoint Security (AV/EDR)
- Firewalls/IPS
- SIEM/Loggers
- OS & Applications



Root Cause

- Malware
- Signature-based Detection
- Inssufficient Heuristics
- Exploit/Payload Obuscration
- Supply Chain Vulnerabilities



Technical Impact

- Undetected Payload Execution
- Command & Control Bypass
- Lateral Movement

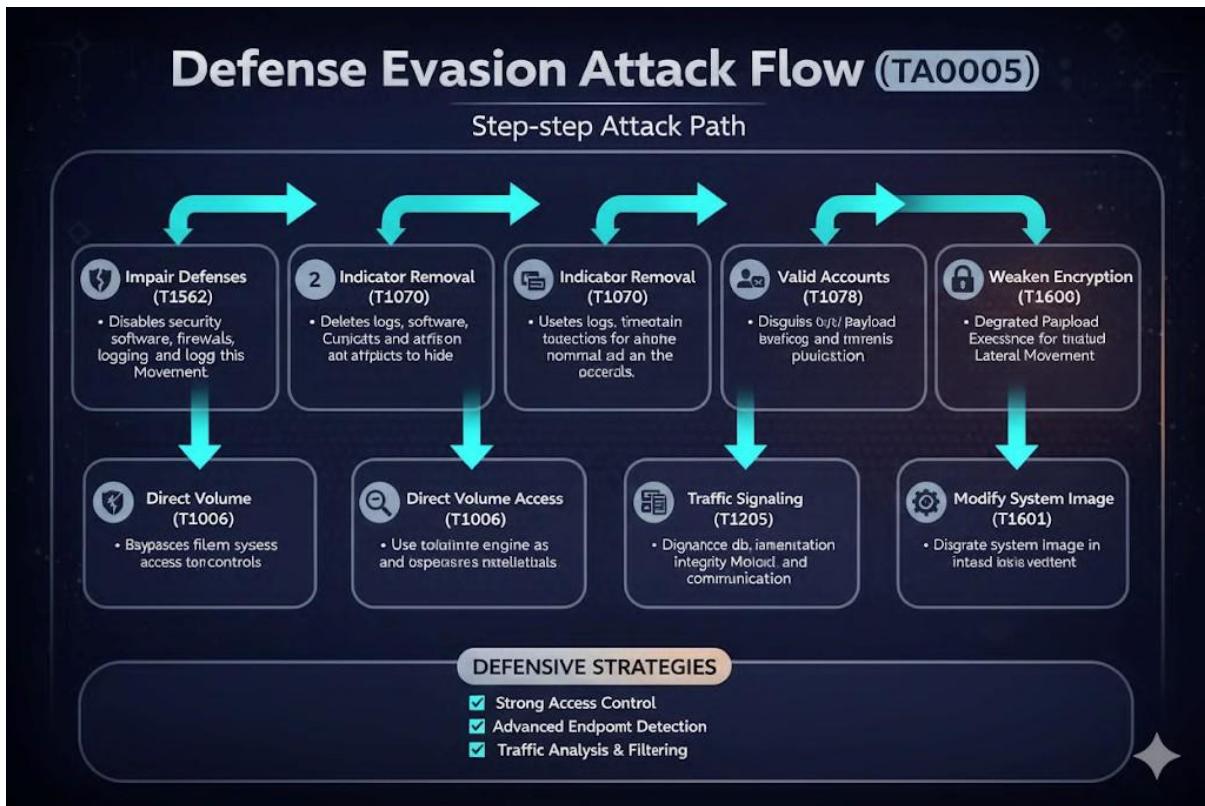
Evasion Flow

```
graph LR; A[Malicious Request (Obsoleted)] --> B[Vulnerable Code/Result]; B --> C[Undetected Payload Execution  
System Persistence  
Lateral Movement]
```

Pseudo-code Example

```
/ Pseudo-code Example
detect_evasion(payload):
    if signature.db.contains(payload):
        if behaviour_engine.is_anomalous():
            return "DETECTED";
        else:
            execute(successfully);
    return (UNDETECTED)
};
```

Image 3 : Attack Flow / Technique



6. Credential Access

Image 1 : Overview

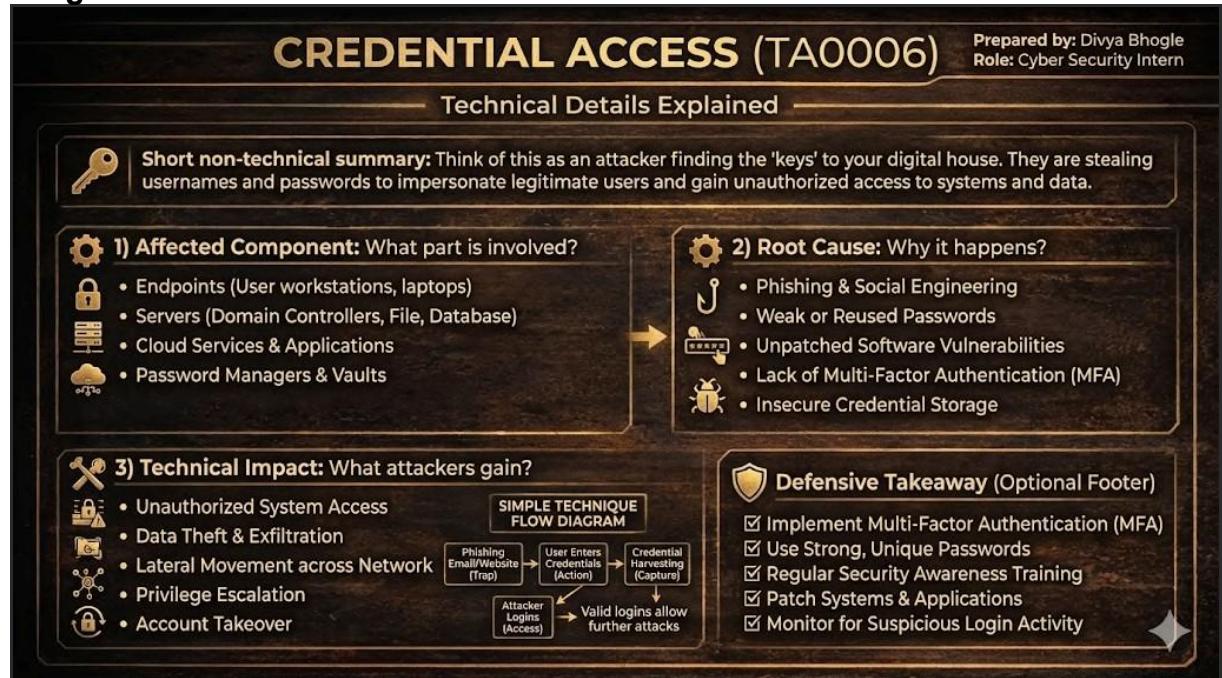


Image 2 : Technical Details

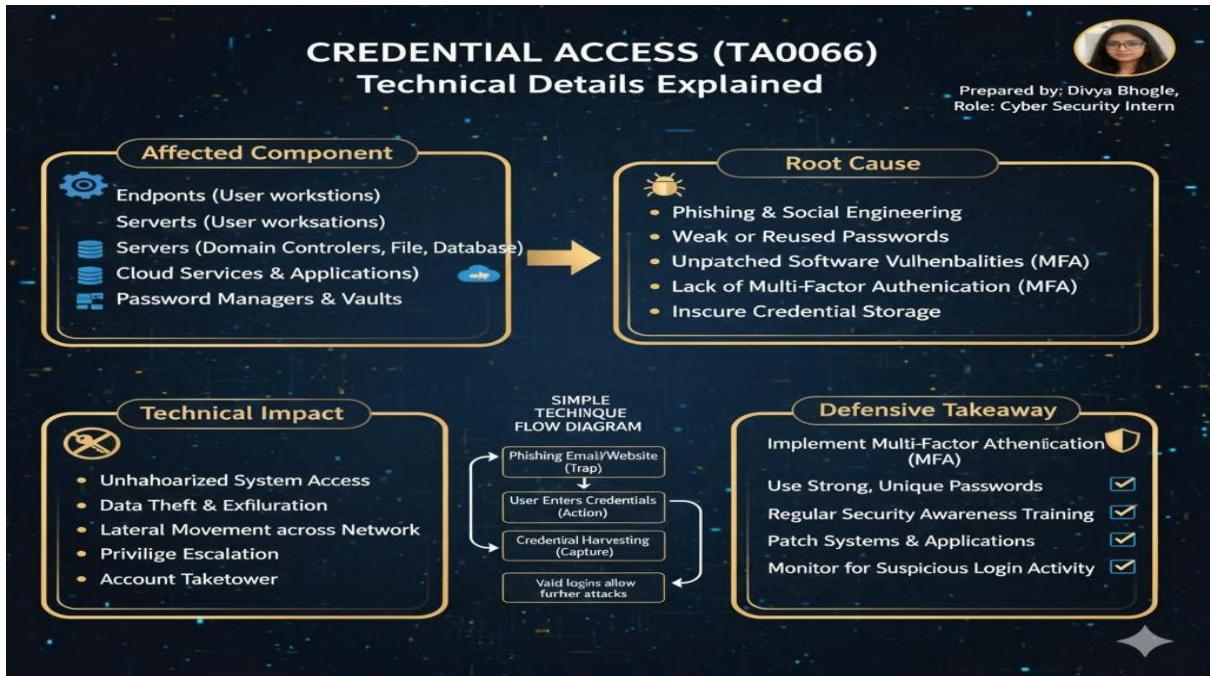
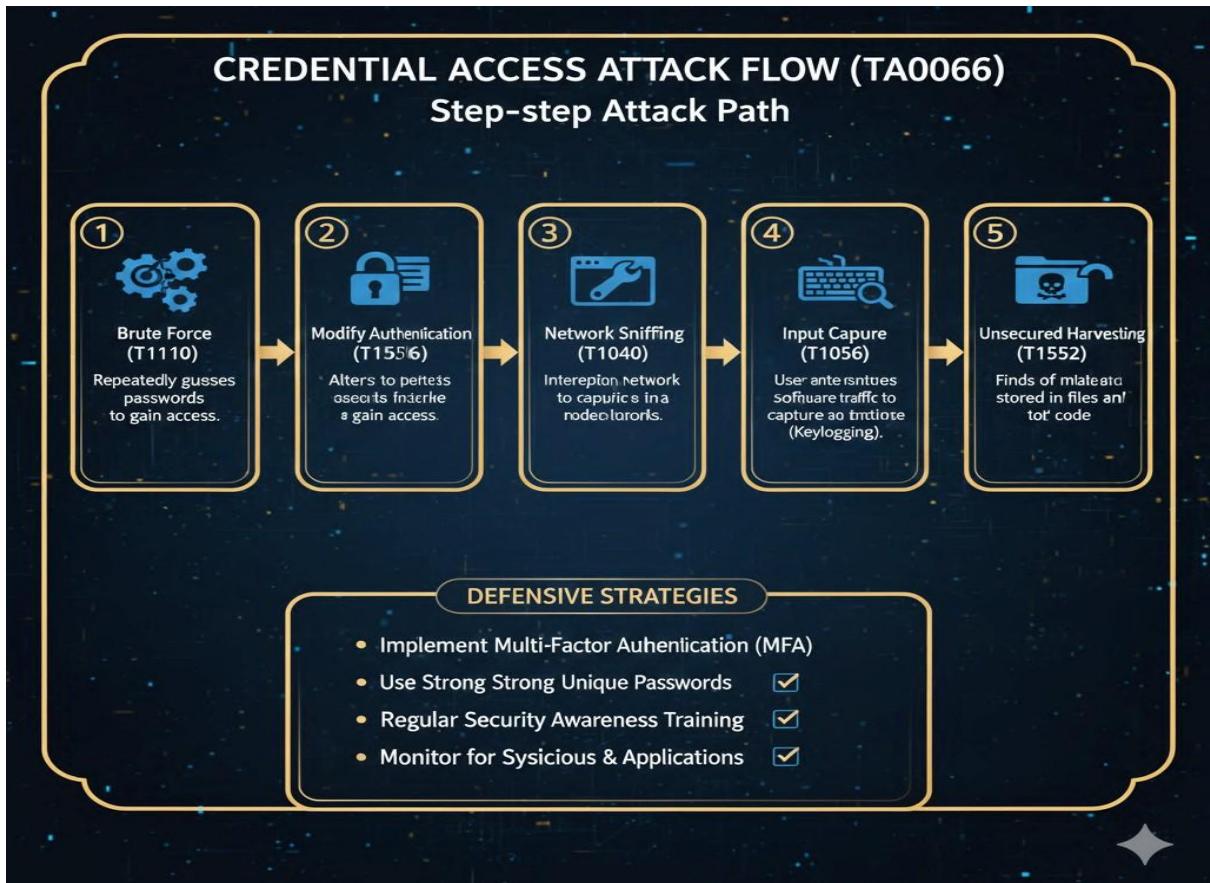


Image 3 : Attack Flow / Technique



7. Discovery (TA0007)

Image 1 : Overview



Image 2 : Technical Details

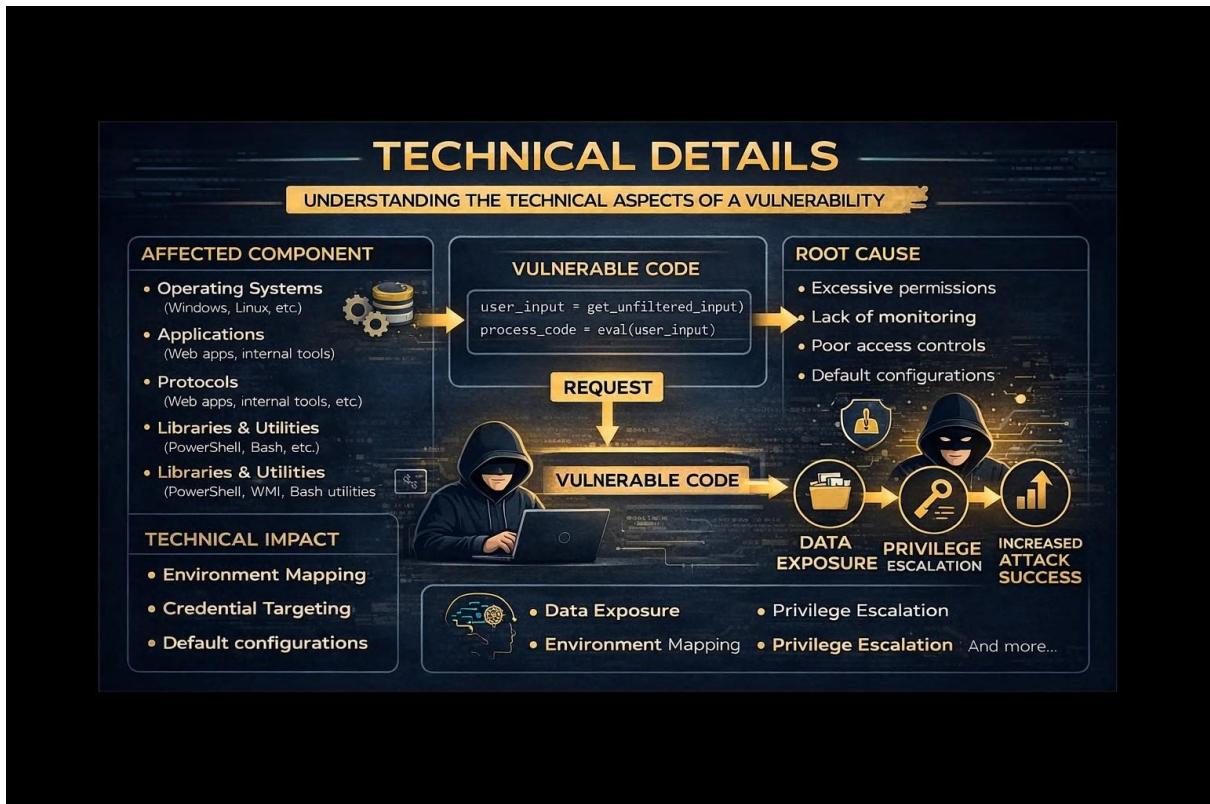
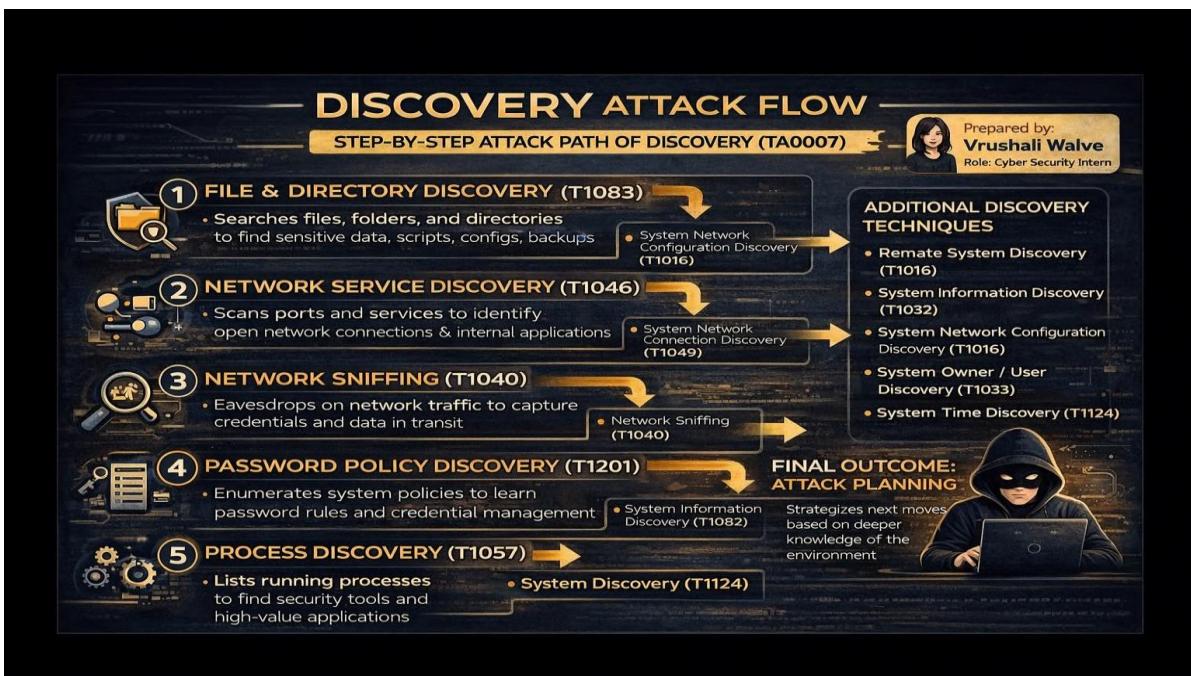


Image 3 : Attack Flow / Technique



8. Lateral Movement

Image 1 : Overview

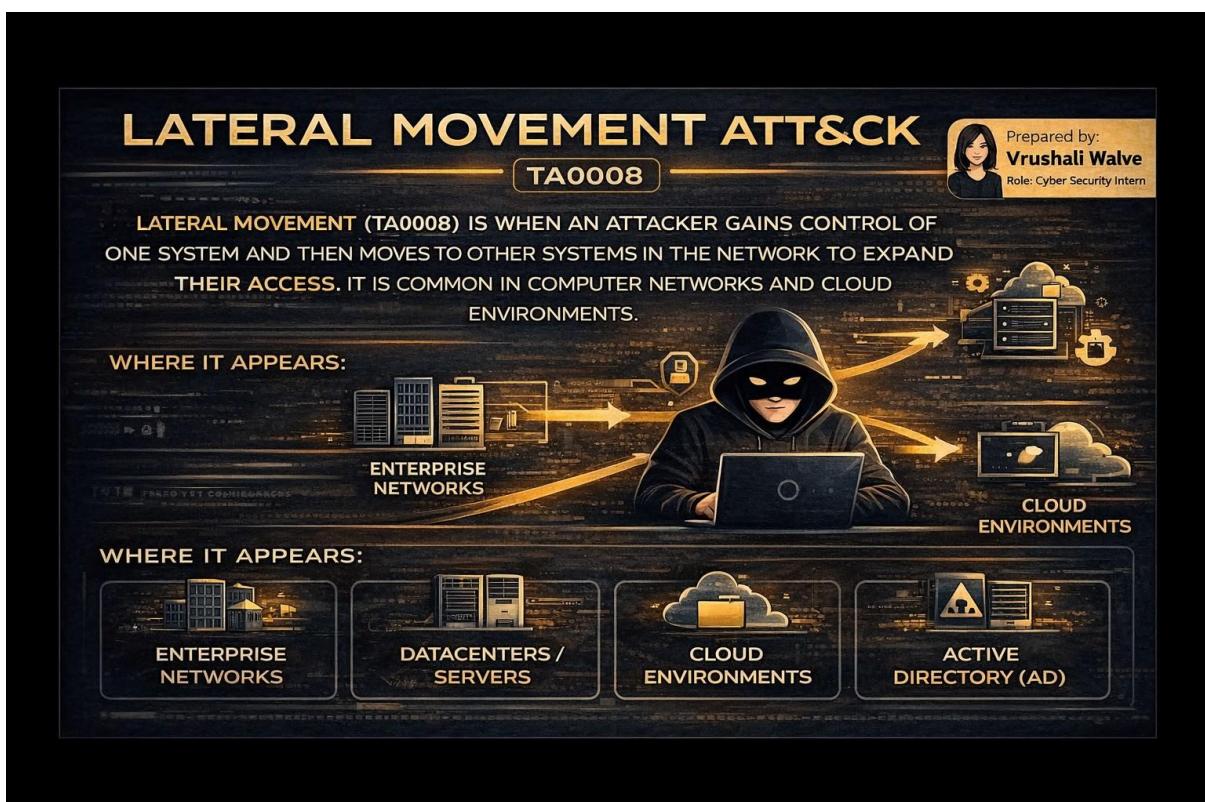


Image 2 : Technical Details

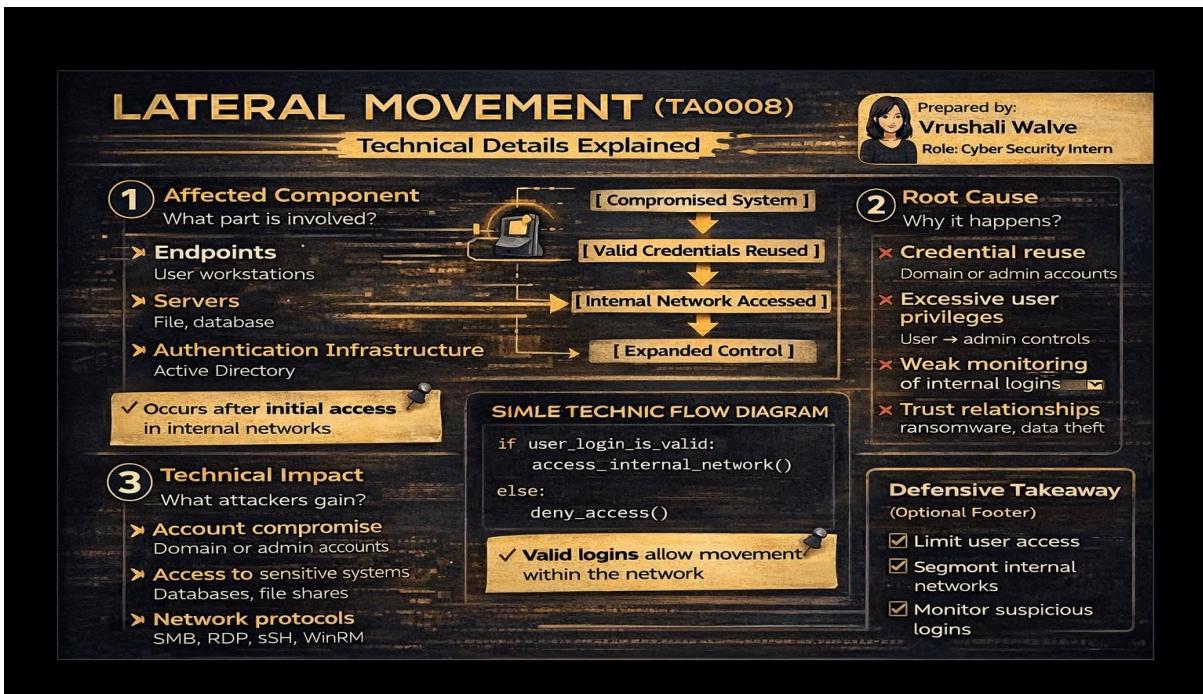
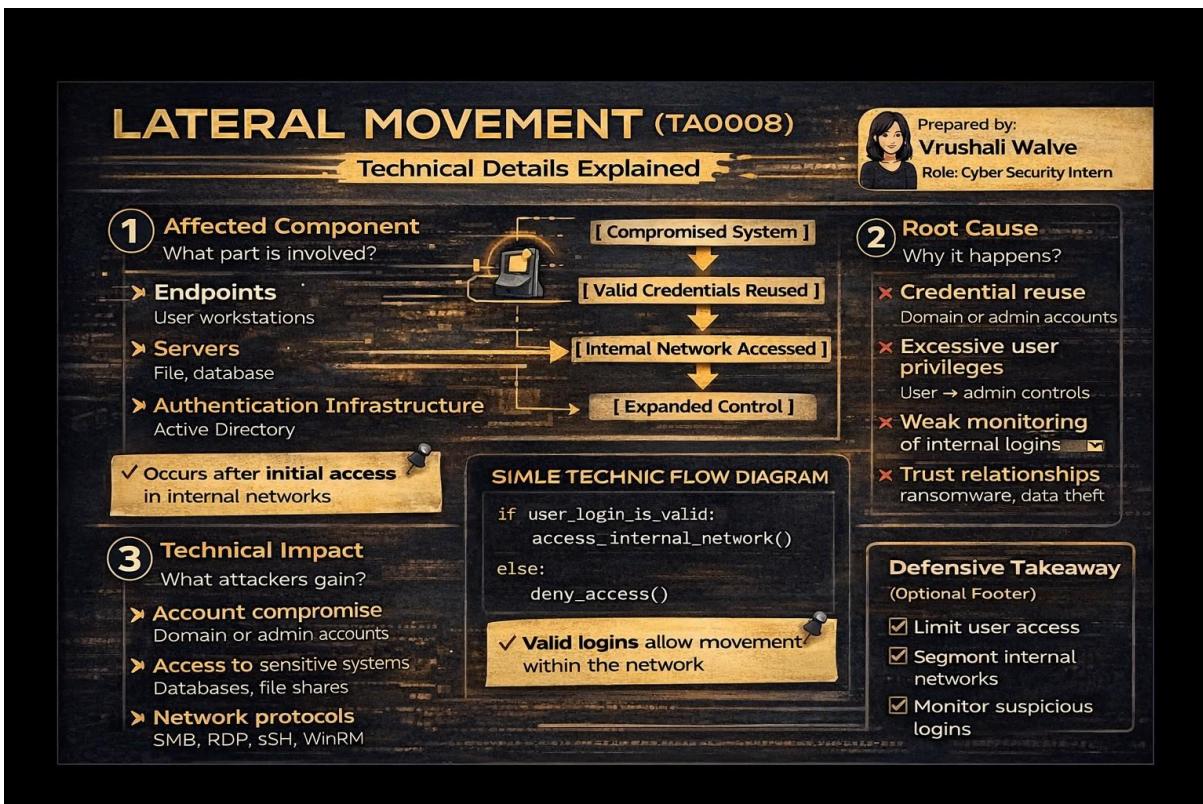


Image 3 : Attack Flow / Technique



9. Collection (TA0009)

Image 1 : Overview

COLLECTION TA0009

Explaining Collection TA0009



Vrushali Walve
Cyber Security Intern

COLLECTION TA0009

Collection TA0009 focuses on gathering credentials, files, screenshots, and other sensitive data from compromised systems.

WHAT IT IS

Collection TA0009 is a category in the MITRE ATT&CK Framework that covers methods used by adversaries to gather data from compromised systems. This can include stealing credentials, capturing screenshots, collecting files, and more.

ATT&CK MATRIX

Reconnaissance	Exploit Development	Initial Access	Persistence	Dataloading	Phishing Escalation	Delivery Evasion	Defense Evasion	Resource Access	Discovery	Discovery
Reconnaissance	Exploit Development	Initial Access	Persistence	Dataloading	Phishing Escalation	Delivery Evasion	Defense Evasion	Resource Access	Discovery	Discovery
Reconnaissance	Exploit Development	Initial Access	Persistence	Dataloading	Phishing Escalation	Delivery Evasion	Defense Evasion	Resource Access	Discovery	Discovery

Collection 9

- ▶ Input Capture → Keylogging
- ▶ Screen Capture → Screenshots
- ▶ Clipboard Data → File Collection
- ▶ Data from Local System
- ▶ Data from Network Shared Drive
- ▶ Data from Cloud Storage

Image 2 : Technical Details

COLLECTION TA0009

Technical Details Explained

FFECTED COMPONENT

What is impacted by Collection TA0009?

- Endpoints (User workstations)
- Servers (File, database)
- Authentication Systems (Credential storage)



ROOT CAUSE

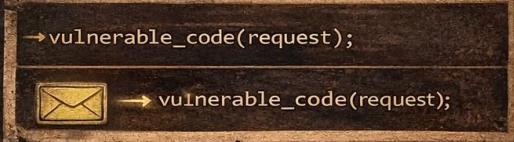
Why Collection TA0009 occurs?

- Weak user access controls
- Lack of security monitoring
- Credential management flaws

TECHNICAL IMPACT

What are the consequences?

- Credential Theft (Usernames, passwords)
- Data Exfiltration (Files, screenshots)
- System Control (Command execution, keylogging)



REQUEST



REQUEST

VULNERABLE CODE

→ vulnerable_code(request);

RESULT



Data & Credentials Stolen

Image 3 : Attack Flow / Technique



10. Command and Control

Image 1 : Overview

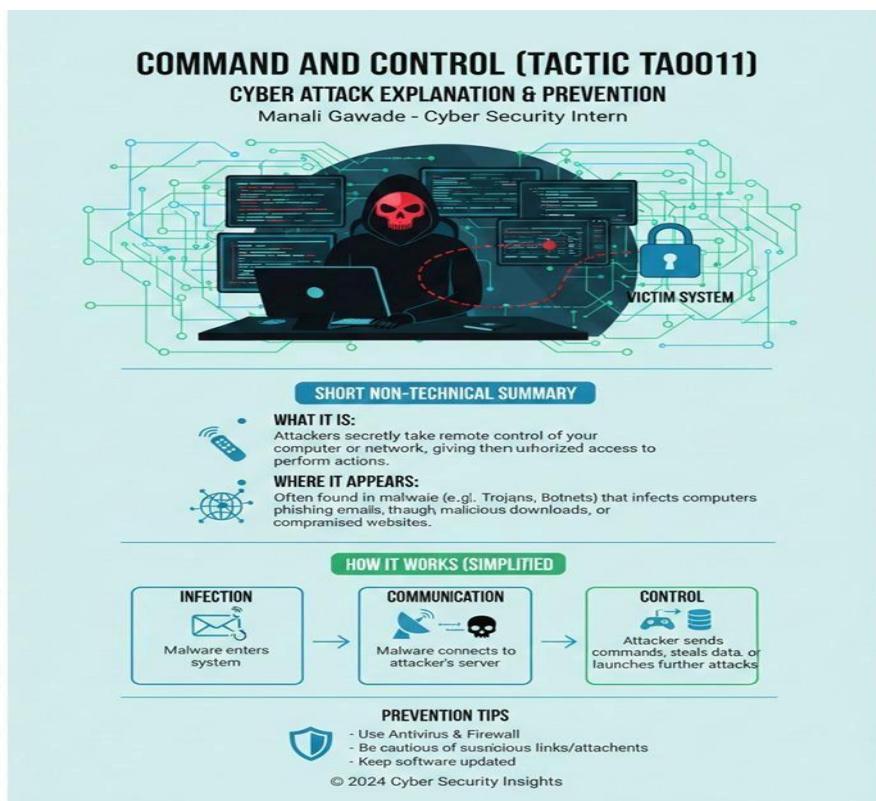


Image 2 : Technical Details

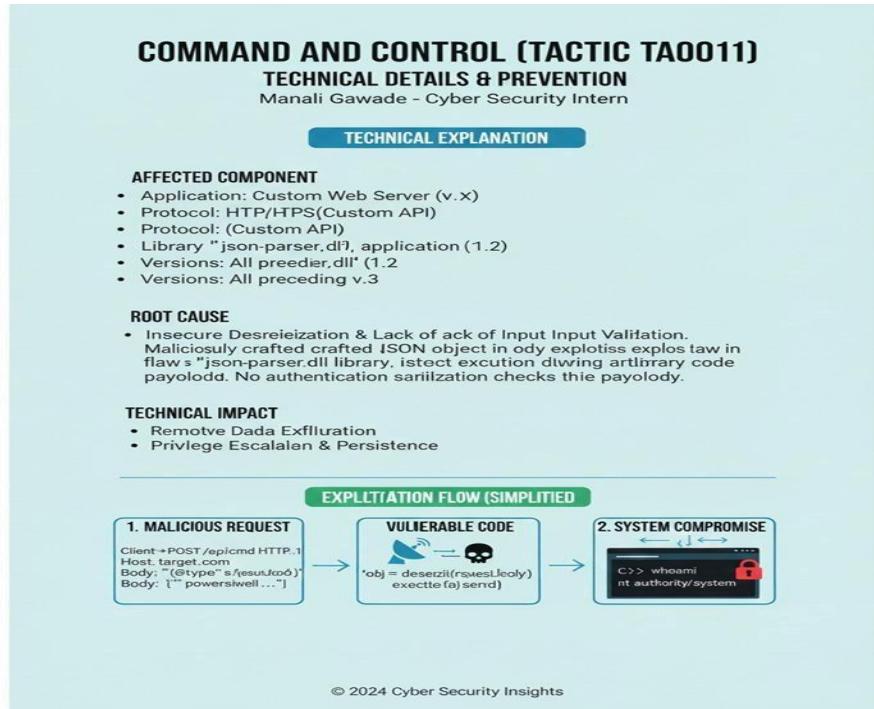
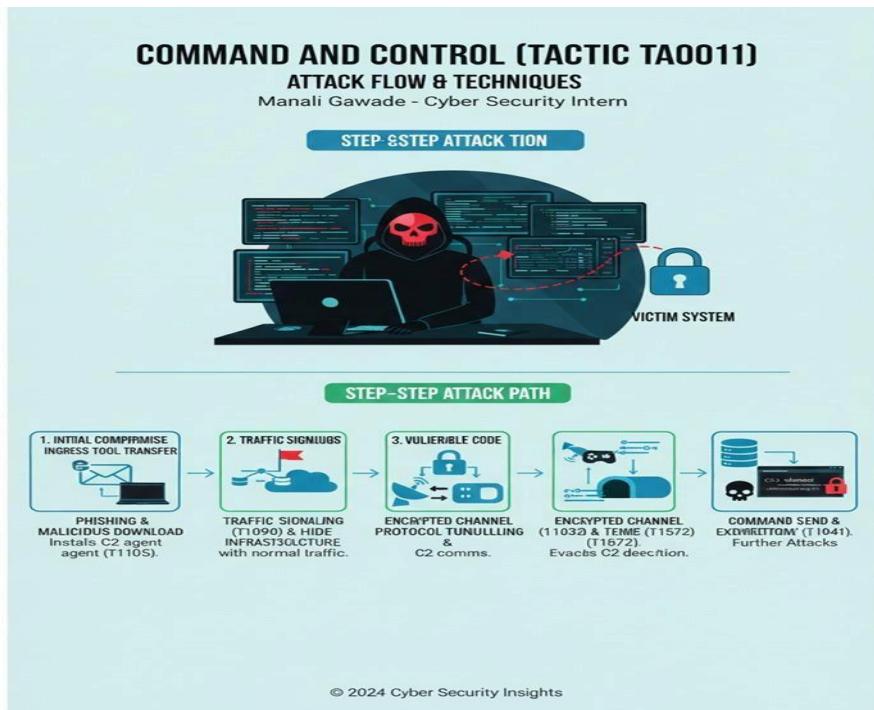


Image 3 : Attack Flow / Techniques



11. Exfiltration

Image 1 : Overview

COMMAND AND CONTROL
CYBER SECURITY VULNERABILITY EXPLAINED

SHORT NON-TECHNICAL SUMMARY

- Malicious actors take remote compromised systems or networks.
- They issue commands to steal data, disrupt operations, or launch further attacks.
- Often uses covert communication channels.

WHERE IT APPEARS

- IOT Devices (Cameras, Routers)
- Enterprise Networks
- Personal Computers
- Mobile Devices
- Critical Infrastructure Systems

IMPACT:
Data Theft, Downtime, Financial Loss, Reputation Damage.

INTERN'S NAME:
Manali Gawade
ROLE: Cyber Security Intern

Image 2 : Technical Details

COMMAND AND CONTROL
TECHNICAL DETAILS EXPLAINED

AFFECTED COMPONENTS

- Applications: Web Servers (Apache, Nginx <v1.20) Custom IoT Apps
- Protocols: Protocols
- DNS, HTTP/HTTPS, IRC custom C2 libraries
- Libraries: libcurl 0, custom <7.8.0, IRC
- Libraries: custom C2 libraries
- Versions: Varies widely, often unpatched or old
- Critical Infrastructure Systems

ROOT CAUSE

- Insecure Input Validation
- Authentication/Authorization Bypass
- Insecure Deserialization Bypass
- Weak Encryption
- Weak Encryption/Obfuscation Vulnerabilities
- Exploiting Unpatched Zero-Day
- Misconfigured Farms/Proxies

TECHNICAL IMPACT

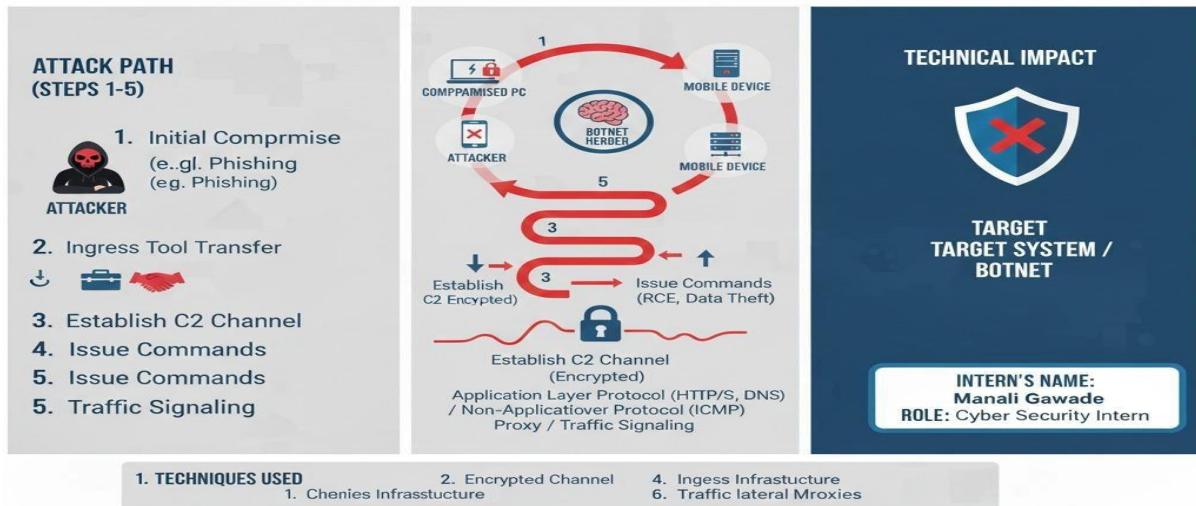
- Remote Code Execution (RCE)
- Data Exfiltration
- Data Extraction/Leakage
- Ransom/Leakages
- Denial of Service
- Privilege Escalation/Privilege Escalation
- Denial of Service/DOS
- Installation of Additional (e.g., Ransomware)
- Network lateral Movement

INTERN'S NAME:
Manali Gawade
ROLE: Cyber Security Intern

Image 3 : Attack Flow / Techniques

COMMAND AND CONTROL

ATTACK FLOW / TECHNIQUE EXPLAINED



12. Impact

Image 1 : Overview

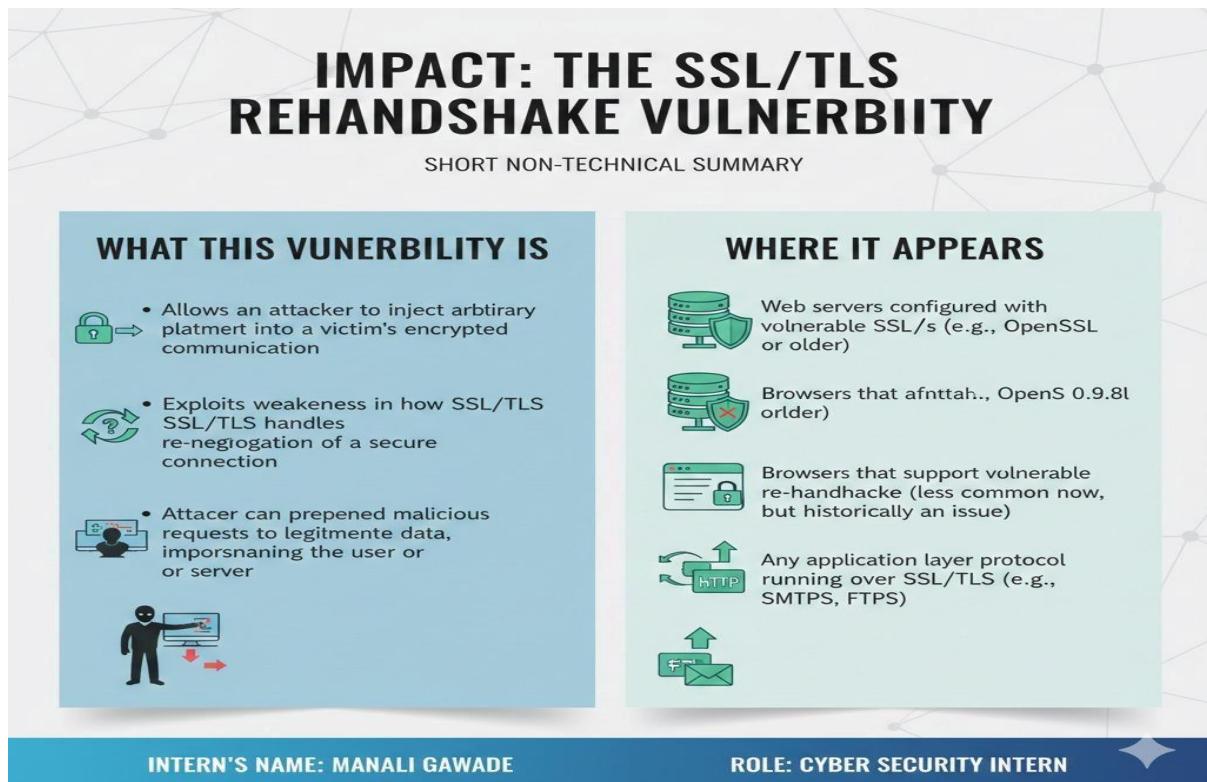


Image 2 : Technical Details

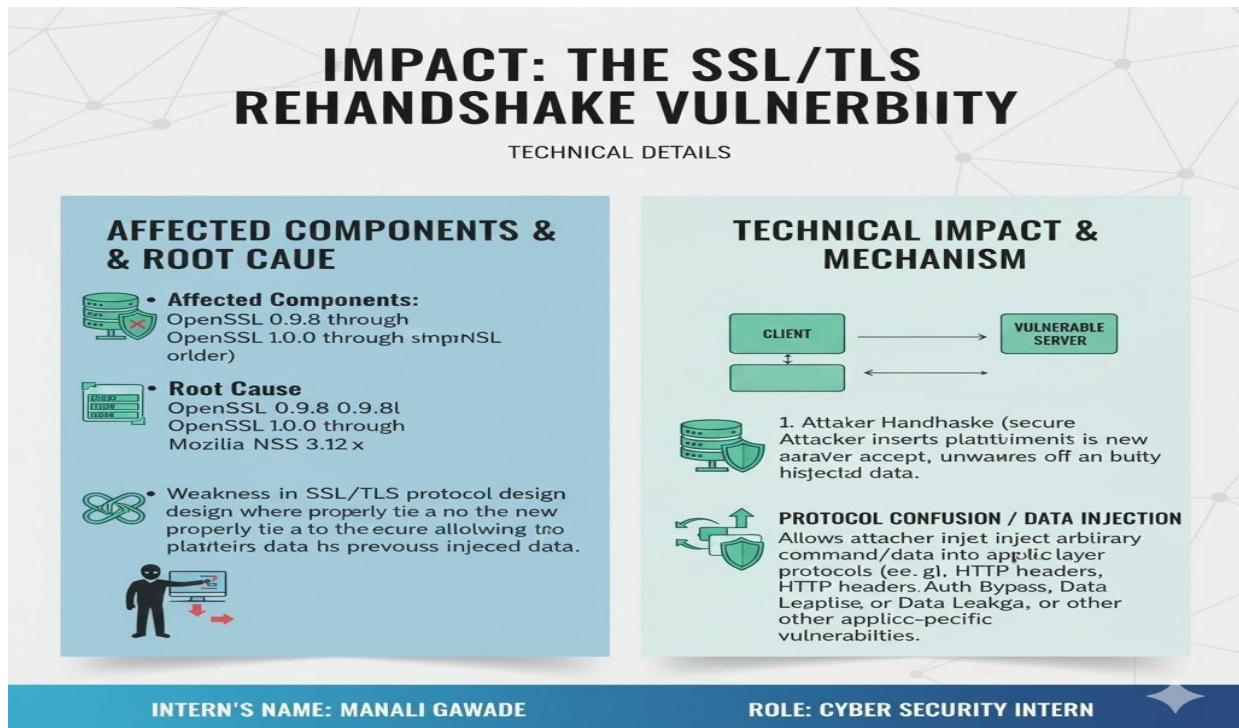


Image 3 : Attack Flow / Techniques

