MITRE ATT&CK Mini-Matrix Report

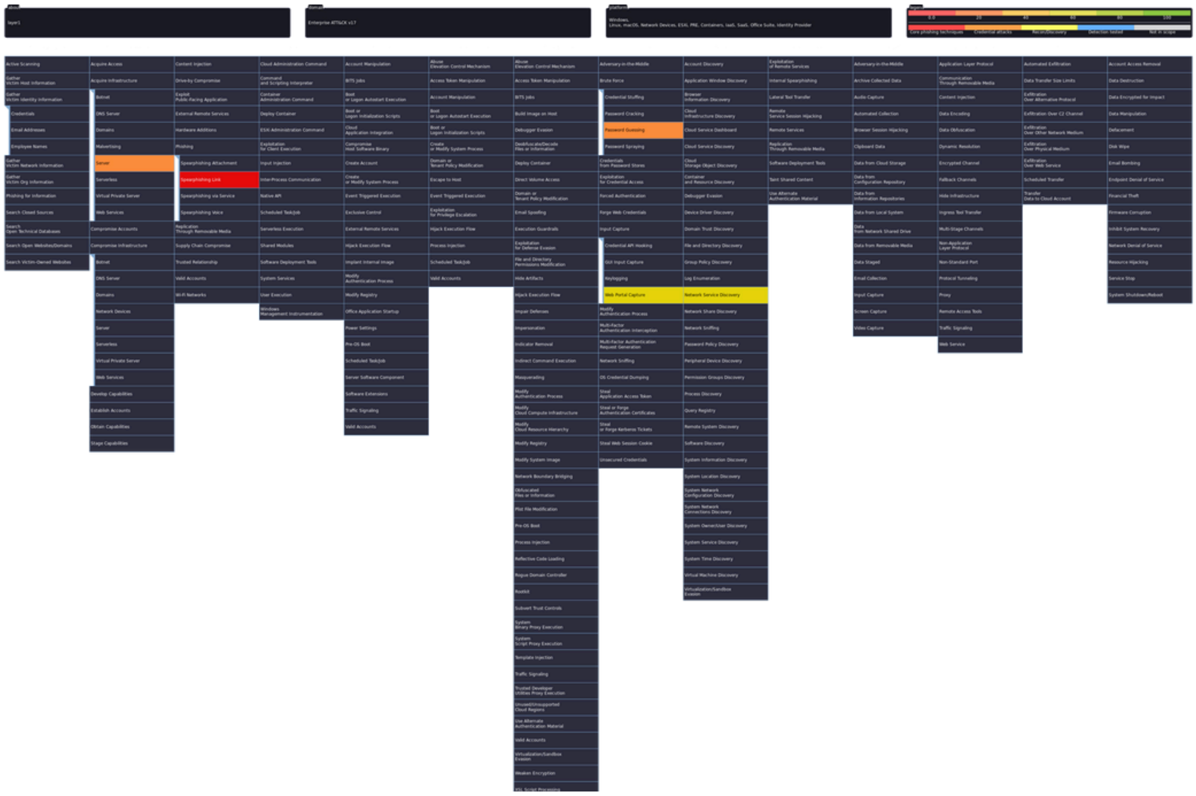
Author: Piyush Ankush
Date: Aug 26, 2025

Project Overview:

Map 5 common phishing-related TTPs to the MITRE ATT&CK framework, simulate attacks in a lab, and document SOC detection strategies.

Key Deliverables:

- **MITRE ATT&CK Matrix (scored + color-coded)**
- **Detection Notes for each technique**
- **Lab Simulations with screenshots**
- **GitHub Repository**



about

layer1

domain

Enterprise ATT&CK v17

platforms

Windows,
Linux, macOS, Network Devices, ESXi, PRE, Containers, IaaS, SaaS, Office Suite, Identity Provider

legend

0.0 20 40 60 80 100

Core phishing techniques | Credential attacks | Recon/Discovery | Detection tested | Not in scope

- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Credentials
- Email Addresses
- Employee Names
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

- Acquire Access
- Acquire Infrastructure
- Botnet
- DNS Server
- Domains
- Malvertising
- Server
- Serverless
- Virtual Private Server
- Web Services
- Compromise Accounts
- Compromise Infrastructure
- Botnet
- DNS Server
- Domains
- Network Devices
- Server
- Serverless
- Virtual Private Server
- Web Services
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities
- Stage Capabilities

- Content Injection
- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Spearphishing Voice
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Wi-Fi Networks

- Cloud Administration Command
- Command and Scripting Interpreter
- Container Administration Command
- Deploy Container
- ESXi Administration Command
- Exploitation for Client Execution
- Input Injection
- Inter-Process Communication
- Native API
- Scheduled Task/Job
- Serverless Execution
- Shared Modules
- Software Deployment Tools
- System Services
- User Execution
- Windows Management Instrumentation

- Account Manipulation
- BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Cloud Application Integration
- Compromise Host Software Binary
- Create Account
- Create or Modify System Process
- Event Triggered Execution
- Exclusive Control
- External Remote Services
- Hijack Execution Flow
- Implant Internal Image
- Modify Authentication Process
- Modify Registry
- Office Application Startup
- Power Settings
- Pre-OS Boot
- Scheduled Task/Job
- Server Software Component
- Software Extensions
- Traffic Signaling
- Valid Accounts

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- Account Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain or Tenant Policy Modification
- Escape to Host
- Event Triggered Execution
- Exploitation for Privilege Escalation
- Hijack Execution Flow
- Process Injection
- Scheduled Task/Job
- Valid Accounts

- Abuse Elevation Control Mechanism
- Access Token Manipulation
- BITS Jobs
- Build Image on Host
- Debugger Evasion
- Deobfuscate/Decode Files or Information
- Deploy Container
- Direct Volume Access
- Domain or Tenant Policy Modification
- Email Spoofing
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- Hijack Execution Flow
- Impair Defenses
- Impersonation
- Indicator Removal
- Indirect Command Execution
- Masquerading
- Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Cloud Resource Hierarchy
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- Obfuscated Files or Information
- Plist File Modification
- Pre-OS Boot
- Process Injection
- Reflective Code Loading
- Rogue Domain Controller
- Rootkit
- Subvert Trust Controls
- System Binary Proxy Execution
- System Script Proxy Execution
- Template Injection
- Traffic Signaling
- Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- XSL Script Processing

- Adversary-in-the-Middle
- Brute Force
- Credential Stuffing
- Password Cracking
- Password Guessing
- Password Spraying
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- Credential API Hooking
- GUI Input Capture
- Keylogging
- Web Portal Capture
- Modify Authentication Process
- Multi-Factor Authentication Interception
- Multi-Factor Authentication Request Generation
- Network Sniffing
- OS Credential Dumping
- Steal Application Access Token
- Steal or Forge Authentication Certificates
- Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Unsecured Credentials

- Account Discovery
- Application Window Discovery
- Browser Information Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Cloud Storage Object Discovery
- Container and Resource Discovery
- Debugger Evasion
- Device Driver Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Group Policy Discovery
- Log Enumeration
- Network Service Discovery
- Network Share Discovery
- Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Location Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtual Machine Discovery
- Virtualization/Sandbox Evasion

- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- Taint Shared Content
- Use Alternate Authentication Material

- Adversary-in-the-Middle
- Archive Collected Data
- Audio Capture
- Automated Collection
- Browser Session Hijacking
- Clipboard Data
- Data from Cloud Storage
- Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- Email Collection
- Input Capture
- Screen Capture
- Video Capture

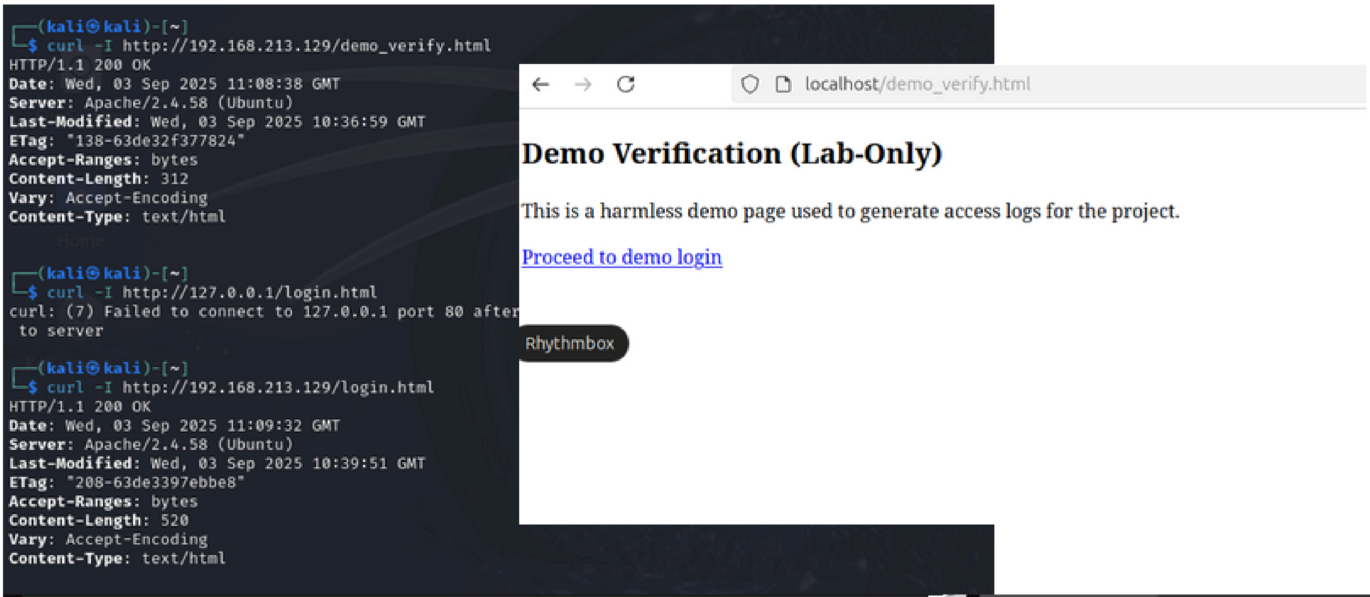
- Application Layer Protocol
- Communication Through Removable Media
- Content Injection
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Hide Infrastructure
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- Remote Access Tools
- Traffic Signaling
- Web Service

- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- Data Manipulation
- Defacement
- Disk Wipe
- Email Bombing
- Endpoint Denial of Service
- Financial Theft
- Firmware Corruption
- Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

Methodology:

1. **Selected techniques (Set B: Phishing chain).**
2. **Researched MITRE IDs, detection notes, and SOC detection methods.**
3. **Simulated techniques (Nmap scan, phishing link, credential capture, password guessing).**
4. **Created ATT&CK Navigator matrix with scoring + legend.**
5. **Compiled results into visual + JSON deliverables.**

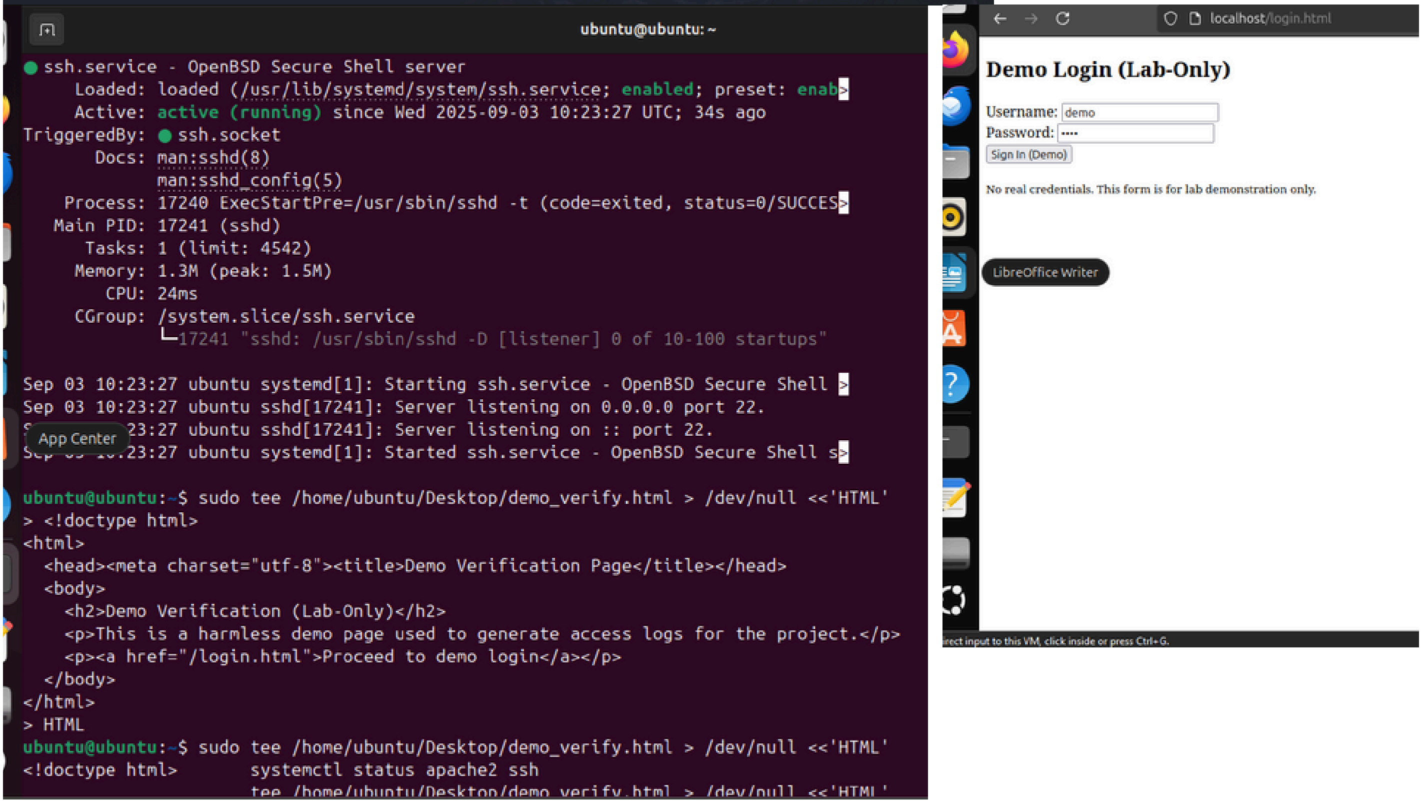


```
┌──(kali㉿kali)-[~]
└─$ curl -I http://192.168.213.129/demo_verify.html
HTTP/1.1 200 OK
Date: Wed, 03 Sep 2025 11:08:38 GMT
Server: Apache/2.4.58 (Ubuntu)
Last-Modified: Wed, 03 Sep 2025 10:36:59 GMT
ETag: "138-63de32f377824"
Accept-Ranges: bytes
Content-Length: 312
Vary: Accept-Encoding
Content-Type: text/html

┌──(kali㉿kali)-[~]
└─$ curl -I http://127.0.0.1/login.html
curl: (7) Failed to connect to 127.0.0.1 port 80 after
 to server

┌──(kali㉿kali)-[~]
└─$ curl -I http://192.168.213.129/login.html
HTTP/1.1 200 OK
Date: Wed, 03 Sep 2025 11:09:32 GMT
Server: Apache/2.4.58 (Ubuntu)
Last-Modified: Wed, 03 Sep 2025 10:39:51 GMT
ETag: "208-63de3397ebbe8"
Accept-Ranges: bytes
Content-Length: 520
Vary: Accept-Encoding
Content-Type: text/html
```

Demo Verification (Lab-Only)

This is a harmless demo page used to generate access logs for the project.

Proceed to demo login

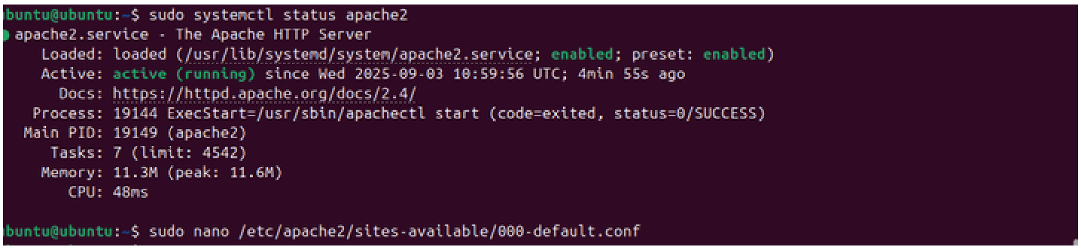


```
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>
     Active: active (running) since Wed 2025-09-03 10:23:27 UTC; 34s ago
TriggeredBy: ● ssh.socket
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 17240 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCES>
   Main PID: 17241 (sshd)
      Tasks: 1 (limit: 4542)
     Memory: 1.3M (peak: 1.5M)
        CPU: 24ms
     CGroup: /system.slice/ssh.service
             └─17241 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 03 10:23:27 ubuntu systemd[1]: Starting ssh.service - OpenBSD Secure Shell >
Sep 03 10:23:27 ubuntu sshd[17241]: Server listening on 0.0.0.0 port 22.
Sep 03 10:23:27 ubuntu sshd[17241]: Server listening on :: port 22.
Sep 03 10:23:27 ubuntu systemd[1]: Started ssh.service - OpenBSD Secure Shell s>

ubuntu@ubuntu:~$ sudo tee /home/ubuntu/Desktop/demo_verify.html > /dev/null <<'HTML'
> <!doctype html>
<html>
  <head><meta charset="utf-8"><title>Demo Verification Page</title></head>
  <body>
    <h2>Demo Verification (Lab-Only)</h2>
    <p>This is a harmless demo page used to generate access logs for the project.</p>
    <p><a href="/login.html">Proceed to demo login</a></p>
  </body>
</html>
> HTML
ubuntu@ubuntu:~$ sudo tee /home/ubuntu/Desktop/demo_verify.html > /dev/null <<'HTML'
<!doctype html>       systemctl status apache2 ssh
                      tee /home/ubuntu/Desktop/demo_verify.html > /dev/null <<'HTML'
```

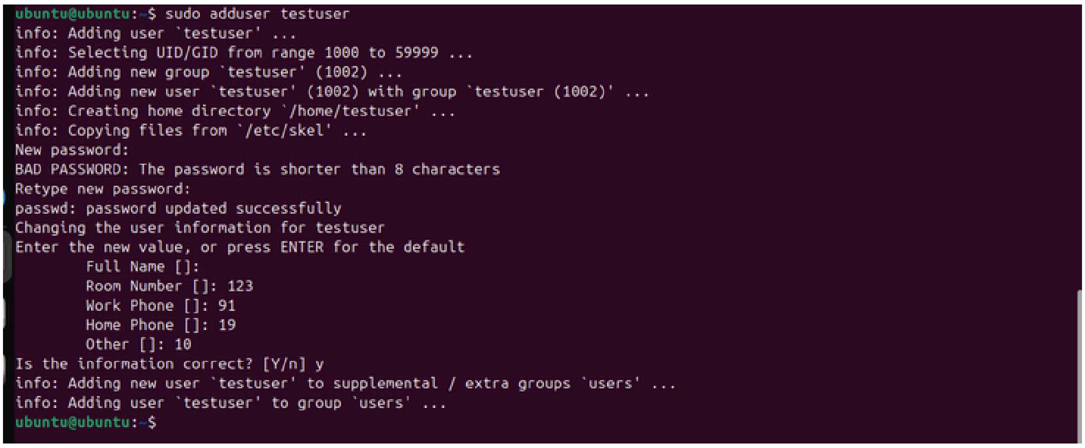
Demo Login (Lab-Only)

Username: demo
Password: ····
Sign In (Demo)

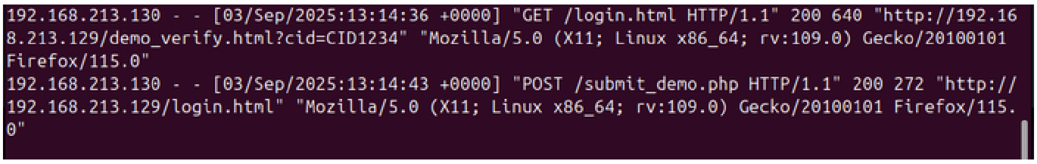
No real credentials. This form is for lab demonstration only.



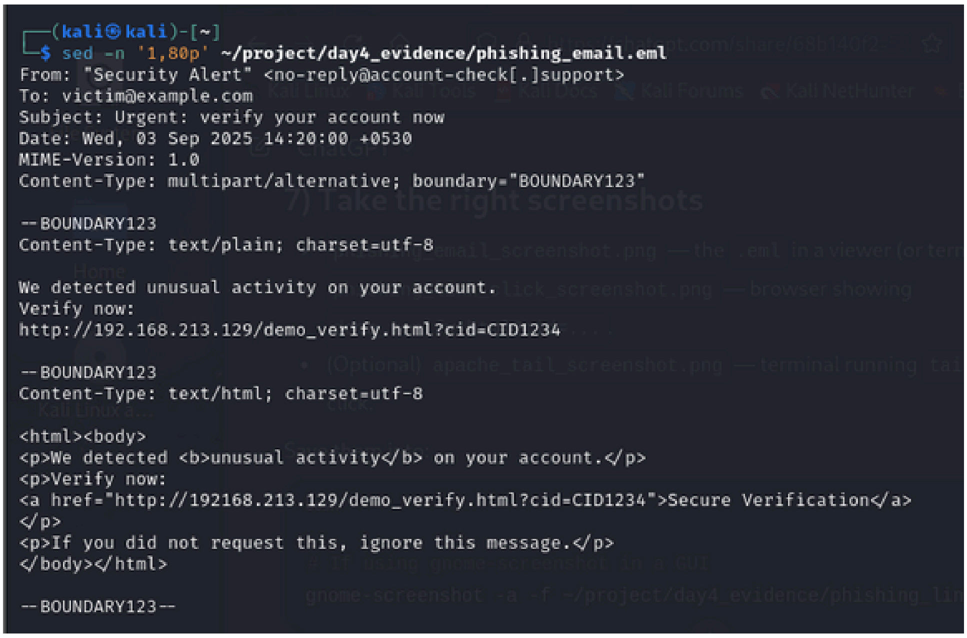
```
buntu@ubuntu:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Wed 2025-09-03 10:59:56 UTC; 4min 55s ago
       Docs: https://httpd.apache.org/docs/2.4/
    Process: 19144 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 19149 (apache2)
      Tasks: 7 (limit: 4542)
     Memory: 11.3M (peak: 11.6M)
        CPU: 48ms

buntu@ubuntu:~$ sudo nano /etc/apache2/sites-available/000-default.conf
```



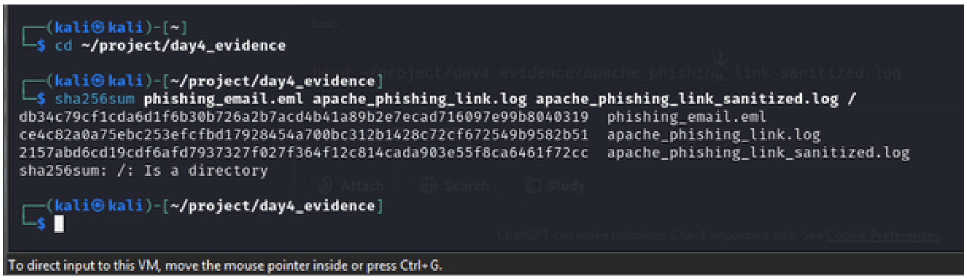
```
ubuntu@ubuntu:~$ sudo adduser testuser
info: Adding user `testuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testuser' (1002) ...
info: Adding new user `testuser' (1002) with group `testuser (1002)' ...
info: Creating home directory `/home/testuser' ...
info: Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []: 123
        Work Phone []: 91
        Home Phone []: 19
        Other []: 10
Is the information correct? [Y/n] y
info: Adding new user `testuser' to supplemental / extra groups `users' ...
info: Adding user `testuser' to group `users' ...
ubuntu@ubuntu:~$
```



```
192.168.213.130 - - [03/Sep/2025:13:14:36 +0000] "GET /login.html HTTP/1.1" 200 640 "http://192.16
8.213.129/demo_verify.html?cid=CID1234" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
Firefox/115.0"
192.168.213.130 - - [03/Sep/2025:13:14:43 +0000] "POST /submit_demo.php HTTP/1.1" 200 272 "http://
192.168.213.129/login.html" "Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.
0"
```

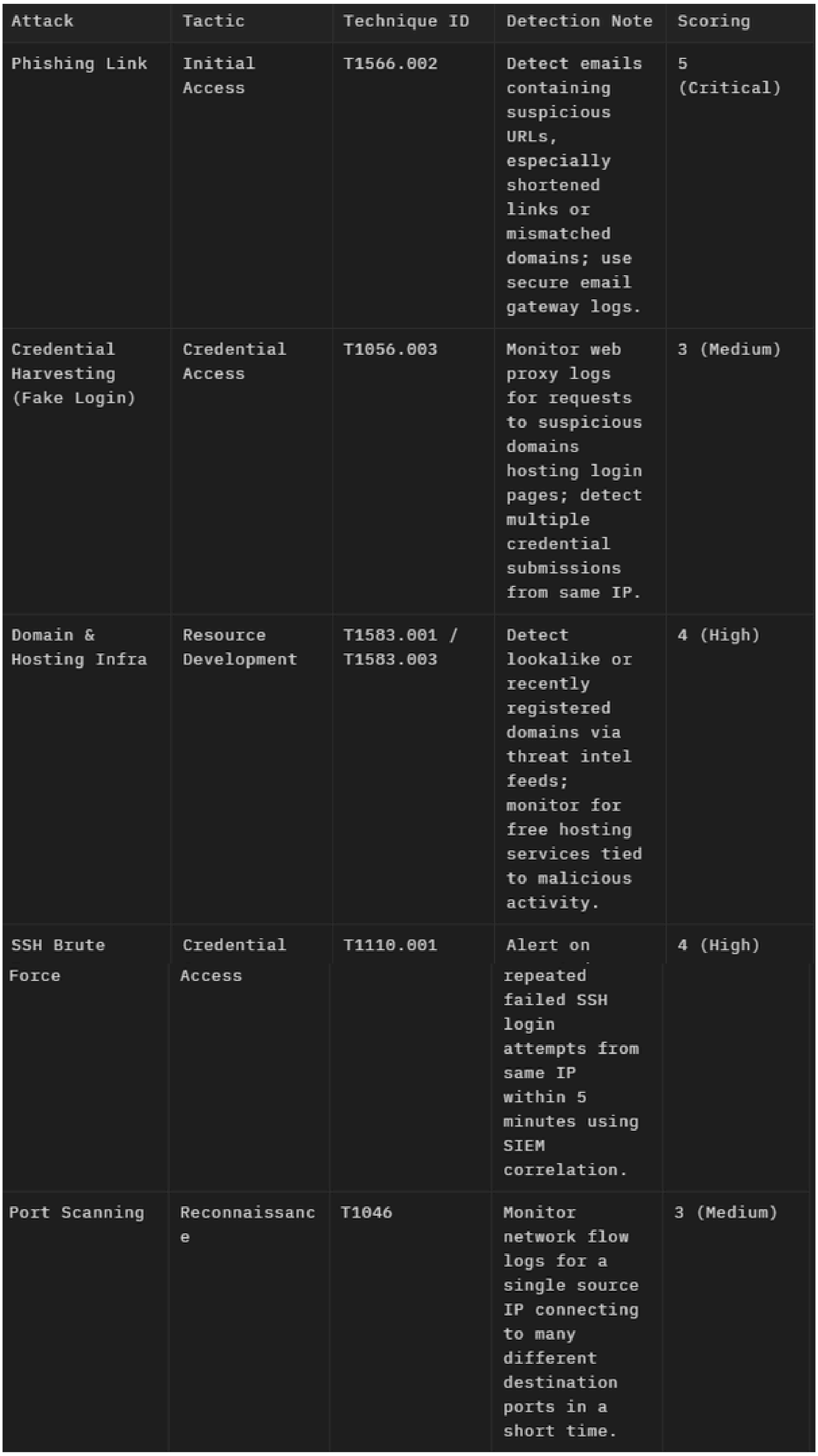


```
┌──(kali㉿kali)-[~]
└─$ sed -n '1,80p' ~/project/day4_evidence/phishing_email.eml
From: "Security Alert" <no-reply@account-check[.]support>
To: victim@example.com
Subject: Urgent: verify your account now
Date: Wed, 03 Sep 2025 14:20:00 +0530
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="BOUNDARY123"

--BOUNDARY123
Content-Type: text/plain; charset=utf-8

We detected unusual activity on your account.
Verify now:
http://192.168.213.129/demo_verify.html?cid=CID1234

--BOUNDARY123
Content-Type: text/html; charset=utf-8

<html><body>
<p>We detected <b>unusual activity</b> on your account.</p>
<p>Verify now:
<a href="http://192168.213.129/demo_verify.html?cid=CID1234">Secure Verification</a>
</p>
<p>If you did not request this, ignore this message.</p>
</body></html>

--BOUNDARY123--
```



```
┌──(kali㉿kali)-[~]
└─$ cd ~/project/day4_evidence

┌──(kali㉿kali)-[~/project/day4_evidence]
└─$ sha256sum phishing_email.eml apache_phishing_link.log apache_phishing_link_sanitized.log /
db34c79cf1cda6d1f6b30b726a2b7acd4b41a89b2e7ecad716097e99b8040319  phishing_email.eml
ce4c82a0a75ebc253efcfbd17928454a700bc312b1428c72cf672549b9582b51  apache_phishing_link.log
2157abd6cd19cdf6afd7937327f027f364f12c814cada903e55f8ca6461f72cc  apache_phishing_link_sanitized.log
sha256sum: /: Is a directory

┌──(kali㉿kali)-[~/project/day4_evidence]
└─$ 
```

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.



Attack	Tactic	Technique ID	Detection Note	Scoring
Phishing Link	Initial Access	T1566.002	Detect emails containing suspicious URLs, especially shortened links or mismatched domains; use secure email gateway logs.	5 (Critical)
Credential Harvesting (Fake Login)	Credential Access	T1056.003	Monitor web proxy logs for requests to suspicious domains hosting login pages; detect multiple credential submissions from same IP.	3 (Medium)
Domain & Hosting Infra	Resource Development	T1583.001 / T1583.003	Detect lookalike or recently registered domains via threat intel feeds; monitor for free hosting services tied to malicious activity.	4 (High)
SSH Brute Force	Credential Access	T1110.001	Alert on repeated failed SSH login attempts from same IP within 5 minutes using SIEM correlation.	4 (High)
Port Scanning	Reconnaissance	T1046	Monitor network flow logs for a single source IP connecting to many different destination ports in a short time.	3 (Medium)

Results & Findings

- **Critical Risks (Score 5): Phishing link delivery is the key threat vector.**
- **High Risks (Score 4): Password brute force & infrastructure setup critical for attackers.**
- **Detection Gaps (Score 3): HTTPS traffic & credential harvesting harder to spot without advanced monitoring.**