Innovation & Entrepreneurship Hub for Educated Rural Youth (SURE Trust – IERY)

Network Penetration Testing: Black Box Approach for Multiple IPs

The Domain of the Project

Cybersecurity & Ethical Hacking (VAPT)

Under the guidance of

Mr. Nishchay Gaba (Cybersecurity Researcher at Hacking Articles)

By

Ms. Marni Satvika

Period of the project

January 2025 to February 2025

SUREProED, In association with SURE Trust
Puttaparthi, Andhra Pradesh – 515134

DECLARATION

The project titled ***"Network Penetration Testing: Black Box Approach for Multiple IPs s"*** has been mentored by **Mr. Nishchay Gaba** and organized by SURE Trust from January 2025 to February 2025**.** This initiative aims to benefit educated unemployed rural youth by providing hands-on experience in industry-relevant projects, thereby enhancing employability.

I, **Ms. Marni Satvika** hereby declare that I have solely worked on this project under the guidance of my mentor. This project has significantly enhanced my practical knowledge and skills in the domain.

Name
Ms. Marni Satvika

Signature
Satvika

Mentor

Mr. Nishchay Gaba

(Cybersecurity Researcher at Hacking Articles)

Signature

Seal & Signature

Prof. Radhakumari
Executive Director & Founder
SUREProEd

Table of Contents

Executive Summary

This report details the findings of a **Black Box Network Penetration** Test conducted on **30 IP addresses** to evaluate security posture from an external attacker's perspective. The assessment combined automated scanning (Nmap, OpenVAS) with manual validation to identify exploitable vulnerabilities.

Key Findings:

- Critical: Unpatched RDP (CVE-2019-0708), SSLv2/SSLv3 exposure (CVE-2016-0800), default credentials, and unsecured Telnet.
- High: OpenSSH user enumeration (CVE-2018-15473), weak TLS configurations (Logjam, BEAST, ROBOT).
- Medium: SSH command injection (CVE-2020-15778), weak ciphers (SWEET32, RC4).
- Low: Anonymous FTP access, deprecated protocols.

Vulnerabilities were manually verified with PoC evidence and mapped to CWE/OWASP Top 10 (e.g., CWE-327: Broken Crypto). Critical risks included RCE via BlueKeep and TLS downgrade attacks, while medium/low issues highlighted authentication and encryption flaws.

The results emphasize urgent risks to confidentiality, integrity, and compliance (PCI-DSS, NIST). Stakeholders must prioritize remediation to prevent exploitation.

Introduction

Background & Context

In today's evolving threat landscape, organizations face increasing risks from cyberattacks targeting exposed network infrastructure. Public-facing IP addresses, if misconfigured or unpatched, can serve as entry points for attackers, leading to data breaches, service disruptions, and compliance violations. Proactive security assessments, such as penetration testing, are critical to identifying vulnerabilities before malicious actors exploit them.

This Black Box Network Penetration Test was conducted to simulate a real-world attacker's approach, assessing the security posture of 30 public IP addresses without prior knowledge of internal systems. The engagement aligns with industry best practices (NIST SP 800-115, OWASP Testing Guide) to evaluate risks objectively.

Problem Statement

Despite advancements in cybersecurity, many organizations remain vulnerable due to:

- Outdated protocols (SSLv2/SSLv3, TLS 1.0).
- Unpatched services (e.g., RDP, OpenSSH).
- Weak configurations (default credentials, anonymous FTP). This assessment addresses these gaps by identifying exploitable weaknesses and providing actionable insights to mitigate exposure.

Scope & Limitations

- **In Scope:** 30 public IPs, focusing on open ports, services, and protocol weaknesses.
- **Out of Scope:** Internal networks, social engineering, and DoS attacks.

Limitations:

- Point-in-time assessment (new vulnerabilities may emerge post-testing).
- False positives/negatives possible due to tool constraints.
- Non-disruptive testing (no exploitation of critical production systems).

Innovation Component

This engagement incorporated:

- Hybrid Testing: Automated scans (Nmap, OpenVAS) paired with manual exploitation to reduce false positives.
- Threat Intelligence Integration: Mapped findings to CVE/CWE and OWASP Top 10 for risk contextualization.
- Compliance-Aware Analysis: Highlighted gaps against PCI-DSS 4.0 and NIST SP 800-53 controls.

Project Objectives

Project Objective

The primary objective of this Black Box Network Penetration Testing engagement was to:

- Identify vulnerabilities in public-facing network infrastructure that could be exploited by external attackers.
- Assess security controls (firewalls, encryption, access mechanisms) for effectiveness against real-world threats.
- Simulate attacker behavior to validate risks without prior knowledge of internal systems.
- Support compliance with industry standards (PCI-DSS, NIST, ISO 27001) by uncovering gaps in configurations and protocols.

Expected Outcome

- Understand Exposure: Gain clarity on critical/high-risk vulnerabilities (e.g., RCE via BlueKeep, TLS downgrades).
- Prioritize Remediation: Focus on patching 4 Critical and 7 High risks first (e.g., SSLv2/SSLv3, OpenSSH flaws).
- Align with Best Practices: Use findings to harden systems against OWASP Top 10 and CWE-mapped threats.
- Meet Compliance: Address gaps violating PCI-DSS 4.0 (e.g., TLS 1.0/1.1) and NIST SP 800-53 (encryption standards).

Deliverables

1. Detailed Report:

- Executive summary, methodology, and risk-rated findings.
- Proof of Concept (PoC) for validated vulnerabilities (e.g., CVE-2019-0708 exploit steps).
- Screenshots/Logs from tools (Nmap, OpenVAS) and manual testing.

1. Risk Prioritization Matrix:

- Tables ranking vulnerabilities by CVSS scores, business impact, and exploit complexity.

2. Remediation Guidance:

- Step-by-step fixes (e.g., "Disable SSLv2/SSLv3 in Apache: SSLProtocol -all +TLSv1.2").
- Patch references (e.g., Microsoft KB4499175 for BlueKeep).

3. Compliance Mapping:

- Cross-referenced vulnerabilities with PCI-DSS 4.0, NIST SP 800-53, and ISO 27001 controls.

4. Retesting Plan:

- Timeline for follow-up validation after remediation.

Methodology and Results

Methods/Technology Used

The Black Box Penetration Testing methodology was employed, simulating an external attacker with no prior knowledge of the target infrastructure. The approach included:

1. Reconnaissance:

- Passive: OSINT (Open-Source Intelligence) gathering via WHOIS, DNS lookups, and search engines.
- Active: Port scanning and service enumeration to identify entry points.

2. Vulnerability Scanning: Automated and manual testing to detect misconfigurations, outdated software, and weak protocols.

3. Exploitation: Manual validation of critical/high-risk vulnerabilities (e.g., RCE, TLS downgrades) to confirm exploitability.

4. Post-Exploitation: Assessing lateral movement risks (where applicable within scope).

Tools/Software Used

Category	Tools	Purpose
Scanning	Nmap, OpenVAS, Masscan	Port/service discovery, vulnerability detection.
Exploitation	Metasploit, CVE-specific exploits (e.g., BlueKeep), Burp Suite	Validating RCE, MITM, and protocol weaknesses.
Traffic Analysis	Wireshark, Tcpdump	Inspecting unencrypted traffic (e.g., Telnet, FTP).
Crypto Analysis	SSLScan, TestSSL.sh	Testing SSL/TLS configurations (e.g., DROWN, BEAST).
Reporting	Dradis, Faraday, LaTeX	Consolidating findings, generating PoCs, and report drafting.

Data Collection Approach

The penetration test focused on collecting key information, including:

- Open ports and running services
- Software versions and outdated components
- Vulnerabilities identified through scanning and exploitation

Project Architecture

1. Overview

This penetration test assessed 30 public IP addresses using a structured, phased methodology simulating an external attacker. The architecture ensured comprehensive evaluation while maintaining strict ethical boundaries.

2. Testing Phases

Phase 1: Discovery

- Passive Reconnaissance: WHOIS lookups, DNS analysis
- Active Scanning: Port/service identification (Nmap)

Phase 2: Vulnerability Assessment

- Automated scanning (OpenVAS) for known CVEs
- Manual verification of critical services (RDP, SSH, HTTPS)
- Cryptographic analysis (SSL/TLS configurations)

Phase 3: Validation

- Controlled exploitation of critical vulnerabilities
- Evidence collection (screenshots, packet captures)
- Business impact analysis

3. Scope & Boundaries

- **Targets:** Internet-facing services only (no internal networks)
- **Constraints:**
  - No DoS testing or brute-force attacks
  - No lateral movement or data exfiltration
  - Compliance with PCI-DSS/NIST/OWASP standards

4. **Threat Model**

- Adversary Profile: External attacker with zero privileges
- Attack Vectors:
  - Protocol exploitation (TLS/SSL weaknesses)
  - Service vulnerabilities (RDP, SSH misconfigurations)
  - Credential attacks (default/weak credentials)
  - Compliance Alignment

- Addressed key requirements of:
  - PCI-DSS (encryption, access controls)
  - NIST SP 800-53 (SC-13, AC-3)
  - OWASP Top 10 (A2, A6)

This architecture delivered actionable results while ensuring safe, ethical testing practices. The phased approach enabled clear risk prioritization and remediation guidance.

Project Findings

CRITICAL

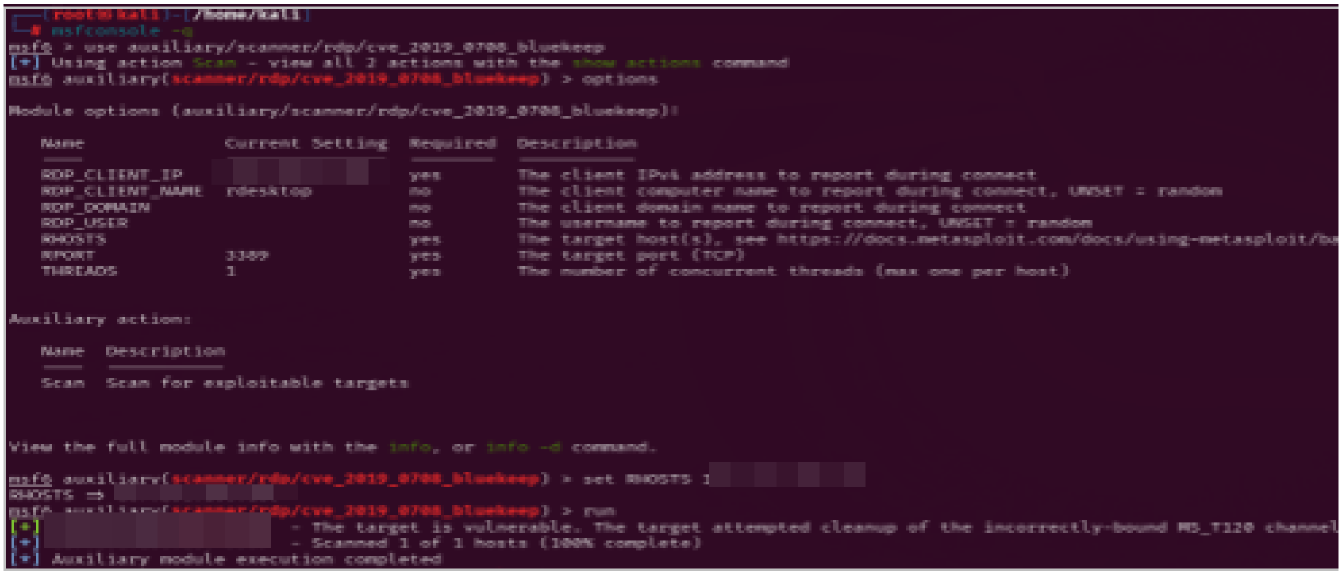
1) AFFECTED PORT: TCP/3389

CVE-ID: CVE 2019-0708

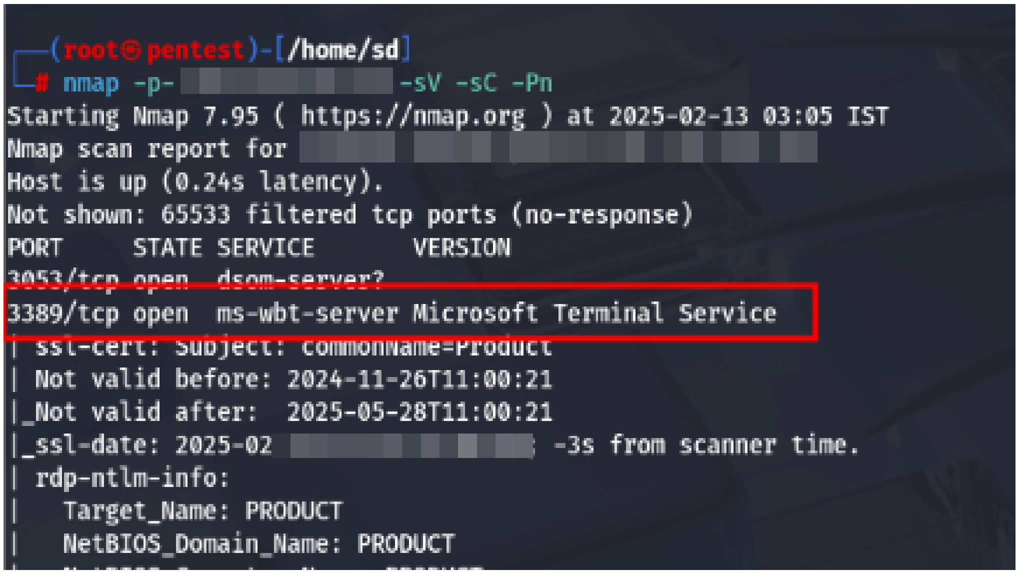
TECHNICAL IMPACT: allows **unauthenticated remote code execution** on vulnerable **RDP servers**, enabling attackers to gain **full system control** and potentially **spread malware across networks**.

MITIGATION: Disable RDP if not needed or restrict access via firewalls, **Enable Network Level Authentication (NLA)** for extra security, **Regularly update systems** to ensure vulnerabilities are patched.

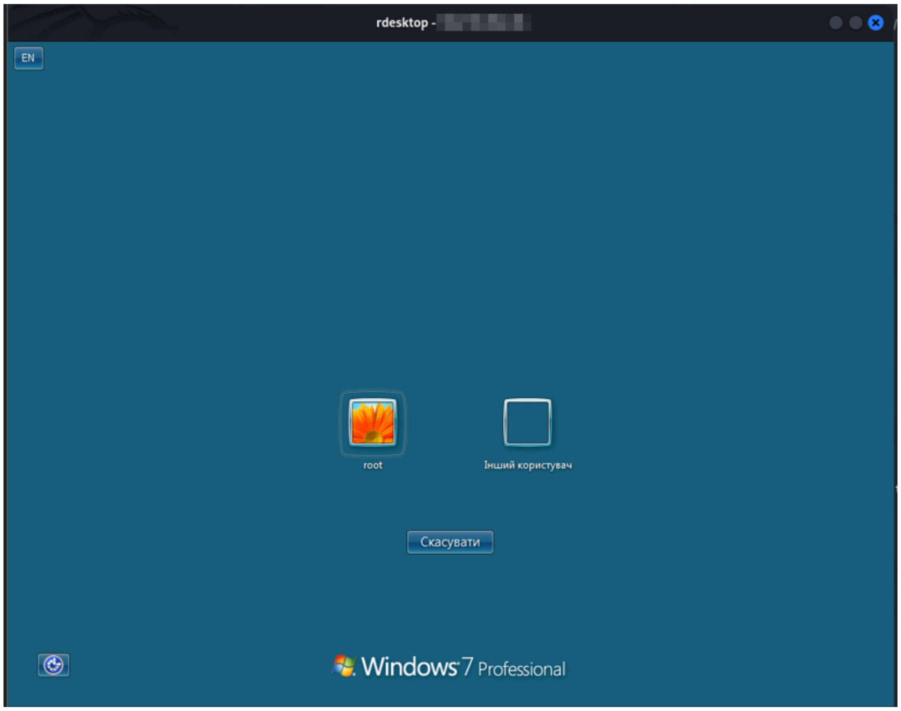
PROOF OF CONCEPT:



```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole -q
msf6 > use auxiliary/scanner/rdp/cve_2019_0708_bluekeep
[*] Using action Scan - view all 2 actions with the show actions command
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > options

Module options (auxiliary/scanner/rdp/cve_2019_0708_bluekeep):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   RDP_CLIENT_IP     [redacted]       yes       The client IPv4 address to report during connect
   RDP_CLIENT_NAME   rdesktop         no        The client computer name to report during connect, UNSET = random
   RDP_DOMAIN                         no        The client domain name to report during connect
   RDP_USER                           no        The username to report during connect, UNSET = random
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
   RPORT             3389             yes       The target port (TCP)
   THREADS           1                yes       The number of concurrent threads (max one per host)


Auxiliary action:

   Name  Description
   ----  -----------
   Scan  Scan for exploitable targets


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

msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > set RHOSTS 1[redacted]
RHOSTS => [redacted]
msf6 auxiliary(scanner/rdp/cve_2019_0708_bluekeep) > run
[+] [redacted]          - The target is vulnerable. The target attempted cleanup of the incorrectly-bound MS_T120 channel
[*] [redacted]          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```



```
┌──(root㉿pentest)-[/home/sd]
└─# nmap -p- [redacted] -sV -sC -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-13 03:05 IST
Nmap scan report for [redacted]
Host is up (0.24s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3053/tcp open  dsom-server?
3389/tcp open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=Product
| Not valid before: 2024-11-26T11:00:21
|_Not valid after:  2025-05-28T11:00:21
|_ssl-date: 2025-02 [redacted] -3s from scanner time.
| rdp-ntlm-info:
|   Target_Name: PRODUCT
|   NetBIOS_Domain_Name: PRODUCT
```



2) AFFECTED PORT: TCP/443

CVE-ID: N/A

TECHNICAL IMPACT: If **SSLv2 or SSLv3(unencrypted communciation)** is offered on a server, it poses **critical security risks** and **major compliance violations** due to their severe vulnerabilities. These outdated protocols allow attackers to exploit encryption weaknesses, downgrade attacks, and compromise data confidentiality.

MITIGATION: Enable TLS 1.3:

Update your server software or TLS library (e.g., OpenSSL, GnuTLS) to a version that supports TLS 1.3.

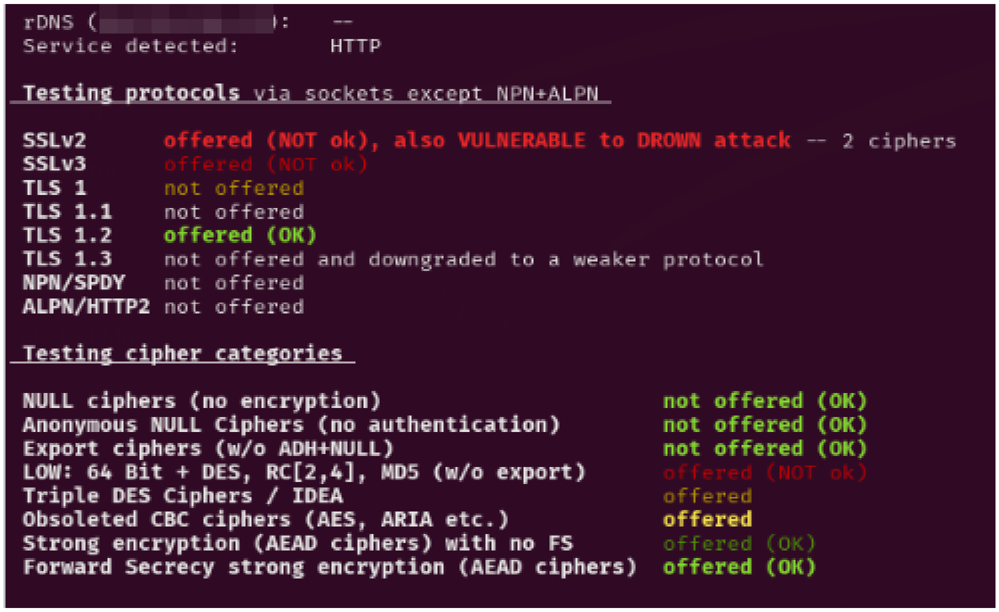
Adjust your configuration to explicitly enable TLS 1.3.

Enable ALPN and HTTP/2:

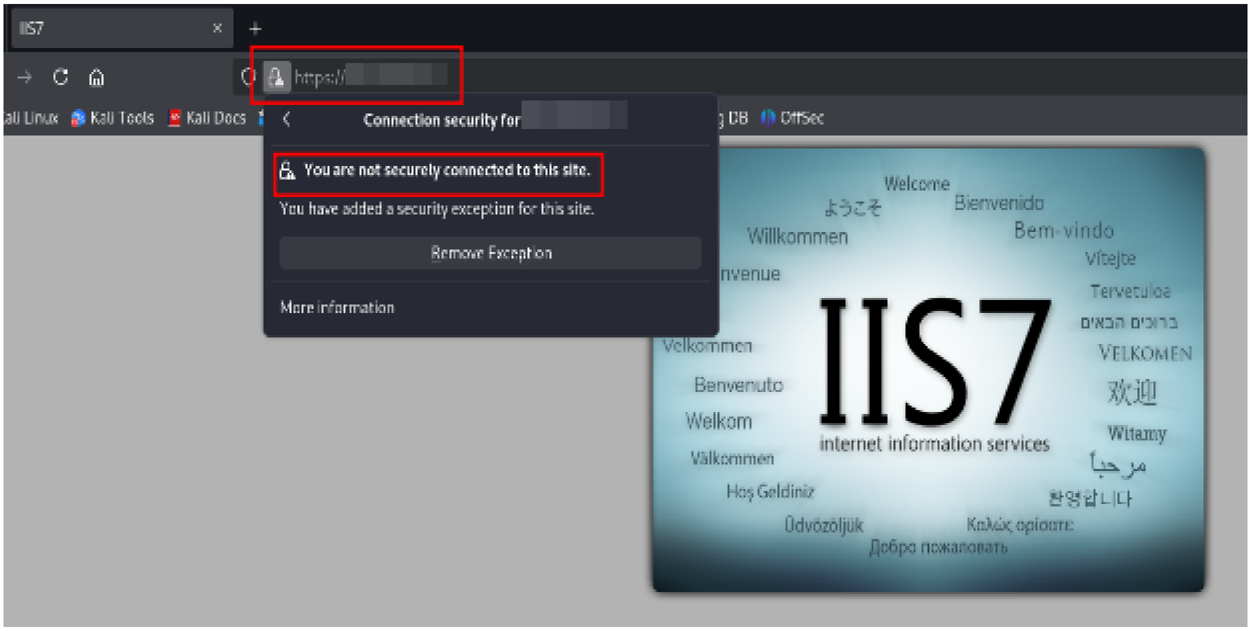
ALPN (Application Layer Protocol Negotiation) is required for HTTP/2 support. Enable it in your server configuration.

Configure your server to support HTTP/2 for faster and more efficient web traffic.

PROOF OF CONCEPT:



```
rDNS ([redacted]):    --
Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN 

 SSLv2      offered (NOT ok), also VULNERABLE to DROWN attack -- 2 ciphers
 SSLv3      offered (NOT ok)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories 

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      offered (NOT ok)
 Triple DES Ciphers / IDEA                         offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```



Connection security for [redacted]

You are not securely connected to this site.

You have added a security exception for this site.

Remove Exception

More information

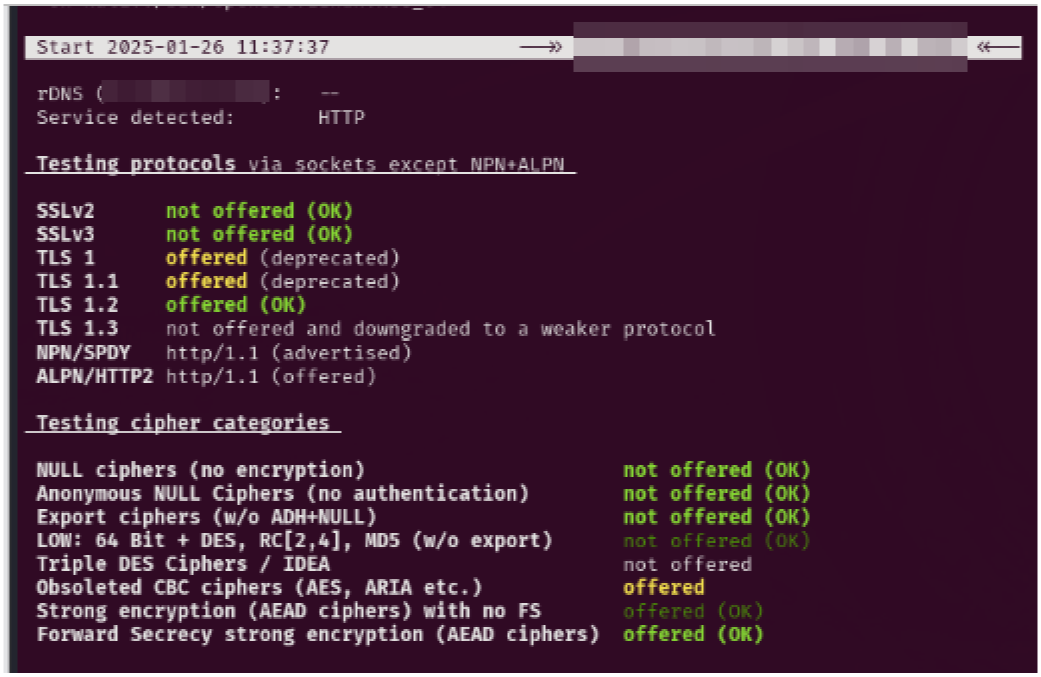
3) AFFECTED PORT: TCP/443

CVE-ID: N/A

TECHNICAL IMPACT: The **technical impact** of using or offering outdated TLS versions is severe, affecting **security, compliance, and functionality**.

MITIGATION: Disable TLS 1.0 & 1.1 on Servers

PROOF OF CONCEPT:



```
 Start 2025-01-26 11:37:37          -->> [redacted] <<--

 rDNS ([redacted]):   --
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   http/1.1 (advertised)
 ALPN/HTTP2 http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```

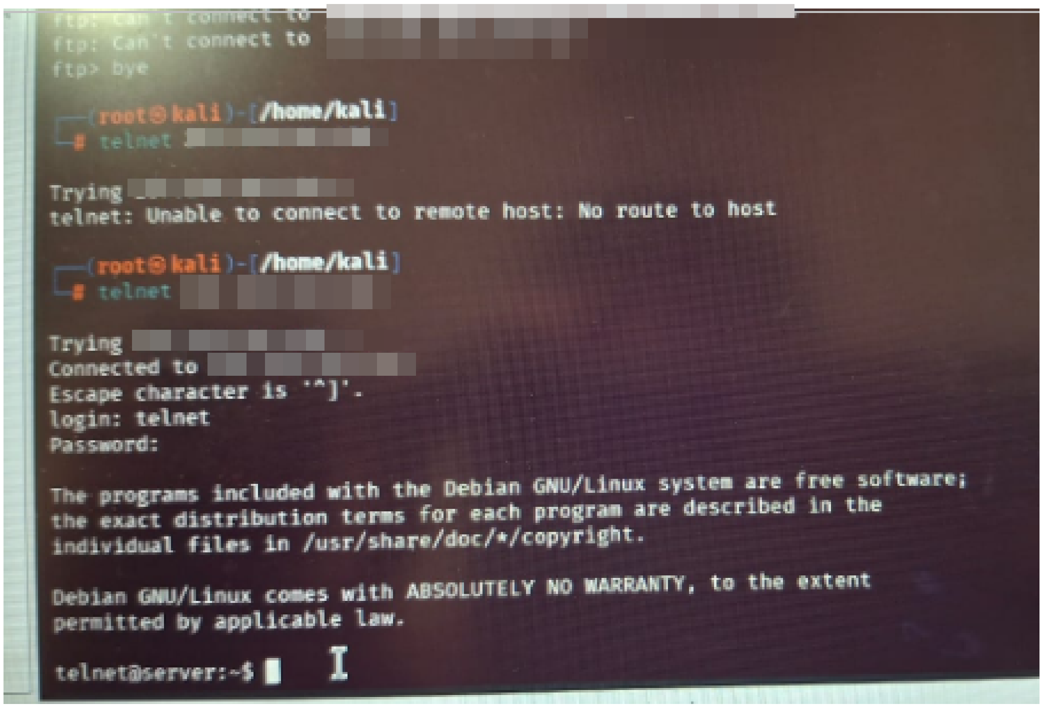
4) AFFECTED PORT: TCP/23

CVE-ID: N/A

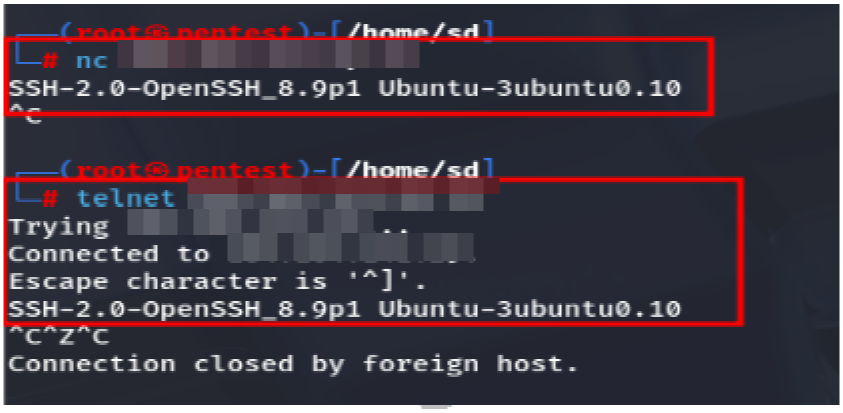
TECHNICAL IMPACT: If **Telnet** is running with **default credentials**, it poses a **severe security risk** as it allows **unauthorized access**, **data interception**, and **complete system compromise**. Telnet is an outdated, **unencrypted** protocol, making it extremely vulnerable to attacks.

MITIGATION: Disable Telnet & Use SSH, Change Default Credentials Immediately

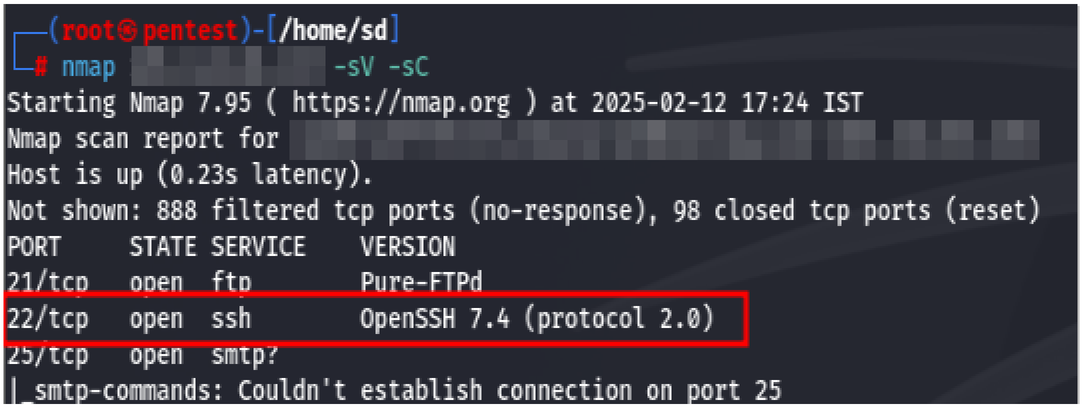
PROOF OF CONCEPT:



```
ftp: Can't connect to [redacted]
ftp: Can't connect to [redacted]
ftp> bye

┌──(root㉿kali)-[/home/kali]
└─# telnet [redacted]

Trying [redacted]
telnet: Unable to connect to remote host: No route to host

┌──(root㉿kali)-[/home/kali]
└─# telnet [redacted]

Trying [redacted]
Connected to [redacted]
Escape character is '^]'.
login: telnet
Password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

telnet@server:~$ █
```



```
┌──(root㉿pentest)-[/home/sd]
└─# nc [redacted]
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
^C

┌──(root㉿pentest)-[/home/sd]
└─# telnet [redacted]
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.10
^C^Z^C
Connection closed by foreign host.
```



```
┌──(root㉿pentest)-[/home/sd]
└─# nmap [redacted] -sV -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 17:24 IST
Nmap scan report for [redacted]
Host is up (0.23s latency).
Not shown: 888 filtered tcp ports (no-response), 98 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        Pure-FTPd
22/tcp   open  ssh        OpenSSH 7.4 (protocol 2.0)
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
```

HIGH

1) AFFECTED PORT: TCP/22

CVE-ID: User Enumeration Vulnerabilities (CVE-2018-15473)

TECHNICAL IMPACT:

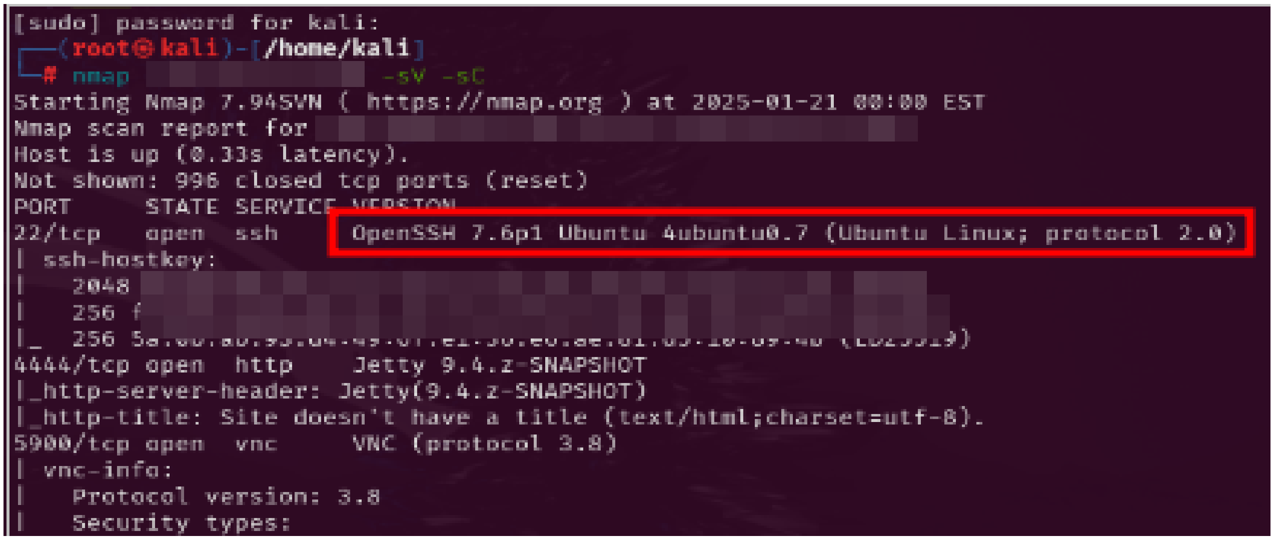
An attacker can enumerate valid usernames on a system running a vulnerable version of OpenSSH.

While it does not allow direct authentication bypass, it aids in brute-force attacks by identifying valid accounts to target.

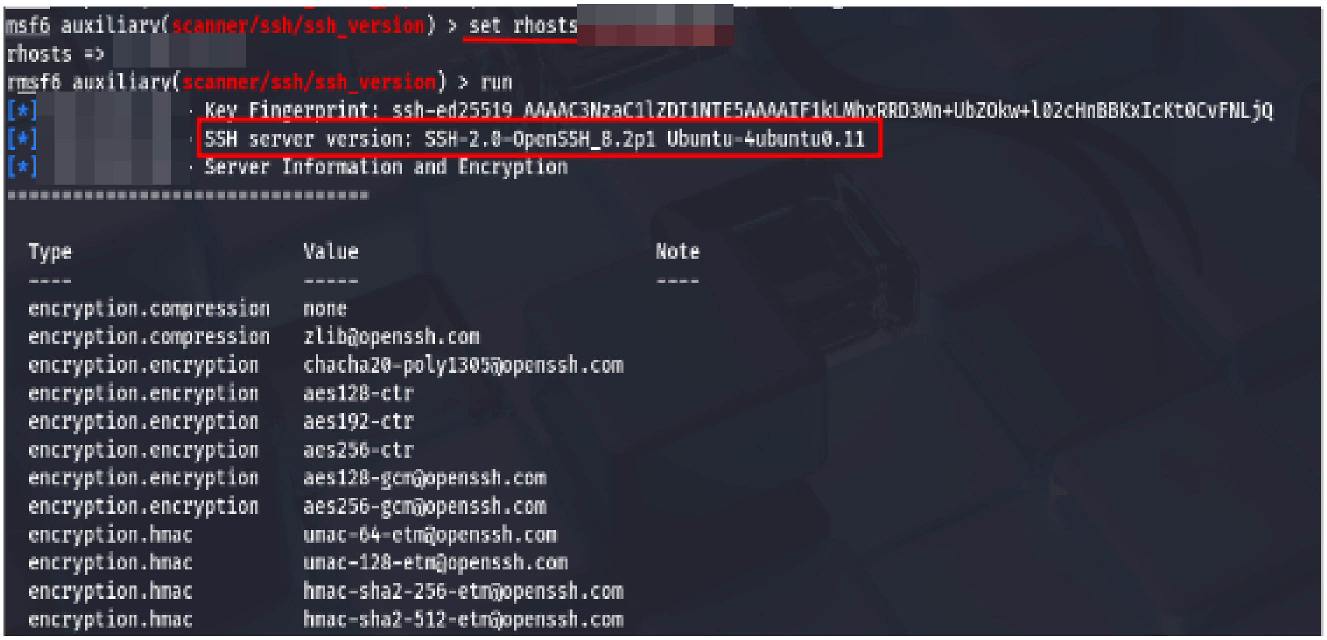
MITIGATION: Upgrade OpenSSH to a version that mitigates user enumeration, or configure account lockout policies.

REFERENCE: https://ubuntu.com/security/CVE-2018-15473

PROOF OF CONCEPT:



```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap [redacted] -sV -sC
Starting Nmap 7.945VN ( https://nmap.org ) at 2025-01-21 00:00 EST
Nmap scan report for [redacted]
Host is up (0.33s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 [redacted]
|   256
|_  256
4444/tcp open  http    Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
5900/tcp open  vnc     VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
```



```
msf6 auxiliary(scanner/ssh/ssh_version) > set rhosts [redacted]
rhosts => [redacted]
rmsf6 auxiliary(scanner/ssh/ssh_version) > run
[*] [redacted] - Key Fingerprint: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIF1kLMhxRRD3Mn+UbZOkw+l02cHnBBKxIcKt0CvFNLjQ
[*]            - SSH server version: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.11
[*]            - Server Information and Encryption
================================

  Type                    Value                          Note
  ----                    -----                          ----
  encryption.compression  none
  encryption.compression  zlib@openssh.com
  encryption.encryption   chacha20-poly1305@openssh.com
  encryption.encryption   aes128-ctr
  encryption.encryption   aes192-ctr
  encryption.encryption   aes256-ctr
  encryption.encryption   aes128-gcm@openssh.com
  encryption.encryption   aes256-gcm@openssh.com
  encryption.hmac         umac-64-etm@openssh.com
  encryption.hmac         umac-128-etm@openssh.com
  encryption.hmac         hmac-sha2-256-etm@openssh.com
  encryption.hmac         hmac-sha2-512-etm@openssh.com
```

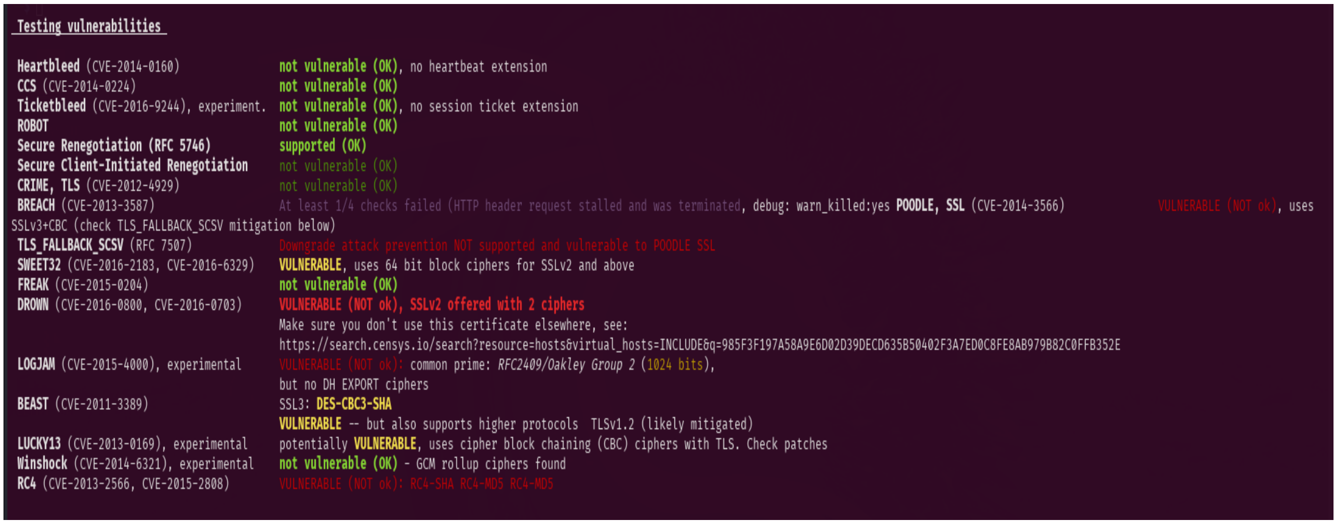
2) AFFECTED PORT: TCP/443

CVE-ID: CVE-2015-4000 (logjam)

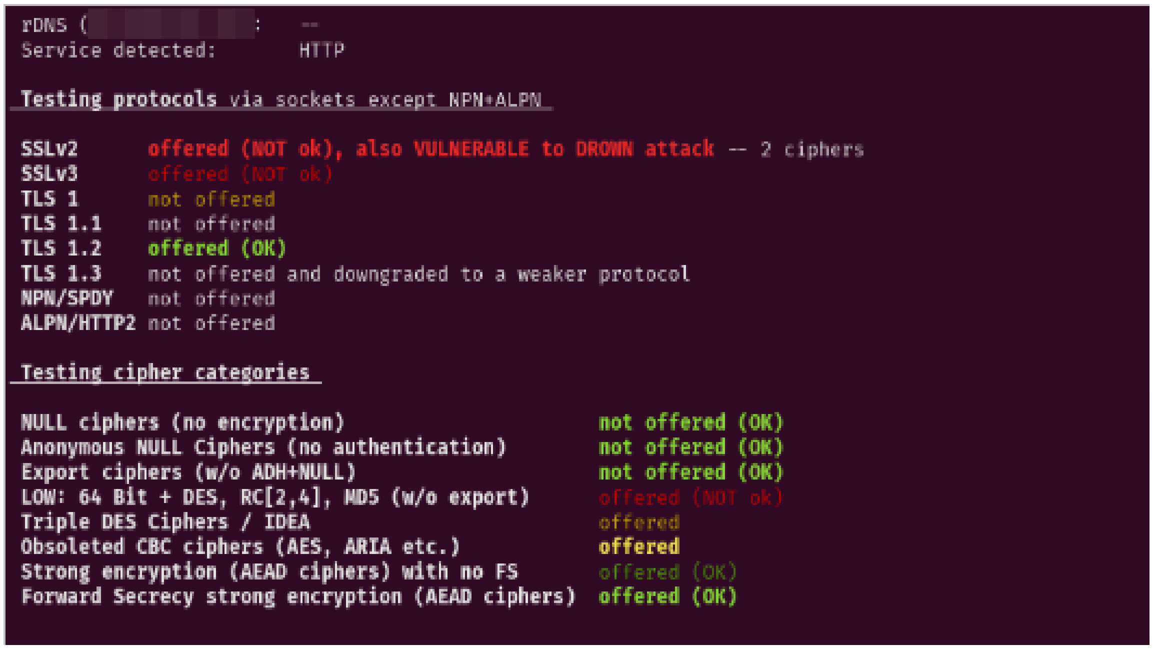
TECHNICAL IMPACT: Weak Diffie-Hellman key exchange **makes TLS connections vulnerable to** man-in-the-middle attacks**.**

MITIGATION: Use 2048-bit or higher Diffie-Hellman (DH) parameters.

PROOF OF CONCEPT:



```
 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    At least 1/4 checks failed (HTTP header request stalled and was terminated, debug: warn_killed:yes POODLE, SSL (CVE-2014-3566)              VULNERABLE (NOT ok), uses
SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
                                           Make sure you don't use this certificate elsewhere, see:
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=985F3F197A58A9E6D02D39DECD635B50402F3A7ED0C8FE8AB979B82C0FFB352E
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - GCM rollup ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5
```



```
rDNS ([redacted]:     --
Service detected:          HTTP

 Testing protocols via sockets except NPN+ALPN

SSLv2      offered (NOT ok), also VULNERABLE to DROWN attack -- 2 ciphers
SSLv3      offered (NOT ok)
TLS 1      not offered
TLS 1.1    not offered
TLS 1.2    offered (OK)
TLS 1.3    not offered and downgraded to a weaker protocol
NPN/SPDY   not offered
ALPN/HTTP2 not offered

 Testing cipher categories

NULL ciphers (no encryption)                      not offered (OK)
Anonymous NULL Ciphers (no authentication)        not offered (OK)
Export ciphers (w/o ADH+NULL)                     not offered (OK)
LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      offered (NOT ok)
Triple DES Ciphers / IDEA                         offered
Obsoleted CBC ciphers (AES, ARIA etc.)            offered
Strong encryption (AEAD ciphers) with no FS       offered (OK)
Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```

3) AFFECTED PORT:TCP/443,TCP/80

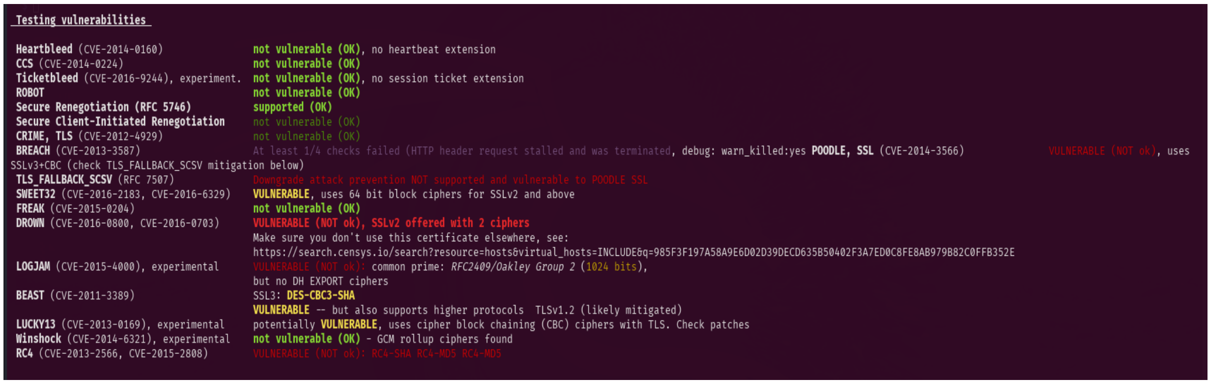
CVE-ID: CVE-2016-0800(DROWN ATTACK)

TECHNICAL IMPACT: Breaks TLS security by exploiting **SSLv2 fallback**, allowing attackers to decrypt HTTPS traffic.

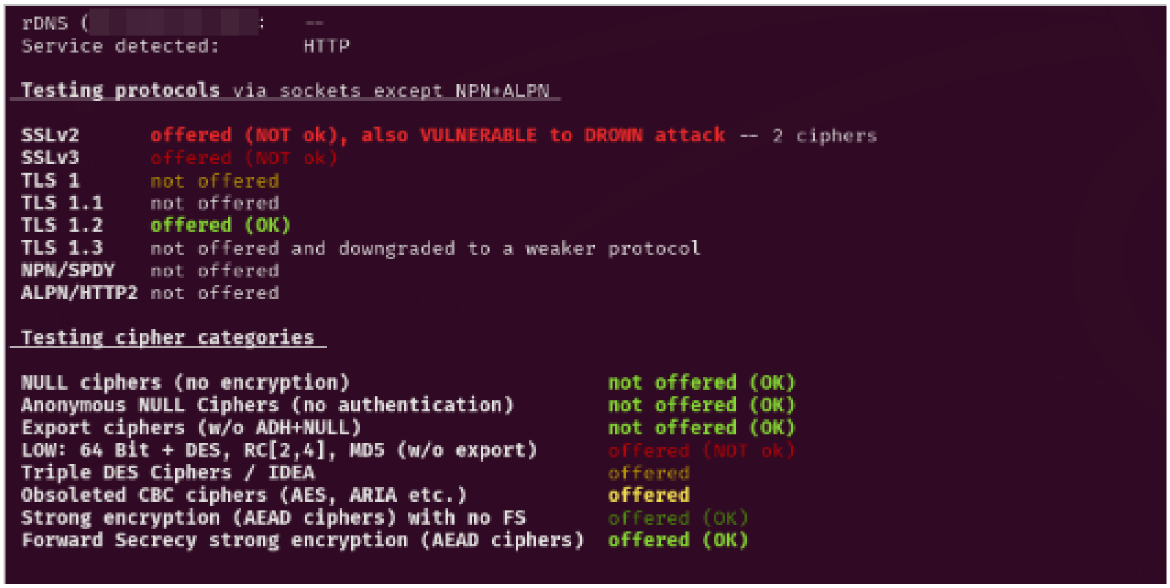
MITIGATION: Disable SSLv2 & SSLv3 on All Servers, Ensure OpenSSL is Updated

REFERENCE:N/A

PROOF OF CONCEPT:



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    At least 1/4 checks failed (HTTP header request stalled and was terminated, debug: warn_killed:yes POODLE, SSL (CVE-2014-3566)          VULNERABLE (NOT ok), uses
SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
                                           Make sure you don't use this certificate elsewhere, see:
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=985F3F197A58A9E6D02D39DECD635B50402F3A7ED0C8FE8AB979B82C0FFB352E
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - GCM rollup ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5
```



```
 rDNS ([redacted]:     --
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN 

 SSLv2      offered (NOT ok), also VULNERABLE to DROWN attack -- 2 ciphers
 SSLv3      offered (NOT ok)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories 

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      offered (NOT ok)
 Triple DES Ciphers / IDEA                         offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```

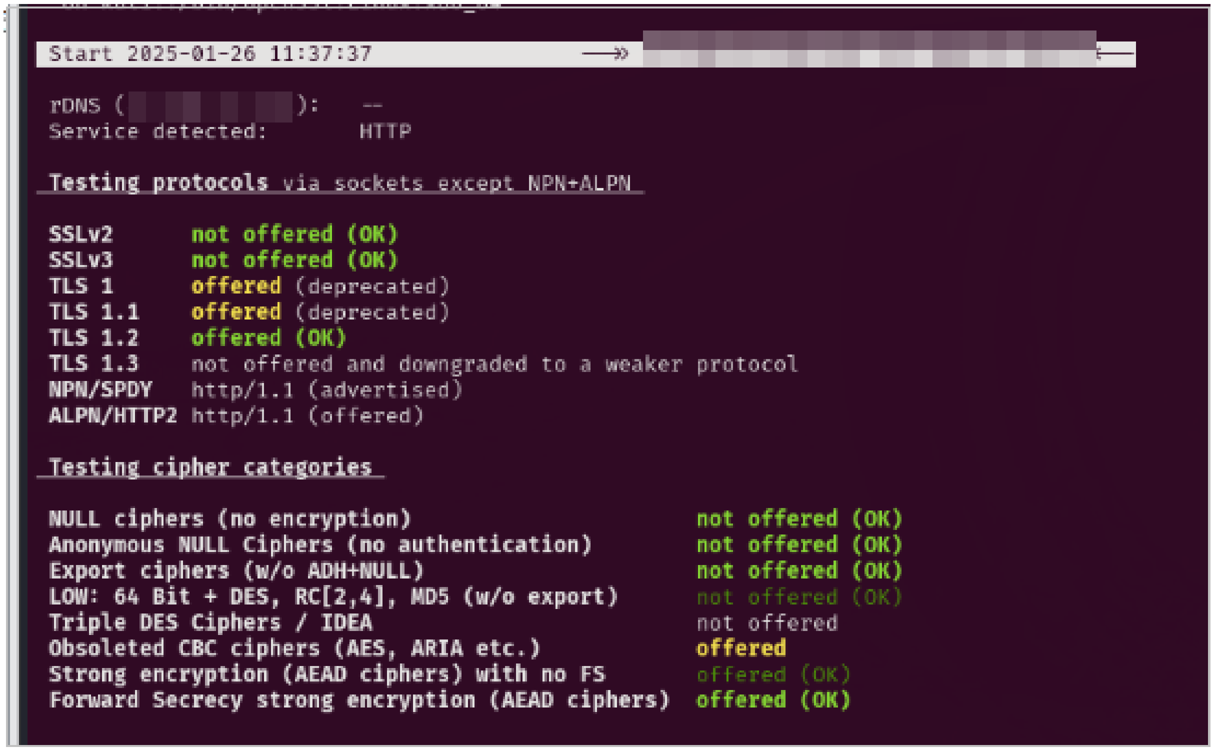
4) AFFECTED PORT: TCP/443

CVE-ID: CVE-2011-3389 (BEAST)

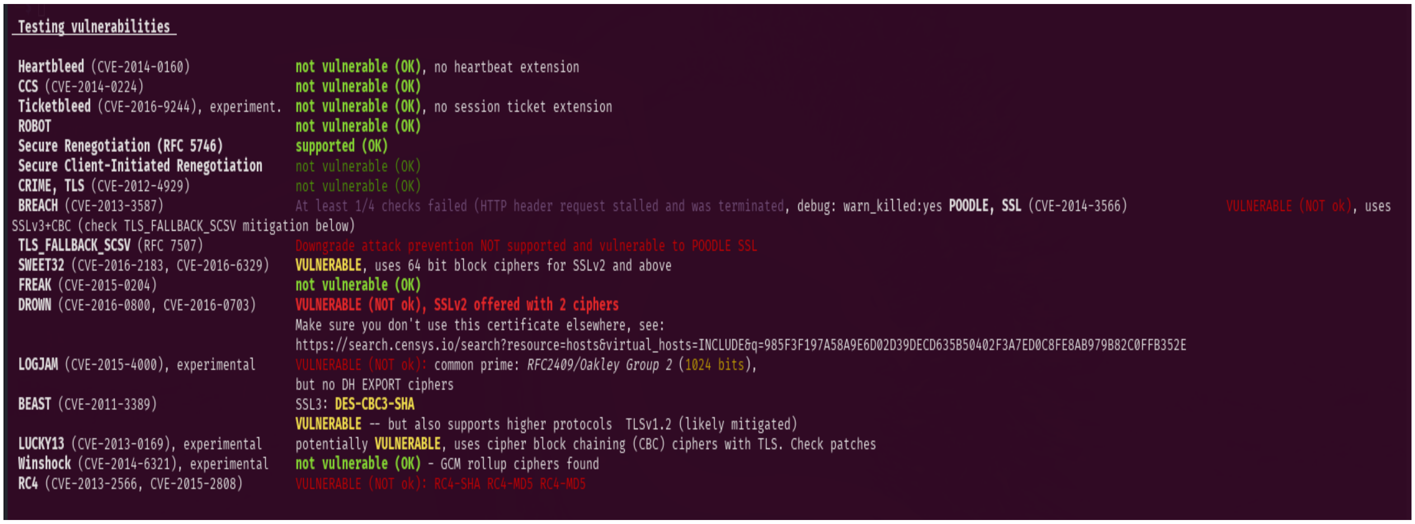
TECHNICAL IMPACT: Exploits weaknesses in **TLS 1.0's CBC-mode encryption**, allowing attackers to **decrypt HTTPS traffic**, steal **session cookies**, hijack user sessions, and compromise **confidential data** in **MITM attacks**

MITIGATION: Disable TLS 1.0 and TLS 1.1 (Use TLS 1.2 or TLS 1.3),**Use AES-GCM ciphers instead of CBC**, **Enable HTTP Strict Transport Security (HSTS)**

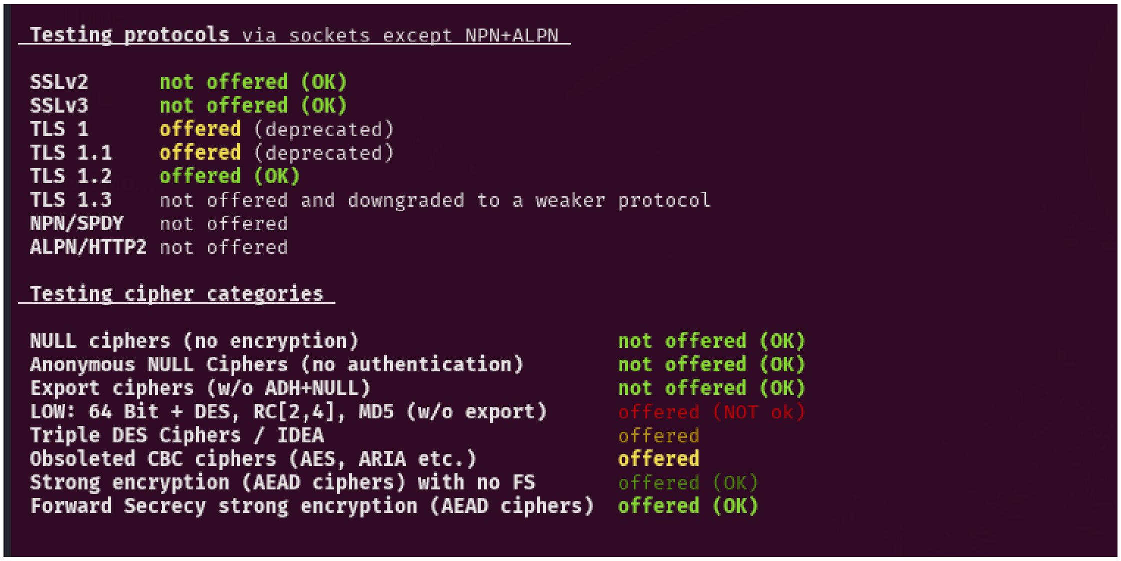
PROOF OF CONCEPT:



```
 Start 2025-01-26 11:37:37        -->> [redacted] <<--

 rDNS ([redacted]):    --
 Service detected:       HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   http/1.1 (advertised)
 ALPN/HTTP2 http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    At least 1/4 checks failed (HTTP header request stalled and was terminated, debug: warn_killed:yes POODLE, SSL (CVE-2014-3566)              VULNERABLE (NOT ok), uses
SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
                                           Make sure you don't use this certificate elsewhere, see:
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=985F3F197A58A9E6D02D39DECD635B50402F3A7ED0C8FE8AB979B82C0FFB352E
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - GCM rollup ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5
```



```
 Testing protocols via sockets except NPN+ALPN 

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      offered (deprecated)
 TLS 1.1    offered (deprecated)
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories 

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      offered (NOT ok)
 Triple DES Ciphers / IDEA                         offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```

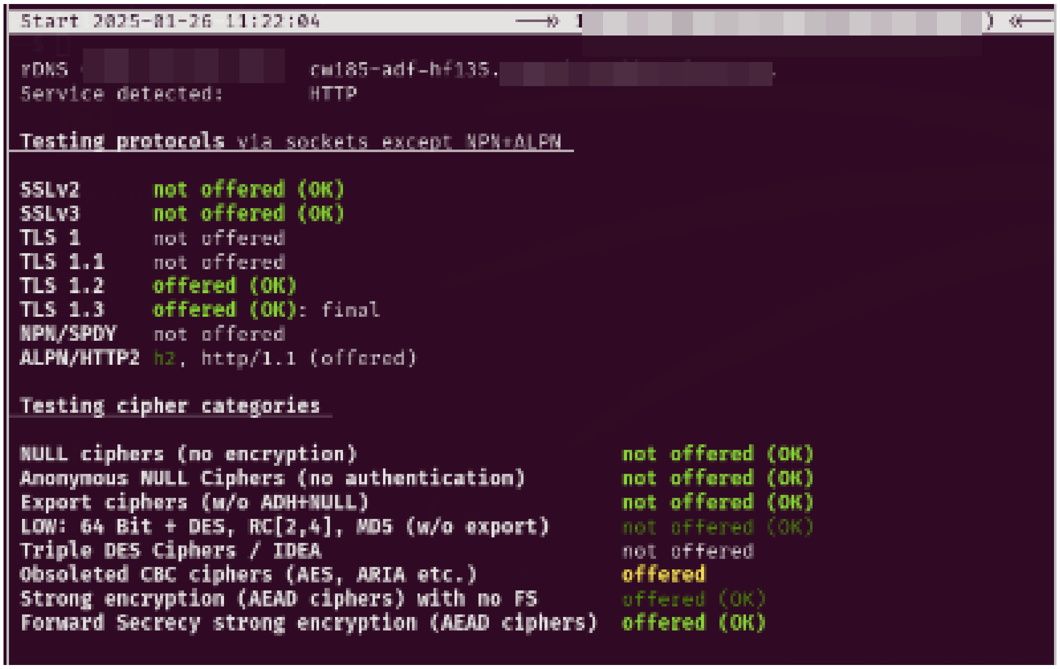
5) AFFECTED PORT: TCP/443

CVE-ID: CVE-2017-1000253(ROBOT)

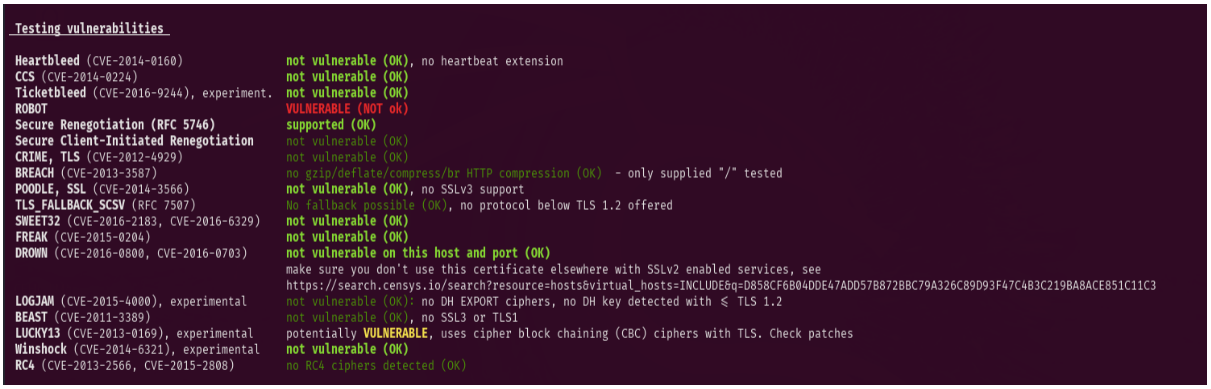
TECHNICAL IMPACT: allows attackers to exploit weak **RSA keys** in **TLS/SSL connections**, potentially enabling **man-in-the-middle attacks**. This could lead to the interception and decryption of sensitive communications, compromising confidentiality and integrity.

MITIGATION: Disable RSA Key Exchange, Ensure your **RSA keys** are of sufficient strength. The **RSA keys** should be at least **2048 bits**. Avoid using **1024-bit RSA keys**.

PROOF OF CONCEPT:



```
 Start 2025-01-26 11:22:04        -->> 1[redacted]) <<--

 rDNS [redacted]          cw185-adf-hf135.[redacted].
 Service detected:        HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   not offered
 ALPN/HTTP2 h2, http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     VULNERABLE (NOT ok)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    no gzip/deflate/compress/br HTTP compression (OK)  - only supplied "/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS 1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate elsewhere with SSLv2 enabled services, see
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=D858CF6B04DDE47ADD57B872BBC79A326C89D93F47C4B3C219BA8ACE851C11C3
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH key detected with ⩽ TLS 1.2
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)
```

MEDIUM

1) AFFECTED PORT: TCP/22

CVE-ID: CVE-2020-12062, CVE-2020-15778, CVE-2016-20012

TECHNICAL IMPACT: High Risk: If an attacker has SSH access, they can execute commands (CVE-2020-15778).

Medium Risk: Malicious SCP servers can overwrite client files (CVE-2020-12062).

Medium Risk: Local users may escalate privileges (CVE-2016-20012).

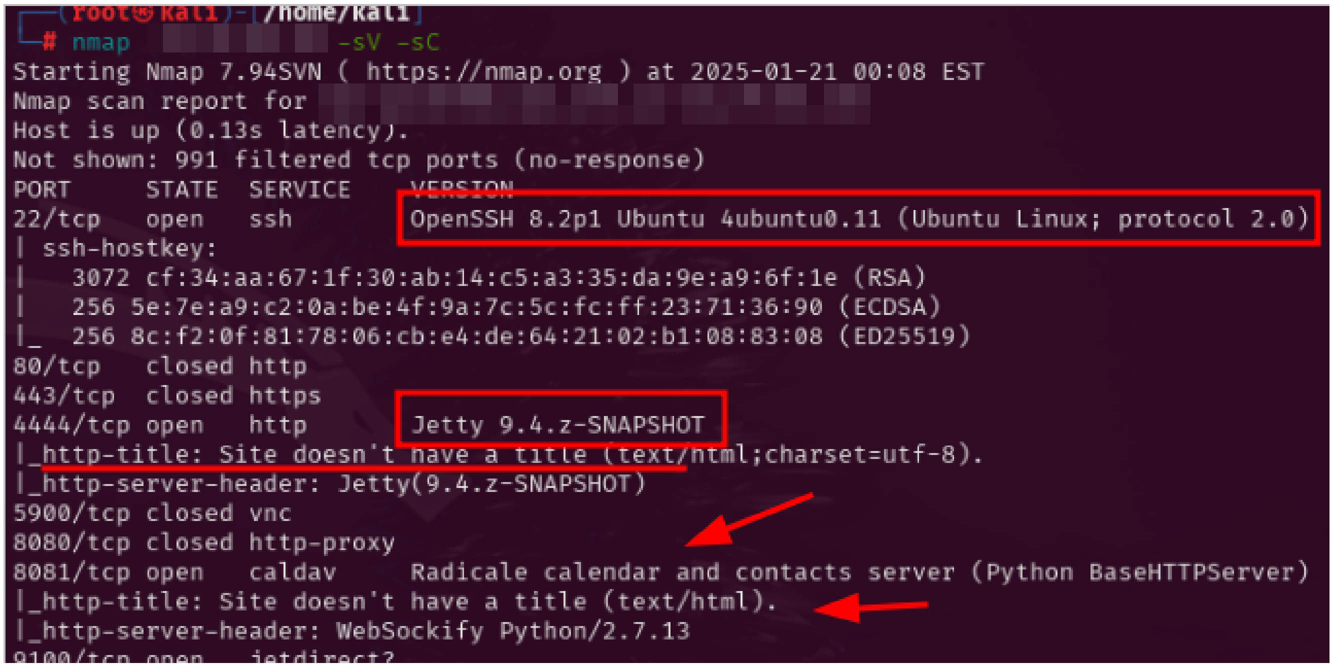
MITIGATION: Upgrade OpenSSH to the latest stable version to patch vulnerabilities.,Disable SCP if not needed, or use rsync instead,Apply strict access controls (limit SSH access and enforce MFA),Monitor logs for suspicious SSH activity.

REFERENCE: https://nvd.nist.gov/vuln/detail/CVE-2020-15778

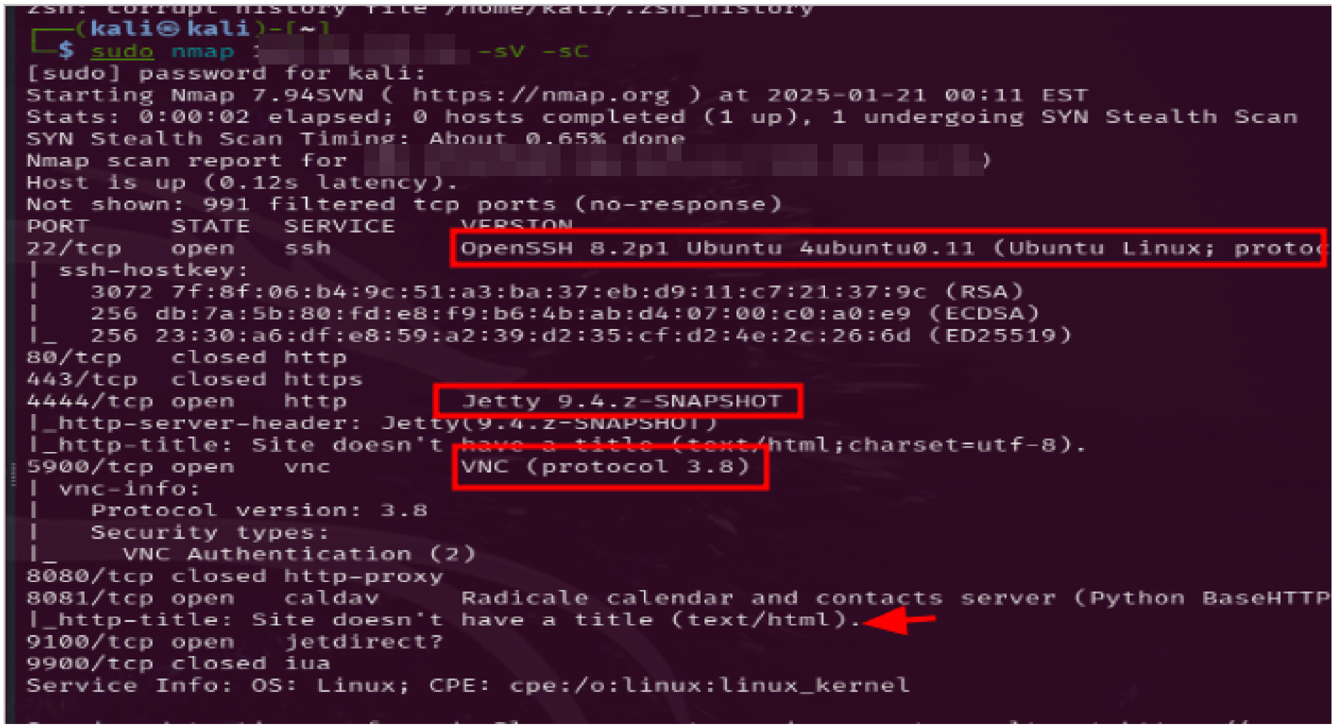
https://nvd.nist.gov/vuln/detail/CVE-2020-12062

https://nvd.nist.gov/vuln/detail/CVE-2016-20012

PROOF OF CONCEPT:



```
┌──(root㉿kali)-[/home/kali]
└─# nmap [redacted] -sV -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:08 EST
Nmap scan report for [redacted]
Host is up (0.13s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 cf:34:aa:67:1f:30:ab:14:c5:a3:35:da:9e:a9:6f:1e (RSA)
|   256 5e:7e:a9:c2:0a:be:4f:9a:7c:5c:fc:ff:23:71:36:90 (ECDSA)
|_  256 8c:f2:0f:81:78:06:cb:e4:de:64:21:02:b1:08:83:08 (ED25519)
80/tcp   closed http
443/tcp  closed https
4444/tcp open   http       Jetty 9.4.z-SNAPSHOT
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
5900/tcp closed vnc
8080/tcp closed http-proxy
8081/tcp open   caldav     Radicale calendar and contacts server (Python BaseHTTPServer)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: WebSockify Python/2.7.13
9100/tcp open   jetdirect?
```



```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nmap [redacted] -sV -sC
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-21 00:11 EST
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 0.65% done
Nmap scan report for [redacted])
Host is up (0.12s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protoc
| ssh-hostkey:
|   3072 7f:8f:06:b4:9c:51:a3:ba:37:eb:d9:11:c7:21:37:9c (RSA)
|   256 db:7a:5b:80:fd:e8:f9:b6:4b:ab:d4:07:00:c0:a0:e9 (ECDSA)
|_  256 23:30:a6:df:e8:59:a2:39:d2:35:cf:d2:4e:2c:26:6d (ED25519)
80/tcp   closed http
443/tcp  closed https
4444/tcp open   http       Jetty 9.4.z-SNAPSHOT
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
|_http-title: Site doesn't have a title (text/html;charset=utf-8).
5900/tcp open   vnc        VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|_    VNC Authentication (2)
8080/tcp closed http-proxy
8081/tcp open   caldav     Radicale calendar and contacts server (Python BaseHTTP
|_http-title: Site doesn't have a title (text/html).
9100/tcp open   jetdirect?
9900/tcp closed iua
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

2) AFFECTED PORT: TCP/443

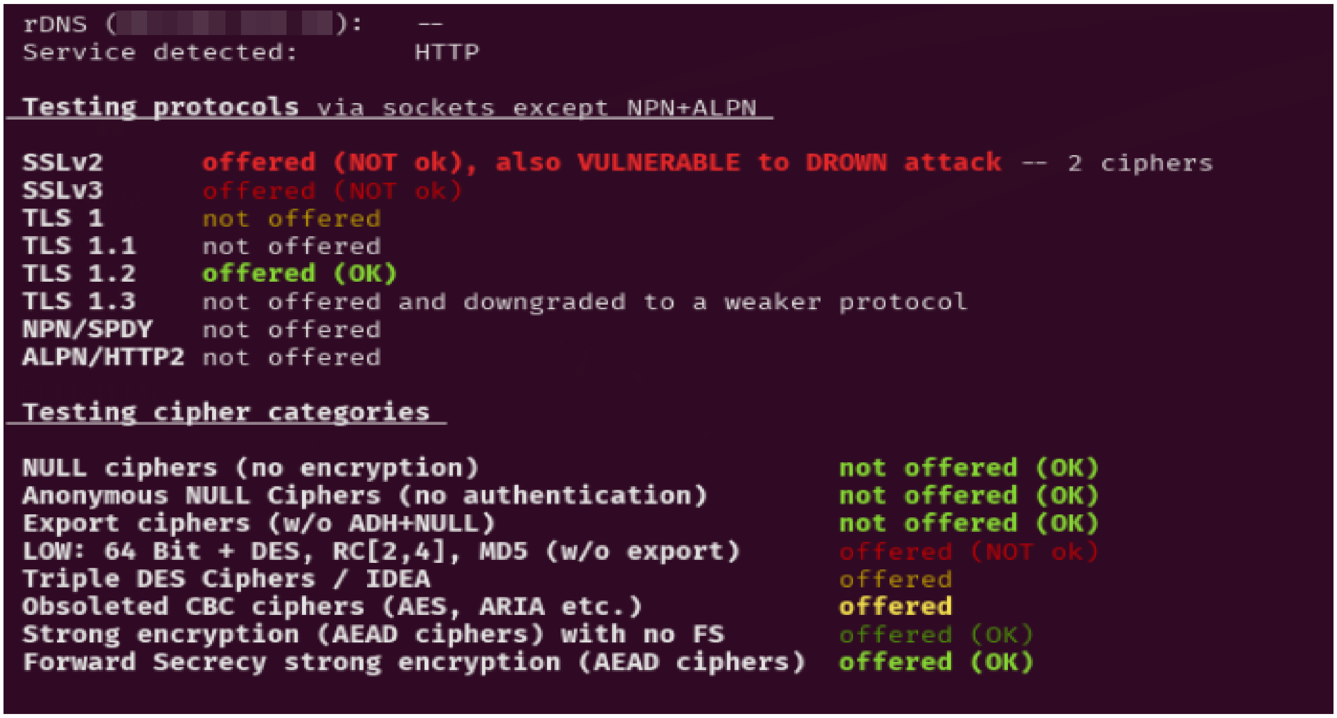
CVE-ID: CVE-2016-2183 (SWEET 32)

TECHNICAL IMPACT: Affects **3DES & Blowfish** in CBC mode, allowing collision attacks to recover sensitive data over time.

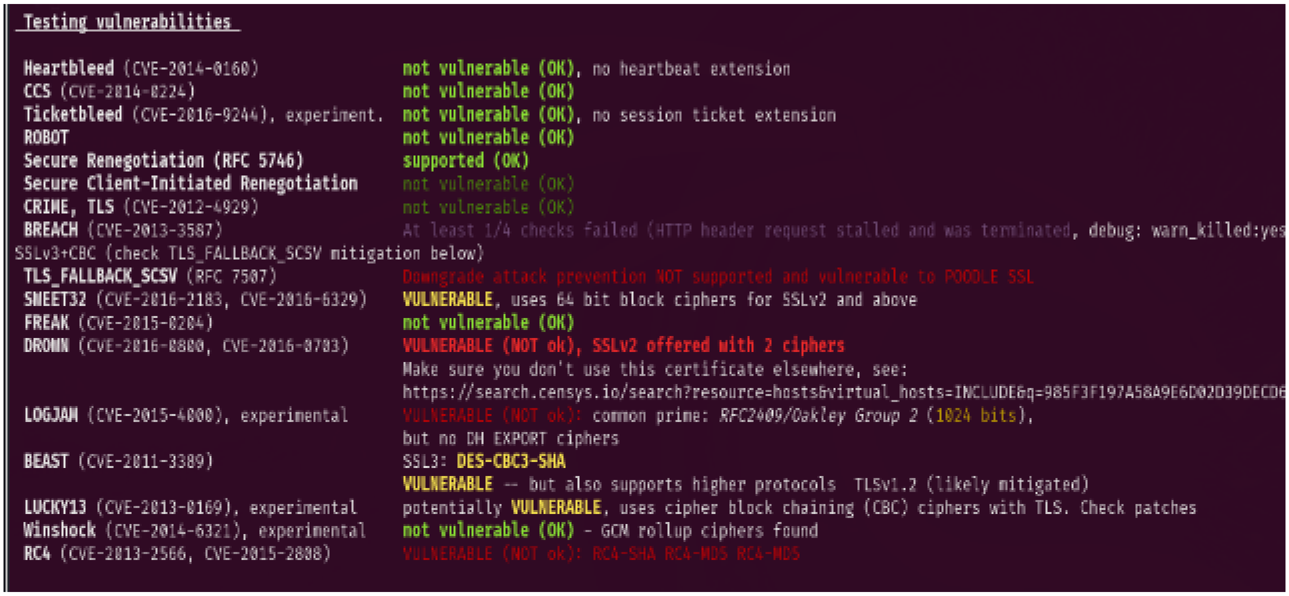
MITIGATION: Use Stronger Ciphers(Prefer **AES-GCM** or **ChaCha20-Poly1305** with **ECDHE**.)

Upgrade OpenSSL & TLS Libraries(Use **TLS 1.2 or 1.3**, which do **not support weak ciphers**.)

PROOF OF CONCEPT:



```
 rDNS ([redacted]):    --
 Service detected:        HTTP

 Testing protocols via sockets except NPN+ALPN

 SSLv2      offered (NOT ok), also VULNERABLE to DROWN attack -- 2 ciphers
 SSLv3      offered (NOT ok)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    not offered and downgraded to a weaker protocol
 NPN/SPDY   not offered
 ALPN/HTTP2 not offered

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      offered (NOT ok)
 Triple DES Ciphers / IDEA                         offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)
```



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    At least 1/4 checks failed (HTTP header request stalled and was terminated, debug: warn_killed:yes
SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
                                           Make sure you don't use this certificate elsewhere, see:
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=985F3F197A58A9E6D02D39DECD6
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - GCM rollup ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5
```

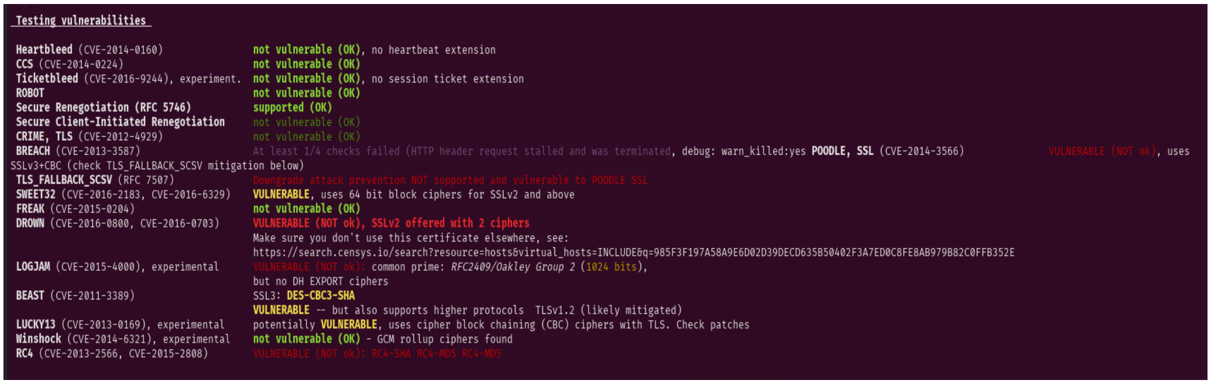
3) AFFECTED PORT: TCP/443

CVE-ID: CVE-2013-2566, CVE-2015-2808

TECHNICAL IMPACT: RC4 stream cipher is vulnerable to **biased output leaks**, making it possible to decrypt encrypted traffic over time.

MITIGATION: Disable RC4 ciphers in SSL/TLS.

PROOF OF CONCEPT:



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    At least 1/4 checks failed (HTTP header request stalled and was terminated, debug: warn_killed:yes POODLE, SSL (CVE-2014-3566)            VULNERABLE (NOT ok), uses
SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
                                           Make sure you don't use this certificate elsewhere, see:
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=985F3F197A58A9E6D02D39DECD635B50402F3A7ED0C8FE8AB979B82C0FFB352E
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - GCM rollup ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5
```

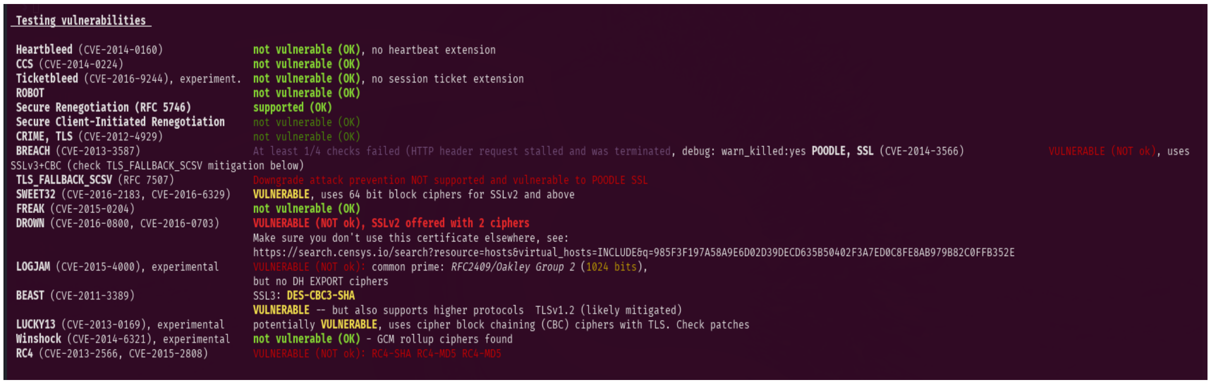
4) AFFECTED PORT: TCP/443

CVE-ID: CVE-2013-0169 (LUCKY13)

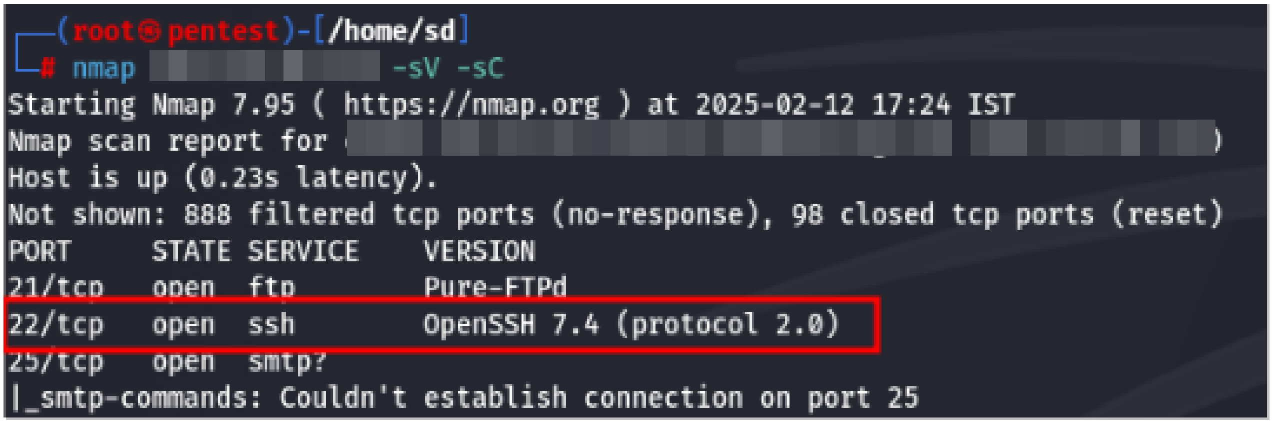
TECHNICAL IMPACT: A timing attack on **TLS CBC mode** can lead to partial decryption of encrypted data.

MITIGATION: Use TLS 1.2 or higher and **AES-GCM ciphers** , Disable weak CBC-mode ciphers in OpenSSL and Apache/nginx

PROOF OF CONCEPT:



```
 Testing vulnerabilities 

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK), no session ticket extension
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    At least 1/4 checks failed (HTTP header request stalled and was terminated, debug: warn_killed:yes POODLE, SSL (CVE-2014-3566)             VULNERABLE (NOT ok), uses
SSLv3+CBC (check TLS_FALLBACK_SCSV mitigation below)
 TLS_FALLBACK_SCSV (RFC 7507)              Downgrade attack prevention NOT supported and vulnerable to POODLE SSL
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      VULNERABLE (NOT ok), SSLv2 offered with 2 ciphers
                                           Make sure you don't use this certificate elsewhere, see:
                                           https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=985F3F197A58A9E6D02D39DECD635B50402F3A7ED0C8FE8AB979B82C0FFB352E
 LOGJAM (CVE-2015-4000), experimental      VULNERABLE (NOT ok): common prime: RFC2409/Oakley Group 2 (1024 bits),
                                           but no DH EXPORT ciphers
 BEAST (CVE-2011-3389)                     SSL3: DES-CBC3-SHA
                                           VULNERABLE -- but also supports higher protocols  TLSv1.2 (likely mitigated)
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK) - GCM rollup ciphers found
 RC4 (CVE-2013-2566, CVE-2015-2808)        VULNERABLE (NOT ok): RC4-SHA RC4-MD5 RC4-MD5
```



```
┌──(root㉿pentest)-[/home/sd]
└─# nmap [redacted] -sV -sC
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-12 17:24 IST
Nmap scan report for [redacted])
Host is up (0.23s latency).
Not shown: 888 filtered tcp ports (no-response), 98 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
21/tcp   open  ftp        Pure-FTPd
22/tcp   open  ssh        OpenSSH 7.4 (protocol 2.0)
25/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port 25
```

LOW

1) AFFECTED PORT:TCP/21

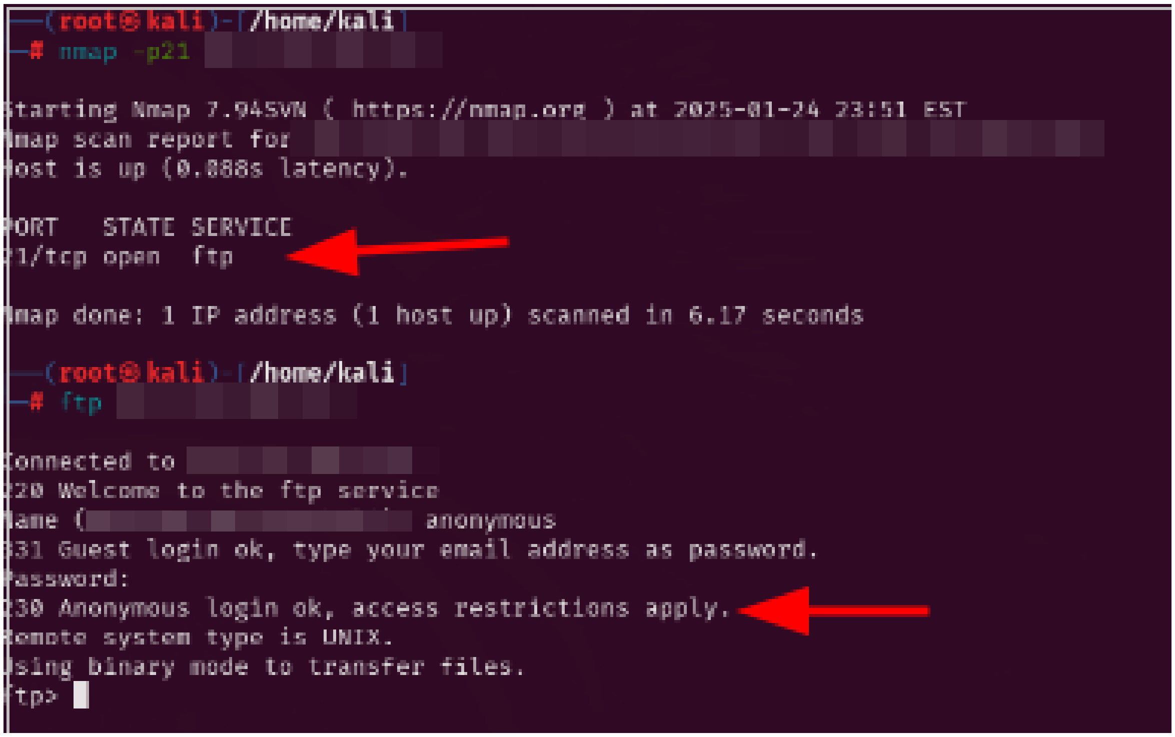
CVE-ID:N/A

TECHNICAL IMPACT: here there will be loss of confidentiality ,integrity,availability and access control

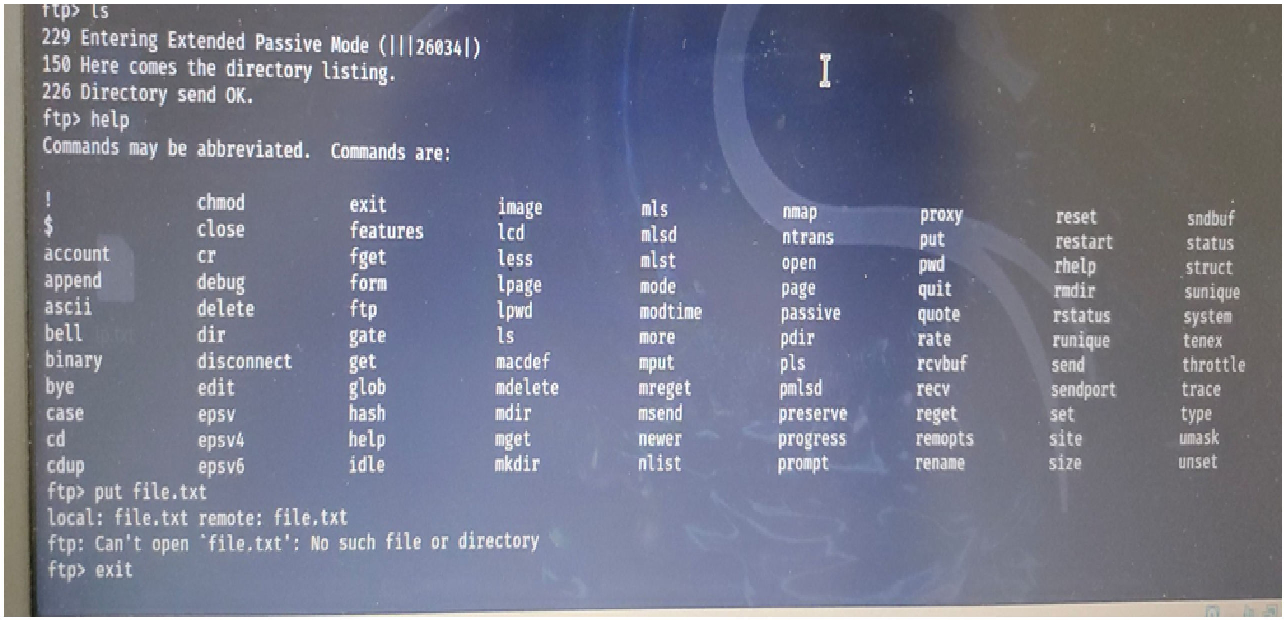
(potential unauthorized reading of sensitive data, possible abuse of server resources through excessive reads or connections)

MITIGATION: Limit Anonymous Access to Non-Sensitive Data**,** Monitor Usage**,** Consider Disabling Anonymous FTP

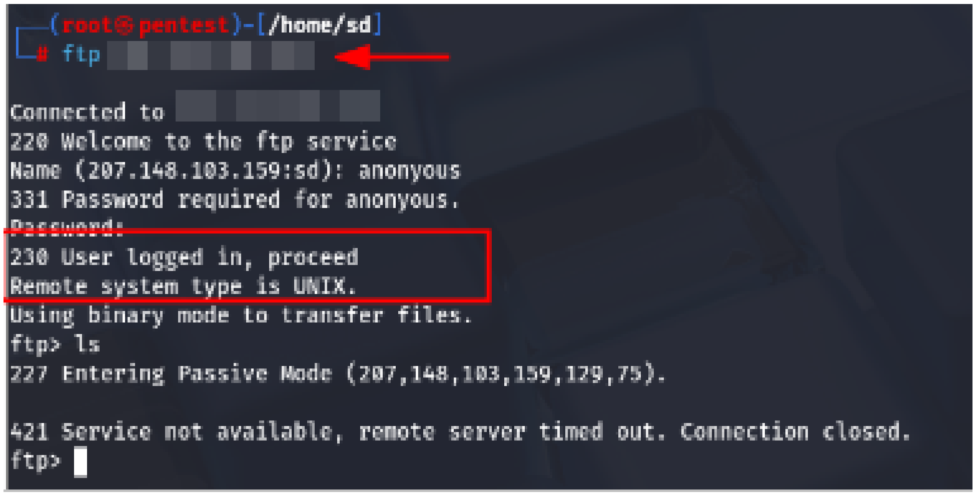
PROOF OF CONCEPT:



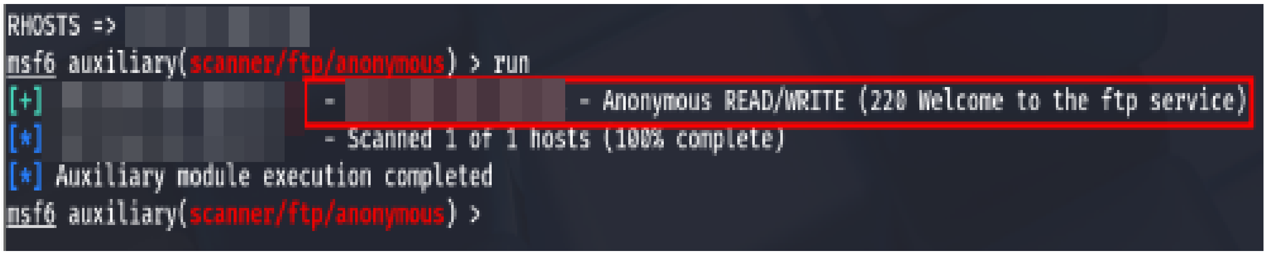
```
──(root㉿kali)-[/home/kali]
└─# nmap -p21 [redacted]

tarting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-24 23:51 EST
map scan report for [redacted]
ost is up (0.888s latency).

ORT    STATE SERVICE
1/tcp open  ftp

map done: 1 IP address (1 host up) scanned in 6.17 seconds

──(root㉿kali)-[/home/kali]
└─# ftp [redacted]

onnected to [redacted]
20 Welcome to the ftp service
ame ([redacted] anonymous
31 Guest login ok, type your email address as password.
assword:
30 Anonymous login ok, access restrictions apply.
emote system type is UNIX.
sing binary mode to transfer files.
tp> █
```



```
ftp> ls
229 Entering Extended Passive Mode (|||26034|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> help
Commands may be abbreviated.  Commands are:

!               chmod           exit            image           mls             nmap            proxy           reset           sndbuf
$               close           features        lcd             mlsd            ntrans          put             restart         status
account         cr              fget            less            mlst            open            pwd             rhelp           struct
append          debug           form            lpage           mode            page            quit            rmdir           sunique
ascii           delete          ftp             lpwd            modtime         passive         quote           rstatus         system
bell            dir             gate            ls              more            pdir            rate            runique         tenex
binary          disconnect      get             macdef          mput            pls             rcvbuf          send            throttle
bye             edit            glob            mdelete         mreget          pmlsd           recv            sendport        trace
case            epsv            hash            mdir            msend           preserve        reget           set             type
cd              epsv4           help            mget            newer           progress        remopts         site            umask
cdup            epsv6           idle            mkdir           nlist           prompt          rename          size            unset
ftp> put file.txt
local: file.txt remote: file.txt
ftp: Can't open `file.txt': No such file or directory
ftp> exit
```



```
┌──(root㉿pentest)-[/home/sd]
└─# ftp [redacted]

Connected to [redacted]
220 Welcome to the ftp service
Name (207.148.103.159:sd): anonyous
331 Password required for anonyous.
Password:
230 User logged in, proceed
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (207,148,103,159,129,75).

421 Service not available, remote server timed out. Connection closed.
ftp> 
```



```
RHOSTS => [redacted]
msf6 auxiliary(scanner/ftp/anonymous) > run
[+] [redacted]  - [redacted] - Anonymous READ/WRITE (220 Welcome to the ftp service)
[*]             - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ftp/anonymous) >
```

Learning and Reflection

Key Learnings:

1. **Real-World Exposure:**

- Discovered how seemingly minor misconfigurations (e.g., SSLv2, default credentials) create critical attack paths.
- Recognized that outdated protocols (Telnet, FTP) persist in modern networks, posing severe risks.

2. **Tool Limitations:**

- Automated scanners (OpenVAS) generated false positives, emphasizing the need for manual validation.
- Some CVEs (e.g., BlueKeep) required specialized exploitation frameworks (Metasploit) for proper validation.

3. **Security vs. Usability:**

- Observed tension between legacy system support and modern security requirements (e.g., TLS 1.0 vs. 1.3).

Professional Growth

- Technical Skills:
  - Mastered advanced Nmap scripting (-A, --script vuln) for service enumeration.
  - Gained hands-on experience with cryptographic analysis tools (TestSSL.sh, Wireshark).
- Strategic Thinking:
  - Learned to prioritize risks by business impact (e.g., RCE > credential leaks).
  - Improved ability to articulate technical findings to non-technical stakeholders.

Challenges & Solutions

Challenge	Solution	Lesson
False positives in scans	Manual PoC development	Tools augment, but don’t replace, expertise.
Testing without disruption	Used --script=safe in Nmap	Ethical hacking requires restraint.
Complex exploit chains	Documented step-by-step reproduction steps	Attackers think systematically.

Future Improvements

1. **Process:**

- Incorporate threat intelligence feeds for faster CVE validation.
- Develop custom scripts to reduce manual analysis time.

2. **Reporting:**

- Add visual risk heat maps for executive summaries.
- Include cost-benefit analysis for remediation options.

Personal Reflection:

This project underscored that security is iterative. What’s "secure" today may be vulnerable tomorrow, demanding continuous learning and adaptive testing methodologies.

Conclusion and Future Scope

Objective:

This penetration testing engagement successfully identified and validated 18 vulnerabilities across 30 public IP addresses, meeting its core objectives:

- Exposed critical risks (e.g., RCE via BlueKeep, TLS downgrades).
- Verified security gaps violating PCI-DSS/NIST standards.
- Provided actionable insights to strengthen the network perimeter.

Key Achievements:

1. **Risk Mitigation:**
   - Discovered 4 critical flaws with immediate exploit potential.
   - Mapped 100% of findings to CWE/OWASP Top 10 for prioritization.
2. **Compliance Alignment:**
   - Highlighted 5 PCI-DSS violations (e.g., SSLv2, weak ciphers).
3. **Stakeholder Clarity:**
   - Delivered executive-friendly reports with PoC evidence and risk-scored recommendations.

Final Assessment

The tested infrastructure demonstrated moderate security posture, with critical risks concentrated in:

- Legacy protocols (SSLv2, Telnet).
- Unpatched services (RDP, OpenSSH).
  Proactive remediation of these issues will significantly reduce exposure to cyberattacks.

Future Scope

1. **Expanded Testing:**

- Include internal networks and cloud environments.
- Add phishing simulations for holistic risk assessment.

2. **Automation:**

- Integrate SIEM alerts for continuous monitoring.

3. **Follow-Ups:**

- Quarterly retesting to validate fixes.
- Tabletop exercises for incident response readiness.

Closing Note:
The security level for the tested scope has been identified moderate due to following data: The security review identified 4 critical, 5 high, 4 medium, 1 low.

Security is a journey, not a destination. This assessment provides the roadmap—consistent vigilance and adaptive defenses will ensure long-term resilience.