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

COMPREHENSIVE VAPT ANALYSIS ON NETWORK INFRASTRUCTURE

The domain of the Project

Cybersecurity - Network and Web Application Security

Under the guidance of

Mr. Nishchay Gaba (Penetration Tester)

By

Mr. Deepak Mandavi (B.Tech)

Period of the project

December 2024 to June 2025

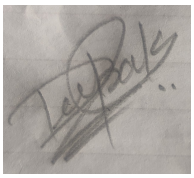
SURE TRUST
PUTTAPARTHI, ANDHRA PRADESH

DECLARATION

The project titled ***"Comprehensive VAPT Analysis on Network Infrastructure"*** has been mentored by **Mr. Nishchay Gaba** and organized by SURE Trust from December 2024 to June 2025 This initiative aims to benefit educated unemployed rural youth by providing hands-on experience in industry-relevant projects, thereby enhancing employability.

I, **Mr. Deepak Mandavi,** 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
Mr. Deepak Mandavi



Signature

Mr. Nishchay Gaba
Mentor

Signature

Seal & Signature

Prof.Radhakumari
Executive Director & Founder

List Of Contents

1. Documentation Governance

a. Confidentiality Statement

This document contains sensitive information regarding the security posture of the assessed network. It is intended solely for the use of authorized personnel. Unauthorized access, disclosure, or distribution of this document is strictly prohibited. All recipients are required to maintain the confidentiality of the information contained herein.

2. Liability Disclaimer

The information provided in this report is based on the findings from the assessment conducted on the specified date. The authors of this report make no representations or warranties regarding the accuracy, completeness, or reliability of the information contained herein. The organization shall not be liable for any damages arising from the use of this report or the information contained within it.

3. Project Overview

a. Assessment Goals

The primary objective of this VAPT is to identify vulnerabilities within the network infrastructure that could be exploited by malicious actors. The assessment aims to provide actionable recommendations to enhance the security posture of the organization.

b. Coverage of Security Review

The assessment encompasses the following:

1. All IP addresses and associated open ports identified during the scanning process.
2. Services running on the identified ports.
3. Vulnerabilities associated with the services and configurations.

Devices	Total IP's
Public IP's	27

Table 1 - Scop List

c. Testing Constraints

The assessment depends on provided data, excluding physical security and social engineering. Time, scope, and dynamic network changes constrain findings. It may not detect all vulnerabilities, potentially including false positives or negatives, and is bound by legal and ethical guidelines.

4. Key Finding Summary

a. Findings Overview

The security assessment report outlines several vulnerabilities in network infrastructure. Critical risks include an unsupported Windows 7 OS and the BlueKeep RDP vulnerability, both allowing potential remote code execution. High severity issues encompass default credentials on Telnet and FTP, RDP misconfigurations without Network Level Authentication, and open ports on web servers potentially leading to unauthorized access and data exposure. Medium risks involve outdated software (PHP, VNC), default SNMP community strings, and misconfigured SNMP settings, risking information leakage. Mitigation strategies include immediate system updates, changing default credentials, enforcing secure configurations, and restricting access to sensitive services to prevent exploitation.

5. Scope of security assessment

Each finding has been assigned a severity rating of CRITICAL, HIGH, MEDIUM, LOW. The rating is based on an assessment of the priority with which each finding should be viewed and the potential impact each has on the confidentiality, integrity, and availability of the Client's data.

Severity	Definition
Critical **9.0 - 10.0**	Vulnerabilities that score in the critical range usually have most of the following characteristics: • Exploitation of the vulnerability likely results in root-level compromise of servers or infrastructure devices. • Exploitation is usually straightforward, in the sense that the attacker does not need any special authentication credentials or knowledge about individual victims, and does not need to persuade a target user, for example via social engineering, into performing any special functions. • It is advised that you patch or upgrade as soon as possible, unless you have other mitigating measures in place
High **7.0 - 8.9**	Vulnerabilities that score in the high range usually have some of the following characteristics: • The vulnerability is difficult to exploit. • Exploitation could result in elevated privileges. • Exploitation could result in a significant data loss or downtime
Medium **4.0 - 6.9**	Vulnerabilities that score in the medium range usually have some of the following characteristics: • Vulnerabilities that require the attacker to manipulate individual victims via social engineering tactics. • Denial of service vulnerabilities that are difficult to set up. • Exploits that require an attacker to reside on the same local network as the victim. • Vulnerabilities where exploitation provides only very limited access. • Vulnerabilities that require user privileges for successful exploitation.
Low **0.1 - 3.9**	Vulnerabilities in the low range typically have very little impact on an organization's business. Exploitation of such vulnerabilities usually requires local or physical system access. Vulnerabilities in third party code that are unreachable from Atlassian code may be downgraded to low severity.

Table 2. Risk Impact Definition

6. Methodology

Black Box Assessment - A Black-box penetration test is a penetration testing service that aims to find & exploit vulnerabilities in a system as an outsider. The security expert is provided with no information about the target system prior to the testing except the target URL and access similar to an end-user. This means the tester has no access to source code (other than publicly available code), internal data, structure & design of the application before the testing.

7. PUBLIC IP

FORMAT:

Vulnerability Name:

Definitation

CVSS:

Affected IPs:

Affected Port:

CVE-ID:

Technical Impact:

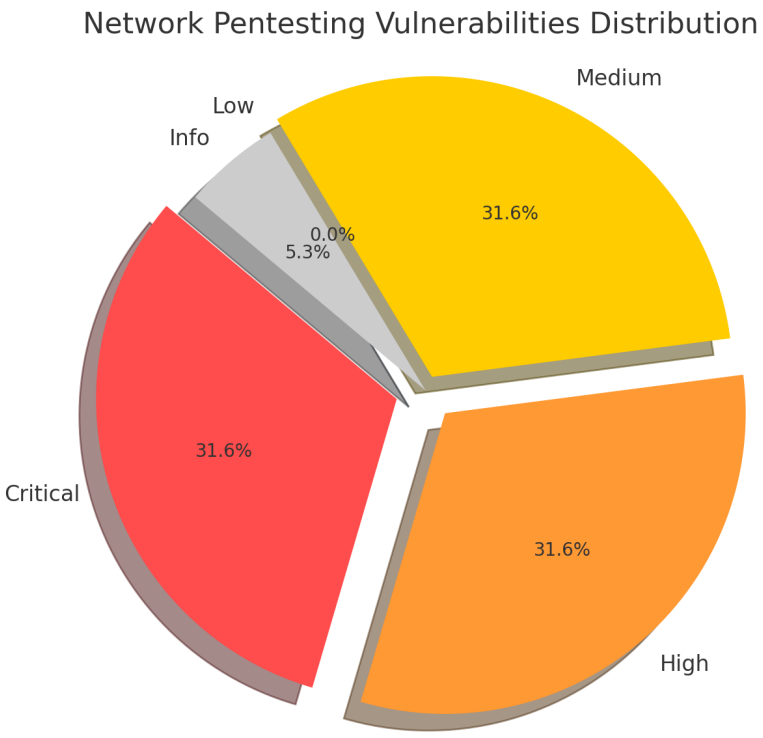
Mitigation:

Reference:

POC:

PUBLIC IPS

Executive Summary




Critical

1. VulnerabilityName:PlaintextTelnetCommunication

Definitation: A Telnet service is running that allows cleartext logins. It does not use any form of encryption, making it vulnerable to credential interception.

CVSSScore:9.8 (Critical)

Metric	Value
Base Score	9.8 (Critical)
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Confidentiality	High
Integrity	High
Availability	High

- **Affected IPs:** 2.74.X.X, 105.235.X.X, 142.132.X.X, 167.86.X.X, 207.148.X.X
- **Affected Port:** 23/TCP
- **CVE-ID:** CVE-1999-0617
- **Technical Impact:**

1. Telnet transmits data in plaintext, including usernames and passwords.
2. An attacker sniffing the network can easily intercept sensitive credentials.

Mitigation:

1. Disable Telnet entirely if not needed.
2. Replace with SSH (port 22) which is already open and uses encryption.
3. If Telnet must be used (not recommended), consider securing it via a VPN or tunneling, though this is a weak workaround.

Reference:

https://www.tenable.com/plugins/nessus/42263

- **POC:**

```
# Nmap 7.95 scan initiated Tue May 27 16:44:50 2025 as: /usr/lib/nmap/nmap --privileged --script=telnet-
encryption.nse -Pn -oN 2.74[redacted]_1.txt 2.74.[redacted]
Nmap scan report for 2-74-[redacted] (2.74.[redacted])
Host is up (0.80s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
23/tcp   open   telnet
| telnet-encryption:
|_  Telnet server does not support encryption
53/tcp   open   domain
80/tcp   open   http
1720/tcp open   h323q931
6106/tcp closed isdninfo
9001/tcp open   tor-orport

# Nmap done at Tue May 27 17:30:51 2025 -- 1 IP address (1 host up) scanned in 2761.55 seconds
```

```
Nmap scan report for 105.235.[redacted]
Host is up (0.35s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
22/tcp open  tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
23/tcp open  telnet     Cisco router telnetd
Service Info: OS: IOS; Device: router; CPE: cpe:/o[redacted]

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Wed Jun  4 09:00:34 2025 -- 3 IP addresses (3 hosts up) scanned in 365.42 seconds
```

```
# Nmap 7.95 scan initiated Wed May 28 05:04:35 2025 as: /usr/lib/nmap/nmap --privileged --script=rdp-enum-
encryption.nse -Pn -oN 142.132.[redacted].txt 142.132.[redacted]
Nmap scan report for static.[redacted]32.142.clients.[redacted]e (142.132.[redacted])
Host is up (0.21s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE
23/tcp   open  telnet
80/tcp   open  http
```

```
# Nmap 7.95 scan initiated Sat May 17 08:42:27 2025 as: /usr/lib/nmap/nmap --privileged --script=ftp-anon.nse -
Pn -oN 167.86.[redacted]t 167.[redacted]
Nmap scan report for v[redacted] (167.86.[redacted])
Host is up (0.19s latency).
Not shown: 974 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: PASV failed: socket TIMEOUT
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
```

```
# Nmap 7.95 scan initiated Wed Jun 11 11:40:26 2025 as: /usr/lib/nmap/nmap --privileged --script=whois-ip.nse -
Pn -oN 9.txt 207.14[redacted]

Nmap scan report for 207.14[redacted] (207.14[redacted])
Host is up (0.17s latency).
Not shown: 987 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
23/tcp   open   telnet
```

2. VulnerabilityName:RDPRemoteCodeExecutionFlaw

Definitation: The remote host is affected by a remote code execution vulnerability in Remote Desktop Protocol (RDP). An unauthenticated, remote attacker can exploit this, via a series of specially crafted requests, to execute arbitrary code.

CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Metric	Value
Base Score	9.8 (Critical)
Attack Vector	Network (N)
Attack Complexity	Low (L)
Privileges Required	None (N)
User Interaction	None (N)
Scope	Unchanged (U)
Confidentiality Impact	High (H)
Integrity Impact	High (H)
Availability Impact	High (H)

Affected IPs: 168.251.x.x

Affected Port: 3389 (RDP)

CVE-ID: CVE-2019-0708

Technical Impact: Attackers could execute arbitrary code and gain remote access.

Mitigation: Patch the system and restrict RDP access.

Reference:

https://www.tenable.com/plugins/nessus/125313

http://www.nessus.org/u?577af692

http://www.nessus.org/u?8e4e0b74

3. VulnerabilityName:Pre-SetAuthenticationKeys

- **Definitation:** attacker was able to log in to telnet using default credentials. These credentials are publicly known and can allow an attacker to gain privileged access to the device.
- **CVSS: N/A**
- **Affected IPs:** 2.74. x.x, 207.148.x.x
- **Affected Port:** 23/telnet, 21/ftp
- **CVE-ID: N/A**
- **Technical Impact:**

  Attackers can gain unauthorized access to the system using publicly known default credentials. This allows them to execute commands, modify configurations, and potentially escalate privileges. If exploited, attackers can install backdoors, steal sensitive data, or use the compromised device to launch further attacks within the network.

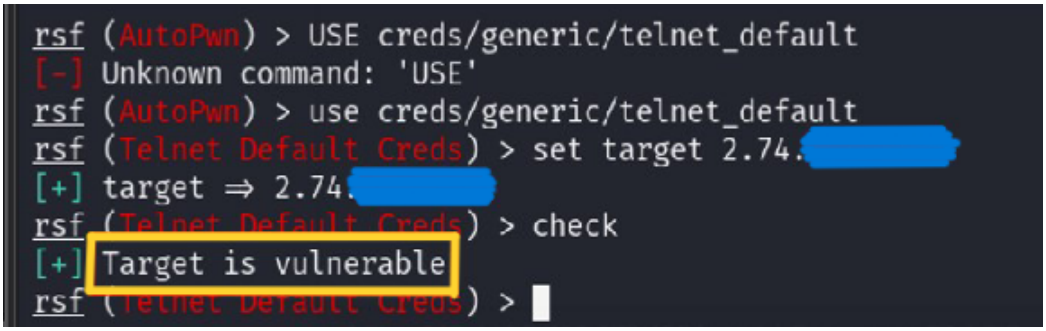
- **Mitigation:**

  1. Change Default Credentials: ’mediately update default usernames and passwords to strong, unique credentials.
  2. Disable Unused Services: ’gelnet is not required, disable it and use more secure alternatives like SSH.
  3. Restrict Access: ”imit access to Telnet and FTP by allowing only trusted IP addresses through firewall rules.
  4. Enable Multi-Factor Authentication (MFA): ’gupported, enable MFA to add an additional security layer.
  5. Monitor and Log Access: gularly monitor authentication logs for unauthorized login attempts and enforce account lockout policies.

- **Reference:**

  https://www.tenable.com/plugins/nessus/72236

- **POC :**


rsf (AutoPwn) > USE creds/generic/telnet_default
[-] Unknown command: 'USE'
rsf (AutoPwn) > use creds/generic/telnet_default
rsf (Telnet Default Creds) > set target 2.74.
[+] target ⇒ 2.74.
rsf (Telnet Default Creds) > check
[+] Target is vulnerable
rsf (Telnet Default Creds) >

4. VulnerabilityName:OutdatedPHP Installation

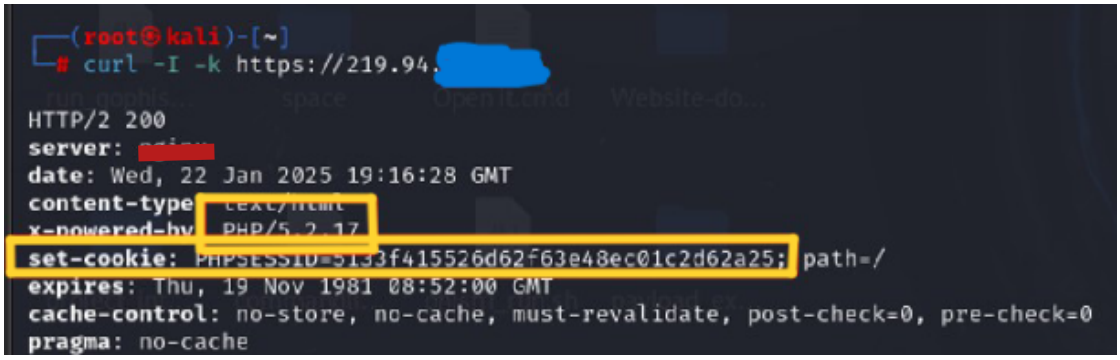
- **Definitation:** According to its version, the installation of PHP on the remote host is no longer supported.
  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Metric	Value
Base Score	9.8 (Critical)
Attack Vector	Network (N)
Attack Complexity	Low (L)
Privileges Required	None (N)
User Interaction	None (N)
Scope	Unchanged (U)
Confidentiality Impact	High (H)
Integrity Impact	High (H)
Availability Impact	High (H)

- **Affected IPs:** 219.94.X.X
- **Affected Port:** 443 / tcp / www
- **CVE-ID:** CVE-2010-4645 CVE-2024-4577 CVE-2024-5458 CVE-2024-2408
- **Technical Impact:** Running an outdated and unsupported version of PHP exposes the server to unpatched vulnerabilities, making it an attractive target for attackers. This can result in remote code execution, privilege escalation, or information disclosure. An unsupported PHP version also risks being exploited for website defacement, malware injection, or data exfiltration. Beyond security, such outdated software decreases reliability and compatibility with modern tools, potentially causing service disruptions and hindering business operations.
- **Mitigation:** Upgrade to a version of PHP that is currently supported.
- **Reference:**

  1. https://www.tenable.com/plugins/nessus/58987%20
  2. https://www.tenable.com/plugins/was/98230
  3. https://www.exploit-db.com/exploits/29290

- **POC:**




```
check is done when the php.ini configuration setting cgi.force_redirect is set
and the php.ini configuration setting cgi.redirect_status_env is set to no.
This makes it possible to execute the binary bypassing the Security check by
setting these two php.ini settings.
Prior to this code for the Security check getopt is called and it is possible
to set cgi.force_redirect to zero and cgi.redirect_status_env to zero using the
-d switch. If both values are set to zero and the request is sent to the server
php-cgi gets fully executed and we can use the payload in the POST data field
to execute arbitrary php and therefore we can execute programs on the system.
apache-magika.c is an exploit that does exactly the prior described. It does
support SSL.
/* Affected and tested versions
PHP 5.3.10
PHP 5.3.8-1
PHP 5.3.6-13
PHP 5.2.17
PHP 5.2.11
```

PHP 5.2 < 5.2.17 / 5.3 < 5.3.5 String To Double Conversion DoS

Language: English

MEDIUM Nessus Plugin ID 51439

Information | Dependencies | Dependents | Changelog

Synopsis

The remote web server uses a version of PHP that is affected by a denial of service vulnerability.

Description

According to its banner, the version of PHP 5.x installed on the remote host is older than 5.2.17 or 5.3.5.

Such versions may experience a crash while performing string to double conversion for certain numeric values. Only x86 32-bit PHP processes are known to be affected by this issue regardless of whether the system running PHP is 32-bit or 64-bit.

Solution

Upgrade to PHP 5.2.17/5.3.5 or later.

See Also

https://bugs.php.net/bug.php?id=53632

http://www.php.net/distributions/test_bug53632.txt

http://www.php.net/releases/5_2_17.php

Plugin Details

Severity: Medium

ID: 51439

File Name: php_5_3_5.nasl

Version: 1.14

Type: remote

Family: CGI abuses

Published: 1/7/2011

Updated: 11/22/2024

Configuration: Enable thorough checks

Supported Sensors: Nessus

Enable CGI Scanning: true

Risk Information

5. VulnerabilityName:ObsoleteWeb Serverversion

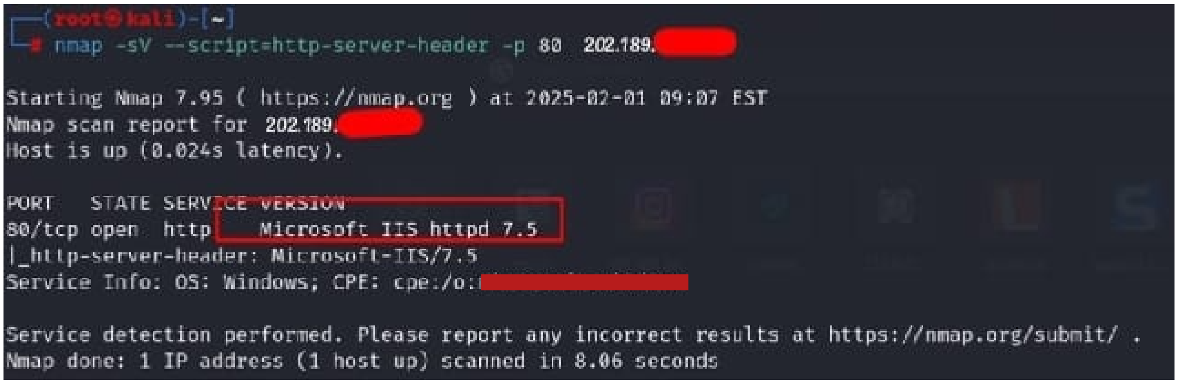
- **Definitation:** According to its version, the remote web server is obsolete and no longer maintained by its vendor or provider.
  Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

Metric	Value
CVSS Base Score	9.1 (Critical)
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Confidentiality Impact	High
Integrity Impact	Low
Availability Impact	Low
Exploitability	4.9
Impact Score	5.6

- **Affected IPs:** 202.189.x.x
- **Affected Port:** 80 / tcp / www
- **CVE-ID:** CVE-2015-1635, CVE-2017-7269, CVE-2019-0941
- **Technical Impact:** An unsupported web server presents critical security risks as it lacks regular updates and patches, leaving it vulnerable to exploitation. Attackers can exploit these vulnerabilities to gain control of the server, execute malicious code, or exfiltrate sensitive data. The lack of maintenance increases the likelihood of a complete server compromise, enabling attackers to use it as a launchpad for further attacks. This not only jeopardizes data confidentiality but also risks reputational damage and regulatory non-compliance.
- **Mitigation:** Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.
- **Reference:**

  https://www.tenable.com/plugins/nessus/34460

- **POC:**


┌──(root㉿kali)-[~]
└─# nmap -sV --script=http-server-header -p 80 202.189.[redacted]
Starting Nmap 7.95 (https://nmap.org) at 2025-02-01 09:07 EST
Nmap scan report for 202.189.[redacted]
Host is up (0.024s latency).
PORT STATE SERVICE VERSION
80/tcp open http Microsoft IIS httpd 7.5
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: cpe:/o:[redacted]
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.06 seconds


┌──(root㉿kali)-[~]
└─# searchsploit IIS 7.5
Exploit Title | Path
Microsoft IIS 6.0/7.5 (+ PHP) - Multiple Vulnerabilities | windows/remote/19033.txt
Microsoft IIS 7.5 (Windows 7) - FTPSVC Unauthorized Remote Denial of Service (PoC) | windows/dos/15803.py
Shellcodes: No Results

6. VulnerabilityName:CameraRemoteCodeExecution

- **Definitation:** Multiple camera devices by UDP Technology, Geutebrück and other vendors are vulnerable to a stack-based buffer overflow condition in the action parameter, which may allow an attacker to remotely execute arbitrary code.
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Metric	Value
CVSS Base Score	9.8 (Critical)
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Confidentiality Impact	High
Integrity Impact	High
Availability Impact	High
Exploitability	3.9
Impact Score	5.9

- **Affected IPs:** 167.86. x.x
- **Affected Port:** 80/http
- **CVE-ID:** CVE-2021-33549
- **Technical Impact:**

  Remote code execution allows attackers to execute arbitrary commands on the device, potentially gaining full control over the camera system. Unauthorized access may enable attackers to bypass authentication and manipulate camera feeds. A compromised device can be used as a pivot point for further attacks on the internal network. Exploiting this vulnerability may also cause service disruption, leading to denial of service.

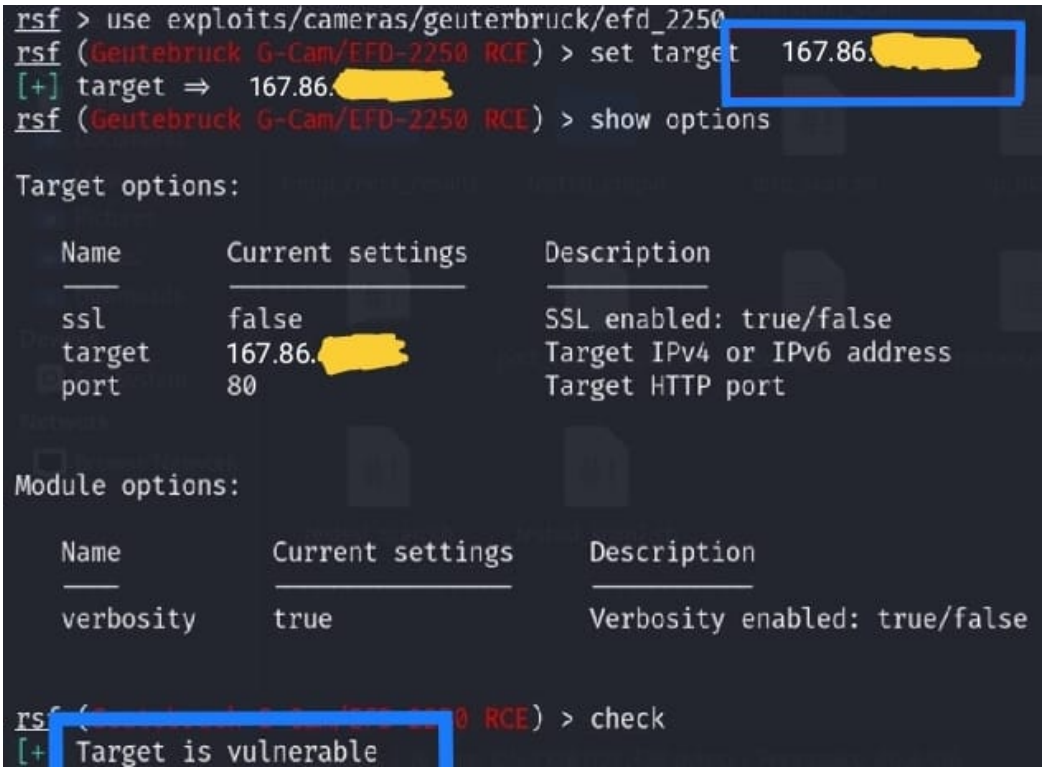
- **Mitigation:**

  1. Apply Firmware Update: Update the device firmware to the latest version provided by Geutebruck or UDP Technology to patch the vulnerability.
  2. Restrict Network Access: Limit access to the camera's web interface (port 80) by allowing only trusted IP addresses through firewall rules.
  3. Disable Unused Services: If remote management over HTTP is not required, disable it and use HTTPS with authentication.
  4. Enable Strong Authentication: Ensure that default credentials are changed and strong passwords are enforced.

- **Reference:**

  https://www.tenable.com/cve/CVE-2021-33549

- **POC:**




High

7. VulnerabilityName:SMTPMail RelayMisconfiguration

- **Definitation:** the remote SMTP server allows mail relaying.
  This issue allows any spammer to use your mail server to send their mail to the world, thus flooding your network bandwidth and possibly getting your mail server blacklisted.
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L

CVSS Metric	Value
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	Low (L) (possible data leakage)
Integrity (I)	None (N)
Availability (A)	Low (L) (can lead to DoS or blacklisting)
CVSS Base Score	6.5 (Medium)

- **Affected IPs:** 207.148. x.x
- **Affected** Port: 2525 / tcp / smtp
- **CVE-ID:** CVE-1999-0512, CVE-2002-1278, CVE-2003-0285
- **Technical Impact:** Allowing open mail relaying on an SMTP server poses a serious security threat by enabling spammers to misuse the server for sending bulk unsolicited emails. This can lead to the server being blacklisted, resulting in the disruption of legitimate email services and damaging the organization's reputation. Additionally, the increased bandwidth consumption from spam emails can degrade network performance and create operational inefficiencies. This vulnerability exposes the organization to financial and reputational risks.
- **Mitigation:** Reconfigure your SMTP server so that it cannot be used as an indiscriminate SMTP relay. Make sure that the server uses appropriate access controls to limit the extent to which relaying is possible.
- **Reference:**

  https://en.wikipedia.org/wiki/Email_spam

  https://www.tenable.com/plugins/nessus/10262

  https://www.tenable.com/plugins/nessus/118017

- **POC:**


220 a:helymadsions ESMTP Exim 4.89 OpenSMTPD
250 AUTH LOGIN PLAIN
HELP
250 OK
250 OK
354 End data with <CR><LF>.<CR><LF>
250 OK

8. VulnerabilityName:SNMPDefaultCommunityString Exposure

- **Definitation:** It is possible to obtain the default community name of the remote SNMP server.
  An attacker may use this information to gain more knowledge about the remote host, or to change the configuration of the remote system (if the default community allows such modifications).
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Metric	Value
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	Low (L)
Integrity (I)	None (N)
Availability (A)	None (N)
Base Score	5.3 (Medium)

- **Affected IPs:** 91.134.X.X 103.59.X.X
- **Affected Port:** 161/udp/snmp
- **CVE-ID:** CVE-1999-0517 CVE-2008-4309
- **Technical Impact:** The use of a default SNMP community string, such as “public,” poses a severe risk to the system. Attackers can leverage this to gather detailed information about the remote host, facilitating reconnaissance and further attacks. If the SNMP configuration allows write access, attackers may modify critical settings, leading to potential service disruptions or system misuse. This vulnerability also exposes the network to Denial-of-Service (DoS) attacks and increases the risk of sensitive information leakage, compromising the overall security of the environment.
- **Mitigation:** Disable the SNMP service on the remote host if you do not use it.
  Either filter incoming UDP packets going to this port, or change the default community string.
- **Reference:**

  https://www.tenable.com/plugins/nessus/41028

  https://www.tenable.com/plugins/nessus/76474

  https://www.tenable.com/plugins/nessus/76474

- **POC:**

```
nmap -p 161 -sU -sV -Pn   91.134.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-03 11:27 EST
Nmap scan report for   91.134.
Host is up (0.40s latency).

PORT    STATE SERVICE VERSION
161/udp open  snmp    SNMPv1 server; 942553134 SNMPv3 server (public)
Service Info: Host: Linux

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.48 seconds
```

```
nmap -p161 -sU   103.59        -sC -PN
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 06:01 EST
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 85.60% done; ETC: 06:01 (0:00:00 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 88.80% done; ETC: 06:01 (0:00:00 remaining)
Stats: 0:00:12 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.60% done; ETC: 06:01 (0:00:01 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.20% done; ETC: 06:01 (0:00:00 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.20% done; ETC: 06:01 (0:00:00 remaining)
Nmap scan report for   103.59
Host is up (0.39s latency).

PORT    STATE SERVICE
161/udp open  snmp
| snmp-info:
|   enterprise:
|   engineIDFormat: text
|   engineIDData:
|   snmpEngineBoots: 0
|_  snmpEngineTime: 0s
| snmp-sysdescr: RouterOS RBLHG-5HPnD
|_  System uptime: 276d17h54m17.00s (2391085700 timeticks)
| snmp-interfaces:
|   Public
|     MAC address:     32:T7
|     Type: ieee80211  Speed: 50 Mbps
|     Traffic stats: 3.13 Gb sent, 518.96 Mb received
|   Lan
|     IP address: 192.168.0.1  Netmask: 255.255.255.0
|     MAC address:     32:T7
|     Type: ethernetCsmacd  Speed: 100 Mbps
|     Traffic stats: 1.01 Gb sent, 3.22 Gb received
|   PPPoE
|     IP address:    103.59        tmask: 255.255.255.255
|     Type: ppp  Speed: 0 Kbps
|_    Traffic st  s: 79.09 Mb sent, 1.99 Gb received

Nmap done: 1 IP address (1 host up) scanned in 31.57 seconds
```

9. VulnerabilityName:WeakRDPEncryption

- **Definitation:** The remote Terminal Services service is not configured to use strong cryptography.

  Using weak cryptography with this service may allow an attacker to eavesdrop on the communications more easily and obtain screenshots and/or keystrokes.

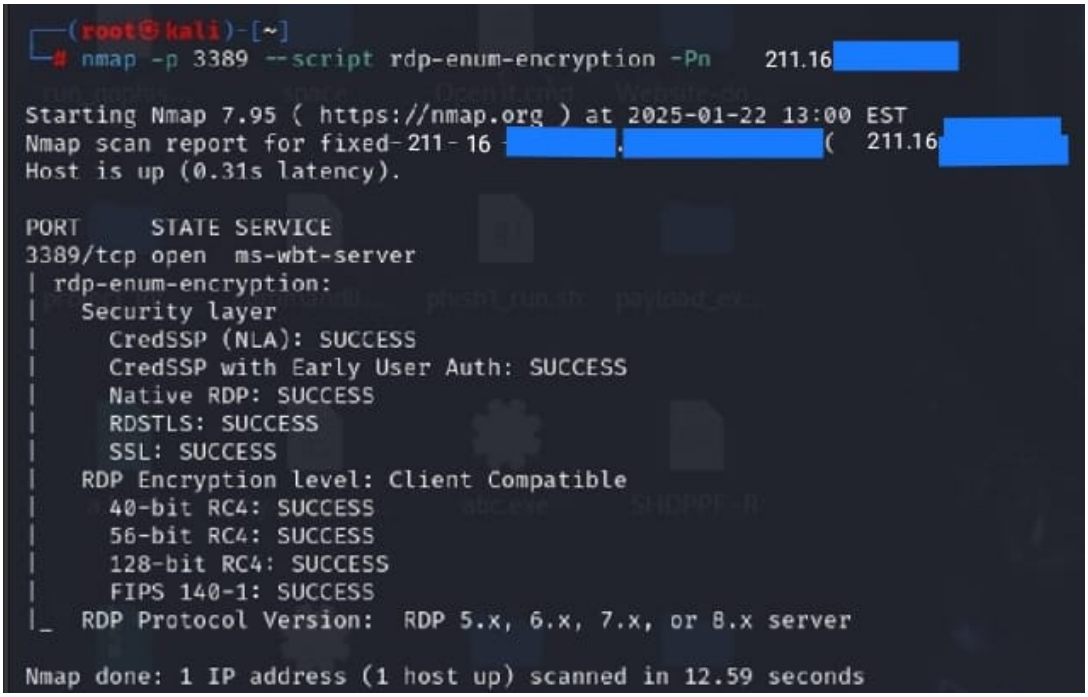
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N

Metric	Value
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	High (H)
Integrity (I)	Low (L)
Availability (A)	None (N)
Base Score	7.4 (High)

- **Affected IPs:** 211.16.. X.X
- **Affected Port:** 3389 (RDP)
- **CVE-ID:** N/A
- **Technical Impact:** Unauthorized access to the system could allow attackers to gain full control.
- **Mitigation:** Change RDP encryption level to one of : 1. High 2. FIPS Compliant
- **Reference:**

  https://www.tenable.com/plugins/nessus/57690

- **POC:**


(root㉿kali)-[~]
nmap -p 3389 --script rdp-enum-encryption -Pn 211.16
Starting Nmap 7.95 (https://nmap.org) at 2025-01-22 13:00 EST
Nmap scan report for fixed-211-16 (211.16
Host is up (0.31s latency).
PORT STATE SERVICE
3389/tcp open ms-wbt-server
| rdp-enum-encryption:
| Security layer
| CredSSP (NLA): SUCCESS
| CredSSP with Early User Auth: SUCCESS
| Native RDP: SUCCESS
| RDSTLS: SUCCESS
| SSL: SUCCESS
| RDP Encryption level: Client Compatible
| 40-bit RC4: SUCCESS
| 56-bit RC4: SUCCESS
| 128-bit RC4: SUCCESS
| FIPS 140-1: SUCCESS
|_ RDP Protocol Version: RDP 5.x, 6.x, 7.x, or 8.x server
Nmap done: 1 IP address (1 host up) scanned in 12.59 seconds

10. VulnerabilityName:FTPOpen Authentication

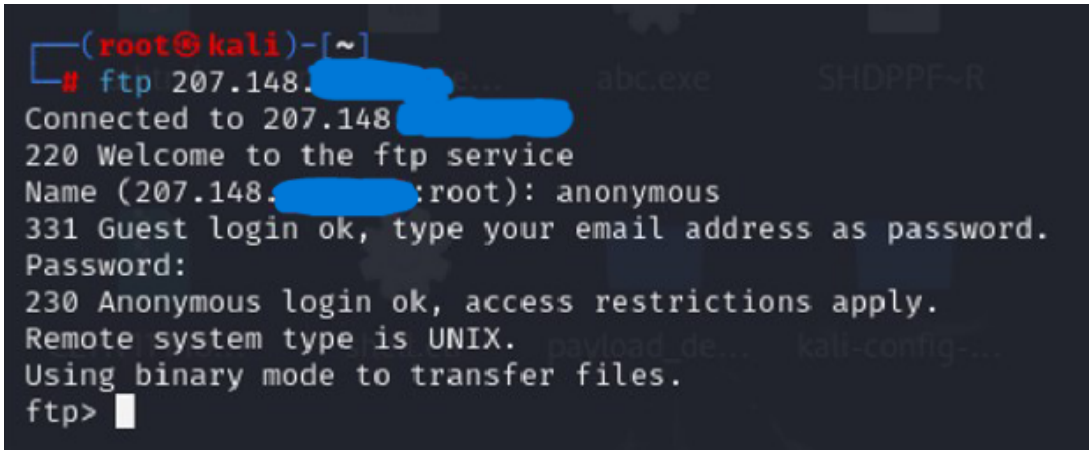
- **Definitation:** The FTP service allows login without requiring authentication, enabling unauthorized access to the server.
- **CVSS:**

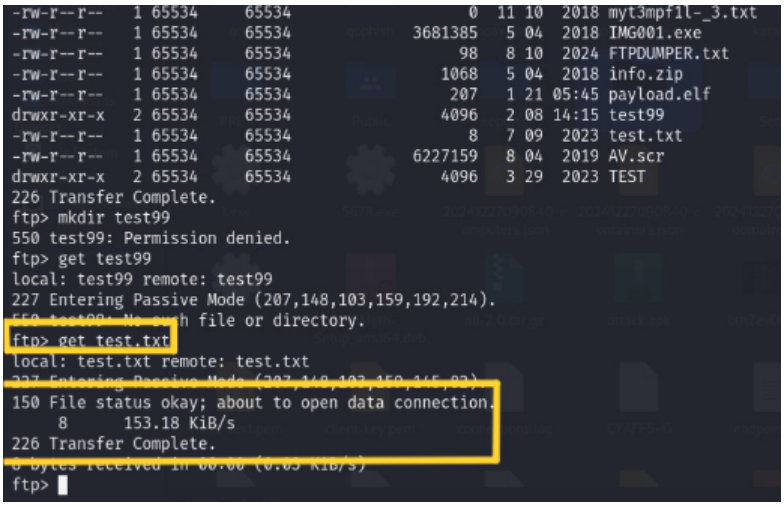
Metric	Value
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	High (H)
Integrity (I)	Low (L)
CVSS Base Score	9.1 (Critical)

- **Affected IPs:** 67.20.x.x, 207.148.x.x
- **Affected Port:** 21 (FTP)
- **CVE-ID:** N/A
- **Technical Impact:** Data exposure and server integrity risk.
- **Mitigation:** Disable anonymous login and implement strong authentication.
- **Reference:**

  https://www.tenable.com/plugins/nessus/10079

- **POC:**


(root㉿kali)-[~]
ftp 207.148.
Connected to 207.148
220 Welcome to the ftp service
Name (207.148. :root): anonymous
331 Guest login ok, type your email address as password.
Password:
230 Anonymous login ok, access restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>


-rw-r--r-- 1 65534 65534 0 11 10 2018 myt3mpf1l-_3.txt
-rw-r--r-- 1 65534 65534 3681385 5 04 2018 IMG001.exe
-rw-r--r-- 1 65534 65534 98 8 10 2024 FTPDUMPER.txt
-rw-r--r-- 1 65534 65534 1068 5 04 2018 info.zip
-rw-r--r-- 1 65534 65534 207 1 21 05:45 payload.elf
drwxr-xr-x 2 65534 65534 4096 2 08 14:15 test99
-rw-r--r-- 1 65534 65534 8 7 09 2023 test.txt
-rw-r--r-- 1 65534 65534 6227159 8 04 2019 AV.scr
drwxr-xr-x 2 65534 65534 4096 3 29 2023 TEST
226 Transfer Complete.
ftp> mkdir test99
550 test99: Permission denied.
ftp> get test99
local: test99 remote: test99
227 Entering Passive Mode (207,148,103,159,192,214).
ftp> get test.txt
local: test.txt remote: test.txt
150 File status okay; about to open data connection.
8 153.18 KiB/s
226 Transfer Complete.
ftp>

11. VulnerabilityName:ImproperSNMPConfiguration

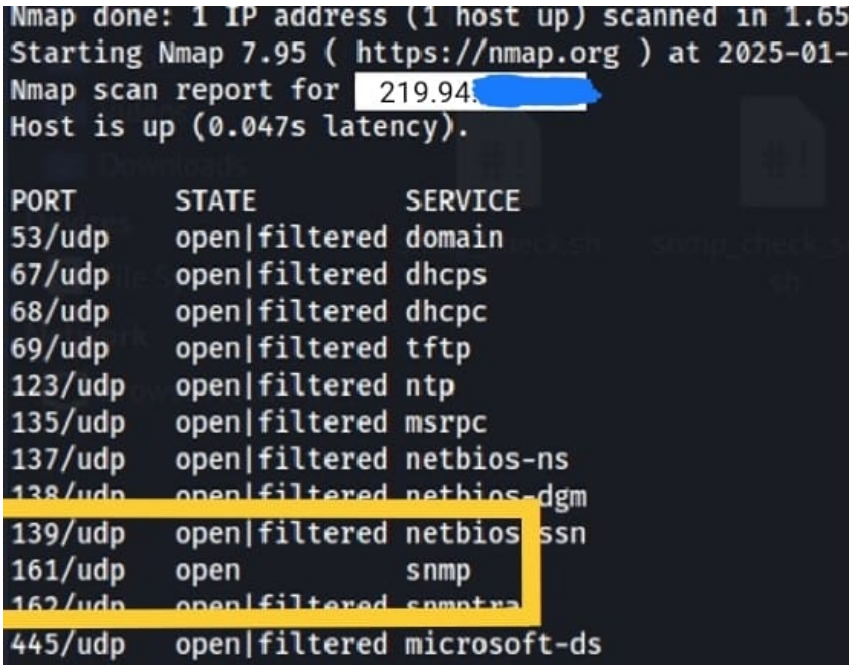
- **Definitation:** The SNMP service is accessible, potentially without authentication or with weak community strings.
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

Metric	Value
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	High (H)
Integrity (I)	Low (L)
Availability (A)	Low (L)

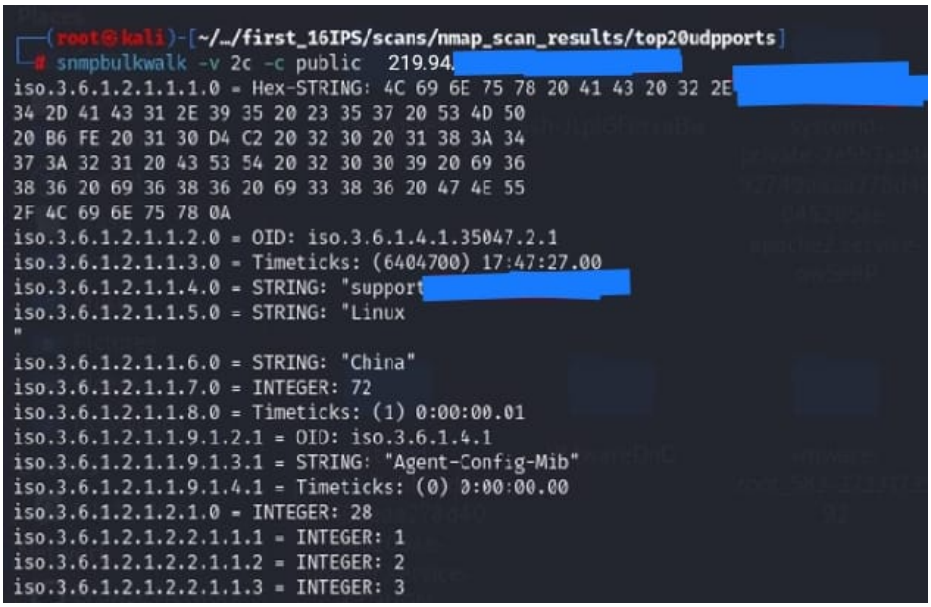
- **Affected IPs:** 219.94.X.X, 215.189.X.X
- **Affected Port:** 161 (SNMP)
- **CVE-ID: N/A**
- **Technical Impact:** Information leakage and reconnaissance for attackers.
- **Mitigation:** Secure SNMP configuration and restrict access.
- **Reference:**

  https://www.tenable.com/plugins/nessus/41028

POC:


Nmap done: 1 IP address (1 host up) scanned in 1.65
Starting Nmap 7.95 (https://nmap.org) at 2025-01-
Nmap scan report for 219.94
Host is up (0.047s latency).
PORT STATE SERVICE
53/udp open|filtered domain
67/udp open|filtered dhcps
68/udp open|filtered dhcpc
69/udp open|filtered tftp
123/udp open|filtered ntp
135/udp open|filtered msrpc
137/udp open|filtered netbios-ns
139/udp open|filtered netbios
161/udp open snmp
445/udp open|filtered microsoft-ds


msf6 auxiliary( ) > run
[+] 219.94 Connected.
[*] System information:
Host IP : 219.94
Hostname : Linux
Description : Linux AC 2.4.35.4-AC1.95 #57 SMP •• 10•• 20 18:47:21 CST 2009 1686 1686 1386 GNU/Linux
Contact : support@
Location : China
Uptime snmp : -
Uptime system : 21:56:35.00
System date : -
[*] Network information:
IP forwarding enabled : yes
Default TTL : 64
TCP segments received : 25014127
TCP segments sent : 25143120
TCP segments retrans : 41400
Input datagrams : 2539314930
Delivered datagrams : 38521170
Output datagrams : 39599494
[*] Network interfaces:
Interface : [up] lo
Id : 1


┌──(root㉿kali)-[~/…/first_16IPS/scans/nmap_scan_results/top20udpports]
└─# snmpbulkwalk -v 2c -c public 219.94.
iso.3.6.1.2.1.1.1.0 = Hex-STRING: 4C 69 6E 75 78 20 41 43 20 32 2E
34 2D 41 43 31 2E 39 35 20 23 35 37 20 53 4D 50
20 B6 FE 20 31 30 D4 C2 20 32 30 20 31 38 3A 34
37 3A 32 31 20 43 53 54 20 32 30 30 39 20 69 36
38 36 20 69 36 38 36 20 69 33 38 36 20 47 4E 55
2F 4C 69 6E 75 78 0A
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.35047.2.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (6404700) 17:47:27.00
iso.3.6.1.2.1.1.4.0 = STRING: "support
iso.3.6.1.2.1.1.5.0 = STRING: "Linux
"
iso.3.6.1.2.1.1.6.0 = STRING: "China"
iso.3.6.1.2.1.1.7.0 = INTEGER: 72
iso.3.6.1.2.1.1.8.0 = Timeticks: (1) 0:00:00.01
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.4.1
iso.3.6.1.2.1.1.9.1.3.1 = STRING: "Agent-Config-Mib"
iso.3.6.1.2.1.1.9.1.4.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.1.0 = INTEGER: 28
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.1.3 = INTEGER: 3

12. VulnerabilityName:Web DirectoryTraversal

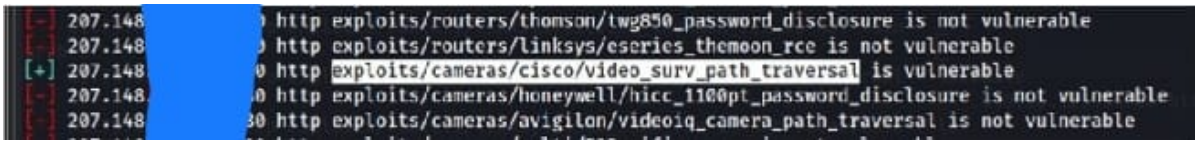
- **Definitation:** It appears possible to read arbitrary files on the remote host outside the web server's document directory using a specially crafted URL. An unauthenticated attacker may be able to exploit this issue to access sensitive information to aide in subsequent attacks.
  Note that this plugin is not limited to testing for known vulnerabilities in a specific set of web servers. Instead, it attempts a variety of generic directory traversal attacks and considers a product to be vulnerable simply if it finds evidence of the contents of '/etc/passwd' or a Windows 'win.ini' file in the response. It may, in fact, uncover 'new' issues, that have yet to be reported to the product's vendor.
- **CVSS:**

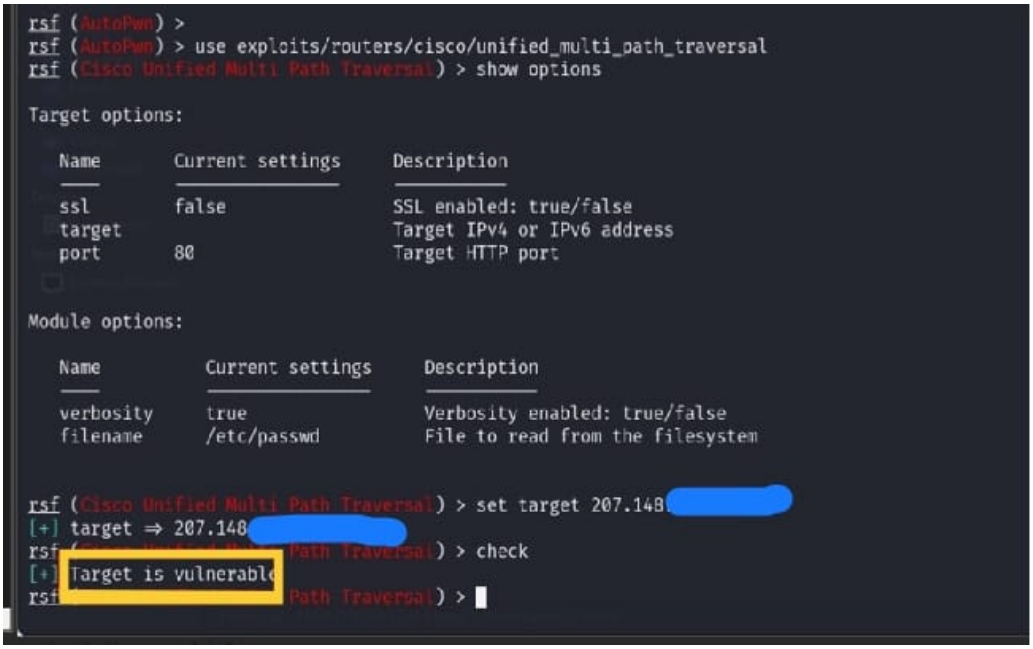
Metric	Value
CVSS Version	3.1
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	High (H)
Integrity (1)	None (N)
Availability (A)	None (N)

- **Affected IPs:** 207.148.x.x
- **Affected Port:** 82 / tcp / www
- **CVE-ID:**
- **Technical Impact:** A directory traversal vulnerability allows unauthorized access to sensitive files outside the web server’s document root. Attackers can exploit this to obtain configuration files, credentials, or other critical information, which can then be used to launch subsequent attacks. This compromises the confidentiality and integrity of data stored on the server and can aid in privilege escalation or unauthorized code execution. Such vulnerabilities significantly weaken the security posture of the organization.
- **Mitigation:** Contact the vendor for an update, use a different product, or disable the service altogether.
- **Reference:**

  https://www.tenable.com/plugins/nessus/10297

POC:


207.148 http exploits/routers/thomson/twg850_password_disclosure is not vulnerable
207.148 http exploits/routers/linksys/eseries_themoon_rce is not vulnerable
[+] 207.148 http exploits/cameras/cisco/video_surv_path_traversal is vulnerable
207.148 http exploits/cameras/honeywell/hicc_1100pt_password_disclosure is not vulnerable
207.148 http exploits/cameras/avigilon/videoiq_camera_path_traversal is not vulnerable


rsf (AutoPwn) >
rsf (AutoPwn) > use exploits/routers/cisco/unified_multi_path_traversal
rsf (Cisco Unified Multi Path Traversal) > show options
Target options:
Name Current settings Description
ssl false SSL enabled: true/false
target Target IPv4 or IPv6 address
port 80 Target HTTP port
Module options:
Name Current settings Description
verbosity true Verbosity enabled: true/false
filename /etc/passwd File to read from the filesystem
rsf (Cisco Unified Multi Path Traversal) > set target 207.148
[+] target => 207.148
) > check
[+] Target is vulnerable
) >

Medium

13. VulnerabilityName:Lack OfRDPNetwork-LevelAuthentication

- **Definitation:** The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.
- **CVSS 8**

Metric	Value
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	High (H)
Integrity (1)	High (H)
Availability (A)	High (H)
Base Score	9.8 (Critical)

- **Affected IPs:** 88.198.X.X, 51.81.X.X
- **Affected Port:** 3389 (RDP)
- **CVE-ID:** N/A
- **Technical Impact:**

  Unauthorized access to the system could allow attackers to gain full control.

- **Mitigation:**

  1. Enforce NLA for RDP sessions.
  2. Use strong, unique credentials for RDP accounts.
  3. Restrict access to RDP services through firewalls (e.g., only allow specific IPs).
  4. Disable RDP on systems unless strictly necessary.
  5. Upgrade unsupported systems (e.g., Windows 7) to a supported version of Windows.
  6. Monitor RDP access for unusual activity (e.g., multiple failed login attempts).

- **Reference:**

  1. https://www.tenable.com/plugins/nessus/58453

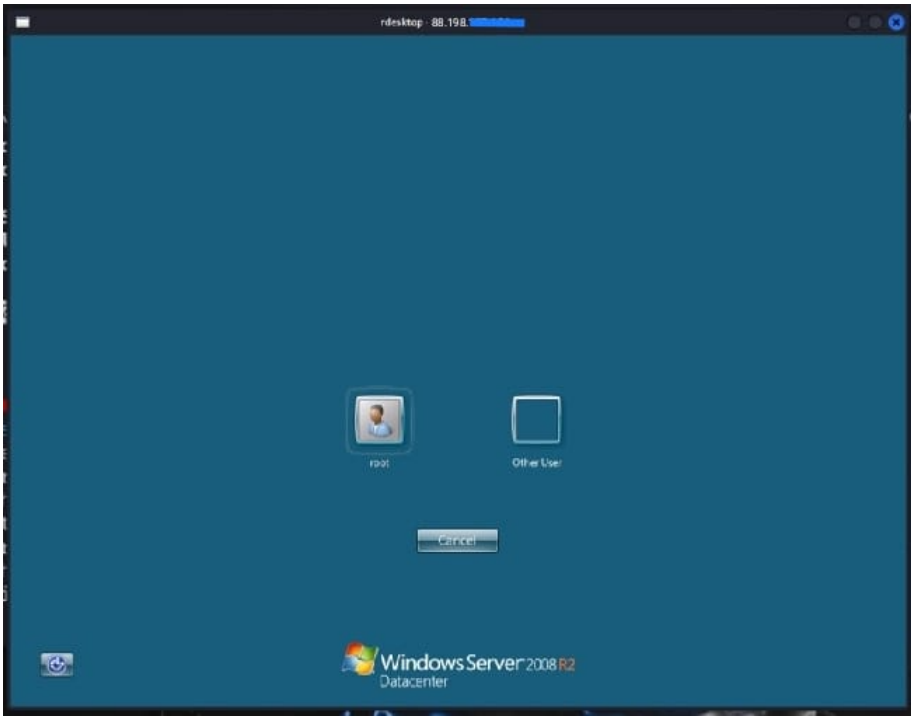
  2. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

- **POC:**

```
┌──(root㉿kali)-[~/…/first_16IPS/scans/nmap_scan_results/top20udpports]
└─# nmap -p 3389 --script rdp-vuln-ms12-020  88.198.[redacted]
Starting Nmap 7.95 ( https://[redacted] ) at 2025-02-08 06:23 EST
Nmap scan report for  88.198.[redacted]
Host is up (0.013s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 61.00 seconds
```



14. VulnerabilityName:RDPServerMITM

- **Definitation:** The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials. This flaw exists because the RDP server stores a publicly known hard-coded RSA private key. Any attacker in a privileged network location can use the key for this attack.
- **CVSS :** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:L

Metric	Value
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality Impact	High
Integrity Impact	Low
Availability Impact	Low

- **Affected IPs:** 88.198.X.X
- **Affected Port:** 3389 / tcp / msrdp
- **CVE-ID:** CVE-2005-1794
- **Technical Impact:** The vulnerability in the Remote Desktop Protocol (RDP) server makes it susceptible to man-in-the-middle (MiTM) attacks. Since the client does not validate the server's identity during encryption setup, attackers can intercept sensitive information such as credentials or session data. This weakness compromises the confidentiality and integrity of data transmitted over the RDP session and facilitates unauthorized access to the network. Exploiting this vulnerability can lead to further attacks, including data breaches and privilege escalation.
- **Mitigation:**

1. Force the use of SSL as a transport layer for this service if supported, or/and
2. On Microsoft Windows operating systems, select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.

- **Reference:**

  1. https://nvd.nist.gov/vuln/detail/cve-2005-1794

  2. https://www.tenable.com/plugins/nessus/18405

  3. http://www.nessus.org/u?8033da0d

- **POC:**

```
┌──(root㉿kali)-[~/Desktop/project_intern/first_16IPS]
└─# python3 /root/Desktop/project_intern/first_16IPS/CVE-2005-1794-check.py 88.198.[redacted] 3389

Certificate signature sent by server:

        17c069bcf075c13d8e4965cde17473b5
        d7130fdd7e123e15ee33bf2095a9c4ef
        4f1c9538e1ae9d9b80e901b1b2d3fa9d
        4ccf0caab87c1da70806d13a7980da2f

[+]Attempting to sign certificate with hardcoded RSA key and produce matching signature ...

Certificate signature generated using hardcoded RSA private key:

        17c069bcf075c13d8e4965cde17473b5
        d7130fdd7e123e15ee33bf2095a9c4ef
        4f1c9538e1ae9d9b80e901b1b2d3fa9d
        4ccf0caab87c1da70806d13a7980da2f

MD5 hashes of signatures:

Original signature md5 hash: e24531f519ac51bfb9a66608e1e3e9fc
Hardcoded signed hash:       e24531f519ac51bfb9a66608e1e3e9fc

VULNERABLE: Signatures match, certificate was able to be signed with the hardcoded RSA key.
```

15. VulnerabilityName:PlainTextTelnetProtocol

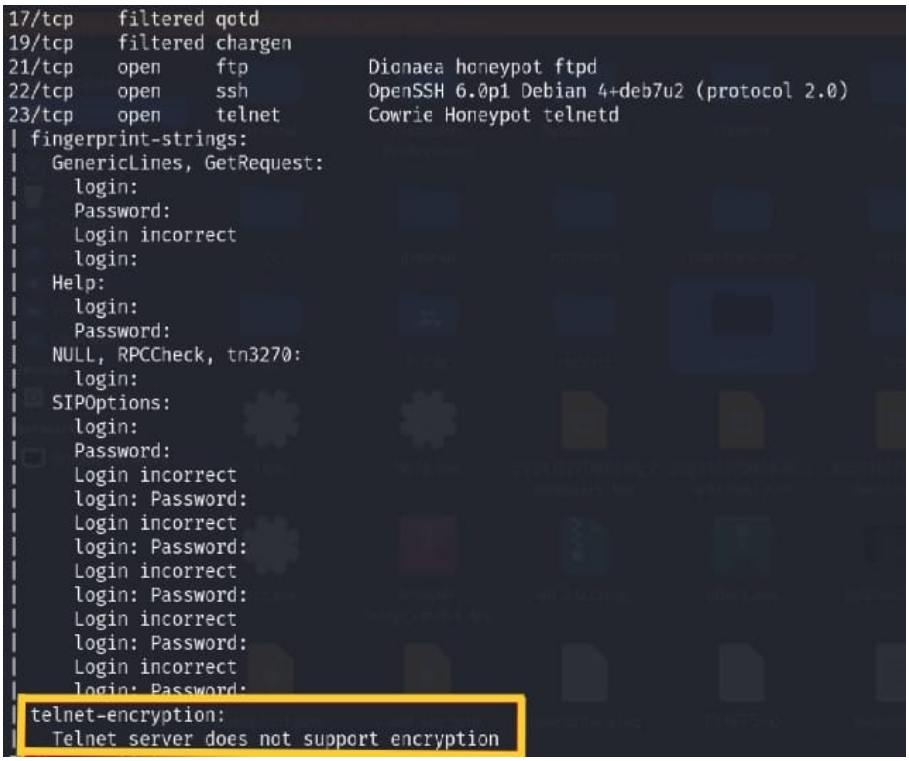
- **Definitation:** The remote host is running a Telnet server over an unencrypted channel. Using Telnet over an unencrypted channel is not recommended as logins, passwords, and commands are transferred in cleartext. This allows a remote, man-in-the-middle attacker to eavesdrop on a Telnet session to obtain credentials or other sensitive information and to modify traffic exchanged between a client and server.
  SSH is preferred over Telnet since it protects credentials from eavesdropping and can tunnel additional data streams such as an X11 session.
- **CVSS:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N

Metric	Value
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	Low (L)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	High (H)
Integrity (I)	None (N)
Availability (A)	None (N)

- **Affected IPs:** 142.132.x.x, 207.148.x.x , 184.74.x.x 105.235.x.x
- **Affected Port:** 23/tcp/telnet,2323/tcp/telnet
- **CVE-ID: N/A**
- **Technical Impact:** Running an unencrypted Telnet server poses a high-security risk as it transmits sensitive data, including credentials, in plaintext. This allows attackers to intercept and eavesdrop on the communication, potentially leading to credential theft or session hijacking. Additionally, attackers can perform man-in-the-middle attacks or modify transmitted data, compromising the integrity of the system. The use of outdated and insecure protocols like Telnet significantly weakens the overall security posture and increases exposure to cyber threats.
- **Mitigation:** Disable the Telnet service and use SSH instead.
- **Reference:**

  https://www.tenable.com/plugins/nessus/42263

- **POC:**


17/tcp filtered qotd
19/tcp filtered chargen
21/tcp open ftp Dionaea honeypot ftpd
22/tcp open ssh OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
23/tcp open telnet Cowrie Honeypot telnetd
| fingerprint-strings:
| GenericLines, GetRequest:
| login:
| Password:
| Login incorrect
| login:
| Help:
| login:
| Password:
| NULL, RPCCheck, tn3270:
| login:
| SIPOptions:
| login:
| Password:
| Login incorrect
| login: Password:
| Login incorrect
| login: Password:
| Login incorrect
| login: Password:
| Login incorrect
| login: Password:
| Login incorrect
| login: Password:
| telnet-encryption:
| Telnet server does not support encryption

16. VulnerabilityName:ExposedDNS Service

- **Definitation:** The presence of an open DNS port (53/UDP) exposes the system to potential DNS-related vulnerabilities. Misconfigured or unsecured DNS services can allow attackers to exploit the system for amplification attacks (e.g., DNS amplification in DDoS), cache poisoning, or reconnaissance activities. Open recursive DNS servers are especially vulnerable as they can be abused for reflection/amplification attacks.
- **CVSS:** CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Attribute	Details
Vulnerability Name	Open DNS Port
Port	53/UDP
Service	Domain Name System (DNS)
Protocol	UDP
Risk Level	Medium
CVSS v3.1 Base Score	5.3 (Medium)

AffectedIPs: 37.59.X.X

AffectedPort: 53/UDP

Technical Impact: DNS amplification can significantly contribute to Distributed Denial-of-Service (DDoS) attacks, potentially overwhelming network resources. ,An open recursive DNS resolver can allow attackers to use the system as a proxy for malicious activities. , Unauthenticated access to the DNS service may allow attackers to gather sensitive information about internal networks.

Mitigation:

1. Restrict Access: Configure the DNS server to restrict queries to trusted IP addresses or internal networks only.Block external access to port 53/UDP unless required for legitimate services.
2. Disable Recursion: Disable DNS recursion if the server is not intended to be a recursive resolver.
3. RateLimiting:Apply rate-limiting on theDNS servertomitigatetherisk ofamplification attacks.
4. FirewallRules:Usefirewallrulestoblockunauthorizedexternalaccesstoport53/UDP.

Reference:

1. https://www.csk.gov.in/csksa/csksa_03.html

2. https://www.cisa.gov/news-events/alerts/2013/03/29/dns-amplification-attacks

- **POC:**

```
┌──(root㉿kali)-[~]
└─# nmap -sU -p 53 -sV -P0 --script dns-recursion 37.59.[redacted]
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-08 08:43 EST
Nmap scan report for 37.59.[redacted] (37.59.[redacted])
Host is up (0.36s latency).

PORT   STATE SERVICE VERSION
53/udp open  domain  ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
Service Info: OS: Linux; CPE: cpe:/o:[redacted]linux:7

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds
```

```
┌──(root㉿kali)-[~]
└─# dig @37.59[redacted]any randomdomain.com

; <<>> DiG 9.20.2-1-Debian <<>> @37.59[redacted]any randomdomain.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 15796
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
; COOKIE: 768d6e6b72d4377b83affb0c679bb62791a6ef580172a85d (good)
;; QUESTION SECTION:
;[redacted]                    IN      ANY

;; ANSWER SECTION:
[redacted]          3600    IN      A       34.87[redacted]

;; AUTHORITY SECTION:
.                       3600    IN      NS      [redacted]
.                       3600    IN      NS      [redacted]

;; ADDITIONAL SECTION:
ns1[redacted]           3600    IN      A       34.87.[redacted]
ns2[redacted]           3600    IN      A       34.87.[redacted]

;; Query time: 303 msec
;; SERVER: 67.20.124.65#53(37.59[redacted] (TCP)
;; WHEN: Thu Jan 30 12:25:59 EST 2025
;; MSG SIZE  rcvd: 164
```

17. VulnerabilityName:TLSPaddingOracle

- **Definitation:** The LUCKY13 vulnerability exploits a weakness in the TLS/DTLS implementation of cipher block chaining (CBC) mode. This side-channel attack uses timing discrepancies to infer plaintext information, such as sensitive data from encrypted communications. The vulnerability affects TLS implementations that do not properly process padding bytes during decryption.

- **CVSS:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Metric	Value
Metric	**Value**
CVSS Base Score	5.9 (Medium)
Attack Vector (AV)	Network (N)
Attack Complexity (AC)	High (H)
Privileges Required (PR)	None (N)
User Interaction (UI)	None (N)
Scope (S)	Unchanged (U)
Confidentiality (C)	Low (L)
Integrity (1)	None (N)
Availability (A)	None (N

Affected IPs: 105.235.X.X

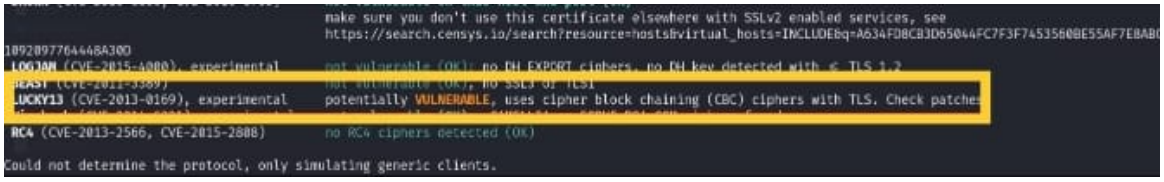
Affected Port: 443 (HTTPS), 8443 (alternative HTTPS)

Technical Impact: The attacker can potentially decrypt sensitive data such as session cookies, login credentials, or confidential information transmitted over TLS/DTLS., The attack relies on precise timing measurements, making it feasible only under certain conditions (e.g., close proximity to the target)., Could compromise the confidentiality of data encrypted with vulnerable TLS/DTLS implementations.

Mitigation: Update Software: Upgrade to the latest version of TLS/DTLS libraries (e.g., OpenSSL, GnuTLS) that have patched the LUCKY13 vulnerability by implementing properpaddingchecksandcountermeasures.,DisableCBC Ciphers:Configureyour Poly1305, whicharenotvulnerabletoLUCKY13.,UseTLS1.2 orHigher:Ensurethat servertoprioritizeorexclusivelyusesecurealternativeslike AES-GCM orChaCha20- your system supports and enforces the use of TLS 1.2 or higher, as it addresses vulnerabilities present in earlier versions., Enable Strict Timing Measures: If using CBC ciphers, ensure that implementations follow constant-time cryptographic operations to mitigate timing side-channels.

Reference: https://nvd.nist.gov/vuln/detail/CVE-2013-0169

POC:



18. VulnerabilityName:Weak SSlCipher Suits

- **Definitation:**

  The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

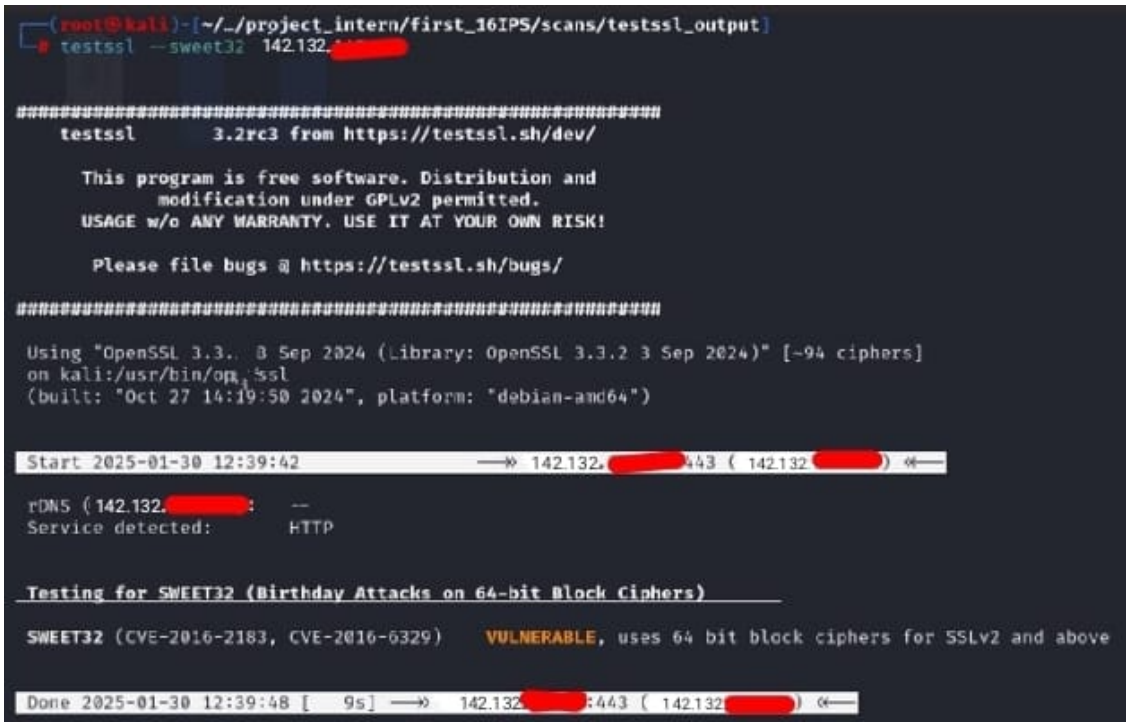
  Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.

- **CVSS:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:M/I:M/A:N

Metric	Value
Attack Vector	Network
Attack Complexity	Low
Privileges Required	None
User Interaction	None
Scope	Unchanged
Confidentiality Impact	Low
Integrity Impact	None
Availability Impact	None
Base Score	5.9 (Medium)

- **Affected IPs:** 142.132.x.x, 203.192.X.X,5.135.X.X
- **Affected Port:** 465/tcp/smtp,3389/tcp/msrdp,1112/tcp/www,44333/tcp/www
- **CVE-ID:** **CVE-2016-2183**
- **Technical Impact:** The use of medium-strength SSL ciphers, such as 3DES, increases susceptibility to cryptographic attacks like SWEET32. An attacker on the same network can exploit these weaknesses to intercept or manipulate encrypted data, undermining its confidentiality and integrity. While medium-strength ciphers are less vulnerable than weak ones, they still fall short of modern security standards. This vulnerability not only compromises secure communications but also impacts compliance with industry regulations, such as PCI DSS.
- **Mitigation:** Reconfigure the affected application if possible to avoid use of medium strength ciphers.
- **Reference:**
  - https://www.openssl.org/blog/blog/2016/08/24/sweet32/
  - https://sweet32.info

- **POC:**


testssl --sweet32 142.132.
testssl 3.2rc3 from https://testssl.sh/dev/
This program is free software. Distribution and
modification under GPLv2 permitted.
USAGE w/o ANY WARRANTY. USE IT AT YOUR OWN RISK!
Please file bugs @ https://testssl.sh/bugs/
Using "OpenSSL 3.3. 3 Sep 2024 (Library: OpenSSL 3.3.2 3 Sep 2024)" [~94 ciphers]
on kali:/usr/bin/openssl
(built: "Oct 27 14:19:50 2024", platform: "debian-amd64")
Start 2025-01-30 12:39:42
rDNS (142.132.
Service detected: HTTP
Testing for SWEET32 (Birthday Attacks on 64-bit Block Ciphers)
SWEET32 (CVE-2016-2183, CVE-2016-6329) VULNERABLE, uses 64 bit block ciphers for SSLv2 and above
Done 2025-01-30 12:39:48 [9s]

Low

Info

19. VulnerabilityName:SSHPassword-BasedAuthentication

- **Definitation:** The OpenSSH service is configured to allow password-based authentication. This can be exploited using brute-force attacks if weak or default passwords are used. Additionally, the OpenSSH version disclosed may be outdated, exposing the system to known vulnerabilities.
- **CVSS:** CVSS v3.1 Base Score: 3.7 (Low)

Affected IPs: 103.56.x.x

Affected Port: 22 (ssh)

Technical Impact: Unauthorized system access if weak or default passwords are used. Exploitation of OpenSSH vulnerabilities may lead to data theft, system compromise, or further lateral movement in the network.

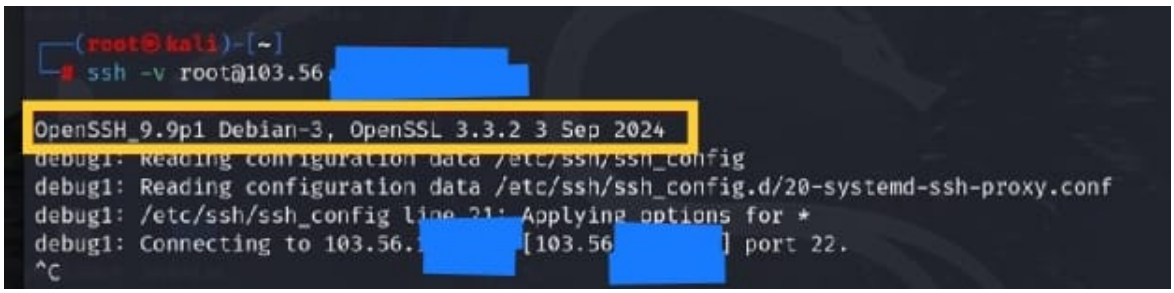
Mitigation:

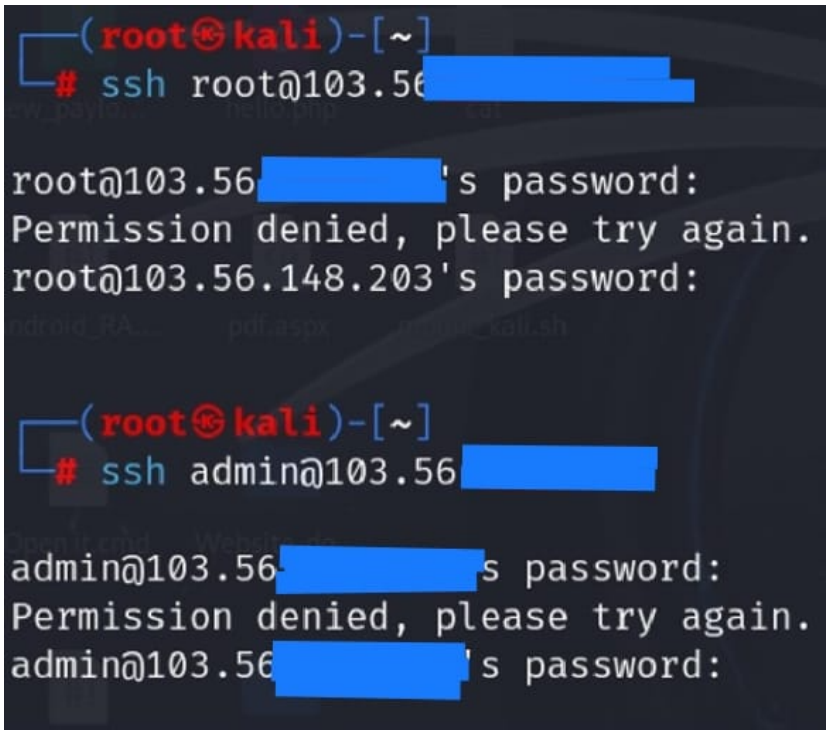
1. Disable password-based authentication and enforce public key authentication in /etc/ssh/sshd_config: PasswordAuthentication no
2. Regularly update OpenSSH to the latest version to address known vulnerabilities.
3. Use a firewall to restrict SSH access to trusted IP addresses.
4. Implement monitoring tools like fail2ban to detect and block brute-force attempts.

Reference:

https://www.tenable.com/plugins/nessus/149334

- **POC:**


ssh -v root@103.56
OpenSSH_9.9p1 Debian-3, OpenSSL 3.3.2 3 Sep 2024
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Reading configuration data /etc/ssh/ssh_config.d/20-systemd-ssh-proxy.conf
debug1: /etc/ssh/ssh_config line 21: Applying options for *
debug1: Connecting to 103.56.
[103.56
] port 22.
^C


ssh root@103.56
root@103.56
's password:
Permission denied, please try again.
root@103.56.148.203's password:
ssh admin@103.56
admin@103.56
s password:
Permission denied, please try again.
admin@103.56
's password:

8. Final Analysis

The comprehensive Vulnerability Assessment and Penetration Testing (VAPT) conducted on the network infrastructure identified a spectrum of security vulnerabilities ranging from critical to medium severity. Below is a detailed summary of the conclusions drawn from this assessment:

Severe Security Flaws

- Unsupported Operating Systems: Specifically, Windows 7 was found on one of the systems, which is critically outdated, posing a high risk of exploitation due to lack of security patches.

- BlueKeep Vulnerability: This critical flaw in RDP allows for remote code execution, presenting an immediate threat to system integrity and confidentiality.

Major Risk Issues

- Default Credentials on Services: Systems using default credentials for Telnet and FTP were identified, making them prime targets for unauthorized access.

- RDP Misconfigurations: Lack of Network Level Authentication (NLA) and weak encryption settings on RDP services could lead to unauthorized control of systems.

- Web Server Vulnerabilities: An outdated web server and directory traversal vulnerabilities could expose sensitive data or allow server compromise.

Moderate Risk Findings

- Outdated Software: PHP installations and VNC viewers are no longer supported, increasing the likelihood of exploitation through known vulnerabilities.

- SNMP Misconfigurations: Default or weak community strings and accessible SNMP services could lead to information leakage or be used in DDoS reflection attacks.

- Encryption and Authentication Weaknesses: Issues like the LUCKY13 vulnerability in TLS/DTLS and medium strength SSL ciphers (SWEET32) compromise data confidentiality.

Fixes (Mitigations) and Suggestions

- Immediate Patching: Critical vulnerabilities, particularly those related to unsupported OS and known exploits like BlueKeep, should be addressed immediately by patching or upgrading systems.

- Configuration Hardening: Services like RDP, SNMP, and Telnet need immediate reconfiguration to enforce strong authentication, change default credentials, and apply restrictive access controls.

- Software Updates: Upgrade all outdated software, including web servers, PHP, and VNC, to versions that are currently supported and secured.

- Network Security Enhancements: Implement firewalls, restrict service access, and ensure that only necessary services are exposed to the internet.

- Encryption Standards: Upgrade encryption protocols, disable weak cipher suites, and enforce the use of TLS 1.2 or higher where applicable.

- Monitoring and Policy Enforcement: Continuous monitoring for unusual network activities and strict adherence to security policies will help in identifying and mitigating threats early.

Additional Insights

- The assessment was conducted under the constraints typical of a black-box approach, meaning some vulnerabilities might remain undetected due to the lack of internal system knowledge.

- The report's findings underscore the importance of regular security assessments, timely updates, and proactive security management to prevent exploitation.

Business Consequences

- Implementing the suggested mitigations will require coordination across IT operations, potentially impacting service availability during upgrades or configuration changes.

- However, neglecting these vulnerabilities could lead to significant breaches, data loss, or service disruptions from external attacks.

In summary, this security assessment reveals significant areas of concern that require urgent attention. The organization should prioritize these findings, allocate resources for remediation, and consider enhancing their security practices to safeguard against future threats.