# Vulnerability Assessment and Penetration Testing Report

Date of Assessment: July 24, 2025
Report Date: July 25, 2025

## 1. Executive Summary

### 1.1. Overview

A vulnerability assessment and penetration test was conducted on two key systems within the environment: a Windows 10 host (`172.31.0.54`) and an Ubuntu Linux host (`172.31.15.88`). The assessment revealed a total of **14 vulnerabilities** requiring remediation across both systems. The findings point to critical and high-risk security gaps related to insecure configurations, outdated protocols, and unpatched software, which expose the organization to significant cyber threats.

### 1.2. Overall Risk Rating: High

The overall risk to the environment is rated as **High**. This is driven by the presence of multiple high-severity vulnerabilities on both systems, most notably the use of default credentials for SNMP services and the support for weak, outdated encryption protocols. A successful compromise of either system could lead to a significant data breach, lateral movement within the network, and a complete loss of system integrity.

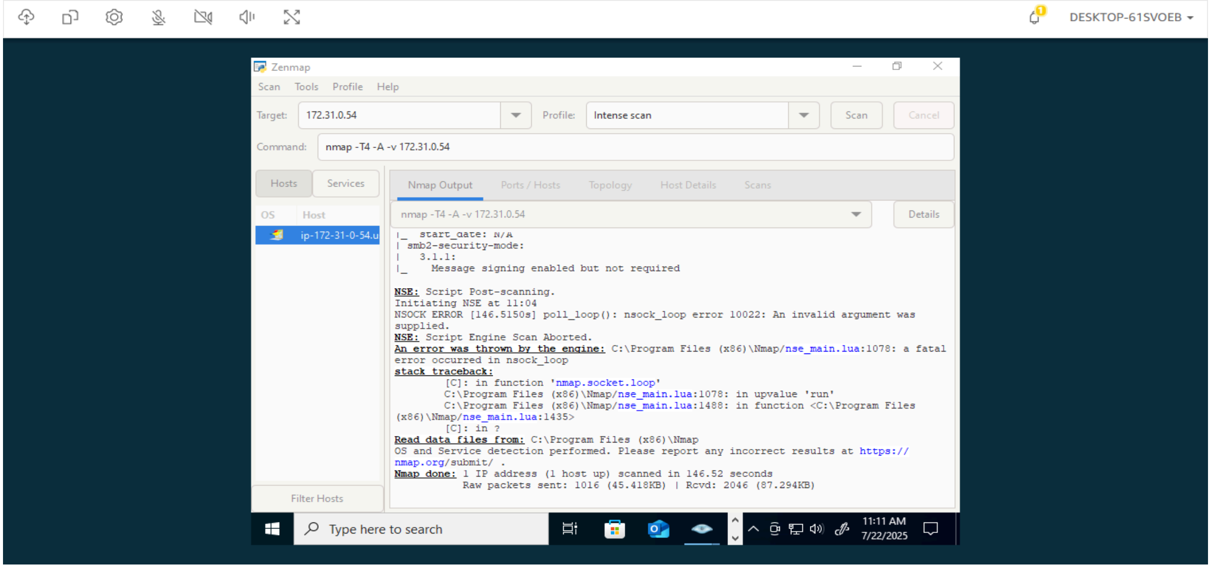
### 1.3. Consolidated Vulnerability Summary

The chart below provides a consolidated view of all identified vulnerabilities across both hosts, categorized by severity.

| Severity | Windows Count | Ubuntu Count | Total Count |
|---|---|---|---|
| Critical | 0 | 0 | 0 |
| High | 2 | 1 | 3 |
| Medium | 5 | 5 | 10 |

| | | | |
|---|---|---|---|
| Low | 0 | 1 | 1 |
| Total | 7 | 7 | 14 |

Windows Host (`172.31.0.54`)



Target: 172.31.0.54

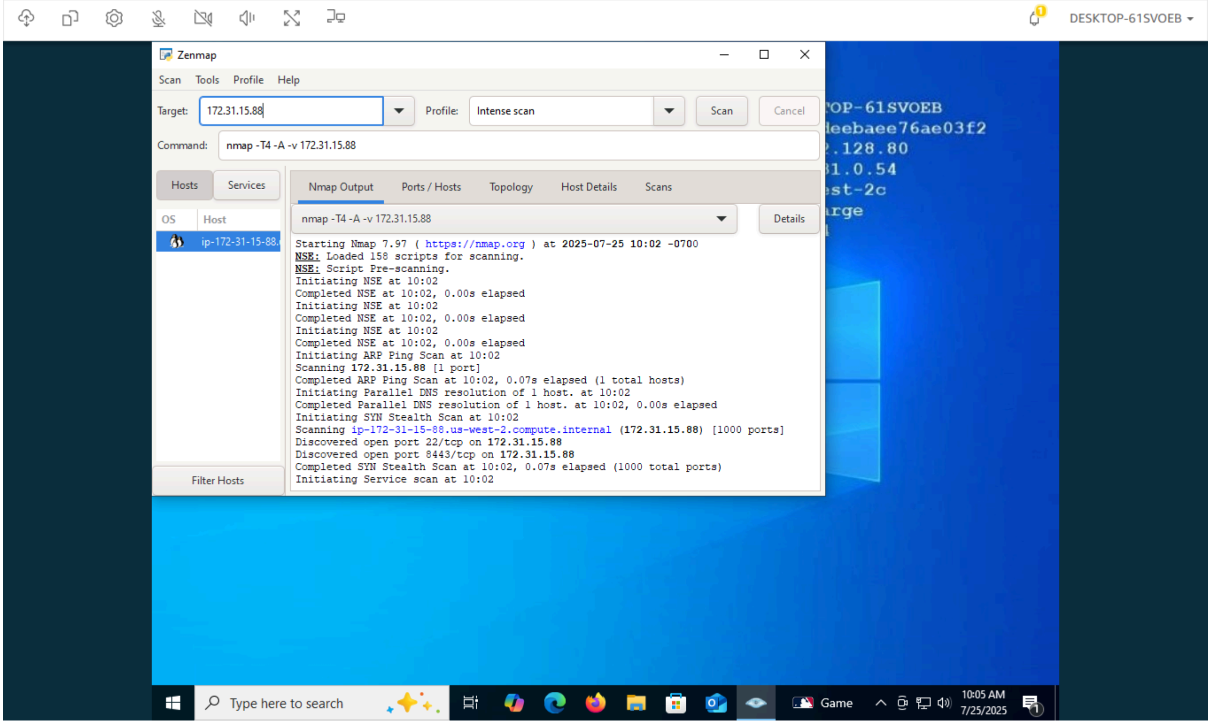
Profile: Intense scan

Command: nmap -T4 -A -v 172.31.0.54

```
nmap -T4 -A -v 172.31.0.54
|_  start_date: N/A
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 11:04
NSOCK ERROR [146.5150s] poll_loop(): nsock_loop error 10022: An invalid argument was
supplied.
NSE: Script Engine Scan Aborted.
An error was thrown by the engine: C:\Program Files (x86)\Nmap/nse_main.lua:1078: a fatal
error occurred in nsock_loop
stack traceback:
        [C]: in function 'nmap.socket.loop'
        C:\Program Files (x86)\Nmap/nse_main.lua:1078: in upvalue 'run'
        C:\Program Files (x86)\Nmap/nse_main.lua:1488: in function <C:\Program Files
(x86)\Nmap/nse_main.lua:1435>
        [C]: in ?
Read data files from: C:\Program Files (x86)\Nmap
OS and Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 146.52 seconds
           Raw packets sent: 1016 (45.418KB) | Rcvd: 2046 (87.294KB)
```

Ubuntu Host (`172.31.15.88`)



Target: 172.31.15.88

Profile: Intense scan

Command: nmap -T4 -A -v 172.31.15.88

```
nmap -T4 -A -v 172.31.15.88
Starting Nmap 7.97 ( https://nmap.org ) at 2025-07-25 10:02 -0700
NSE: Loaded 158 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:02
Completed NSE at 10:02, 0.00s elapsed
Initiating NSE at 10:02
Completed NSE at 10:02, 0.00s elapsed
Initiating NSE at 10:02
Completed NSE at 10:02, 0.00s elapsed
Initiating ARP Ping Scan at 10:02
Scanning 172.31.15.88 [1 port]
Completed ARP Ping Scan at 10:02, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:02
Completed Parallel DNS resolution of 1 host. at 10:02, 0.00s elapsed
Initiating SYN Stealth Scan at 10:02
Scanning ip-172-31-15-88.us-west-2.compute.internal (172.31.15.88) [1000 ports]
Discovered open port 22/tcp on 172.31.15.88
Discovered open port 8443/tcp on 172.31.15.88
Completed SYN Stealth Scan at 10:02, 0.07s elapsed (1000 total ports)
Initiating Service scan at 10:02
```

## 1.4. Key Recommendations

The following strategic initiatives should be prioritized to address the most critical risks identified across the environment:

1. Eliminate Insecure Defaults: Immediately change the default "public" SNMP community string on both the Windows and Ubuntu hosts. If SNMP is not essential, the service should be disabled.
2. Modernize Cryptographic Standards: Systematically disable weak and deprecated protocols and ciphers across all services. This includes disabling TLS 1.0, TLS 1.1, and Triple-DES (3DES) ciphers on the Windows host.
3. Implement a Patch Management Program: Address known vulnerabilities by applying security patches for all operating systems and services, particularly for OpenSSH and CUPS on the Ubuntu host to mitigate the Terrapin and printer registration flaws.
4. Enforce Strong Authentication: Replace all self-signed SSL certificates with certificates from a trusted authority. Additionally, enforce Network Level Authentication (NLA) for RDP on the Windows host to prevent pre-authentication attacks.

# 2. Technical Report

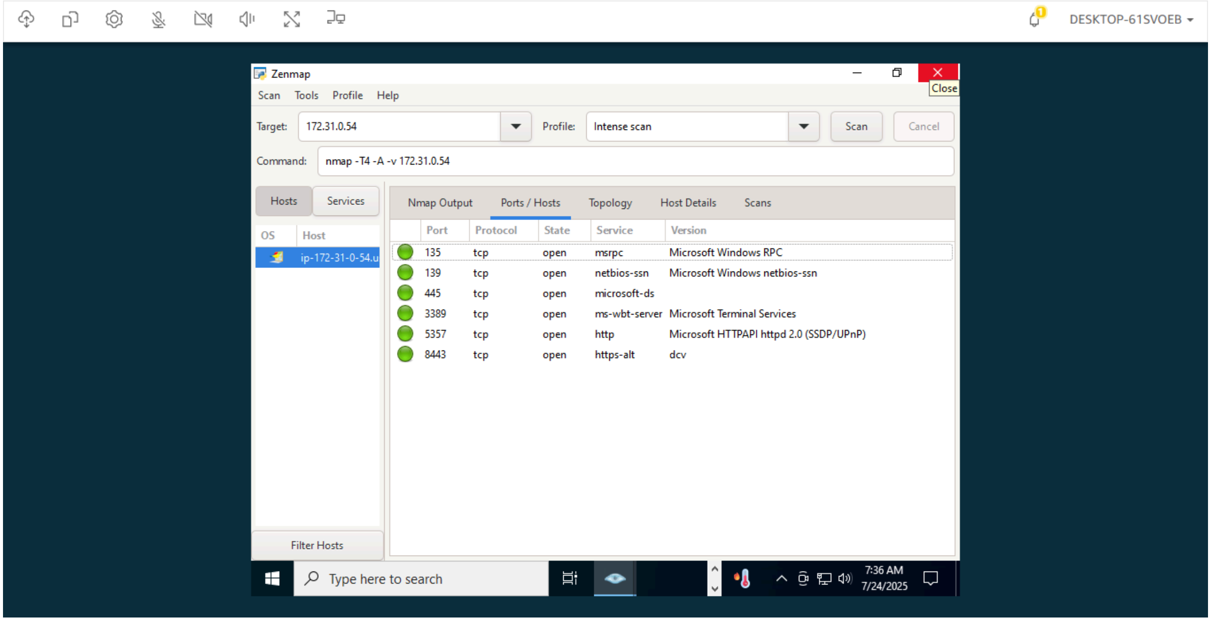
## 2.1. Windows Host (`172.31.0.54`)

### High-Severity Vulnerabilities

| | |
|---|---|
| **Vulnerability Title** | SSL Medium Strength Cipher Suites Supported (SWEET32) |
| **Severity** | High (CVSS: 7.5) |
| **Description** | The host supports Triple-DES ciphers, which are vulnerable to the SWEET32 birthday attack. This allows a man-in-the-middle attacker to recover plaintext data from long-duration encrypted sessions. |
| **Impact** | An attacker could decrypt sensitive information, such as login credentials or confidential data, by capturing and analyzing encrypted traffic. |
| **Proof of Concept** | Nessus plugin 42873 detected the use of 3DES cipher suites on ports 3389 and 8443. The Nmap scan below confirms the open ports. |
| **Remediation** | Reconfigure affected services to disable support for all 64-bit block ciphers. Prioritize strong ciphers like AES-GCM. |

| | |
|---|---|
| **Vulnerability Title** | SNMP Agent Default Community Name (public) |
| **Severity** | High (CVSS: 7.5) |
| **Description** | The SNMP service is configured with the default "public" community string, allowing any unauthenticated remote user to query system and network information. |
| **Impact** | An attacker can perform detailed reconnaissance to map the network and plan more targeted attacks. |
| **Proof of Concept** | Nessus plugin 41028 confirmed the ability to query the SNMP agent with the "public" string. |
| **Remediation** | Change the default community string to a strong, unique value or disable the SNMP service if not required. |

Evidence: Nmap Intense Scan showing open ports and services on `172.31.0.54`.



Target: 172.31.0.54

Profile: Intense scan

Command: nmap -T4 -A -v 172.31.0.54

| Port | Protocol | State | Service | Version |
|---|---|---|---|---|
| 135 | tcp | open | msrpc | Microsoft Windows RPC |
| 139 | tcp | open | netbios-ssn | Microsoft Windows netbios-ssn |
| 445 | tcp | open | microsoft-ds | |
| 3389 | tcp | open | ms-wbt-server | Microsoft Terminal Services |
| 5357 | tcp | open | http | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP) |
| 8443 | tcp | open | https-alt | dcv |

### Medium-Severity Vulnerabilities

- TLS Version 1.0 / 1.1 Protocol Detection (CVSS 6.5): Legacy TLS versions with known weaknesses are enabled on ports 3389 and 8443.

- SSL Certificate Cannot Be Trusted / Self-Signed (CVSS 6.5): Services on ports 3389 and 8443 use self-signed certificates, enabling man-in-the-middle attacks.
- Terminal Services Doesn't Use Network Level Authentication (NLA) (CVSS 4.0): RDP is not configured to require NLA, exposing it to pre-authentication attacks and brute-forcing.

## 2.2. Ubuntu Host (`172.31.15.88`)

### High-Severity Vulnerabilities

| | |
|---|---|
| **Vulnerability Title** | SNMP Agent Default Community Name (public) |
| **Severity** | High (CVSS: 7.5) |
| **Description** | The SNMP service is configured with the default "public" community string, allowing unauthenticated information disclosure. |
| **Impact** | An attacker can gather sensitive system and network details to facilitate further attacks. |
| **Proof of Concept** | Nessus plugin 41028 confirmed the ability to query the SNMP agent with the "public" string. |
| **Remediation** | Change the default community string to a strong, unique value or disable the SNMP service if not required. |

### Medium-Severity Vulnerabilities

| | |
|---|---|
| **Vulnerability Title** | SSH Terrapin Prefix Truncation Weakness |
| **Severity** | Medium (CVSS: 5.9) |
| **Description** | The SSH service is vulnerable to the Terrapin attack (CVE-2023-48795), allowing a man-in-the-middle attacker to downgrade connection security by truncating extension negotiation messages. |

| | |
|---|---|
| **Impact** | An attacker could disable certain security features in OpenSSH extensions, weakening the security of the SSH connection. |
| **Proof of Concept** | Nessus plugin 187315 detected that the SSH server supports vulnerable cipher modes and lacks the required counter-measures. |
| **Remediation** | Update the OpenSSH server and client to a patched version (e.g., OpenSSH 9.6 or later) or disable the vulnerable ciphers. |

- SSL Certificate Cannot Be Trusted / Self-Signed / Expired (CVSS 6.5): The certificate on port 8443 is self-signed and expired, enabling man-in-the-middle attacks.
- CUPS cups-browsed Remote Unauthenticated Printer Registration (CVSS 5.3): An unauthenticated attacker can register printers on the CUPS service due to insufficient validation.

**Low-Severity Vulnerabilities**

- ICMP Timestamp Request Remote Date Disclosure (CVSS 2.1): The host responds to ICMP timestamp requests, revealing the system time, which could aid time-based attacks.