Vulnerability Scanning a Target Machine

Jackson McCullough

August 2025

1 Preface

This report presents a vulnerability scan to focus on possible solutions, analysis, and management of vulnerabilities found. The target machine was a misconfigured Linux system that was intentionally designed to be vulnerable. This machine is a machine called "Vulnix" that was taken from **Vulnhub**, which is a site whose goal is to provide materials such as vulnerable systems to give hands-on experience in security, networks, and computer software.

2 Setup

Using a Kali Linux machine to run the vulnerability scan, and the Vulnix machine as the vulnerable host.
The process began with running **ifconfig** to get the IP address for the address and subnet mask of the kali machine. A /24 subnet (since my Kali machine and Vulnix machine are on the same network) based on the mask to scan the whole subnet to see which IP Vulnix was working with.
I am running **Nessus**, first running the host discovery to find the IP that Vulnix is running with, then running a basic network vulnerability scan.

3 Analysis

Host discovery gave us the IP of **192.168.219.xxx**, so that was taken to run the basic network scan.
As seen, there was 42 vulnerabilities, some having multiple issues within them causing the number to go up.

The Vulnerabilities (including issues within main vulnerabilities) are totaled to:

- Critical: 7
- High: 12

- Medium: 45
- Low: 10

3.1 Critical Severity

NFS Exported Share Information Disclosure:

- CVSS: 10.0
- At least one NFS share was found accessible: port **2049**, directory **/home/vulnix**. An attacker could potentially mount this share to read or modify files remotely.
- **Solution**: Configure the NFS on the remote host to make it where only authorized hosts can mount remote shares. Also would need to create/enforce appropriate file system privileges

Canonical Ubuntu Linux SEoL (12.04.x):

- CVSS: 10.0
- Found on **TCP Port 22**, the host is running on an outdated version of Linux (Ubuntu 12.04). This means that this OS no longer receives maintenance, patches, or additional security. This gives the possibility that vulnerabilities present are, and will remain, unpatched.
- **Solution**: Simple solution of updating the host to a current version of Ubuntu that is supported

SSL Version 2 and 3 Protocol Detection:

- CVSS: 9.8
- Host is running old versions of SSL, meaning that there is very poor encryption, leaving it very vulnerable for MiTM attacks or easily decrypt any communications. Neither SSL 2.0 nor 3.0 are suitable for secure communication. There are five instances of this issue on **Ports 995, 993, 143, 110, 25**
- **Solution**: Disable any SSL version and upgrade to TLS 1.2 or higher for better security and encryption.

3.2 High Severity

rlogin Service Detection:

- CVSS: 7.5 (with an EPSS of .50, so likely chance of exploitation)

- rlogin service detected running on the host. It is a software very vulnerable to being exploited, especially for MiTM attacks, especially since data passed between the client and server are not encrypted. Could be possible to bypass authentication if the host was also vulnerable to TCP number guessing or IP spoofing. found on port **513/tcp/login**.
- **Solution:** The best solution here would be to disable the rlogin service and use SSH instead.

NFS Shares World Readable

- CVSS: 7.5
- NFS server is exporting one or more shares with no restrictions of access(detected on port **2049 / tcp / rpc-nfs_acl**), so anyone who connects to this server is able to access and read the contents of the directory.
- **Solution:** Apply restrictions on the NFS server to improve security, including:
  - **Mount access control:** restrict which clients can mount NFS shares, allowing only trusted clients to prevent unauthorized access.
  - **Root access control:** enable **root_squash** so that root users on clients do not have root privileges on the server.
  - **System updates:** regularly patch NFS daemons and client systems to maintain secure configurations and patch management.

SSL Medium Strength Cipher Suites Supported (SWEET32)

- CVSS: 7.5
- Host supports SSL ciphers that are medium strength (key length is [64,112) bits, or uses 3DES encryption), this leaves the ciphers susceptible to birthday attacks. This was found on messaging service ports **(IMAP, SMTP, POP3)**.
- **Solution:** Simply just need to avoid using medium-strength ciphers, so removing those, and reconfigure the applications to using AES. Also updating any SSL or TLS libraries so they will not allow by default lower-strength encryptions

OpenSSL Heartbeat Information Disclosure (Heartbleed):

- CVSS: 7.5(however, EPSS score of .94)
- When a heartbeat request was sent, server appears to be affected by an out-of-bound read flaw. Meaning that the OpenSSL library is out of date(since older versions do not validate length of heartbeat requests),

which means an attacker could configure their own special heartbeat request and possibly get leaked data from the RAM(up to 64KB), with that data having the possibility of being sensitive information. This was also found on the messaging service ports.

- **Solution:** Upgrading to OpenSSL 1.0.1g or later will fix this, this is when the vulnerability has been patched and will not be an issue. This vulnerability can be abused as long as the older versions are in use.

3.3 Medium Severity

There were 45 medium-severity vulnerabilities, so they will be grouped and solved whole form.

- CVSS: 4.3-6.5
- There was a total of 45 medium-severity vulnerabilities. They all revolved around issues with **SSL/TLS, OpenSSL**, including certificate misconfigurations, weak hashing algorithms, and risks that could enable MiTM attacks.
- **Solution:** A complete revamp of the SSL/TLS configuration is needed in order to maintain proper security, with fixes as follows:
  - Upgrade Protocols
    - Disable SSL, TLS 1.0, and TLS 1.1
    - Only allow TLS 1.2 and TLS 1.3
  - Harden Cipher Suites
    - Disable weak ciphers (RC4, 3DES, MD5, etc.)
    - Use strong ciphers (AES-GCM, CHACHA20)
  - Deploy Valid Certificates
  - Monitor and Renew Certificates Regularly

There was one vulnerability that was medium-severity that was apart from SSL/TLS:
Finger Service Remote Information Disclosure:

- CVSS: 5.0
- This service helps with system logging, showing who is currently logged into the remote system. This service gives attackers useful information about the user
- **Solution:** Simply disabling this service can patch this vulnerability.

3.4 Low Severity

SSH Issues: A lot of the low-severity vulnerabilities come from SSH issues, like weak cipher modes, hashing algorithms, and MAC algorithms.

- CVSS: 2.6-3.7
- **Solutions:** The best solutions here will be strengthening the security of algorithm and encryption with the SSH. Such as :
  - Enabling CTR or GCM cipher mode rather than CBC
  - Enabling HMAC-SHA-256 or AES-GCM(with GMAC) rather than the currently enabled MD5 or 96-bit MAC algorithms
  - Disabling weak algorithms as a whole

4 Conclusion

Overall, the greatest portion of the vulnerabilities comes from the SSL/TLS that the system has been using over time. This highlights the importance of regularly updating cryptographic protocols and enforcing secure configurations, as well as keeping all libraries and the system as a whole patched and up-to-date.