Name : Patel Dhruv Nirmalkumar
Email : dhruvpatel.00700@gmail.com
Phone : 9426176903
Task : 15

Vulnerability Assessment Report

Executive Summary

This report presents the findings of a vulnerability assessment conducted on the target system (localhost – 127.0.0.1) running **Ubuntu 22.04 LTS**.

The assessment identified vulnerabilities ranging from **Critical to Medium severity**, primarily caused by:

- Outdated software components
- Missing security patches
- Suboptimal security configurations

The most significant risks identified:

- An outdated **OpenSSH server** vulnerable to Remote Code Execution (RCE)
- An outdated Linux kernel with multiple privilege escalation vulnerabilities

Immediate remediation is strongly recommended to reduce the risk of system compromise.

---

1. Scope and Methodology

1.1 Scope

The assessment scope was limited to:

- Local system (127.0.0.1)
- Network services
- System configurations
- Installed packages and patch levels

The objective was to identify security weaknesses exploitable by attackers with local or network access.

1.2 Methodology

The following tools and techniques were used:

• Nmap (Network Mapper)

- Port scanning
- Service version detection
- OS detection
- Vulnerability script scanning

• Lynis

- System auditing
- Security misconfiguration detection
- Hardening recommendations

• Manual Analysis

- Review of scan outputs
- CVE correlation
- CVSS scoring verification
- Cross-referencing Ubuntu Security Notices (USN)

---

2. Findings

2.1 VULN-001: Outdated OpenSSH Server

Description

The system is running **OpenSSH 8.9p1**, which is affected by:

- **CVE-2024-6387** (regreSSHion)
- Critical Remote Code Execution (RCE)
- Signal handler race condition in `sshd`
- Allows unauthenticated remote attackers to execute arbitrary code as **root**

Severity

Critical

CVSS v3.1 Score

9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Impact

- Full system compromise
- Root-level code execution
- Complete confidentiality, integrity, and availability loss

2.2 VULN-002: Outdated Linux Kernel

Description

The system is running **Linux kernel 6.1.102**.

Ubuntu Security Notices (USN) indicate multiple vulnerabilities affecting the 6.1.x series for Ubuntu 22.04 LTS, including:

- Privilege escalation
- Denial of service
- Information disclosure

Severity

High

CVSS v3.1 Score

Typically around **7.8 (High)**

Impact

- Local privilege escalation
- Kernel-level compromise
- Service disruption

2.3 VULN-003: VNC Authentication Enabled

Description

- VNC service running on **port 5900**
- Protocol version 3.8
- Uses VNC authentication

While not inherently vulnerable, risks include:

- Weak password usage
- Brute-force attacks
- Potential authentication bypass (e.g., CVE-2006-2369 for RealVNC)

Severity

Medium

CVSS v3.1 Score

5.3

Impact

- Unauthorized remote desktop access
- Data exposure
- Session hijacking

2.4 VULN-004: Weak SSH Configuration

Description

The Lynis audit identified configuration weaknesses in `/etc/ssh/sshd_config`, including:

- AllowTcpForwarding enabled
- Default SSH port (22)
- PermitRootLogin possibly enabled
- High authentication attempt limits
- X11 forwarding enabled

These are not direct vulnerabilities but increase attack surface.

Severity

Medium

CVSS v3.1 Score

4.3

Impact

- Easier brute-force attacks
- Lateral movement
- Persistence opportunities

2.5 VULN-005: Missing Security Patches

Description

Pending security updates detected via `apt-get upgrade -s`.

Affected packages may include:

- libpython3.10
- gnupg
- libglib2.0
- openssl
- libxml2
- mysql-client
- openjdk-11-jre
- xserver-xorg-core

Unpatched systems accumulate risk over time.

Severity

High

Impact

- Exposure to known CVEs
- Potential remote/local exploitation
- Increased attack surface

3. Risk Classification

Severity	Description
Critical	Immediate action required. Exploitation leads to full system compromise.
High	Significant risk. May result in privilege escalation or data breach.
Medium	Moderate risk. Could allow unauthorized access or service disruption.
Low	General hardening recommendations.

4. Remediation Recommendations

4.1 Critical Findings

VULN-001 – Outdated OpenSSH

Immediate Actions:

```
sudo apt update
sudo apt upgrade openssh-server
```

Additional controls:

- Restrict SSH access to trusted IP addresses
- Disable SSH exposure to the internet if unnecessary
- Implement firewall rules
- Consider Fail2Ban

4.2 High Findings

VULN-002 – Outdated Kernel

```
sudo apt update
sudo apt upgrade
sudo reboot
```

Ensure the new kernel is loaded after reboot.

VULN-005 – Missing Security Patches

- Establish a regular patching schedule
- Enable unattended security updates
- Monitor Ubuntu Security Notices

4.3 Medium Findings

VULN-003 – VNC Service

Recommended actions:

- Identify exact VNC server version
- Upgrade if outdated
- Use strong passwords
- Tunnel VNC over SSH
- Restrict access via firewall
- Disable if not required

VULN-004 – Harden SSH Configuration

Update /etc/ssh/sshd_config:

```
AllowTcpForwarding no
ClientAliveCountMax 2
Compression no
LogLevel VERBOSE
MaxAuthTries 3
MaxSessions 2
PermitRootLogin no
TCPKeepAlive no
X11Forwarding no
AllowAgentForwarding no
```

Optional:

- Change SSH port from 22 to a non-standard port

Restart SSH:

```
sudo systemctl restart sshd
```
