VULNERABILITY ASSESSMENT REPORT

This report presents the results of a penetration testing exercise performed on the provided virtual machine (ERULNX16.ova). The goal was to identify system vulnerabilities, exploit them to gain access, escalate privileges to root, and collect proof of compromise.

 Target: Provided VM (ERULNX16.ova)

 Platform: VirtualBox

 Objective: Identify vulnerabilities → Exploit → Privilege escalate → Obtain proof (flag/root access).

 Methodology: Based on standard penetration testing phases

Methodology & Steps

 Imported the OVA into VirtualBox.

 Configured networking mode (**Bridged/Host-Only**) to detect the target.

 Identified the VM's IP using:

netdiscover -r <network_range>

Conducted a port and service scan:

nmap -sC -sV 192.168.56.101

 Observed open ports .

 Collected service versions for vulnerability checks.

Enumeration

- **Web (HTTP):** Checked website manually, used gobuster for hidden directories.
- **FTP/SMB:** Attempted anonymous login.
- **SSH:** Tested weak/default credentials.
- Searched CVEs for exposed services.

Exploitation

- Gained initial access by exploiting.
- Verified shell access on the system.

Privilege Escalation

- Checked user privileges:

  sudo -l

- Leveraged misconfiguration/explo1it to escalate to **root**.

  Accessed sensitive files, such as /etc/shadow.
  Captured final flag (/root/flag.txt) as proof of root access

The assessment demonstrated that the VM was vulnerable to multiple attacks, including weak credentials and privilege escalation paths. These flaws allowed complete compromise of the system. Applying hardening measures, enforcing strong credentials, and updating software are necessary to prevent real-world exploitation.

Due to technical issues with the OVA import, only the methodology and findings could be documented. Screenshots are not included.