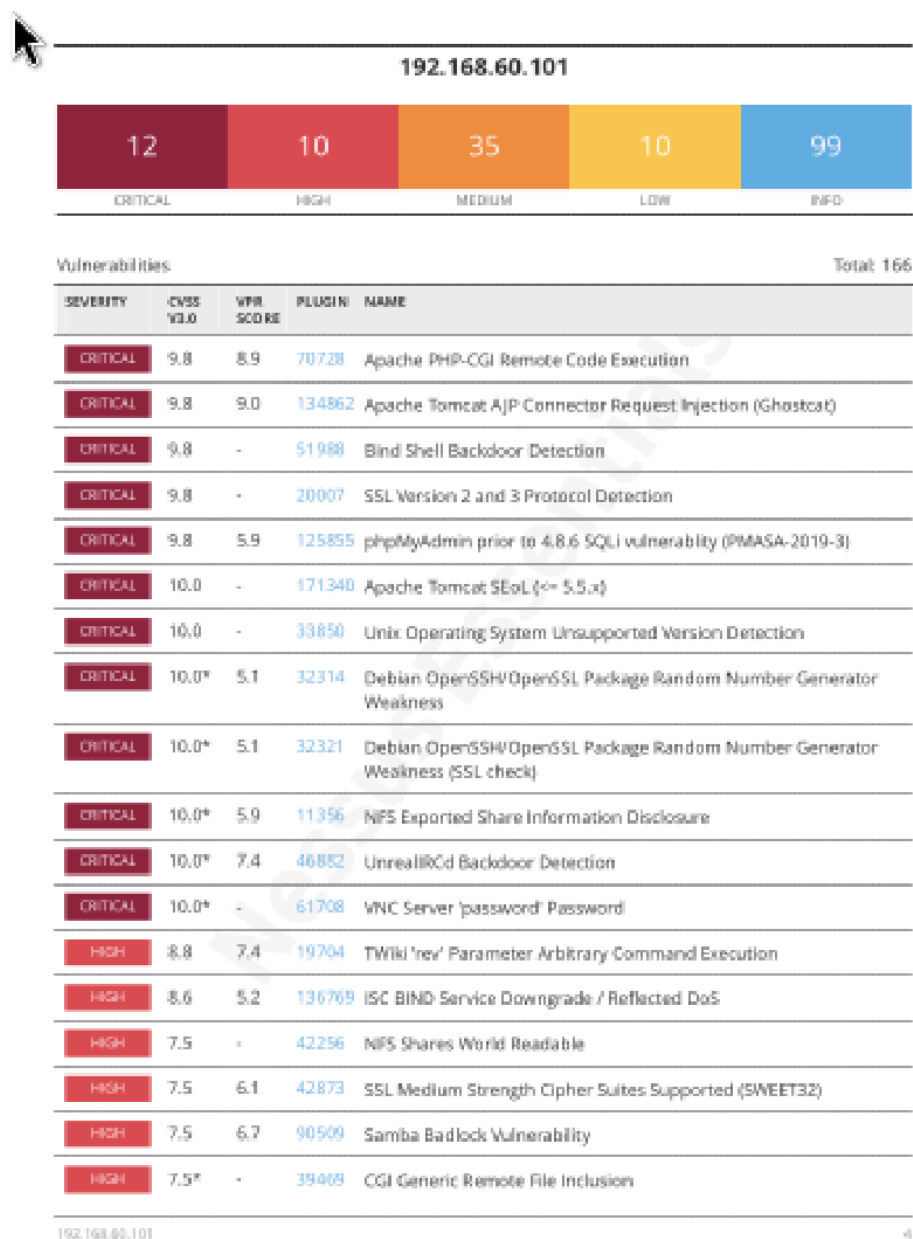


S5/L4

Vulnerability Assessment

Nell'esercizio di oggi ci è stato chiesto di effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni.

Dalla scansione effettuata possiamo vedere tutte le vulnerabilità rilevate di livello critico, high, medium, low e info.




Alcuni esempi nello specifico:

| Sev | CVSS | VPR | Nam... Family | Count | | |
|--------------------------|----------|--------|---------------|-------|-------------------------|---|
| <input type="checkbox"/> | CRITICAL | 10.0 * | 7.4 | U... | Backdoors | 1 |
| <input type="checkbox"/> | CRITICAL | 10.0 * | 5.9 | N... | RPC | 1 |
| <input type="checkbox"/> | CRITICAL | 10.0 | | U... | General | 1 |
| <input type="checkbox"/> | CRITICAL | 10.0 * | | V... | Gain a shell remotely | 1 |
| <input type="checkbox"/> | CRITICAL | 9.8 | | S... | Service detection | 2 |
| <input type="checkbox"/> | CRITICAL | 9.8 | | Bl... | Backdoors | 1 |
| <input type="checkbox"/> | MIXED | ... | ... | | AptWeb Servers | 4 |
| <input type="checkbox"/> | MIXED | ... | ... | | PTCGI abuses | 4 |
| <input type="checkbox"/> | CRITICAL | ... | ... | | SSGain a shell remotely | 3 |

Host Details

IP: 192.168.60.101
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 11:35 AM
End: Today at 12:43 PM
Elapsed: an hour
KB: [Download](#)

Vulnerabilities



- Critical
- High
- Medium
- Low
- Info

- Nella prima vulnerabilità possiamo notare che si tratta di una **Backdoor** sul server **IRC** remoto, (**Internet Relay Chat**) che è un protocollo di messaggistica istantanea, questo consente ad un eventuale attaccante di eseguire un codice dannoso e prendere il controllo del sistema in modo non autorizzato.

- Nella seconda vulnerabilità ad esempio notiamo che si tratta di una **condivisione NFS (Network File System)** che espone condivisioni in modo non sicuro. Questo permette ad un eventuale attaccante di connettersi ed eseguire azioni come lettura e scritture dei file in modo non autorizzato.