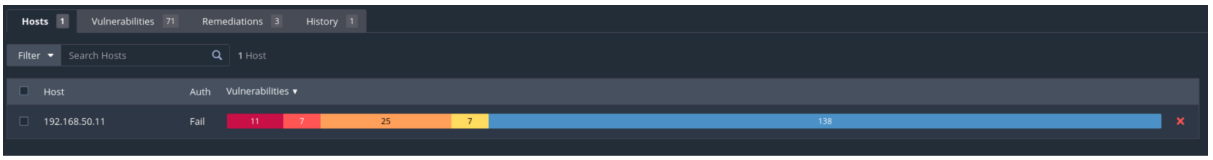
REPORT S5/L3

Obiettivo:

Esercizio Traccia Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

1. INFORMAZIONI GENERALI

Target (Metasploitable): IP 192.168.50.11
Porte: solo le porte comuni
Tipo di scansione: Basic Network Scan
Vulnerabilità trovate: 71
Livello di rischio globale: critico



2. VULNERABILITA' CRITICHE SELEZIONATE(3)

Data l'elevata quantità di vulnerabilità riscontrate, sono state isolate le tre criticità che permettono un compromesso immediato e totale del sistema

Porta	Servizio	Vulnerabilità	Gravità	Descrizione	Soluzione
6667	TCP	UNREALLRCD BACKDOOR DETECTION	CRITICAL	Il server IRC remoto è una versione di UnrealIRCd con una backdoor che consente a un aggressore di eseguire codice arbitrario sull'host interessato.	Scaricare nuovamente il software, verificarlo utilizzando i checksum MD5/SHA1 pubblicati e reinstallarlo.

80	TCP	CANONICAL UBUNTU LINUX SEoL(8.04.x)	CRITICAL	Secondo la sua versione, Canonical Ubuntu Linux è la 8.04.x. Pertanto, non è più supportato dal suo fornitore o provider.	Aggiorna a una versione di Canonical Ubuntu Linux attualmente supportata.
5900	TCP	VNC SERVER ‘password’ PASSWORD	CRITICAL	Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password". Un aggressore remoto e non autenticato potrebbe sfruttare questa vulnerabilità per assumere il controllo del sistema.	Proteggere il servizio VNC con una password complessa.

3. Conclusioni e Raccomandazioni

L'elevato numero di vulnerabilità (71) è riconducibile principalmente all'obsolescenza del sistema operativo.

Azioni Prioritarie:

1. **Bonifica Immediata**: Cambiare la password del servizio VNC e chiudere la porta 6667 per neutralizzare la backdoor.
2. **Migrazione**: Poiché Ubuntu 8.04 non riceve più aggiornamenti di sicurezza, è indispensabile migrare i servizi su una distribuzione moderna.
3. **Hardening**: Implementare politiche di password forti e disabilitare i servizi non necessari rilevati durante la scansione.