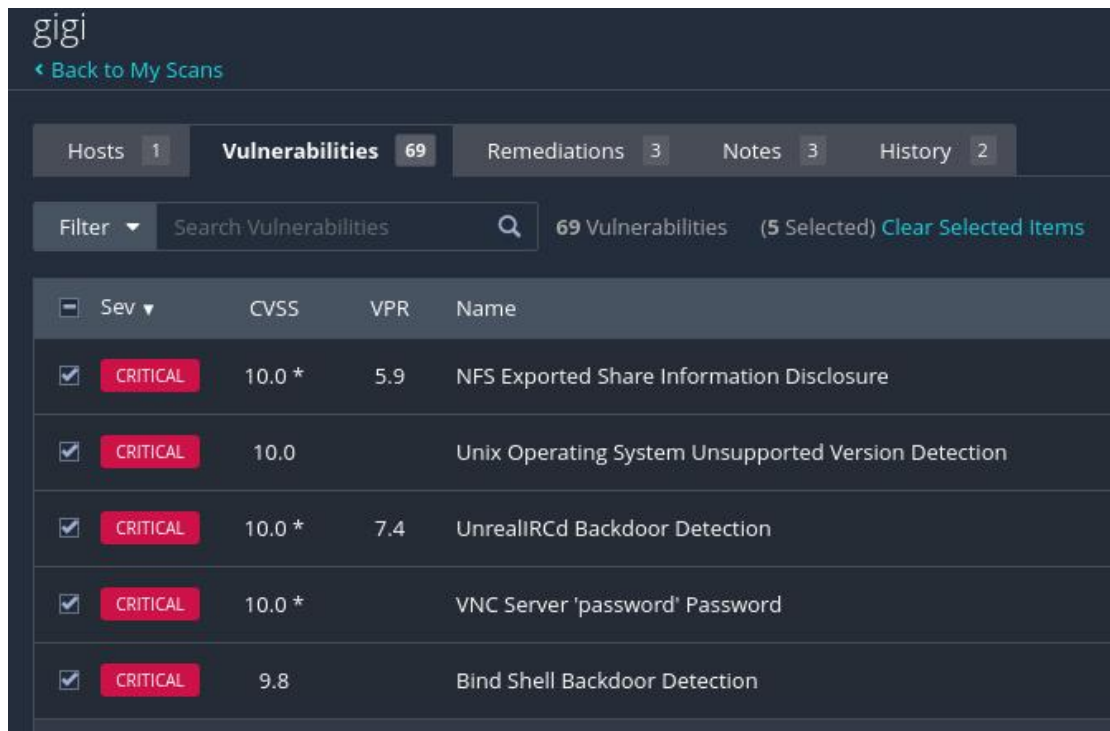


SCAN IP VULNERABILITIES



The screenshot shows the GIGI vulnerability scanner interface. At the top, there's a navigation bar with 'Back to My Scans'. Below it, a tab bar shows 'Hosts 1', 'Vulnerabilities 69', 'Remediations 3', 'Notes 3', and 'History 2'. A search bar is present with the text 'Search Vulnerabilities'. Below the search bar, a table lists vulnerabilities. The table has columns for 'Sev', 'CVSS', 'VPR', and 'Name'. Five vulnerabilities are selected, each with a checkbox and a 'CRITICAL' label. The selected vulnerabilities are: NFS Exported Share Information Disclosure (CVSS 10.0, VPR 5.9), Unix Operating System Unsupported Version Detection (CVSS 10.0), UnrealIRCd Backdoor Detection (CVSS 10.0, VPR 7.4), VNC Server 'password' Password (CVSS 10.0), and Bind Shell Backdoor Detection (CVSS 9.8).

Sev	CVSS	VPR	Name
<input checked="" type="checkbox"/> CRITICAL	10.0 *	5.9	NFS Exported Share Information Disclosure
<input checked="" type="checkbox"/> CRITICAL	10.0		Unix Operating System Unsupported Version Detection
<input checked="" type="checkbox"/> CRITICAL	10.0 *	7.4	UnrealIRCd Backdoor Detection
<input checked="" type="checkbox"/> CRITICAL	10.0 *		VNC Server 'password' Password
<input checked="" type="checkbox"/> CRITICAL	9.8		Bind Shell Backdoor Detection

- **NFS EXPORTED SHARE INFORMATION DISCLOSURE:** NFS è esposto dal server remoto che potrebbe essere stato montato durante la scannerizzazione. Un attaccante potrebbe profittarne e usarlo sia per leggere che scrivere come host remoto. Questo fa sì che i dati privati possano essere letti da terzi ed espone a file entranti da terzi come virus o disinformazione.
- **UNIX OPEATING SYSTEM UNSUPPORTED VERSION DETECTION:** la versione attuale non è supportata dal host remoto, esponendo la sicurezza del prodotto del venditore.
- **UNREALIRCd BACKDOOR DETECTION:** IRC server è un un backdoor, questo permette che l'attaccante abbia costante accesso al dispositivo, così da poter eseguire attacchi.
- **VNC SERVER 'PASSWORD' PASSWORD:** VNC server che si trova nel host remoto possiede una password troppo semplice, Nessus è stuato capace di loggare usando "password" come password. Questo può essere usato dal attaccante come exploit per poter prendere controllo del sistema.
- **BIND SHELL BACKDOOR DETECTION:** è stata rilevata una backdoor che utilizza una "shell", la quale è in ascolto senza autorizzazione. Un attaccante potrebbe approfittarsene e usarlo per mandare dei comandi direttamente.