



VULNERABILITY SCANNER NESSUS

SCANSIONE INIZIALE

Nella fase iniziale ho eseguito la scansione sulla macchina Metasploitable, sono venute fuori diverse vulnerabilità (come si può vedere in figura), quelle che andrò a risolvere sono le seguenti:

- NFS Exported Share Information Disclosure
- VNC Server 'password' Password
- Bind Shell Backdoor Detection

The screenshot shows the Tenable Nessus Essentials interface. The main panel displays the results of a scan for a host named META. The 'Vulnerabilities' tab is selected, showing 70 vulnerabilities. The table lists the following vulnerabilities:

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0 *	5.9	NFS Exported Share Inform...	RPC	1
CRITICAL	10.0		Unix Operating System Uns...	General	1
CRITICAL	10.0 *		VNC Server 'password' Pass...	Gain a shell remotely	1
CRITICAL	9.8		Bind Shell Backdoor Detecti...	Backdoors	1
MIXED	DNS (Multiple Issues)	DNS	5
MIXED	Apache Tomcat (Multip...	Web Servers	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	SSL (Multiple Issues)	Service detection	3
HIGH	7.5		NFS Shares World Readable	RPC	1

The right sidebar shows the 'Scan Details' for the selected scan, including the policy, status, severity base, scanner, start/end times, and elapsed time. Below this is a 'Vulnerabilities' section with a pie chart showing the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

NFS Exported Share Information Disclosure

NFS è un protocollo per la condivisione di file e directory e, se non è configurato in maniera sicura, potrebbe consentire a dei malintenzionati di accedere a risorse non autorizzate. Per aggirare questo problema ho modificato il file `/etc/exports` e ho modificato l'ultima riga perché in questa c'era il simbolo «/» che sta a significare che si può montare tutto. Mettendolo a commento con il simbolo «#» ho risolto questa vulnerabilità. Infatti nella figura a destra notiamo che questo tipo di vulnerabilità non è presente in «CRITICAL».

SCAN 2

The screenshot shows the Nessus Essentials interface for a scan named 'scan3'. The 'Vulnerabilities' tab is selected, showing 63 vulnerabilities. The table lists the following vulnerabilities:

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Uns...	General	1
CRITICAL	9.8		Bind Shell Backdoor Detecti...	Backdoors	1
MIXED	DNS (Multiple Issues)	DNS	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	SSL (Multiple Issu	Plugin ID: 10205	3

The Scan Details panel on the right indicates the scan was completed at 7:50 AM on 27/10/2023, with a severity base of CVSS v3.0 and a scanner of Local Scanner.

VNC Server 'password' Password

Questa vulnerabilità riguarda il VNC server in quanto per accedervi la password è «password», questo non va bene perché è molto debole e un possibile attaccante potrebbe accedere senza problemi. Per risolvere ho usato il comando «vncpasswd» sulla macchina Metasploitable e ho inserito una password più forte.

Come si può vedere nell'immagine a destra, rifacendo un'altra scansione, questa vulnerabilità non compare più come «CRITICAL».

SCAN 3

The screenshot shows the Tenable Nessus Essentials interface. The main panel displays the results of a scan named 'scan3'. The 'Vulnerabilities' tab is selected, showing a table of 63 vulnerabilities. The table has columns for Severity (Sev), CVSS, VPR, Name, Family, and Count. The 'password' vulnerability is no longer listed as critical. The left sidebar shows folders like 'My Scans', 'All Scans', and 'Trash', and resources like 'Policies', 'Plugin Rules', and 'Terrascan'. The right sidebar shows scan details and a vulnerability distribution pie chart.

Sev	CVSS	VPR	Name	Family	Count
CRITICAL	10.0		Unix Operating System Uns...	General	1
CRITICAL	9.8		Bind Shell Backdoor Detecti...	Backdoors	1
MIXED	DNS (Multiple Issues)	DNS	4
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	SSL (Multiple Issues)	Service detection	3
HIGH	7.5 *	6.7	rlogin Service Detection	Service detection	1
HIGH	7.5 *	6.7	rsh Service Detection	Service detection	1
HIGH	7.5	6.7	Samba Badlock Vuln	SSL (Multiple Issues)	1

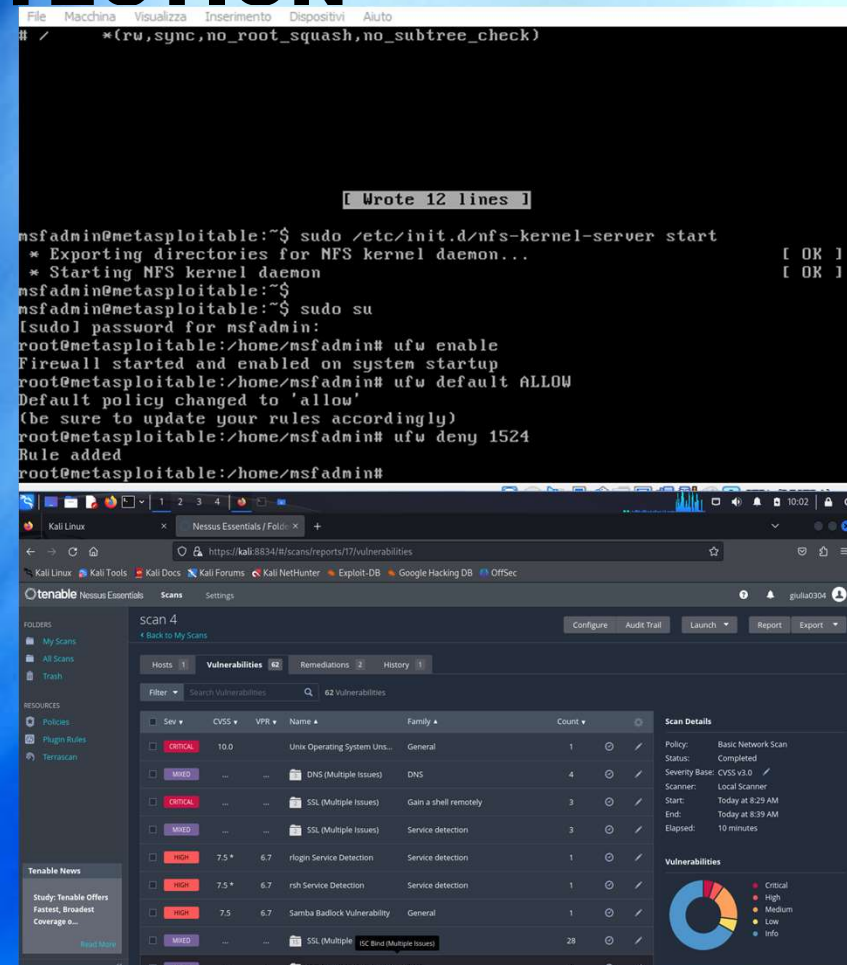
BIND SHELL BACKDOOR DETECTION

Questo tipo di vulnerabilità ci dice che una shell è in ascolto su una porta remota senza autenticazione. Un malintenzionato potrebbe sfruttare questa cosa connettendosi alla porta e prendere il controllo.

Per risolvere questa vulnerabilità ho usato dei comandi:

- «ufw enable» per attivare il firewall
- «ufw default ALLOW» che permette tutte le connessioni di base.
- «ufw deny 1524» per chiudere la seguente porta che è responsabile della backdoor.

Così facendo non risulterà più come vulnerabilità critica.



REPORT NESSUS

I PDF DEI REPORT SONO INVIATI SEPARATAMENTE

- **SCANSIONEINIZIALE.PDF**
- **SCANSIONEFINALE.PDF**