Vulnerability Scanning

L’obiettivo di questo esercizio è quello di prendere confidenza con il vulnerability scanner Nessus e comprendere come esso venga utilizzato per individuare vulnerabilità note all’interno di un sistema. La macchina scelta come target è Metasploitable, utilizzata esclusivamente per scopi didattici e di test in ambienti controllati. L’uso di Nessus consente di simulare un’attività reale di analisi della sicurezza, focalizzandosi in questo caso sulle porte di rete più comuni, ovvero quelle su cui solitamente girano i servizi maggiormente esposti.

1. Preparazione

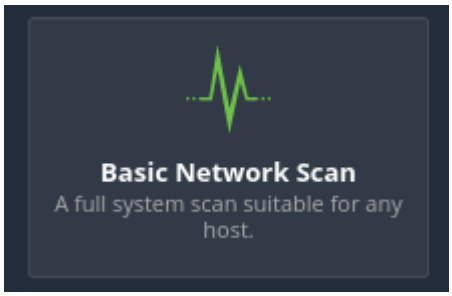
La prima macchina è Metasploitable, che funge da target della scansione. Una volta avviata, si accede alla console e si recupera il suo indirizzo IP utilizzando il comando “ ip a ”. L’indirizzo IP ottenuto è 192.168.60.10, questo indirizzo sarà quello da inserire in Nessus come obiettivo della scansione.

La seconda macchina è quella su cui è installato Nessus, quindi Kali Linux oppure direttamente il Nessus installato su Windows. Dopo aver avviato Nessus, si accede all’interfaccia web tramite browser all’indirizzo `https://kali:8834` e si effettua il login con le credenziali configurate durante l’installazione.

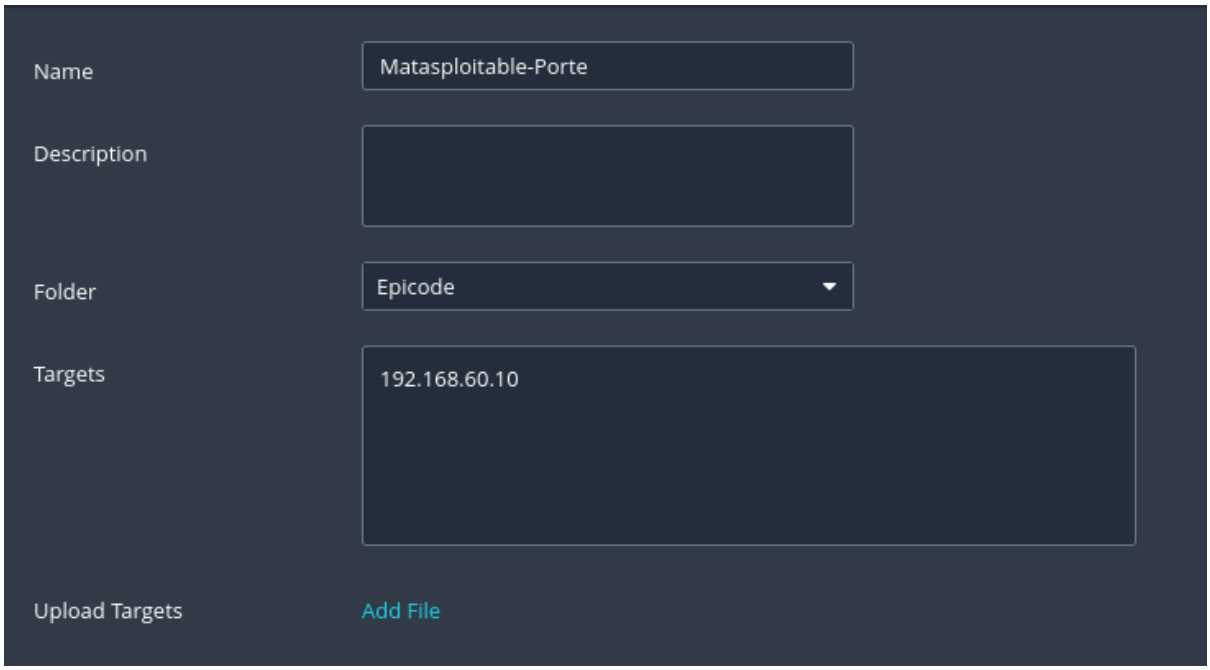
2. Configurazione della scansione in Nessus

Una volta effettuato l’accesso a Nessus, procedo alla creazione di una nuova scansione. Dalla dashboard principale seleziono l’opzione per creare una nuova scansione. A questo punto Nessus propone diversi template; per questo esercizio si può scegliere il template “Basic Network Scan” che fornisce una configurazione predefinita adatta a una scansione di rete standard. In alternativa, per un maggiore controllo, si può utilizzare

“Advanced Scan”, ma ai fini dell’esercizio il Basic Network Scan è più che sufficiente.



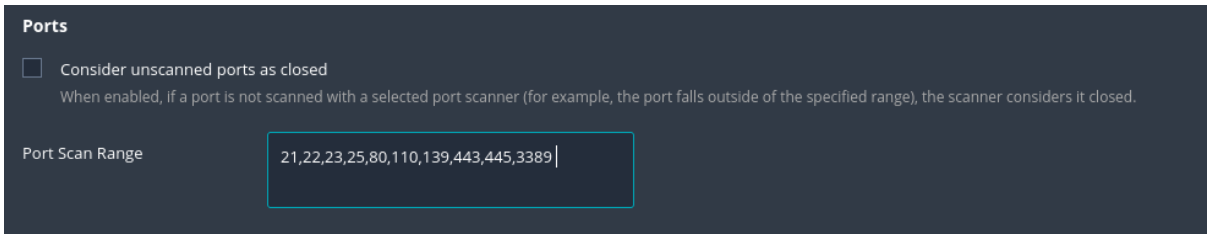
Dopo aver selezionato il template si apre la schermata di configurazione della scansione. Nel campo Name inserisco un nome significativo, ad esempio “Metasploitable – Porte”.



Nel campo Targets si inserisce l’indirizzo IP della macchina Metasploitable quindi `192.168.60.10`

A questo punto è fondamentale configurare correttamente le porte da analizzare. Nella sezione dedicata alle impostazioni avanzate, si trova l’opzione “Port scan range”. Qui non si lasciano tutte le porte, ma si specificano solo quelle indicate nell’esercizio. Il valore da inserire è il seguente:

```
21,22,23,25,80,110,139,443,445,3389
```



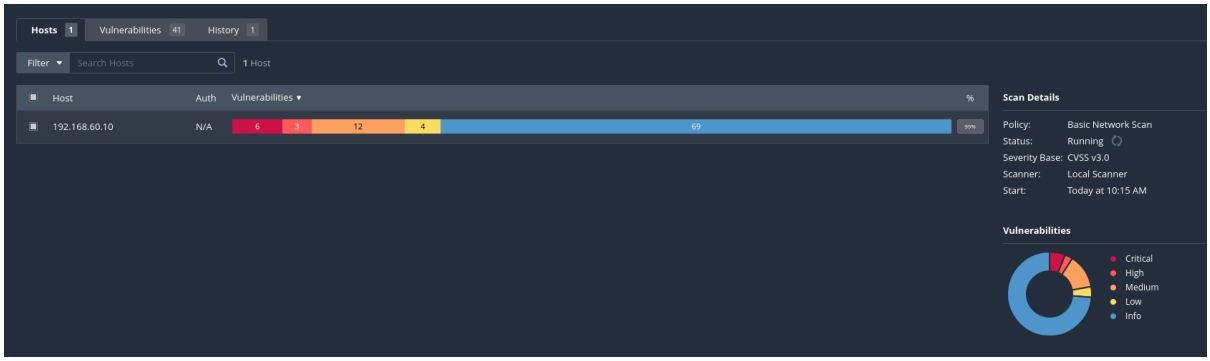
Questa configurazione dice a Nessus di limitare la scansione esclusivamente a queste porte, riducendo il tempo di scansione e focalizzandosi sui servizi più comuni come FTP, SSH, Telnet, SMTP, HTTP, POP3, SMB, HTTPS e RDP.

Una volta verificato che tutte le impostazioni siano corrette, la scansione può essere salvata.

3. Esecuzione della scansione

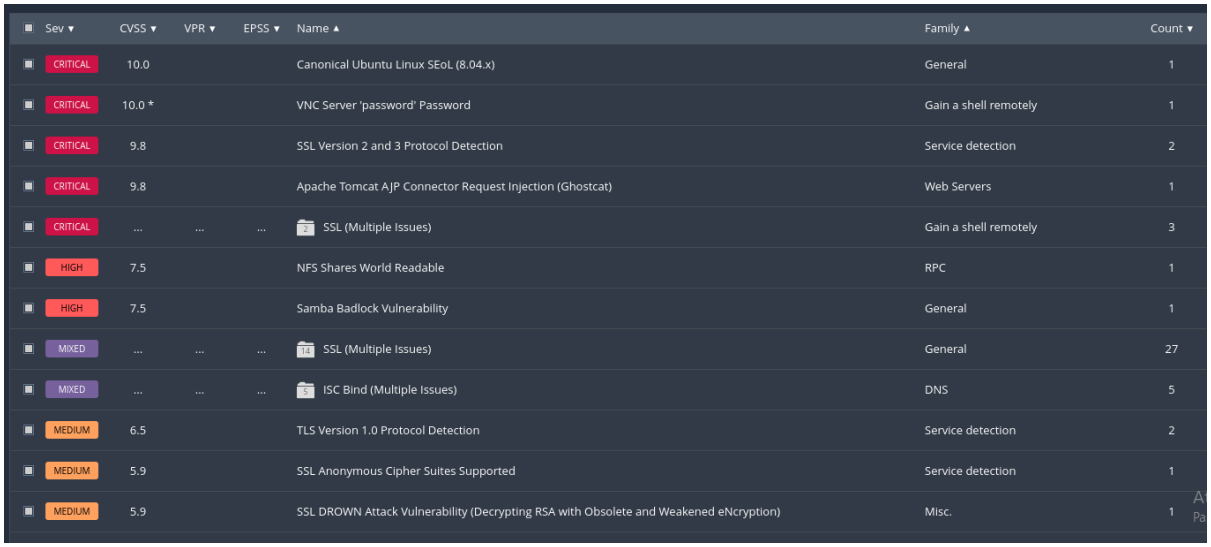
Dopo aver salvato la configurazione, dalla lista delle scansioni si seleziona quella appena creata e si avvia cliccando su “Launch”. Nessus inizia così la scansione della macchina Metasploitable.

Durante questa fase Nessus effettua diverse operazioni, verifica se le porte specificate sono aperte, identifica i servizi in ascolto su tali porte, rileva le versioni dei software e confronta queste informazioni con il proprio database di vulnerabilità note. Questo processo può richiedere diversi minuti, a seconda delle risorse disponibili e del numero di controlli eseguiti. Al termine della scansione lo stato passa da “Running” a “Completed”, indicando che l’analisi è stata completata correttamente.



4.Analisi del report di Nessus

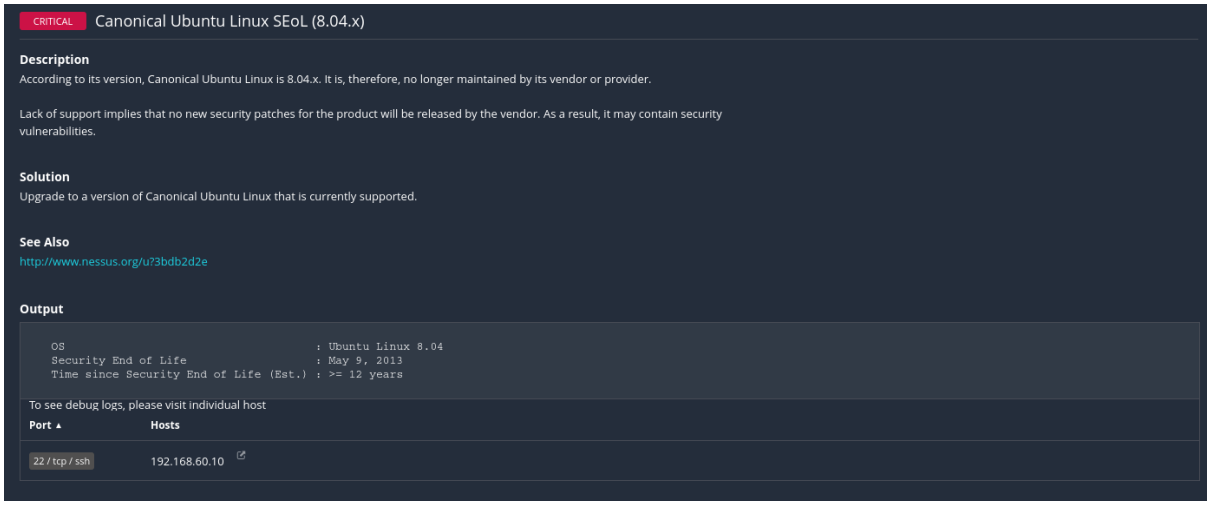
Una volta completata la scansione, si accede ai risultati cliccando sulla scansione. Nessus mostra un riepilogo generale in cui sono evidenziate le vulnerabilità suddivise per livello di gravità: Critical, High, Medium, Low e Informational.



Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0			Canonical Ubuntu Linux SEoL (8.04.x)	General	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5			NFS Shares World Readable	RPC	1
HIGH	7.5			Samba Badlock Vulnerability	General	1
MIXED	...	...	...	SSL (Multiple Issues)	General	27
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	5.9			SSL Anonymous Cipher Suites Supported	Service detection	1
MEDIUM	5.9			SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1

Analizzando il report relativo a Metasploitable è normale trovare numerose vulnerabilità ad alta e critica gravità. Sulla porta 21 è presente un servizio FTP vulnerabile come vsftpd con backdoor nota. Sulla porta 23 è generalmente attivo Telnet, che trasmette le credenziali in chiaro ed è considerato insicuro. Le porte 139 e 445 mostrano vulnerabilità legate al protocollo SMB, come versioni obsolete di Samba affette da exploit noti. Anche i servizi web sulle porte 80 e 443 possono presentare versioni di Apache vulnerabili.

Per ogni vulnerabilità, Nessus fornisce una descrizione dettagliata che spiega in cosa consiste il problema, perché rappresenta un rischio per la sicurezza e quali potrebbero essere le conseguenze di un eventuale attacco. Vengono inoltre indicati riferimenti esterni come CVE, link a database di vulnerabilità e suggerimenti per la mitigazione, come aggiornamenti software o modifiche di configurazione.



Se necessario, è possibile approfondire ulteriormente una vulnerabilità cercando il codice CVE su Internet, così da comprendere meglio il funzionamento dell'exploit associato.

Conclusione

In conclusione, l'esercizio ha permesso di comprendere in modo pratico come effettuare una scansione di vulnerabilità utilizzando Nessus e come analizzare i risultati ottenuti. L'utilizzo della macchina Metasploitable ha reso evidente quanto un sistema non aggiornato o mal configurato possa essere esposto a numerose vulnerabilità. Attraverso l'analisi del report finale è stato possibile capire l'importanza della prevenzione, degli aggiornamenti di sicurezza e del controllo dei servizi attivi, evidenziando come strumenti di vulnerability scanning siano fondamentali per migliorare la sicurezza delle infrastrutture di rete.