PRATICA S5L3:

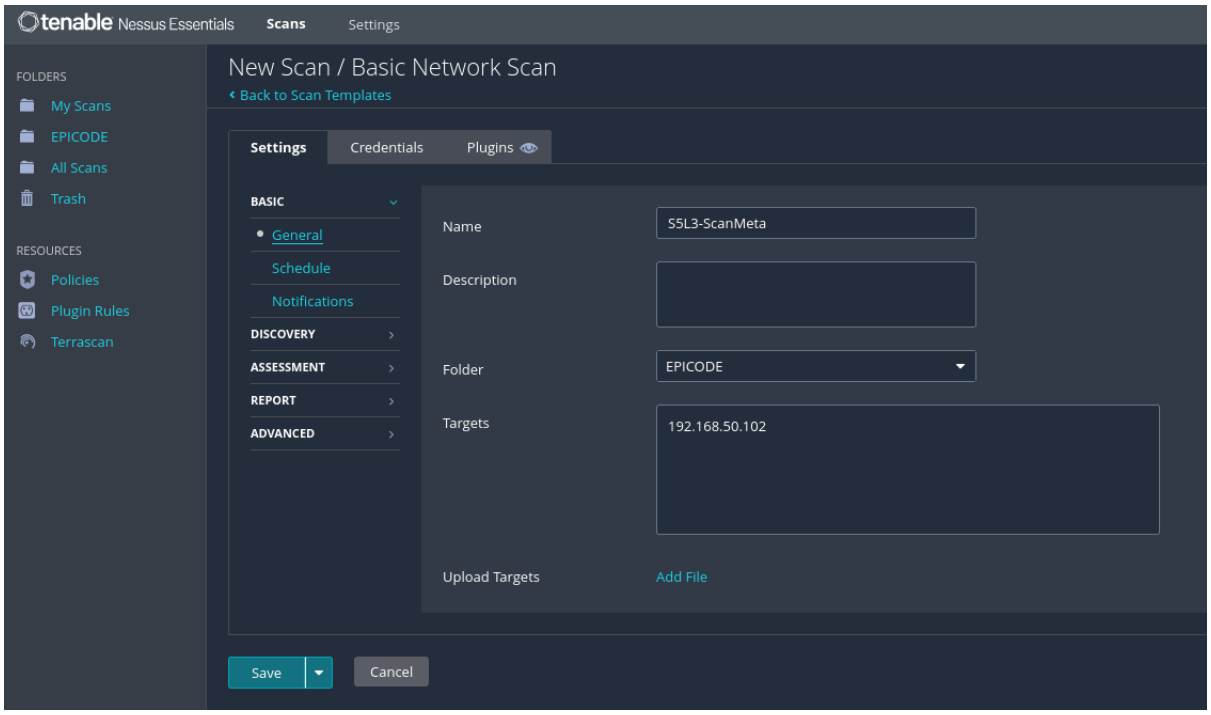
Obbiettivo: Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus, concentrandosi sulle porte comuni. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità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

Configurazione:

Dopo aver creato una cartella chiamata *EPICODE* e avviato una nuova scansione, ho selezionato come policy *Basic Network Scan* e l'ho configurata nel seguente modo:

Nelle impostazioni BASIC > General:

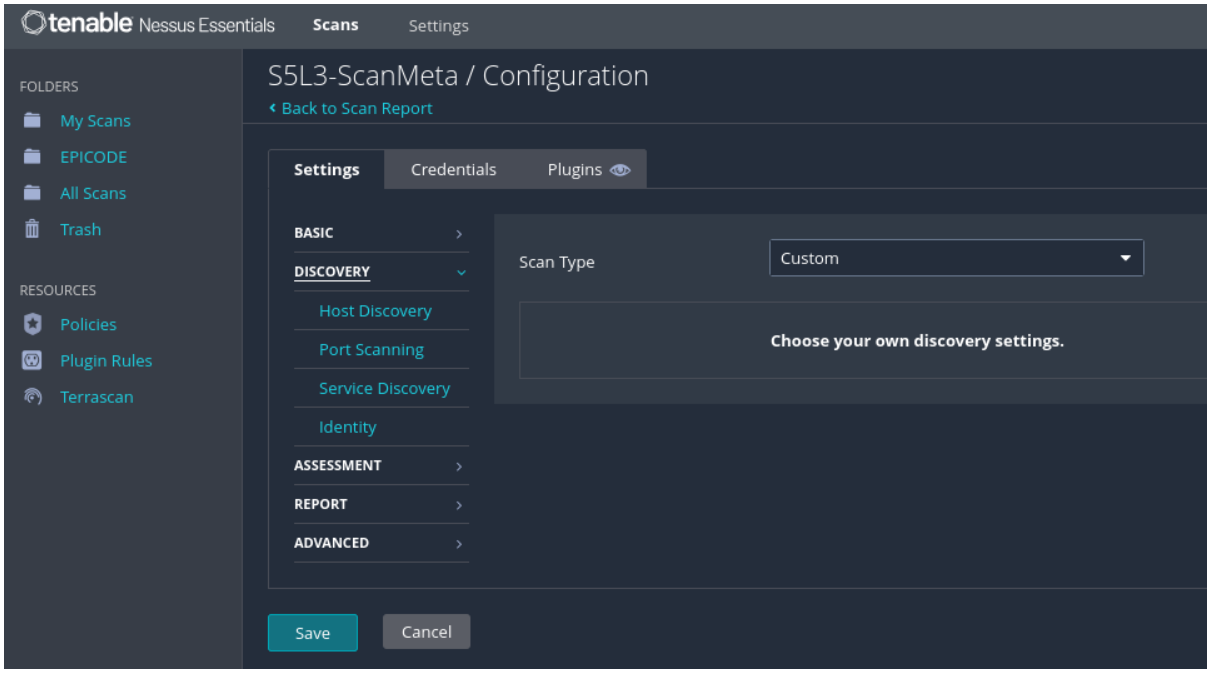
- **Name:** S5L3-ScanMeta
- **Target:** 192.168.50.102 (indirizzo IPv4 della VM Metasploitable)



Nelle impostazioni DISCOVERY:

Ho impostato lo **Scan Type** su **Custom**, in modo da concentrare l'analisi di Nessus

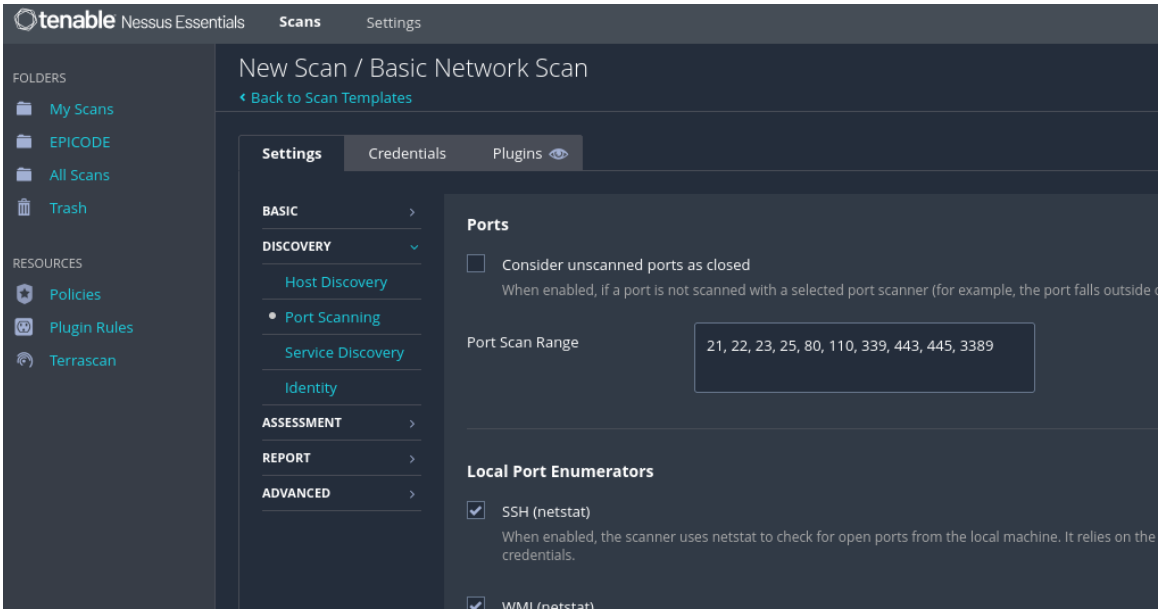
sulle porte comuni.



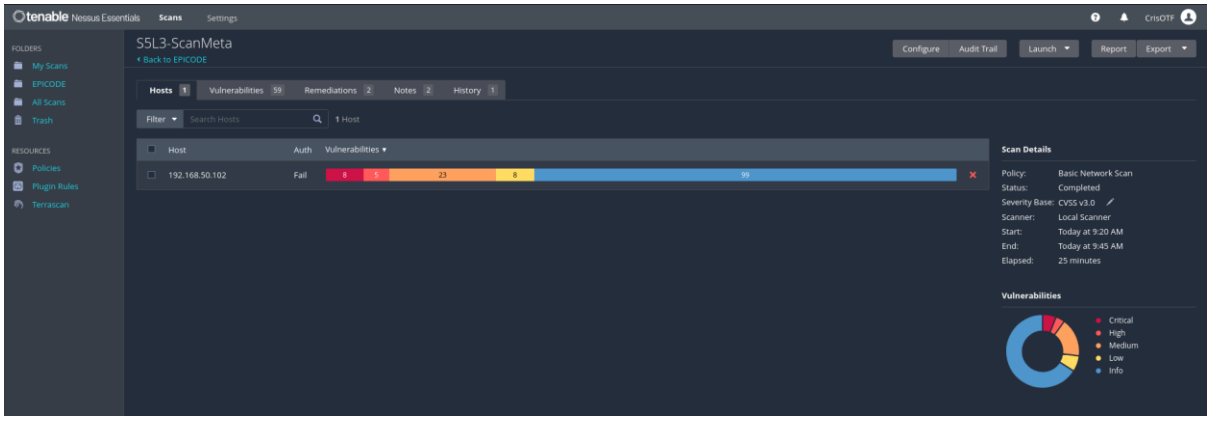
In DISCOVERY > Port Scanning:

Ho specificato il **Port Scan Range** con le seguenti porte:

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



Dopo aver salvato le configurazioni, ho avviato la scansione, ottenendo il seguente risultato finale:



Analisi del Report:

Per esaminare più dettagliatamente i risultati della scansione, ho proceduto con la generazione e il download del report finale. Questa operazione mi ha permesso di visualizzare in modo strutturato tutte le informazioni raccolte durante l'analisi, comprese le vulnerabilità rilevate, i livelli di rischio associati (basso, medio, alto, critico) e le soluzioni per risolvere le vulnerabilità. Grazie a questo documento, è stato possibile identificare con precisione i punti deboli del sistema Metasploitable, facilitando così una valutazione più approfondita dello stato di sicurezza della rete simulata. Prendiamo atto che sono suggerimenti validi ma non perfetti.

Esempio di vulnerabilità:

- 20007 - SSL Version 2 and 3 Protocol Detection:

  Durante l'analisi della macchina target è stata individuata la possibilità di stabilire connessioni cifrate utilizzando **SSL 2.0** e **SSL 3.0**. Queste versioni del protocollo SSL sono considerate **obsolescenti e insicure** da tempo, a causa di numerose debolezze strutturali nei loro meccanismi crittografici.

  Tra le principali vulnerabilità associate vi sono:

  - **Cifratura debole** con gestione insicura del padding (soprattutto con CBC)
  - **Rinegoziazione della sessione vulnerabile**, esponendo le comunicazioni ad attacchi di tipo man-in-the-middle
  - **Possibilità di downgrade** della connessione, consentendo a un attaccante di forzare l'uso di SSL anche se il server supporta protocolli più sicuri

  Queste debolezze rendono possibile l'intercettazione o la manipolazione dei dati cifrati, compromettendo gravemente la sicurezza della comunicazione

Raccomandazioni

Si consiglia di:

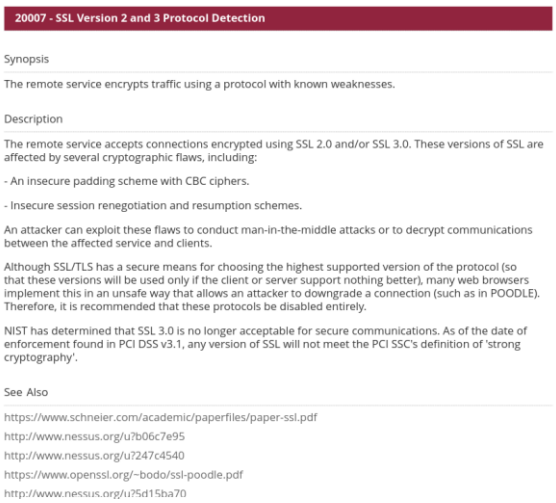
- **Disabilitare completamente SSL 2.0 e SSL 3.0** nella configurazione del servizio esposto
- **Forzare l'uso di TLS 1.2 o superiore**, garantendo che vengano utilizzate solo **suite di cifratura aggiornate e sicure**

L'intervento è fortemente raccomandato per evitare che attaccanti possano intercettare o manipolare dati sensibili durante la comunicazione.

Riferimenti utili

Inoltre, Nessus fornisce una serie di collegamenti utili per approfondire le vulnerabilità legate all'uso di SSL 2.0 e SSL 3.0. Tra questi si trovano analisi tecniche, documentazione ufficiale e studi accademici che spiegano le debolezze crittografiche e gli attacchi associati:

- Schneier – Analisi accademica su SSL
- Nessus – Documentazione aggiuntiva 1
- Nessus – Documentazione aggiuntiva 2
- OpenSSL – Documento tecnico sull'attacco POODLE
- Nessus – Approfondimento tecnico 3
- Imperial Violet – Spiegazione dell'attacco POODLE
- RFC 7507 – TLS Fallback Signaling Cipher Suite Value
- RFC 7568 – Deprecazione ufficiale di SSL 3.0



20007 - SSL Version 2 and 3 Protocol Detection

Synopsis

The remote service encrypts traffic using a protocol with known weaknesses.

Description

The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.

- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.

NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70