

Traccia Esercizio:

Obiettivo:

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.

Fasi dell'Esercizio:

1. **Configurazione della Scansione:**
 - Target: Metasploitable
 - Porte: Solo le porte comuni (es. 21, 22, 23, 25, 80, 110, 139, 443, 445, 3389)
 - Tipo di Scansione:
 - Puoi scegliere tra:
 - Basic Network Scan: Configurazione predefinita per una scansione di rete.
 - Advanced Scan: Configurabile in base alle tue esigenze specifiche.
2. **Esecuzione della Scansione:**
 - Avvia la scansione configurata su Nessus.
 - Attendi il completamento della scansione e assicurati che tutte le porte specificate siano state analizzate.

Obiettivo:

3. **Analisi del Report:**
 - Una volta completata la scansione, scarica e analizza il report generato da Nessus.
 - Per ogni vulnerabilità riportata:
 - Leggi attentamente la descrizione fornita nel report.
 - Approfondisci ulteriormente utilizzando i link e le risorse suggerite nel report.
 - Cerca ulteriori informazioni sul Web, se necessario.

Obiettivi dell'Esercizio:

1. **Pratica con Nessus:**
 - Imparare a configurare e avviare scansioni con Nessus.
 - Capire come restringere le scansioni a porte specifiche.
2. **Familiarizzazione con le Vulnerabilità:**
 - Conoscere alcune delle vulnerabilità comuni che si possono incontrare.
 - Imparare a interpretare i risultati dei report di Nessus.
 - Sviluppare la capacità di approfondire e comprendere le vulnerabilità utilizzando risorse aggiuntive.

Obiettivo:

Risultato Atteso:

Al termine dell'esercizio, lo studente dovrebbe essere in grado di:

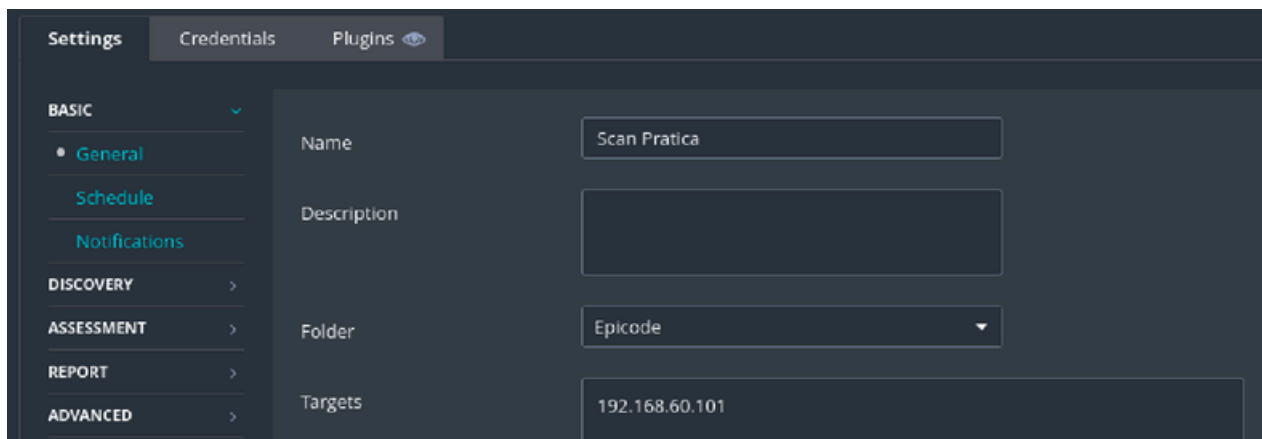
- Configurare e avviare scansioni di vulnerabilità con Nessus.
- Analizzare i report di vulnerabilità e comprendere le informazioni fornite.

Esecuzione:

Creiamo una **nuova scansione** su **"NESSUS"**, inseriamo un nome e l'indirizzo:

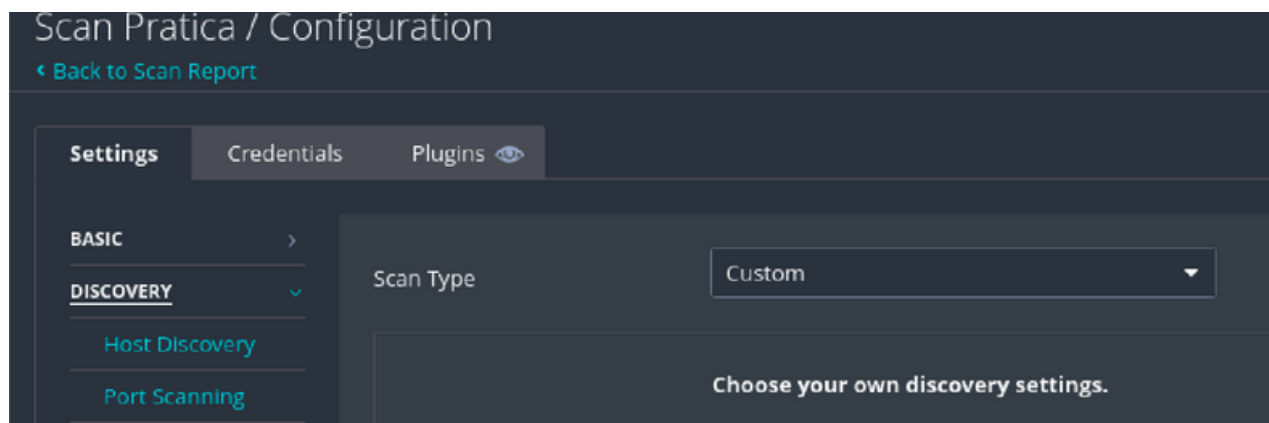
NAME: Scansione Pratica

TARGETS: indirizzo della **metasploitable2**, 192.168.60.101



The screenshot shows the 'Settings' page in Nessus. The 'BASIC' tab is selected, and the 'General' sub-tab is active. The 'Name' field is filled with 'Scan Pratica'. The 'Description' field is empty. The 'Folder' dropdown is set to 'Epicode'. The 'Targets' field contains the IP address '192.168.60.101'.

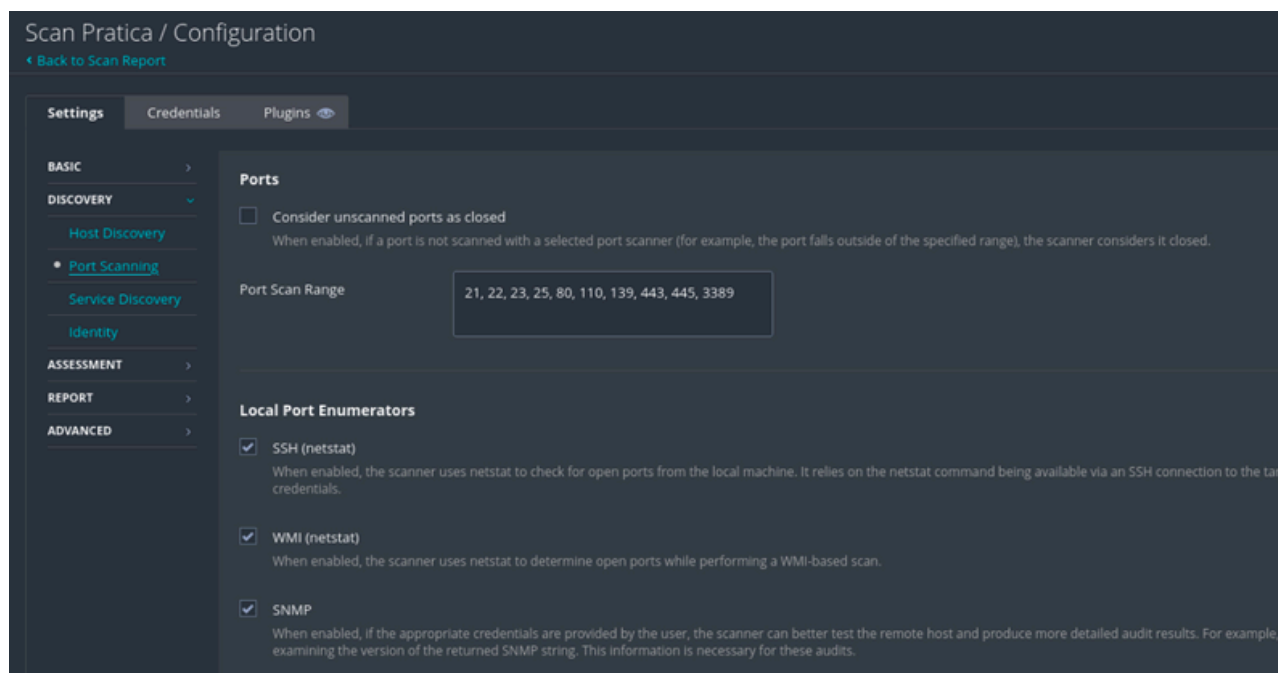
Ora per poter **impostare le porte** andiamo su **"Discovery"** e selezioniamo **"Scan Type"**, impostiamolo su **"Custom"**.



The screenshot shows the 'Scan Pratica / Configuration' page. The 'Settings' tab is selected, and the 'Discovery' sub-tab is active. The 'Scan Type' dropdown is set to 'Custom'. Below the dropdown, there is a text prompt: 'Choose your own discovery settings.'

Andiamo nella sezione **“Port Scanning”** e inseriamo in **“Port Scan”** le porte che vogliamo analizzare.

Input delle porte, quando molteplici, va inserito usando “,” oppure “-” per definire un range.



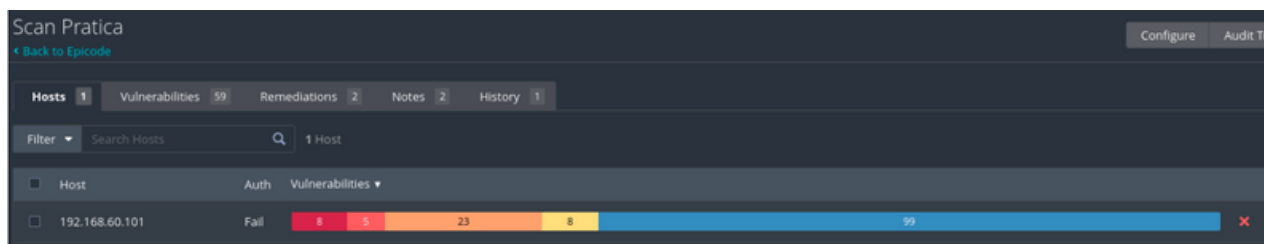
Una volta settato tutto **avviamo** la **scansione** utilizzando il pulsante **“Play”**.

***Nota:** che nello screenshot e' presenta una data, significa che e' gia stata avviata una scansione in data tale. Possiamo cmq riusare questa scansione con le stesse opzioni o modificarle per ogni esigenza.*

Name	Scan Type	Schedule	Last Scanned
Scan Pratica	Vulnerability	On Demand	Today at 8:13 AM

Finita le scansioni possiamo vedere i risultati.

Risultati scansione:



Il tool e' accompagnato da un **interfaccia** molto **leggibile**. **Colori e numeri** ci **indicano** molto chiaramente **la gravita delle vulnerabilita'** trovate.

Hosts: raggruppa i risultati divisi per ogni Hosts

Vulnerabilities: filtra i risultati per le vulnerabilita' scoperte sulla macchina "Target"

Remediations: sono i rimedi, soluzioni per risolvere problemi di sicurezza trovati. *Approfittiamo di questi suggerimenti, ma **RICORDIAMO**, sono suggerimenti quindi dobbiamo analizzando il problema **personalmente** per capire la logica, cosa implica e porre rimedio al problema di sicurezza.*

Notes: note sulla scansione

History: storico delle scansioni

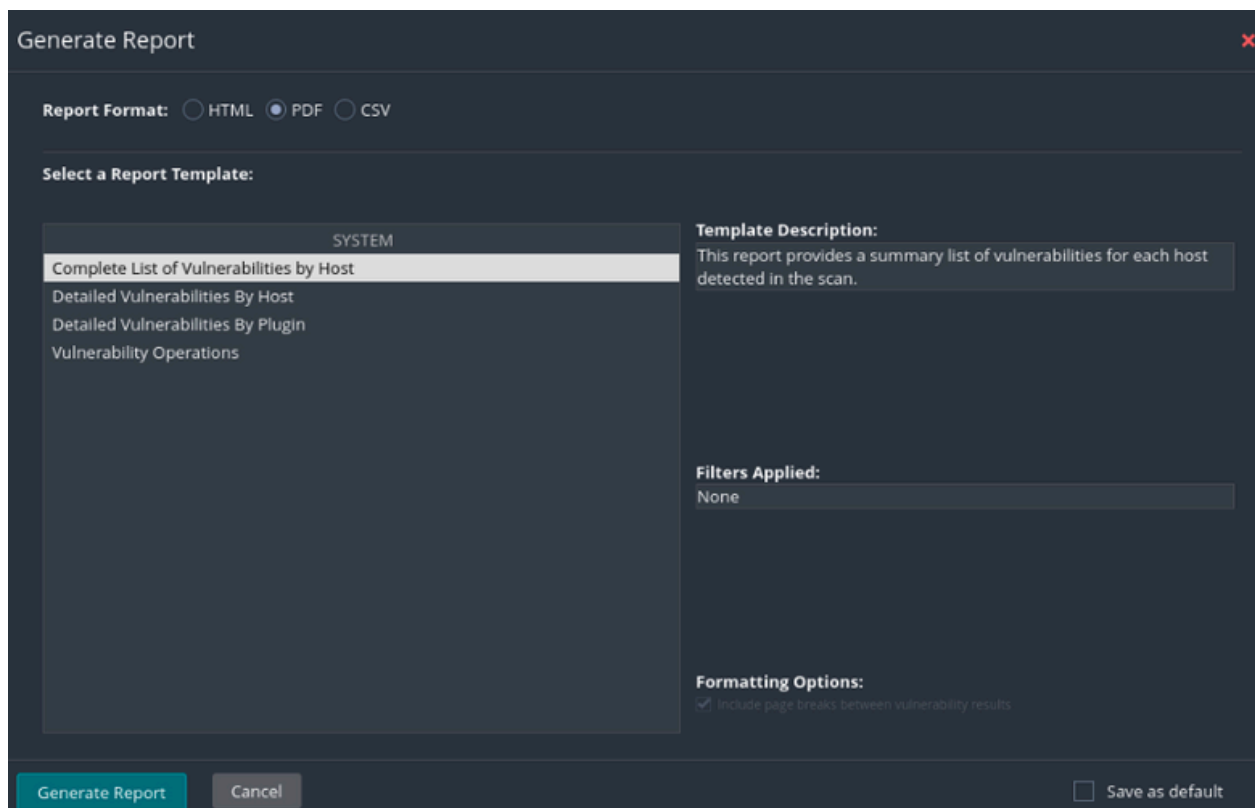
In foto possiamo vedere alcune vulnerabilita' segnalate, ci prenderemo cure partendo da quelle piu' gravi

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	8.9	0.9447	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1	
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2	
CRITICAL	SSL (Multiple Issues)	Gain a shell remotely	3	
HIGH	7.5	5.9	0.8111	Samba Badlock Vulnerability	General	1	
HIGH	7.5			NFS Shares World Readable	RPC	1	
MIXED	SSL (Multiple Issues)	General	28	
MIXED	ISC Bind (Multiple Issues)	DNS	5	
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2	
MEDIUM	5.9	4.4	0.027	SSL Anonymous Cipher Suites Supported	Service detection	1	
MEDIUM	5.9	3.6	0.9035	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1	
MIXED	SSH (Multiple Issues)	Misc.	6	
MIXED	DNS (Multiple Issues)	DNS	4	

Ora che la scansione e' terminata possiamo visualizzare comodamente i risultati, possiamo anche utilizzare la **generazione di report automatica**.

Per avere il report completo selezionata la scansione utilizziamo **"REPORT"** in alto a destra e selezioniamo l'opzione piu' utile per le nostre esigenze.

Possiamo anche non stampare un report e analizzare tutto da dentro il programma



Esempio analisi del report: *prendiamo in esempio una vulnerabilita' trovata*

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.

Analizzando il report si evince facilmente che il servizio remoto cripta il traffico utilizzando protocolli con vulnerabilit  note.

Nella descrizione abbiamo una descrizione di cosa comporta e sotto troviamo diversi riferimenti al argomento che possono aiutarci ad analizzare il problema.

In questo caso sappiamo gi  che la scelta migliore   sfruttare la tecnologia TLS cambiando il tipo da SSL a TLS ma apriamo un attimo la documentazione aggiuntiva per

capire come e quanto ci possono essere utili le ulteriori informazioni dateci

Link1: <https://www.schneier.com/wp-content/uploads/2016/02/paper-ssl.pdf>

Vediamo subito che la documentazione   molto completa e tecnica.

Un ottimo modo per approfondire nel dettaglio le vulnerabilit , capirne il funzionamento, come mitigarle e come sfruttarle anche per test di attacco.

Analysis of the SSL 3.0 protocol

David Wagner
University of California, Berkeley
 daw@cs.berkeley.edu

Bruce Schneier
Counterpane Systems
 schneier@counterpane.com

Abstract

The SSL protocol is intended to provide a practical, application-layer, widely applicable connection-oriented mechanism for Internet client/server communications security. This note gives a detailed technical analysis of the cryptographic strength of the SSL 3.0 protocol. A number of minor flaws in the protocol and several new active attacks on SSL are presented; however, these can be easily corrected without overhauling the basic structure of the protocol. We conclude that, while there are still a few technical wrinkles to iron out, on the whole SSL 3.0 is a valuable contribution towards practical communications security.

gives some background on SSL 3.0 and its predecessor SSL 2.0. Sections 3 and 4 explore several possible attacks on the SSL protocol and offer some technical discussion on the cryptographic protection afforded by SSL 3.0; this material is divided into two parts, with the SSL record layer analyzed in Section 3 and the SSL key-exchange protocol considered in Section 4. Finally, Section 5 concludes with a high-level view of the SSL protocol's strengths and weaknesses.

2 Background

SSL is divided into two layers, with each layer using services provided by a lower layer and providing services to a higher layer. The SSL record layer is the lower layer, and the SSL key-exchange protocol is the higher layer.

Allego sia il report della scansione che il primo collegamento di documentazione nella stessa repository su github.