

## Obiettivo dell'Esercizio

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.
  - Configurare le scansioni.
  - Familiarizzare con alcune 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.

### 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.
- 

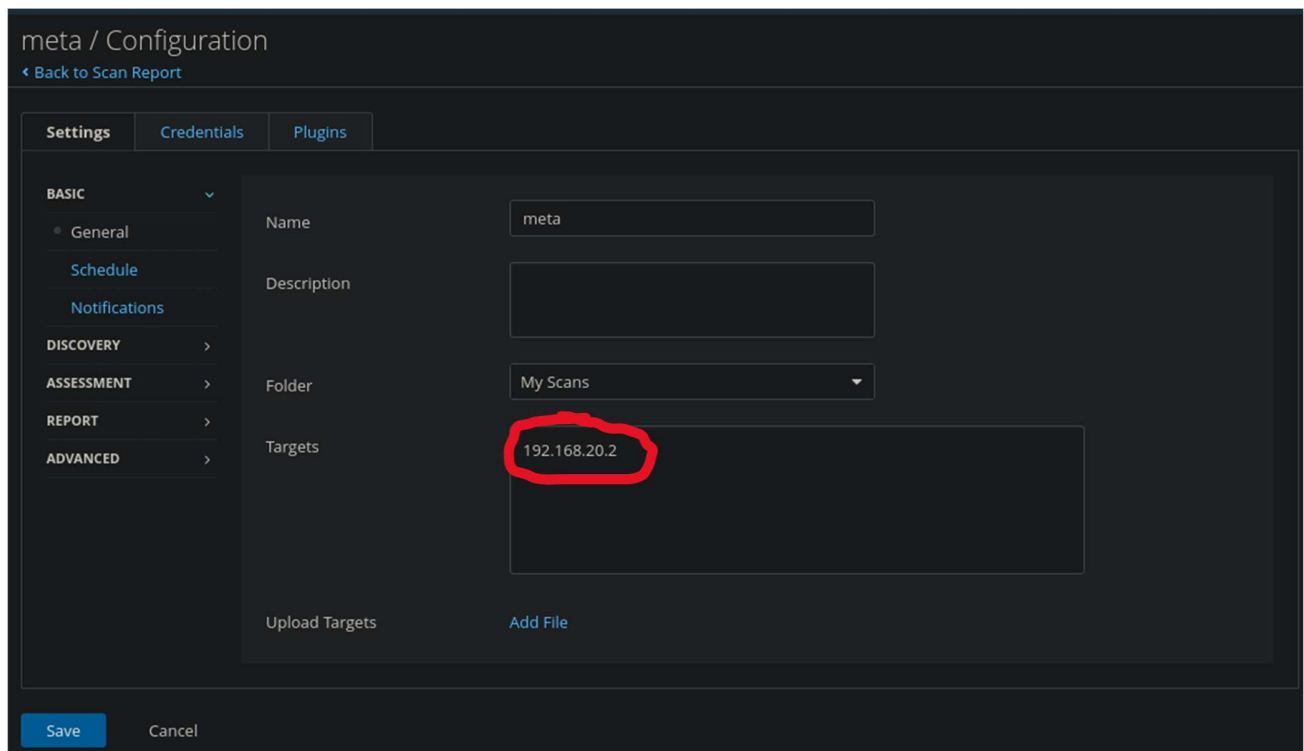
## Risultato Atteso

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.

## SVOLGIMENTO

Inizio con il configurare la scansione. Imposto ip di target (macchina metasploitable tramite pfsense), ip 192.168.20.2



The screenshot shows the 'meta / Configuration' page in Nessus. The 'Settings' tab is active, and the 'BASIC' section is expanded. The 'General' sub-tab is selected. The 'Name' field is set to 'meta'. The 'Description' field is empty. The 'Folder' is set to 'My Scans'. The 'Targets' field contains the IP address '192.168.20.2', which is circled in red. Below the 'Targets' field, there are links for 'Upload Targets' and 'Add File'. At the bottom of the page, there are 'Save' and 'Cancel' buttons.

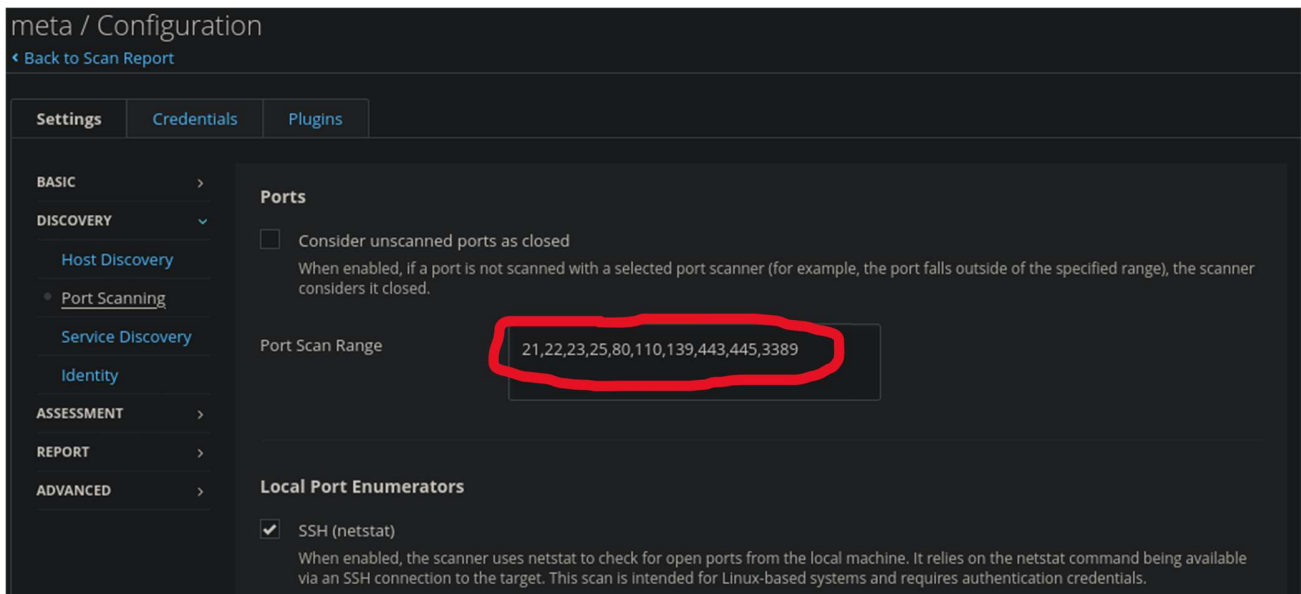
Settings	Credentials	Plugins
<b>BASIC</b>		
General		
Schedule		
Notifications		
DISCOVERY		
ASSESSMENT		
REPORT		
ADVANCED		

Name	meta
Description	
Folder	My Scans
Targets	192.168.20.2

Upload Targets Add File

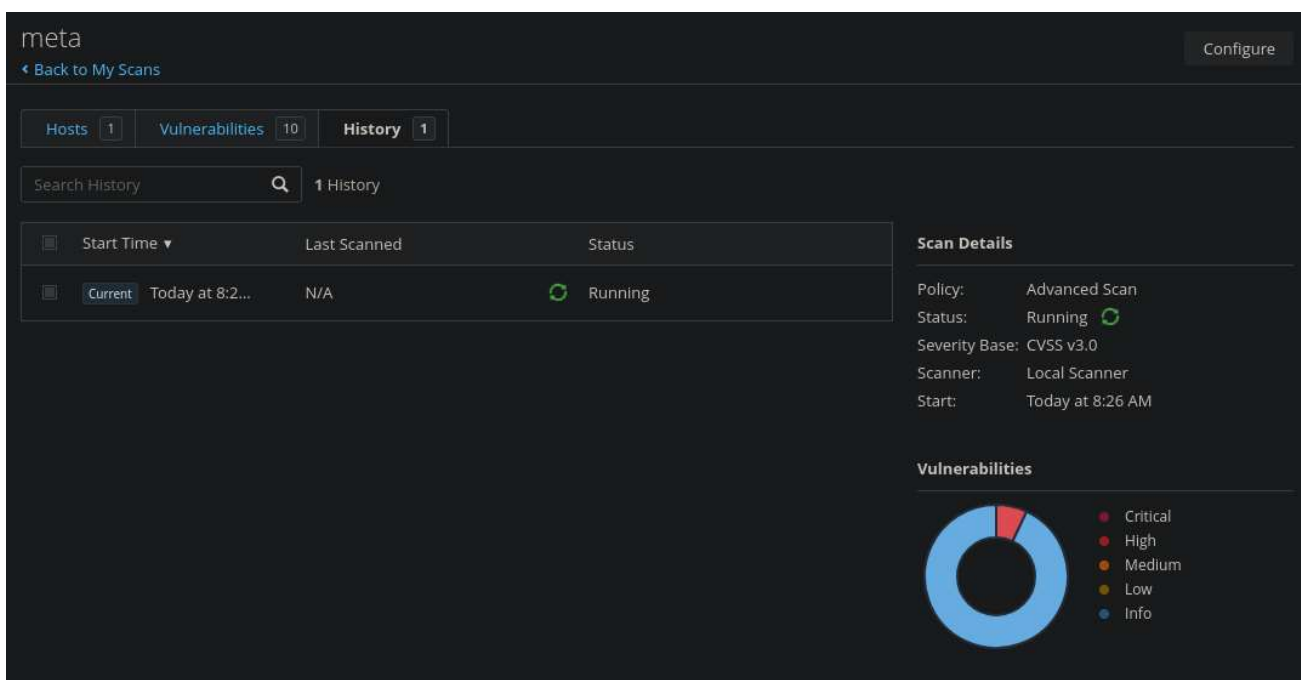
Save Cancel

Imposto le porte target menzionate nel testo dell'esercizio:



Avvio quindi la scansione del target. Uso CVSS v3.0 perché è la severity consigliata.

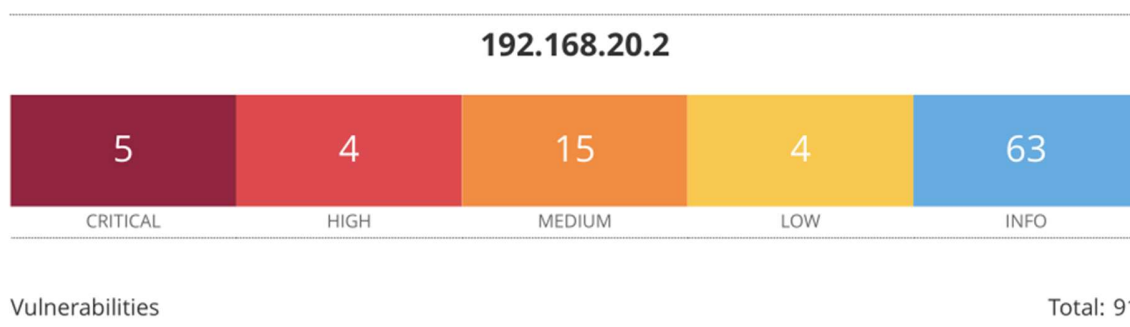
La **Severity CVSS v3.0** si riferisce al **Common Vulnerability Scoring System (CVSS)** nella sua versione 3.0, un sistema standardizzato utilizzato per valutare la gravità delle vulnerabilità di sicurezza informatica.



Il CVSS v3.0 classifica le vulnerabilità in quattro livelli di gravità in base al **Base Score**:

#### Base Score Severity

0.0	Nessuna (None)
0.1 - 3.9	Bassa (Low)
4.0 - 6.9	Media (Medium)
7.0 - 8.9	Alta (High)
9.0 - 10.0	Critica (Critical)



Partiamo analizzando le vulnerabilità critiche.

Vengono classificate secondo questi parametri:

- **SEVERITY e CVSS** mostrano la gravità tecnica.
- **VPR e EPSS** aiutano a capire l'urgenza e la probabilità di sfruttamento.
- **PLUGIN NAME** guida nell'identificazione e nella risoluzione.

Nello specifico:

- **SEVERITY (Gravità)**: Indica il livello di rischio della vulnerabilità (Critica, Alta, Media o Bassa), basato sul punteggio CVSS.
- **CVSS V3.0**: Un sistema di punteggio (da 0 a 10) che misura la gravità tecnica di una vulnerabilità, tenendo conto di fattori come facilità di exploitazione e impatto su confidenzialità, integrità e disponibilità.
- **VPR SCORE (Vulnerability Priority Rating)**: Un punteggio (da 0 a 10) calcolato da Tenable per aiutare a **prioritizzare** le vulnerabilità, considerando probabilità di sfruttamento, rilevanza e impatto nel mondo reale.
- **EPSS SCORE (Exploit Prediction Scoring System)**: Valuta la probabilità che una vulnerabilità venga sfruttata, con valori da **0.0** (improbabile) a **1.0** (altamente probabile).

- **PLUGIN NAME:** È il nome del plugin Nessus che descrive la vulnerabilità, spiega come rilevarla e fornisce istruzioni per risolverla.

Vulnerabilities					Total: 91
SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9741	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0*	5.1	0.1994	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.1994	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password

## 1. Apache Tomcat AJP Connector Request Injection (Ghostcat)

- **Descrizione:** Questa vulnerabilità (CVE-2020-1938) consente a un attaccante di inviare richieste malevole al connettore AJP di Apache Tomcat, permettendo l'accesso non autorizzato ai file sensibili sul server o l'esecuzione di codice arbitrario.

Il **connettore AJP (Apache JServ Protocol)** di **Apache Tomcat** è un protocollo progettato per consentire la comunicazione tra il server web **Apache HTTP Server** (o altri server frontend) e il **servlet container** Apache Tomcat.

- **Impatto:** Accesso non autorizzato ai dati e possibile compromissione del server.
- **Soluzione:**
  - Disabilitare il connettore AJP se non necessario.
  - Configurare il connettore AJP per accettare connessioni solo da fonti fidate.
  - **Aggiornare Apache Tomcat:** Applicare una versione sicura (ad esempio, **Tomcat 9.0.31**, **8.5.51** o successive), che include correzioni per questa vulnerabilità.

## 2. SSL Version 2 and 3 Protocol Detection

- **Descrizione:** SSLv2 e SSLv3 sono protocolli crittografici obsoleti con gravi vulnerabilità di sicurezza, come POODLE (Padding Oracle). Questi protocolli non garantiscono la sicurezza delle comunicazioni.
- **Impatto:** Un attaccante può intercettare o manipolare i dati crittografati.

- **Soluzione:**
  - Disabilitare SSLv2 e SSLv3 nelle configurazioni del server.
  - **Aggiornare il software del server:** Assicurati che il server web (es. Apache HTTP Server, Nginx) o applicazioni supportino solo TLS 1.2 o TLS 1.3.
  - Verifica i file di configurazione del server:
    - **Apache HTTP Server:** Modifica ssl.conf per includere solo protocolli sicuri, TLS 1.2 o TLS 1.3.
    - **Nginx:** Configura nel blocco ssl i protocolli TLS 1.2 o TLS 1.3.

### 3. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

- **Descrizione:** Questo problema è legato a una vulnerabilità nei pacchetti OpenSSH/OpenSSL di Debian, che generano numeri casuali prevedibili. Ciò rende le chiavi crittografiche insicure e facilmente crackabili./
- **Impatto:** Le chiavi SSH o SSL generate in ambienti vulnerabili possono essere compromesse, permettendo attacchi man-in-the-middle o accesso non autorizzato.
- **Soluzione:**
  - **Aggiornare OpenSSL e OpenSSH:** Installa le versioni aggiornate dei pacchetti openssl e openssh-server
  - Rigenera tutte le chiavi crittografiche esistenti, SSL e SSH a 2048 e 4096 bit

### 4. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL Check)

- **Descrizione:** Variante della vulnerabilità precedente, specificamente rilevata durante il controllo delle connessioni SSL. Conferma che i certificati e le chiavi sono stati generati utilizzando un RNG debole.
- **Impatto:** Lo stesso della vulnerabilità sopra.
- **Soluzione:**
  - Aggiornare i pacchetti OpenSSL e rigenera tutte le chiavi.

### 5. VNC Server 'password' Password

- **Descrizione:** Questa vulnerabilità si verifica quando un server VNC è configurato con la password predefinita "password", che è facilmente indovinabile e consente l'accesso non autorizzato.
- **Impatto:** Un attaccante può accedere al server VNC e controllare la macchina remota.

- **Soluzione:**

- Configurare una password robusta per il server VNC
- **Aggiorna il server VNC:** Installa l'ultima versione del software VNC (ad esempio, **TigerVNC**, **RealVNC**) per assicurarti che siano applicate correzioni per eventuali vulnerabilità.
- Abilita ulteriori livelli di sicurezza, come il tunneling SSH.

HIGH	8.6	5.2	0.0053	<a href="#">136769</a>	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	<a href="#">42256</a>	NFS Shares World Readable
HIGH	7.5	5.1	0.0398	<a href="#">42873</a>	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0489	<a href="#">90509</a>	Samba Badlock Vulnerability
MEDIUM	6.5	4.4	0.004	<a href="#">139915</a>	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	<a href="#">51192</a>	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	<a href="#">57582</a>	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	<a href="#">104743</a>	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	4.4	0.9723	<a href="#">136808</a>	ISC BIND Denial of Service
MEDIUM	5.9	4.4	0.003	<a href="#">31705</a>	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	3.6	0.935	<a href="#">89058</a>	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	0.0079	<a href="#">65821</a>	SSL RC4 Cipher Suites Supported (Bar Mitzvah)

MEDIUM	5.3	4.0	0.0225	<a href="#">11213</a>	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	-	<a href="#">57608</a>	SMB Signing not required
MEDIUM	5.3	-	-	<a href="#">15901</a>	SSL Certificate Expiry
MEDIUM	5.3	-	-	<a href="#">45411</a>	SSL Certificate with Wrong Hostname
MEDIUM	5.3	-	-	<a href="#">26928</a>	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	7.3	0.0135	<a href="#">52611</a>	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	3.7	0.9488	<a href="#">81606</a>	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FRE

LOW	3.7	4.5	0.9689	<a href="#">83738</a>	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Support (Logjam)
LOW	3.4	5.1	0.9746	<a href="#">78479</a>	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
LOW	2.1*	2.2	0.8939	<a href="#">10114</a>	ICMP Timestamp Request Remote Date Disclosure
LOW	2.6*	-	-	<a href="#">10407</a>	X Server Detection