

## ESERCIZIO S5 L3

### 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.

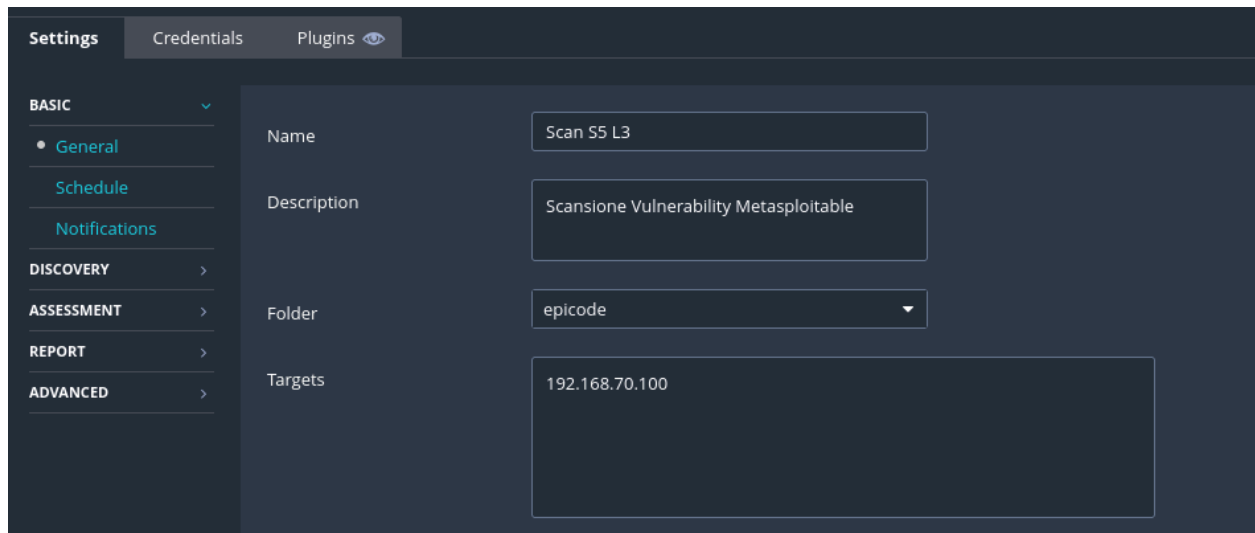
### RISPOSTA

Apro il programma Nessus, e creo una nuova folder cliccando su >>> **New Folder**.

Nomino la cartella “**epicode**” e successivamente clicco su >>> “**Create New Scan**” nella zona centrale della pagina, per iniziare la configurazione della scansione.

Ora scelgo il tipo di scansione che voglio utilizzare >>> “**Basic Network Scan**”

Comincio nella sezione “**Settings**” a modificare/definire le impostazioni che desidero per lo scan che andrò ad effettuare. Entro nella sezione **Basic** >>> **General**:

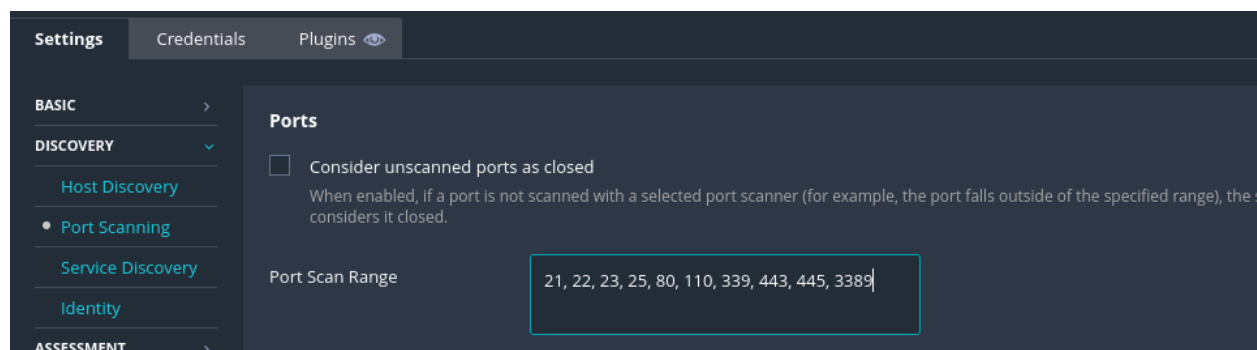


The screenshot shows the Nessus 'Settings' page for a new scan configuration. The interface has a dark theme. At the top, there are tabs for 'Settings', 'Credentials', and 'Plugins'. On the left, a sidebar lists categories: 'BASIC' (with a dropdown arrow), 'DISCOVERY', 'ASSESSMENT', 'REPORT', and 'ADVANCED'. Under 'BASIC', there are sub-items: 'General' (selected with a dot), 'Schedule', and 'Notifications'. The main area on the right contains four configuration fields: 'Name' with the value 'Scan S5 L3', 'Description' with the value 'Scansione Vulnerability Metasploitable', 'Folder' with a dropdown menu showing 'epicode', and 'Targets' with a text input containing '192.168.70.100'.

Field	Value
Name	Scan S5 L3
Description	Scansione Vulnerability Metasploitable
Folder	epicode
Targets	192.168.70.100

In questa sezione imposto un nome per la scansione nella sezione **Name**, una descrizione della scansione che effettuerò nella sezione **Description**, seleziono la **folder** interessata ed infine inserisco il target digitando l'indirizzo IP (in questo caso della VM Metasploitable) **192.168.70.100** che si trova sulla stessa rete interna della VM Kali.

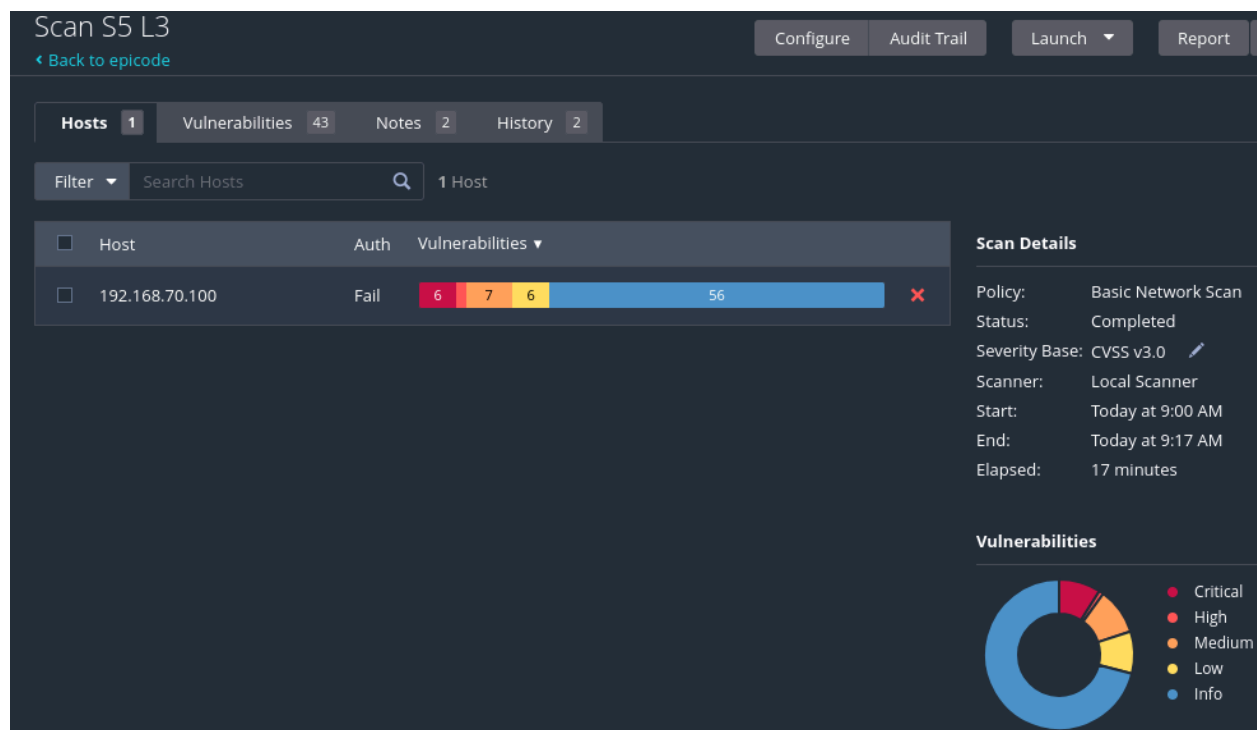
Una volta settate queste impostazioni **Basic**, avanzo nella sezione **Discovery**.



In questa sezione, dovendo selezionare le porte da scansionare, clicco su >>> **Custom** per poter inserire manualmente porta per porta, permettendomi di eseguire una scansione mirata. Come visibile dallo screenshot ho inserito **solamente le porte target**, nella sezione **Port Scan Range**.

Il prossimo passo è **salvare** e poi lanciare ( **launch**) lo scan con il **tasto play** ( triangolino).

Ora non mi resta che attendere i completamento della scansione:



Una volta completata come possiamo notare, il programma attraverso delle colorazioni ci indica i livelli di criticità delle vulnerabilità trovate.

Successivamente clicco sul tasto >>> **Report** >>> **PDF** >>> **Generate Report** per ottenere un report dettagliato nel formato selezionato.

Generate Report

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

- SYSTEM
- Complete List of Vulnerabilities by Host
- Detailed Vulnerabilities By Host
- Detailed Vulnerabilities By Plugin
- Vulnerability Operations

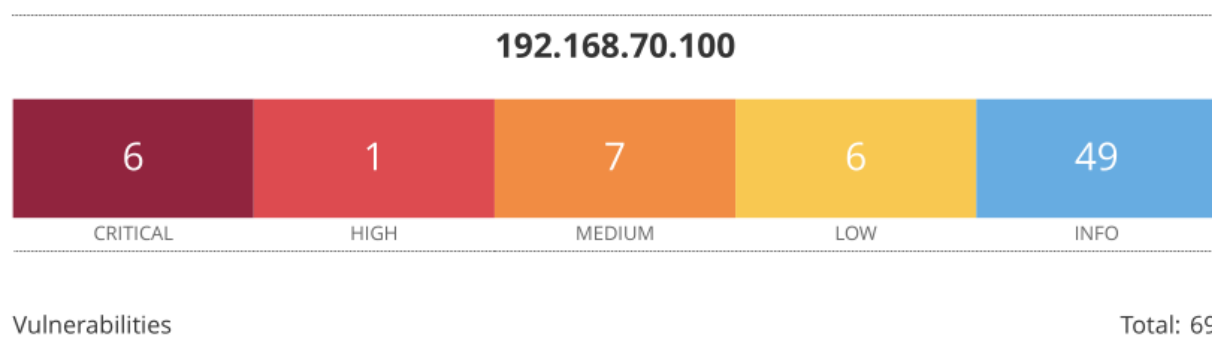
Template Description:  
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:  
None

Formatting Options:  
☒ Include page breaks between vulnerability results

Generate Report Cancel Save as default

Il report generato selezionando **“Complete List of Vulnerabilities by Host”** ha una struttura in cui viene indicato l’**IP target** >>> **numero delle vulnerabilità trovate** >>> **classificazione della criticità tramite colorazione** >>> **descrizione vulnerabilità**.



Inoltre descrive le vulnerabilità in questo modo:

CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	7.5	6.1	0.4158	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate

Se invece selezioniamo l'ultima voce "Vulnerability Operations" il report generato oltre ad avere la stessa modalità grafica di rappresentazione delle vulnerabilità e livelli di criticità, si focalizza sulla **descrizione, fonti e soluzioni** a queste vulnerabilità.

Tra le vulnerabilità ho scelto:

#### 61708 - VNC Server 'password' Password

##### Synopsis

A VNC server running on the remote host is secured with a weak password.

##### Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

##### Solution

Secure the VNC service with a strong password.

##### Risk Factor

Critical

La vulnerabilità riscontrata in questo caso viene classificata come **"critical"** e riguarda la **debolezza della password** del server **VNC**. Non possiede altre fonti o link attraverso cui possiamo accedere ad ulteriori informazioni data la semplicità della vulnerabilità.

Questa debolezza ha permesso a **Nessus** di eseguire il login usando la VNC authentication ed una password. Questo tipo di vulnerabilità può permettere ad un attaccante di eseguire un exploit e prendere il controllo del sistema.

**La soluzione prevede la messa in sicurezza del server VNC reimpostando una password più forte e complessa, perciò più sicura.**

