

SCANSIONE DEI PROBLEMI SU META

La prima parte di questo progetto consiste nell'effettuare una scansione con l'applicativo Nessus su Metasploitable.

Di seguito mostro i passaggi per effettuare la scansione. Le due macchine sono in bridge e hanno gli indirizzi IP impostati in DHCP, l'indirizzo target della scansione è 192.168.1.179

-Per effettuare una scansione con nessus, inizialmente si deve attivare il server con il seguente comando:

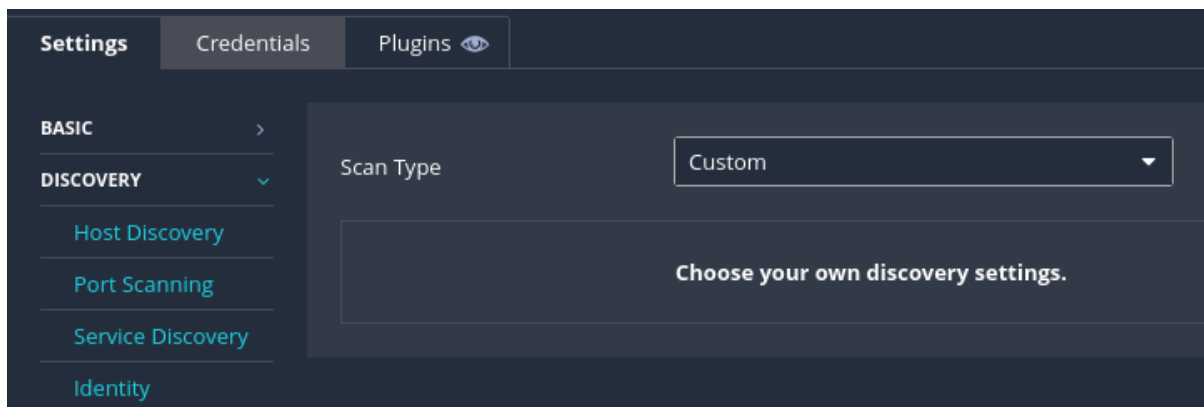
```
(kali㉿kali)-[~]
$ sudo systemctl start nessusd.service
```

- Successivamente dal web browser deve essere inserito il seguente url

<https://kali:8834>

- Una volta aperto il programma deve essere selezionata "new scan" e poi "Basic Network Scan"

E una volta dentro a Basic Network Scan si può scegliere qualsiasi configurazione per fare lo scan. Sul mio ho scelto non le custom, ma le personalizzate:



Andando su Host Discovery ho scelto di fare una scansione anche su porte UDP:

Ping Methods

☒ ARP
Ping a host using its hardware address via Address Resolution Protocol (ARP). This only works on a local network.

☒ TCP
Destination ports:
Destination ports can be configured to use specific ports for TCP ping. This specifies the list of ports that are checked via TCP ping. Type one of the following: built-in, a single port, or a comma-separated list of ports.

☒ ICMP
☐ Assume ICMP unreachable from the gateway means the host is down
Assume ICMP unreachable from the gateway means the host is down. When a ping is sent to a host that is down, its gateway may return an ICMP unreachable message. When this option is enabled, when the scanner receives an ICMP Unreachable message, it considers the targeted host dead. This approach helps speed up discovery on some networks. Note: Some firewalls and packet filters use this same behavior for hosts that are up, but connected to a port or protocol that is filtered. With this option enabled, this leads to the scan considering the host is down when it is indeed up.

Maximum number of retries:
Specifies the number of attempts to retry pinging the remote host.

☒ UDP
Ping a host using the User Datagram Protocol (UDP). UDP is a stateless protocol, meaning that communication is not performed with handshake dialogues. UDP-based communication is not always reliable, and because of the nature of UDP services and screening devices, they are not always remotely detectable.

Dopo ho effettuato lo scan. E Nessus mi mostra tutte gli errori e mi da l'opzione di fare un report in pdf, html o csv

<input type="checkbox"/> Host	Vulnerabilities ▾
<input type="checkbox"/> 192.168.1.179	<div><div>12</div><div>7</div><div>25</div><div>8</div><div>134</div></div> ✕

All Vulnerabilities

Dove effettuare il report

Generate Report ✕

Report Format: ☐ HTML ☒ PDF ☐ CSV

Select a Report Template:

SYSTEM	Template Description:
Complete List of Vulnerabilities by Host	This report presents detailed vulnerabilities by host.
Detailed Vulnerabilities By Host	
Detailed Vulnerabilities By Plugin	
Vulnerability Operations	

Scegliere il tipo di report.