S5/L3

09/01/2025

VULNERABILITY SCANNING

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.

3. **Analisi del Report:**

○ Una volta completata la scansione, scarica e analizza il report generato da Nessus.
○ Per ogni vulnerabilità riportata:

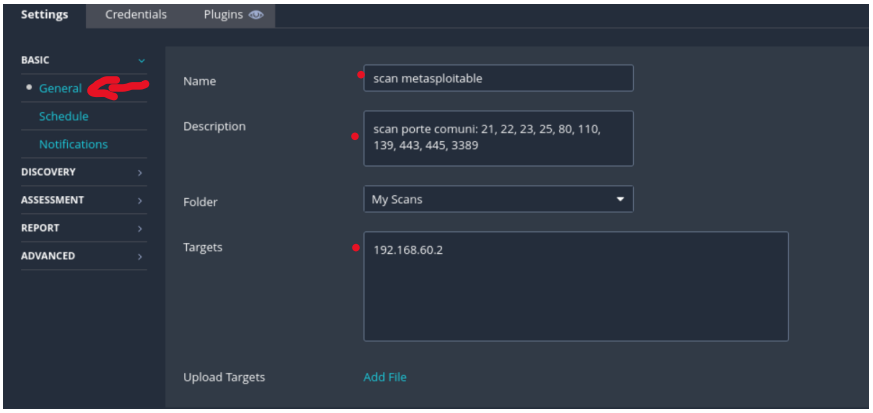
■ Leggi attentamente la descrizione fornita nel report.

■ Approfondisci ulteriormente utilizzando i link e le risorse suggerite nel report.

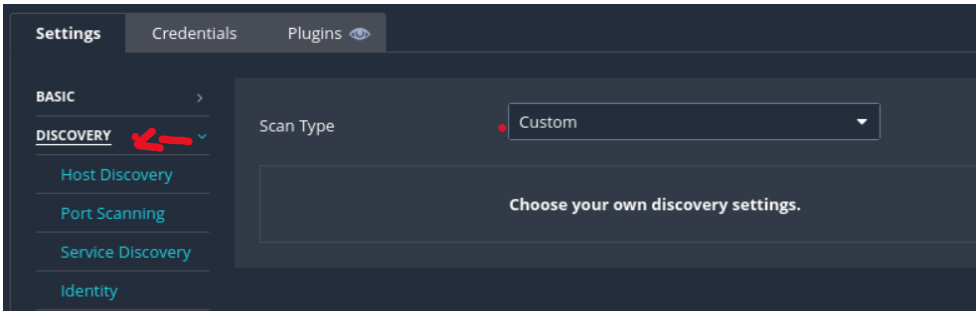
■ Cerca ulteriori informazioni sul Web, se necessario.

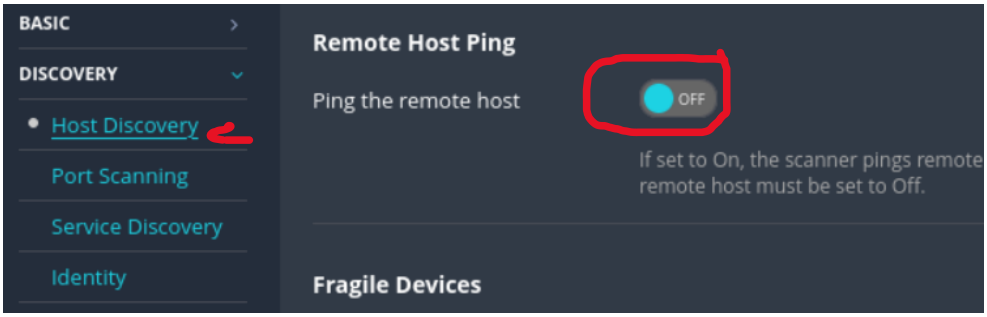
Ho cominciato con avviare il servizio dal terminale di kali

Poi tramite il browser sono entrato dentro Nessus-----> https://kali:8834 e ho avviato una nuova scansione, nello specifico una Basic Network Scan. In General ho impostato il nome della scan e il target:

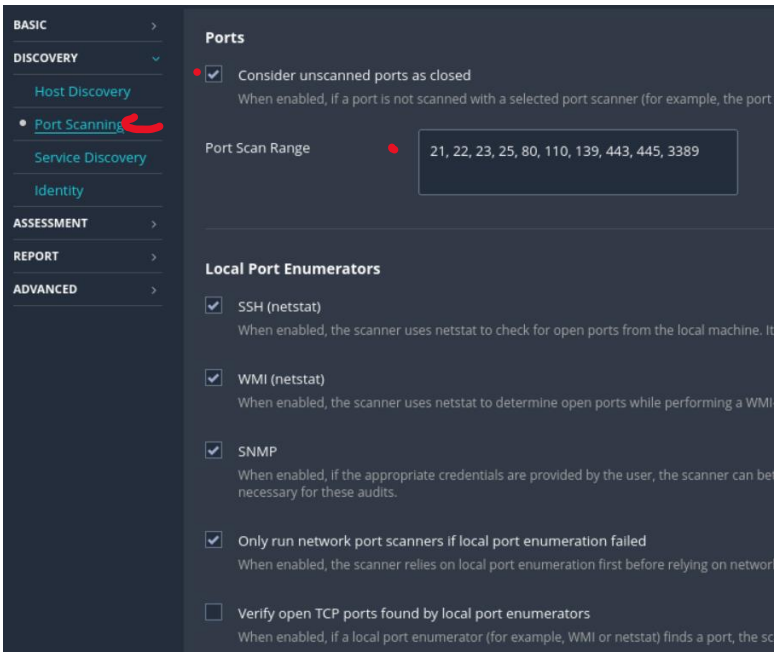


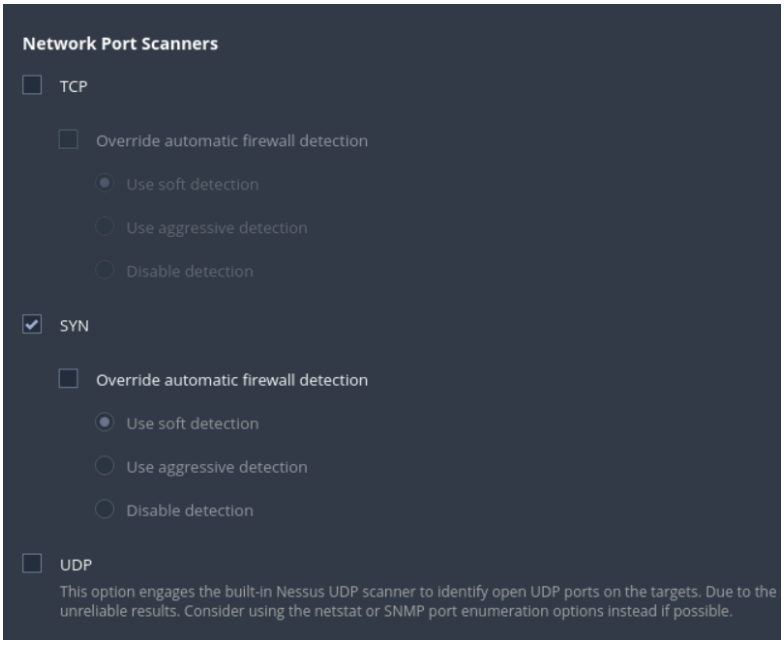
Proseguendo in Discovery ho impostato queste configurazioni:





Qui ho impostato le porte interessate dallo scan





Ho avviato la scansione e una volta completata ho estratto il report

192.168.60.2

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	2	12	3	62

Scan Information

Start time:	Thu Jan 9 09:47:08 2025
End time:	Thu Jan 9 10:07:25 2025

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.60.2
MAC Address:	08:00:27:6D:84:56
OS:	Unix

Prenderò come esempio la prima vulnerabilità critica che ha trovato:

Vulnerabilities

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Synopsis

The remote SSH host keys are weak.

Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

See Also

http://www.nessus.org/u?107f9bdc

http://www.nessus.org/u?f14f4224

Il report ci dà una descrizione della vulnerabilità, una serie di link dove possiamo prendere informazioni sul tipo di vulnerabilità, su quale servizio e porta si trova, come poter risolvere, il livello di CVSS e il fattore di rischio.

Solution

192.168.60.2 4

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Risk Factor

Critical

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVSS v2.0 Temporal Score

8.3 (CVSS2#E:F/RL:OF/RC:C)

References

BID	29179
CVE	CVE-2008-0166
XREF	CWE:310

Exploitable With

Core Impact (true)

Plugin Information

Published: 2008/05/14, Modified: 2024/07/24

Plugin Output

tcp/22/ssh

Tutte queste informazioni sono riportate per tutte le altre vulnerabilità trovate dalla scansione.