

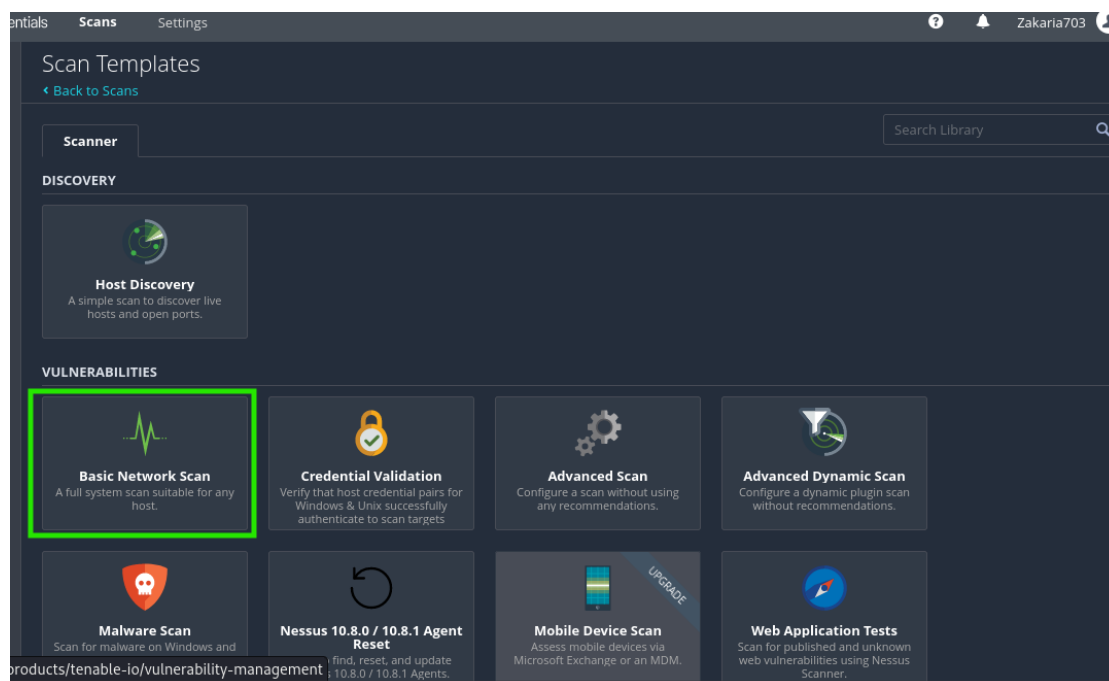
S5/L3

L'esercizio di oggi consiste nell'effettuare 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.

Prima cosa attiviamo il service di Nessus tramite il comando:

```
(kali@kali)-[~]  
$ sudo systemctl start nessusd.service  
[sudo] password for kali:
```

Dopo di che possiamo aprire Firefox ed andare sul sito <https://Kali/8834>, e andiamo a creare una nuova scansione e selezioniamo Basic Network Scan



Poi bisogna inserire i parametri importanti come l'indirizzo del target e le porte da analizzare mentre per il resto se non ci sono specifiche si possono lasciare di default.

Poi avviamo la scansione e si attende che venga completata.

Una volta completata la scansione come prima cosa controlliamo se tutte le porte interessate sono state analizzate.

192.168.50.20

8	5	21	5	126
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Jan 9 09:38:28 2025
End time:	Thu Jan 9 10:01:57 2025

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.50.20
MAC Address:	08:00:27:47:AB:3E
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Questa è la prima pagina del report dove troviamo tutte le vulnerabilità e informazioni come l'orario della scansione, ip del target ecc.

CRITICAL

VNC Server 'password' 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.

Output

```
Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.20

Come possiamo notare qua una delle vulnerabilità critiche è dovuta dalla password del server VNC che è troppo semplice, come possiamo vedere in basso dove c'è l'output Nessus è entrato scrivendo semplicemente "password".

vulnerabilities 01

CRITICAL Bind Shell Backdoor Detection

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :
```

```
This produced the following truncated output (limited to 10 lines) :
----- snip -----
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
----- snip -----
```

To see debug logs, please visit individual host

Qua invece ci dice che c'è un programma in ascolto senza nessuna autenticazione è che quindi potrebbe essere pericoloso per un attaccante dato che potrebbe connettersi e "ascoltare" tutto.

La soluzione che ci consiglia è verificare se è stato compromesso è in caso reinstallare il sistema.

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.

In questo caso invece ci viene segnalato che usiamo delle versioni obsolete che hanno delle vulnerabilità, un attaccante potrebbe usare queste crepe per fare un attacco di man-in-the-middle.

La soluzione che ci fornisce è di disattivare queste 2 versioni ed invece utilizzare versioni migliori come ad esempio TLS 1.2 che è un protocollo molto più sicuro.

90509 - Samba Badlock Vulnerability

Synopsis

An SMB server running on the remote host is affected by the Badlock vulnerability.

Description

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

See Also

<http://badlock.org>

<https://www.samba.org/samba/security/CVE-2016-2118.html>

Qui invece ci viene segnalato che il server SMB è affetto da una vulnerabilità quindi questa dovrebbe essere una vulnerabilità che deve essere risolta al più presto.

Per risolverla dobbiamo aggiornare il server ad una versione più nuova.

Spesso quando si risolvono le vulnerabilità, non ne risolviamo solo una ma anche altre magari di livello più basso dato che ad esempio aggiornando il sistema, i creatori risolvono anche altri problemi.