

NESSUS

Traccia: 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.

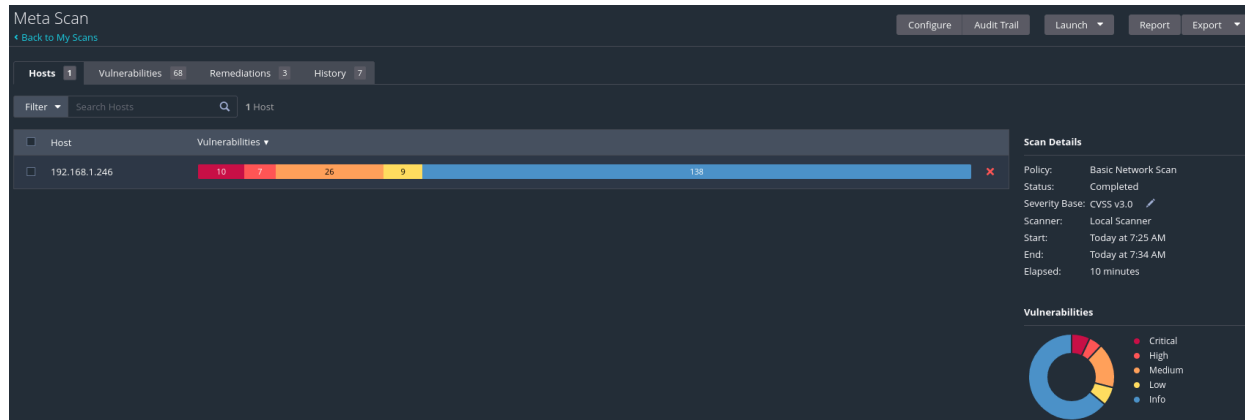
Fasi dell'Esercizio:

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: Esercizio Traccia
 - 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.

Oggi siamo andati a vedere come funziona il software Nessus, ovvero una applicazione atta alla scansione delle vulnerabilità. Le vulnerabilità sono considerate informazioni in quanto, a differenza dei dati (i quali sono oggettivi come porte aperte/chiuso oppure le caratteristiche del sistema operativo), sono considerate soggettive in quanto sottoposte ad una valutazione "variabile".

Ciò che faremo con Nessus sarà la scansione della macchina vulnerabile Metasploitable2 ed andremo ad analizzare 5 delle sue vulnerabilità critiche.

Di seguito andremo a vedere la panoramica generale del risultato ottenuto da questa scansione:



Ciò che emerge dal risultato finale saranno vulnerabilità di vario tipo:

- 10 vulnerabilità **critiche**;
- 7 vulnerabilità **alte**;
- 26 vulnerabilità **medie**;
- 9 vulnerabilità **basse**;
- 138 vulnerabilità **info** (ovvero rischio quasi irrilevante).

Ora ci concentreremo su 5 vulnerabilità critiche e sulla loro risoluzione.

UnrealIRCd Backdoor Detection

Questa è una delle vulnerabilità più gravi che si possono incontrare durante una scansione, in quanto le Backdoors sono una sorta di porta perennemente aperta ad eventuali attacchi esterni, significa che una parte del codice sorgente è stata malevolmente modificata proprio allo scopo di aver garantito un costante accesso al dispositivo in qualsivoglia momento ed avere completo controllo di esso, letteralmente una “porta sul retro” sempre aperta, se il dispositivo è in funzione.

CRITICAL UnrealIRCd Backdoor Detection

Description
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

Solution
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

See Also
<https://seclists.org/fulldisclosure/2010/jun/277>
<https://seclists.org/fulldisclosure/2010/jun/284>
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

Output
The remote IRC server is running as :
uid=0(root) gid=0(root)
To see debug logs, please visit individual host

Port **Hosts**
6697 / tcp / irc 192.168.1.246

L'azione che viene consigliata per la sua risoluzione è di riscaricare il software, verificare che sia aggiornato correttamente ed, infine, reinstallarlo.

VNC Server 'password' Password

Questa vulnerabilità invece ci comunica che è stata utilizzata una password debole, facile da trovare quindi, per un malintenzionato, è semplice accedere al servizio.

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	192.168.1.246

La soluzione suggerita è quella di cambiare la password con una più sicura.

SSL Version 2 and 3 Protocol Detection

Questo tipo di vulnerabilità ci comunica l'utilizzo dei protocolli SSLv2 e SSLv3 considerati obsoleti ed insicuri nella protezione delle comunicazioni tramite HTTPS. Provoca delle gravi falle a livello di crittografia in quanto facilmente soggetta ad attacchi man-in-the-middle, decrittazione del traffico e compromissione dell'integrità dei dati. Il protocollo SSL di base è considerato sicuro, ma le versioni 2 e 3 sono considerate obsolete per l'utilizzo moderno poichè superate dal protocollo TLS, versione più sicura ed aggiornata.

CRITICAL SSL Version 2 and 3 Protocol Detection

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.
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution
Consult the application's documentation to disable SSL 2.0 and 3.0.
Use TLS 1.2 (with approved cipher suites) or higher instead.

See Also
<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>
<http://www.nessus.org/u7b06c7e95>
<http://www.nessus.org/u7247c4540>
<https://www.openssl.org/~bodo/ssl-poodle.pdf>
<http://www.nessus.org/u75d15ba70>
<https://www.imperialviolet.org/2014/10/14/poodle.html>
<https://tools.ietf.org/html/rfc7507>
<https://tools.ietf.org/html/rfc7568>

La soluzione suggerita è: disabilitare SSLv2 e SSLv3 e sostituirla con la versione TLS 1.2 o versioni più aggiornate.

Bind Shell Backdoor Detection

Troviamo un'altra vulnerabilità di tipo backdoor, in questo caso di tipo bind shell. Consente all'attaccante di collegarsi al dispositivo tramite shell collegata ad una determinata porta rimanendo in ascolto di connessioni esterne, consentendogli completo controllo sulla macchina compromessa. E' una backdoor difficile da rilevare, spesso viene piazzata tramite malware su porte non comuni o mascherate da servizi legittimi.

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

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.1.246

La soluzione è di verificare se l'host remoto è stato compromesso e reinstallare il sistema, se necessario.

Apache Tomcat SEoL(<=5.5.x)

L'ultima vulnerabilità che andremo ad analizzare ha a che fare con una specifica versione di Apache Tomcat 5.5.x, sul quale sono state rilevate delle falle a livello di sicurezza che espongono i web server a vari attacchi. La sigla SEoL sta ad indicare un software arrivato a "fine vita", quindi non riceve più aggiornamenti di sicurezza, esponendo il dispositivo che lo usa a maggior rischio di attacchi.

CRITICAL Apache Tomcat SEoL (<= 5.5.x)

Description

According to its version, Apache Tomcat is less than or equal to 5.5.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache Tomcat that is currently supported.

See Also

<https://tomcat.apache.org/tomcat-55-eol.html>

Output

```
URL : http://192.168.1.246:8180/
Installed version : 5.5
Security End of Life : September 30, 2012
Time since Security End of Life (Est.) : >= 12 years
```

To see debug logs, please visit individual host

Port ▲	Hosts
8180 / tcp / www	192.168.1.246

La soluzione in questo caso suggerita è l'aggiornamento di Apache Tomcat alla versione più recente supportata dal dispositivo.