Consegna S5/L4

di Giuseppe Lupoi

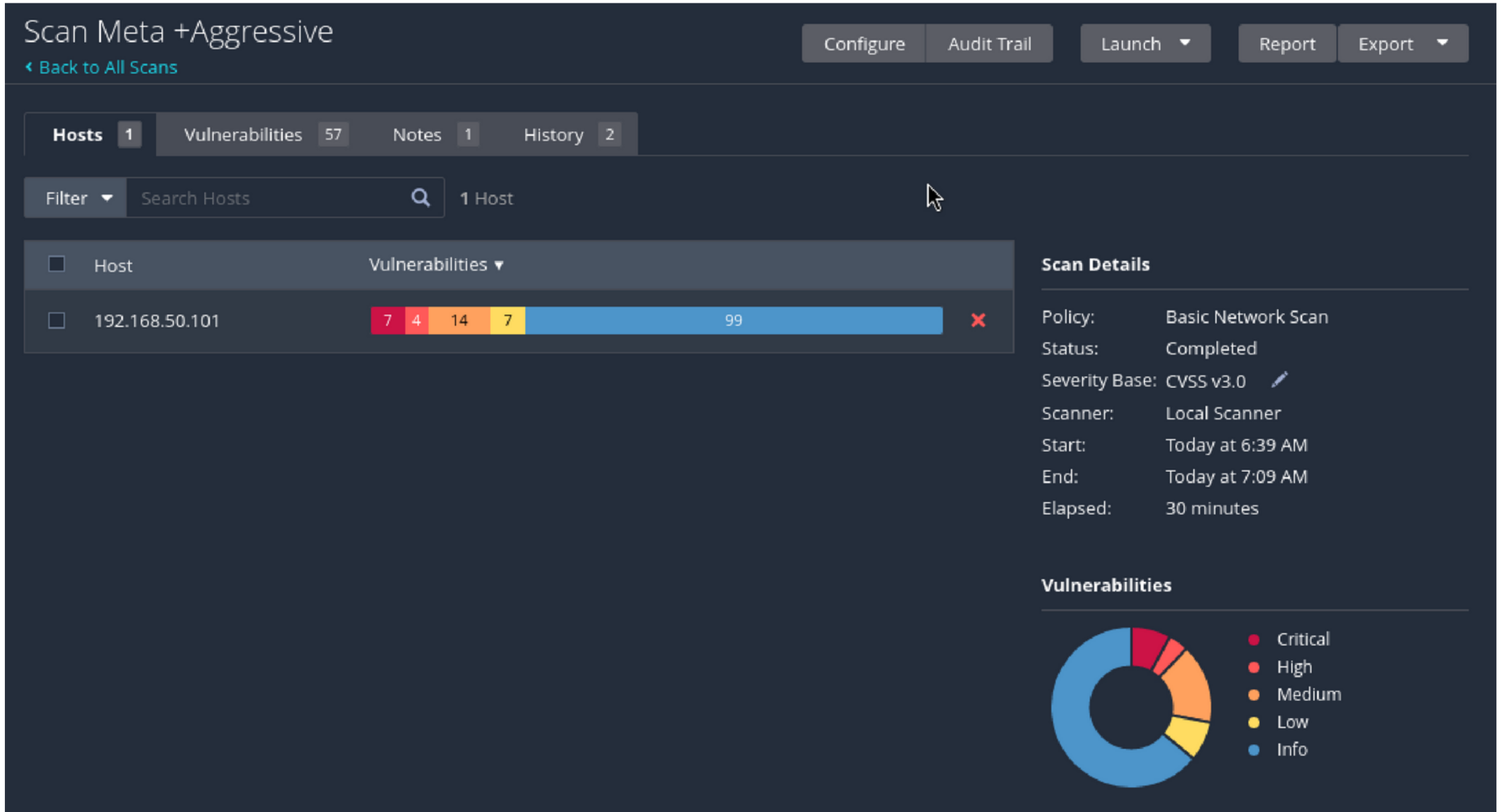
Traccia

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni (potete scegliere come scansione il «basic network scan», o l'advanced e poi configurarlo) A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Gli obiettivi dell'esercizio sono:

- **Fare pratica con lo strumento, con la configurazione e l'avvio delle scansioni**
- **Familiarizzare con alcune delle vulnerabilità note che troverete spesso.**

Come richiesto dall'esercizio di oggi, ho prima scaricato **Nessus** dal browser per poi installarlo con i suoi pacchetti da terminale ed infine avviarlo.
Dopo aver creato il mio account su Nessus ho proseguito impostando una scansione sulla macchina **Metasploitable** con **IP 192.168.50.101**, come vediamo dalla figura in seguito dopo aver avviato la scansione ci troveremo davanti a questa pagina e dovremmo aspettare il completamente della scansione per vedere tutti i risultati.



192.168.50.101

7	4	14	7	99
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time: Thu Dec 21 06:39:37 2023
End time: Thu Dec 21 07:09:50 2023

Host Information

Netbios Name: METASPLOITABLE
IP: 192.168.50.101
MAC Address: CA:01:D0:D2:AF:9A
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities

51988 - Bind Shell Backdoor Detection

Synopsis

The remote host may have been compromised.

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.

Risk Factor

Critical

CVSS v3.0 Base Score

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

CVSS v2.0 Base Score

192.168.50.101 4

Dal primo scan effettuato, aprendo il report avremo esposte tutte le vulnerabilità trovate da Nessus.
Nei riquadri rossi possiamo notare:

- Le vulnerabilità scovate e il loro livello di rischio
- Le info sulla macchina analizzata ovvero il nome, indirizzo IP, MAC e sistema operativo.

Di seguito la lista delle vulnerabilità trovate con descrizione, soluzione, i vari livelli di rischio ed alcuni link per avere maggiori info.

Procederò andando ad analizzare le vulnerabilità di livello **critical** partendo dalla prima:

51988 - Bind Shell Backdoor Detection

Score: 9.8/10

Dove controllando il report e link correlati ci viene detto che;
L'host remoto potrebbe essere stato compromesso.
Esiste una shell in ascolto sulla porta remota senza nessuna autorizzazione o richiesta.
Un malintenzionato potrebbe dunque collegarsi alla shell ed inviare comandi direttamente da remoto.

Soluzione: Verificare se l'host è stato compromesso, ed in tal caso, sarà necessario reinstallare il sistema.

Procederò andando ad analizzare le vulnerabilità di livello **critical**:

32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Score: 10/10

Dove controllando il report e link correlati ci viene detto che;
Le chiavi dell'host remoto sono deboli, le suddette chiavi sono state generate su sistema Debian o Ubuntu che contiene un bug nel file di generazione di numeri casuali della libreria OpenSSL.
Questo problema è dovuto al fatto che un packager Debian ha rimosso tutte le fonti nella versione remota di OpenSSL.
Dunque un malintezionato potrebbe facilmente ottenere la chiave privata per poi piazzarsi "in mezzo" alla comunicazione.

Soluzione: Prendere in considerazione la generazione di nuove chiavi crittografate sopratutto per SSH, SSL e OpenVPN.

Procederò andando ad analizzare le vulnerabilità di livello **critical**:

32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Score: 10/10

Dove controllando il report e link correlati ci viene detto che;
Il certificato SSL remoto utilizza una chiave debole.
Il certificato x509 sul server è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
Questo problema è dovuto al fatto che un packager Debian ha rimosso tutte le fonti nella versione remota di OpenSSL.
Dunque un malintezionato potrebbe facilmente ottenere la chiave privata per poi piazzarsi "in mezzo" alla comunicazione.

Soluzione: Prendere in considerazione la generazione di nuove chiavi crittografate sopratutto per SSH, SSL e OpenVPN.

Procederò andando ad analizzare le vulnerabilità di livello **critical**:

11356 - NFS Exported Share Information Disclosure

Score: 10/10

Dove controllando il report e link correlati ci viene detto che;
Questa vulnerabilità consente di accedere alle condivisioni NFS sull'host.
Dove almeno una delle condivisioni NFS esportate sul server risulterebbe compromessa,
un malintenzionato potrebbe dunque sfruttare questo errore per leggere o eventualmente
scrivere sul file system dell'host remoto.

Soluzione: Configurare NFS dell'host remoto per consentire solo ad utenti autorizzati di montare,
leggere o modificare le condivisioni.

Procederò andando ad analizzare le vulnerabilità di livello **critical**:

20007 - SSL Version 2 and 3 Protocol Detection

Score: 10/10

Dove controllando il report e link correlati ci viene detto che;
Il servizio crittografa il traffico utilizzando un protocollo con punti deboli noti tra cui:
SSL 2 e/o 3 affetti da errori come;

- Uno schema di riempimento non sicuro con cifrari CBC
- Schemi di rinegoziazione e ripresa delle sessioni non sicuri

Un hacker potrebbe sfruttare queste falle e condurre un “man-in-the-middle” per codificare il traffico tra il servizio interessato e il client.
Il NIST ha stabilito che versioni di SSL 3.0 o inferiore non sono più accettabili per comunicazioni sicure, a partire dalla data di applicazione di PCI DSS v3.1 qualsiasi versione di SSL inferiore non soddisferà la definizione di “forte”.

Soluzione: Si consiglia un consulto con la documentazione per disattivare SSL 3.0 o inferiore, per poi procedere con l’installazione di TLS 1.2 o versioni successive

Procederò andando ad analizzare le vulnerabilità di livello **critical**:

33850 - Unix Operating System Unsupported Version Detection

Score: 10/10

Dove controllando il report e link correlati ci viene detto che;
Il sistema operativo in esecuzione sull'host non è più supportato.
Ciò significa che Unix in esecuzione, secondo il numero di versione riportato, non sarà più supportato dal fornitore, ciò significa che non riceverà nuove patch o aggiornamenti di sicurezza.

Soluzione: Eseguire, se possibile, l'upgrade ad una versione del sistema Unix attualmente supportata

Procederò andando ad analizzare le vulnerabilità di livello **critical**:

61708 - VNC Server 'password' Password

Score: 10/10

Dove controllando il report e link correlati ci viene detto che;
Un server VNC in esecuzione sull'host è protetto con una password debole.
Nessus è riuscito ad accedere utilizzando l'autenticazione VNC con una password "password".
Un malintenzionato da remoto potrebbe sfruttare questa falla per prendere il controllo del sistema, anche se non autorizzato.

Soluzione: Cambiare la password del servizio VNC con una molto più complessa