Report di Analisi di Vulnerabilità con Nessus su Metasploitable2

Data: 22/12/23

Guglielmo Carratello

Introduzione:

Nel corso dell'analisi di sicurezza su Metasploitable2, ho utilizzato Nessus, una potente piattaforma di scansione delle vulnerabilità, per identificare potenziali rischi nella configurazione del sistema. Questo report evidenzierà una serie di vulnerabilità trovate da Nessus e l'obiettivo del progetto prevede di scegliere quattro vulnerabilità critiche individuate durante la scansione e spiegare come sono state risolte.

Report vulnerabilità trovate da Nessus:

Vulnerabilities Total: 103

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	-	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

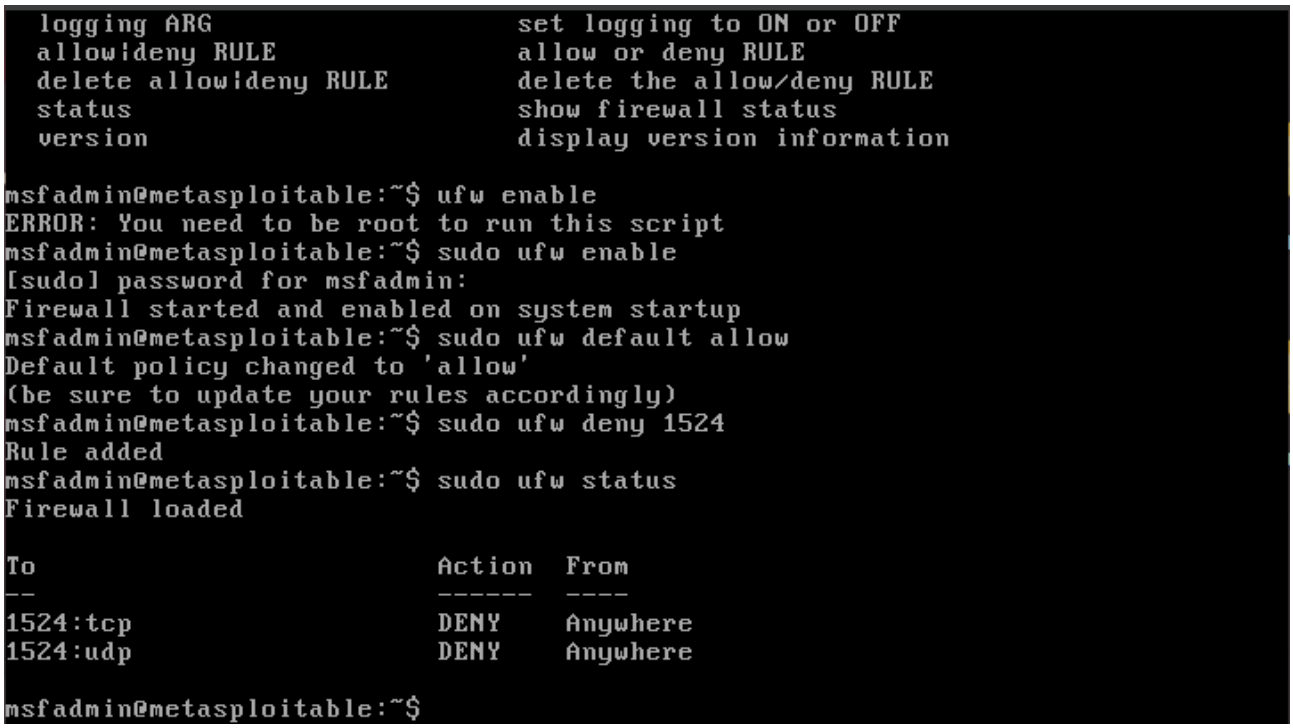
1. Vulnerabilità: Bind Shell Backdoor Detenction

Nature of Vulnerability: Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla come connessione alla porta remota e invio diretto di comandi.

Soluzione Applicata:

Dopo l'individuazione della vulnerabilità, sono state adottate le seguenti misure correttive:

Abbiamo attivato il firewall di Metasploitable2 ed aggiunto una regola che bloccasse i pacchetti in entrata alla porta 1524 (la porta sul quale era in ascolto la backdoor) .



2. Vulnerabilità: NFS Exported share Information Disclosure

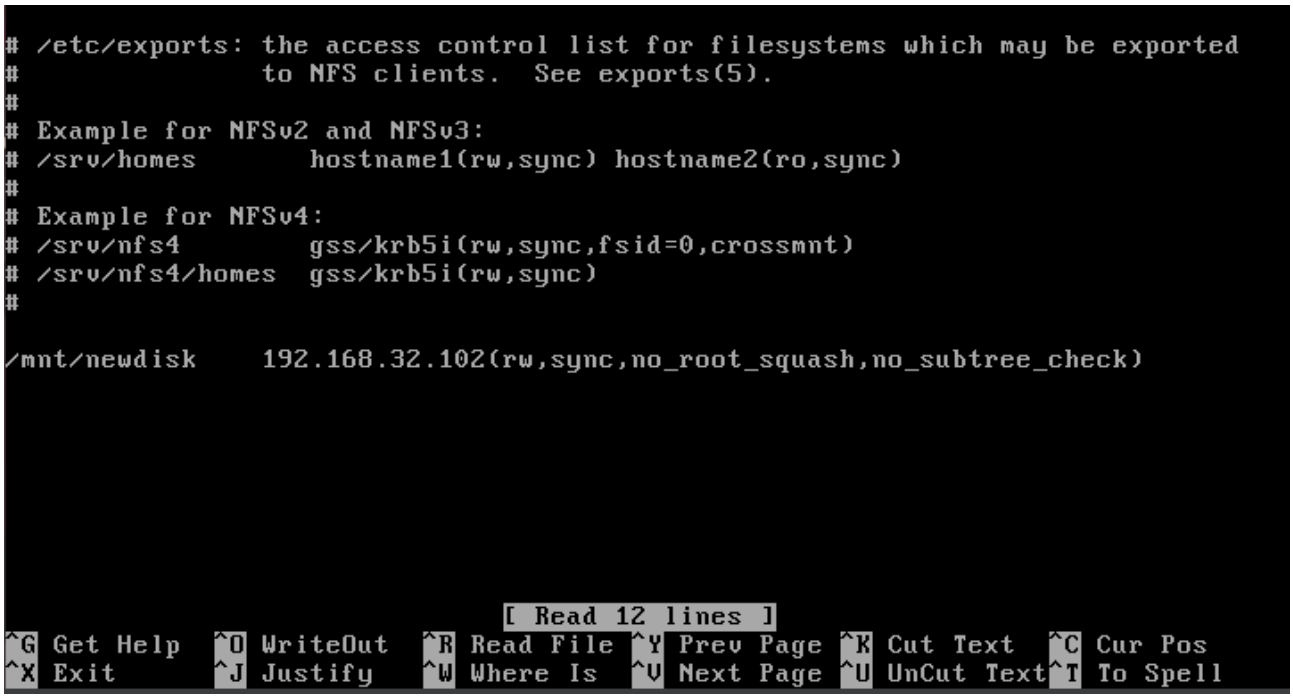
Nature of Vulnerability: Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questo per leggere (e possibilmente scrivere) file su un host remoto.

Soluzione Applicata:

Le seguenti azioni sono state implementate per risolvere questa vulnerabilità:

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le condivisioni remote. Per fare ciò abbiamo raggiunto la cartella /etc/exports, modificato il file

aggiungendo come unico host nella riga iniziava con ‘/’ mnt/newdisk e a seguire l’indirizzo IPv4 della nostra macchina Metasploitable2 con indirizzo IPv4 192.168.32.102 come da screen.



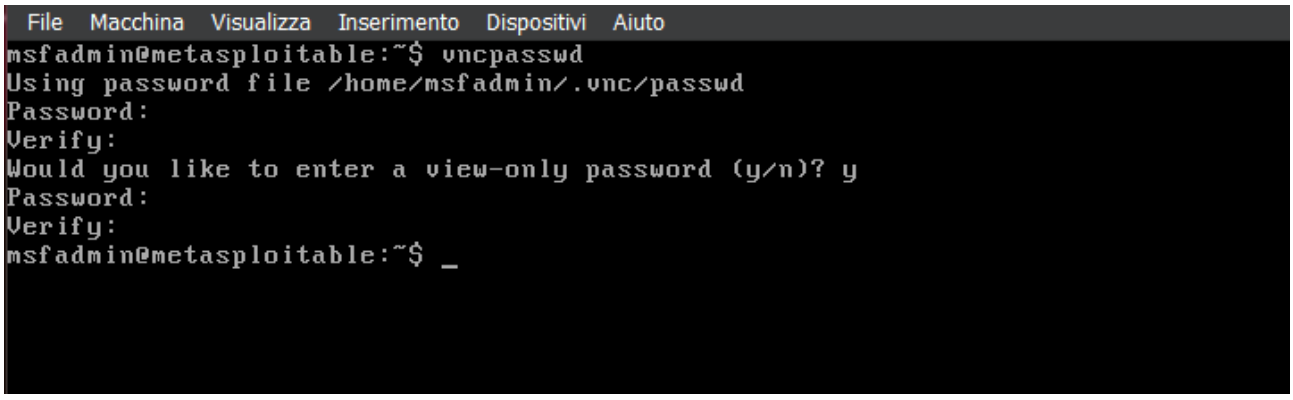
3. Vulnerabilità: VNC Server ‘password’ Password

Nature of Vulnerability: Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password semplice come 'password'. Un utente malintenzionato remoto e non autenticato potrebbe sfruttare questo per prendere il controllo del sistema.

Soluzione Applicata:

Per affrontare questa vulnerabilità, sono state eseguite le seguenti operazioni:

Proteggere il servizio VNC con una password complessa. Su Metasploitable2 abbiamo utilizzato il comando ‘vncpasswd’ per cambiare la password del server VNC. Con l’utilizzo di una password complessa è stato possibile rimediare alla vulnerabilità trovata



4. Vulnerabilità:

Nature of Vulnerability: La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è influenzata da un difetto, noto come Badlock, che esiste in Security Account Manager (SAM) e Local Security Authority (Criteri di dominio) (LSAD) a causa di una negoziazione non corretta del livello di autenticazione tramite procedura remota dei canali di chiamata (RPC). Un utente malintenzionato man-in-the-middle che è in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questo difetto per forzare un downgrade

Soluzione Applicata:

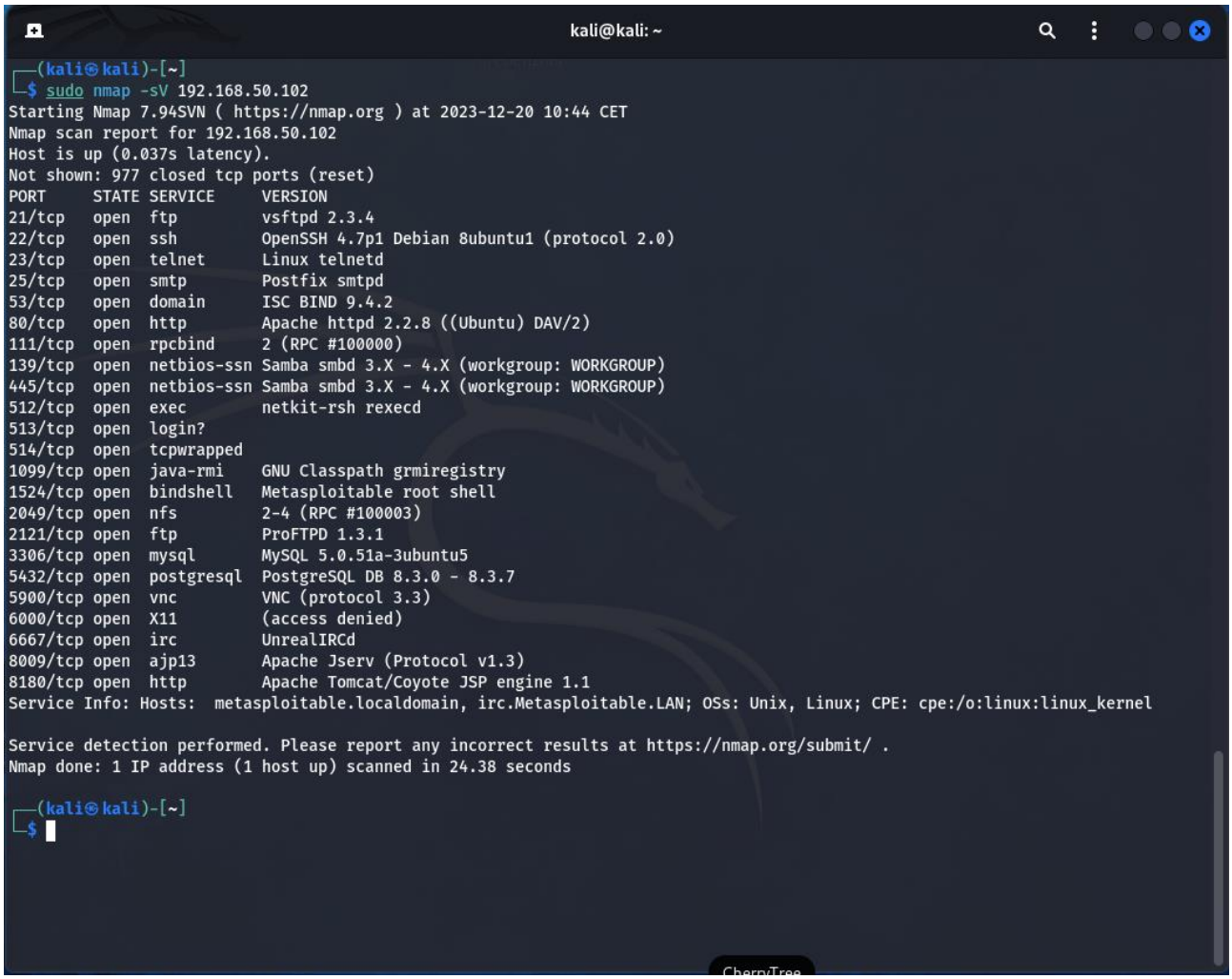
La risoluzione di questa vulnerabilità è stata gestita attraverso le seguenti misure:

Per risolvere il problema sarebbe necessario un aggiornamento del servizio SAMBA cosa non possibile data la mancanza della connessione ad internet. Abbiamo deciso di risolvere il problema utilizzando il firewall di Metasploitable2 impostando una nuova regola che bloccasse il traffico di dati sulle porte collegate al servizio SAMBA.

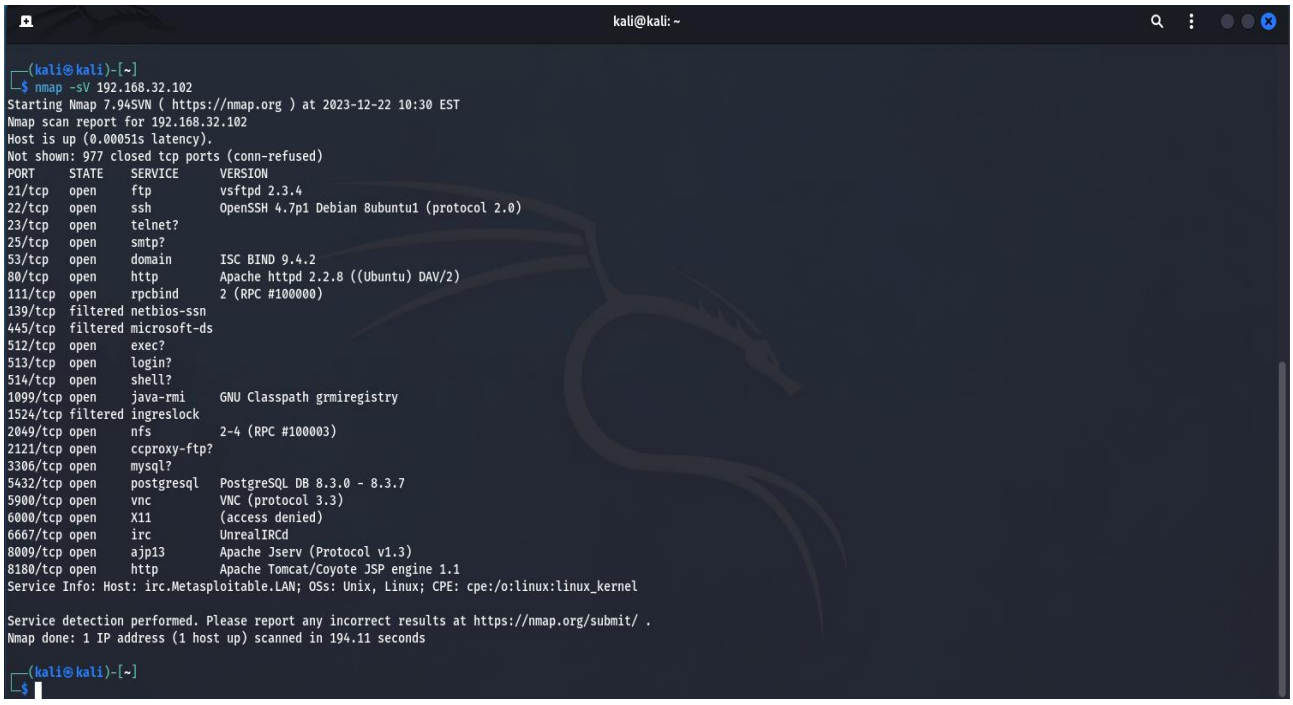
```
root@metasploitable:/etc/samba# sudo ufw enable
Firewall started and enabled on system startup
root@metasploitable:/etc/samba# sudo ufw default allow
Default policy changed to 'allow'
(be sure to update your rules accordingly)
root@metasploitable:/etc/samba# sudo ufw deny 139
Rule added
root@metasploitable:/etc/samba# sudo ufw deny 445
Rule added
root@metasploitable:/etc/samba# sudo ufw status
Firewall loaded

To                         Action  From
--                         ------  ----
1524:tcp                   DENY    Anywhere
1524:udp                   DENY    Anywhere
139:tcp                    DENY    Anywhere
139:udp                    DENY    Anywhere
445:tcp                    DENY    Anywhere
445:udp                    DENY    Anywhere

root@metasploitable:/etc/samba# _
```

Conclusione:

Per conoscere quali porte erano aperte ai servizi SAMBA e Backdoor è stato utilizzato nmap con una scansione di tipo -sV nel quale è possibile vedere il tipo di servizio in ascolto su ogni porta aperta. Di seguito la scansione nmap prima dell risoluzione per vedere i servizi in ascolto:



Di seguito lo scan di nmap dopo le risoluzioni:



Si noti come nelle porte che prima presentavano i servizi backdoor e SAMBA adesso risultano filtrate e non viene mostrato il servizio in ascolto.

Dopo aver implementato le soluzioni descritte, è stata condotta una nuova scansione con Nessus per garantire l'efficacia delle misure correttive. Tutte e quattro le vulnerabilità critiche sono state risolte con successo, riducendo significativamente i rischi di sicurezza associati al sistema.

Allegato Report dopo la risoluzione:

Vulnerabilities Total: 79

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	-	136808	ISC BIND Denial of Service
MEDIUM	5.9	-	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	-	11213	HTTP TRACE / TRACK Methods Allowed

Questo report mira a fornire una panoramica delle vulnerabilità individuate dopo la risoluzione delle vulnerabilità scelte del sistema Metasploitable2 dopo l'analisi con Nessus.