

Traccia:

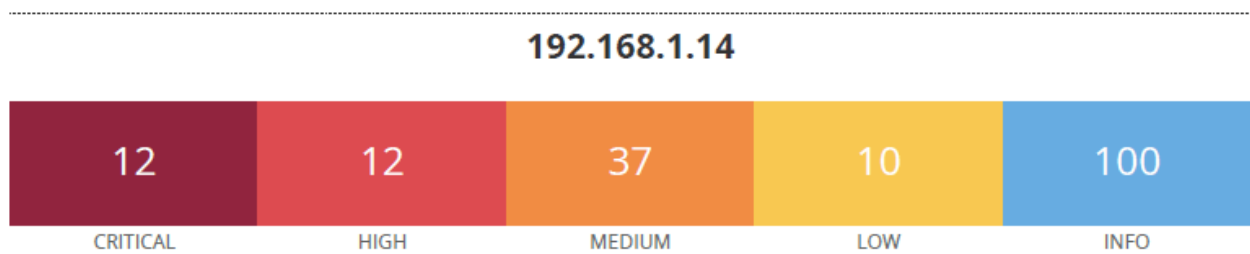
Effettuare una scansione completa sul target Metasploitable.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche e provate ad implementare delle azioni di rimedio.

N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili.

Vi consigliamo tuttavia di utilizzare magari questo approccio per non più di una vulnerabilità. Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Come da immagine, una volta effettuato lo scan tramite nessus su macchina metasploitable, il report generato ha evidenziato una serie di vulnerabilità sfruttabili. Precisamente 12 critiche, 12 alte, 37 medie, 10 basse e 100 informative.



La prima vulnerabilità analizzata è la seguente:

51988 - Bind Shell Backdoor Detection

Sinossi

L'host remoto potrebbe essere stato compromesso.

Descrizione

Una backdoor bind shell è un tipo di vulnerabilità di sicurezza in cui un aggressore ha creato una shell, o interfaccia a riga di comando, legata a una porta specifica su un sistema compromesso. Nel caso della vulnerabilità con ID 51988, la backdoor è in ascolto sulla porta 1524/tcp. Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla collegandosi alla porta remota e inviando direttamente i comandi.

Exploit:

Per sfruttare questa vulnerabilità e ottenere l'accesso alla shell, è possibile utilizzare uno strumento come Netcat o Telnet per connettersi al sistema remoto sulla porta 1524/tcp. Una volta connessi, sarà possibile inviare comandi alla shell e riceverne l'output.

Soluzione

Per mitigare il rischio di una backdoor bind shell, è possibile implementare diverse soluzioni:

1. **Aggiornamenti software:** Assicurarsi che tutto il software del sistema sia aggiornato e che siano state applicate tutte le patch di sicurezza.
2. **Regole del firewall:** Configurare le regole del firewall per bloccare il traffico in entrata sulla porta 1524/tcp, che è la porta predefinita utilizzata dalla backdoor. In questo modo si impedisce agli aggressori esterni di connettersi alla shell.

Servizio xinetd in ascolto su porta 1524 con PID 4464

```
root@metasploitable:/# sudo netstat -tulnp | grep 1524
tcp        0      0 0.0.0.0:1524        0.0.0.0:*          LISTEN      4464/xinetd
root@metasploitable:/# kill 4464
root@metasploitable:/# sudo netstat -tulnp 1524
```

Configurazione Firewall con regola per rigettare le connessioni tcp su 1524. Comando:

```
sudo iptables -A INPUT -p tcp --dport 1524 -j REJECT
```

```
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            udp dpt:nfs
REJECT     tcp  -- anywhere              anywhere               tcp dpt:ingreslock
reject-with icmp-port-unreachable

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

Kali non riesce più a connettersi alla porta 1524

```
(kali@kali)-[~]
$ nc 192.168.1.11 1524/tcp
(UNKNOWN) [192.168.1.11] 1524 (ingreslock) : Connection refused
```

Seconda vulnerabilità:

11356 - NFS Exported Share Information Disclosure

Sinossi

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione

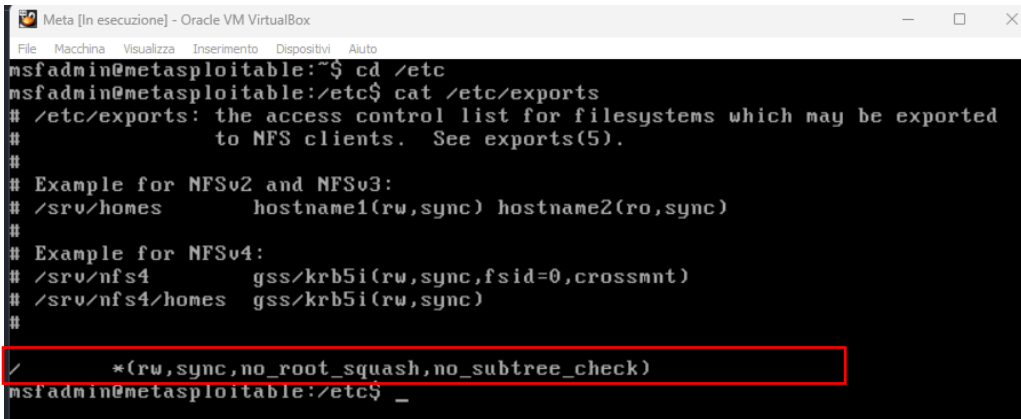
La vulnerabilità NFS (Network File System) Exported Share Information Disclosure, identificata da CVE-1999-0170, CVE-1999-0211 e CVE-1999-0554, si riferisce al rischio associato alle condivisioni NFS non correttamente configurate. Quando le condivisioni NFS non sono adeguatamente protette, un utente malintenzionato può essere in grado di accedere e potenzialmente manipolare dati sensibili sull'host remoto.

Soluzione

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

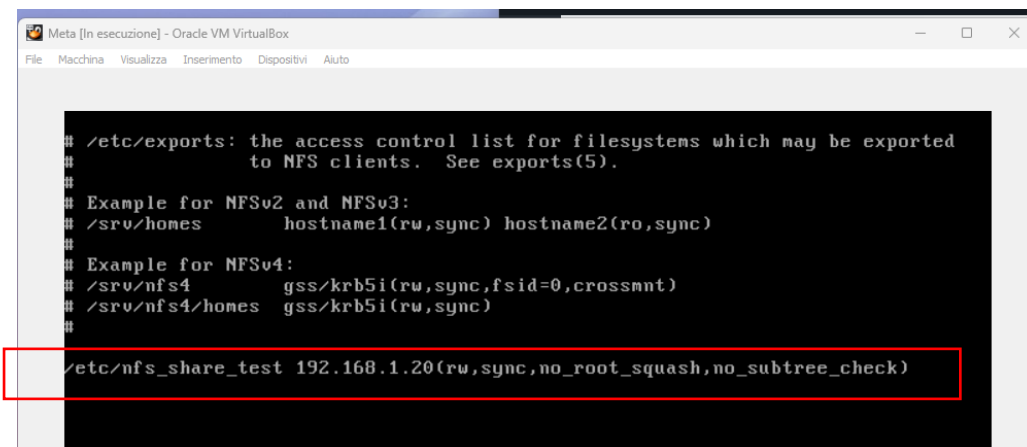
1. **Limitare le esportazioni NFS a client specifici:** Nel file `/etc/exports`, specificare gli indirizzi IP dei client che possono accedere alle condivisioni NFS. In questo modo si limiterà l'accesso alla condivisione NFS al client con indirizzo IP specificato.
Ho configurato anche il file `/etc/hosts.allow` con l'indirizzo di Kali. La cartella condivisa in questione è la `nsf_share_test`.
Di seguito gli screen della configurazione.

Comando `cat /etc/exports` per visualizzare i permessi, che in questo caso risulta che tutte le directory sono condivisibili. (/)



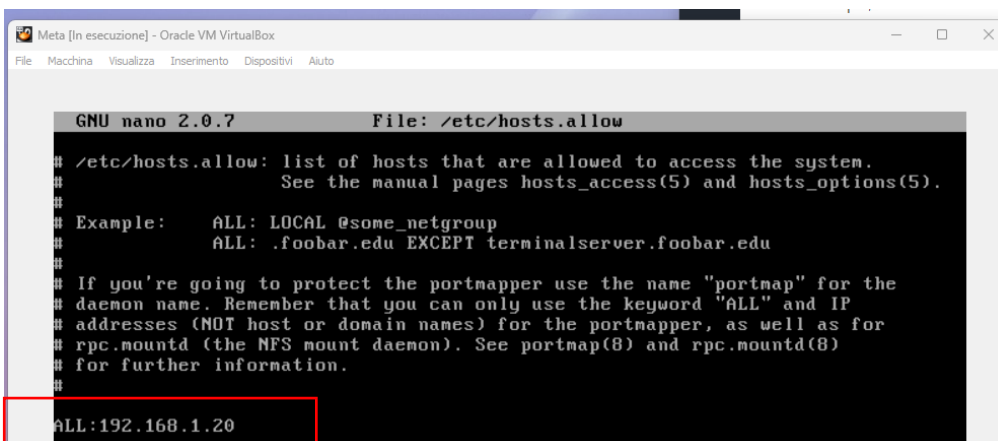
```
Meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
msfadmin@metasploitable:~$ cd /etc
msfadmin@metasploitable:/etc$ cat /etc/exports
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/ *(rw,sync,no_root_squash,no_subtree_check)
msfadmin@metasploitable:/etc$ _
```

Configurazione file `/etc/exports` per far in modo che solamente la directory `nsf_share_test` sia condivisibile con IP di Kali 192.168.1.20. Permessi di lettura e scrittura, i dati vengono scritti in modo sincrono sulla memoria.



```
Meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients. See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
/etc/nfs_share_test 192.168.1.20(rw,sync,no_root_squash,no_subtree_check)
```

Configurazione file `hosts.allow` in modo da permettere solo al IP di Kali 192.168.1.20 di accedere al sistema.



```
Meta [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
# See the manual pages hosts_access(5) and hosts_options(5).
#
# Example: ALL: LOCAL @some_netgroup
# ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
ALL:192.168.1.20
```

2. **Utilizzare le regole del firewall:** È possibile utilizzare le regole del firewall per limitare l'accesso al servizio NFS. Ad esempio, su Linux, si può usare iptables per bloccare tutto il traffico in entrata alla porta NFS (2049) e consentire solo il traffico da client affidabili.

Comando utilizzato per bloccare il traffico in entrata sulla porta 2049 e consentirlo solo a Kali.

```
sudo iptables -A INPUT -p udp --dport 2049 -s 192.168.1.20 -j ACCEPT
```

-A INPUT: Specifica che la regola verrà aggiunta alla catena INPUT, che gestisce il traffico in ingresso.

-p udp: Specifica il protocollo di trasporto da filtrare, in questo caso UDP.

--dport 2049: Specifica la porta di destinazione, che nel caso di NFS è la porta 2049, la porta predefinita utilizzata per le comunicazioni NFS.

-s 192.168.1.20: Specifica l'indirizzo IP sorgente del traffico che verrà consentito. In questo caso, è l'indirizzo IP 192.168.1.20 di Kali

-j ACCEPT: Specifica l'azione da intraprendere se il pacchetto corrisponde alla regola, in questo caso, accetta il pacchetto e consente il passaggio attraverso il firewall.

La terza vulnerabilità:

61708 - VNC Server 'password' Password

Sinossi

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

Descrizione

Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è stato in grado di effettuare il login utilizzando l'autenticazione VNC e una password "password". Un aggressore remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.

L'opzione "password" del server VNC 61708 serve a proteggere l'accesso remoto al server richiedendo l'inserimento di una password prima di stabilire una connessione. Si tratta di un'importante funzione di sicurezza, in quanto aiuta a prevenire l'accesso non autorizzato al server e ai sistemi collegati.

Per impostare una password nel server VNC 61708, è possibile utilizzare lo strumento di configurazione del server VNC o l'interfaccia a riga di comando del server VNC. Quando si imposta la password, è importante sceglierne una forte e unica che non possa essere facilmente indovinata o forzata. È inoltre buona norma cambiare regolarmente la password per aumentare ulteriormente la sicurezza.

Una volta impostata la password, a qualsiasi utente che tenti di connettersi al server VNC verrà richiesto di inserire la password. Se non viene inserita la password corretta, la connessione viene rifiutata.

La funzione "password" del Server VNC 61708 è uno strumento essenziale per garantire l'accesso remoto ai sistemi e proteggere i dati.

Exploit:

Innanzitutto, è necessario identificare il sistema di destinazione che esegue la versione vulnerabile del server VNC 61708, in questo caso metasploitable. È possibile utilizzare vari strumenti come Nmap, Nessus o qualsiasi altro scanner di rete per identificare il server VNC e la sua versione.

Una volta identificato il sistema di destinazione, è possibile utilizzare uno strumento come **Hydra** per forzare la password VNC. Hydra è un potente strumento di cracking delle password che può essere utilizzato per

eseguire un **attacco a dizionario sul server VNC**. Ecco un esempio di comando per utilizzare Hydra per forzare la password VNC:

```
hydra -L usernames.txt -P passwords.txt vnc://target_ip -s 5900 -t 4
```

In questo comando, *usernames.txt* è un file contenente un elenco di nomi utente da provare, *passwords.txt* è un file contenente un elenco di password da provare, *target_ip* è l'indirizzo IP del sistema di destinazione e *5900* è la porta predefinita del server VNC. L'opzione *-t* specifica il numero di thread da utilizzare per l'attacco.

Se il server VNC utilizza una password debole, Hydra dovrebbe essere in grado di decifrarla in pochi minuti. Una volta ottenuta la password, potete utilizzare un client VNC come **TightVNC** o **RealVNC** per connettervi al server VNC e ottenere l'accesso remoto al sistema di destinazione.

Una volta ottenuto l'accesso al sistema di destinazione, è possibile eseguire diverse azioni come installare malware, rubare dati sensibili o spostarsi lateralmente all'interno della rete.

Soluzione

Proteggere il servizio VNC con una password forte. ES: Al-87We

Configurazione di una nuova pass con comando vncpasswd

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Warning: password truncated to the length of 8.
Verify:
```

Configurazione firewall per permettere solo ad ip Kali 192.168.1.20 di mettersi in ascolto sulla porta 5900

Comando: `sudo iptables -A INPUT -p tcp --dport 5900 -s 192.168.1.20 -j ACCEPT`

```
ACCEPT      tcp    --  kali.station          anywhere              tcp dpt:5900
```

Quarta vulnerabilità:

33850 - Unix Operating System Unsupported Version Detection

Sinossi

Il sistema operativo in esecuzione sull'host remoto non è più supportato.

Descrizione

Secondo il numero di versione dichiarato, il sistema operativo Unix in esecuzione sull'host remoto non è più supportato.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, è probabile che contenga vulnerabilità di sicurezza.

Exploit:

Per sfruttare questa vulnerabilità, un utente malintenzionato dovrebbe creare un payload dannoso che si rivolge alla versione specifica del sistema operativo Unix non supportata. Questo payload verrebbe inviato al sistema interessato attraverso un servizio vulnerabile, come SSH.

1. **Identificare il sistema di destinazione:** L'attaccante deve identificare il sistema di destinazione che esegue la versione non supportata del sistema operativo Unix. Questo può essere fatto scansionando la rete alla ricerca di sistemi che eseguono versioni vulnerabili note di Unix.
2. **Creare il payload dannoso:** L'aggressore deve creare un payload che si rivolga alla versione specifica del sistema operativo Unix. Questo payload potrebbe includere comandi per aumentare i privilegi, eseguire codice arbitrario o ottenere un accesso non autorizzato al sistema.
3. **Inviare il payload al sistema di destinazione:** L'aggressore deve inviare il payload dannoso al sistema di destinazione attraverso un servizio vulnerabile, come SSH. Questo può essere fatto utilizzando uno strumento come Metasploit o creando manualmente un comando SSH.
4. **Eseguire il payload:** Una volta che il payload è stato ricevuto dal sistema di destinazione, deve essere eseguito. Ciò potrebbe essere fatto sfruttando una vulnerabilità di iniezione di comandi nel servizio SSH.
5. **Ottenere un accesso non autorizzato o aumentare i privilegi:** Dopo aver eseguito il payload, l'aggressore otterrebbe l'accesso non autorizzato al sistema o l'escalation dei privilegi, a seconda del payload utilizzato.

Soluzione

La soluzione a questa vulnerabilità consiste nell'aggiornare il sistema operativo Unix a una versione supportata. L'aggiornamento a una versione supportata garantisce che il sistema riceva le patch di sicurezza e gli aggiornamenti più recenti dal fornitore, riducendo il rischio di sfruttamento.

Quinta vulnerabilità:

171340 - Apache Tomcat SEoL (<= 5.5.x)

Sinossi

Sull'host remoto è installata una versione non supportata di Apache Tomcat.

Descrizione

Secondo la sua versione, Apache Tomcat è inferiore o uguale a 5.5.x. Pertanto, non è più mantenuto dal suo fornitore o provider.

La mancanza di supporto implica che il fornitore non rilascerà nuove patch di sicurezza per il prodotto. Di conseguenza, potrebbe contenere vulnerabilità di sicurezza.

Exploit:

Per sfruttare Apache Tomcat SEoL (<= 5.5.x), è possibile utilizzare il framework Metasploit per sfruttare una vulnerabilità nota (CVE-2010-1157) che consente il caricamento e l'esecuzione di file arbitrari.

Soluzione

Aggiornare a una versione di Apache Tomcat attualmente supportata.

Conclusione scan post remediation:

Una volta effettuate le implementazioni ho effettuato nuovamente lo scan sulla macchina Metasploitable da Kali.

Come possiamo osservare dal report post remediation. La vulnerabilità n1, cioè la **51988 Bind Shell Backdoor** non è più presente in elenco. Possiamo controllare dall'immagine sotto.

Stessa cosa possiamo notare con la vulnerabilità n3. La **61708 VNC Server Password**.

Discorso diverso per le vulnerabilità **33850** e **171340** che richiedevano un semplice aggiornamento alla versione più recente patchata, cosa che però non ho voluto fare intenzionalmente per evitare di "pulire" troppo Metasploitable, visto che comunque è una macchina vulnerabile di default.

Vulnerabilities					Total: 156
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME	
CRITICAL	9.8	8.9	70728	Apache PHP-CGI Remote Code Execution	
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection	
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)	
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)	
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection	
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure	
CRITICAL	10.0*	7.4	46882	UnrealIRCd Backdoor Detection	

Ultima vulnerabilità, la **11356 NFS Exported Share**, che possiamo ancora vedere in elenco ma che però è stata risolta configurando i permessi per una cartella condivisa precisa con un IP preciso, come possiamo vedere dall'immagine sotto la soluzione è andata a buon fine.

Plugin Information

Published: 2003/03/12, Modified: 2023/08/30

Plugin Output

udp/2049/rpc-nfs

The following NFS shares could be mounted :

+ /etc/nfs_share_test