

Scansione Completa su Metasploitable:

Analisi e risoluzione
vulnerabilità



Sommario

Punti principali di questa presentazione

- Traccia esercizio
- Modalità scansione e risultati
- Analisi vulnerabilità - VULNERABILITÀ: Server ‘password’ Password
- VULNERABILITÀ: Bind Shell Backdoor Detection
- VULNERABILITÀ: NFS Exported Share Information Disclosure
- VULNERABILITÀ: Apache Tomcat AJP Connector Request Injection (Ghostcat)

Traccia:

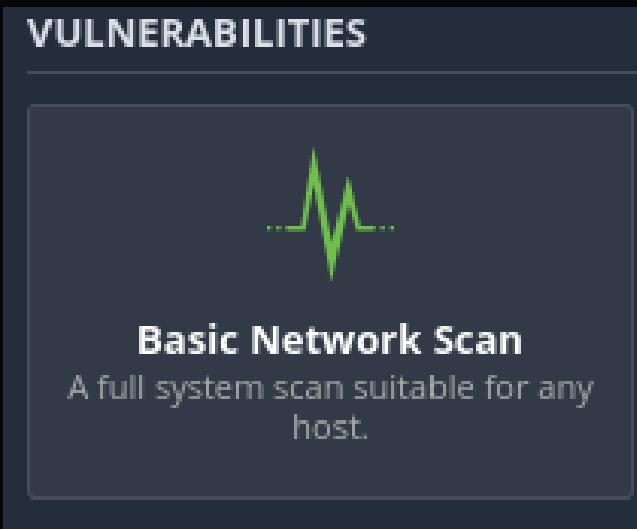
Effettuare una scansione completa sul target Metasploitable. Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche / high e provate ad implementare delle azioni di rimedio.

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.



Modalità scansione e risultati



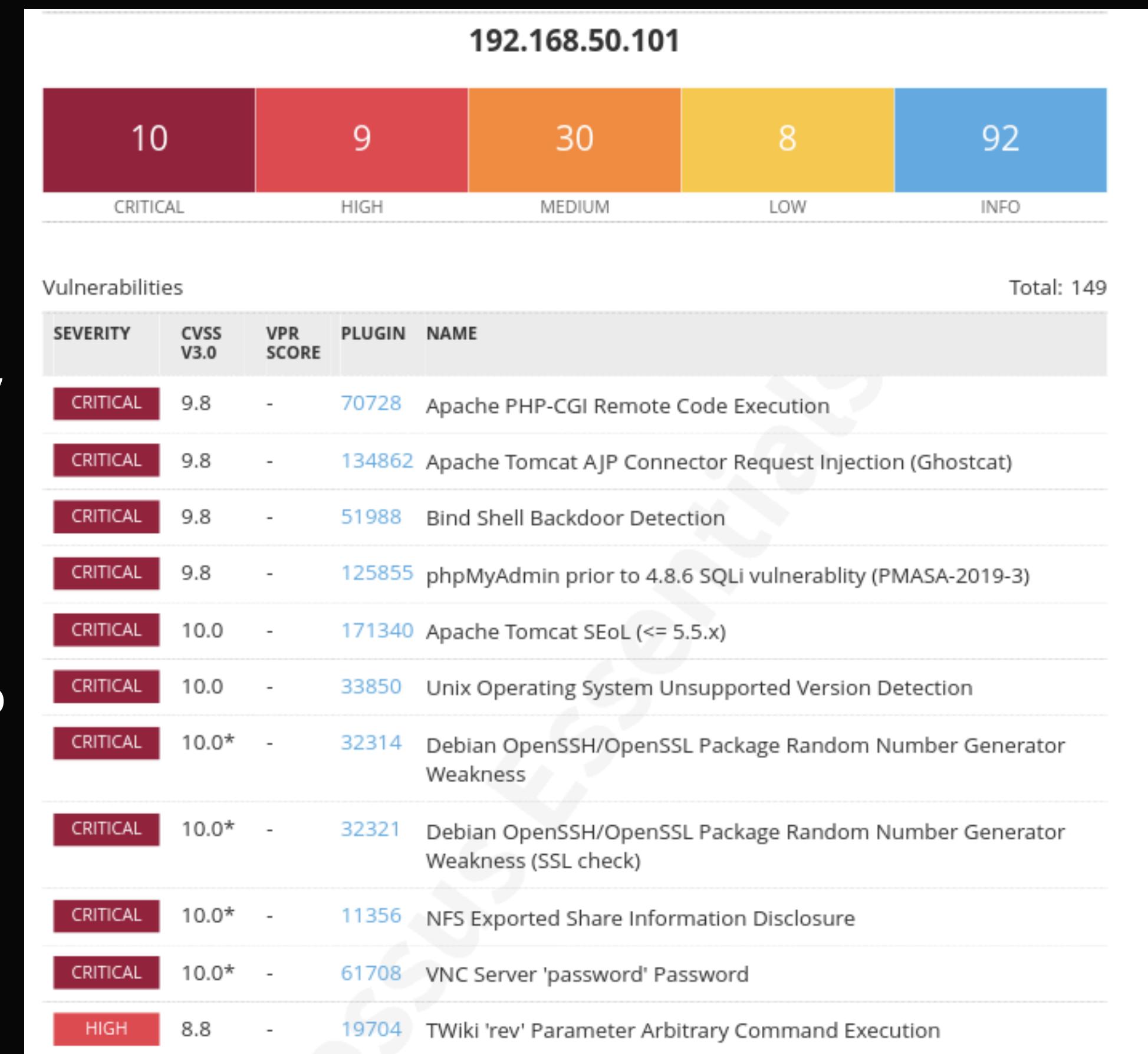
Si è programmata una scansione completa su Nessus utilizzando il tool 'Basic Network Scan'. In questa scansione si è deciso di fare una **scansione di tutte le porte** e per tutti i tipi di **vulnerabilità web**



Il target della scansione è Metasploitable 2

A seguito della scansione effettuata, Nessus ha redatto un report delle vulnerabilità trovate, dividendole per livello di criticità.

In questo report si analizzano solo 4 delle vulnerabilità di livello critico trovate.



Analisi vulnerabilità

1. VULNERABILITÀ: 61708 - VNC Server 'password' Password

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.

Soluzione

Proteggere il servizio VNC con una password forte.

Risoluzione:

Si è cambiata la password del server VNC, tramite il terminale di Meta.

Si sono presi i permessi di amministrazione usando il comando **sudo su**, e tramite il comando **vncpasswd** si è cambiata la password.

```
root@metasploitable:/home/msfadmin# 
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

Output	
Port	Hosts
5900 / tcp / vnc	192.168.50.101

Analisi vulnerabilità

2. VULNERABILITÀ: 51988 - Bind Shell Backdoor Detection

Descrizione

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.

Soluzione

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Risoluzione:

Questa vulnerabilità indica la presenza di una backdoor sulla porta 1524. Per far fronte a tale problematica si possono usare 2 metodi:

- chiusura della porta 1524
- creare una regola firewall che filtri il traffico verso la porta

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	192.168.50.101

Risoluzione 1:

Tramite il comando **sudo netstat -tulnp | grep 1524** (con -t tcp, -u udp, -l listening per le porte in ascolto, -n numeric, -p programma che sta usando quella porta) dal terminale di Meta si va a verificare lo stato della porta 1524 e il processo che la sta utilizzando.

Con il comando **sudo kill 4408** si va a chiudere la porta 1524, e quindi il programma che la stava usando.

Da Kali si verifica che la porta sia stata chiusa con il comando:

sudo nmap -sS -p 1524 indirizzo_ip_Meta

The screenshot shows the 'Edit Firewall rule' screen in Pfsense. The rule is set to 'Block' and is currently 'Disabled'. It applies to the 'LAN' interface and TCP protocol. The source is set to 'not' 192.168.49.100 and the destination is 192.168.50.101. The destination port range is 1524. Logging is enabled. A large white arrow points from this rule to the 'nmap' command output on the right.



```
msfadmin@metasploitable:~$ sudo netstat -tulpn | grep 1524
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
tcp        0      0 0.0.0.0:1524          0.0.0.0:*                LISTEN
4408/xinetd
msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ sudo kill 4408
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

```
Nmap was able to execute the command "id" using the
(kali㉿kali)-[~]
$ sudo nmap -sS -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 13:24 CEST
Nmap scan report for 192.168.50.101
Host is up (0.00026s latency).

PORT      STATE SERVICE
1524/tcp  closed  ingreslock
MAC Address: 08:00:27:76:1A:F6 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.14 seconds
To see debug logs, please visit individual host
```

Risoluzione 2:

Si è creata una regola firewall utilizzando Pfsense che filtrasse il traffico sulla porta 1524.

Dal terminal di Kali si è verificata l'effettività della regola firewall con il comando **sudo nmap -Pn -p 1524 indirizzo_ip_Meta**.

Si noti dall'output come la porta 1524 ora sia filtrata.

The screenshot shows the 'Floating' tab of the Firewall Rules list. It displays three rules: an 'Anti-Lockout Rule' (disabled), a 'Default allow LAN to any rule' (disabled), and a new rule that matches traffic from 192.168.49.100 to 192.168.50.101 on port 1524.

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
1	*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule
2	*	LAN net	*	*	*	*	none		Default allow LAN to any rule
3	TCP	192.168.49.100	*	192.168.50.101	1524	*	none		

```
(kali㉿kali)-[~]
$ sudo nmap -Pn -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-10 16:29 CEST
Nmap scan report for 192.168.50.101
Host is up.

PORT      STATE SERVICE
1524/tcp  filtered  ingreslock
to: | (other) | 1524
Nmap done: 1 IP address (1 host up) scanned in 15.08 seconds
Specify the port or port range for the destination of the packet for this rule
```

Analisi vulnerabilità

3. VULNERABILITÀ: 11356 - NFS Exported Share Information Disclosure

Descrizione

Almeno una delle condivisioni NFS esportate dal server remoto potrebbe essere montata dall'host di scansione. Un utente malintenzionato potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione

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

Risoluzione:

Si va a modificare il file di configurazione <exports> dal terminale di Meta per cambiare i permessi agli utenti che accedono all'host remoto.

```
GNU nano 2.0.7          File: /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,async,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,async)
#
# *(rw,async,no_root_squash,no_subtree_check)
```



```
GNU nano 2.0.7          File: /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,async,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,async)
#
# *(ro,sync,no_root_squash,no_subtree_check)
```

Analisi vulnerabilità

4. VULNERABILITÀ: 134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat)

Descrizione

È stata riscontrata una vulnerabilità nella lettura/inclusione di file in AJP connector. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione web da un server vulnerabile.

Nei casi in cui il server vulnerabile consente il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file e ottenere l'esecuzione di codice remoto (RCE).

Soluzione

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o versione successiva.

Risoluzione:

Per risolvere questa vulnerabilità si è aggiornato Apache2 alla versione più recente.

In particolare, in questo caso, non è stato possibile aggiornare Apache2 in quanto Meta è una distribuzione Ubuntu non più supportata, e quindi risulta difficile trovare i pacchetti giusti dai repo ufficiali per l'aggiornamento.

In una situazione ideale sarebbe possibile aggiornare Apache2 e quindi risolvere tale vulnerabilità

```
msfadmin@metasploitable:~$ sudo apt-get install true --only-upgrade apache2
E: Sense only is not understood, try true or false.
msfadmin@metasploitable:~$ sudo apt-get true install --only-upgrade apache2
E: Sense only is not understood, try true or false.
msfadmin@metasploitable:~$ sudo apt-get --only-upgrade true install apache2
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  apache2-mpm-worker apache2.2-common
Suggested packages:
  apache2-doc
The following packages will be REMOVED:
  apache2-mpm-prefork
The following NEW packages will be installed:
  apache2-mpm-worker
The following packages will be upgraded:
  apache2 apache2.2-common
2 upgraded, 1 newly installed, 1 to remove and 136 not upgraded.
Need to get 1042kB of archives.
After this operation, 24.6kB of additional disk space will be used.
Do you want to continue [Y/n]? y
WARNING: The following packages cannot be authenticated!
  apache2 apache2.2-common apache2-mpm-worker
Install these packages without verification [y/N]? _
```