

VULNERABILITY SCANNING



Scansione delle Vulnerabilità

LABORATORIO EPICODE

Obiettivo

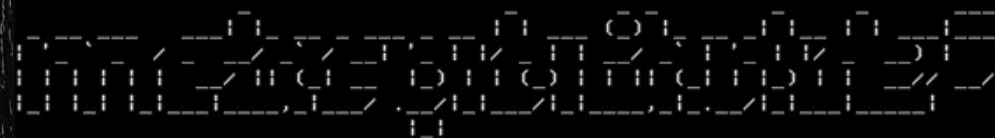
Prenderemo in esame 2 Vulnerabilità di livello **CRITICAL** e 2 Vulnerabilità di livello **HIGH** in modo da esaminarle nel dettaglio ed applicare i suoi relativi rimedi

Effettueremo una scansione completa delle Vulnerabilità sul Target Metasploitable_2

Indirizzo IP dell'Host: 192.168.50.1

```
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out'

[ OK ]
```



Warning: Never expose this VM to an untrusted network!

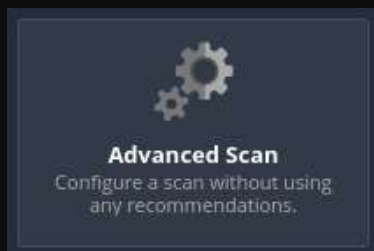
Contact: [msfdev\[at\]metasploit.com](mailto:msfdev[at]metasploit.com)

Login with msfadmin/msfadmin to get started

metasploitable login: _

Come su richiesta, abbiamo selezionato una Scansione Avanzata in modo da analizzare:

- ✓ Informazioni generali
- ✓ Metodi Ping (ARP, TCP E UDP)
- ✓ Port Scanning
- ✓ Login e Password
- ✓ Impostazioni Web Application
- ✓ Impostazioni Malware



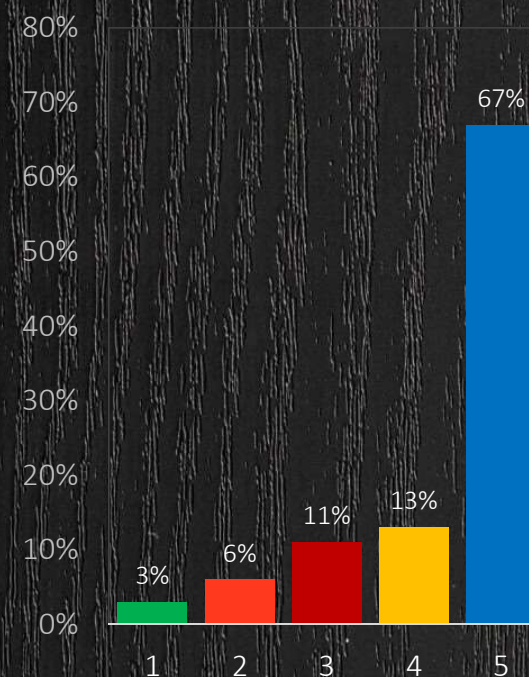
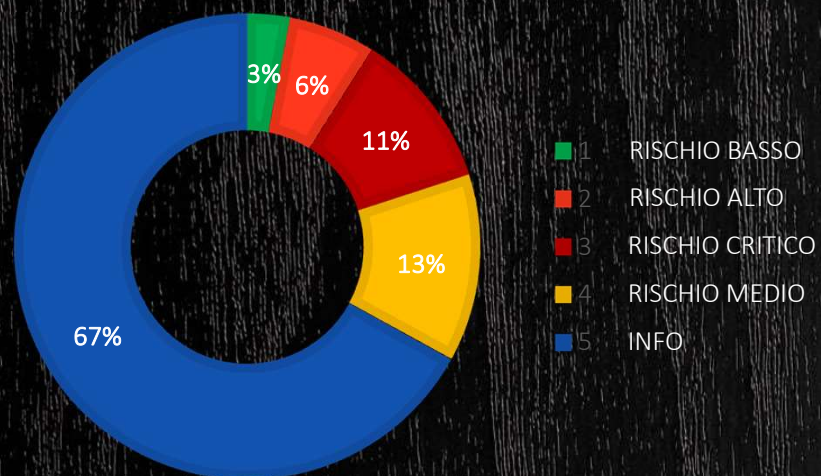
Scansione Avanzata

Fornisce un maggiore controllo sull'efficienza della scansione e sulle operazioni di una scansione, nonché la possibilità di abilitare il debug dei plug-in.

Risultati Analisi

Nell'Analisi Avanzata applicando i diversi filtri abbiamo riscontrato le seguenti Vulnerabilità di cui:

GRAFICO



Vulnerabilità Critiche

Tra le 8 riscontrate esamineremo le 2 Vulnerabilità Critiche selezionate

1

CRITICAL

NFS Exported Share Information Disclosure

2

CRITICAL

Bind Shell Backdoor Detection

Nell'Analisi Avanzata applicando i diversi filtri abbiamo riscontrato le seguenti 2 vulnerabilità critiche:

- NFS Exported Share Information Disclosure: 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 questo per leggere (ed eventualmente scrivere) file sull'host remoto.
- Bind Shell Backdoor Detection: una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

1 – CRITICAL: NFS Exported Share Information Disclosure

Analisi nel dettaglio

CRITICAL

NFS Exported Share Information Disclosure

Descrizione: Divulgazione delle informazioni sulle condivisioni esportate

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 questo per leggere (ed eventualmente scrivere) file sull'host remoto.

Soluzione:

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

Soluzione a NFS Exported Share Information Disclosure

NFS (Network File System) è un protocollo di rete utilizzato in ambiente Unix per la condivisione di file. Sviluppato originariamente da Sun Microsystems nel 1984 come progetto sperimentale, divenne presto uno standard pubblico. NFS è stato il primo file system di rete ad essere basato sul protocollo IP, favorendone la diffusione e promuovendo l'interoperabilità tra sistemi eterogenei. Giunto ormai alla versione 4.2, NFS continua ad essere attivamente supportato dalla IETF (Internet Engineering Task Force).

Nella terminologia di NFS, le directory da condividere si chiamano "export". La lista degli export si trova nel file `/etc/exports`. Per aggiungere un export, è sufficiente aprire il file `/etc/exports` con un editor di testo.

Ogni riga corrisponde ad un export, specificando il percorso locale della directory da esportare, le modalità di accesso ed i client autorizzati a collegarsi.

```
[ Wrote 12 lines ]
root@metasploitable:/etc# cat 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 192.168.50.100(rw,sync,no_root_squash) 192.168.50.100(ro,sync,no_r
# ot_squash)
#
# Example for NFSv4:
# /srv/nfs4   gss/krb5i(rw,sync,fsid=0,crossmnt,no_root_squash)
# /srv/nfs4/homes gss/krb5i 192.168.50.100(rw,sync,no_root_squash)
#
# *(rw,sync,no_root_squash,no_subtree_check)
root@metasploitable:/etc#
```

Per porre rimedio all'errore critico che permette ad un client remoto di assumere eventuali privilegi, inseriremo l'opzione «no_root_squash» per impedire all'utente root di un client di assumere i privilegi di root anche sul server: questa opzione permette di evitare errori potenzialmente dannosi, proteggendo i file sul server; inoltre è possibile restringere l'accesso ai client, discriminandoli attraverso indirizzo IP o nome host

2 – CRITICAL: Bind Shell Backdoor Detection:

Analisi nel dettaglio

CRITICAL

NFS Exported Share Information Disclosure

Descrizione: Rilevamento backdoor di shell vincolata

- Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarlo collegandosi alla porta remota e inviando direttamente i comandi.

Soluzione:

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

Soluzione a Bind Shell Backdoor

Detection

Abbiamo provato ad effettuare una scansione con nmap per comprendere dove fosse situata la bindshell trovata nelle vulnerabilità ed l'abbiamo rilevata sulla porta aperta 1524

```
(kali@kali)-[~]
$ nmap -sV 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-11 18:40 EDT
Nmap scan report for 192.168.50.101
Host is up (0.00014s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login?
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
```

Come funziona una Bind Shell

Un programma dannoso viene eseguito sul computer della vittima, spesso a causa di una vulnerabilità o di ingegneria sociale.

Il programma apre una porta di rete specifica, in genere su un numero di porta predefinito.

L'aggressore si connette a questa porta aperta utilizzando un programma client.

Una volta stabilita la connessione, l'aggressore ha accesso a un prompt dei comandi sul sistema della vittima.

Le Bind Shell possono essere utilizzate dagli hacker per l'accesso e il controllo non autorizzati su una macchina remota, rendendoli un significativo problema di sicurezza.

Per porre rimedio all'errore critico di una Backdoor dovremmo reinstallare il sistema operativo o effettuare un aggiornamento completo del sistema ma per motivi didattici sulla macchina Metasploitable non abbiamo potuto effettuare l'aggiornamento in quanto il sistema, essendo datato, non ci permette di effettuare nessun upgrade

Vulnerabilità Alte

Tra le 2 riscontrate esamineremo le 2 Vulnerabilità Alte selezionate

1

HIGH

Samba Badlock Vulnerability

2

HIGH

NFS Shares World Readable

Nell'Analisi Avanzata applicando i diversi filtri abbiamo riscontrato le seguenti 2 vulnerabilità Alte:

- **Samba Badlock Vulnerability:** La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici.
- **NFS Shares World Readable:** Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP o intervallo IP).

1 – HIGH: Samba Badlock Vulnerability

Analisi nel dettaglio

HIGH

Samba Badlock Vulnerability

Descrizione: Vulnerabilità del badlock di Samba

- La versione di Samba, un server CIFS/SMB per Linux e Unix, in esecuzione sull'host remoto è affetta da un difetto, noto come Badlock, presente nel Security Account Manager (SAM) e nella Local Security Authority (Domain Policy) (LSAD) a causa di una negoziazione impropria del livello di autenticazione sui canali RPC (Remote Procedure Call). Un utente malintenzionato man-in-the-middle in grado di intercettare il traffico tra un client e un server che ospita un database SAM può sfruttare questa falla per forzare un downgrade del livello di autenticazione, che consente l'esecuzione di chiamate di rete Samba arbitrarie nel contesto dell'utente intercettato, come visualizzare o modificare dati sensibili di sicurezza nel database di Active Directory (AD) o disabilitare servizi critici.

Soluzione:

Aggiornare alla versione Samba 4.2.11 / 4.3.8 / 4.4.2 o successiva.

Soluzione a Samba Badlock Vulnerability

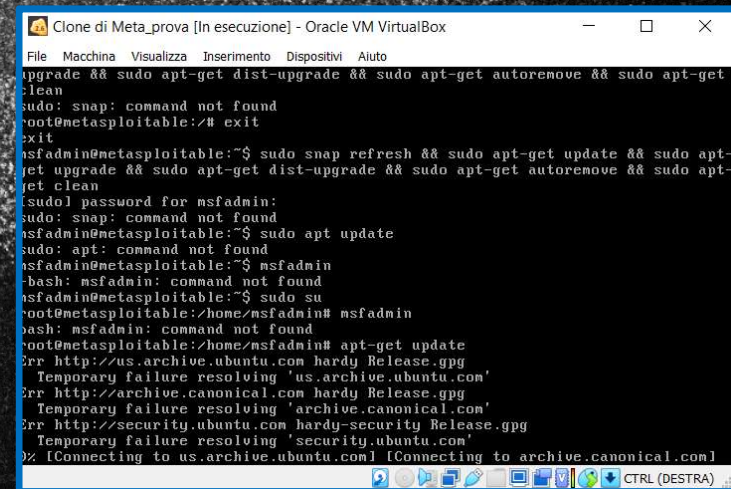
Abbiamo provato ad effettuare un scansione con nmap per individuare la versione di Samba

```
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)  
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
```

Successivamente abbiamo provato ad effettuare l'aggiornamento, ma siccome il sistema è molto datato non abbiamo potuto scaricare gli aggiornamenti necessari

La vulnerabilità Badlock (CVE-2016-2118) è stata inizialmente considerata una falla di sicurezza critica che potrebbe potenzialmente consentire a un utente malintenzionato di intercettare e manipolare il traffico tra server e client Samba, portando a vari rischi per la sicurezza tra cui attacchi man-in-the-middle, accesso non autorizzato a dati sensibili ed esecuzione di codice arbitrario su sistemi vulnerabili... Il nome "Badlock" è stato dato alla vulnerabilità come parte di una campagna di marketing coordinata volta a sensibilizzare l'opinione pubblica sul problema prima della sua divulgazione pubblica. Tuttavia, la gravità della vulnerabilità è stata dibattuta all'interno della comunità della sicurezza informatica, con alcuni esperti che hanno criticato l'hype che la circonda.

Dopo la sua scoperta, il team di Samba ha rilasciato rapidamente delle patch per risolvere la vulnerabilità Badlock. Si consiglia vivamente agli amministratori di sistema di applicare tempestivamente queste patch per mitigare il rischio di sfruttamento.



```
Clone di Meta_prova [In esecuzione] - Oracle VM VirtualBox  
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto  
upgrade && sudo apt-get dist-upgrade && sudo apt-get autoremove && sudo apt-get  
clean  
sudo: snap: command not found  
root@metasploitable:~# exit  
exit  
msfadmin@metasploitable:~$ sudo snap refresh && sudo apt-get update && sudo apt-  
get upgrade && sudo apt-get dist-upgrade && sudo apt-get autoremove && sudo apt-  
get clean  
[sudo] password for msfadmin:  
sudo: snap: command not found  
msfadmin@metasploitable:~$ sudo apt update  
sudo: apt: command not found  
msfadmin@metasploitable:~$ msfadmin  
bash: msfadmin: command not found  
msfadmin@metasploitable:~$ sudo su  
root@metasploitable:/home/msfadmin# msfadmin  
bash: msfadmin: command not found  
root@metasploitable:/home/msfadmin# apt-get update  
Err http://us.archive.ubuntu.com hardy Release.gpg  
Temporary failure resolving 'us.archive.ubuntu.com'  
Err http://archive.canonical.com hardy Release.gpg  
Temporary failure resolving 'archive.canonical.com'  
Err http://security.ubuntu.com hardy-security Release.gpg  
Temporary failure resolving 'security.ubuntu.com'  
% [Connecting to us.archive.ubuntu.com] [Connecting to archive.canonical.com]
```

2 – HIGH: NFS Shares World Readable

Analisi nel dettaglio

HIGH

NFS Shares World Readable

Descrizione: NFS condivide la leggibilità mondiale

- Il server NFS remoto sta esportando una o più condivisioni senza limitare l'accesso (in base a nome host, IP o intervallo IP).

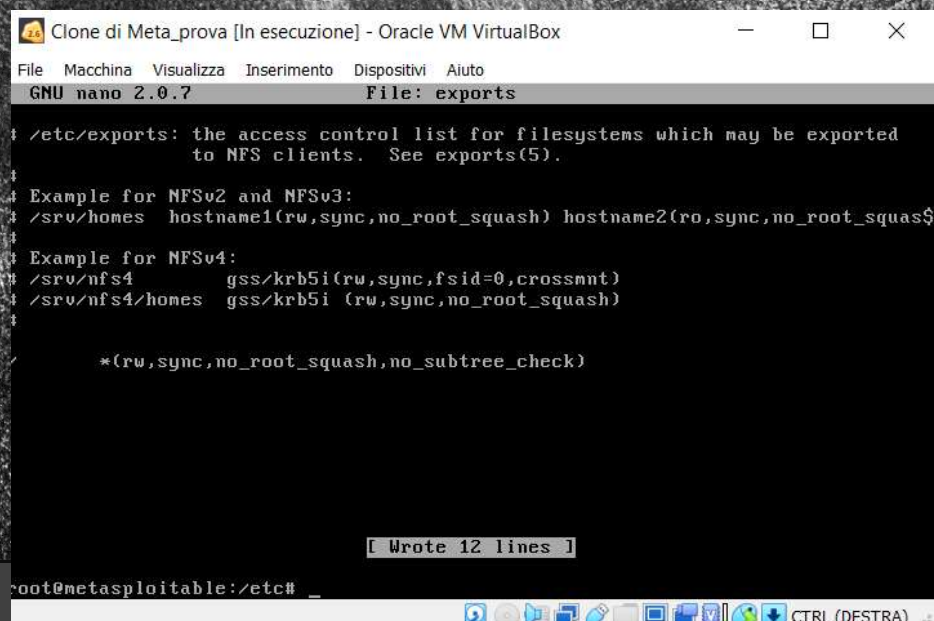
Soluzione:

Posizionare le opportune restrizioni su tutte le condivisioni NFS.

Soluzione a NFS Shares World Readable

Abbiamo posizionato le opportune restrizioni su tutte le condivisioni NFS

NFS Shares World Readable è soggetto a segnalazioni di falsi positivi da parte della maggior parte delle soluzioni di valutazione delle vulnerabilità. AVDS è l'unico a utilizzare test basati sul comportamento che eliminano questo problema. Per tutti gli altri strumenti VA i consulenti per la sicurezza consiglieranno la conferma mediante osservazione diretta. In ogni caso, le procedure di test di penetrazione per il rilevamento di NFS Shares World Readable producono il più alto tasso di accuratezza del rilevamento, ma la rarità di questa costosa forma di test ne diminuisce il valore. L'ideale sarebbe avere la precisione del pentesting e le possibilità di frequenza e portata delle soluzioni VA, e questo è possibile solo con AVDS.



```
Clone di Meta_prova [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: 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,no_root_squash) hostname2(ro,sync,no_root_squash)
#
# Example for NFSv4:
# /srv/nfs4 gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i (rw,sync,no_root_squash)
#
# *(rw,sync,no_root_squash,no_subtree_check)

[Wrote 12 lines ]
root@metasploitable:/etc# _
```


Conclusioni

In conclusione abbiamo effettuato delle operazioni di risanamento sul target Metasploitable2 in esame in modo da mitigare alcune Vulnerabilità per riuscire a rafforzare il sistema operativo.

Abbiamo quindi effettuato successivamente un'analisi avanzata con Nessus e riscontrato alcuni miglioramenti inerenti alle problematiche precedentemente riscontrate.

Grazie per l'attenzione

Mario Marsicano 

+1 23 987 6554 

mario@gmail.com 

www.epicode.com 