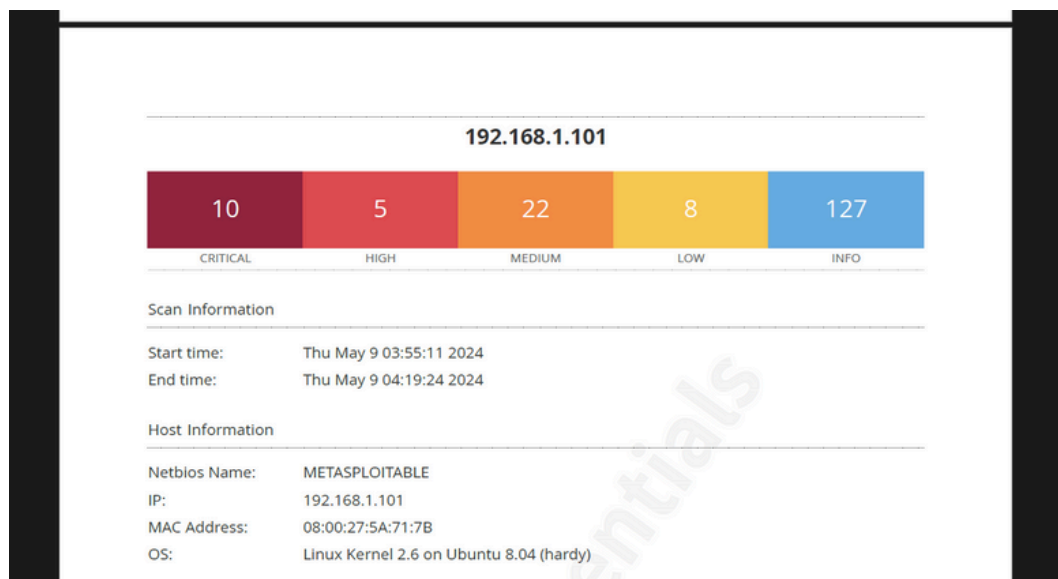


Metasploitable Nessus Scan

L'esercizio richiede di prendere 4 vulnerabilità di livello critico e risolverle. La scansione effettuata ha trovato solo 3 di quelle richieste.



1. Bind Shell Backdoor Detection

La prima vulnerabilità è una shell non autenticata, alla quale si può accedere senza credenziali semplicemente collegandosi dalla porta 1524, evidenziata in figura, con un'applicazione come Netcat. Da questa shell un utente malevolo potrebbe inserire comandi dall'esterno e potenzialmente arrivare ad ottenere i privilegi da amministratore, in pratica "impossessandosi" della macchina.

Potenziale Soluzione

Si potrebbe configurare la shell in modo che venga richiesta un'autenticazione prima di poter immettere input, questo sarebbe una buona misura di prevenzione. La soluzione se il problema è già in atto consiste nel killare il processo che tiene aperta la shell.

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

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Plugin Information

Published: 2011/02/15, Modified: 2022/04/11

Plugin Output

tcp/1524/wild_shell

Beerus 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 -----
```

2. NFS Exported Share Information Disclosure

La seconda grave vulnerabilità consente al potenziale attaccante di avere accesso non autorizzato a file e cartelle tramite NFS (protocollo che permette a dispositivi client di accedere a directory situate in server remoti). Una situazione del genere darebbe la possibilità all'attaccante di accedere a dati sensibili come dati con informazioni sugli utenti, dati di configurazione e la sicurezza del sistema.

Potenziale Soluzione

Implementare un sistema di autenticazione delle directory o anche dei singoli file così da limitare il loro accesso esclusivamente al personale scelto. Attivare degli alert che notifichino quando qualcuno di diverso dal personale autorizzato tenta di visualizzare o modificare file e directory.

Synopsis

It is possible to access NFS shares on the remote host.

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Risk Factor

Critical

VPR Score

5.9

CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

Exploitable With

Metasploit (true)

Plugin Information

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

Plugin Output

udp/2049/rpc-nfs

The following NFS shares could be mounted :

* /

192.168.1.101

14

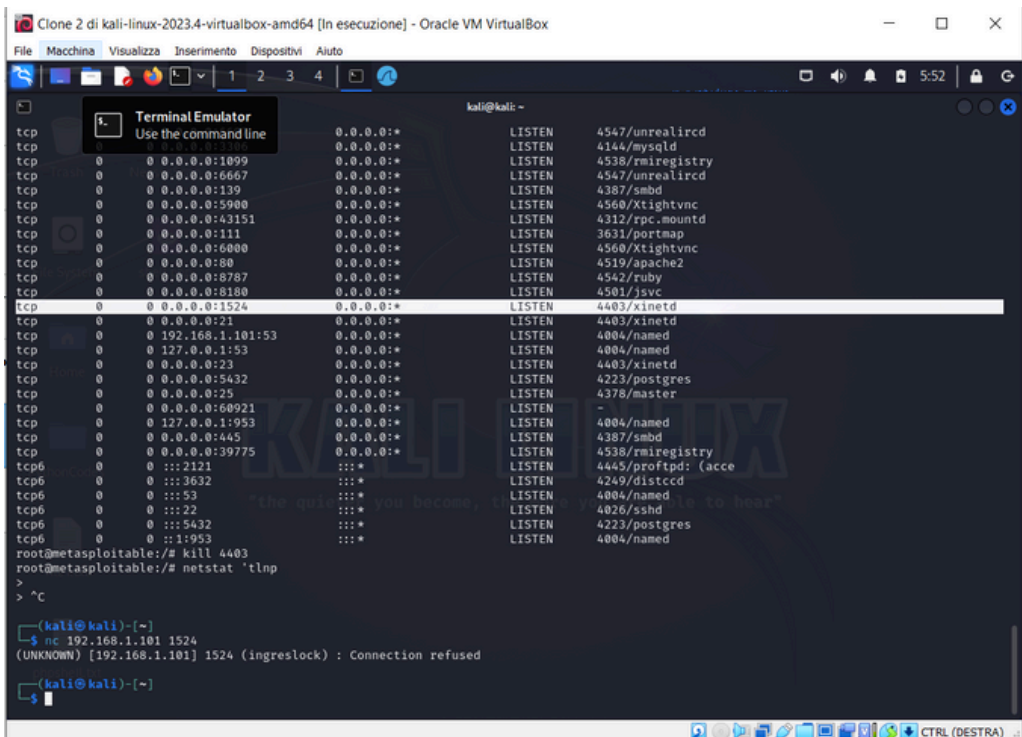
```
+ Contents of / :
+ .
+ ..
+ bin
+ boot
+ cdrom
+ dev
+ etc
+ home
+ initrd
+ initrd.img
+ lib
+ lost+found
+ media
+ mnt
+ mntsup.out
+ opt
+ proc
+ root
+/sbin
+ srv
+ sys
+ tmp
+ usr
+ var
+ vmlinuz
```

3. VNC Server ‘password’ Password

In questo caso Nessus durante la scansione ha tentato un piccolo bruteforce delle credenziali, e avendo Metasploitable ancora i settaggi di default è riuscito a loggarsi immettendo la parola “password” (presente nell’elenco di credenziali molto usate e quindi tentate per prime) nel campo della password appunto.

Potenziale soluzione

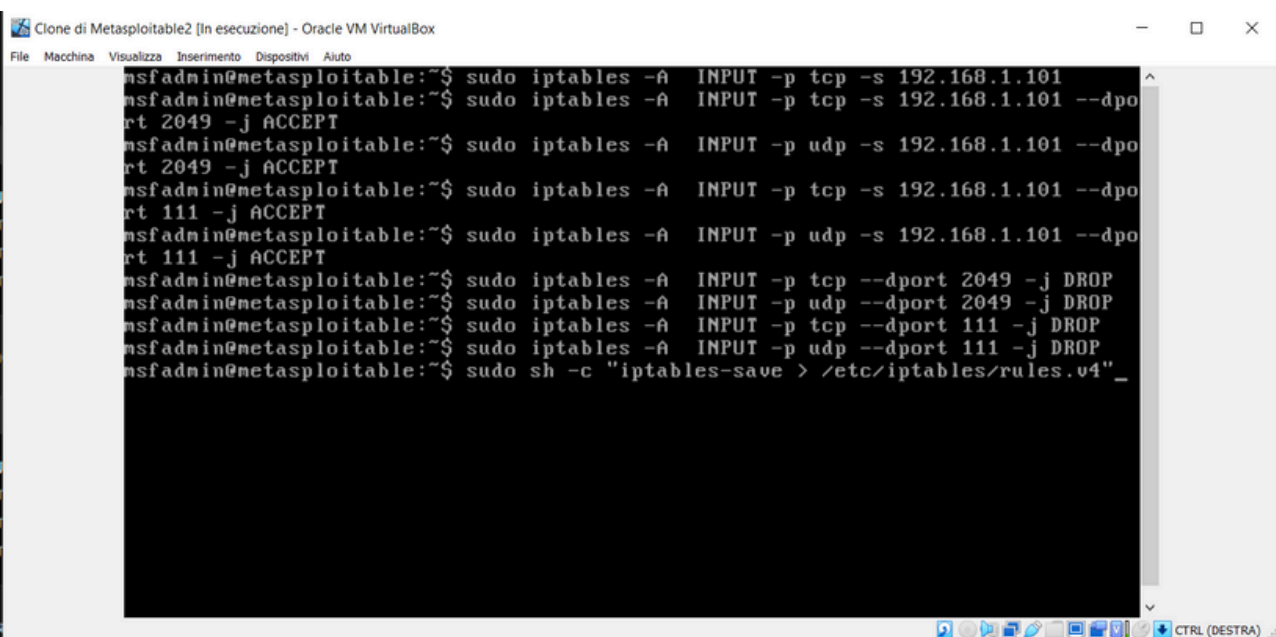
Potenziare le credenziali e nello specifico impostare una password lunga (almeno 8-10 caratteri) così da rendere il potenziale processo di bruteforce molto lungo e dunque nella pratica impossibile da attuare.



2. NFS Exported Share Information Disclosure

Non sono riuscito a risolvere questa criticità ma in generale il mio obiettivo era di applicare un sistema di autenticazione che permettesse solo all'host di visualizzare i file e modificarli. Ho fatto varie ricerche e tentativi con diversi comandi ma non sono riuscito nella pratica nonostante credo che in teoria l'idea sia giusta. Metto uno screen di uno dei tentativi durante il quale tentavo di rendere possibile la visualizzazione solo nel caso di richiesta da parte di un ip preciso, quello dell'host.

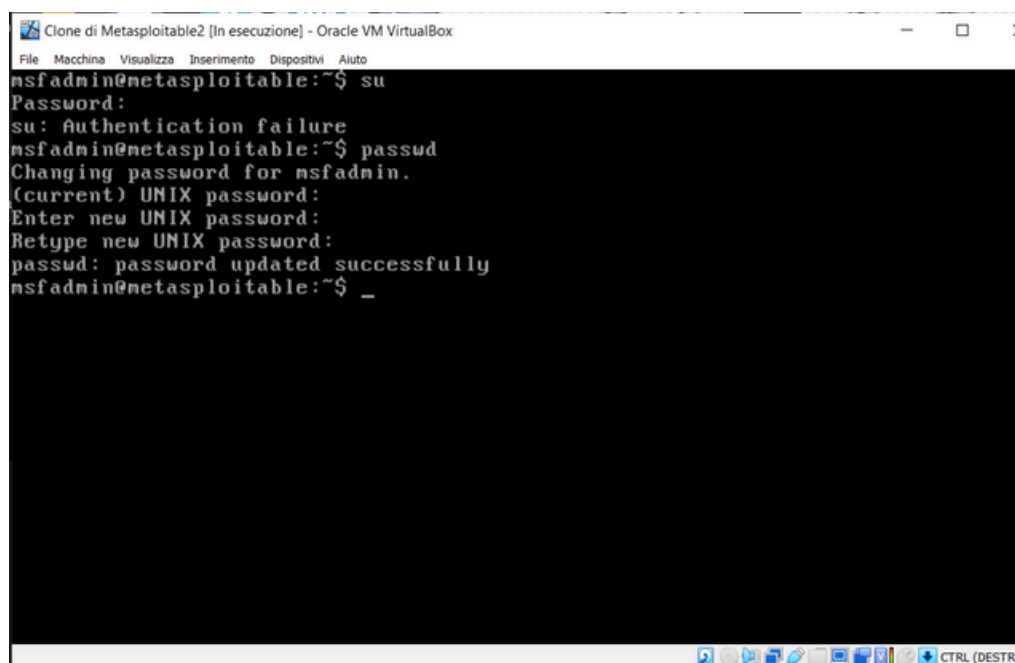
Con il senno di poi avrei dovuto provare a collegarmi prima da kali con netcat, almeno avrei avuto un terminale più user friendly dal quale fare i tentativi.

A screenshot of a terminal window titled "Clone di Metasploitable2 [In esecuzione] - Oracle VM VirtualBox". The terminal shows a series of commands and their outputs for configuring iptables. The user is msfadmin@metasploitable. The commands include: 1. sudo iptables -A INPUT -p tcp -s 192.168.1.101 --dport 2049 -j ACCEPT. 2. sudo iptables -A INPUT -p udp -s 192.168.1.101 --dport 2049 -j ACCEPT. 3. sudo iptables -A INPUT -p tcp -s 192.168.1.101 --dport 111 -j ACCEPT. 4. sudo iptables -A INPUT -p udp -s 192.168.1.101 --dport 111 -j ACCEPT. 5. sudo iptables -A INPUT -p tcp --dport 2049 -j DROP. 6. sudo iptables -A INPUT -p udp --dport 2049 -j DROP. 7. sudo iptables -A INPUT -p tcp --dport 111 -j DROP. 8. sudo iptables -A INPUT -p udp --dport 111 -j DROP. The final command is sudo sh -c "iptables-save > /etc/iptables/rules.v4".

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.1.101 --dport 2049 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.1.101 --dport 2049 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp -s 192.168.1.101 --dport 2049 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp -s 192.168.1.101 --dport 111 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp -s 192.168.1.101 --dport 111 -j ACCEPT
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 2049 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp --dport 2049 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 111 -j DROP
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p udp --dport 111 -j DROP
msfadmin@metasploitable:~$ sudo sh -c "iptables-save > /etc/iptables/rules.v4"
```

3. VNC Server 'password' Password

La risoluzione di questo problema consisteva esclusivamente nel cambiare la password di default in una originale e non comune. In seguito al comando 'passwd' ci viene richiesto prima di confermare la vecchia password, poi di digitare e confermare la nuova.

A screenshot of a terminal window titled "Clone di Metasploitable2 [In esecuzione] - Oracle VM VirtualBox". The terminal shows the execution of the 'su' command followed by 'passwd'. The output shows an authentication failure for 'su', then the 'passwd' command is run. The prompt asks for the current UNIX password, then for a new UNIX password, and finally to retype the new UNIX password. The output confirms the password was updated successfully.

```
msfadmin@metasploitable:~$ su
Password:
su: Authentication failure
msfadmin@metasploitable:~$ passwd
Changing password for msfadmin.
(current) UNIX password:
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@metasploitable:~$ _
```