

Remediation Meta

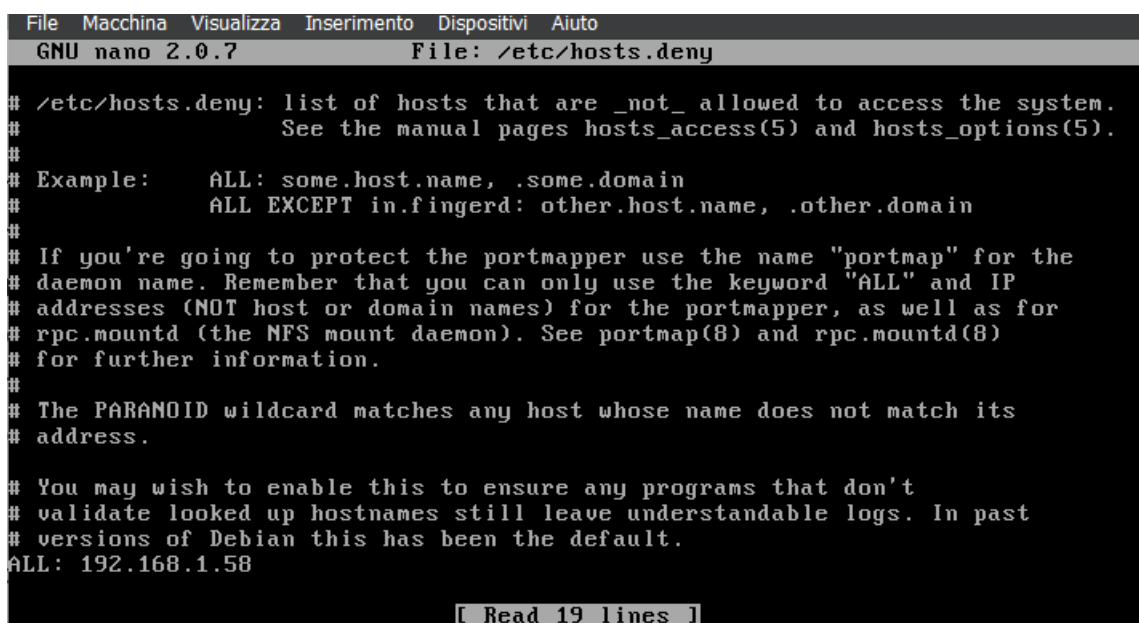
In questo report, spiego come risolvere 3 delle criticità che ho trovato durante la scansione

- NFS Exported Share Information Disclosure

Si tratta di una vulnerabilità di un sistema che utilizza il protocollo NFS (Network File System) per condividere file e risorse. Si riferisce al fatto che potrebbero esserci falle che consentono a utenti non autorizzati di ottenere informazioni sensibili o dettagli sulla condivisione NFS, causate da una configurazione errata dei permessi o autorizzazioni di accesso sulla condivisione NFS.

Per risolvere il problema, si agirà in questo modo:

- 1) Per prima cosa, aprire Metasploitable e scrivere il comando
`sudo nano /etc/hosts.deny`



```
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/hosts.deny

# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# 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.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
ALL: 192.168.1.58

[ Read 19 lines ]
```

- 2) In questa schermata possiamo inserire gli indirizzi IP dei dispositivi della quale vogliamo bloccare la scansione nella riga con scritto ALL. Possiamo inserire un indirizzo IP specifico (in questo caso l'indirizzo di kali con la quale ho effettuato la scansione) oppure bloccare tutti gli indirizzi IP scrivendo ALL. Dopodichè salviamo le modifiche e riavviamo la macchina.

- **VNC Server password «password»**

Il VNC (Virtual Network Computing) è un protocollo utilizzato per la condivisione del desktop remoto. La vulnerabilità VNC password indica che vi è configurata una password molto debole e può essere facilmente indovinata da attacchi di forza bruta o altri metodi di hacking.

Per risolvere il problema, si agirà in questo modo:

- 1) Per prima cosa, scrivere il comando `vncpasswd` per accedere alla configurazione della password.

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

- 2) Configureremo una password più efficace della quale ci verrà chiesta la conferma. Infine, riavvieremo la macchina

- 3) Ho anche impostato una regola per bloccare la porta 5900 che fa per la gestione del traffico con pfSense

Action	Block		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	TCP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.58 /
Display Advanced			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any .			
Destination			
Destination	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.101 /
Destination Port Range	(other)	5900	(other)
From		Custom	To
		Custom	Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			

- Bind shell backdoor detection

Si riferisce alla capacità di identificare e rilevare la presenza di backdoor di tipo "Bind Shell" su un sistema o in una rete. Una backdoor è un accesso che può essere sfruttato dai malintenzionati per prendere il controllo remoto. La porta in questione attaccata è la porta 1524, e come si può notare nell'immagine si riesce ad entrarci dentro

```
(kali㉿kali)-[~]  
$ nc 192.168.1.101 1524  
root@metasploitable:/# id  
uid=0(root) gid=0(root) groups=0(root)  
root@metasploitable:/# whoami  
root  
root@metasploitable:/# ^C
```

Per risolvere, agiremo in questo modo:

- 1) Per prima cosa su metasploitable verificheremo tramite il comando `sudo lsof -i :1524` il PID della porta (ovvero un'applicazione o processo che sta utilizzando una specifica, in questo caso la 1524)

```
msfadmin@metasploitable:~$ sudo lsof -i :<1524>  
-bash: syntax error near unexpected token `1524'  
msfadmin@metasploitable:~$ sudo lsof -i :1524  
[sudo] password for msfadmin:  
COMMAND  PID  USER   FD   TYPE    DEVICE  SIZE  MODE  NAME  
xinetd   4448 root    12u  IPv4    12089          TCP  *:ingreslock (LISTEN)
```

- 2) Dopodichè andremo a "killare" il PID tramite il comando `sudo kill -9 4448`

```
msfadmin@metasploitable:~$ sudo kill -9 4448
```

- 3) Se riproveremo a contattare la porta, il collegamento fallirà.

```
(kali㉿kali)-[~]  
$ nc 192.168.1.101 1524  
(UNKNOWN) [192.168.1.101] 1524 (ingreslock) : Connection refused
```

- 4) Infine, per rifiutare il traffico sulla porta anche quando riavviamo il sistema, impostiamo una regola firewall con pfsense

Action	Block		
Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.			
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Interface	LAN		
Choose the interface from which packets must come to match this rule.			
Address Family	IPv4		
Select the Internet Protocol version this rule applies to.			
Protocol	TCP		
Choose which IP protocol this rule should match.			
Source			
Source	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.58 /
Display Advanced			
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain its default value, any .			
Destination			
Destination	<input type="checkbox"/> Invert match	Address or Alias	192.168.1.101 /
Destination Port Range	(other)	1524	(other) 1524
From Custom To Custom			
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			

La vulnerabilità **rexecd service detection** richiesta dall'esercizio non è stata trovata durante la scansione iniziale.

