"CONSEGNA ESAME S5L5"

lannone luca

"TRACCIA"



Traccia:

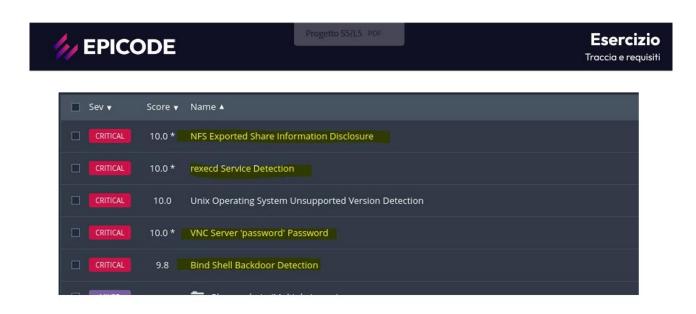
Effettuare una scansione completa sul target Metasploitable.

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.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.

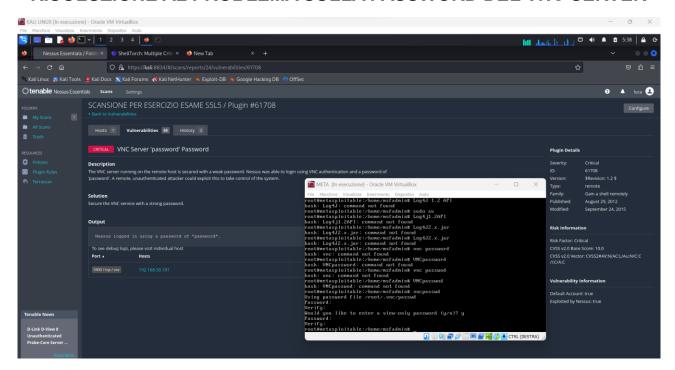


L'esercizio e stato svolto utilizzando l'applicazione NESSUS per la ricerca di eventuali criticità poste sull'IP:192.168.50.101

Riconducibile alla macchina di META siccome la risoluzione di tutte le criticità ci avrebbe messo nella condizione di

sostituire componenti hardware abbiamo risolto solo alcune di esse come possiamo vedere nel proseguo della medesima relazione

"RISOLUZIONE AL PROBLEMA SULLA PASSWORD DEL VNC SERVER"



Per risolvere la seguente criticità siamo andati a variare la "password"-"VNC server" in modo da risolverla inquanto la non risoluzione della medesima avrebbe permesso ad un eventuale attaccante connesso da remoto il controllo del sistema.

"RISOLUZIONE ALLA CRITICITA' SU <<RLOGIN>> E <<RSH SERVICE>>"

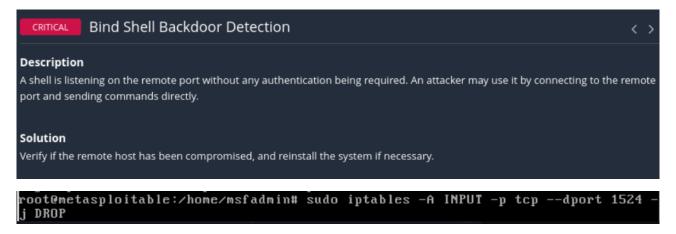
HIGH	7.5 *	5.9	rlogin Service Det	Service detection	1	0	1
HIGH	7.5 *	5.9	rsh Service Detec	Service detection	1	0	1

```
nowait root
#<off># netbios-ssn
                       stream
                                                       /usr/sbin/tcpd
                               tcp
                                                                       /usr/sbS
telnet
                               nowait
                                       telnetd /usr/sbin/tcpd /usr/sbin/in.te$
               stream
                       tcp
#<off># ftp
                       stream
                               tcp
                                       nowait root
                                                       /usr/sbin/tcpd /usr/sb$
tftp
                               wait
                                       nobody /usr/sbin/tcpd /usr/sbin/in.tf$
               dgram
                       udp
                               nowait
                                               /usr/sbin/tcpd /usr/sbin/in.rs$
#shell
                                       root
               stream
                       tcp
                                               /usr/sbin/tcpd /usr/sbin/in.rl$
#login
               stream
                               nowait
                                       root
                       tcp
                               nowait root
                                               /usr/sbin/tcpd /usr/sbin/in.re$
Hexec
               stream
                      tcp
ingreslock stream tcp nowait root /bin/bash bash -i
```

Per risolvere la seguente criticità abbiamo commentato sulla linea di "**login**" e "**exec**".

Successivamente abbiamo fatto il restart del servizio "xinetd".

"RISOLUZIONE DELLE CRITICITA' RELATIVI ALLA VULNERABILITA' BIND SHELL BACKDOOR DETECTION"



Questa criticità è stata risolta andando a chiudere la porta "**tcp:1524**" attraverso la riga di comando sovrastante.

La non risoluzione della seguente criticità avrebbe potuto permettere la connessionedi un attaccante da porta remota il quale avrebbe potuto modificare, cancellare o inviare comandi direttamente.

Inoltre avrebbe potuto inserire un codice malevolo.

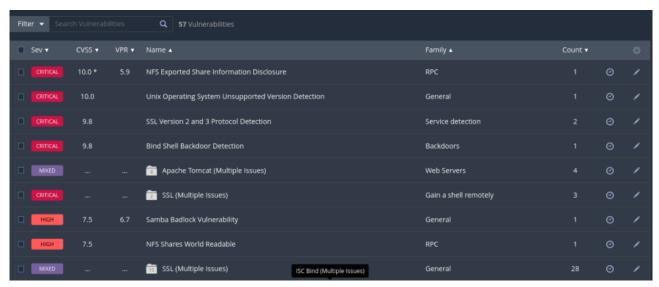
```
lost is up (0.00033s latency).
Not shown: 977 closed tcp ports (reset)
            STATE
                           SERVICE
             open
22/tcp
23/tcp
                           ssh
telnet
             open
            open
open
                           domain
3/tcp
11/tcp
39/tcp
                           rpcbind
netbios-ssn
             open
45/tcp
512/tcp
             open
                           exec
512/tcp open
513/tcp open
514/tcp open
1099/tcp open
1524/tcp filtered
2049/tcp open
2121/tcp open
                           login
                           shell
                           rmiregistry
                           ingreslock
                           ccproxy-ftp
3306/tcp open
5432/tcp open
                           mysql
postgresql
900/tcp open
                           vnc
X11
5000/tcp open
5667/tcp open
8009/tcp open
8180/tcp open
                           unknown
MAC Address: 08:00:27:CA:2B:54 (Oracle VirtualBox virtual NIC)
  map done: 1 IP address (1 host up) scanned in 1.40 seconds
```

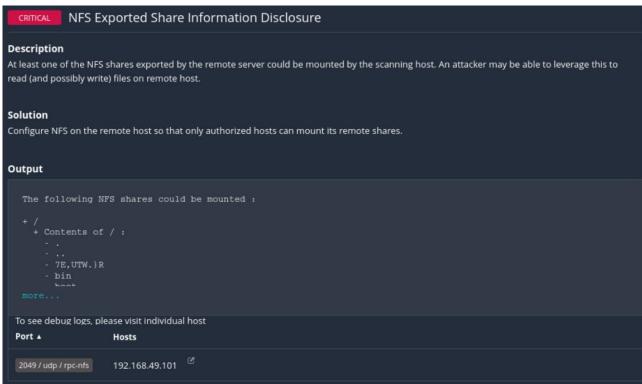
Come si può evincere dall'immagine sovrastante e stato eseguito un comando <<nmap>> per controllare che la porta "tcp:1524" risultasse effettivamente "filtrata" dal "firewall".

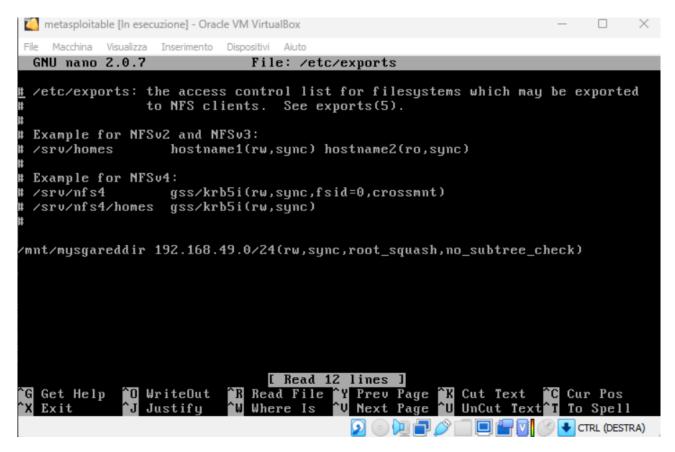


Successivamente è stato eseguito un controllo ulteriore attraverso **NESSUS** per controllare che la **vulnerabilità** fosse del tutto **INATTIVA**

"RISOLUZIONE DELLA CRITICITA': NFS EXPORTED SHARE INFORMATION DISCLOSURE"







Questa criticità è stata risolta limitando gli accessi ai soli utenti sotto lo stesso **Network** così da impedire a utenti esterni l'accesso.

La non risoluzione di questa porblematica avrebbe potuto permettere ad un attaccante sia la lettura che la scrittura dei file da un host remoto.

"SCANNER FINALE CON LE CRITICITA' RISOLTE NON PIU' " IDENTIFICATE"



Come possiamo vedere le criticità che abbiamo risolto non vengono visualizzate all'interno della scansione eseguita successivamente all'applicazione delle risoluzioni delle medesime.