

Test modulo M3

Qui vedremo la risoluzione di alcune problematiche che erano risultate nella prima scansione effettuata.

Problematica 1

NFS Exported Share Info Disclosure

Questa vulnerabilità permetteva ad un malintenzionato di poter leggere e scrivere file sulla nostra macchina.

Risoluzione: per risolvere questa vulnerabilità entriamo nella configurazione di NFS e andiamo a commentare con il '#' l'ultima stringa di codice che permetteva a qualsiasi host di poter creare sessioni remote.

Altra soluzione era quella di andare a specificare host per host quelli autorizzati alla condivisione.

Successivamente col comando '**exportfs -ra**' andiamo ad aggiornare le esportazioni NFS senza andare a riavviare il servizio e con il comando '**showmount -e localhost**' andiamo a verificare quali esportazioni sono presenti (nel nostro caso non visualizziamo risultati).

```
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,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)
#
#/*              *(rw,sync,no_root_squash,no_subtree_check)
```

```
msfadmin@metasploitable:~$ exportfs -ra
exportfs: could not open /var/lib/nfs/etab for locking
exportfs: can't lock /var/lib/nfs/etab for writing
msfadmin@metasploitable:~$ sudo su
root@metasploitable:/home/msfadmin# exportfs -ra
root@metasploitable:/home/msfadmin# showmount -e localhost
Export list for localhost:
root@metasploitable:/home/msfadmin#
```

Problematica 2

VNC Server 'password' Password

Ci viene rilevata una password debole del sistema

Risoluzione: qui molto semplicemente, utilizzando i privilegi d'amministratore, siamo andati a modificare una password considerata dal sistema debole andando a inserirne una più forte ed efficace con il comando '**vncpasswd**' (nello screen per questioni di privacy la password non viene mostrata).

```
root@metasploitable:/etc/unreal/modules# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/etc/unreal/modules#
```

Problematica 3

Bind Shell Backdoor Detection

Qui la problematica rilevata faceva riferimento ad una shell in ascolto senza alcuna necessità di autenticazione.

Risoluzione: Tramite il nostro firewall Pfsense abbiamo creato una regola che andasse a bloccare il traffico verso la porta 1524. Questa prima risoluzione lascia la porta attiva, ma filtrata permettendo così una gestione del traffico sulla porta sicura.

Un'altra soluzione è quella di andare a chiudere completamente la porta eliminando così ogni possibilità di accesso. Purtroppo questo non è sempre possibile perché non sappiamo l'utilizzo che il cliente o l'azienda va a farne.

Qui verifichiamo come la regola Firewall abbiamo correttamente filtrato il traffico sulla porta.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	*	*	*	1524	*	none			
2/17 KIB	IPv4 *	*	*	*	*	*	none			

```
(kali@kali)-[~]
$ sudo nmap -sS -p 1524 192.168.50.101
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-30 09:13 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0041s latency).

PORT      STATE      SERVICE
1524/tcp  filtered  ingreslock

Nmap done: 1 IP address (1 host up) scanned in 0.55 seconds
```

Problematica 4

UnrealIRCd Backdoor Detection

Qui ci viene segnalata una backdoor sul server ICR

Soluzione: possiamo vedere nel primo screen che la porta 6697, designata all' ICR server è sempre in ascolto.

Per risolvere la problematica nel nostro caso è quello di dover chiudere la porta 6697 entrando nei file di configurazione e andando a ricercare la porta "incriminata" e andandola a chiudere (aggiungendo un '#' affianco al valore LISTEN della porta).

Successivamente si dovrà procedere con la sanificazione della porta per evitare la trapielazione di informazioni sensibili, effettuare test e analisi e verificare ulteriormente tutti gli accessi.

```
COMMAND  PID USER  FD  TYPE DEVICE SIZE NODE NAME
unrealirc 4672 root   3u  IPv4 12292      TCP *:6697 (LISTEN)
sleep    10981 root   3u  IPv4 12292      TCP *:6697 (LISTEN)
telnet    10982 root   3u  IPv4 12292      TCP *:6697 (LISTEN)
sh        10983 root   3u  IPv4 12292      TCP *:6697 (LISTEN)
sh        10984 root   3u  IPv4 12292      TCP *:6697 (LISTEN)
telnet    10985 root   3u  IPv4 12292      TCP *:6697 (LISTEN)
root@metasploitable:/home/msfadmin#
```

```
GNU nano 2.0.7      File: /etc/unreal/unrealircd.conf      Modified
      hostname      *@*;
      class          clients;
      maxperip 5;
};

#listen      *:6697
{
      options
      {
              clientonly;
      };
};

#listen      *:6667;

log "ircd.log" {
      maxsize 2097152;
      flags {
              oper;
              kline;
      };
};
```

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo nmap -sS -p 6667 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-30 11:11 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0056s latency).

PORT      STATE SERVICE
6667/tcp  closed irc

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

Problematica 5

Rexecd Service Detection

Rexecd è un servizio che consente agli utenti di una rete di eseguire i comandi da remoto, purtroppo questo metodo non ha dei buoni mezzi di autenticazioni quindi potrebbe essere utilizzato facilmente da malintenzionati.

Risoluzione: Per rimuovere la problematica dobbiamo entrare nella cartella del processo, essendoci prima autenticati come amministratore e disattivarlo o aggiornarlo alle nuove normative. Nel nostro caso lo disabilitiamo aggiungendo un semplice '#' alla sua riga di comando andando a disabilitare il servizio.

Metaspoitable2 [In esecuzione] - Oracle VM VirtualBox

File Macchina Visualizza Inserimento Dispositivi Aiuto

GNU nano 2.0.7File: /etc/inetd.confModified

#<off># netbios-ssnstream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.telnetdstream tcp nowait telnetd /usr/sbin/tcpd /usr/sbin/in.tftpdgram udp wait nobody /usr/sbin/tcpd /usr/sbin/in.rshstream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rloginstream tcp nowait root /usr/sbin/tcpd /usr/sbin/in.rexecdstream tcp nowait root /bin/bash bash -i