REMEDIATION REPORT
PROGETTO M3-W12D4

Federica Di Fiore
Cybersecurity Analyst PT

INDICE

INTRODUZIONE

Questo report descrive le azioni di remediation effettuate su quattro vulnerabilità critiche rilevate durante una scansione iniziale effettuata sul target Metasploitable. Lo scopo di questa esercitazione è limitare l'esposizione al rischio della macchina oppure, ove possibile, disattivare i servizi vulnerabili e garantire un buon livello di sicurezza.

Tra le tante vulnerabilità trovate da Nessus, è stata posta maggiore attenzione sulle seguenti:

- VNC Server 'password' Password
- Rexecd Service Detection
- NFS Exported Share Information Disclosure
- Bind Shell Backdoor Detection

Di seguito verranno spiegati i provvedimenti adottati per la risoluzione di tutte le problematiche richieste.

SVOLGIMENTO

CONTROLLO COMUNICAZIONE TRA LE DUE MACCHINE

In questa prima fase del nostro progetto, dopo aver impostato da Virtual Box sia su Kali Linux, sia su Metasploitable la rete selezionando “Scheda con Bridge”, permettendo quindi ad entrambe l’accesso alla connessione Internet, possiamo avviarle ed effettuare un semplice ping da Kali verso il nostro target. Ricordiamoci però che Metasploitable spesso al primo avvio non presenta alcun Indirizzo IP, sarà quindi necessario chiedere alla macchina di impostarne uno tramite il comando:

- `Sudo dhclient eth0` > in questo modo otterremo il nostro IP che sarà 192.168.178.58

Successivamente servirsi di quest’ultimo per pingare Metasploitable da Kali.

```
msfadmin@metasploitable:~$ sudo dhclient eth0
Internet Systems Consortium DHCP Client V3.0.6
Copyright 2004-2007 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/eth0/08:00:27:8d:ef:9c
Sending on   LPF/eth0/08:00:27:8d:ef:9c
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 7
DHCPOFFER of 192.168.178.58 from 192.168.178.1
DHCPREQUEST of 192.168.178.58 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.178.58 from 192.168.178.1
bound to 192.168.178.58 -- renewal in 385920 seconds.
msfadmin@metasploitable:~$ _
```

FIGURA 1 RICHIESTA INDIRIZZO IP A METASPLOITABLE

```
┌──(kali㉿kali)-[~]
└─$ ping 192.168.178.58
PING 192.168.178.58 (192.168.178.58) 56(84) bytes of data.
64 bytes from 192.168.178.58: icmp_seq=1 ttl=64 time=0.495 ms
64 bytes from 192.168.178.58: icmp_seq=2 ttl=64 time=0.203 ms
64 bytes from 192.168.178.58: icmp_seq=3 ttl=64 time=0.215 ms
64 bytes from 192.168.178.58: icmp_seq=4 ttl=64 time=0.234 ms
64 bytes from 192.168.178.58: icmp_seq=5 ttl=64 time=0.196 ms
^C
— 192.168.178.58 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4080ms
rtt min/avg/max/mdev = 0.196/0.268/0.495/0.113 ms
```

FIGURA 2 PING DA KALI A METASPLOITABLE

FASE 1 –VNC SERVER ‘PASSWORD’ PASSWORD

Il servizio VNC era configurato con una password predefinita e facilmente individuabile, rendendolo quindi accessibile da remoto facilmente. Per poter visualizzare questo servizio, è stato utilizzato il comando

- `pgrep -l vnc` che restituisce il processo attivo `Xtightvnc` con PID `4551`

```
msfadmin@metasploitable:~$ pgrep -l vnc
4551 Xtightvnc
```

FIGURA 3 INDIVIDUAZIONE PID VNC SERVER 'PASSWORD' PASSWORD

La soluzione la otteniamo semplicemente digitando a terminale:

- `sudo pkill Xtightvnc` > in questo modo il processo VNC è stato terminato con successo. La porta 5901 (usata di default dal VNC) non risulta più attiva.

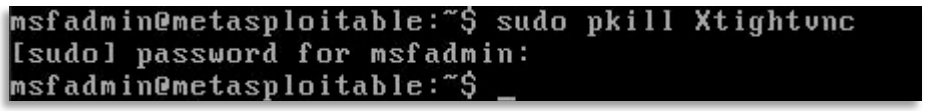

FIGURA 4 - PROCEDURA PER KILLARE IL SERVIZIO VNC

FASE 2 - REXECD SERVICE DETECTION

Rexecd permette l'esecuzione remota di comandi. Il servizio era in ascolto sulla porta TCP 512, verificato tramite il comando

- `netstat -tulnp`

L'azione correttiva effettuata in questo caso, è stata semplicemente terminare il processo digitando a terminale

- `sudo fuser -k 512/tcp`

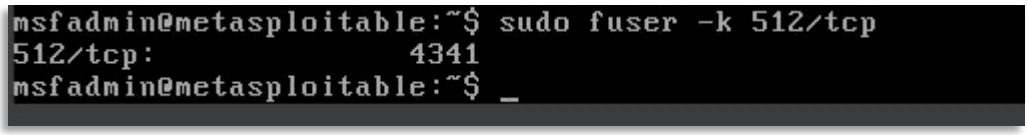

FIGURA 5 AZIONE CORRETTIVA REXECD

Il comando `fuser` ci serve per identificare i processi che stanno usando un determinato file o socket, ad esempio una porta di rete. Associandolo a `-k` stiamo dicendo alla VM di terminare i processi trovati. In risposta troveremo `512/tcp: 4341` che sarebbe il nostro processo con PID 4341 in ascolto sulla porta TCP 512.

FASE 3 – NFS EXPORTED SHARE INFORMATION DISCLOSURE

Tramite i comandi `rpcinfo -p` e `netstat -tulnp` è stato scoperto che il demone NFS risultava attivo. È importante gestire questa problematica in quanto NFS Daemon è un servizio che si occupa di gestire le richieste di accesso ai file condivisi attraverso la rete. Esso è considerato una vulnerabilità perché permette:

1. Il montaggio remoto di directory senza autenticazione;
2. L'esfiltrazione di dati sensibili;
3. L'esecuzione di codice dannoso, perché un malintenzionato potrebbe sfruttare i permessi errati.

Di conseguenza ci si trova davanti ad un reale pericolo per il nostro sistema.

Nella fase di remediation è stato quindi eseguito il comando:

- `sudo /etc/init.d/nfs-kernel-server stop`

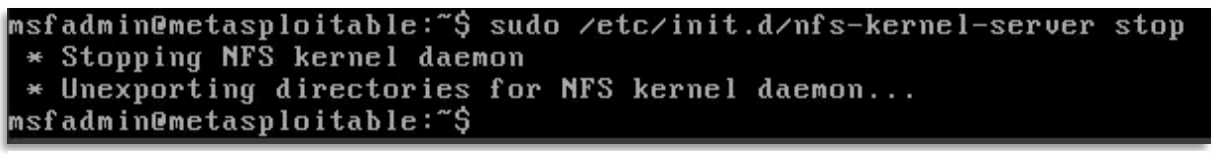

FIGURA 6 REMEDIATION NFS DAEMON

In questo modo il servizio è stato disattivato, impedendo le condivisioni non sicure.

FASE 4 – BIND SHELL BACKDOOR DETECTION

In questa fase si presterà attenzione ad una shell bindata che è stata trovata in ascolto sulla porta TCP 1524, e che potrebbe trattarsi di una potenziale backdoor.

Essa è individuabile tramite il comando `netstat -tulnp` che darà questo tipo di risultati

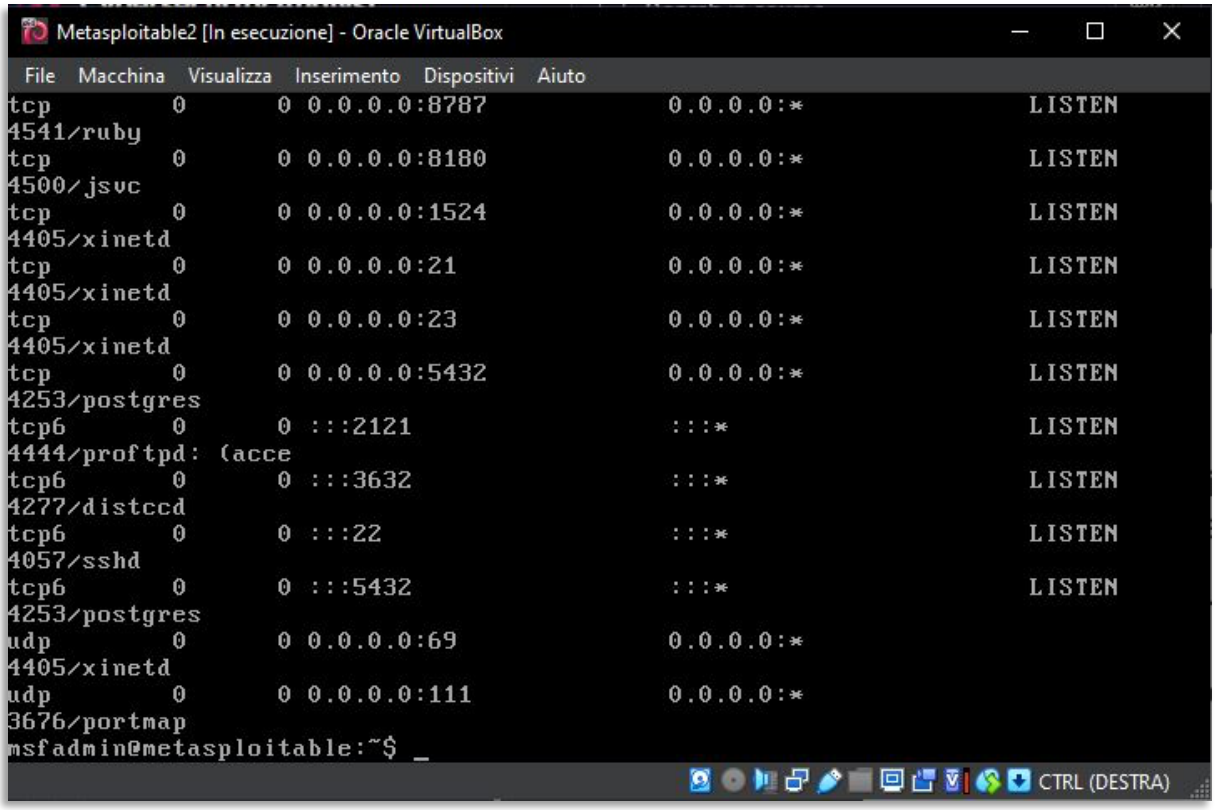

FIGURA 7 INDIVIDUAZIONE BACKDOOR

In questa schermata è visibile l'output del comando appena dato, con un elenco di tutte le porte TCP e UDP in ascolto, con il relativo PID, ed ecco che tra tutte ne compare una particolarmente sospetta, ovvero la `tcp 0 0 0.0.0.0:1524 0.0.0.0:* LISTEN` che non sembra associata né ad un processo di sistema legittimo, né ad un processo visibile. La Bind Shell apre una porta che rimane in ascolto, in attesa di una connessione da parte di un potenziale malintenzionato.

Per la risoluzione di questa problematica si è deciso di fare affidamento su una regola firewall iptables, ovvero digitando a terminale `sudo iptables -A INPUT -p tcp --dport 1524 -j DROP`, che scarta automaticamente tutti i pacchetti in ingresso verso questa porta senza alcuna risposta.

Successivamente applichiamo il comando `sudo iptables -L -n` per verificare che la regola sia stata correttamente inserita.

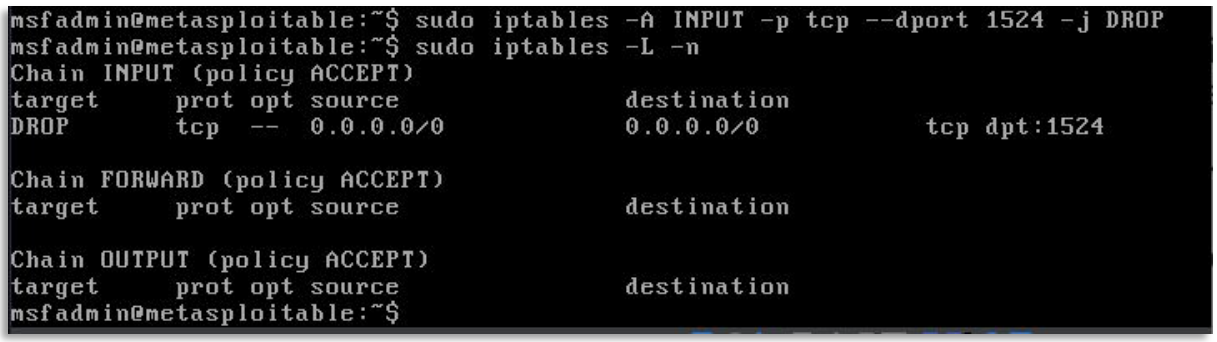

FIGURA 8 REGOLA FIREWALL IPTABLES

Le quattro vulnerabilità critiche rilevate nella prima scansione di Nessus sono state mitigate tramite azioni mirate, che hanno incluso l'eliminazione di processi, la disattivazione di servizi e l'applicazione di regole firewall. La successiva scansione con Nessus ha confermato la rimozione di tali vulnerabilità, garantendo quindi il miglioramento della sicurezza del sistema target.