CSPT0524

Esercitazione Analisi delle vulnerabilità e azioni di rimedio M3 W12 D4

INFORMAZIONI DEL DOCUMENTO

1. Autore Giovanni D'Abrosca

2. Nome Documento Analisi delle vulnerabilità e azioni di rimedio M3 W12 D4

3. Data Emissione 10/02/2025

Traccia esercizio:

Esercizio Traccia e requisiti Effettuare una scansione completa sul target Metasploitable2.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità critiche 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.

Screenshot e spiegazione dei passaggi della remediation

In prima analisi ho preso la vulnerabilità OpenSSH 4.7.1 che girava sulla porta 22 e ho proceduto a disinstallare la stessa. Questa particolare vulnerabilità permetteva potenzialmente agli attaccanti di ottenere un accesso non autorizzato al sistema, compromettendo così la sicurezza dell'intero ambiente. L'azione di disinstallazione ha rimosso il servizio vulnerabile, eliminando il rischio associato. Dopo aver completato questo passaggio, ho eseguito una nuova scansione sul target per verificare l'efficacia dell'azione di rimedio.

```
root@metasploitable:/home/msfadmin# apt-get remove --purge openssh-server -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
   openssh-server*
0 upgraded, 0 newly installed, 1 to remove and 138 not upgraded.
After this operation, 668kB disk space will be freed.
(Reading database ... 37634 files and directories currently installed.)
Removing openssh-server ...
 * Stopping OpenBSD Secure Shell server sshd

I OK 1
Purging configuration files for openssh-server ...
```

Di seguito è riportato lo screenshot dei risultati della scansione effettuata con nmap:

Dalla scansione si può osservare che la porta 22, precedentemente occupata dal servizio OpenSSH 4.7.1 vulnerabile, risulta ora chiusa, confermando così l'efficacia della disinstallazione eseguita.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-09 23:58 CET
Nmap scan report for 192.168.51.120
Host is up (0.00087s latency).
Not shown: 65506 closed tcp ports (reset)
              STATE SERVICE
21/tcp
23/tcp
               open ftp
open telnet
                                              vsftpd 2.3.4
Linux telnetd
Postfix smtpd
53/tcp
80/tcp
                                              ISC BIND 9.4.2
Apache httpd 2.2.8 ((Ubuntu) DAV/2)
                          domain
111/tcp
139/tcp
445/tcp
                         rpcbind 2 (RPC #100000)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
               open
open
512/tcp
513/tcp
                          exec
login?
                                              netkit-rsh rexecd
1099/tcp
1524/tcp
                         java-rmi GNU Classpath grmiregistry
bindshell Metasploitable root shell
                                             ProfTPD 1.3.1

MySQL 5.0.51a-3ubuntu5

distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))

PostgreSQL DB 8.3.0 - 8.3.7
 3306/tcp
3632/tcp open
5432/tcp open
                          postgresql
                                               VNC (protocol 3.3)
6000/tcp open
6667/tcp open
                                             (access denied)
UnrealIRCd
                                             Apache Jserv (Protocol v1.3)

Apache Tomcat/Coyote JSP engine 1.1

Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)

1-4 (RPC #100005)

1-3 (RPC #100005)
8009/tcp open
8180/tcp open
                          ajp13
http
8787/tcp open
37186/tcp open
                          nlockmgr
                         java-rmi
status
                                              GNU Classpath grmiregistry
1 (RPC #100024)
 Service İnfo: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

In seconda analisi, ho preso il servizio telnet che girava sulla porta 23 e ho proceduto a disinstallare il servizio e a modificare il file di configurazione nella directory /etc/inetd.conf. Questa vulnerabilità poteva permettere agli attaccanti di intercettare comunicazioni non criptate, esponendo dati sensibili. Dopo aver rimosso il servizio telnet, ho eseguito una nuova scansione sul target per verificare l'efficacia delle azioni di rimedio.

Di seguito è riportato lo screenshot della disinstallazione del servizio telnet.

```
root@metasploitable:/home/msfadmin# apt-get remove --purge telnetd -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages will be REMOVED:
   telnetd*
0 upgraded, 0 newly installed, 1 to remove and 138 not upgraded.
After this operation, 147kB disk space will be freed.
(Reading database ... 37621 files and directories currently installed.)
Removing telnetd ...
groupdel: group telnetd does not exist
Purging configuration files for telnetd ...
```

Di seguito è la modifica effettuata al file di configurazione nella directory /etc/inetd.conf:

Questa modifica ha garantito che il servizio telnet non venga più avviato, prevenendo così le intercettazioni di comunicazioni non crittografate.

```
GNU nano 2.0.7
                             File: /etc/inetd.conf
#<off># netbios-ssn
                                                  root
                         stream
                                 tcp
                                          nowait
                                                           /usr/sbin/tcpd
                                                                           /usr/sb$
#<off># telnet
                         stream
                                 tcp
                                          nowait
                                                  telnetd /usr/sbin/tcpd
                                                                           /usr/sb9
#<off># ftp
                                                  root
                         stream
                                 tcp
                                          nowait
                                                           /usr/sbin/tcpd
                                                                           /usr/sb9
                                                  /usr/sbin/tcpd /usr/sbin/in.tf
#tftp
                dgram
                         udp
                                 wait
                                          nobody
#shell
                                          root
                stream
                         tcp
                                 nowait
                                                  /usr/sbin/tcpd
                                                                  /usr/sbin/in.rs
#login
                                                                  /usr/sbin/in.rl$
                                          root
                stream
                         tcp
                                 nowait
                                                  /usr/sbin/tcpd
                                 nowait
                                          root
#exec
                         tcp
                                                                   /usr/sbin/in.re$
                stream
                                                  /usr/sbin/tcpd
#ingreslock stream tcp nowait root /bin/bash bash -i
```

Successivamente, ho eseguito una nuova scansione con nmap per verificare l'efficacia delle modifiche. Lo screenshot dei risultati della scansione mostra che la porta 23, precedentemente utilizzata dal servizio telnet vulnerabile, risulta ora chiusa, confermando l'efficacia della disinstallazione e della modifica del file di configurazione.

Ecco lo screenshot della scansione effettuata con nmap:

```
-$ nmap -sV -p- 192.168.51.120
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-10 00:22 CET
Nmap scan report for 192.168.51.120
Host is up (0.0016s latency).
Not shown: 65511 closed tcp ports (reset)
PORT
          STATE SERVICE
                               VERSION
          open ftp
                               vsftpd 2.3.4
21/tcp
          open smtp
open domain
25/tcp
                               Postfix smtpd
53/tcp
                               ISC BIND 9.4.2
          open http Apache httpd 2.2.8 ((Ubuntu) DAV/2) open rpcbind 2 (RPC #100000)
80/tcp
111/tcp
          open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP) open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
139/tcp
445/tcp
1099/tcp open java-rmi GNU Classpath grmiregistry
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open ftp ProFTPD 1.3.1
3306/tcp open mysql MySQL 5.0.51a-3ub
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
3632/tcp open distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
                          VNC (protocol 3.3)
5900/tcp open vnc
6000/tcp open X11
                               (access denied)
                         UnrealIRCd
6667/tcp open
6697/tcp open
                  irc
                               UnrealIRCd
                  ajp13
http
                             Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
8009/tcp open
8180/tcp
          open
8787/tcp open
                              Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
                  drb
37066/tcp open
                  java-rmi GNU Classpath grmiregistry
42160/tcp open status
                               1 (RPC #100024)
                               1-3 (RPC #100005)
44193/tcp open
47477/tcp open nlockmgr
                              1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.57 seconds
```

In terza analisi, ho affrontato la chiusura di ulteriori porte vulnerabili su Metasploitable2, assicurandomi che fossero completamente disabilitate e che il sistema fosse protetto contro possibili attacchi. Le porte interessate erano le seguenti: 139, 445, 3306, 5432, 37066, 42160, 44193 e 47477.

Per ciascuna di queste porte, ho proceduto alla disinstallazione dei relativi servizi vulnerabili. Ad esempio, le porte 139 e 445 erano utilizzate dal servizio SMB (Server Message Block), noto per essere vulnerabile a diverse tipologie di attacchi. Dopo aver disinstallato il servizio SMB, ho applicato delle regole firewall tramite iptables per garantire che le porte rimanessero chiuse e inaccessibili.

La porta 3306, utilizzata dal database MySQL, e la porta 5432, relativa al database PostgreSQL, erano entrambe esposte a potenziali exploit che potevano compromettere l'integrità dei dati. Ho disinstallato i servizi MySQL e PostgreSQL e configurato iptables per bloccare l'accesso a queste porte.

Le porte 37066, 42160, 44193 e 47477 erano utilizzate da servizi meno comuni, ma comunque vulnerabili. Ho proceduto alla loro disinstallazione e ho applicato regole firewall specifiche per prevenire qualsiasi accesso futuro attraverso queste porte.

Dopo aver completato questi passaggi, ho eseguito una scansione completa con nmap per verificare l'efficacia delle disinstallazioni e delle regole firewall. I risultati della scansione confermano che tutte le porte menzionate risultano ora chiuse, garantendo così un ambiente di sistema più sicuro e protetto da potenziali attacchi.

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 17:19 CET
Nmap scan report for 192.168.51.120
Host is up (0.0018s latency).
Not shown: 65515 closed tcp ports (reset)
PORT STATE SERVICE VERSION
          open
25/tcp
                 smtp
                          Postfix smtpd
53/tcp
          open
                domain ISC BIND 9.4.2
80/tcp
                           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp
                 rpcbind 2 (RPC #100000)
          open
                 java-rmi GNU Classpath grmiregistry
2049/tcp
                           2-4 (RPC #100003)
          open
2121/tcp
          open
                           ProFTPD 1.3.1
3632/tcp
                          distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5900/tcp
                           VNC (protocol 3.3)
          open
6000/tcp
                           (access denied)
          open
6667/tcp
                           UnrealIRCd
          open
6697/tcp
          open
                          Apache Jserv (Protocol v1.3)
Apache Tomcat/Coyote JSP engine 1.1
8009/tcp
          open
                           Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
8787/tcp
          open
                drb
                           1 (RPC #100024)
38017/tcp open
40382/tcp open
                 java-rmi GNU Classpath grmiregistry
                           1-3 (RPC #100005)
41960/tcp open
44139/tcp open
                nlockmgr 1-4 (RPC #100021)
                       metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Wmap done: 1 IP address (1 host up) scanned in 131.56 seconds
```

Infine, come quarto caso, ho affrontato la disinstallazione del servizio VNC su Metasploitable2. Il servizio VNC, noto per essere vulnerabile a diverse tipologie di attacchi, rappresentava un rischio significativo per la sicurezza del sistema. Procedendo con la disinstallazione di VNC, ho eliminato una potenziale via di accesso per gli aggressori, garantendo un ulteriore livello di protezione per il sistema.

Di seguito lo screen di una nuova scansione con nmap:

```
192.168.51.120
Starting Nmap 7.95 ( https://nmap.org ) at 2025-02-11 17:55 CET
Nmap scan report for 192.168.51.120
Host is up (0.0010s latency).
Not shown: 65517 closed tcp ports (reset)
          STATE SERVICE VERSION
PORT
21/tcp
          open ftp
                         vsftpd 2.3.4
25/tcp
                         Postfix smtpd
          open
                         ISC BIND 9.4.2
          open
80/tcp
          open
                         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
                rpcbind 2 (RPC #100000)
          open
1099/tcp
                java-rmi GNU Classpath grmiregistry
          open
2049/tcp
                         2-4 (RPC #100003)
          open
2121/tcp
                         ProFTPD 1.3.1
          open
3632/tcp
          open
                distccd distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
6667/tcp
6697/tcp
                         UnrealIRCd
          open
                         UnrealIRCd
          open
8009/tcp
          open
8180/tcp
          open
                         Apache Tomcat/Coyote JSP engine 1.1
8787/tcp
                         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
40107/tcp open
                java-rmi GNU Classpath grmiregistry
44489/tcp open
                         1 (RPC #100024)
54099/tcp open
                         1-3 (RPC #100005)
                mountd
60175/tcp open
                nlockmgr 1-4 (RPC #100021)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Unix
```

In conclusione, secondo il mio parere, disinstallare i servizi non rappresenta una vera e propria remediation. Idealmente, avrei preferito aggiornare il sistema Metasploitable2 aggiungendo i link aggiornati nella sources.list di Metasploitable. Tuttavia, questo tentativo si è rivelato infruttuoso poiché Metasploitable2 si basa su un sistema obsoleto, "Ubuntu 8.04". Di conseguenza, non sono riuscito ad aggiornare i vari servizi disinstallati, limitando le possibilità di migliorare la sicurezza del sistema attraverso aggiornamenti più recenti e sicuri. Questa situazione evidenzia l'importanza di operare su piattaforme supportate e aggiornate per garantire una protezione efficace contro le minacce più recenti.