Report Remediation Metasploitable

Sommario

Introduzione

- **Obiettivo del test**: L'obiettivo principale del test è identificare le vulnerabilità esistenti, valutarne il livello di rischio e comprendere l'impatto potenziale su dati, servizi e operatività aziendale. Attraverso queste attività, è stato possibile delineare un piano di intervento prioritario per mitigare i rischi riscontrati.

- **Scopo del report:** Lo scopo di questo report è fornire una panoramica dettagliata delle attività correttive eseguite per chiudere le vulnerabilità rilevate, descrivendo sia in termini generali che tecnici:
    - le azioni intraprese,
    - le motivazioni alla base degli interventi,
    - gli strumenti utilizzati,
    - e i risultati ottenuti.

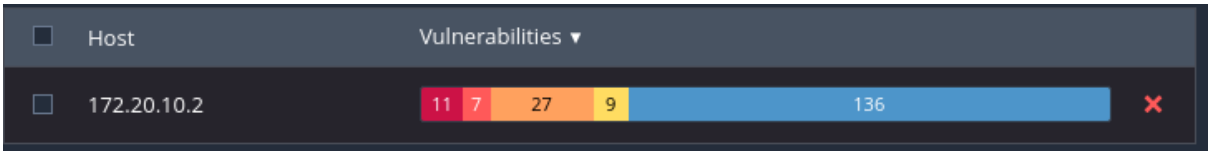
Sintesi dei Risultati

La scansione ha evidenziato che Metasploitable presenta un alto livello di vulnerabilità, con diverse criticità individuate in componenti chiave. Tuttavia, non tutte le falle rilevate sono irreparabili: una parte significativa può essere mitigata o risolta tramite aggiornamenti, configurazioni corrette e buone pratiche di sicurezza. La situazione è seria, ma gestibile con un piano d'azione mirato.

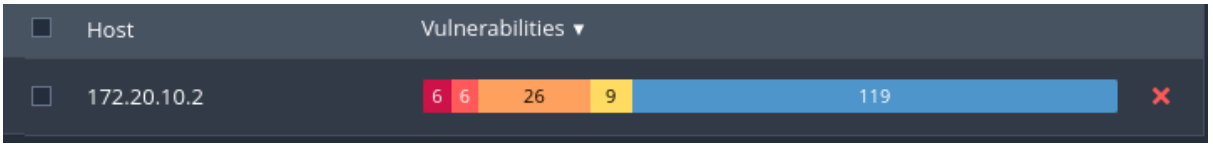
Vulnerabilità Identificate e Risolte

- **Totale vulnerabilità critiche rilevate**: 7
- **Vulnerabilità critiche risolte**: 3
- **Vulnerabilità alte risolte:** 2
- **Vulnerabilità Non risolte**: 4

Prima di intervenire:



Dopo le remediation:



Quick summary

Durante l'analisi della macchina Metasploitable, sono state individuate diverse vulnerabilità critiche sfruttabili in scenari reali. Queste falle rappresentano debolezze note nei servizi esposti e potrebbero consentire a un attaccante non autenticato di ottenere accesso remoto, eseguire codice arbitrario o compromettere la sicurezza della macchina.

Per ridurre drasticamente la superficie d'attacco e mitigare le vulnerabilità rilevate, si consiglia di adottare le seguenti misure:

- **Rimozione o aggiornamento** dei servizi vulnerabili, come UnrealIRCd, Tomcat, e versioni obsolete di VNC e SSH.
- **Modifica delle credenziali predefinite** e implementazione di autenticazioni robuste, specialmente nei servizi remoti.
- **Disabilitazione di protocolli insicuri**, quali SSLv2 e SSLv3

Dettaglio dei risultati

Di seguito viene documentata ogni vulnerabilità critica e alta trovata e una possibile soluzione sulla macchina metasploitable, con la soluzione:

Titolo	UnrealiRCd Backdoor detention	Gravita	Critica 10.0

Descrizione:
Il server IRC remoto è una versione di Unrealircd con una backdoor che consente a un aggressore di eseguire codice arbitrario sull'host interessato.**CVE-2010-2075**

Soluzione:
Il servizio UnrealIRCd, noto per includere una backdoor nelle versioni vulnerabili di Metasploitable, è stato rimosso completamente dal sistema, eliminando i binari, i file di

configurazione e i riferimenti all'avvio automatico. Questo intervento riduce la superficie di attacco associata a servizi IRC non sicuri.

```
msfadmin@metasploitable:/$ rm -rf /root/KeithNet/Unreal
msfadmin@metasploitable:/$ _
```

Titolo	Apache Tomcat AJP Connector Request Injection	Gravità	Critica 9.8

Descrizione:

È stata rilevata una vulnerabilità di lettura/inclusione di file nel connettore AJP. Un aggressore remoto e non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file delle applicazioni web da un server vulnerabile. Nei casi in cui il server vulnerabile consenta il caricamento di file, un aggressore potrebbe caricare codice JavaServer Pages (JSP) dannoso in diversi tipi di file e ottenere l'esecuzione di codice remoto (RCE).**CVE-2020-1938**.

Soluzione:

In questo caso è stata adottata la misura di disabilitazione completa del connettore AJP (Apache JServ Protocol).Questa scelta è motivata dal fatto che l'AJP non era utilizzato, rendendo inutile e potenzialmente pericolosa la sua esposizione.La disabilitazione è stata effettuata modificando il file di configurazione `server.xml`, situato nella directory `conf/` all'interno della home di Tomcat commentando la riga <connector.

```
  GNU nano 2.0.7     File: /usr/share/tomcat5.5/conf/server.xml       Modified

                        noCompressionUserAgents="gozilla, traviata"
                        compressableMimeType="text/html,text/xml"
        -->

    <!-- Define a SSL HTTP/1.1 Connector on port 8443 -->
    <!--
    <Connector port="8443" maxHttpHeaderSize="8192"
               maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
               enableLookups="false" disableUploadTimeout="true"
               acceptCount="100" scheme="https" secure="true"
               clientAuth="false" sslProtocol="TLS" />
    -->

    <!-- Define an AJP 1.3 Connector on port 8009 -->
#    <Connector port="8009"
#               enableLookups="false" redirectPort="8443" secret="Lapasswordpiu$
```

Titolo	Bind Shell Backdoor Detection	Gravità	Critica 9.8

Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un aggressore potrebbe utilizzarla connettendosi alla porta remota e inviando comandi direttamente.

Soluzione:

l file `/etc/inetd.conf` rappresenta il principale file di configurazione del demone `inetd`, un "super-server" che gestisce l'avvio e la supervisione di numerosi servizi di rete in ambiente Unix/Linux,ed è una soluzione che vedremo speso in questo report.In pratica, `inetd` ascolta le richieste sulle porte di rete specificate nel file `inetd.conf` e, al

manifestarsi di una connessione, avvia il servizio corrispondente solo su richiesta, ottimizzando così le risorse di sistema.
In questo caso commentando la riga igresslock non si avvierà il servizio.

```
msfadmin@metasploitable:~$ sudo nano /etc/inetd.conf
#ingreslock stream tcp nowait root /bin/bash bash -i
```

Titolo	Rexecd Service Detection	Gravità	Alta 7.5

Descrizione:
Il servizio rexecd è in esecuzione sull'host remoto. Questo servizio è progettato per consentire agli utenti di una rete di eseguire comandi da remoto. Tuttavia, rexecd non fornisce alcun metodo di autenticazione valido, quindi potrebbe essere utilizzato impropriamente da un aggressore per eseguire la scansione di un host di terze parti.

Soluzione:
Per disattivare il servizio rexecd, è stata modificata la configurazione del demone inetd, che gestisce l'avvio di servizi di rete su richiesta. In particolare, nel file /etc/inetd.conf, è stata commentata la riga relativa al servizio rexec.

```
#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/s
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.t
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/s
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.t
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.r
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.r
#exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.r
ingreslock stream tcp nowait root /bin/bash bash -i
```

Titolo	Rlogin service	Gravità	Alta 7.5

Descrizione:
Il servizio rlogin è in esecuzione sull'host remoto. Questo servizio è vulnerabile poiché i dati vengono trasmessi tra il client e il server rlogin in chiaro. Un aggressore man-in-the-middle può sfruttare questa vulnerabilità per intercettare login e password. Inoltre, potrebbe consentire accessi non autenticati correttamente senza password.

Soluzione:
Anche qua per disattivare il servizio Rlogin è stata modificata la configurazione del demone inetd, commentando la riga relativa al servizio login.

```
#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/s
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.t
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/s
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.t
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.r
#login          stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.r
#exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.r
ingreslock stream tcp nowait root /bin/bash bash -i
```

Vulnerabilità non risolte.

Titolo	VNC Server ‘password’ password	Gravità	Critica 10.0

Descrizione:
Il server VNC in esecuzione sull'host remoto è protetto da una password debole. Nessus è riuscito ad accedere utilizzando l'autenticazione VNC e la password "password". Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per assumere il controllo del sistema.
Soluzione provata:
Cambiare la password di accesso VNC con una chiave complessa e non banale.Per cambiarla basta usare vncpassw.

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

Titolo	Debian OpenSSH/OpenSSL Package Random Number Generator weakness	Gravità	Critica 10.0

Descrizione:
Il certificato x509 remoto sul server SSL remoto è stato generato su un sistema Debian o Ubuntu che contiene un bug nel generatore di numeri casuali della sua libreria OpenSSL.
Il problema è dovuto alla rimozione da parte di un pacchettizzatore Debian di quasi tutte le fonti di entropia nella versione remota di OpenSSL.
Un aggressore può facilmente ottenere la parte privata della chiave remota e utilizzarla per decifrare la sessione remota o impostare un attacco man-in-the-middle.**CVE-2008-0166.**

Soluzione provata:
Le chiavi SSH generate tramite versioni vulnerabili del pacchetto OpenSSL sono state rimosse e rigenerate utilizzando il comando `ssh-keygen`, mitigando così il rischio associato alla debolezza del generatore di numeri casuali.

```
msfadmin@metasploitable:~$ sudo rm /etc/ssh/ssh_host_*
```

```
msfadmin@metasploitable:~$ sudo ssh-keygen -t rsa -f /etc/ssh/ssh_host_rsa_key -
N ''
Generating public/private rsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_rsa_key.
Your public key has been saved in /etc/ssh/ssh_host_rsa_key.pub.
The key fingerprint is:
e2:9d:ec:4f:0f:a3:64:cc:a1:e4:2d:db:14:88:77:f6 root@metasploitable
msfadmin@metasploitable:~$ sudo ssh-keygen -t dsa -f /etc/ssh/ssh_host_dsa_key -
N ''
Generating public/private dsa key pair.
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
e0:53:c4:34:6b:af:dd:ab:65:ac:7b:d0:c0:93:0f:6a root@metasploitable
```

Titolo	SSL Version 2 and 3 Protocol Detection	Gravità	Critica 9.8

Descrizione:
Il servizio remoto crittografa il traffico utilizzando un protocollo con debolezze note.
Un aggressore può sfruttare queste falle per condurre attacchi man-in-the-middle o per decifrare le comunicazioni tra il servizio interessato e il client

Soluzione provata:
E' stato abilitato solo i protocolli sicuri che era commentato di default, questa configurazione forza il server a rifiutare connessioni che utilizzano SSLv2, protocolli notoriamente insicuri e soggetti a diverse vulnerabilità critiche, come POODLE (Padding Oracle On Downgraded Legacy Encryption). L'intervento risolve positivamente la vulnerabilità rilevata da Nessus associata alla **CVE-2015-0204**.

```
  GNU nano 2.0.7     File: /etc/apache2/mods-available//ssl.conf      Modified

#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
#SSLCipherSuite ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+SSLv2:+EXP:+eNULL
   enable only secure ciphers:
#SSLCipherSuite HIGH:MEDIUM:!ADH

   enable only secure protocols: SSLv3 and TLSv1, but not SSLv2
   SSLProtocol all -SSLv2 -SSLv3 +TLSv1

</IfModule>
```

Scansione finale

Al termine delle attività di mitigazione, è stata eseguita una scansione di verifica per accertare l'efficacia delle modifiche apportate e verificare l'assenza delle vulnerabilità precedentemente rilevate.

La scansione è stata effettuata utilizzando Nessus.

I risultati della scansione finale hanno confermato che alcuni dei servizi vulnerabili precedentemente rilevati risultano disabilitati o non più accessibili.

Sev	CVSS ▾	VPR	EPSS	Family	Count
CRITICAL	10.0 *	5.1	0.0165	Gain a shell remotely	2
CRITICAL	10.0			General	1
CRITICAL	10.0 *			Gain a shell remotely	1
CRITICAL	9.8			Service detection	2
HIGH	7.5 *	8.4	0.4664	Service detection	1
HIGH	7.5	5.9	0.7865	General	1
HIGH	7.5			RPC	1

Riflessioni finali

L’attività ha permesso di individuare e mitigare alcune delle vulnerabilità critiche presenti nel sistema Metasploitable. Attraverso l’applicazione di azioni mirate è stato possibile ridurre drasticamente la superficie di attacco del sistema.
La scansione finale ha confermato l’efficacia delle misure adottate.