

Traccia:

Effettuare una scansione completa sul target Metasploitable.

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.

Consegna:

- 1. Esercizio Traccia e requisiti Scansione iniziale dove si vede il grafico con tutte le vulnerabilità e le vulnerabilità da risolvere (tecnico, già riassunto) - ScansioneInizio.pdf**
- 2. Screenshot e spiegazione dei passaggi della remediation - RemediationMeta.pdf**
- 3. Scansione dopo le modifiche che evidenzia la risoluzione dei problemi/vulnerabilità (il grafico che mostra tutte le vulnerabilità) - ScansioneFine.pdf**

Oppure un report unico, a vostra scelta. Penso sia più comodo farne tre comunque.

Nota: i report possono essere lasciati in inglese, senza problemi.

Se risolvete le 4 vulnerabilità, potete risolverne una quinta (a scelta), ad esempio con una regola di firewall

Apache Tomcat AJP Connector Request Injection (Ghostcat)

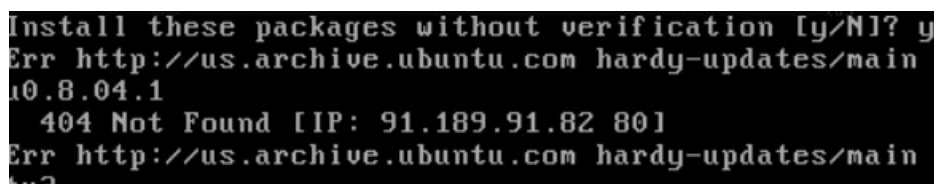
Criticità: 9.8

Plugin: 134862

Descrizione: L'AJP Connector di Tomcat, responsabile della vulnerabilità "Ghostcat", di solito opera sulla porta 8009. Questa porta permette la comunicazione tra Tomcat e altri server web come Apache HTTP. Il connettore AJP è in ascolto su host remoto. Un attaccante non autenticato potrebbe sfruttare questa vulnerabilità per leggere file di una web application da un server vulnerabile. Nei casi in cui il server consente il caricamento file, un aggressore potrebbe caricare JavaServer Pages (JSP) codice maligno con all'interno una vasta varietà di file e ottenere l'esecuzione del codice da remoto (RCE)

Risoluzione al problema: Bisognerebbe disabilitare AJP se non necessario o limitare l'accesso agli ip di fiducia. In alternativa l'opzione che suggerisco che secondo me è la migliore è cancellare questa vecchia versione di Tomcat e installarne una nuova che non sia vulnerabile.

Dato che questa macchina Metasploitable è basata su una vecchia versione di Ubuntu (Hardy Heron 8.04) usare il comando di base per aggiornare i pacchetti < **sudo apt-get update** > o installarli < **sudo apt-get install ..** > non funzionerà correttamente restituendo errore 404 Not Found in quanto i repository ufficiali sono troppo vecchi e potrebbero non esistere più.



Un modo potrebbe essere quello di modificare il file nella sources list sostituendo tutte le righe che fanno riferimento a **us.archive.ubuntu.com** e **security.ubuntu.com** con i repository legacy:

```
deb http://old-releases.ubuntu.com/ubuntu/ hardy main restricted universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ hardy-updates main restricted universe multiverse
deb http://old-releases.ubuntu.com/ubuntu/ hardy-security main restricted universe multiverse
```

Per poi aggiornare tutto o in alternativa, l'opzione per cui io ho optato, scaricarlo manualmente usando il comando

wget <https://downloads.apache.org/tomcat/tomcat-7/v7.0.100/bin/apache-tomcat-7.0.100.tar.gz>.

Attenzione: Bisogna ricordare come ho detto già in precedenza che la nostra versione di Metasploitable è basata su una vecchia versione di Ubuntu (Hardy Heron 8.04) di conseguenza utilizza vecchie librerie come Perl v.5.8.8(linguaggio di programmazione), quindi installare pacchetti troppo aggiornati non sarà possibile a meno che non la si aggiorni. Dato che questo è un ambiente volutamente vulnerabile per scopi educativi e di testing al momento sconsiglio di aggiornarla (ma per una risoluzione ai problemi più efficace ed ottimale si consiglia sempre di eseguire gli aggiornamenti alle versioni più recenti).

Detto ciò, si aggiorna la versione di Tomcat 5.5 con vulnerabilità Ghostcat ad una versione più recente ma comunque abbastanza vecchia da essere compatibile con la Perl suggerisco di scaricare la versione 7.0.100.

Procedere prima col rimuovere la vecchia versione di Tomcat utilizzando il seguente comando:

sudo apt-get remove tomcat5.5

sudo apt-get purge tomcat5.5

E poi rimuovere manualmente tutte le cartelle o i file relativi a Tomcat 5.5

```

File Macchina Visualizza Inserimento Dispositivi Aiuto
Package tomcat5.5 is not installed, so not removed
The following packages were automatically installed and are no longer required:
libcommons-collections3-java jsvc gappletviewer-4.2 libecj-java
libcommons-pool-java liboro-java libgcj8-1 debhelper libgcj-bc
intltool-debian libcommons-el-java antlr libregex-java
libcommons-modeler-java libgcj8-dev java-common liblog4j1.2-java po-debconf
libgcj8-jar ecj-gcj libportlet2.4-java libtomcat5.5-java gij-4.2
libbcel-java libcommons-io-java ant libcommons-launcher-java gcj-4.2
libcommons-logging-java ecj libcommons-fileupload-java gcj-4.2-base
libgcj-common gij gjdoc libjaxp1.3-java java-gcj-compat-headless
libgcj8-1-awt libcommons-dbcj-java libxerces2-java libcommons-daemon-java
java-gcj-compat libcommons-validator-java libcommons-collections-java
sgml-base libcommons-beanutils-java libstruts1.2-java java-gcj-compat-dev
fastjar rhino libcommons-digester-java html2text libportlet2.3-java
libecj-java-gcj libmx4j-java
Use 'apt-get autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 136 not upgraded.
msfadmin@metasploitable:~$ cd /etc/t
terminfo/ timezone tomcat5.5/
msfadmin@metasploitable:~$ sudo rm -rf /etc/tomcat5.5
msfadmin@metasploitable:~$ sudo rm -rf /var/cache/tomcat5.5
msfadmin@metasploitable:~$ sudo cp -r /home/msfadmin/apache-tomcat-7.0.100 /usr/
local/tomcat
msfadmin@metasploitable:~$ sudo chown -R msfadmin:msfadmin /usr/local/tomcat
msfadmin@metasploitable:~$

```

Dopo aver installato la nuova versione di Tomcat (7.0.100), assicurarsi che i permessi dei file siano corretti. Se necessario, modificare i permessi con:

sudo chown -R msfadmin:msfadmin /usr/local/tomcat e poi riavviare il servizio.

Per verificare se Tomcat sta girando correttamente, controllare la versione con il seguente comando:
/usr/local/tomcat/bin/version.sh

```

File Macchina Visualizza Inserimento Dispositivi Aiuto
at java.lang.Class.initializeClass(libgcj.so.81)
msfadmin@metasploitable:~$ /usr/local/tomcat/bin/startup.sh
Using CATALINA_BASE:   /usr/local/tomcat
Using CATALINA_HOME:   /usr/local/tomcat
Using CATALINA_TMPDIR: /usr/local/tomcat/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bi
/tomcat-juli.jar
Tomcat started.
msfadmin@metasploitable:~$ /usr/local/tomcat/bin/version.sh
Using CATALINA_BASE:   /usr/local/tomcat
Using CATALINA_HOME:   /usr/local/tomcat
Using CATALINA_TMPDIR: /usr/local/tomcat/temp
Using JRE_HOME:        /usr
Using CLASSPATH:       /usr/local/tomcat/bin/bootstrap.jar:/usr/local/tomcat/bi
/tomcat-juli.jar
Server version: Apache Tomcat/7.0.100
Server built:   Feb 11 2020 08:31:12 UTC
Server number:  7.0.100.0
OS Name:        Linux
OS Version:     2.6.24-16-server
Architecture:   i386
JVM Version:    1.5.0
JVM Vendor:     Free Software Foundation, Inc.
msfadmin@metasploitable:~$

```

P.s. In caso l'installazione manuale con **wget** dia problemi sulla macchina Metasploitable per motivi di versione obsoleta o mancanza di connessione ad internet si può installare il pacchetto su un'altra macchina, ad esempio Linux, e trasferirlo su Meta con **scp**

```

C:\home\kali> wget https://archive.apache.org/dist/tomcat/tomcat-7/v7.0.100/bin/apache-tomcat-7.0.100.tar.gz
--2024-09-29 13:20:47-- https://archive.apache.org/dist/tomcat/tomcat-7/v7.0.100/bin/apache-tomcat-7.0.100.tar.gz
Resolving archive.apache.org (archive.apache.org) ... 65.108.204.189, 2a01:4f9:1a:a084::2
Connecting to archive.apache.org (archive.apache.org)|65.108.204.189|:443 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 9619338 (9.2M) [application/x-gzip]
Saving to: 'apache-tomcat-7.0.100.tar.gz'

apache-tomcat-7.0.100.tar.gz  100%[=====>]  9.17M  14.9MB/s  in 0.6s

2024-09-29 13:20:48 (14.9 MB/s) - 'apache-tomcat-7.0.100.tar.gz' saved [9619338/9619338]

C:\home\kali> scp -oHostKeyAlgorithms+=ssh-rsa apache-tomcat-7.0.100.tar.gz msfadmin@192.168.1.14:/home/msfadmin/
msfadmin@192.168.1.14's password:
apache-tomcat-7.0.100.tar.gz                                100% 9394KB   3.6MB/s   00:02

```

Bind Shell Backdoor Detection

Criticità: 9.8

Plugin: 51988

Descrizione: presenza di una **Bind Shell** in ascolto su una porta remota. Una Bind Shell è un tipo di shell che apre una porta in ascolto per una connessione in entrata, consentendo a un attaccante di connettersi alla macchina e ottenere accesso alla shell di comando. Queste backdoor sono estremamente pericolose perché consentono accesso remoto non autorizzato.

Risoluzione al problema: Come prima cosa individuare la Backdoor per poi rimuoverla e per maggiore sicurezza, configura un firewall per bloccare l'accesso remoto alle porte non necessarie.

Per individuare la Backdoor consiglio di usare nmap dalla macchina Linux per fare uno script delle vulnerabilità sulla macchina target Metasploitable, ci vorrà un po' di tempo ma così sapremo

esattamente quali porte sono aperte e quali vulnerabilità contengono. Come si può vedere dall'immagine qui sotto la Backdoor si trova nella porta 21 sul servizio ftp che utilizza la versione **vsftpd 2.3.4**, questa versione è nota per avere una grave vulnerabilità che include una backdoor integrata. Questa backdoor permette a chiunque si connetta al servizio FTP sulla porta 21 di ottenere una shell remota come utente root, rappresentando un rischio critico per la sicurezza.

```
File Actions Edit View Help
C:\home\kali> sudo nmap --script=vuln 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-29 07:58 EDT
Nmap scan report for 192.168.50.101
Host is up (0.021s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|     vsFTPD version 2.3.4 backdoor
|       State: VULNERABLE (Exploitable)
|       IDs:   BID:48539  CVE:CVE-2011-2523
|         vsFTPD version 2.3.4 backdoor, this was reported on 2011-07-04.
|       Disclosure date: 2011-07-03
|       Exploit results:
|         Shell command: id
|         Results: uid=0(root) gid=0(root)
|       References:
|         https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_
backdoor.rb
|         https://www.securityfocus.com/bid/48539
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|         http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|_
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
| smtp-vuln-cve2010-4344:
|_ The SMTP server is not Exim: NOT VULNERABLE
53/tcp    open  domain
80/tcp    open  http
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| http-slowloris-check:
|   VULNERABLE:
|     Slowloris DOS attack
|       State: LIKELY VULNERABLE
|       IDs:   CVE:CVE-2007-6750
|         Slowloris tries to keep many connections to the target web server open and hold
|         them open as long as possible. It accomplishes this by opening connections to
|         the target web server and sending a partial request. By doing so, it starves
|         the http server's resources causing Denial Of Service.
```

Bisogna disabilitare e fermare immediatamente il servizio FTP per prevenire accessi non autorizzati, eseguire comandi come:

```
sudo service vsftpd stop
sudo systemctl disable vsftpd
```

Non funzionerà in quanto Metasploitable 2 utilizza un sistema di init più vecchio (init.d invece di systemctl o service). Utilizzare quindi i seguenti comandi:

```
sudo /etc/init.d/vsftpd stop
sudo /etc/init.d/vsftpd disable
```

Una volta disabilitato il servizio si può procedere col bloccare la porta 21 per tutte le connessioni in entrata tramite iptables

```
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 21 -j DROP
msfadmin@metasploitable:~$ sudo iptables-save
# Generated by iptables-save v1.3.8 on Sun Sep 29 14:07:24 2024
*filter
:INPUT ACCEPT [34638:297709711]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [17650:28417121]
COMMIT
# Completed on Sun Sep 29 14:07:24 2024
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
msfadmin@metasploitable:~$ _
```

Dopo aver applicato queste regole, il traffico sulla porta 21 sarà bloccato, impedendo accessi non autorizzati tramite vsftpd o altre potenziali vulnerabilità.

Se ciò non bastasse a risolvere il problema consiglio anche di rimuovere la versione vsftpd 2.3.4 con **sudo apt-get remove vsftpd** in quanto non necessaria se non si utilizza il protocollo FTP per trasferire file o per altri scopi, in caso di necessità invece sostituirla con una versione non vulnerabile

Debian Open SSH/Open SSL

Criticità: 10.0

Plugin: 32321

Descrizione: Questa vulnerabilità riguarda una debolezza nella generazione di numeri casuali nel pacchetto OpenSSH/OpenSSL su sistemi Debian e Ubuntu, che causa la creazione di chiavi SSL deboli. Nello specifico, il problema è stato causato dalla rimozione accidentale di quasi tutte le fonti di entropia nel generatore di numeri casuali di OpenSSL. Essendo queste chiavi facilmente prevedibili, un attaccante potrebbe ricavare la chiave privata con sufficiente potenza computazionale in modo tale da poter decifrare il traffico cifrato, eseguire attacchi man-in-the-middle e ottenere dati sensibili.

Risoluzione al problema: Per risolvere la vulnerabilità che riguarda Debian Open SSH/Open SSL è necessario eseguire l'aggiornamento del pacchetto per poi rigenerare le chiavi crittografiche. Purtroppo come ho già detto all'inizio, questa vecchia versione di Meta non permette l'aggiornamento dei pacchetti ma bisogna installarli manualmente dal sito ufficiale. La versione da installare più aggiornata e compatibile con questa macchina Meta è la versione di **OpenSSL 1.0.2u**. Prima di installare bisogna spostarsi nella directory giusta **/usr/local/src** dopo di ch  si pu  eseguire il comando per installarlo:

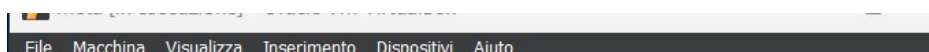
sudo wget <https://www.openssl.org/source/openssl-1.0.2u.tar.gz>

Bisogner  poi estrarre l'archivio con il comando **sudo tar -xzf openssl-1.0.2u.tar.gz** e poi spostarsi nella cartella openssl-1.0.2u. Per la configurazione e la compilazione si eseguono i rispettivi comandi:

./config

make

sudo make install



bisognerà compilare alcune informazioni per il certificato, dopo di che si trovano ed elimina la vecchia chiave con il vecchio certificato, qui salvate come "snakeoil.key" e "snakeoil.pem" e si spostano la **new_key.pem** e il **new_cert.pem** nelle directory di quelle vecchie. Vanno modificati poi i permessi di scrittura e lettura della chiave in modo tale che solo il proprietario del file possa leggerlo e scriverlo.

```
File Macchina Visualizza Inserimento Dispositivi Aiuto
Verifying - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
or some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:it
State or Province Name (full name) [Some-State]:rm
Locality Name (eg, city) []:rm
Organization Name (eg, company) [Internet Widgits Pty Ltd]:cane
Organizational Unit Name (eg, section) []:it
Common Name (eg, YOUR name) []:mesploitabile
Email Address []:msfadmin@meta.com
msfadmin@metasploitable:~$ sudo find /etc/ssl -name "*.key"
/etc/ssl/private/ssl-cert-snakeoil.key
msfadmin@metasploitable:~$ sudo find /etc/ssl -name "*.pem"
/etc/ssl/certs/ssl-cert-snakeoil.pem
msfadmin@metasploitable:~$ sudo find /etc/ssl -name "*.crt"
msfadmin@metasploitable:~$
```

Sostituire poi nel file di configurazione le vecchie chiavi con quelle nuove

```
SSLEngine on
SSLCertificateFile /etc/ssl/certs/your_cert.pem
SSLCertificateKeyFile /etc/ssl/private/your_key.pem
SSLCertificateChainFile /etc/ssl/certs/chain.pem #
```

Chiave SSH:

Eseguire il seguente comando **ssh-keygen -t rsa -b 4096** dove -t rsa specifica che il tipo di chiave da generare sarà RSA e il -b 4096 indica la lunghezza della chiave a 4096 bit. Una volta generata la chiave verrà chiesto dove la si vuole salvare, volendo si può scegliere un percorso in particolare, altrimenti premere invio per il percorso predefinito e impostare una passphrase (seguiranno una serie di domande personali a cui rispondere) per una maggiore sicurezza. Ora che la chiave è stata generata creare un file con nano dove verrà incollata manualmente

nano ~/.ssh/authorized_keys

Dato che sulla macchina Meta cliccare con il destro per copiare e incollare non funziona si dovrà copiare la chiave nella cartella temporanea **tmp** con il comando:

scp ~/.ssh/id_rsa.pub msfadmin@192.168.50.101:/tmp

poi spostarla nel file creato prima con nano con il comando:

cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys .

Dopo aver spostato la chiave eliminare il file **tmp** creato precedentemente.

Assicurarsi che file e directory abbiano i permessi corretti.

La directory **.ssh** deve avere permessi di lettura, scrittura ed esecuzione solo per il proprietario (700).

Il file **authorized_keys** deve avere permessi di lettura e scrittura solo per il proprietario (600).

Per migliorare ulteriormente la sicurezza, disabilitare l'accesso SSH tramite password nel file di configurazione di SSH sul server **sudo nano /etc/ssh/sshd_config**

#PasswordAuthentication yes
PasswordAuthentication no

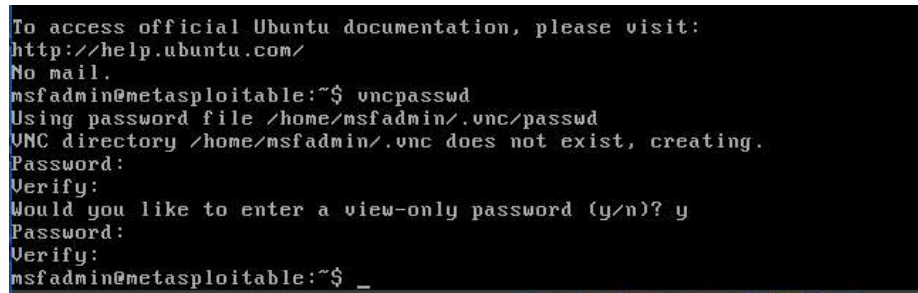
VNC Server 'password' Password

Criticità: 10.0

Plugin: 61708

Descrizione: Il server VNC è protetto da una password debole. Nessus è stato in grado di accedere utilizzando l'autenticazione VNC e una password di "password". Un utente malintenzionato da remoto e non autenticato potrebbe sfruttare questo problema per assumere il controllo del sistema.

Risoluzione al problema: Cambiare la password con una sicura e limitare l'accesso al servizio VNC. Per modificare la password si può utilizzare il seguente comando **vncpasswd**, come possiamo vedere dall'immagine qui sotto. Il sistema ha creato la directory **~/.vnc** per la prima volta chiedendo di impostare una password, suggerendo che non esisteva una configurazione precedente, lasciando di conseguenza il sistema vulnerabile.



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$ _
```

Una volta creata la password, è consigliabile riavviare il servizio VNC per applicare le modifiche.

Un'ulteriore misura di sicurezza essenziale è utilizzare un tunnel SSH per accedere al server VNC. Questo impedirà che il traffico VNC venga intercettato in rete. Quindi creare un tunnel SSH con il seguente comando:

ssh -L 5901:localhost:5901 <user>@<remote_server_ip>

Questo reindirizzerà il traffico dalla macchina locale alla porta 5901 del server remoto.

```
meta [in esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
FQDN (Fully Qualified Domain Name) and the DNS domain name (which is
part of the FQDN) in the /etc/hosts file.
sfadmin@metasploitable:~$ hostname -i
127.0.1.1
sfadmin@metasploitable:~$ ssh -L 5901:localhost:5901 msfadmin@127.0.1.1
Warning: Permanently added '127.0.1.1' (RSA) to the list of known hosts.
sfadmin@127.0.1.1's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
or mail.
Last login: Sun Sep 29 18:39:32 2024 from 192.168.50.101
sfadmin@metasploitable:~$
```

Se questo non dovesse bastare impostare dei firewall di sicurezza per bloccare l'accesso VNC a IP non autorizzati, consentendo solo connessioni da reti sicure:

```
sudo iptables -A INPUT -p tcp --dport 5900 -s [trusted IP] -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 5900 -j DROP
```

E con questo abbiamo risolto le 4 vulnerabilità richieste dalla traccia, possiamo riassumere il tutto dicendo che il modo migliore per far fronte a queste vulnerabilità è:

Aggiornare e Applicare Patch: Assicurarsi che tutti i software (Apache, BIND, OpenSSH, Samba, ecc.) siano aggiornati alle versioni più recenti e sicure.

Rimuovere Servizi Non Necessari: Disabilitare eventuali servizi o protocolli non utilizzati, come AJP o versioni obsolete di SSL.

Rafforzare la Sicurezza: Limitare l'accesso a servizi come VNC, NFS e Samba solo agli IP o utenti fidati. Implementare password forti e uniche.

Utilizzare Crittografia Forte: Assicurarsi che tutte le comunicazioni utilizzino protocolli di crittografia robusti (TLS 1.2 o superiore) e suite di cifratura forti.

Usare i Firewall per Bloccare le Porte: Assicurarsi di avere una configurazione corretta dei firewall che è essenziale per la sicurezza, specialmente su server esposti.

Auditing e Monitoraggio: Eseguire costantemente audit del sistema per rilevare eventuali cambiamenti o nuove vulnerabilità e impostare sistemi di monitoraggio per rilevare eventuali violazioni della sicurezza.

Vulnerabilità aggiuntiva: SSL Version 2 and 3 Protocol Detection

Criticità: 9.8

Plugin: 20007

Descrizione: SSLv2 e SSLv3 sono protocolli deprecati, noti per avere molte vulnerabilità. Lasciare attivi questi protocolli potrebbe esporre il server ad attacchi come POODLE (Padding Oracle On Downgraded Legacy Encryption), che permette di decifrare il contenuto delle comunicazioni crittografate e man-in-the-middle.

Risoluzione al problema: Per risolvere la vulnerabilità di **SSL** (ad esempio SSLv2/SSLv3) e migliorare la sicurezza del server, bisogna modificare la configurazione di **Apache** per disabilitare le vecchie versioni di **SSL** e utilizzare solo protocolli più sicuri come **TLS**. Per farlo modificare o aggiungere alcune direttive di sicurezza al file

/etc/apache2/mods-available/ssl.conf

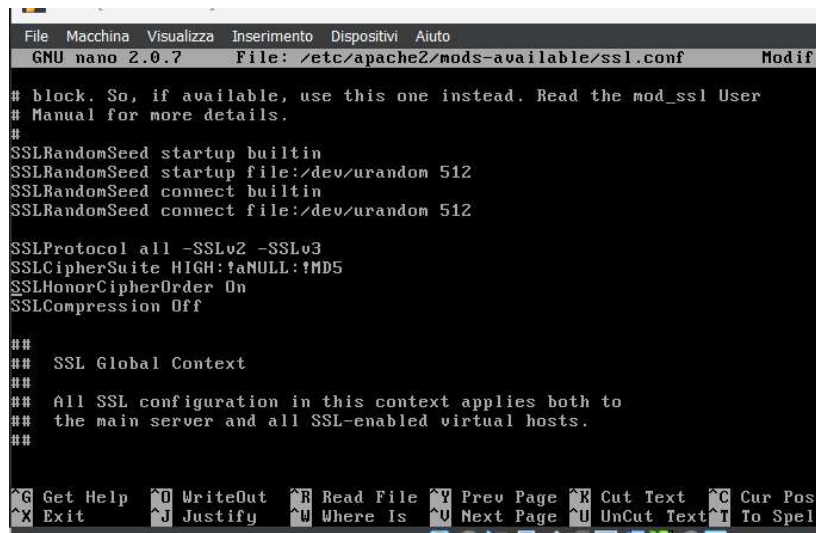
Fare in modo che il file abbia le seguenti configurazione dove:

SSLProtocol all -SSLv2 -SSLv3: accetta tutti i protocolli, tranne **SSLv2** e **SSLv3**.

SSLCipherSuite HIGH:!aNULL:!MD5: accetta solo le suite di cifratura forti (**HIGH**), esclude quelle che non forniscono autenticazione (**aNULL**) e quelle che utilizzano **MD5**.

SSLHonorCipherOrder On: fa in modo che il server preferisca le ciphersuites più sicure in caso di negoziazione.

SSLCompression Off: disabilita la compressione SSL per evitare attacchi di tipo **CRIME**.



```
File Macchina Visualizza Inserimento Dispositivi Aiuto
GNU nano 2.0.7 File: /etc/apache2/mods-available/ssl.conf Modif
# block. So, if available, use this one instead. Read the mod_ssl User
# Manual for more details.
#
SSLRandomSeed startup builtin
SSLRandomSeed startup file:/dev/urandom 512
SSLRandomSeed connect builtin
SSLRandomSeed connect file:/dev/urandom 512

SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite HIGH:!aNULL:!MD5
SSLHonorCipherOrder On
SSLCompression Off

##
## SSL Global Context
##
## All SSL configuration in this context applies both to
## the main server and all SSL-enabled virtual hosts.
##

^G Get Help ^O WriteOut ^R Read File ^V Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^U Where Is ^N Next Page ^U UnCut Text ^T To Spell
```

Salva le modifiche e riavvia il servizio apache2.