

REPORT TECNICO NESSUS SCAN & VULNERABILITIES ASSESSMENT

PROGETTO W12-D5



Redatto da Andrea Sciattella

09/05/2024

INDICE

1. Traccia	3
2. Sommario esecutivo	4
3. Introduzione	5
4. Remediation Action	6
134862- Ghostcat.....	6/7
51988- Bind Shell Backdoor	8/10
11356- NFS Exported Share Information Disclosure	11/13
61708- VNC Server 'password' Password.....	14
5. Conclusioni.....	15

TRACCIA

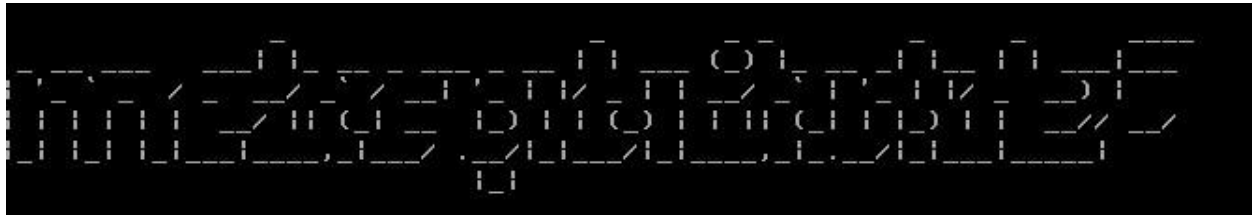
Effettuare una scansione completa sul target **Metasploitable**.

Scegliete da un minimo di 2 fino ad un massimo di 4 vulnerabilità **critiche** e provate ad **implementare delle azioni di rimedio**.

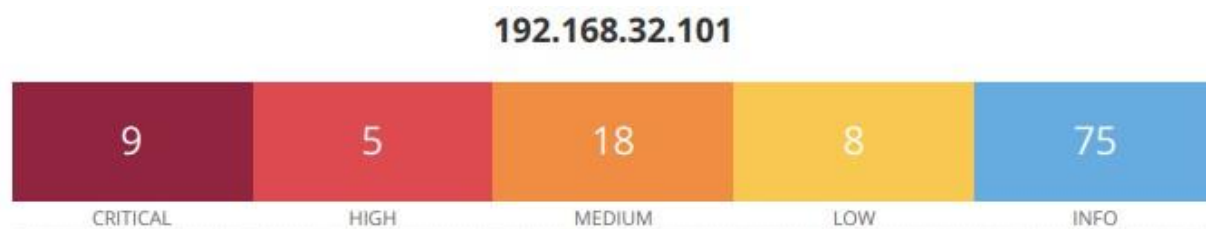
N.B. le azioni di rimedio, in questa fase, potrebbero anche essere delle regole firewall ben configurate in modo da limitare eventualmente le esposizioni dei servizi vulnerabili. Vi consigliamo tuttavia di utilizzare magari questo approccio **per non più di una vulnerabilità**.

Per dimostrare l'efficacia delle azioni di rimedio, eseguite nuovamente la scansione sul target e confrontate i risultati con quelli precedentemente ottenuti.

Ai fini della soluzione, abbiamo scelto le vulnerabilità in giallo nella figura in slide 3.



1. SOMMARIO ESECUTIVO



Vulnerabilities

Total: 115

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password

INFORMAZIONI HOST:

Nome NetBIOS: "METASPLOITABLE";

Indirizzo IP: 192.168.32.101;

Indirizzo MAC: 08:00:27:03:10:A4;

OS: Unix-Linux, Linux Kernel 2.6 on Ubuntu 8.04.

La scansione effettuata, dalla durata di circa 20 minuti, è riuscita a rilevare 116 vulnerabilities, divise in 9 **CRITIC**, 1 **HIGH**, 22 **MEDIUM**, 8 **LOW** e 75 addizionali categorizzate in **INFO**.

INTRODUZIONE

Per la produzione scritta di questa prova siamo stati incaricati di produrre un **report scritto di una scan e a seguito di un remediation plan per l'host METASPLOITABLE.**

Il tool utilizzato è *Tenable Nessus*, un software tipo Client-Server di scansione per tutti i tipi di vulnerabilità, uno dei migliori in questi ambiti.

Una volta installato il tool sulla nostra VM di Kali Linux e controllata la connettività tra le macchine, abbiamo configurato una scansione completa a tutte le porte dell'indirizzo IP 192.168.32.101(**Metasploitable**).

Vulnerabilities					Total: 115
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME	
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)	
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection	
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection	
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)	
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection	
CRITICAL	10.0*	5.1	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	
CRITICAL	10.0*	5.1	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure	
CRITICAL	10.0*	-	61708	VNC Server 'password' Password	

Successivamente abbiamo scelto 4 delle 9 vulnerabilità critiche che andremo a risolvere una ad una, che sono:

- ***Apache Tomcat AJP connector Request Injection (anche detta Ghostcat),***
- ***Bind Shell Backdoor che è stata rilevata,***
- ***NFS Exported Share Information Disclosure,***
- ***VNC Server 'password' Password.***

REMEDIATION ACTION

134862 - Iniezione di richieste del connettore AJP di Apache Tomcat (Ghostcat)

Sinossi:

Sull'host remoto è in ascolto un connettore AJP vulnerabile.

Descrizione:

È stata riscontrata una vulnerabilità nella lettura/inclusione di file nel connettore AJP. Un aggressore remoto non autenticato potrebbe sfruttare questa vulnerabilità per leggere i file dell'applicazione web da un server vulnerabile.

Nei casi in cui il server vulnerabile consente l'upload di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file e ottenere un accesso di codice remoto (RCE).

Soluzione:

Aggiornare la configurazione AJP per richiedere l'autorizzazione e/o aggiornare il server Tomcat a 7.0.100, 8.5.51, 9.0.31 o successivo.

Referenze:

CVE CVE-2020-1745

CVE CVE-2020-1938

XREF CISA-KNOWN-EXPLOITED:2022/03/17

XREF CEA-ID:CEA-2020-0021

Plugin Output:

tcp/8009/ajp13

Risk Factor:

High

CVSS v3.0 Base Score 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

La prima Vulnerability che andremo a sistemare è la ID:134862, anche detta Ghostcat:

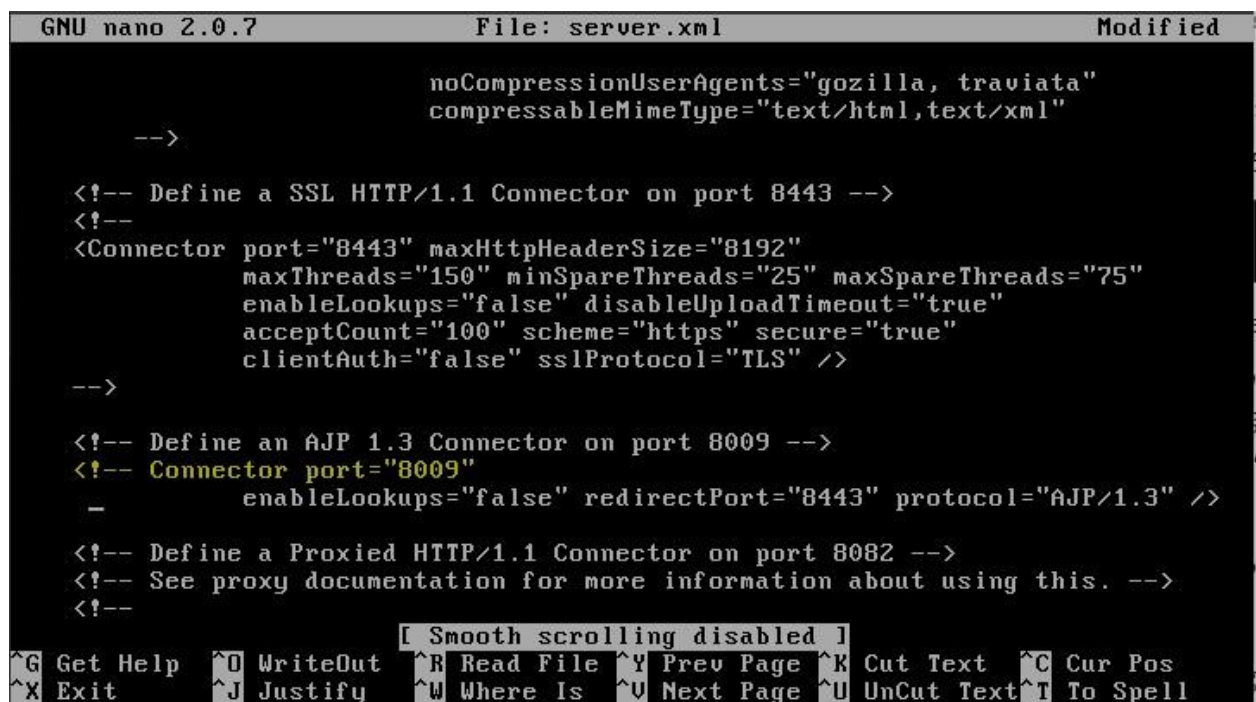
1. Seguiamo il path /etc/tomcat5.5,

```
root@metasploitable:/# cd etc/  
root@metasploitable:/etc# cd tomcat5.5/  
root@metasploitable:/etc/tomcat5.5#
```

2. Apriamo il file di configurazione del server Apache Tomcat5.5 (server.xml),

(Apache Tomcat è un server web open source sviluppato dalla Apache Software Foundation. Implementa le specifiche JavaServer Pages e servlet, fornendo quindi una piattaforma software per l'esecuzione di applicazioni web sviluppate in linguaggio Java)

3. Commentiamo il file nella sezione per rimuovere "AJP 1.3 on port 8009".



```
GNU nano 2.0.7 File: 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" protocol="AJP/1.3" />  
-->  
  
<!-- Define a Proxyed HTTP/1.1 Connector on port 8082 -->  
<!-- See proxy documentation for more information about using this. -->  
<!--  
  
[ Smooth scrolling disabled ]  
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

Oltre a questa modifica possiamo aggiungere un modo di autenticazione aggiuntivo alla porta con l'implementazione dell'attributo "secret".

Il report Nessus consiglia inoltre di implementare **l'aggiornamento dell'applicazione** a una delle **versioni recenti** poiché per la versione 5.5 è terminato il supporto e lo sviluppo di patch d'aggiornamento.

51988 - Bind Shell Backdoor Detection

Sinossi:

L'host remoto potrebbe essere stato compromesso.

Descrizione:

Una shell è in ascolto sulla porta remota senza che sia richiesta alcuna autenticazione. Un utente malintenzionato può utilizzarla

connettendosi alla porta remota e inviando direttamente i comandi.

Soluzione:

Verificare se l'host remoto è stato compromesso e, se necessario, reinstallare il sistema.

Fattore di rischio:

Critico

Punteggio base CVSS v3.0:

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Punteggio base CVSS v2.0:

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Informazioni sul plugin:

Pubblicato: 2011/02/15, Modificato: 2022/04/11

Output del plugin:

tcp/1524/wild_shell

La prossima vulnerabilità che sistemeremo è ID: **51988**, una backdoor pronta all'uso che permette l'entrata nel nostro sistema Metasploitable come utente Root, molto pericolosa data la sua efficacia.

1. Il primo passo è identificare la porta e il servizio in ascolto nel nostro sistema che permette il funzionamento di questa backdoor. Andiamo a connetterci tramite il comando **netcat** **INDIRIZZO IP (192.168.32.101** nel nostro caso) **PORTA (1524** come rilevato da *Nessus*) da Kali a Meta per confermare la presenza di questa vulnerabilità;

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)~  
$ netcat 192.168.32.101 1524  
root@metasploitable:~# ls  
bin  
boot  
cdrom  
dev  
etc  
home  
initrd  
initrd.img  
lib  
lost+found  
media  
mnt  
nohup.out  
opt  
proc  
root  
sbin  
srv  
sys  
tmp  
usr  
var  
vmlinuz  
root@metasploitable:~#
```

2. Ora dobbiamo trovare il **PID** (*Process Identifier*) del processo nella **porta 1524** che permette l'ingresso all'host senza autenticazione;

```
kali@kali: ~  
File Actions Edit View Help  
root@metasploitable:~# netstat -tulpn  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name  
tcp 0 0 0.0.0.0:47584 0.0.0.0:* LISTEN 4586/rmiregistry  
tcp 0 0 0.0.0.0:512 0.0.0.0:* LISTEN 4471/xinetd  
tcp 0 0 0.0.0.0:513 0.0.0.0:* LISTEN 4471/xinetd  
tcp 0 0 0.0.0.0:2049 0.0.0.0:* LISTEN -  
tcp 0 0 0.0.0.0:514 0.0.0.0:* LISTEN 4471/xinetd  
tcp 0 0 0.0.0.0:60421 0.0.0.0:* LISTEN 3690/rpc.statd  
tcp 0 0 0.0.0.0:8009 0.0.0.0:* LISTEN 4548/jsvc  
tcp 0 0 0.0.0.0:6697 0.0.0.0:* LISTEN 4606/unrealircd  
tcp 0 0 0.0.0.0:3306 0.0.0.0:* LISTEN 4193/mysql  
tcp 0 0 0.0.0.0:1099 0.0.0.0:* LISTEN 4586/rmiregistry  
tcp 0 0 0.0.0.0:6667 0.0.0.0:* LISTEN 4606/unrealircd  
tcp 0 0 0.0.0.0:139 0.0.0.0:* LISTEN 4436/smbd  
tcp 0 0 0.0.0.0:5900 0.0.0.0:* LISTEN 4604/Xtightvnc  
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 3674/portmap  
tcp 0 0 0.0.0.0:6000 0.0.0.0:* LISTEN 4604/Xtightvnc  
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 4567/apache2  
tcp 0 0 0.0.0.0:8787 0.0.0.0:* LISTEN 4590/ruby  
tcp 0 0 0.0.0.0:8180 0.0.0.0:* LISTEN 4548/jsvc  
tcp 0 0 0.0.0.0:1524 0.0.0.0:* LISTEN 4471/xinetd
```

3. Spostiamoci su Meta e **killiamo** il processo individuato tramite **PID** poco fa;

```
msfadmin@metasploitable:~$ sudo kill 4477
[sudo] password for msfadmin:
msfadmin@metasploitable:~$
```

4. Dopo aver terminato il processo che consente l'accesso alla backdoor, riproviamo tramite *netcat* su **Kali** ad entrare usando la **porta 1524**;

```
(kali@kali)-[~]
$ netcat 192.168.32.101 1524
(UNKNOWN) [192.168.32.101] 1524 (ingreslock) : Connection refused
```

Come possiamo vedere siamo riusciti ad eliminare momentaneamente il processo e di conseguenza la backdoor nel sistema, ma per rendere l'azione completamente definitiva, abbiamo due opzioni possibili:

- **Formattare il sistema**, per eliminare ogni file malevolo nel sistema;
- **Attivare e configurare una regola del firewall** per la porta in questione, in modo da bloccare ogni accesso alla porta 1524.

5. La nostra scelta è quella di implementare un regola firewall tramite *IPTABLES* (firewall di linux), utilizzando l'utente **root** e la riga *iptables -A INPUT -p tcp --dport 1524 -j DROP* che andrà a DROPPARE le richieste in INPUT alla PORTA 1524;

```
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 1524 -j DROP
root@metasploitable:/home/msfadmin# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ingreslock
DROP      tcp  --  anywhere              anywhere               tcp dpt:ingreslock
```

6. Riproviamo la connessione con *Netcat* su Kali per vedere se la regola firewall è entrata in vigore;

```
(kali@kali)-[~]
$ netcat 192.168.32.101 1524
```

Come possiamo vedere dall'ultimo screen la nostra regola funziona e dropa ogni pacchetto alla porta 1524, rendendo INACCESSIBILE e impossibile utilizzare la backdoor installata.

11356 - Divulgazione di informazioni sulle azioni esportate da NFS

Sinossi:

È possibile accedere alle condivisioni NFS sull'host remoto.

Descrizione:

Almeno una delle condivisioni NFS esportate dal server remoto può essere montata dall'host di scansione. Un attaccante potrebbe essere in grado di sfruttare questa possibilità per leggere (ed eventualmente scrivere) i file sull'host remoto.

Soluzione:

Configurare NFS sull'host remoto in modo che solo gli host autorizzati possano montare le sue condivisioni remote.

Fattore di rischio:

Critico

Punteggio VPR:

5.9

Punteggio base CVSS v2.0:

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Riferimenti

CVE CVE-1999-0170

CVE CVE-1999-0211

CVE CVE-1999-0554

Sfruttabile con:

Metasploit (vero)

Informazioni sul plugin:

Pubblicato: 2003/03/12, Modificato: 2023/08/30

Output del plugin:

udp/2049/rpc-nfs

Passiamo ora alla ID: **11356**, vulnerabilità che permette alle condivisioni NFS di essere montate da host esterni, creando la possibilità di leggere (ed eventualmente scrivere) i file sull'host remoto.

1. Per prima cosa andiamo a modificare il file locato in `/etc/exports`, in cui modificheremo gli host autorizzati e i permessi di lettura/scrittura;

```
GNU nano 2.0.7      File: exports      Modified
# /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)
#
/mnt/nfs_progetto  *(ro,root_squash,subtree_check)
```

In questo modo abbiamo reindirizzato il percorso del file ad una directory creata appositamente in `/mnt/nfs_progetto` dando gli attributi `ro` (SOLO LETTURA), `root_squash` (una misura di sicurezza che limita i privilegi di root sui file condivisi) e `subtree_check` (che attiva il controllo delle sottodirectory).

2. Il secondo file da modificare è posizionato sempre in `/etc`, nominato `hosts.allow`, che contiene elenchi di regole che specificano quali client possono accedere ai servizi di rete configurati;

```
GNU nano 2.0.7      File: hosts.allow
# /etc/hosts.allow: list of hosts that are allowed to access the system.
#                 See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: LOCAL @some_netgroup
#              ALL: .foobar.edu EXCEPT terminalserver.foobar.edu
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
#ALL:ALL
```

Commentando la riga, negherà l'accesso a tutti gli host che proveranno ad accedere al sistema dal momento che non c'è una regola effettiva.

3. L'ultimo file da modificare è posizionato sempre nella directory /etc ed è nominato hosts.deny, che a differenza dell'hosts.allow specifica gli host a cui è espressamente negato l'accesso ai servizi di rete;

```
GNU nano 2.0.7      File: hosts.deny      Modified
# /etc/hosts.deny: list of hosts that are _not_ allowed to access the system.
#                  See the manual pages hosts_access(5) and hosts_options(5).
#
# Example:      ALL: some.host.name, .some.domain
#              ALL EXCEPT in.fingerd: other.host.name, .other.domain
#
# If you're going to protect the portmapper use the name "portmap" for the
# daemon name. Remember that you can only use the keyword "ALL" and IP
# addresses (NOT host or domain names) for the portmapper, as well as for
# rpc.mountd (the NFS mount daemon). See portmap(8) and rpc.mountd(8)
# for further information.
#
# The PARANOID wildcard matches any host whose name does not match its
# address.
#
# You may wish to enable this to ensure any programs that don't
# validate looked up hostnames still leave understandable logs. In past
# versions of Debian this has been the default.
ALL: 192.168.32.100
```

Abbiamo inserito **ALL** (che indica tutti i servizi) e l'indirizzo IPv4 (192.168.32.100) della nostra macchina **Kali**.

Una volta modificati tutti e tre i file (non necessariamente con le mie stesse istruzioni, ma in base allo scenario e alle proprie esigenze), la vulnerabilità è stata rimossa del tutto.

61708 - VNC Server 'password' Password

Sinossi:

Un server VNC in esecuzione sull'host remoto è protetto da una password debole.

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 una password "password". Un aggressore remoto e non autenticato potrebbe sfruttare questa falla per prendere il controllo del sistema.

Soluzione:

Proteggere il servizio VNC con una password forte.

Fattore di rischio:

Critico

Punteggio base CVSS v2.0:

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

Informazioni sul plugin:

Pubblicato: 2012/08/29, Modificato: 2015/09/24

Output del plugin:

tcp/5900/vnc

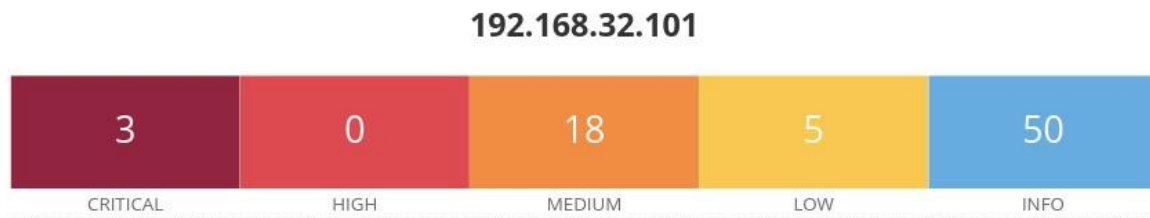
Ora tratteremo la Vulnerabilità ID: **61708**, cioè la password del server VNC impostata di base su "password", risolvere quest'ultima può essere un passaggio molto facile ma delicato.

1. La soluzione a questa vulnerability è creare una password forte contro gli attacchi di Brute Force (nel nostro caso abbiamo inserito "P6tdRIT4hF0Ylxl");

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Verify:
```

Si potrebbe anche implementare una regola di firewall per regolare il traffico in questa porta.

CONCLUSIONE



Vulnerabilities Total: 76

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	-	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
MEDIUM	8.6	-	136769	ISC BIND Service Downgrade / Reflected DoS
MEDIUM	7.5	-	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	7.5	-	90509	Samba Badlock Vulnerability
MEDIUM	6.5	-	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted

Terminata la Remediation Action, abbiamo ripetuto la scansione già usata ad inizio V.A. che ha rilevato 3 **CRITIC**, 0 **HIGH**, 18 **MEDIUM**, 5 **LOW** e 50 addizionali categorizzate in **INFO**.

Per concludere, la scansione *Nessus* eseguita sull'host **Metaspoitable** (IPv4 192.168.32.101) ha evidenziato originariamente **9 Vulnerabilità critiche** ed attraverso le nostre attività di remediation, siamo riusciti a risolverne con successo 4, riducendo il rischio di esposizione a potenziali minacce.

Tuttavia, restano ancora vulnerabilità non affrontate, che richiedono attenzione e azioni immediate per garantire la sicurezza e l'integrità del sistema.