

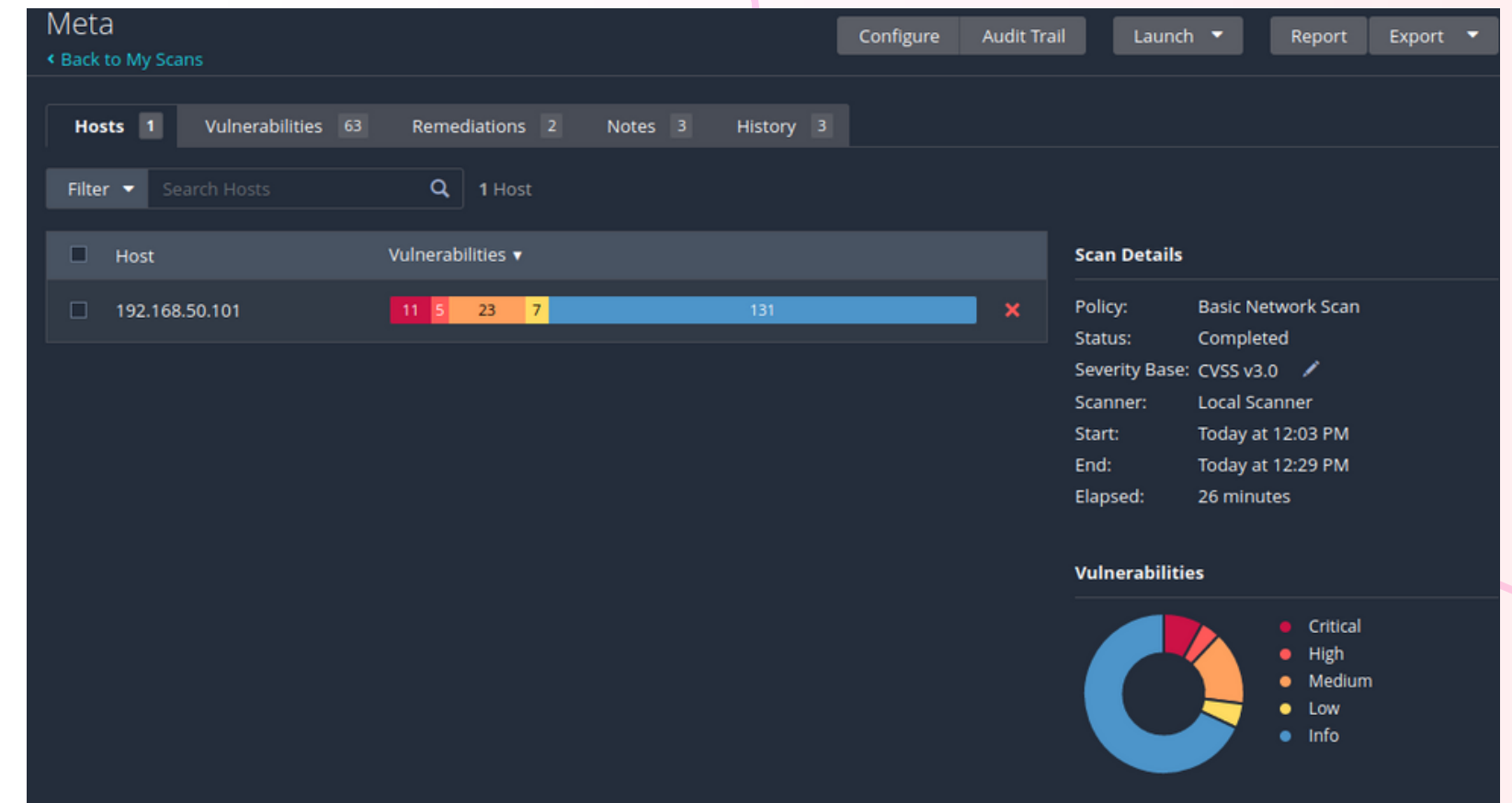


S5 L5 Project Remediation Plan

Daniele Zizzi

Scansione con Nessus verso metasploit

Utilizzando l'applicativo Nessus, ho effettuato una scansione delle vulnerabilità di Metasploit. A scansione ultimata, ho ricevuto il report delle vulnerabilità, classificate per grado di rischio. In seguito, ho visionato le più gravi ed ho applicato alcune modifiche al sistema metasploit, per risolverle.



Di seguito, il report della prima scansione, con le vulnerabilità prese in esame



192.168.50.101				
9	4	17	6	75
CRITICAL	HIGH	MEDIUM	LOW	INFO
Vulnerabilities				
				Total: 111
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*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	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
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	6.7	90509	Samba Badlock Vulnerability
MEDIUM	6.5	3.6	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
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service

Come prima falla grave, ho trovato l'NFS di linux, ovvero il servizio NETWORK FILE SHARING. Tale servizio, permette di montare delle cartelle del sistema e quindi di visualizzarle e modificarne il contenuto a seconda dei permessi assegnati.

Leggendo il file exports, utilizzando il comando "sudo nano /etc/exports", possiamo notare che, nell'ultima riga, vi è una regola che permette di montare tutte cartelle presenti nel sistema con tutti i permessi.

Quindi ho semplicemente commentato con "#", tale riga, in modo da disattivare la regola. Risolvendo così, tale vulnerabilità. Poi ho riavviato il servizio, in modo da fargli leggere le nuove impostazioni.

CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

```
GNU nano 2.0.7      File: exports
# /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)
#
/*(rw,sync,no_root_squash,no_subtree_check)
```

```
#/      *(rw,sync,no_root_squash,no_subtree_check)
```

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

VNC server, è un servizio che permette di controllare una macchina da remoto, in interfaccia grafica.

In questo caso, la falla è presente per colpa di una password troppo banale, in questo caso “password”.

Con il comando `sudo su`, sono passato all'utente root.

Ho lanciato il comando “`vnc password`”, per poter modificare la password di autenticazione al server VNC.

Dopo la modifica, ho riavviato il server, affinché leggesse la nuova configurazione con “`vncserver`”

CRITICAL VNC Server 'password' Password

Description

The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.

Solution

Secure the VNC service with a strong password.

```
msfadmin@metasploitable:~$ sudo su
```

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

```
root@metasploitable:/home/msfadmin# vncserver

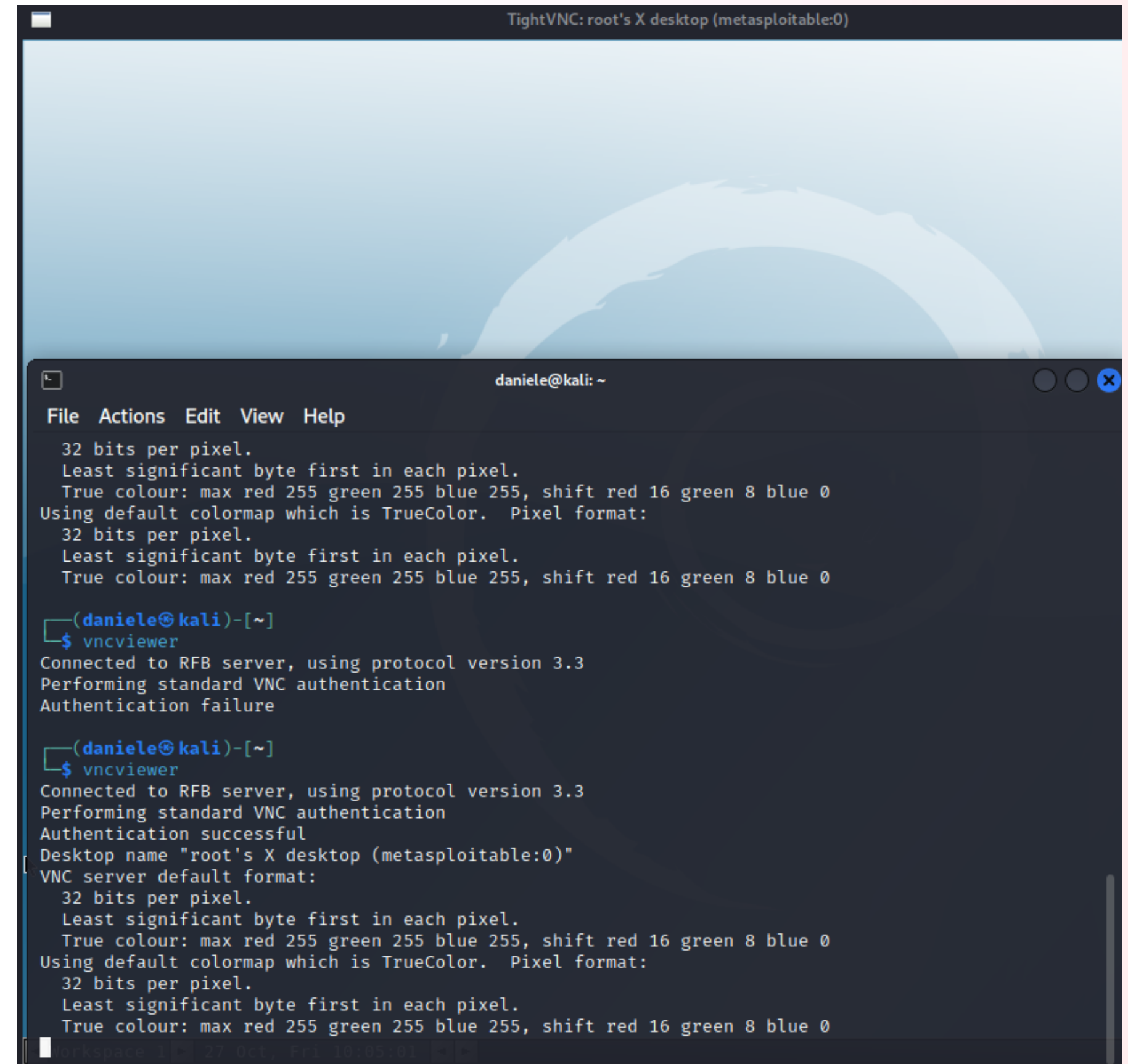
New 'X' desktop is metasploitable:2

Starting applications specified in /root/.vnc/xstartup
Log file is /root/.vnc/metasploitable:2.log
```


In seguito, ho verificato che la password richiesta per l'accesso, fosse realmente quella impostata da me in precedenza.

Ho tentato di rifare il login con la password "password", ed ho ottenuto "authentication failure".

Ho ritentato con la password impostata da me e sono riuscito ad effettuare il login.



The screenshot shows a VNC viewer window titled "TightVNC: root's X desktop (metasploitable:0)". Inside the viewer is a terminal window titled "daniele@kali: ~". The terminal shows the output of the "vncviewer" command, which includes color format information and authentication status. The first attempt shows "Authentication failure", and the second attempt shows "Authentication successful".

```
TightVNC: root's X desktop (metasploitable:0)

(daniele@kali)-[~]
$ vncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication failure

(daniele@kali)-[~]
$ vncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0

workspace 1 | 27 Oct, Fri 10:05:01 | 5/5
```

La bind shell backdoor detection, è una vulnerabilità che sfrutta il servizio ingreslock sulla porta tcp 1524, che permette di connettersi alla macchina ed inviare comandi senza bisogno di autenticazione. Quindi installare backdoor e ottenere i privilegi di amministratore. Questo tipo di attacco, a differenza della reverse shell, viene effettuato dall'attaccante verso il bersaglio.

Per chiudere tale falla, ho modificato il file di configurazione inetd.conf, che gestisce i servizi in una rete, andando a disattivare la regola ingreslock.

inetd viene utilizzato per ridurre il carico di sistema, invocando i "daemon", solo quando necessario.

CRITICAL Bind Shell Backdoor Detection

Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.

```
Meta [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
GNU nano 2.0.7      File: /etc/inetd.conf      Modified

#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sb$
telnet                stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te$
#<off># ftp              stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sb$
tftp                  dgram   udp      wait    nobody   /usr/sbin/tcpd  /usr/sbin/in.tf$
shell                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs$
login                 stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl$
exec                  stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re$
#ingreslock stream tcp nowait root /bin/bash bash -i
```

Il protocollo samba, viene utilizzato per la condivisione di file e stampanti in windows. In questo caso, la vulnerabilità, deriva da un impropria autenticazione tra client e server, rendendo possibile attacchi di tipo man in the middle.

Per ovviare a ciò, basterebbe aggiornare il protocollo in questione all'ultima versione disponibile. Non potendo fare ciò con la metasploit, ho deciso di bloccare, tramite firewall, la porta che erogano tale servizio, abilitando il firewall di meta con il comando "ufw enable" e aggiungendo le regole "ufw deny 445" e "ufw deny 139".

Con il comando "ufw status", ho visualizzato le regole attive nel firewall.

HIGH Samba Badlock Vulnerability

Description
The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

Solution
Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

```
445:tcp DENY Anywhere
445:udp DENY Anywhere
139:tcp DENY Anywhere
139:udp DENY Anywhere
```


Di seguito, il report della scansione finale, dove si evince la mancaza delle vulnerabilità precedentemente risolte.



192.168.50.101				
5	2	14	6	63
CRITICAL	HIGH	MEDIUM	LOW	INFO
Vulnerabilities				
				Total: 90
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	3.6	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
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	5.1	136808	ISC BIND Denial of Service
MEDIUM	5.9	3.6	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	4.4	89058	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
MEDIUM	5.9	4.4	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	4.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.3	-	15901	SSL Certificate Expiry



**Get protected
today!**