

PROGETTO S5L5

SCANSIONE COMPLETA METASPLOITABLE 2: ANALISI E RISOLUZIONE VULNERABILITÀ



Simone La Porta

SOMMARIO



01

TRACCIA PROGETTO

02

SCANSIONE E REPORT

03

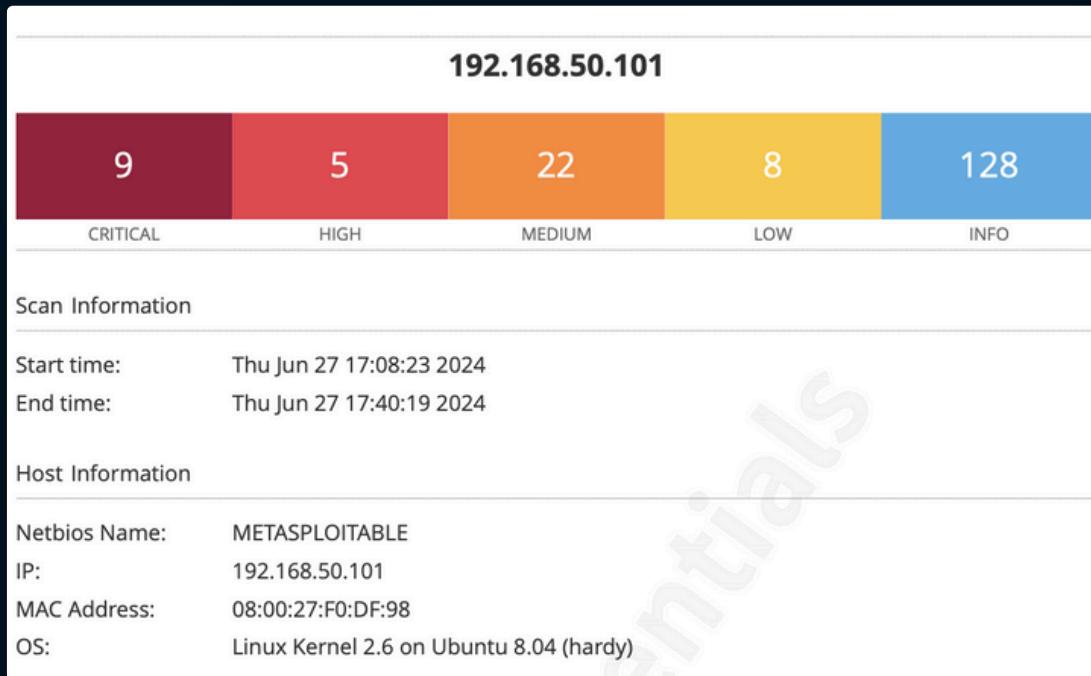
ANALISI E RISOLUZIONE VULNERABILITÀ CRITICHE

- ID 51988 - BIND SHELL BACKDOOR DETECTION
- ID 32314 - DEBIAN OPENSSH/OPENSSL PACKAGE RANDOM NUMBER GENERATOR WEAKNESS
- ID 11356 - NFS EXPORTED SHARE INFORMATION DISCLOSURE
- ID 61708 - VNC SERVER "PASSWORD" PASSWORD
- ID 20007 - SSL VERSION 2 AND 3 PROTOCOL DETECTION
- ID 33850 - UNSUPPORTED UNIX OPERATING SYSTEM DETECTION
- ID 134862 - APACHE TOMCAT AJP CONNECTOR REQUEST INJECTION (GHOSTCAT)

01

TRACCIA

- Effettuare una scansione completa sul target Metasploitable 2.
- Selezionare da un minimo di 2 a un massimo di 4 vulnerabilità critiche o ad alto rischio e implementare delle azioni di rimedio. Le azioni di rimedio potrebbero includere configurazioni di firewall per limitare le esposizioni dei servizi vulnerabili.
- Dopo aver implementato le azioni di rimedio, eseguire nuovamente la scansione sul target e confrontare i risultati con quelli precedentemente ottenuti.



02

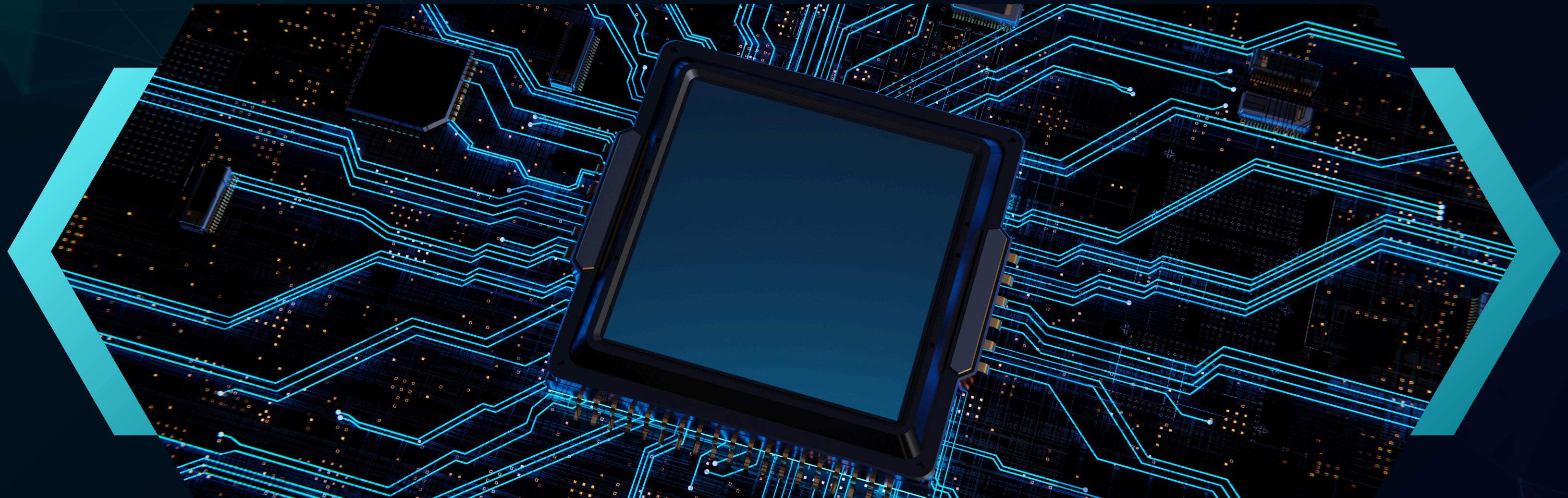
SCANSIONE E REPORT

- Per la scansione, è stato utilizzato Nessus con il tool "Basic Network Scan". La scansione ha coperto tutte le porte e tutte le tipologie di vulnerabilità web, con il target specifico di Metasploitable 2.
- Nessus ha prodotto un report delle vulnerabilità rilevate, suddivise per livello di criticità.
- In questa analisi ci si è dedicati alla risoluzione delle sole vulnerabilità critiche riscontrate.



03

ANALISI E RISOLUZIONE VULNERABILITÀ CRITICHE



ID 51988 - BIND SHELL BACKDOOR DETECTION

DESCRIZIONE

- Una shell è in ascolto sulla porta remota 1524 senza autenticazione.
- Necessario verificare se l'host remoto è stato compromesso e reinstallare il sistema se necessario e chiudere la porta 1524.

RISOLUZIONE

- Chiudere la porta 1524:
 - Utilizzare il comando "sudo netstat -tulnp | grep 1524" per verificare lo stato della porta e il processo che la utilizza.
 - Utilizzare "sudo kill <PID>" per terminare il processo che utilizza la porta 1524.
 - Verificare la chiusura della porta con il comando "sudo nmap -sS -p 1524 <indirizzo_ip_Meta>".
- Configurare una regola firewall:
 - Configurare una regola firewall su *iptables* per filtrare il traffico sulla porta 1524 con il comando "sudo iptables -A INPUT -p tcp --dport 1524 -j DROP".
 - Verificare l'efficacia della regola con "sudo nmap -Pn -p 1524 <indirizzo_ip_Meta>".

```
msfadmin@metasploitable:~$ sudo netstat -tulnp | grep 1524
tcp      0      0 0.0.0.0:1524          0.0.0.0:*
LISTEN
4544/xdinetd
msfadmin@metasploitable:~$ sudo kill 4544
msfadmin@metasploitable:~$ sudo iptables -A INPUT -p tcp --dport 1524 -j DROP
```

```
(root㉿kali)-[~/home/kali]
# nmap -sS -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 11:57 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).

PORT      STATE SERVICE
1524/tcp  closed  ingreslock
MAC Address: 08:00:27:F0:DF:98 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
```

```
(root㉿kali)-[~/home/kali]
# nmap -Pn -p 1524 192.168.50.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-28 12:00 CEST
Nmap scan report for 192.168.50.101
Host is up (0.0014s latency).

PORT      STATE SERVICE
1524/tcp  filtered  ingreslock
MAC Address: 08:00:27:F0:DF:98 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.46 seconds
```

ID 32314 - DEBIAN OPENSSH/OPENSSL PACKAGE RANDOM NUMBER GENERATOR WEAKNESS

DESCRIZIONE

- La chiave host SSH generata su Debian o Ubuntu è debole a causa di un problema nel generatore di numeri casuali della libreria OpenSSL.
- Necessario rigenerare tutte le chiavi crittografiche SSH, le chiavi SSL e OpenVPN.

RISOLUZIONE

- Rigenerare tutte le chiavi crittografiche SSH:
 - Eliminare le vecchie chiavi con il comando "sudo rm /etc/ssh/ssh_host_*".
 - Rigenerare le chiavi utilizzando il comando "sudo dpkg-reconfigure openssh-server".
- Rigenerare le chiavi SSL e OpenVPN seguendo le istruzioni specifiche nei rispettivi file di configurazione.

```
root@metasploitable:/home/msfadmin# rm /etc/ssh/  
ssh/ ssl/  
root@metasploitable:/home/msfadmin# rm /etc/ssh/ssh_host_*  
root@metasploitable:/home/msfadmin# dpkg-reconfigure openssh-server  
Creating SSH2 RSA key; this may take some time ...  
Creating SSH2 DSA key; this may take some time ...  
* Restarting OpenBSD Secure Shell server sshd [ OK ]  
root@metasploitable:/home/msfadmin#
```

ID 11356 - NFS EXPORTED SHARE INFORMATION DISCLOSURE

DESCRIZIONE

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

RISOLUZIONE

Configurare NFS sull'host remoto, modificando il file "/etc(exports" per restringere i permessi di accesso:

- Modificare la seguente riga per limitare l'accesso solo agli host autorizzati della rete 192.168.50.0/24:
 - "/path/to/share 192.168.50.0/24(ro,sync,no_subtree_check)"
- Riavviare il servizio NFS con il comando "sudo exportfs -ra".

```
# /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)
```

PRE

```
# /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)
#
#           192.168.50.0/24(ro,sync,no_root_squash,no_subtree_check)
```

POST

ID 61708 - VNC SERVER "PASSWORD" PASSWORD

DESCRIZIONE

- Il server VNC in esecuzione sull'host remoto è protetto da una password debole ("password").
- Un aggressore remoto non autenticato potrebbe sfruttare questa situazione per prendere il controllo del sistema.
- Necessario proteggere il servizio VNC con una password più complessa.

RISOLUZIONE

- Cambiare la password del server VNC:
 - Utilizzare il comando "vncpasswd" per impostare una nuova password più robusta: "5-a:76B/".
- Implementare l'autenticazione a due fattori (2FA) seguendo le istruzioni specifiche del provider VNC.
- Configurare il firewall per permettere l'accesso VNC solo da indirizzi IP autorizzati:
 - Aggiungere una regola firewall su *iptables* con il comando "sudo iptables -A INPUT -p tcp --dport 5900 -s <IP\autorizzato> -j ACCEPT".
 - Bloccare tutti gli altri accessi con il comando "sudo iptables -A INPUT -p tcp --dport 5900 -j DROP".

```
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin# iptables -A INPUT -p tcp --dport 5900 -j DROP
P
root@metasploitable:/home/msfadmin#
```

ID 20007 - SSL VERSION 2 AND 3 PROTOCOL DETECTION

DESCRIZIONE

- Il servizio remoto accetta connessioni criptate usando SSL 2.0 e/o SSL 3.0, che presentano diverse vulnerabilità crittografiche.
- Necessario disabilitare SSL 2.0 e 3.0 e utilizzare TLS 1.2 o versioni superiori con suite di cifratura approvate.

RISOLUZIONE

- Disabilitare SSL 2.0 e 3.0:
 - Modificare il file di configurazione del servizio che utilizza SSL/TLS per disabilitare SSL 2.0 e 3.0.
 - Ad esempio, per Apache, modificare il file "/etc/apache2/mods-available/ssl.conf" modificando la riga **SSLProtocol all -SSLv2 -SSLv3** con un protocollo più sicuro.
 - Riavviare il servizio per applicare le modifiche, ad esempio "sudo service apache2 restart".

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

</IfModule>
"/etc/apache2/mods-available/ssl.conf" 60L, 2157C written
root@metasploitable:/home/msfadmin# service apache2 restart
```

ID 33850 - UNSUPPORTED UNIX OPERATING SYSTEM DETECTION

DESCRIZIONE

- Il sistema operativo Unix in esecuzione sull'host remoto non è più supportato dal fornitore.



RISOLUZIONE

- Aggiornare a una versione di Unix attualmente supportata:
 - Eseguire il backup dei dati importanti.
 - Scaricare ad esempio l'ultima versione di Ubuntu Server LTS.
 - Seguire le istruzioni di installazione per aggiornare il sistema operativo.

ID 134862 - APACHE TOMCAT AJP CONNECTOR REQUEST INJECTION (GHOSTCAT)

DESCRIZIONE

- Vulnerabilità nel connettore AJP di Apache Tomcat che consente la lettura o l'inclusione di file.
- 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 il caricamento di file, un utente malintenzionato potrebbe caricare codice JavaServer Pages (JSP) dannoso all'interno di una serie di tipi di file e ottenere l'esecuzione di codice remoto (RCE).
- Necessario

RISOLUZIONE

- Aggiornare Apache Tomcat:
 - Scaricare l'ultima versione di Apache Tomcat.
 - Seguire le istruzioni di aggiornamento specifiche per Apache Tomcat.
- Disabilitare il connettore AJP se non necessario:
 - Modificare il file "server.xml" di Tomcat per commentare o rimuovere la configurazione del connettore AJP.
- Implementare un WAF per proteggere il server:
 - Configurare e implementare un Web Application Firewall (WAF) come ModSecurity.

ID 134862 - APACHE TOMCAT AJP CONNECTOR REQUEST INJECTION (GHOSTCAT)

- Disabilitare il connettore AJP modificando il file "server.xml" di Tomcat.
- Riavviare il servizio Apache Tomcat.
- Verificare che il connettore non sia più in ascolto sulla porta 8009 tramite "sudo netstat -tulnp | grep 8009".

```
<!--  
<!-- Define an AJP 1.3 Connector on port 8009 -->  
<Connector port="8009"  
enableLookups="false" redirectPort="8443" protocol="AJP/1.3" />  
-->
```

```
root@metasploitable:/home/msfadmin# /etc/init.d/tomcat5.5 stop  
* Stopping Tomcat servlet engine tomcat5.5 [ OK ]  
root@metasploitable:/home/msfadmin# /etc/init.d/tomcat5.5 start  
* Starting Tomcat servlet engine tomcat5.5 [ OK ]  
root@metasploitable:/home/msfadmin# netstat -tulnp | grep 8009
```

CONFRONTO PRE/POST RISOLUZIONE VULNERABILITÀ

- Dopo aver agito per risolvere le vulnerabilità, si è effettuata un'altra scansione per verificare l'effettività delle soluzioni adottate.**
- Si può notare come le uniche vulnerabilità non scomparse sono quelle che necessitano di un aggiornamento software.**

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
7	4	16	7	68

Vulnerabilities Total: 102

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
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
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable
HIGH	7.5	5.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	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	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	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	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

PRE

192.168.50.101

CRITICAL	HIGH	MEDIUM	LOW	INFO
3	2	13	6	34

Vulnerabilities Total: 58

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*	5.1	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	5.1	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	4.4	136808	ISC BIND Denial of Service
MEDIUM	5.9	4.4	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	-	15901	SSL Certificate Expiry
MEDIUM	5.3	-	26928	SSL Weak Cipher Suites Supported
MEDIUM	4.0*	6.3	52611	SMTP Service STARTTLS Plaintext Command Injection
MEDIUM	4.3*	-	90317	SSH Weak Algorithms Supported
MEDIUM	4.3*	3.7	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)

POST

THANK YOU