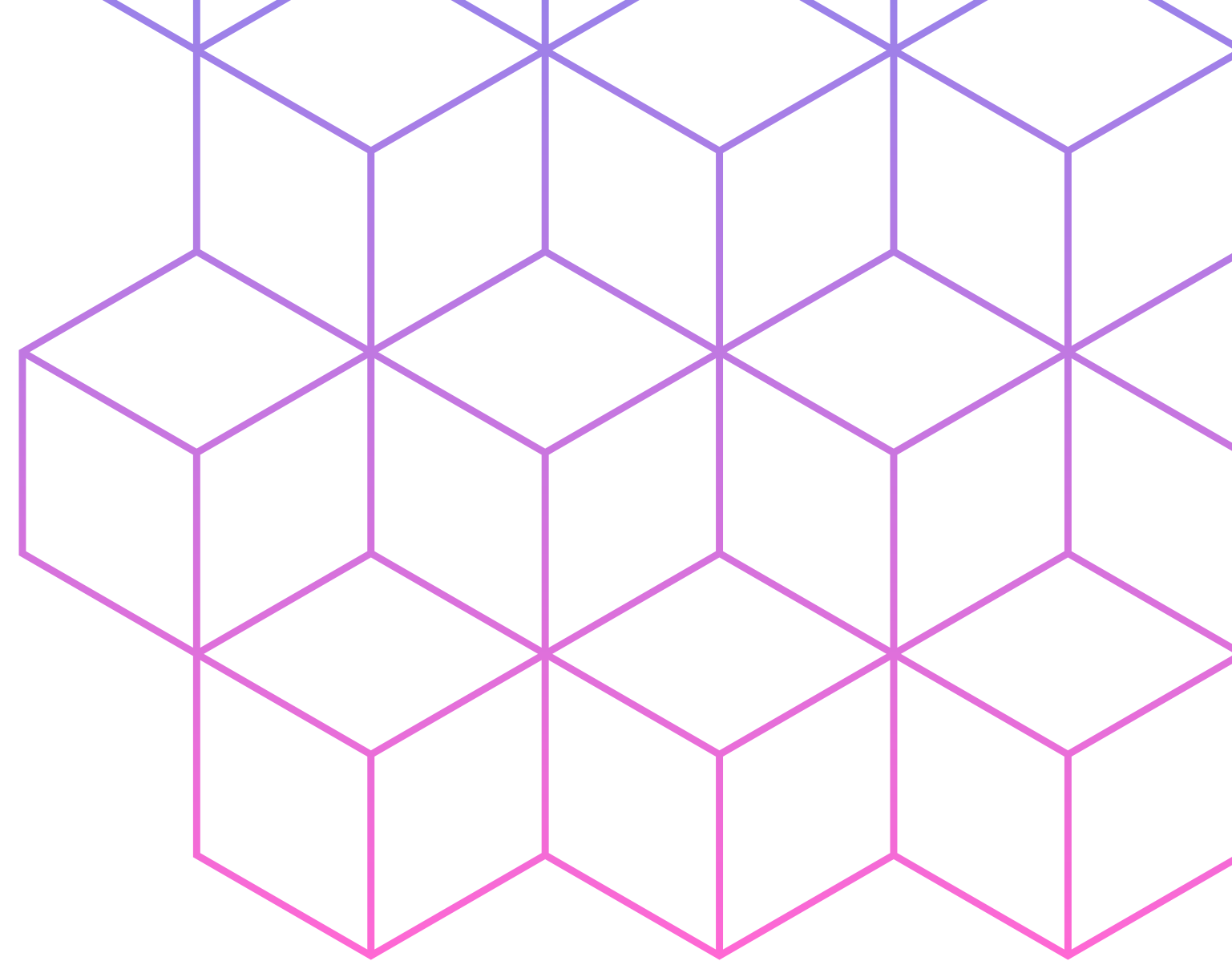
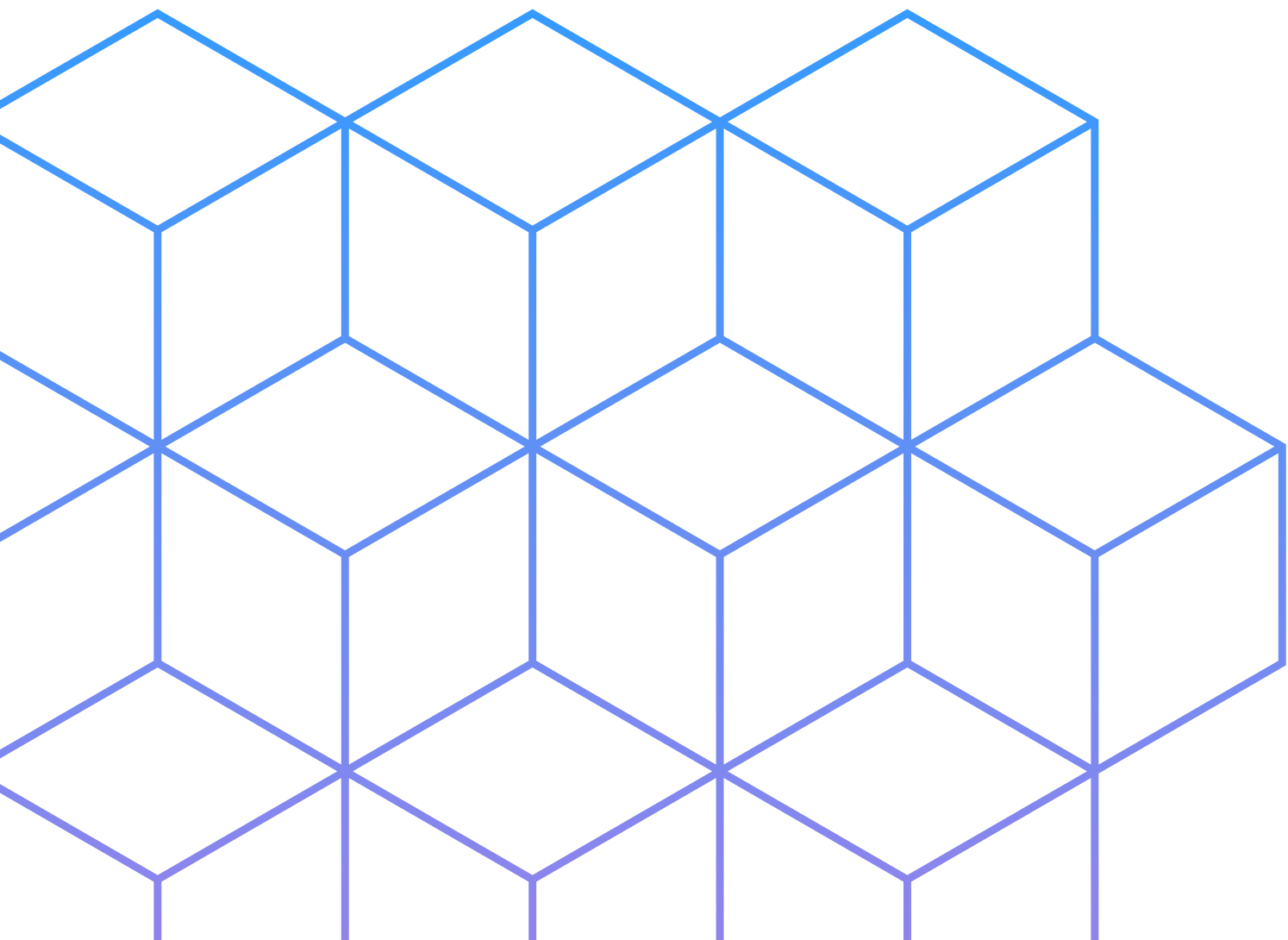
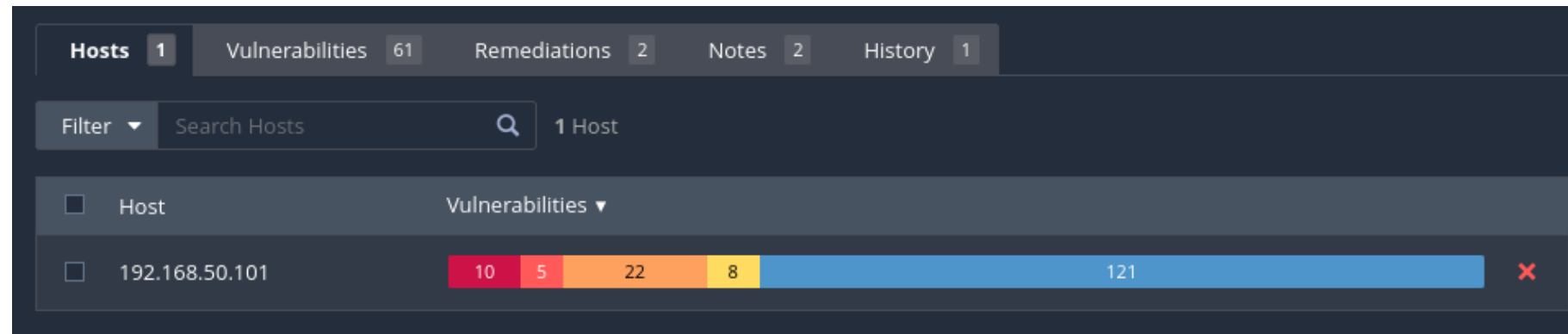


# ***S<sub>5</sub>L<sub>5</sub>***



Elaborato da: Antonio Perna.



# Panoramica

Il progetto di oggi ci chiedeva di fare una scansione completa sulla macchina di metasploitable da nessus, vedere le vulnerabilità e dare delle soluzioni per correggerle.

Apache Tomcat AJP Connector  
Request Injection (Ghostcat)

Bind Shell Backdoor Detection

SSL Version 2 and 3 Protocol  
Detection

VNC Server 'password'  
Password

Unix Operating System  
Unsupported Version  
Detection

Debian OpenSSH/OpenSSL  
Package Random Number  
Generator Weakness

NFS Exported Share  
Information Disclosure

**Indices**

# Apache Tomcat AJP Connector Request Injection (Ghostcat)

## **CRITICAL** Apache Tomcat AJP Connector Request Injection (Ghostcat)

### **Description**

A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).

### **Solution**

Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.

## Descrizione

Questa è una vulnerabilità critica che consente agli attaccanti di eseguire codice arbitrario sul server utilizzando una richiesta appositamente progettata.

## Soluzione

- Aggiorna Apache Tomcat alla versione più recente che risolve questa vulnerabilità.
- Configura correttamente le impostazioni di sicurezza di Apache Tomcat per mitigare questo tipo di attacco.

# Bind Shell Backdoor Detection

## Descrizione

Questa vulnerabilità indica la presenza di un backdoor nel sistema che potrebbe essere utilizzato per ottenere accesso non autorizzato.

## Soluzione

- Indaga sulla presenza del backdoor e rimuovilo dal sistema.
- Analizza i file di log e l'attività di rete per identificare come è stato introdotto il backdoor.

**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.

**Output**  

```
Nessus was able to execute the command "id" using the
following request :

This produced the following truncated output (limited to 10 lines) :
..... snip .....
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

..... snip .....
```

# Bind Shell Backdoor Detection

## Soluzione

- Indaga sulla presenza del backdoor e rimuovilo dal sistema.
- Analizza i file di log e l'attività di rete per identificare come è stato introdotto il backdoor.

```
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ nc 192.168.50.101 1524
root@metasploitable:/# ^C

(kali㉿kali)-[~]
$ nc 192.168.50.101 1524
(UNKNOWN) [192.168.50.101] 1524 (ingreslock) : Connection refused

(kali㉿kali)-[~]
$ 
No such process

root@metasploitable:/# ps
  PID TTY          TIME CMD
  8995 ?        00:00:00 bash
  9008 ?        00:00:00 ps
root@metasploitable:/# sudo kill 4407
root@metasploitable:/# ^C

(kali㉿kali)-[~]
$ nc 192.168.50.101 1524
root@metasploitable:/# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/# whoami
root
root@metasploitable:/# sudo lsof -i :1524
COMMAND PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd   4452 root  12u  IPv4  12070      TCP *:ingreslock (LISTEN)
bash     9015 root   0u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
bash     9015 root   1u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
bash     9015 root   2u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
bash     9015 root  255u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
lsof     9029 root   0u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
lsof     9029 root   1u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
lsof     9029 root   2u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
root@metasploitable:/# sudo kill 12070
root@metasploitable:/# sudo lsof -i :1524
COMMAND PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd   4452 root  12u  IPv4  12070      TCP *:ingreslock (LISTEN)
bash     9015 root   0u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
bash     9015 root   1u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
bash     9015 root   2u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
bash     9015 root  255u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
lsof     9033 root   0u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
lsof     9033 root   1u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
lsof     9033 root   2u  IPv4  25674      TCP 192.168.50.101:ingreslock→192.168.50.100:34750 (ESTABLISHED)
root@metasploitable:/# sudo kill 4452
```

## Soluzione

Andiamo ad accedere alla root di meta con il comando “nc ip porta” poi con il comando sudo lsof -i :1524 vediamo il pid e con kill pid togliamo l’accesso



# SSL Version 2 and 3 Protocol Detection

## Descrizione

Indica la presenza di supporto per i protocolli SSL versione 2 e 3, che sono noti per avere vulnerabilità di sicurezza serie.

## Soluzione

- Disabilita il supporto per SSL versione 2 e 3 e utilizza solo TLS.
- Aggiorna i servizi e le librerie SSL/TLS a versioni più recenti che non supportano SSL v2 e v3.

CRITICAL

SSL Version 2 and 3 Protocol Detection

< >

Description

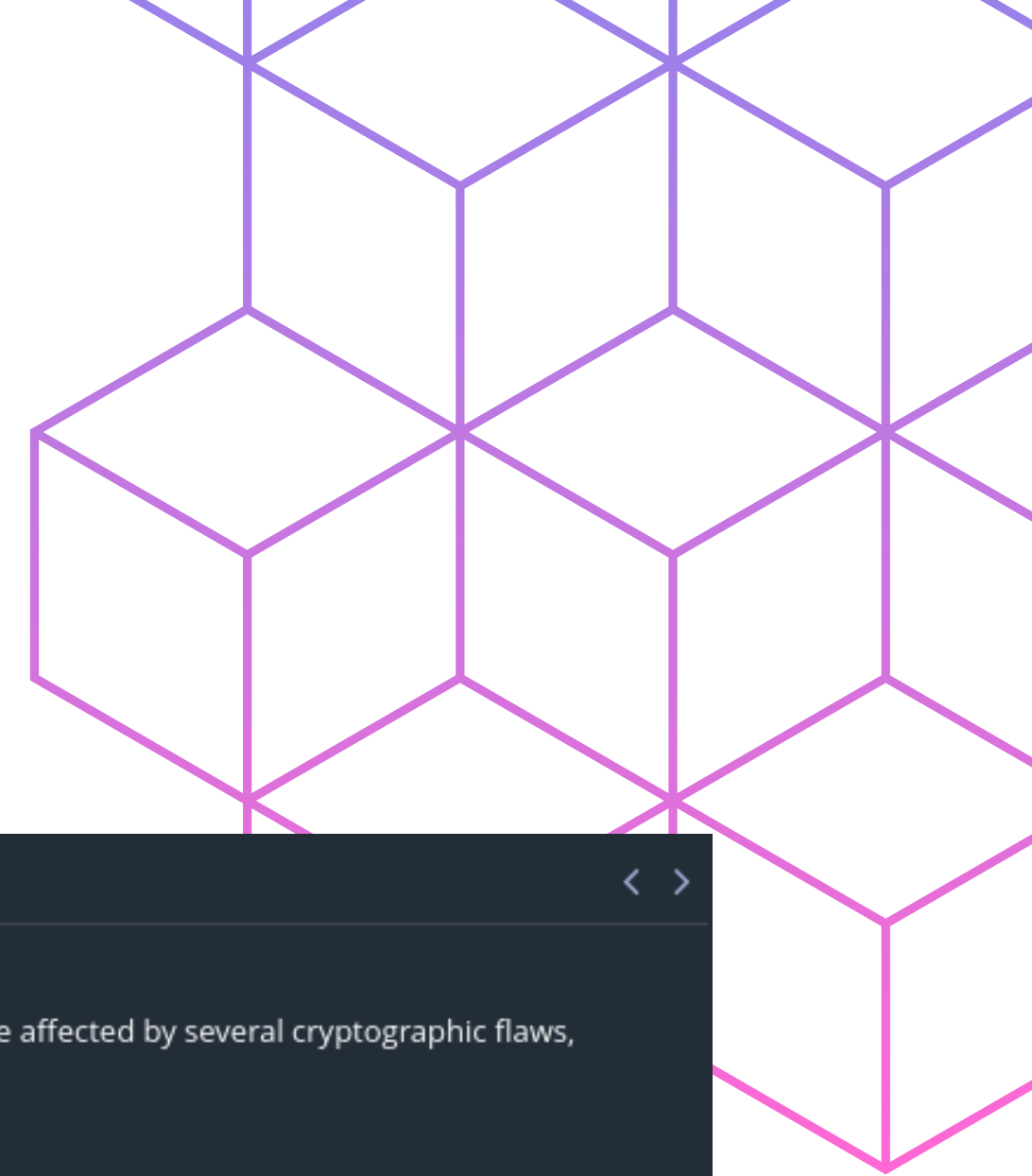
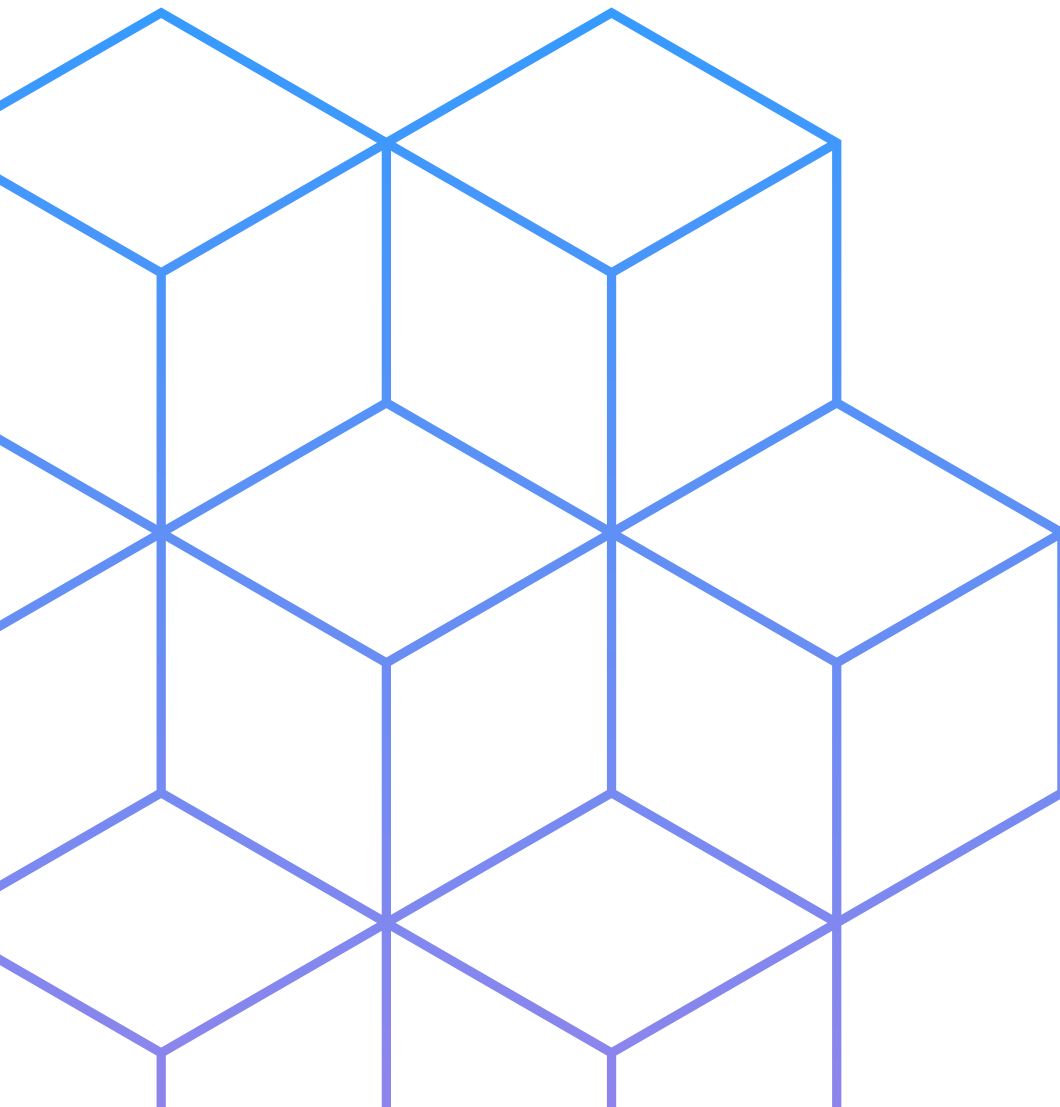
The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including:

- An insecure padding scheme with CBC ciphers.
- Insecure session renegotiation and resumption schemes.

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.  
  
Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely.  
  
NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.  
Use TLS 1.2 (with approved cipher suites) or higher instead.



# Unix Operating System Unsupported Version Detection

1

## Descrizione

Questa vulnerabilità segnala l'uso di una versione non supportata di un sistema operativo Unix, che potrebbe non ricevere più aggiornamenti di sicurezza.

2

## Soluzione

- Aggiorna il sistema operativo Unix a una versione supportata che riceva ancora aggiornamenti di sicurezza.

CRITICAL

### Unix Operating System Unsupported Version Detection

< >

#### Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

#### Solution

Upgrade to a version of the Unix operating system that is currently supported.



# Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

## Descrizione

Queste sono vulnerabilità che coinvolgono la generazione casuale di numeri nei pacchetti di OpenSSH/OpenSSL su sistemi Debian. Potrebbero consentire ad un attaccante di prevedere i numeri casuali utilizzati per crittografare le comunicazioni.

## Soluzione

- Aggiorna i pacchetti OpenSSH e OpenSSL a versioni che risolvono questa vulnerabilità.
- Monitora l'attività del sistema per eventuali segni di compromissione.

CRITICAL

## Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

### Description

The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.

### Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.

### Solution

Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.



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.

# NFS Exported Share Information Disclosure

## Descrizione

Indica una vulnerabilità che consente agli attaccanti di accedere a informazioni sensibili da condivisioni NFS esposte.

## Soluzione

- Limita l'accesso alle condivisioni NFS solo ai client autorizzati.
- Imposta correttamente le autorizzazioni sui file e sulle cartelle esportate via NFS per proteggere i dati sensibili.



## NFS Exported Share Information Disclosure

### Soluzione

- Limita l'accesso alle condivisioni NFS solo ai client autorizzati.
- Imposta correttamente le autorizzazioni sui file e sulle cartelle esportate via NFS per proteggere i dati sensibili.

```
msfadmin@metasploitable:~$ /etc/exports
-bash: /etc/exports: Permission denied
msfadmin@metasploitable:~$ /etc/hosts.allow
-bash: /etc/hosts.allow: Permission denied
msfadmin@metasploitable:~$ /etc/hosts.deny
-bash: /etc/hosts.deny: Permission denied
```

### Soluzione

Per limitare l'accesso ai file andiamo ad inserire i comandi “/etc/exports”, “/etc/hosts.allow” e “/etc/hosts.deny” e vediamo che toglie tutti i permessi

# VNC Server 'password' Password

## Descrizione

Indica la presenza di password predefinite o facilmente prevedibili per un server VNC, che potrebbero essere sfruttate per ottenere accesso non autorizzato.

## Soluzione

- Cambia la password predefinita del server VNC.
- Se possibile, usa meccanismi di autenticazione più robusti, come l'uso di chiavi SSH anziché password.

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.

Output

Nessus logged in using a password of "password".

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.50.101

# VNC Server 'password' Password

## Soluzione

- Cambia la password predefinita del server VNC.
- Se possibile, usa meccanismi di autenticazione più robusti, come l'uso di chiavi SSH anziché password.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
VNC directory /home/msfadmin/.vnc does not exist, creating.
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

## Soluzione

Su metasploitable, per risolvere questa vulnerabilità, andiamo a digitare il comando “vncpasswd” che ci fa reimpostare la password e risolviamo.