

# NESSUS

Nell'esercizio odierno è stato studiato il funzionamento del software Nessus, tool che fornisce informazioni soggettive in grado di effettuare, dato un indirizzo IP, con il quale la nostra macchina sia comunicante, un ping, invierà pacchetti TCP con la TWH completa, in modo da scansionare le porte aperte, SO e registri, ed infine proverà tramite diversi exploit ad attaccare la macchina.

Al fine di prendere confidenza con il software in questione, è stato effettuato uno scan sulla macchina vulnerabile Metasploitable 2. Dopo un po' di tempo il software ha fornito come risultati 9 vulnerabilità critiche, nonché altre vulnerabilità più o meno gravi. In seguito alla scansione sono state fornite ulteriori informazioni sulle vulnerabilità trovate, spiegando nel dettaglio come sia stato possibile sfruttarle e le possibili soluzioni per limitare il problema, stilando in totale 4 report differenti.

The screenshot shows the Nessus Essentials web interface. The left sidebar contains navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'TerraScan'. The main area displays a table of vulnerabilities. The table has columns for severity (e.g., CRITICAL, HIGH, MEDIUM, LOW), score, plugin ID, name, category, and actions. A summary on the right shows a donut chart for vulnerability counts by severity and a table with scan details like IP, MAC, OS, Start/End time, and Elapsed time.

Severity	Score	Plugin ID	Vulnerability Name	Category	Count
CRITICAL	10.0	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0	*	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	0.9728	Apache Tomcat AJP Connector Request Injection (GHOSTCAT)	Web Servers	1
CRITICAL	9.8	*	SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8	*	Bind Shell Backdoor Detection	Backdoors	1
HIGH	7.5	0.0358	Samba Badlock Vulnerability	General	1
HIGH	7.5	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5	0.015	rsh Service Detection	Service detection	1
HIGH	7.5	*	NFS Shares World Readable	RPC	1
MEDIUM	6.5	*	TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5	*	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	0.9524	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MEDIUM	5.9	0.0031	SSL Anonymous Cipher Suites Supported	Service detection	1
LOW	3.7	0.9736	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)	Misc.	1
LOW	2.6	*	X Server Detection	Service detection	1
LOW	2.1	0.8808	ICMP Timestamp Request Remote Date Disclosure	General	1
CRITICAL	...	...	SSL (Multiple Issues)	Gain a shell remotely	3

This screenshot shows a detailed report for the 'UnrealIRCd Backdoor Detection' vulnerability. It includes a description of the remote IRC server, a solution to re-download and re-install the software, and a list of references. The 'Output' section shows the command 'uid=0(root) gid=0(root)' and a table of affected hosts.

**Vulnerabilities** 66

**CRITICAL** UnrealIRCd Backdoor Detection

**Description**  
The remote IRC server is a version of UnrealIRCd with a backdoor that allows an attacker to execute arbitrary code on the affected host.

**Solution**  
Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

**See Also**  
<https://seclists.org/fulldisclosure/2010/jun/277>  
<https://seclists.org/fulldisclosure/2010/jun/284>  
<http://www.unrealircd.com/txt/unrealsecadvisory.20100612.txt>

**Output**

The remote IRC server is running as :

```
uid=0(root) gid=0(root)
```

To see debug logs, please visit individual host

Port	Hosts
6667 / tcp / irc	192.168.178.28

# UnrealIRCd

In modo particolare è stata inoltre effettuata una ricerca, nonché analisi in articolare su 5 vulnerabilità critiche. La prima è una vulnerabilità relativa alla UnrealIRCd Backdoor, in cui se ci si informa sui link forniti da Nessus ci dirà che “Abbiamo scoperto che il file Unreal3.2.8.1.tar.gz sui nostri mirror è stato sostituito qualche tempo fa con una versione dotata di backdoor (trojan). Questa backdoor consente a una persona di eseguire QUALSIASI comando con il file privilegi dell'utente che esegue l'ircd. La backdoor può essere eseguita indipendentemente da qualsiasi utente restrizioni”. In seguito a questa informazione viene suggerita una soluzione, quale re-installare il software, verificandone l'integrità e scaricarlo.

## VNC SERVER vulnerability

**Vulnerabilities** 66

**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	192.168.178.28 <a href="#">🔗</a>

La seconda vulnerabilità critica riguarda la password della macchina vulnerabile, in modo particolare la password base per quanto riguarda la sicurezza del VNC Server (Virtual Network Computing), la quale è stata facilmente bypassata dal software Nessus senza alcun problema. Come soluzione sarebbe opportuno cambiare la password in una molto più efficace.

# APACHE Tomcat AJP

## 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.

### See Also

<http://www.nessus.org/u?8ebe6246>  
<http://www.nessus.org/u?4e287adb>  
<http://www.nessus.org/u?cbc3d54e>  
<https://access.redhat.com/security/cve/CVE-2020-1745>  
<https://access.redhat.com/solutions/4851251>  
<http://www.nessus.org/u?dd218234>  
<http://www.nessus.org/u?dd772531>  
<http://www.nessus.org/u?2a01d6bf>  
<http://www.nessus.org/u?3b5af27e>  
<http://www.nessus.org/u?9dab109f>  
<http://www.nessus.org/u?5eafc70>

### Output

Nessus was able to exploit the issue using the following request :

```
0x0000: 02 02 00 08 48 54 54 50 2F 31 2E 31 00 00 0F 2F    ....HTTP/1.1.../
0x0010: 61 73 64 66 2F 78 78 78 78 78 2E 6A 73 70 00 00    asdf/xxxxx.jsp..
0x0020: 09 6C 6F 63 61 6C 68 6F 73 74 00 FF FF 00 09 6C    .localhost.....l
0x0030: 6F 63 61 6C 68 6F 73 74 00 00 50 00 00 09 A0 06    ocalhost..P.....
0x0040: 00 0A 6B 65 65 70 2D 61 6C 69 76 65 00 00 0F 41    ..keep-alive...A
0x0050: 63 63 65 70 74 2D 4C 61 6E 67 75 61 67 65 00 00    ccept-Language..
0x0060: 0F 6F 6F 2D 5F 53 2F 6F 6F 73 73 73 73 73 00    asdf/xxxxx.jsp..
more...
```

La terza vulnerabilità critica trovata riguarda Apache. Nessus ci dice che è presente un file read/inclusion nel connettore AJP, un protocollo binario che può inoltrare richieste in entrata da un server Web a un server delle applicazioni che si trova dietro il server Web. Ci dice inoltre che un attaccante senza shell privilegiata potrebbe utilizzarlo per poter leggere i file dell'applicazione web da un server vulnerabile, oppure, in caso sia consentito l'upload dei file, di caricare pagine malevole con lo scopo di inserire codice malevolo ed ottenere l'RCE remote code execution. Nei link sotto riportati sono elencate tutte le vulnerabilità delle varie versioni con le possibili soluzioni per mitigare il problema.

Inseguito come soluzione ci viene proposto di fare un update alla configurazione del protocollo AJP in modo che sia accessibile solo a chi abbia l'autorizzazione e/o di aggiornare il server Tomcat alle versioni più recenti.

# SSL v2/3 e Protocol Detection

## **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.

### **See Also**

<https://www.schneier.com/academic/paperfiles/paper-ssl.pdf>  
<http://www.nessus.org/u?b06c7e95>  
<http://www.nessus.org/u?247c4540>  
<https://www.openssl.org/~bodo/ssl-poodle.pdf>  
<http://www.nessus.org/u?5d15ba70>  
<https://www.imperialviolet.org/2014/10/14/poodle.html>  
<https://tools.ietf.org/html/rfc7507>  
<https://tools.ietf.org/html/rfc7568>

Come quarta vulnerabilità analizzata, avremo due versioni di SSL, una tipologia di crittografia, spiegando che il servizio di accesso remoto utilizza delle versioni di quest'ultima che peccano di cryptographic flaws, ovvero hanno delle screpolature nella crittografia utilizzata. A causa di queste screpolature un possibile man in the middle potrebbe sniffare i dati decriptando eventuali comunicazioni in atto. Le versioni di SSL e TLS vengono solitamente "scelte" alla versione più aggiornata, ma solo se supportate dal client o dal server, in caso contrario verrà utilizzata la versione precedente. Come soluzione, siccome le nuove versioni possono non essere supportate, ci viene suggerito di disabilitare le due versioni di SSL, tramite un procedimento documentato dai link forniti dal software, ed utilizzare TLS 1.2 o +.

# Bind Shell Backdoor

Vulnerabilities 66

## 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 -----
```

To see debug logs, please visit individual host

Port ▲

Hosts

1524 / tcp / wild_shell	192.168.178.28	🔗
-------------------------	----------------	---

Come quinta vulnerabilità è stato rilevata una shell in ascolto su una porta in remoto, senza alcuna autorizzazione. Potrebbe essere sfruttata per inviare direttamente comandi sulla macchina vulnerabile, ragion per cui ci viene suggerito di verificare se l'host remoto sia stato compromesso, e se necessario, re installare il sistema.