

## Vulnerability scanner: Nessus

Lo studente effettuerà un Vulnerability Scanning sulla macchina Metasploitable utilizzando Nessus. Questo esercizio ha lo scopo di fare pratica con lo strumento Nessus, la configurazione delle scansioni, e di familiarizzare con alcune delle vulnerabilità note.

Tramite l' utilizzo del vulnerability scanner Nessus, viene avviata una scansione su applicazioni, dispositivi e reti per individuare vulnerabilità sull' obiettivo prestabilito.

In questo caso, si procederà con l' avvio di una scansione con il plug in "*basic network scan*", fornendo l' indirizzo ip della macchina metasploitable. Al termine della scansione, nell' immagine sottostante sono rappresentate le vulnerabilità rilevate e ordinate in base alla criticità, dalla più alta alla più bassa.

The screenshot displays the Nessus interface for a scan on metasploitable2 (192.168.1.90). The main table lists 67 vulnerabilities, sorted by severity. The right sidebar shows host details and a vulnerability distribution chart.

Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6988	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1
HIGH	7.5			NFS Shares World Readable	RPC	1
MIXED	...	...	...	SSL (Multiple Issues)	General	28
MIXED	...	...	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5			TLS Version 1.0 Protocol Detection	Service detection	2

**Host Details:**  
IP: 192.168.1.90  
MAC: 08:00:27:4A:84:8E  
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)  
Start: Today at 9:36 AM  
End: Today at 9:46 AM  
Elapsed: 9 minutes  
KB: [Download](#)

**Vulnerabilities:**  
Critical: 1  
High: 4  
Medium: 2  
Low: 0  
Info: 0

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Sulla base di questo elenco, ne verranno analizzate alcune.

## 1° Vulnerabilità

La prima da analizzare è una backdoor. Essa consente un accesso non autorizzato all'attaccante su un dispositivo, all'insaputa dell'utente. Questo permette il controllo del dispositivo da remoto. E' stata trovata sulla porta 1524.

La soluzione proposta da Nessus, è di reinstallare il sistema.

**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	192.168.1.90 <a href="#">🔗</a>

## 2° Vulnerabilità

La seconda è sempre una backdoor ed è stata trovata sulla porta 6697. Questa backdoor permette all'attaccante di eseguire del codice sulla macchina host.

La soluzione proposta da Nessus, è di scaricare di nuovo il software e, prima di installarlo, fare un controllo dell'integrità del software attraverso algoritmi di hashing (MD5/SHA1).

metasploitable2 / Plugin #46882

[← Back to Vulnerabilities](#)

Vulnerabilities 67

**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
6697 / tcp / irc	192.168.1.90 <a href="#">🔗</a>

### 3° Vulnerabilità

La terza vulnerabilità riguarda una vecchia versione (2.0/3.0) del protocollo di cifratura SSL. La versione utilizzata dalla macchina è affetta da importanti difetti di crittografia che consente di eseguire un attacco *man-in-the-middle*. E' stata trovata sulla porta 25. La soluzione proposta da Nessus, è di disabilitare queste versioni di SSL e di passare all' utilizzo del protocollo di cifratura TLS.

metasploitable2 / Plugin #20007

[← Back to Vulnerabilities](#)

Vulnerabilities 67

**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.

## 4° Vulnerabilità

La quarta vulnerabilità riguarda l' uso di una password troppo debole da parte dell' utente. Un attaccante può accedere al dispositivo, in modo anche autenticato, attraverso il server VNC, exploitando la debolezza della password. E' stata trovata sulla porta 5900. La soluzione proposta da Nessus, è l' uso di una password forte.

metasploitable2 / Plugin #61708 <https://www.exploit-db.com/>

[Back to Vulnerabilities](#)

Vulnerabilities 67

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	192.168.1.90 <a href="#">🔗</a>

## 5° Vulnerabilità

La quinta vulnerabilità riguarda una versione obsoleta del protocollo SAMBA. Questa versione è affetta da un errore che permette all' attaccante, attraverso il *M/ITM*, di passare ad un livello di autenticazione più debole, in modo da poter ottenere permessi per vedere o modificare dati sensibili. E' stata trovata sulla porta 445.

La soluzione proposta da Nessus, è l' utilizzo di versioni più recenti del protocollo SAMBA.

metasploitable2 / Plugin #90509

[Back to Vulnerabilities](#)

Vulnerabilities 67

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.

**See Also**

<http://badlock.org>  
<https://www.samba.org/samba/security/CVE-2016-2118.html>

**Output**

```
Nessus detected that the Samba Badlock patch has not been applied.
```

To see debug logs, please visit individual host

Port ▲	Hosts
445 / tcp / cifs	192.168.1.90 