

# S5-L3

*Vulnerability scanning with  
Nessus on Meta2*

Presented By:  
**Mattia Di Donato**



# TRACCIA:

Si richiede una scansione tramite l'utilizzo di Nessus di un sistema operativo (abbiamo utilizzato per questa evenienza metasploitable2).

si fornirà poi un report di n.5 vulnerabilità trovate e su come risolverle al meglio.

**1**

**Ambiente Nessus  
dopo scansione**

**2**

**Vulnerabilità  
trovate**

**3**

**Conclusioni**

# 1. AMBIENTE NESSUS DOPO SCANSIONE

The screenshot displays the Nessus Essentials web interface in a browser window. The address bar shows the URL `https://localhost:8834/#/scans/reports/5/hosts/2/vulnerabilities`. The interface includes a sidebar with navigation options like 'My Scans', 'All Scans', 'Trash', 'Policies', 'Plugin Rules', and 'Terrascan'. The main content area shows the scan results for host 'Metasploitable2 / 192.168.0.235'. A table lists 66 vulnerabilities, with columns for severity, CVSS, VPR, EPSS, family, and count. A 'Host Details' panel on the right provides information about the host, including its IP, MAC, OS, and scan duration. A donut chart at the bottom right visualizes the distribution of vulnerability severities.

**Vulnerabilities** 66

Filter Search Vulnerabilities 66 Vulnerabilities

Sev	CVSS	VPR	EPSS	Family	Count
CRITICAL	10.0 *	7.4	0.6988	Backdoors	1
CRITICAL	10.0 *			Gain a shell remotely	1
CRITICAL	9.8			Service detection	2
CRITICAL	9.8			Backdoors	1
MIXED	...	...	...	Web Servers	4
CRITICAL	...	...	...	Gain a shell remotely	3
HIGH	7.5	5.9	0.0358	General	1
HIGH	7.5 *	5.9	0.015	Service detection	1

**Host Details**

- IP: 192.168.0.235
- MAC: 2A:7A:7E:36:B7:80
- OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
- Start: Today at 1:07 PM
- End: Today at 1:33 PM
- Elapsed: 25 minutes
- Download

**Vulnerabilities**

- Critical
- High
- Medium
- Low
- Info



# 2.1 VULNERABILITÀ TROVATE

Da una prima rilevazione abbiamo potuto constatare una vulnerabilità della porta 6667 che è usata per il protocollo IRC (internet relay chat) la quale viene utilizzata per la comunicazione in tempo reale tra più utenti in una chatroom

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

192.168.0.235



## 2.2 VULNERABILITÀ TROVATE

Da una seconda rilevazione abbiamo potuto constatare una vulnerabilità della porta 5900 che è usata per il protocollo VNC (virtual network computing) la quale consente il controllo remoto di un computer. È una porta esposta a diversi rischi di sicurezza, soprattutto se non configurata e protetta adeguatamente.

**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	192.168.0.235

## 2.3 VULNERABILITÀ TROVATE

Da una terza rilevazione abbiamo potuto constatare una vulnerabilità della porta 445 che è usata per il protocollo SMB (server message Block) che consente la condivisione di file, stampanti e altre risorse su reti Windows.

**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	192.168.0.235 



## 2.4 VULNERABILITÀ TROVATE

Da una quarta rilevazione abbiamo potuto constatare una vulnerabilità della porta 23 che è usata per il protocollo telnet che consente l'accesso remoto a dispositivi e server. Tuttavia, Telnet è noto per essere insicuro, poiché trasmette dati, inclusi i dettagli di autenticazione, in chiaro senza crittografia

[illegible]

## 2.5 VULNERABILITÀ TROVATE

Da una quinta e ultima rilevazione abbiamo potuto constatare una vulnerabilità nelle porte 5432 e 25 che sono usate rispettivamente per i protocolli PostgreSQL e SMTP (simple mail transfer protocol). La prima è utilizzata per la gestione di database. È una porta target per attacchi quando il database è accessibile tramite Internet senza adeguate misure di sicurezza. La seconda è utilizzata principalmente per l'invio di e-mail. È una delle porte maggiormente bersagliate per attacchi legati allo spam e al phishing, oltre che per l'accesso non autorizzato.

### Description

The remote x509 certificate on the remote SSL server 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 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.

### See Also



<http://www.nessus.org/u?107f9bdc>

<http://www.nessus.org/u?f14f4224>

### Output

No output recorded.

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.0.235 
25 / tcp / smtp	192.168.0.235 



# 3. CONCLUSIONI

Per la risoluzione delle vulnerabilità fornite vi consigliamo di utilizzare le seguenti soluzioni:

**Porta 6667 (IRC):** Disabilitare la porte se non necessaria, limitare l'accesso al firewall, aggiornare software IRC, usare crittografia forte e crittografia TLS.

**Porta 5900 (VNC):** Usare password complesse, limitare l'accesso al firewall, utilizzare una VPN o SSH per crittografie, aggiornare il software VNC e monitorare le connessioni.

**Porta 445 (SMB):** Disabilitare SMBv2 o 3 e fare un upgrade, bloccare la porta su reti pubbliche, usare autenticazione forte, aggiornare il sistema operativo, abilitare TLS, e limitare l'accesso tramite firewall.

**Porta 23 (telnet):** Disabilitare Telnet e usare SSH, limitare l'accesso tramite firewall, usare VPN per l'accesso remoto, e aggiornare i dispositivi.

**Porta 5432 (PostgreSQL):** Limitare l'accesso tramite firewall, usare password complesse, abilitare SSL, aggiornare PostgreSQL, e monitorare i log di accesso.

**Porta 25 (SMTP):** Disabilitare open relay, abilitare STARTTLS, richiedere autenticazione, impostare limiti sulle connessioni, abilitare filtri anti-spam, e monitorare i log SMTP.

# THANK YOU

MATTIA DI DONATO