

## Nessus\_Essentials

entrando su Nessus Essentials, ho avviato una nuova scansione e utilizzando la scansione Base ho inserito i dati dell'indirizzo ip di metasploitable che dopo essere stato analizzato mi ha rivelato 9 criticità di cui 5 mostrate qui sotto:

Criticità numero 1:

**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	192.168.1.164

Come soluzione consiglia di disinstallare e reinstallare il software **“UnrealIRCd Backdoor Detection”** usando la versione pubblicata. (qui è stata lasciata anche una backdoor)

Criticità numero 2:

**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	192.168.1.164

Come soluzione consiglia di Modificare la Password di **“VNC Server 'password' Password”** usandone una più forte.

### Criticità numero 3:

**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.

Come soluzione consiglia di Disabilitare SSL 2.0 e 3.0 e di usare TLS 1.2.

### Criticità numero 4:

**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.

Come soluzione consiglia di verificare se l'host remoto è stato compromesso e in caso di manomissione di reinstallare direttamente tutto il sistema. qui è stata lasciata anche una Backdoor.

### Criticità numero 5:

**CRITICAL** Debian OpenSSH/OpenSSL Package Random Number Generator W... >

**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.

Come soluzione consiglia di Crittografare il materiale e rigenerare le chiavi SSH, SSL, OpenVPN, attenzione perchè si è deboli agli attacchi man in the middle.

Diego Petronaci