

Dopo la scansione ho trovato le seguenti vulnerabilità critiche.

Hosts	1	Vulnerabilities	71	Remediations	3	History	1
Filter	▼	Search Vulnerabilities	🔍	71 Vulnerabilities			
<input type="checkbox"/>	Sev	CVSS	VPR ▲	Name	Family	Count	⚙️
<input type="checkbox"/>	CRITICAL	10.0 *	5.9	NFS Exported Shar...	RPC	1	🕒 ✎
<input type="checkbox"/>	CRITICAL	10.0		Unix Operating Sys...	General	1	🕒 ✎
<input type="checkbox"/>	CRITICAL	10.0 *	7.4	UnrealIRCd Backdo...	Backdoors	1	🕒 ✎
<input type="checkbox"/>	CRITICAL	10.0 *		VNC Server 'passw...	Gain a shell remotely	1	🕒 ✎
<input type="checkbox"/>	CRITICAL	9.8		SSL Version 2 and ...	Service detection	2	🕒 ✎
<input type="checkbox"/>	CRITICAL	9.8		Bind Shell Backdoo...	Backdoors	1	🕒 ✎
<input type="checkbox"/>	HIGH	7.5		NFS Shares World ...	RPC	1	🕒 ✎

Prima vulnerabilità

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.

Il problema di questo servizio è la scarsa sicurezza della password del servizio VNC.

Così tramite il comando **vncpasswd** ho potuto cambiare la password per renderla più sicura.

```
msfadmin@metasploitable:~$ vncpasswd
Using password file /home/msfadmin/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:
msfadmin@metasploitable:~$
```

Seconda vulnerabilità

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.

Questa vulnerabilità viene dalla versione Unix non supportata. Ho aggiornato tramite i comandi:

sudo apt-get update e sudo apt-get upgrade

```
msfadmin@metasploitable:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

Scan Finale

■	CRITICAL	9.8	SSL Version 2 and 3 Protocol Detection	Service detection	2
■	CRITICAL	9.8	Bind Shell Backdoor Detection	Backdoors	1
■	CRITICAL	10.0 *	NFS Exported Share Information Disclosure	RPC	1
■	CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
■	CRITICAL	10.0 *	UnrealIRCd Backdoor Detection	Backdoors	1