

## INIZIO SCANSIONE

Nel seguente report, ho selezionato e riportato solamente le vulnerabilità che risolto, per un totale di 3 vulnerabilità

192.168.50.3	
11	6
24	8
134	
CRITICAL	HIGH
MEDIUM	LOW
INFO	
Scan Information	
Start time:	Sat Sep 2 14:29:42 2023
End time:	Sat Sep 2 14:49:33 2023
Host Information	
Netbios Name:	METASPLOITABLE
IP:	192.168.50.3
MAC Address:	08:00:27:BC:3B:1B
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Vulnerabilities	
51988 - Bind Shell Backdoor Detection	
Synopsis	
The remote host may have been compromised.	
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.	
Risk Factor	
Critical	
CVSS v3.0 Base Score	
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)	
CVSS v2.0 Base Score	
10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)	
Plugin Information	
Published: 2011/02/15, Modified: 2022/04/11	
Plugin Output	
tcp/1524/wild_shell	

```
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 -----
```

## 11356 - NFS Exported Share Information Disclosure

### Synopsis

It is possible to access NFS shares on the remote host.

### Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

### Solution

Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

### Risk Factor

Critical

### VPR Score

5.9

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### References

CVE	CVE-1999-0170
CVE	CVE-1999-0211
CVE	CVE-1999-0554

### Exploitable With

Metasploit (true)

### Plugin Information

Published: 2003/03/12, Modified: 2018/09/17

### Plugin Output

udp/2049/rpc-nfs

```
The following NFS shares could be mounted :
+ /
```

```
+ Contents of / :  
- .  
- ..  
- bin  
- boot  
- cdrom  
- dev  
- etc  
- home  
- initrd  
- initrd.img  
- lib  
- lost+found  
- media  
- mnt  
- nohup.out  
- opt  
- proc  
- root  
- sbin  
- srv  
- sys  
- tmp  
- usr  
- var  
- vmlinuz
```

## 61708 - VNC Server 'password' Password

### Synopsis

A VNC server running on the remote host is secured with a weak 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.

### Risk Factor

Critical

### CVSS v2.0 Base Score

10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)

### Plugin Information

Published: 2012/08/29, Modified: 2015/09/24

### Plugin Output

tcp/5900/vnc

Nessus logged in using a password of "password".