NFS Exported Share Information Disclosure [11356]
Sum-up: It is possible to access NFS (Network File System) shares on the remote host.
Solution: Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
Per risolvere questo problema ho editato il file exports dentro /etc/exports

```
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#

/       192.168.49.100(rw,sync,no_root_squash,no_subtree_check)
```

Errore 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.
Ho cambiato la password della vnc

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# cd..
bash: cd..: command not found
root@metasploitable:/home/msfadmin# cd ..
root@metasploitable:/home# cd ..
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# cd root
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
root@metasploitable:~# sudo vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:~#
```

BindShell Backdoor Detection [51988]
Sum-up: The remote host may have been compromised (tcp/1524/wild_shell).
Solution: Verify if the remote host has been compromised, and reinstall the system if necessary.
wild_shell is a renown malware that allows access to the infected machine without any credential, allowing the attacker to execute commands on the compromised systems.

Ho creato la tabella del firewall tramite il comando "iptables-save > fwrules" nella cartella /etc/init.d/.

Il sistema è stato messo sotto controlla dal firewall tramite il comando "sudo iptables -A INPUT -p tcp --dport 1524 -j DROP", e salvata la nuova regola nel file "fwrules" con il comando precedente.

Per forzare il caricamento della regola all'avvio, ho aggiunto il comando "iptables-restore < /etc/init.d/fwrules" al file "/etc/rc.local", che viene eseguito all'avvio del sistema.