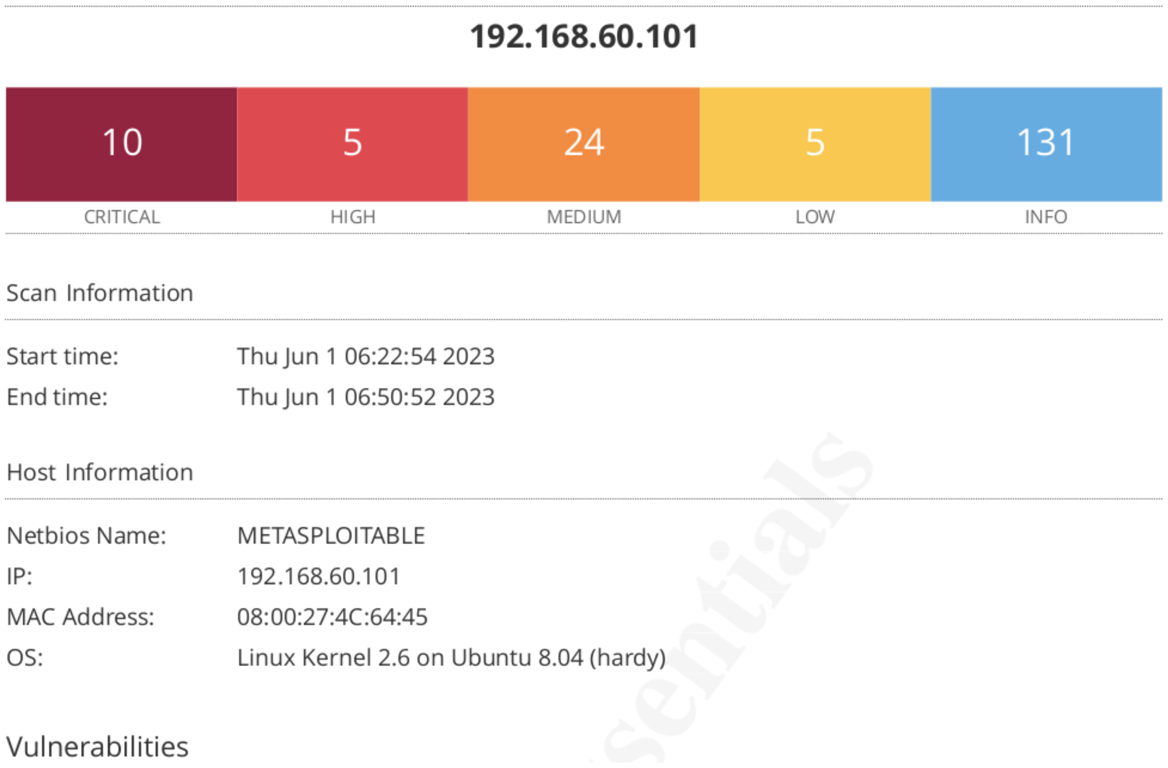
Scan con nessus 1



192.168.60.101

10	5	24	5	131
CRITICAL	HIGH	MEDIUM	LOW	INFO

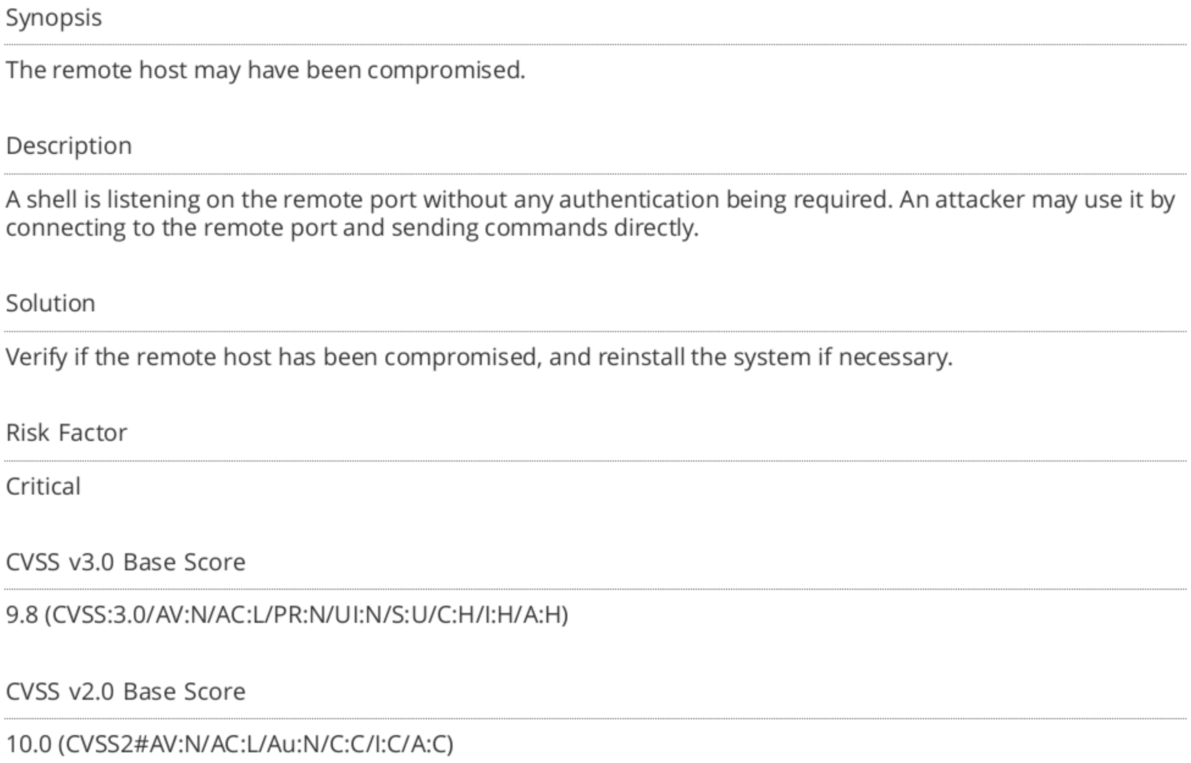
Scan Information

Start time:	Thu Jun 1 06:22:54 2023
End time:	Thu Jun 1 06:50:52 2023

Host Information

Netbios Name:	METASPLOITABLE
IP:	192.168.60.101
MAC Address:	08:00:27:4C:64:45
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)

Vulnerabilities



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)

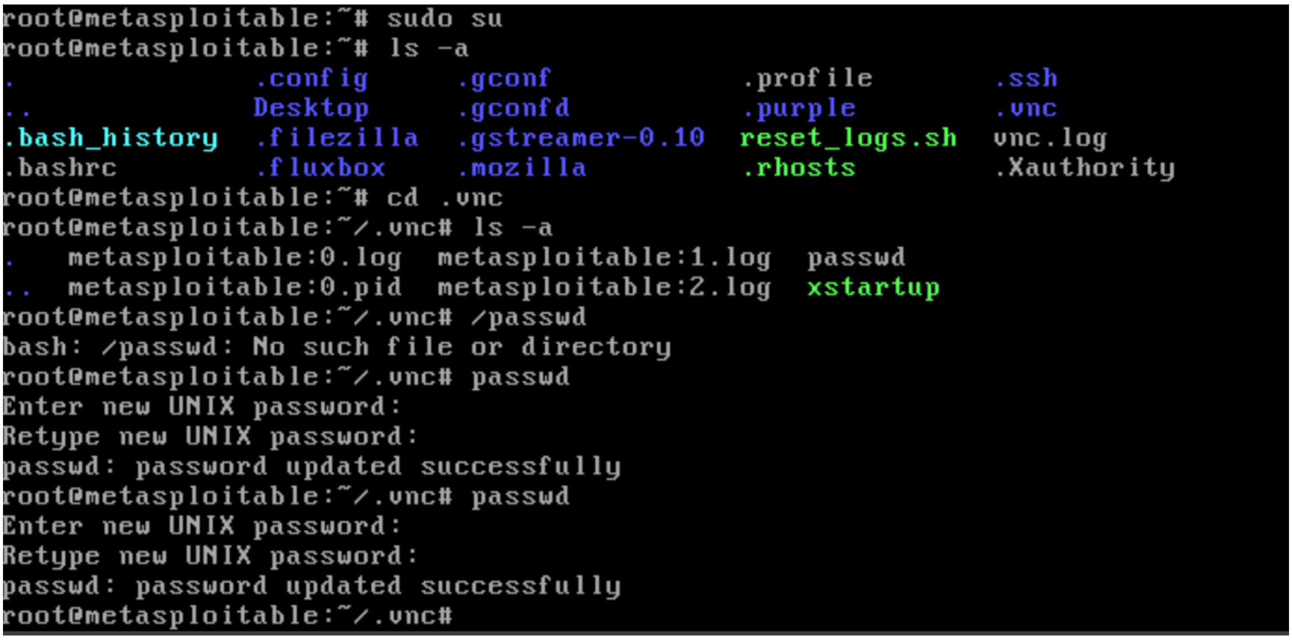
CVSS v2.0 Base Score

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

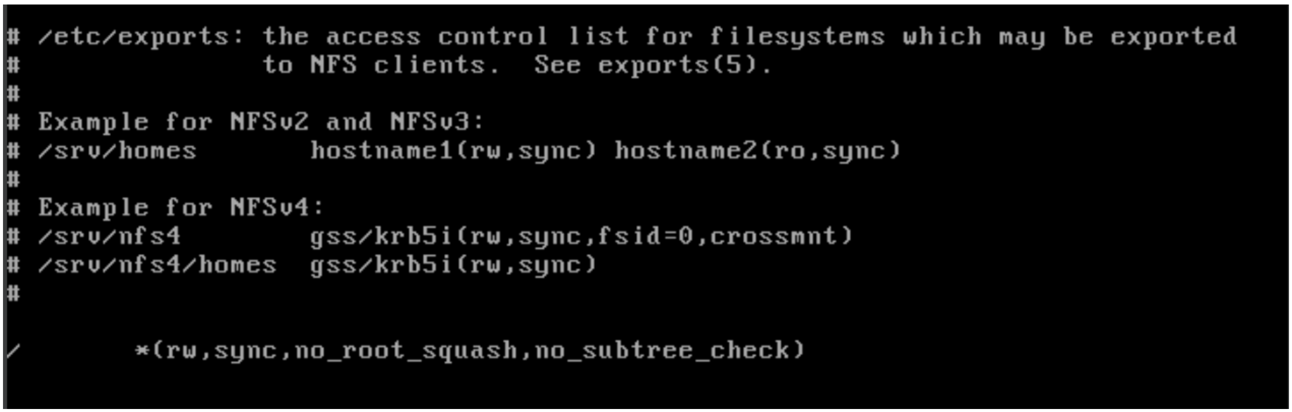
Risolusione vulnerabilità

VNC Server password

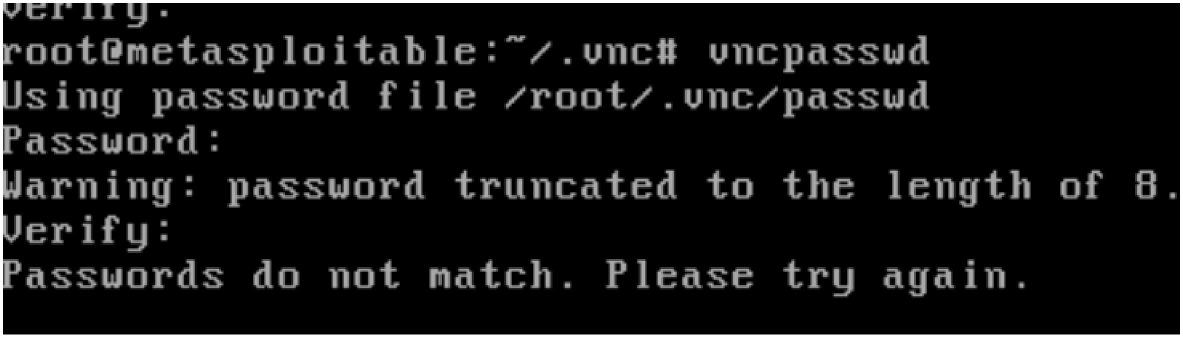
Ho cambiato la password in ottootto del server vnc



```
root@metasploitable:~# sudo su
root@metasploitable:~# ls -a
.               .config     .gconf           .profile       .ssh
..              Desktop     .gconfd          .purple        .vnc
.bash_history   .filezilla  .gstreamer-0.10  reset_logs.sh  vnc.log
.bashrc         .fluxbox    .mozilla         .rhosts        .Xauthority
root@metasploitable:~# cd .vnc
root@metasploitable:~/.vnc# ls -a
.   metasploitable:0.log  metasploitable:1.log  passwd
..  metasploitable:0.pid  metasploitable:2.log  xstartup
root@metasploitable:~/.vnc# /passwd
bash: /passwd: No such file or directory
root@metasploitable:~/.vnc# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:~/.vnc# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:~/.vnc#
```



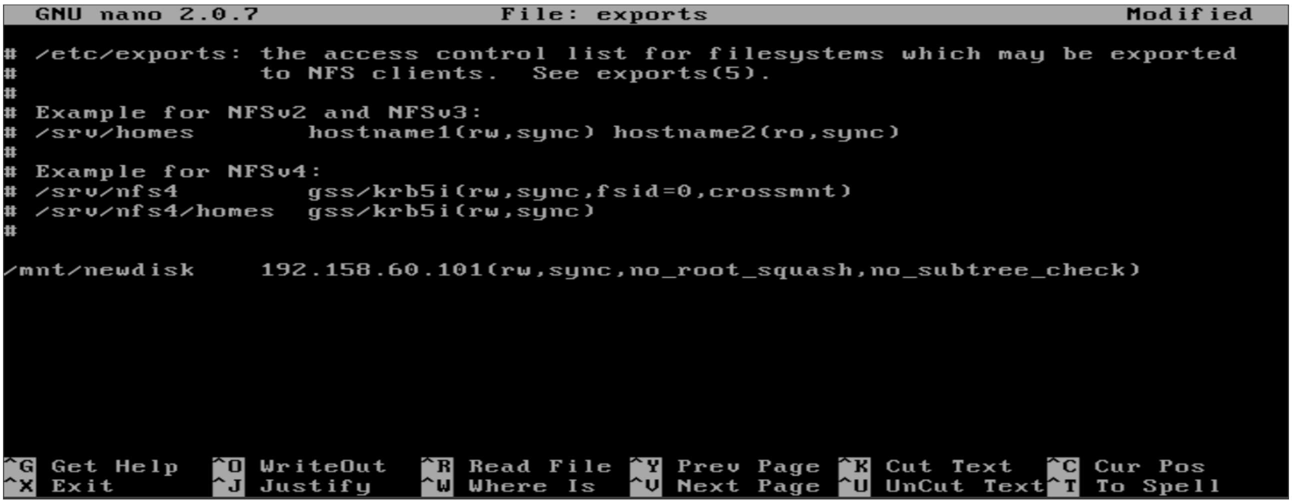
```
# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes       hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4        gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes  gss/krb5i(rw,sync)
#


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



```
Verify:
root@metasploitable:~/.vnc# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Passwords do not match. Please try again.
```

NFS Exported Share Information Disclosure

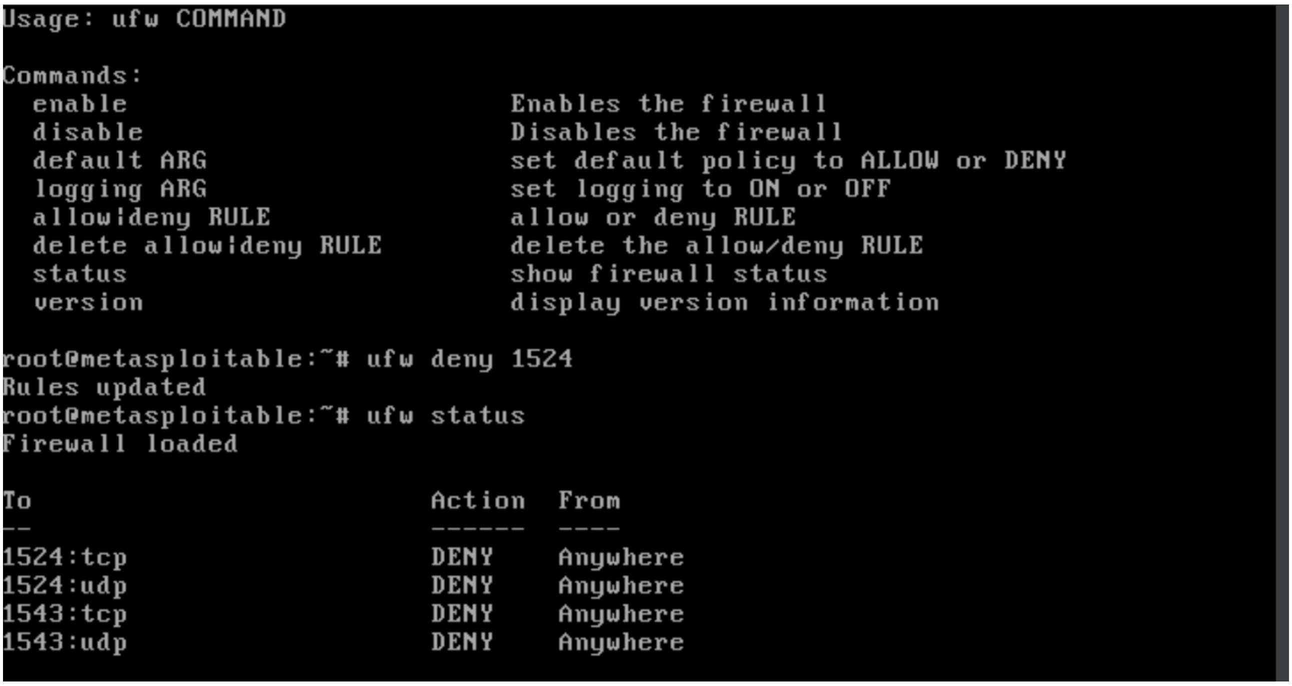
Copro le informazioni della machina



```
  GNU nano 2.0.7                File: exports                        Modified

# /etc/exports: the access control list for filesystems which may be exported
#               to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /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)
#

/mnt/newdisk     192.158.60.101(rw,sync,no_root_squash,no_subtree_check)
```

Bind Shell Backdoor Detection

Abilito il firewall di Mestasploitableet



```
Usage: ufw COMMAND

Commands:
  enable                          Enables the firewall
  disable                         Disables the firewall
  default ARG                     set default policy to ALLOW or DENY
  logging ARG                     set logging to ON or OFF
  allow|deny RULE                 allow or deny RULE
  delete allow|deny RULE          delete the allow/deny RULE
  status                          show firewall status
  version                         display version information

root@metasploitable:~# ufw deny 1524
Rules updated
root@metasploitable:~# ufw status
Firewall loaded

To                           Action  From
--                           ------  ----
1524:tcp                     DENY    Anywhere
1524:udp                     DENY    Anywhere
1543:tcp                     DENY    Anywhere
1543:udp                     DENY    Anywhere
```

Scan con nessus 2

Vulnerabilities

33850 - Unix Operating System Unsupported Version Detection

Synopsis

The operating system running on the remote host is no longer supported.

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.

Risk Factor

Critical

CVSS v3.0 Base Score

10.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/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)

References

XREF	IAVA:0001-A-0502
XREF	IAVA:0001-A-0648

Plugin Information

Published: 2008/08/08, Modified: 2023/05/18

Plugin Output

tcp/0