

Progetto settimanale

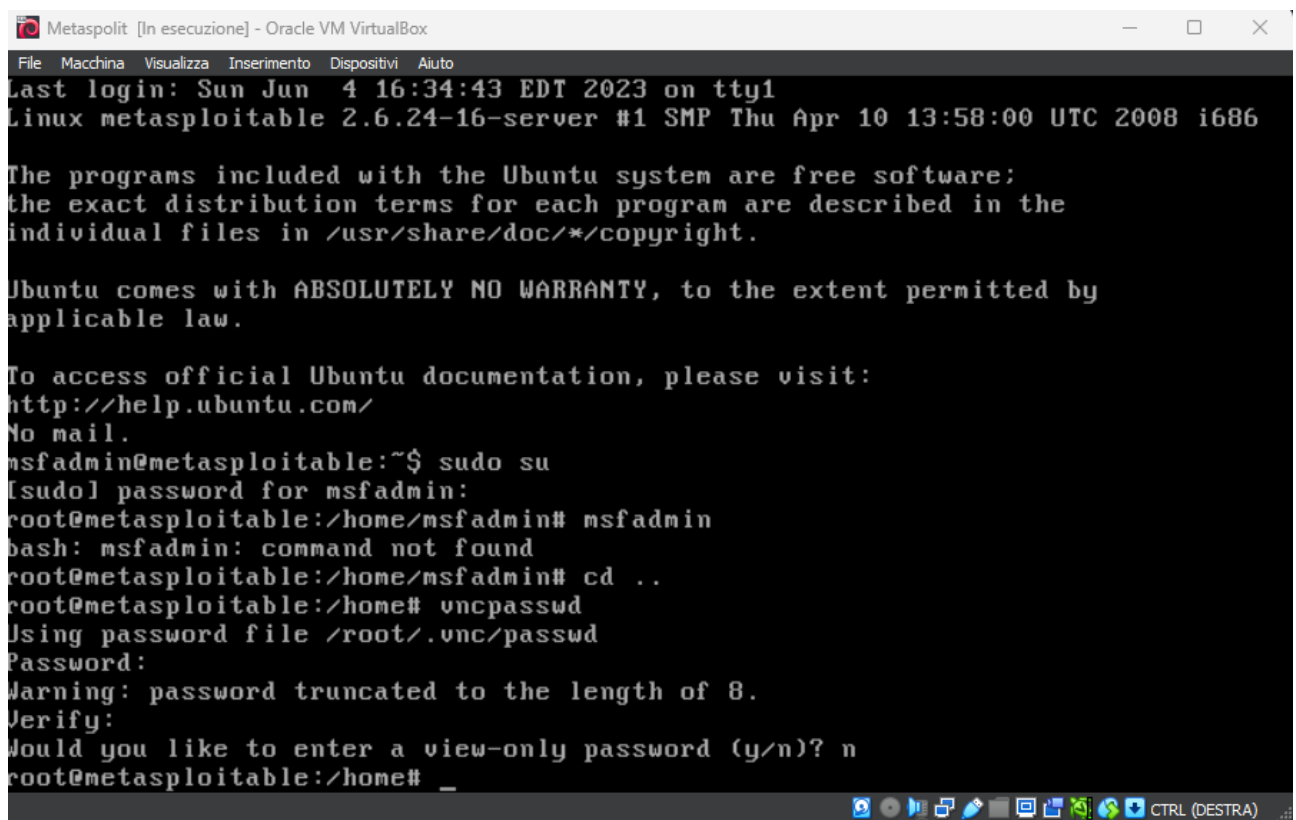
Gentile Prof,

In seguito all'analisi delle vulnerabilità presenti in diversi **aspetti di sicurezza**, desidero presentarle un report dettagliato sulle vulnerabilità riscontrate e le relative soluzioni adottate.

VNC (Virtual Network Computing) - Vulnerabilità della password del server VNC

Descrizione: Il VNC è un sistema utilizzato per il controllo remoto di un computer, consentendo l'accesso e la visualizzazione dei dati presenti. La vulnerabilità riscontrata riguarda la debolezza della password predefinita del server VNC.

Soluzione: Per aggirare questa vulnerabilità, è stato necessario cambiare la password predefinita. La nuova password è stata impostata come "#81FDICrUpYtw" e include caratteri speciali, lettere e numeri. Per implementare questa soluzione, sono stati eseguiti i seguenti comandi:



```
Metasploit [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
Last login: Sun Jun  4 16:34:43 EDT 2023 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.

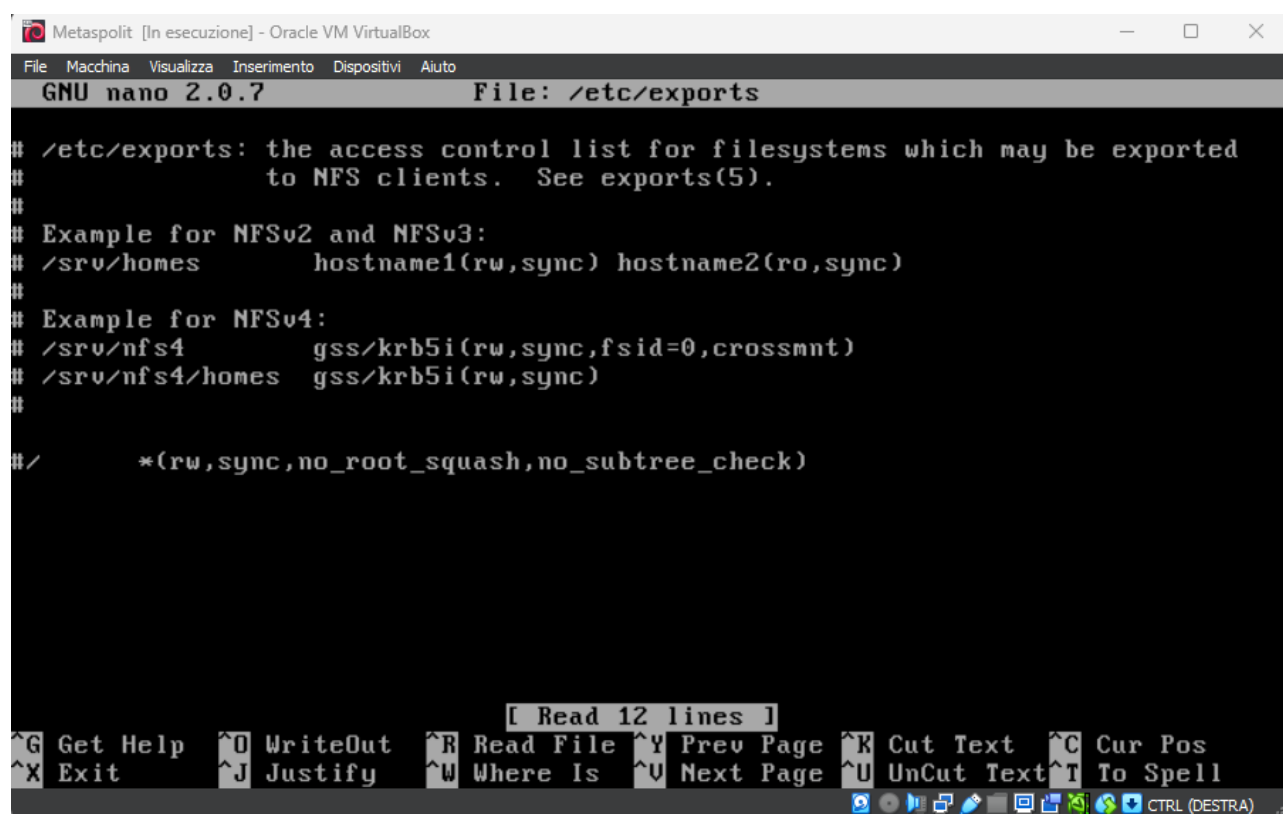
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# msfadmin
bash: msfadmin: command not found
root@metasploitable:/home/msfadmin# cd ..
root@metasploitable:/home# vncpasswd
Using password file /root/.vnc/passwd
Password:
Warning: password truncated to the length of 8.
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home#
```

NFS (Network File System) - Divulgazione delle informazioni condivise

Descrizione: Il protocollo NFS consente l'accesso e la condivisione di file tra sistemi.

Tuttavia, se le informazioni/file/directory condivisi non sono adeguatamente protetti, potrebbero essere vulnerabili ad attacchi hacker che potrebbero rubare dati sensibili, come nomi, indirizzi e dati aziendali.

Soluzione: Per evitare questa vulnerabilità, è stata apportata una modifica al file `/etc/exports` concedendo i permessi di root e aggiungendo il commento `"#"` come indicato nella foto allegata al report.



The screenshot shows a Metasploit terminal window titled "Metasploit [In esecuzione] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.0.7 text editor, editing the file `/etc/exports`. The content of the file is as follows:

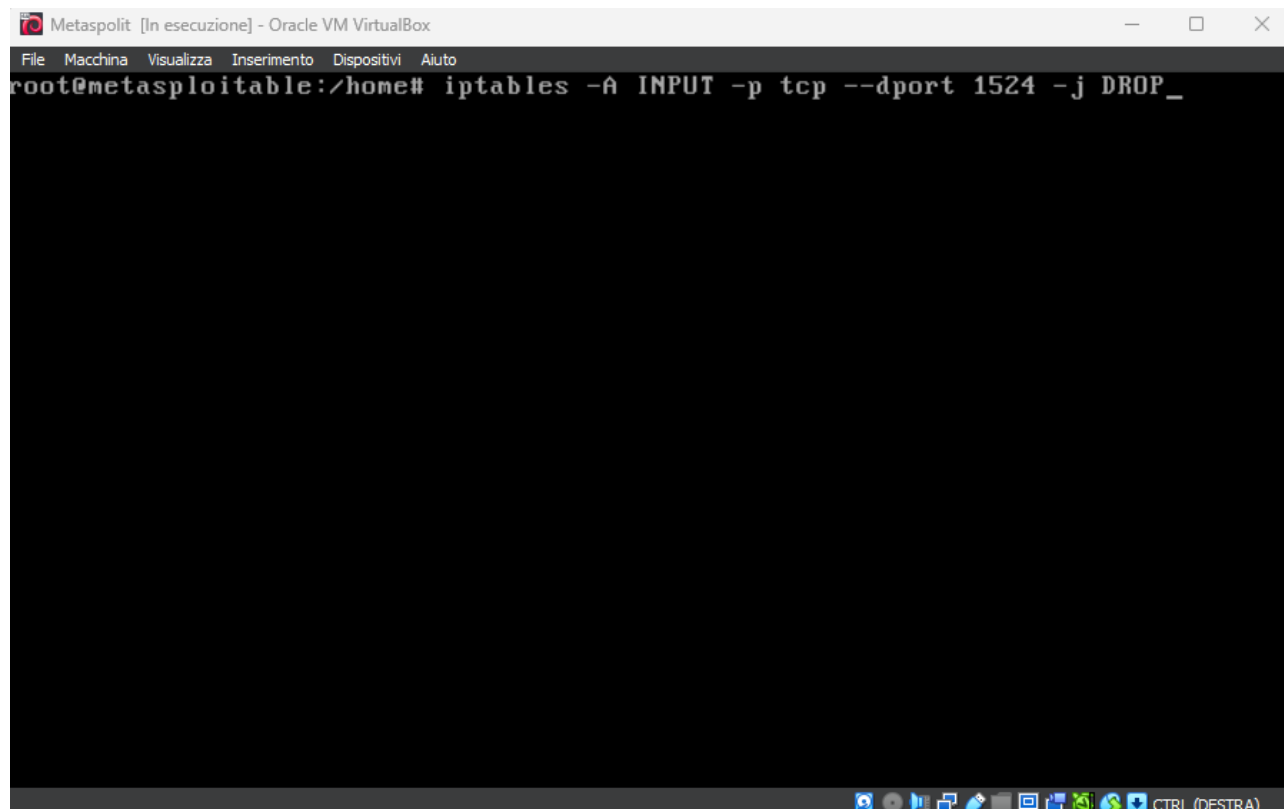
```
# /etc/exports: the access control list for filesystems which may be exported
# to NFS clients.  See exports(5).
#
# Example for NFSv2 and NFSv3:
# /srv/homes      hostname1(rw,sync) hostname2(ro,sync)
#
# Example for NFSv4:
# /srv/nfs4       gss/krb5i(rw,sync,fsid=0,crossmnt)
# /srv/nfs4/homes gss/krb5i(rw,sync)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

At the bottom of the terminal, there is a status bar with various keyboard shortcuts: `^G Get Help`, `^O WriteOut`, `^R Read File`, `^Y Prev Page`, `^K Cut Text`, `^C Cur Pos`, `^X Exit`, `^J Justify`, `^W Where Is`, `^V Next Page`, `^U UnCut Text`, `^T To Spell`. A message `[Read 12 lines]` is also visible above the shortcuts.

Bind Shell Backdoor Detection (porta 1524)

Descrizione: Si tratta di una vulnerabilità associata a una backdoor di tipo bind shell, che consente a un attaccante di accedere a un dispositivo, come un computer o un cellulare, aggirando i sistemi di protezione.

Soluzione: Per risolvere questa vulnerabilità, è stata aggiunta la seguente linea di comando per bloccare il traffico sulla porta 1524:



```
Metasploit [In esecuzione] - Oracle VM VirtualBox
File  Macchina  Visualizza  Inserimento  Dispositivi  Aiuto
root@metasploitable:/home# iptables -A INPUT -p tcp --dport 1524 -j DROP_
```

Questa regola permette di **impedire** il traffico proveniente dall'indirizzo IP specificato verso la **porta 1524**.

Analisi del servizio tramite Nmap

Descrizione: Durante l'analisi di sicurezza, è stato eseguito un comando Nmap per identificare i servizi in esecuzione sull'indirizzo IP 192.168.50.101.

Di seguito è riportato il risultato dell'analisi:

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.50.101
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-04 13:23 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

Comando eseguito:

```
sudo nmap -sS 192.168.50.101
```

Risultato dell'analisi:

```
Starting Nmap 7.93 (https://nmap.org) at 2023-06-04 13:23 EDT
Nmap scan report for 192.168.50.101
Host is up (0.0016s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    filtered ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
```

Spiegazione: Il comando Nmap eseguito ha scansionato l'indirizzo IP 192.168.50.101 per determinare lo stato dei servizi aperti su tale host.

Di seguito sono elencati i servizi identificati con i rispettivi stati:

Porta 21/tcp: Aperta - servizio FTP.

Porta 22/tcp: Filtrata - servizio SSH.

Porta 23/tcp: Aperta - servizio Telnet.

Porta 25/tcp: Aperta - servizio SMTP (Simple Mail Transfer Protocol).

Porta 53/tcp: Aperta - servizio DNS (Domain Name System).

Porta 80/tcp: Aperta - servizio HTTP.

Porta 111/tcp: Aperta - servizio RPCBIND (Remote Procedure Call Bindings).

Porta 139/tcp: Aperta - servizio NetBIOS-SSN (NetBIOS Session Service).

Porta 445/tcp: Aperta - servizio Microsoft-DS (Microsoft Directory Services).

L'esecuzione del comando Nmap consente di ottenere informazioni sullo stato dei servizi, aiutando a identificare eventuali vulnerabilità o esposizioni potenziali.

Conclusione:

Sulla base delle informazioni fornite riguardanti le vulnerabilità identificate e le relative soluzioni adottate, è possibile trarre le seguenti conclusioni:

VNC Server Password: La vulnerabilità relativa alla password predefinita del server VNC è stata risolta mediante l'implementazione di una password complessa e sicura.

NSF Exported Share Information Disclosure: Per mitigare la divulgazione non autorizzata delle informazioni condivise tramite il protocollo NFS, sono state apportate modifiche ai permessi di root e sono stati aggiunti commenti appropriati nel file di configurazione.

Bind Shell Backdoor Detection (Porta 1524): La vulnerabilità associata a una backdoor di tipo bind shell è stata affrontata mediante l'aggiunta di una regola di blocco del traffico sulla porta 1524.

Debian OpenSSL Package Random Number Generator Weakness: Questa vulnerabilità non è stata trattata direttamente nel report fornito. Si consiglia di adottare le misure di sicurezza appropriate, come l'aggiornamento del pacchetto OpenSSL a una versione più recente, per mitigare tale vulnerabilità.

Inoltre, l'analisi dei servizi tramite il comando Nmap ha fornito un'istantanea dello stato dei servizi sull'indirizzo IP specificato. È importante monitorare costantemente tali servizi e prendere le misure necessarie per garantire la sicurezza e la protezione dei dati.

Complessivamente, il report sottolinea l'importanza di adottare misure preventive solide per garantire la sicurezza delle reti e dei sistemi. È consigliabile continuare a monitorare e valutare regolarmente le vulnerabilità, adottare pratiche di sicurezza solide e rimanere aggiornati sulle ultime patch e correzioni di sicurezza.