VNC SERVER “PASSWORD” PASSWORD

Ricordiamo quanto sia importante utilizzare password sicure per qualsiasi tipo di accesso, in questo caso al server VNC (ovvero Virtual Network Computing). Per ovviare a questo è sufficiente cambiare password con una più sicura. Per fare ciò lanciamo il seguente comando dalla console di Metasploitable:

vncpasswd

Da qui si avvia una semplice procedura di cambio password. Il programma non ha molti vincoli se non quello di lunghezza, quindi sta a noi utilizzare una password sicura, possiamo generarla con generatori pseudocasuali (vedi report precedenti su password sicure).

NFS Exported Share Information Disclosure

Tale criticità viene dal fatto che il Network File System di Linux in Metasploitable accetta ogni tipo di richiesta da qualsiasi ip si colleghi a tale servizio. Andiamo subito a verificare i permessi concessi da tale servizio utilizzando il comando:

sudo nano etc/exports

Così si apre tale file di configurazione:

```
  GNU nano 2.0.7                File: /etc/exports

# /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)
```

Come possiamo vedere ogni IP (*) ha permesso RW (read e write) e quindi può scrivere e leggere qualsiasi file.

Ci sono molte soluzioni a tale problema, personalmente ritengo che spegnere tale servizio di sharing sia la più completa per cercare di mitigare il problema.

1. Utilizziamo il comando:
    a. *ps -A*
    b. per vedere tutti i processi attivi e prendiamo nota di quelli che hanno come descrizione il nome del servizio interessato. Infine utilizziamo il comando
    c. *sudo killall <PID_DEL_PROCESSO>*
    d. per terminare tali processi.
2. Modificare le regole dal file citato sopra per esempio mettendo come permesso read only (ro).
3. Impostiamo un firewall con iptables:
    a. Per fare ciò è sufficiente aggiungere una regola digitado il comando:
    b. *sudo iptables -I FORWARD -p UDP -s 192.168.50.100 –dport 2049 -j DROP*

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 2049 -A 192.168.50.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-25 10:25 EST

┌──(kali㉿kali)-[~]
└─$
```

Bind Shell Backdoor Detection

Non sono riuscito a trovare nessun metodo alternativo a quello di impostare un firewall con iptables usando il comando:

sudo iptables -I FORWARD -p TCP -s 192.168.50.100 –dport 1524 -j REJECT