Alaimo Alessandro
25/11/2022

Remedetion Meta

Prendiamo in esame 4 degli rischi critici che abbiamo scansionato ed andiamo a risolverli nel seguente modo.

1) 10203 - rexecd Service Detection

Seguendo la risoluzione di Nessus, andiamoa commentare la stringa seguente per risolvere il rischio:

```
  GNU nano 2.0.7            File: /etc/inetd.conf

#<off># netbios-ssn     stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb
telnet          stream  tcp     nowait  telnetd /usr/sbin/tcpd  /usr/sbin/in.te
#<off># ftp             stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sb
tftp            dgram   udp     wait    nobody  /usr/sbin/tcpd  /usr/sbin/in.tf
shell           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rs
login           stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.rl
#exec            stream  tcp     nowait  root    /usr/sbin/tcpd  /usr/sbin/in.re
ingreslock stream tcp nowait root /bin/bash bash -i
```

2) 11356 - NFS Exported Share Information Disclosure

Seguendo la risoluzione di Nessus, andiamo ad impostare l'IP di Metasploit nel seguente campo:

```
  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)
#

/       192.168.50.101(rw,sync,no_root_squash,no_subtree_check)
```

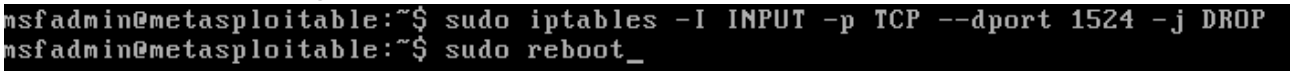
3) 61708 - VNC Server 'password' Password

Seguendo la risoluzione di Nessus, andiamo a cambiare la password per andare ad impostarne una più forte, nel mio caso "kU#@mj3u", nel seguente modo:

```
msfadmin@metasploitable:~$ sudo su
[sudo] password for msfadmin:
root@metasploitable:/home/msfadmin# loadkeys it
Loading /usr/share/keymaps/it.map.bz2
root@metasploitable:/home/msfadmin# vncpasswd
Using password file /root/.vnc/passwd
Password:
Verify:
Would you like to enter a view-only password (y/n)? n
root@metasploitable:/home/msfadmin#
```

4) 51988 - Bind Shell Backdoor Detection

Per la risoluzione di questo rischio, sono andato ad impostare una regola nel firewall nel seguente modo:



N.B: Usando il firewall IPTABLES, ad ogni riavvio, si resetterà la regola impostata poiché temporanea, ergo dovrà essere inserita nuovamente