REPORT REMEDIATION_META

FRANCESCO PERSICHETTI

51988 - Bind Shell Backdoor Detection

Per ovviare al problema della backdoor è bastato aggiungere una regola sul firewall della macchina Metasploitable. Il comando utilizzato è il seguente “sudo iptables -I INPUT -p tcp -s IPKALI --dport 1524 -j DROP” dove “iptables” è il firewall di metasploitable, “INPUT” è per indicare dove bloccare i pacchetti (in questo caso in entrata), “-p” per indicare il tipo di protocollo da bloccare (in questo caso TCP), “-s” per indicare la sorgente da cui arriva il pacchetto (in questo caso dall’indirizzo della macchina kali 192.168.50.100) e “DROP” che serve a scartare il pacchetto

```
msfadmin@metasploitable:~$ sudo iptables -I INPUT -p tcp -s 192.168.50.100 --dpo
rt 1524 -j DROP
msfadmin@metasploitable:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  192.168.50.100       anywhere            tcp dpt:ingreslock

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
msfadmin@metasploitable:~$ _
```

11356 - NFS Exported Share Information Disclosure

Per risolvere il problema del NFS siamo andati dentro il file “etc/exports” per cambiare l’indirizzo IP dell’host autorizzato a modificare le condivisioni. Nel nostro caso abbiamo inserito l’IP di Metasploitable (evidenziato in rosso)

```
  GNU nano 2.0.7             File: /etc/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)
#

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

61708 - VNC Server 'password' Password

Il problema che dava questa vulnerabilità era riscontrare una password troppo debole a difesa del sistema. Passando in “root” con il comando “sudo su”, digitiamo il comando “vncpasswd” per impostare una password più forte di quella di default, mantenendoci entro gli 8 caratteri come richiesto da Metasploitable (nel caso la password scelta fosse più lunga il sistema la troncherebbe comunque a 8 caratteri)