S5 L4

Effettuare un Vulnerability Assessment con Nessus sulla macchina Metasploitable indicando come target solo le porte comuni.

A valle del completamento della scansione, analizzate attentamente il report per ognuna delle vulnerabilità riportate, approfondendo qualora necessario con i link all'interno dei report e/o con contenuto da Web.

Fare un report su 3 criticità a scelta di cui 2 critiche e 1 media

1

Bind Shell Backdoor Detection

Questa vulnerabilità riguarda una shell in ascolto su una determinata porta dove non è richiesta autenticazione, permettendo l'accesso non autorizzato anche a un criminale informatico.

Una possibile soluzione è chiudere la porta aperta se non utilizzata oppure implementare un'autenticazione sicura.

La porta in questione è la 1524 e tramite telnet è possibile accedervi e controllare il bersaglio target come screen di seguito:

1

```
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-11 14:50 CET
Nmap scan report for 192.168.50.101
Host is up (0.00075s latency).

PORT     STATE SERVICE
1524/tcp open  ingreslock
MAC Address: 08:00:27:23:71:C8 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 13.16 seconds

┌──(kali㉿kali)-[~]
└─$ telnet 192.168.50.101 1524
Trying 192.168.50.101 ...
Connected to 192.168.50.101.
Escape character is '^]'.
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:23:71:c8
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: 2002:9547:339f:0:a00:27ff:fe23:71c8/64 Scope:Global
          inet6 addr: fe80::a00:27ff:fe23:71c8/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3806 errors:0 dropped:0 overruns:0 frame:0
          TX packets:75 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:251232 (245.3 KB)  TX bytes:11164 (10.9 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:298 errors:0 dropped:0 overruns:0 frame:0
          TX packets:298 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:120469 (117.6 KB)  TX bytes:120469 (117.6 KB)

root@metasploitable:/# root@metasploitable:/# reboot
```

2

Apache Tomcat SEoL (<= 5.5.x)

In questo caso abbiamo una versione di Apache Tomcat obsoleta e non più supportata, questo espone il servizio a potenziali rischi.

Aggiornandola possiamo garantire più sicurezza perché potrebbero essere stati corretti i potenziali exploit.

3 HTTP TRACE / TRACK Methods Allowed

E’ stato identificato il metodo http TRACE abilitato, questo metodo è usato per finalità di debugging ma potrebbe essere sfruttato per finalità diverse.

Inviando una richiesta TRACE la risposta dal server riflette l'intera richiesta TRACE, incluso l'header "Host".

Questo può essere utilizzato dall'attaccante per ottenere informazioni sulla struttura del server, eventualmente rivelando dettagli sensibili.

Disabilitare questo metodo è consigliabile.