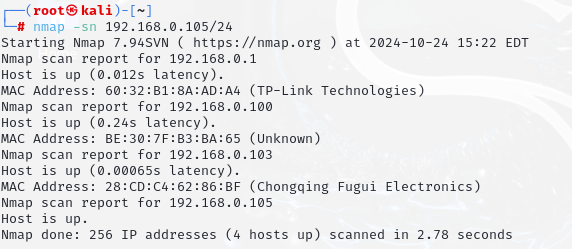
28.09.2024

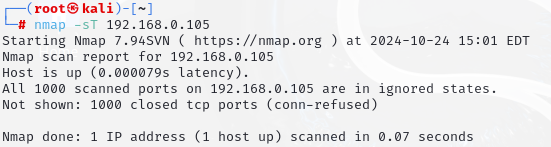
Discovery Scan

* sudo -i
* nmap -sn 192.168.0.105/24



Common scanning commands:

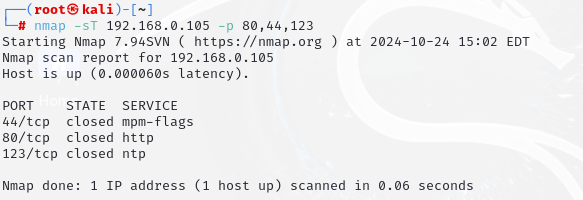
* nmap -sT 192.168.0.105(default TCP scan method)



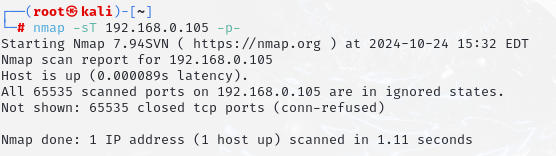
* nmap –sT 192.168.0.105 –p 80 (for single port)



* nmap –sT 192.168.0.105 –p 80,44,123



* nmap –sT 192.168.0.105 –p- (for scanning all port (65535 port))



* nmap –sU 192.168.0.105 –p 80 (for scanning UDP port)
* nmap 192.168.0.105 –p 80 –sv (show service version (is it latest or old version))
* nmap 192.168.0.105 –p 80 –sv -O (for show operating system details)

Nmap Scan Speed

* -T0-T5 (slow to fast search T1-T2..-T5)

Normally use T4

* nmap 192.168.10.100 –p 80 –sv -T4

Inverse Scan (For bypass firewall)

* First send reset (allow firewall)
* If port in open, there was no any response and vice versa
* Download : Metasploitable-3 (Windows 2008)
* ping 192.168.10.100
* If ttl value 64,63 this is linux
* If ttl value 128,127 this is windows
* nmap 192.168.10.198 (showing blocking our ping probes)
* 2 technique for bypass

–sX –xmass

–sX –Maimon scan

nmap 192.168.10.198 –sX –p 137,139,445 (if ip not work,create new ip on virtual box)