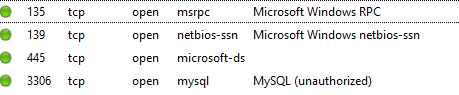
Activity VI : Recon and Defense (Network I)

Instructors : Kunwadee Sripanidkulchai, Ph.D.​

Q1. Notice the open ports. Does anything look suspicious, i.e., some ports that you are not aware of that are open on the VM or on your notebook?

Port that I’m not aware on Notebook: msrpc(135), microsift-ds(445), netbios\_ssn(139)

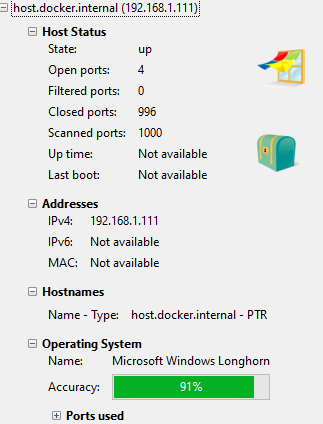


On VM the port opened is what I expected



Q2. Look at the information provided by nmap about your OS's. Is the information correct? Why is it or why is it not correct?

It’s correct

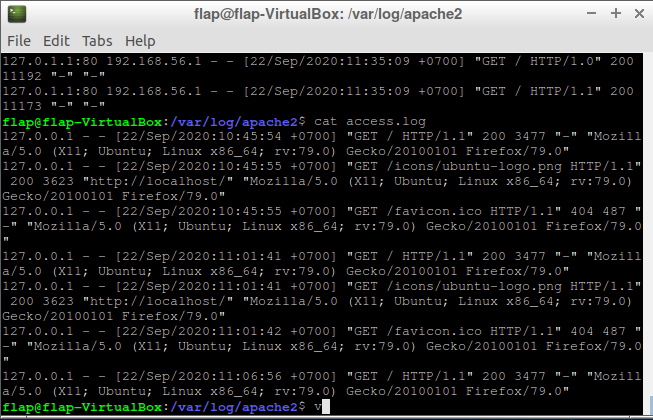


Q3. What do you think about the information you can get using nmap? Scary?

It knows I’ve docker but beside that it’s not scary yet maybe I’m not running many service that’s sensitive

Q4. Look at the access.log file for the web server in your Linux VM. What IP addresses do you see accessing the Web server? Who owns these IP addresses?

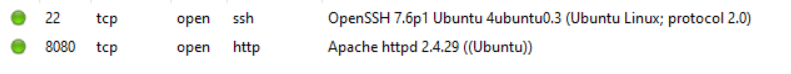
It’s from browser within VM



Q5. Find the nmap scan in the Web server log. Copy the lines from the log file that were created because of the nmap scan.

127.0.1.1:80 192.168.56.1 - - [22/Sep/2020:12:23:12 +0700] "GET / HTTP/1.1" 200 11173 "-" "-" 

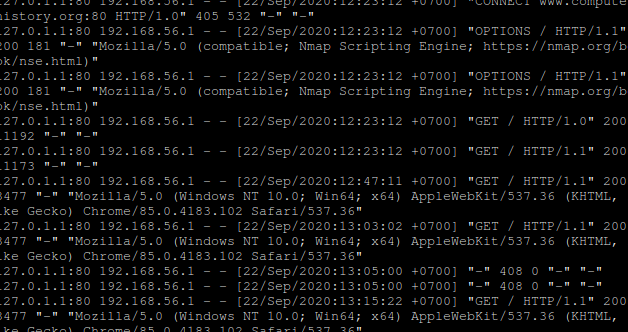
Q6. After you successfully install your iptable rule(s), how do the reported results from your new nmap scan compare to your previous scan before using iptables? Look to see if OS detection, port open results, etc. have changed. Something(s) have definitely changed.



Nothing change

Q7. Notice that nmap can still figure out you have Apache httpd running. Look at the access.log file for the web server in your Linux VM. Are the logs the same as in Part II?

Yes



Q8. Explain how you could prevent nmap from reaching the web server while still allowing legitimate clients to get service. Will a firewall be sufficient for this? Or do you need some other device? Please think critically about this.

Initially we can filter by browser application but if nmap sproof that there is no way.

We need tools to supervise how frequent one ip send request

Q9. What are your firewall rules? Run iptables -L on your VM and enter the output here.

