IGNITE CYBER SECURITY COHORT 1

NAME: BRIAN ODE

PHONE NUMBER: 0748267005

EMAIL: odebriangis@gmail.com

ASSIGNMENT: NMAP

SUMMARY REPORT

After identifying a target to hack or perform a security audit it is important to enumerate information about the target of interest as this gives us options where we can start our attack vector. One of the most important tool I learnt this week was Nmap. Nmap is a tool that has the capabilities of mapping the network and inform us the ports that are open and closed in a certain system of interest.

In this class week I learnt how to use different Nmap commands to enumerate the target. I also learnt how I can evade detection by intrusion detection system and avoid being blocked by the firewall. I also learnt the 3-way handshake where the server communicates with a client.

I learnt the following commands;

Getting help using the nmap –h command.

-scanning using TCP CONNECT connect – St

Scanning using half open –sS

Scanning using the UDP scan –Su

Using FIN scan (-sF to scan

Scanning the top 1000 ports –-top—port

Scanning specific ports

Scanning all the ports using –p- command.

Nmap engine

I also learnt about the different types of scan supported by nmap which includes safe,intrusive,vuln,exploit,aut,brute,discovery which can be used under different scenarios.

Example

Safe – this performs only scripts which are considered safe.

Intrusive – they are not safe and may likely affect the target.

Vuln – this script scans for vulnerabilities.

Exploit- attempts to exploit a target.

Brute- attempts to brute force credentials for running services.

Discovery – attempts to query running services.

I also leant that nmap scripts are written in Lua and are stored in /usr/share/nmap/scripts

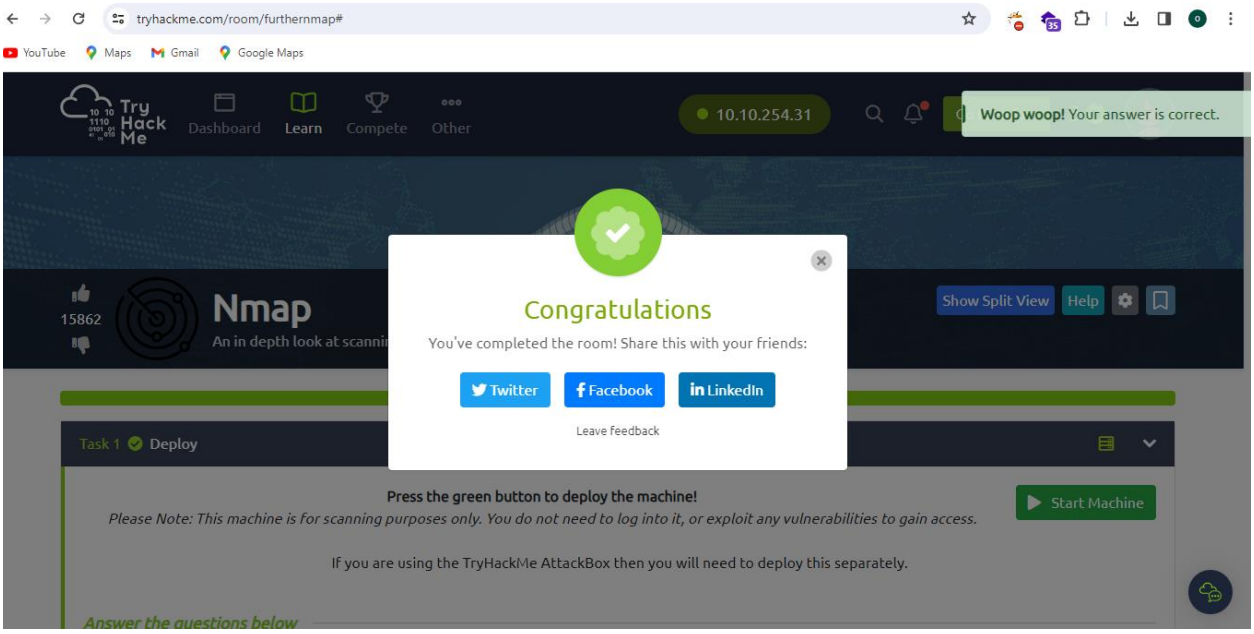
I learnt that syn scan has some disadvantages that is it requires to be run using sudo permissions and it can sometime bring down unstable services (DDOS attack)

CONCLUSION

Nmap is a powerful tool when it comes to enumeration of the target. Nmap can use different flags when scanning to evade firewall and also return results for specific user need. Scanning of

targets should be done with caution as it may lead to DDOS of unstable services which in some countries its considered a crime. We should scan networks that we have permission to.

BUDGE



REFERENCE