Lab 5

Lab 5 - Vulnerability Scanning & Patching – NMAP

By

Lukas Fuller

IAE-201-D02

IA-500: Introduction to Information Assurance

**Abstract**

The objective of this lab is to introduce students to NMAP and ZenMap. The student will be able to use NMAP to scan a network and find computers. They will also be able to understand the ports that are open on a computer using NMAP.

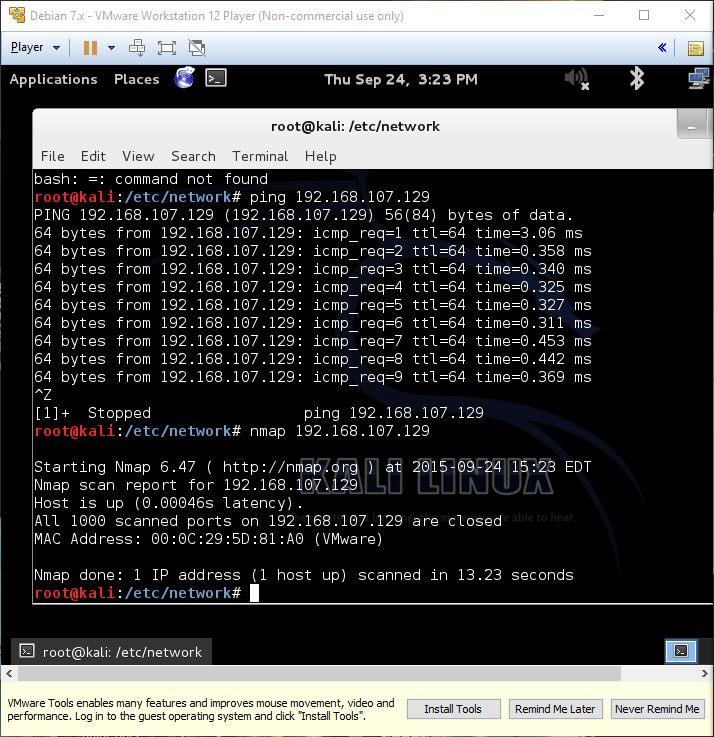
**Materials**

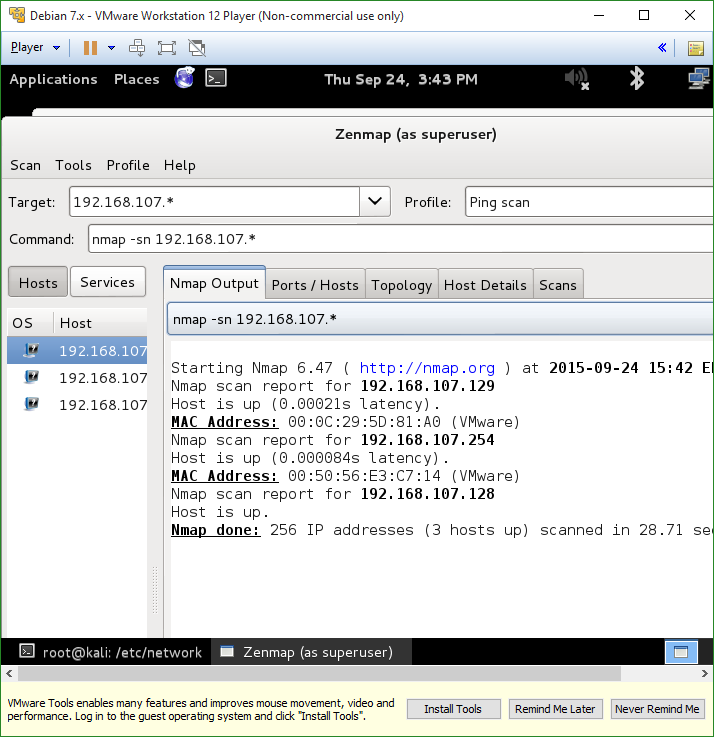
1. Kali Linux VM
2. Metasploitable VM

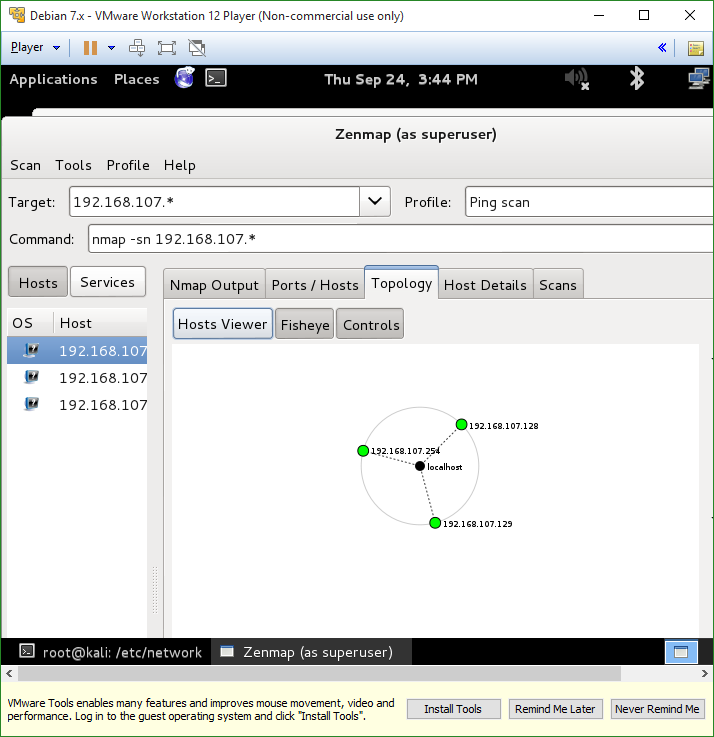
**Conclusion**

Although I had a few problems with initially creating a VM with metasploit on it, I now have a better understanding of how UNIX works and how NMAP and ZenMap function. NMAP is very useful for identifying simple vulnerabilities in a system like which ports are open, the state of the ports, the type of device, the operating system of the device, and a few others through different forms of scanning. This could help in penetration testing to find any weaknesses in a system or in a bad situation a hacker could abuse the vulnerabilities to get past a system’s defenses. ZenMap is very similar, but it allows you to gather more information on the target system and gives you more options on what type scan you want. Also, it says that it is discrete, but I’m pretty sure there is a way to identify when someone is scanning your system. Maybe that’s something I’ll learn later, but as of now I feel like I have a decent grasp on how to use Kali and some of the functions on it.

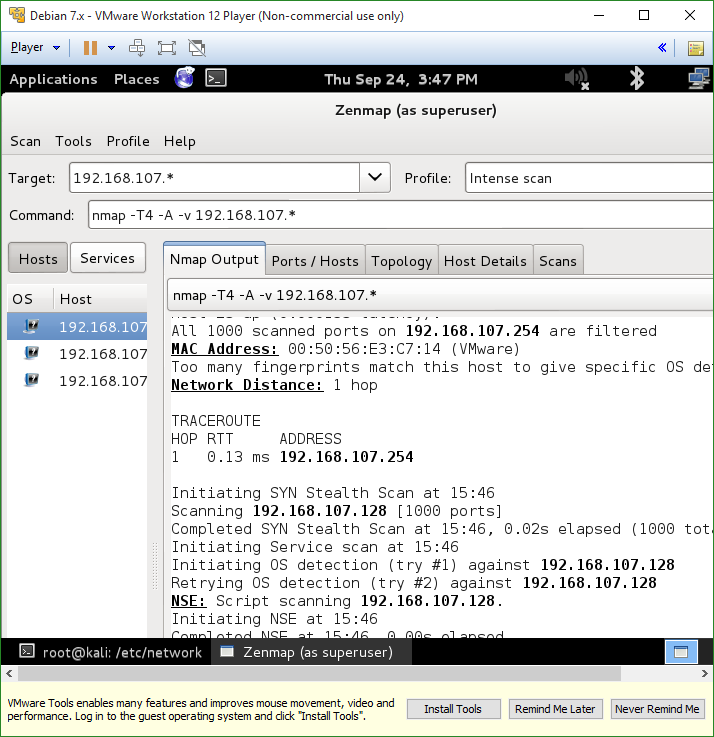
**Screenshots**

1. NMAP command

2. ZenMap Ping scan the LAN 

3. ZenMap’s Topology viewer

4. ZenMap intense scan



**Questions**

1. What is NMAP? **a tool that hackers use to view information about a host computer like IP information, what the system’s OS is, general system info, and it can ping the system**
2. What is ZenMap? **A tool that hackers use to gather information about a target computer like what ports are open, host details, different scanning options to detail more about the host while remaining discreet**
3. Are you allowed to scan any IP address on the internet or your school/business’s intranet? Why or why not? **No, only doing a simple NMAP ping, but more than that is illegal (mainly the system cannot allocate enough resources in the VM to complete the scan)**
4. How do you perform a regular scan on the host at 192.168.100.2 via NMAP? **nmap 192.168.100.2**
5. How do you perform a ping scan on the host at 192.168.100.10 via NMAP? **nmap -sP 192.168.100.10**
6. How do you perform a ping scan on the LAN at 192.168.50.0 via NMAP? **nmap –sP 192.168.50.0**
7. How do you perform a regular scan on the LANs at 192.168.0.0 via NMAP? **nmap -sP 192.168.0.\***
8. Using the Kali VM and ZenMap, what is the command used to complete an “Intense scan” with NMAP? **nmap –T4 –A –v**
9. What does the Topology view of ZenMap do? **It shows you the network you scanned with a visual representation that displays if a system has open or closed ports, and how big the dot is shows how many services it has open**
10. What does the Host Details view of ZenMap do? **It shows the status of the host, including the IP, the number of closed, scanned ports, up time, last boot, etc.**
11. Why is ZenMap so useful? **It is helpful in finding vulnerabilities of a host discreetly**