**PRACTICAL-3**

**AIM: Study and Configure Nmap (Network mapping tool) on Linux/Windows. Explore the various command for scanning your host/ips, ports and various services running on port. Prepare the document of at least 25 Nmap commands. Use the Nmap scrip and launch the DoS attack by flooding the packages in regular interval.**

**Software Requirements:** Nmap

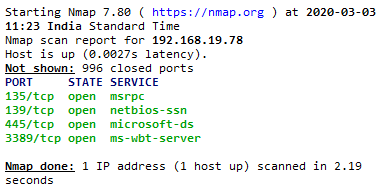
**Theory/Logic**: Network Mapped (Nmap) is a network scanning and host detection tool that is very useful during several steps of penetration testing. Nmap is not limited to merely gathering information and enumeration, but it is also powerful utility that can be used as a vulnerability detector or a security scanner. So Nmap is a multipurpose tool, and it can be run on many different operating systems including Windows, Linux, BSD, and Mac. Nmap is a very powerful utility that can be used to:

* Detect the live host on the network (host discovery)
* Detect the open ports on the host (port discovery or enumeration)
* Detect the software and the version to the respective port (service discovery)
* Detect the operating system, hardware address, and the software version
* Detect the vulnerability and security holes (Nmap scripts)

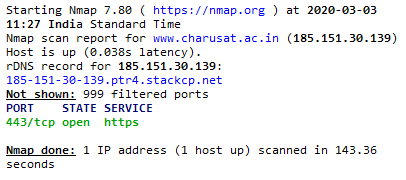
**Output:**

This are the commands used in the Nmap:

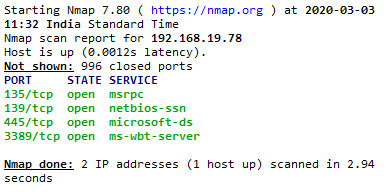
1. Scan Single IP**:**nmap 192.168.1.1



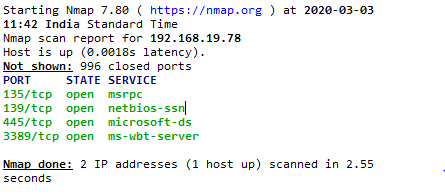
1. Scan a host: nmap[www.testhost.com](http://www.testhost.com)



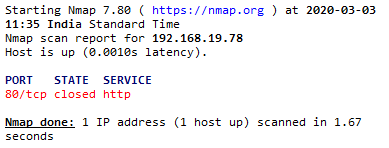
1. Scan range of IPs: nmap192.168.1.1-20



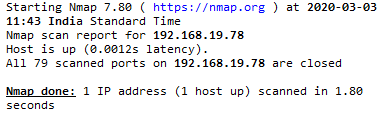
1. Scan targets from a text file: nmap -iL ip.txt



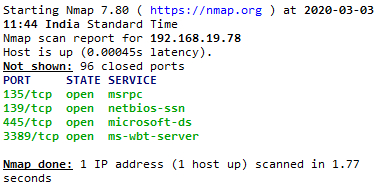
1. Scan Single port**:**nmap -p 22 192.168.1.1



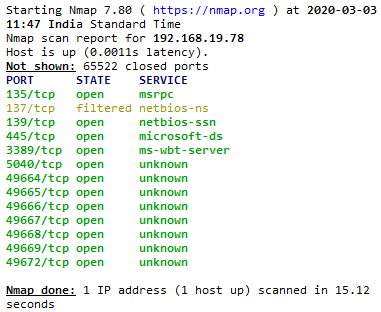
1. Scan range of ports**:**nmap -p 22-100 192.168.1.1



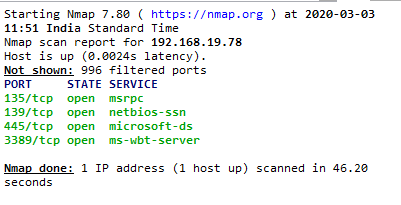
1. Scan 100 most common ports**:**nmap -F 192.168.1.1



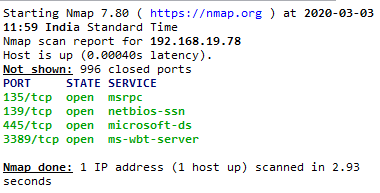
1. Scan all ports**:**nmap -p- 192.168.1.1



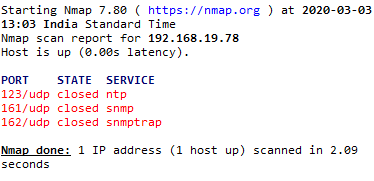
1. Scan using TCP connect**:**nmap -sT 192.168.1.1



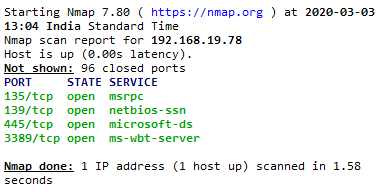
1. Scan using TCP SYN scan(default)**:**nmap -sS 192.168.1.1



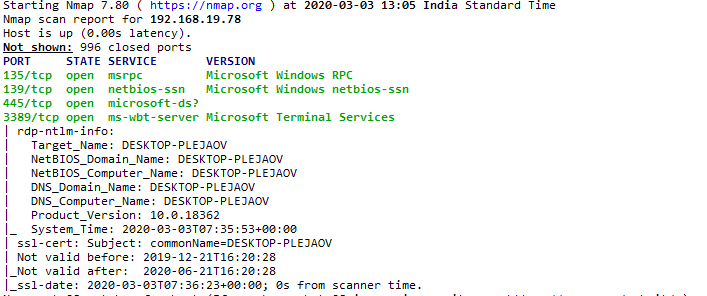
1. Scan UDP ports: nmap -sU -p 123,161,162 192.168.1.1



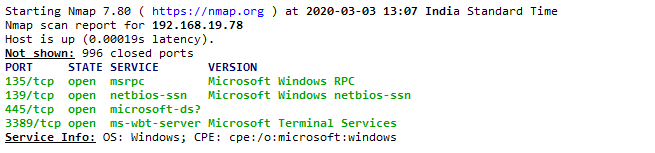
1. Scan Selected ports – ignore discovery: nmap -Pn -F 192.168.1.1



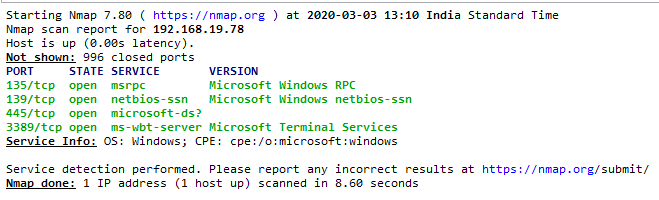
1. Detect OS and Services: nmap -A 192.168.1.1



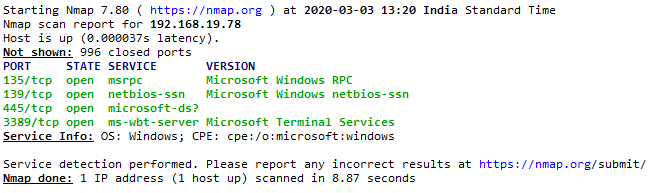
1. Standard Service Detection: nmap -sV 192.168.1.1



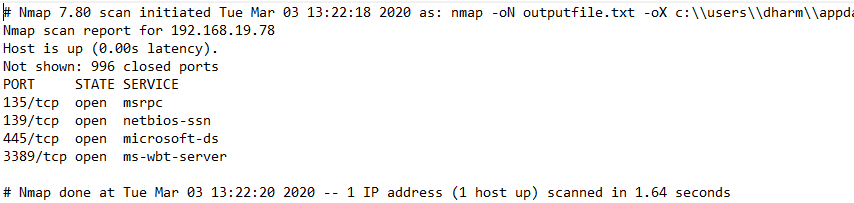
1. More Aggressive Service Detection: nmap -sV --version-intensity 5 192.168.1.1



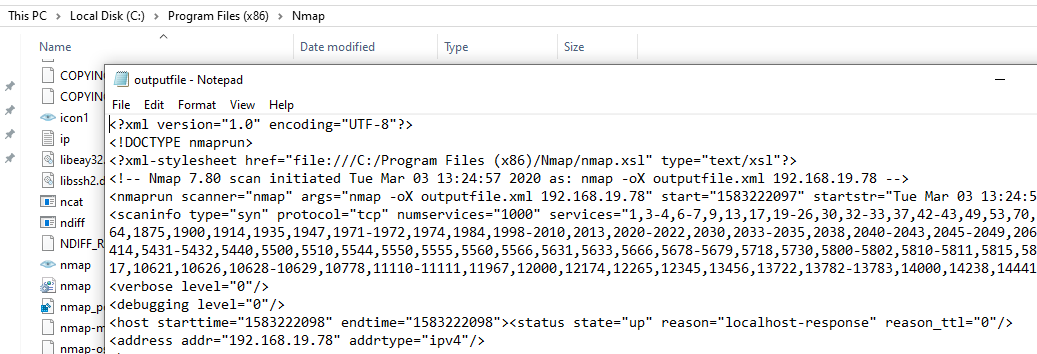
1. Lighter Banner Grabbing Detection: nmap -sV --version-intensity 0 192.168.1.1



1. Save default output file: nmap -oN outputfile.txt 192.168.1.1

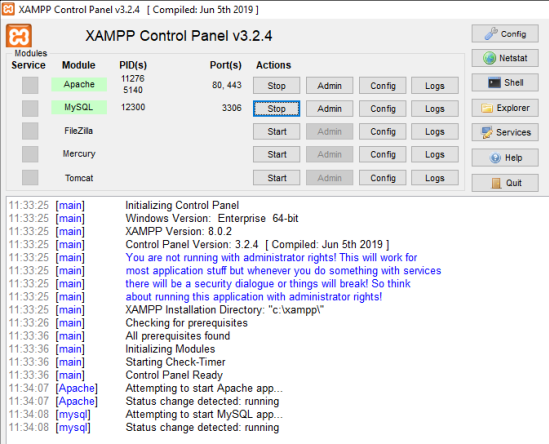


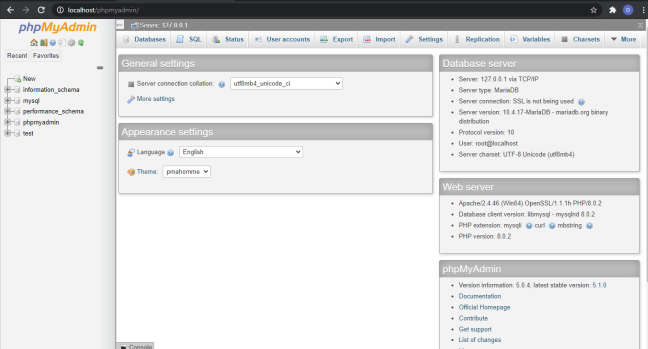
1. Save output as XML file: nmap -oX outputfile.xml 192.168.1.1



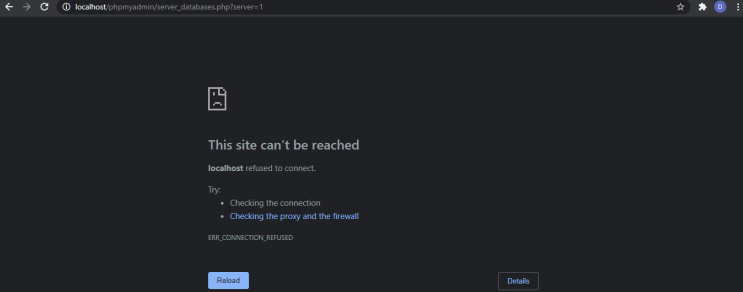
1. Similarly, you can store in form of grep file: nmap -oG outputfile.txt 192.168.1.1 and also in all the formats: nmap -oAoutputfile 192.168.1.1
2. There are 581 scripts in Nmap to see list of them you can use “locate nse | grep script” and to see individual scripts you can use “--script-help=$scriptname”.

**DOS ATTACK**









**Conclusion:** To conclude, we have learnt Nmap commands and Dos Attack in this practical.