**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.**

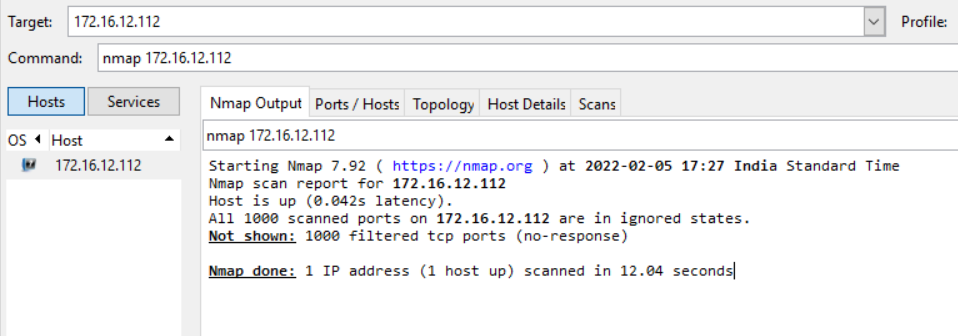
**Hardware Requirements:** Computer/Laptop

**Software Requirements:** Nmap

**1. Scan a system with Hostname and IP address :-**

Command: nmap 172.16.12.112

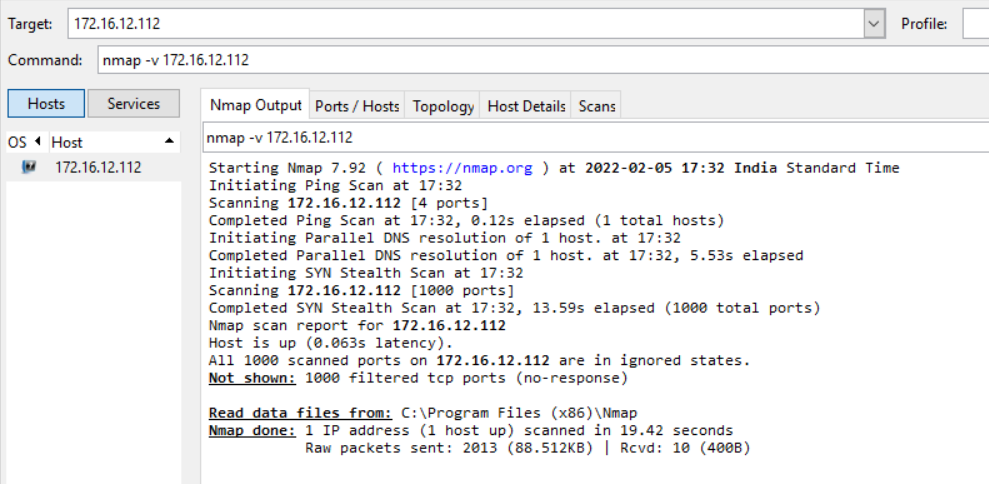
Output:



**2. Scan using “-v” option :-**

Command: nmap -v 172.16.12.112

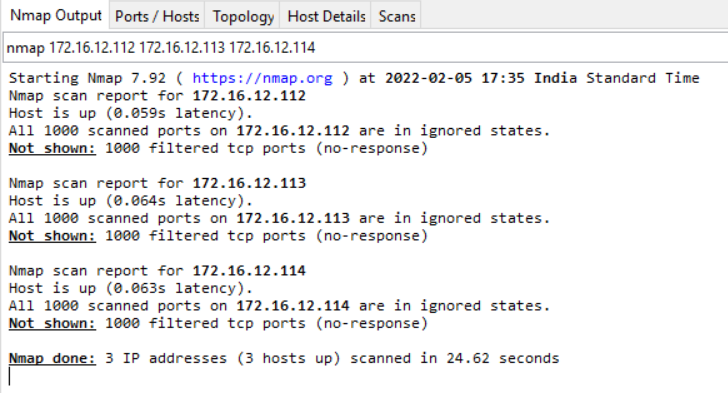
Output:



**3. Scan multiple Hosts :-**

Command: nmap 172.16.12.112 172.16.12.113 172.16.12.114

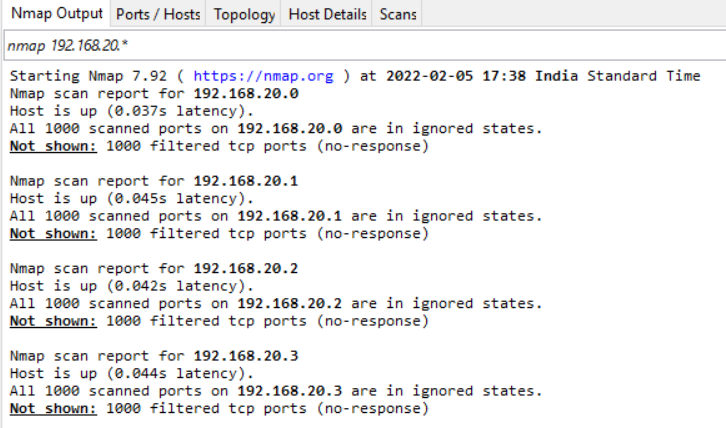
Output:



**4. Scan Whole subnet :-**

Command: nmap 192.168.20.\*

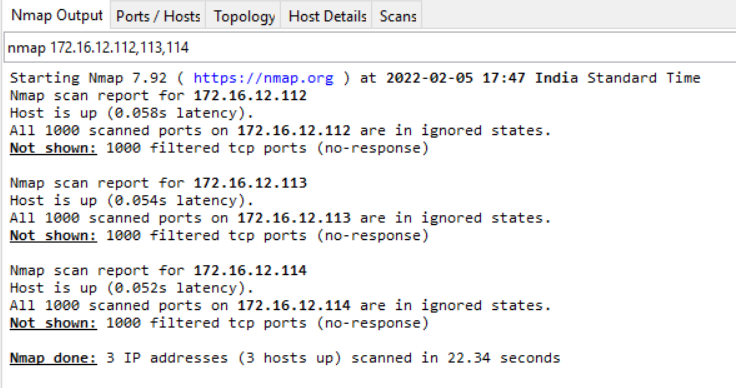
Output:



**5. Scan multiple server using last octet of IP address :-**

Command: nmap 172.16.12.112,113,114

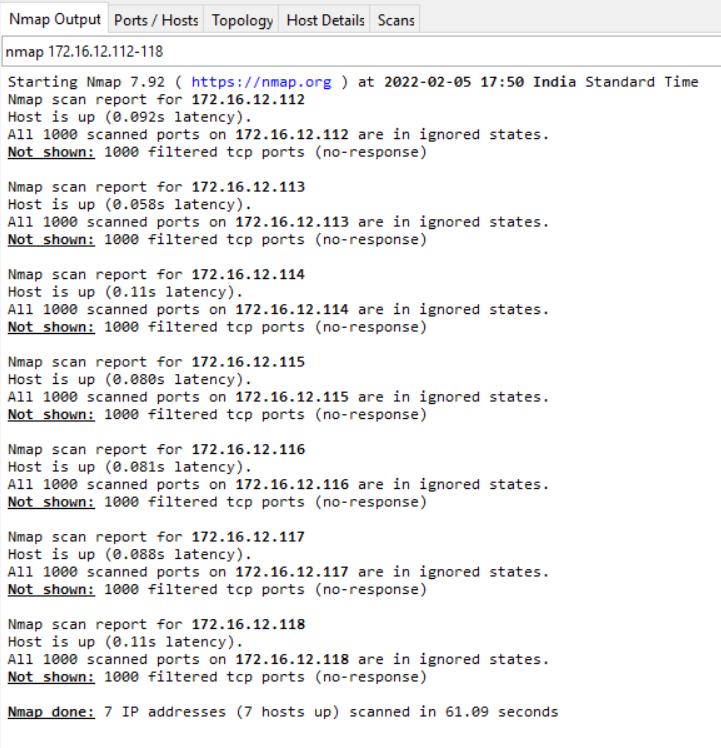
Output:



**6. Scan an IP address range :-**

Command: nmap 172.16.12.112-118

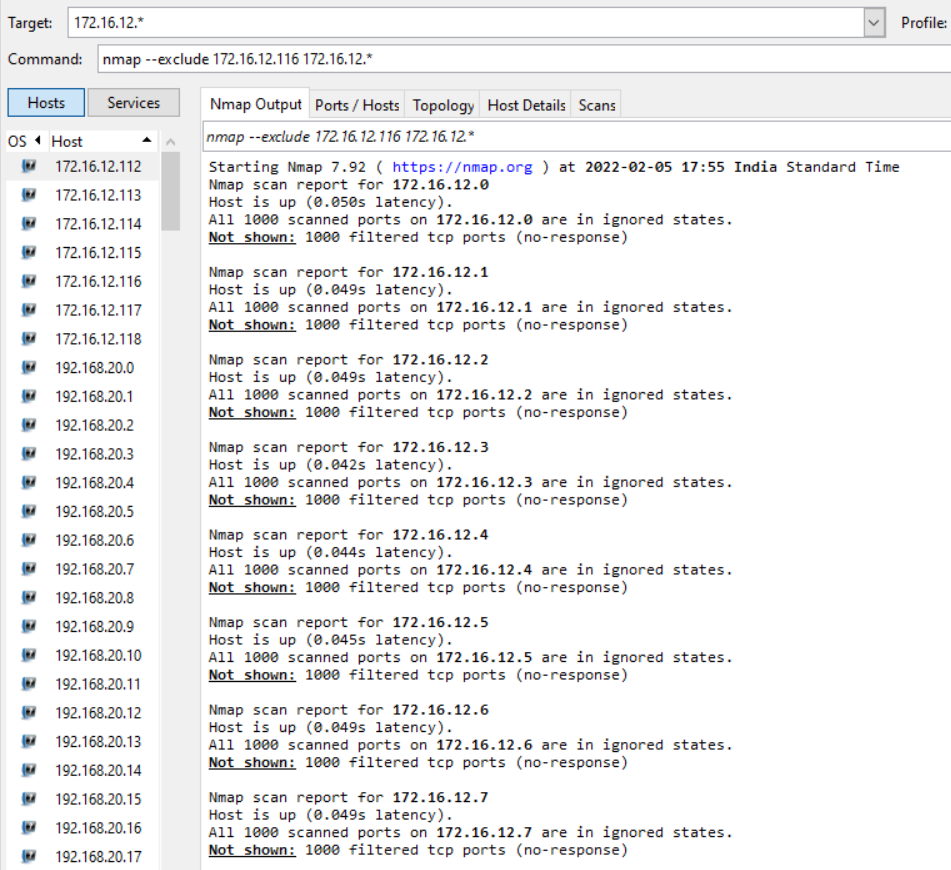
Output:



**7. Scan network excluding Remote Host :-**

Command: nmap --exclude 172.16.12.116 172.16.12.\*

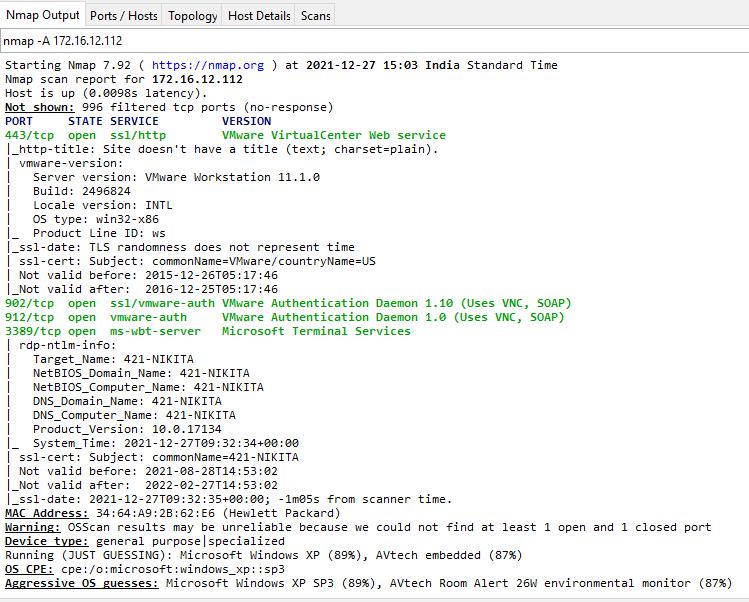
Output:

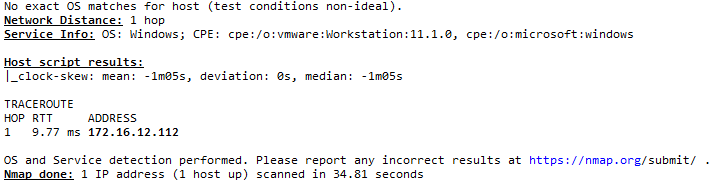


**8. Scan OS information :-**

Command: nmap –A 172.16.12.112

Output:

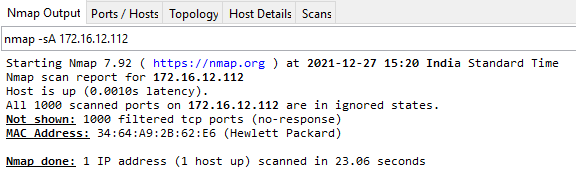




**9. Scan a Host to Detect Firewall :-**

Command: nmap –sA 172.16.12.112

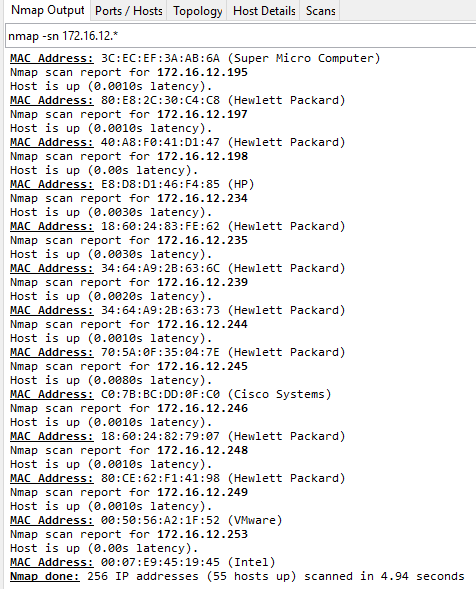
Output:



**10. Find out Live host in a network :-**

Command: nmap –sn 172.16.12.\*

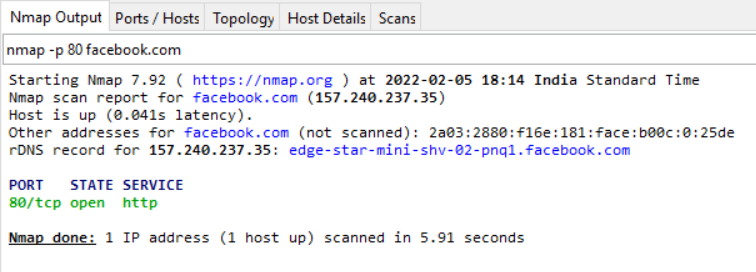
Output:



**11. Scan for Specific ports :-**

Command: nmap -p 80 facebook.com

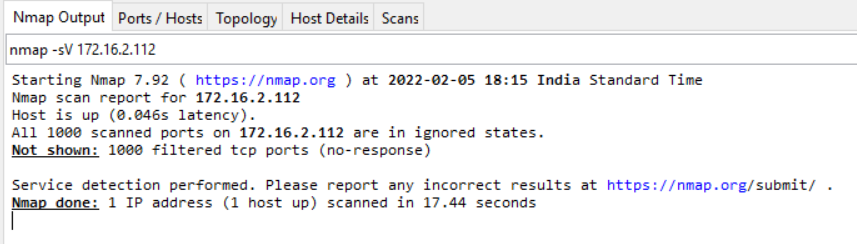
Output:



**12. Find host Services version Number :-**

Command: nmap -sV 172.16.2.112

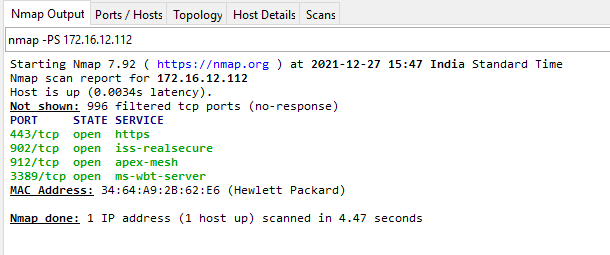
Output:



**13. Scan remote host using TCP ACk(PA) and TCP syn(PS) :-**

Command: nmap –PS 172.16.12.112

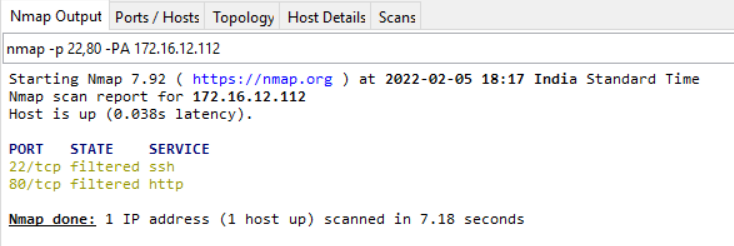
Output:



**14. Scan remote host for specific ports with TCP ACK :-**

Command: nmap -p 22,80 -PA 172.16.12.112

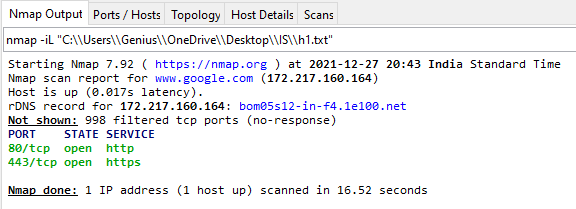
Output:



**15. Scan targets from Text file :-**

Command: nmap –iL C:\Users\Genius\OneDrive\Desktop\IS\h1.txt

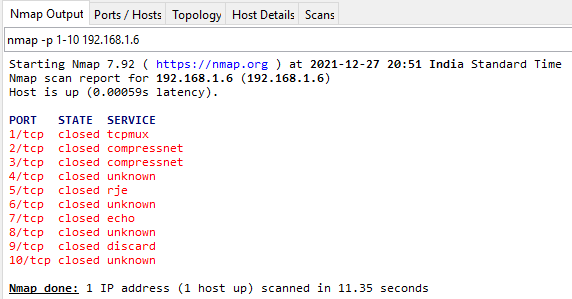
Output:



**16. Scan a range of ports :-**

Command: nmap –p 1-10 192.168.1.6

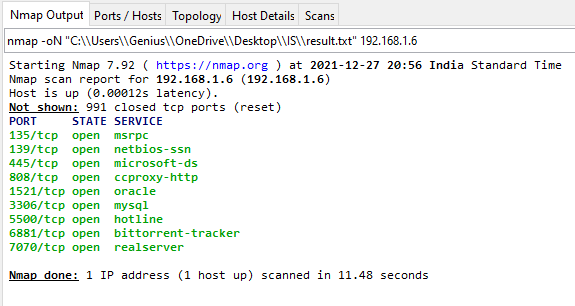
Output:



**17. Save default output to file :-**

Command: nmap –oN "C:\\Users\\Genius\\OneDrive\\Desktop\\IS\\result.txt” 192.168.1.6

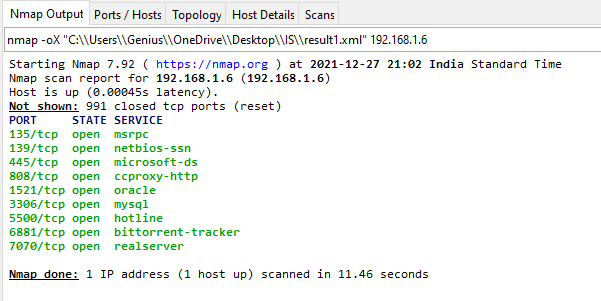
Output:



**18. Save result as Xml :-**

Command: nmap -oX "C:\\Users\\Genius\\OneDrive\\Desktop\\IS\\result1.xml" 192.168.1.6

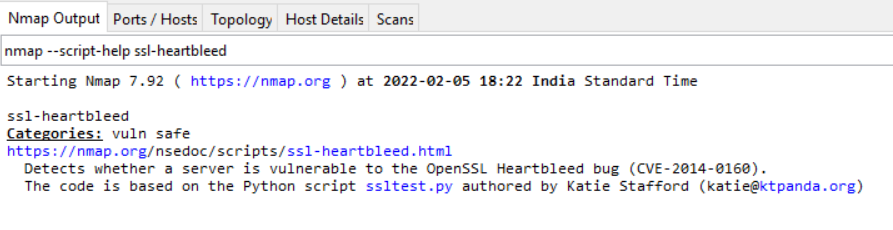
Output:



**19. Get help for a script :-**

Command: nmap --script-help=ssl-heartbleed

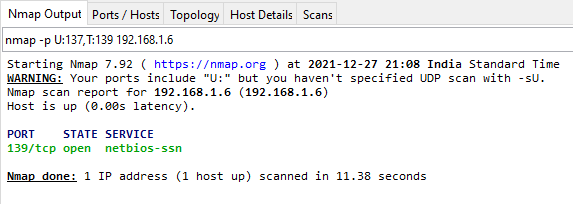
Output:



**20. Specify UDP or TCP scan :-**

Command: nmap –p U:137,T:139 192.168.1.6

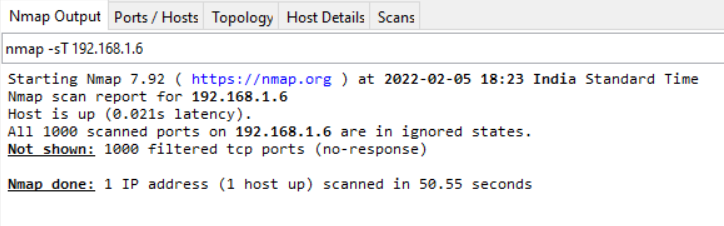
Output:



**21. Scan using TCP connect:-**

Command: nmap -sT 192.168.1.6

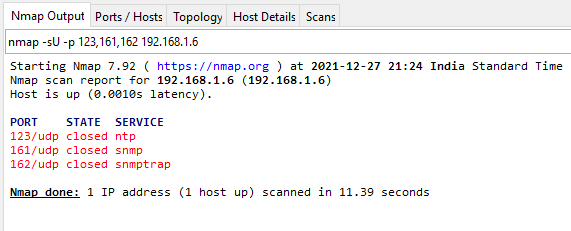
Output:



**22. Scan using UDP ports :-**

Command: nmap –sU –p 123,162,162 192.168.1.6

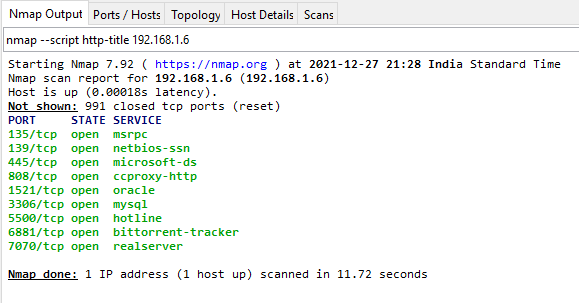
Output:



**23. Gather page Titles from HTTP Servers :-**

Command: nmap --script =http-title 192.168.1.6

Output:

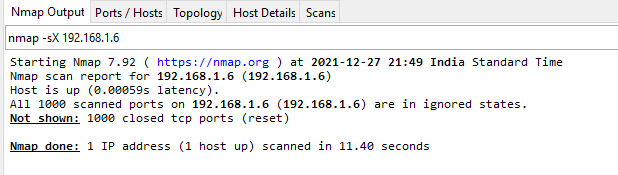


**24. Xmas Scan :-**

Command: nmap –sX 192.168.1.6

Meaning: - Nmap Xmas scan was considered a stealthy scan which analyzes responses to Xmas packets to determine the nature of the replying device.

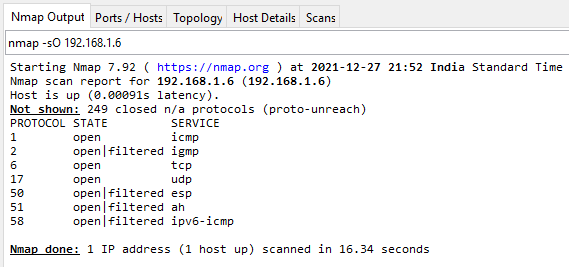
Output:



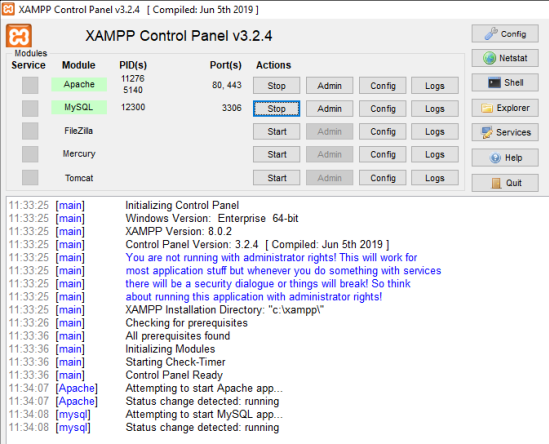
**25. IP protocol Scan :-**

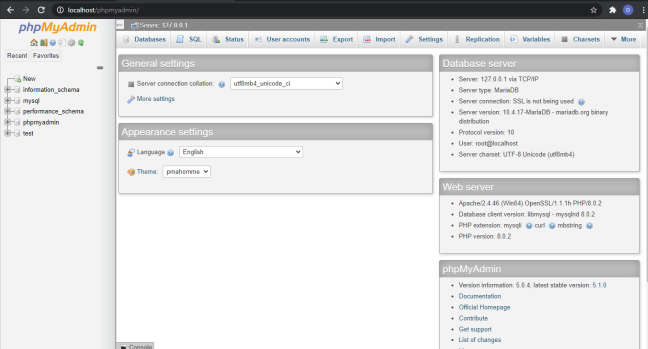
Command: nmap –sO 192.168.1.6

Output:



**DoS Attack :-**







Therefore, DoS command has been successfully implemented.