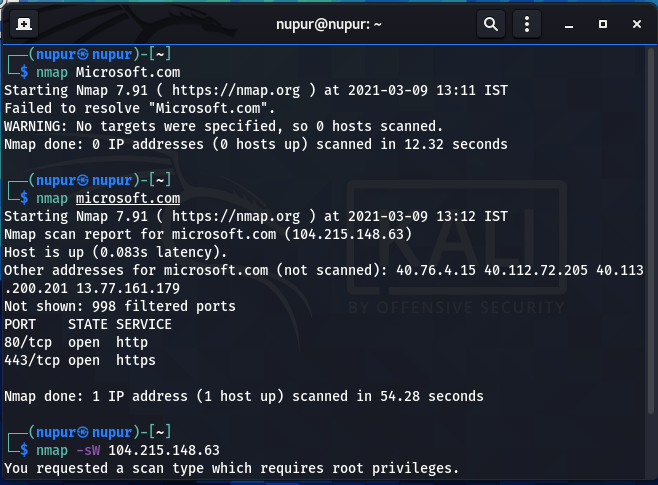
**Assignment on Nmap Commands**

**Submitted by : Madhur Nagrath**

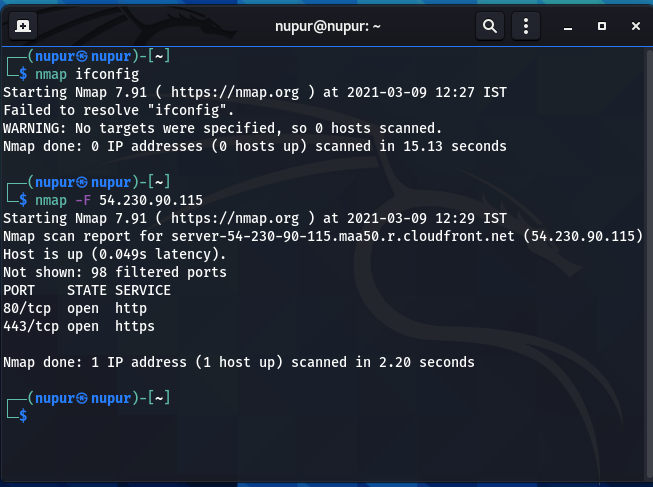
**Roll No. 19csu169**

Write commands and print and explain the output for

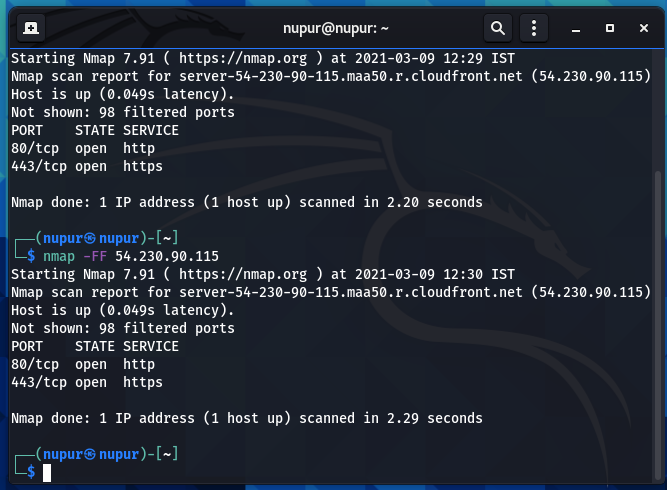
1. **Spoof MAC Address**

****

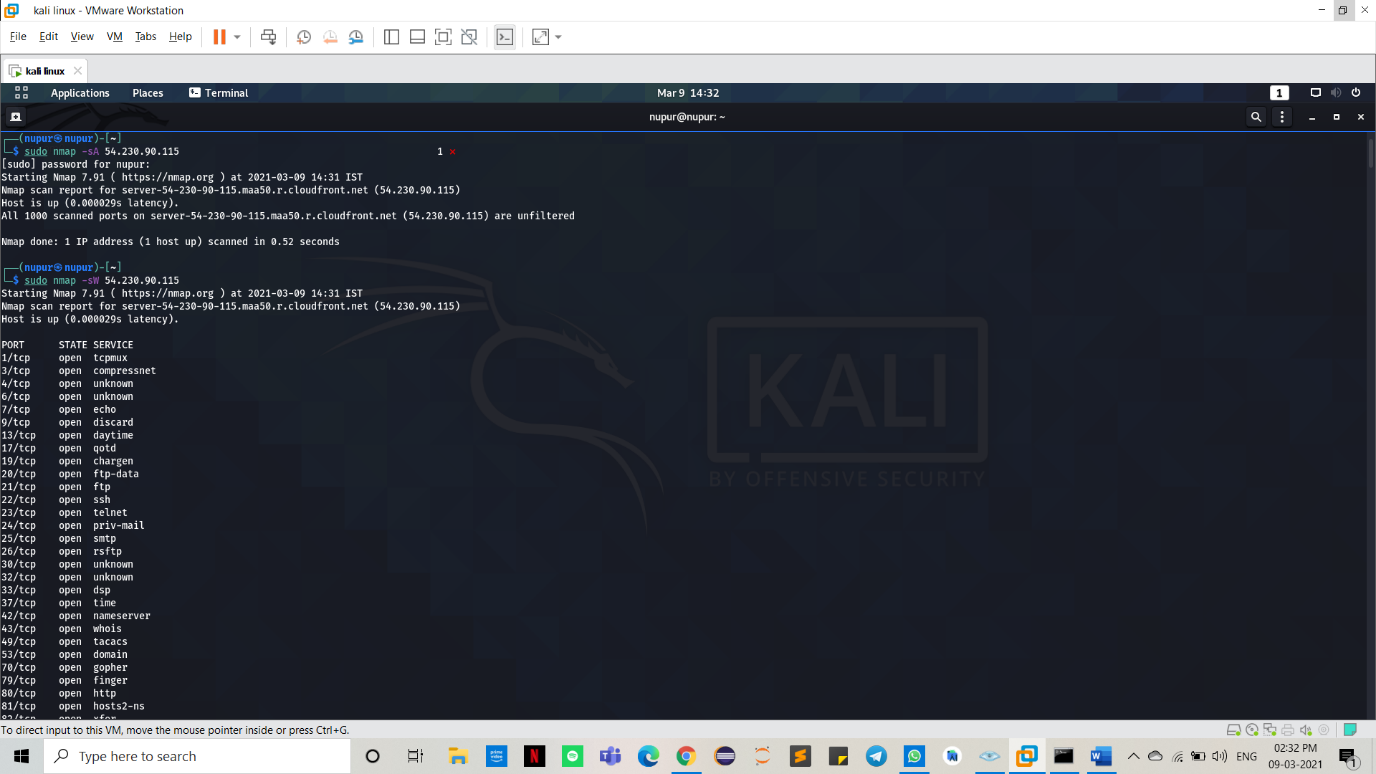
1. **Spoof IP Address**

****

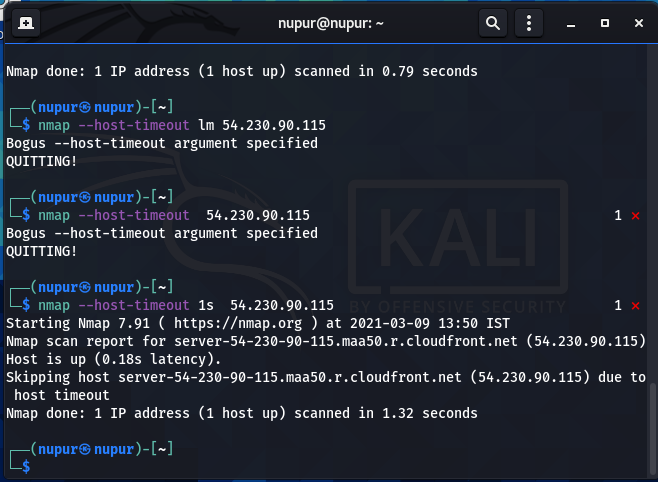
1. **Fragment Packets (-f)**
2. **Further fragment packets (**twice, -ff)

****

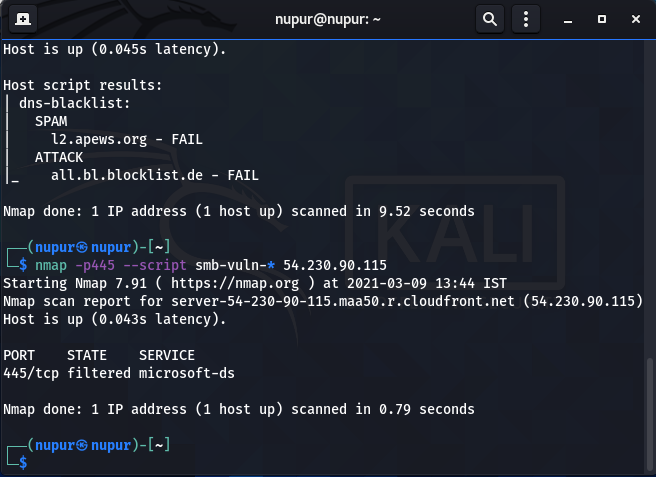
1. **TCP Window Scan (-sW), explain result difference if firewall is enabled or disabled (Hint: filtered or closed)**
2. **TCP ACK Scan (-sA)**

****

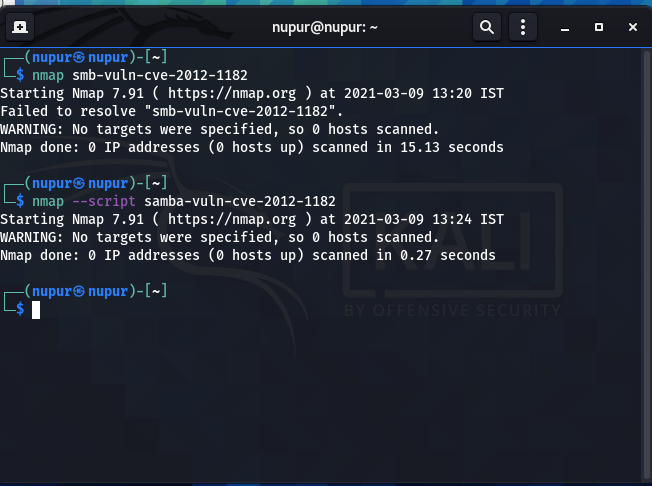
1. **Host Timeout Option (–host-timeout)**

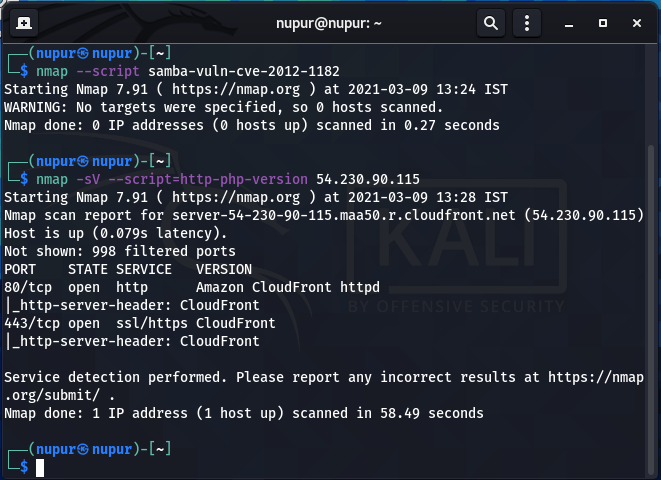
****

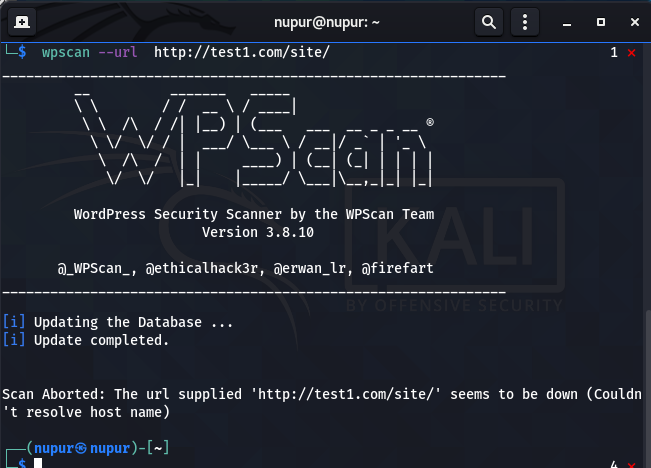
1. **smb-check-vulns (Hint:** script that can scan to check the vulnerabilities) explain which type of vulnerabilities can be exploited)

****

1. **samba-vuln-cve-2012-1182, (hint :**The script to perform the desired scanning against the target machine to find the Samba heap overflow vulnerability CVE-2012-1182)

****

1. **http-php-version (hint:** this script has been created to get the PHP version from the web server.****
2. Penetration testing on a website which is based on **WordPress**

****

1. **dns-blacklist (Hint:** script find the blacklisted IP addresses)

