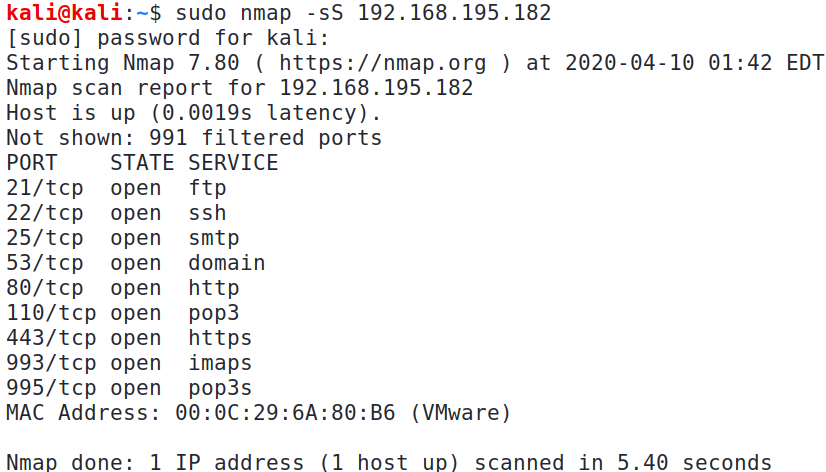
**Practical 2 Sample Test Report**

**Sample test report for web-server2**

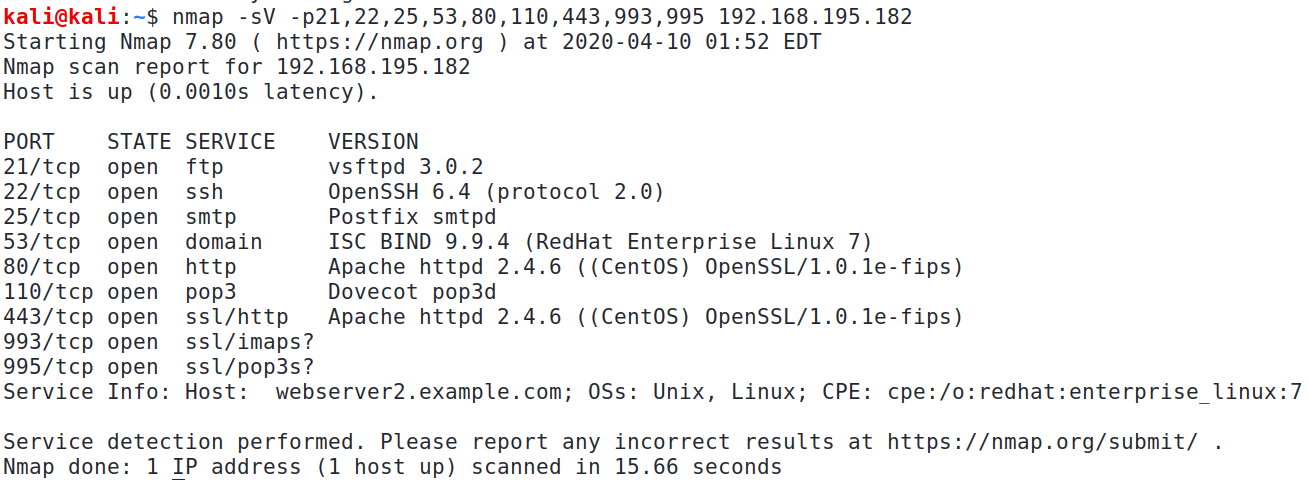
1. First do a basic port scan on web-server2 (scanning the most common 1000 TCP ports).



Change to the IP of your web-server2

1. Quite a number of TCP ports are opened on web-server2! Nmap also lists the service name that is commonly used for that particular port number. To verify the service that is running on each opened port, and its version number, we can try banner grabbing on each port, or we can also use the Nmap -sV option for service detection.

For the scan to run faster, we can specify to scan only the opened ports using the -p option.



1. The Nmap -sV returns the service name and version number for most of the opened ports, including the operating system of web-server2.

Fill up the tables. For the vulnerabilities and concerns, you would need to do some research on any vulnerabilities on the services found.

**Sample Test Report for web-server2**

|  |  |
| --- | --- |
| IP address | OS |
| 192.168.195.182 | Linux |

|  |  |  |  |
| --- | --- | --- | --- |
| Port | TCP or UDP | Protocol name | Remarks (eg banner information) |
| 21 | TCP | FTP | Vsftpd 3.0.2 |
| 22 | TCP | SSH | OpenSSH 6.4 (protocol 2.0) |
| 25 | TCP | SMTP | Postfix |
| 53 | TCP | DNS | Bind 9.9.4 |
| 80 | TCP | HTTP | Apache httpd 2.4.6 |
| 110 | TCP | POP3 | Dovecot |
| 443 | TCP | HTTPS | Apache httpd 2.4.6 |
| 993 | TCP | IMAPS | Nil |
| 995 | TCP | POP3S | Nil |

|  |
| --- |
| Concern or Vulnerability #1 |
| As POP3S is available, the unsecured version POP3 running on Port 110 may not be needed. |
| Recommendations |
| Disable POP3. |

|  |
| --- |
| Concern or Vulnerability #2 |
| FTP which has no encryption, is running on Port 21 |
| Recommendations |
| If FTP is not required, disable it. |

Note : We did not scan for UDP ports in this example.

*End*