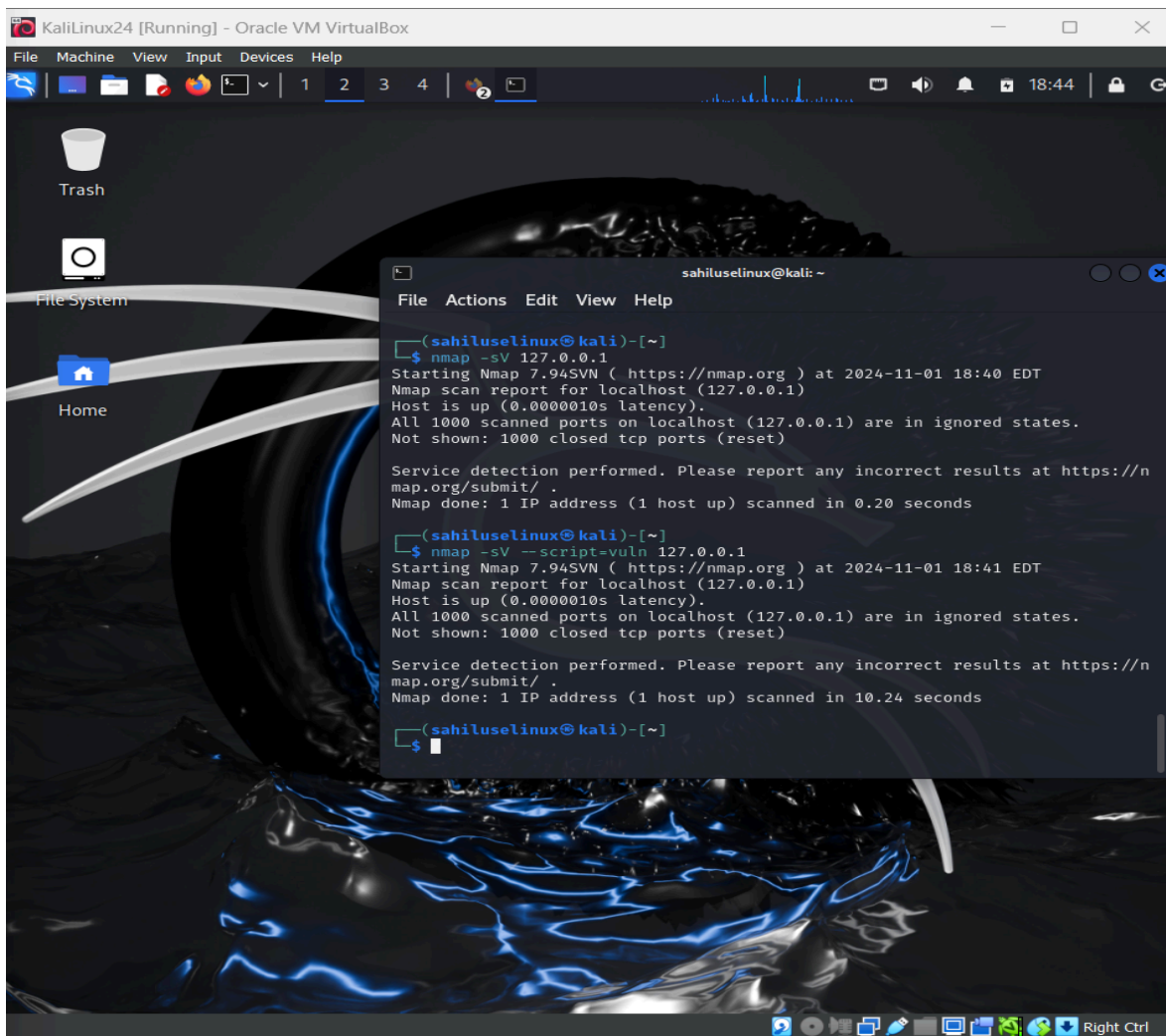


Vulnerability Report

I used the commands from the steps to scan for any open ports on a network or active device. I used Kali Linux and I was prompted to scan Debian's IP address. Debian's IP address is found by using the command "ip addr". This will show the IP address and other various information such as "inet6" and MAC addresses. The IP address for Debian was 127.0.0.1/8 , and starting nmap with this IP address scanned for every single IP address possible starting with the last digit which was "1". "All 1000 scanned ports on local host 127.0.0.1 are in ignored states." This implies that Debian has a pre-installed firewall that blocks nmap from scanning it. The "1000" means that nmap only scans the 1000 most common ports.



```
(sahiluslinux@kali)-[~]
$ nmap -sV 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 18:40 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

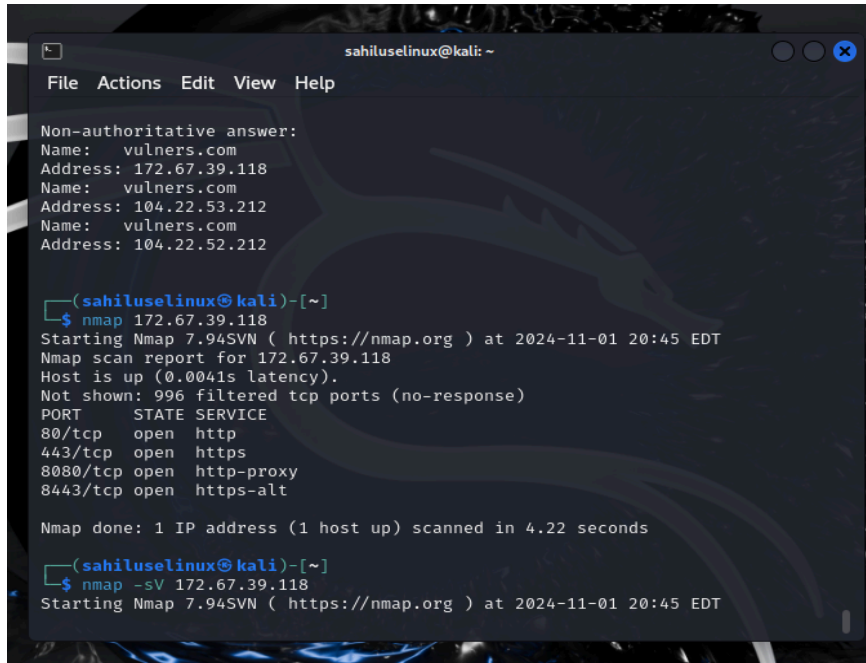
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds

(sahiluslinux@kali)-[~]
$ nmap -sV --script=vuln 127.0.0.1
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 18:41 EDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.24 seconds

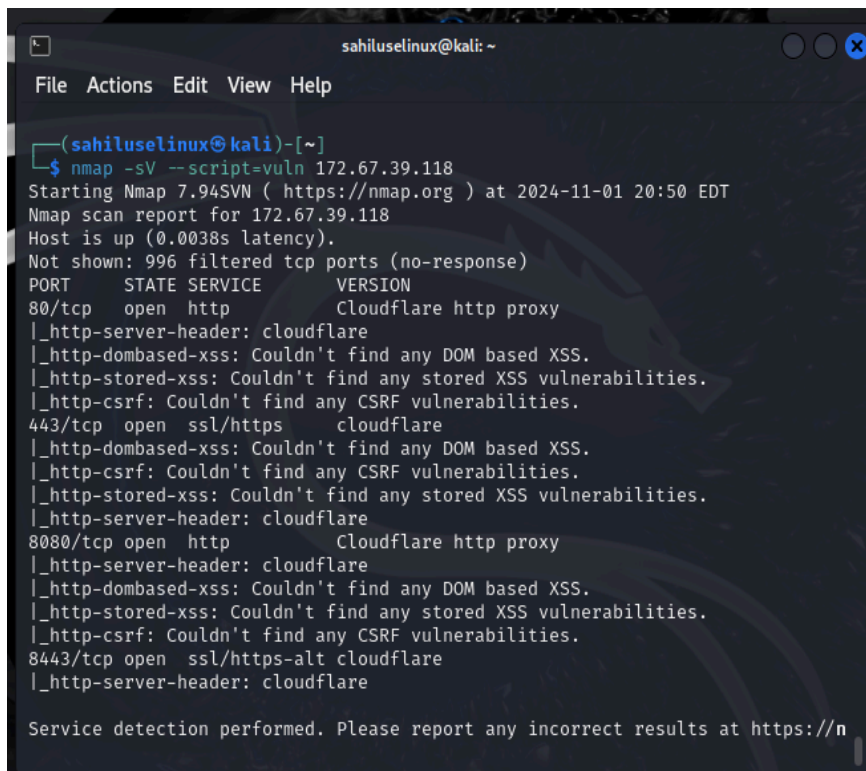
(sahiluslinux@kali)-[~]
$
```

With the other commands to enumerate ports and verify services, this did not work with Debian. I tried vulners.com. I used the command `nslookup vulners.com` to acquire their IP address. I then proceeded to start scanning with their IP address.



```
sahiluslinux@kali: ~  
File Actions Edit View Help  
Non-authoritative answer:  
Name:   vulners.com  
Address: 172.67.39.118  
Name:   vulners.com  
Address: 104.22.53.212  
Name:   vulners.com  
Address: 104.22.52.212  
  
(sahiluslinux@kali)-[~]  
$ nmap 172.67.39.118  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 20:45 EDT  
Nmap scan report for 172.67.39.118  
Host is up (0.0041s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
80/tcp    open  http  
443/tcp   open  https  
8080/tcp  open  http-proxy  
8443/tcp  open  https-alt  
  
Nmap done: 1 IP address (1 host up) scanned in 4.22 seconds  
  
(sahiluslinux@kali)-[~]  
$ nmap -sV 172.67.39.118  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 20:45 EDT
```

As you can see on the image, you can see that because it's a public website/database, results do actually show. Like 80, 443, 8080, and 8843 with different levels of security.



```
sahiluslinux@kali: ~  
File Actions Edit View Help  
  
(sahiluslinux@kali)-[~]  
$ nmap -sV --script=vuln 172.67.39.118  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-01 20:50 EDT  
Nmap scan report for 172.67.39.118  
Host is up (0.0038s latency).  
Not shown: 996 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Cloudflare http proxy  
|_http-server-header: cloudflare  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_http-csrf: Couldn't find any CSRF vulnerabilities.  
443/tcp   open  ssl/https    cloudflare  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-csrf: Couldn't find any CSRF vulnerabilities.  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_http-server-header: cloudflare  
8080/tcp  open  http         Cloudflare http proxy  
|_http-server-header: cloudflare  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_http-csrf: Couldn't find any CSRF vulnerabilities.  
8443/tcp  open  ssl/https-alt cloudflare  
|_http-server-header: cloudflare  
  
Service detection performed. Please report any incorrect results at https://n
```

In this image, I did a detailed scan and it gave me much more information but couldn't find vulnerabilities whether it was in XSS or CSRF. It also specifies which version it is like cloudflare http proxy for ports 80 and 8080. The rest were just cloudflare versions.