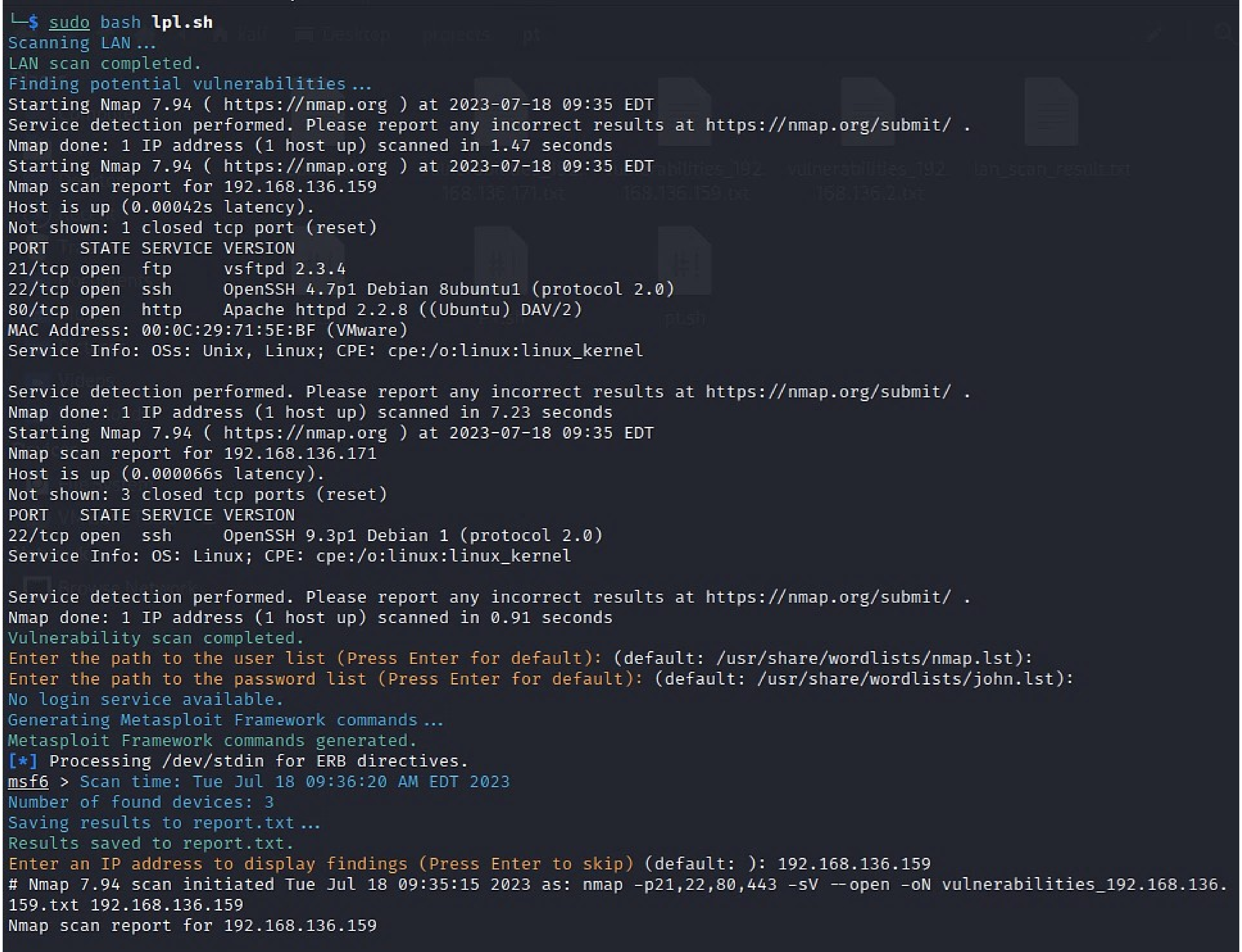
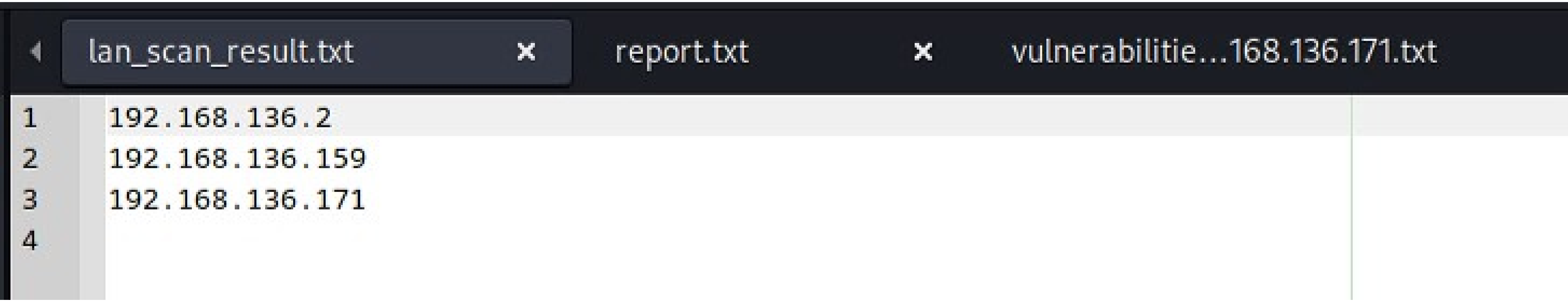
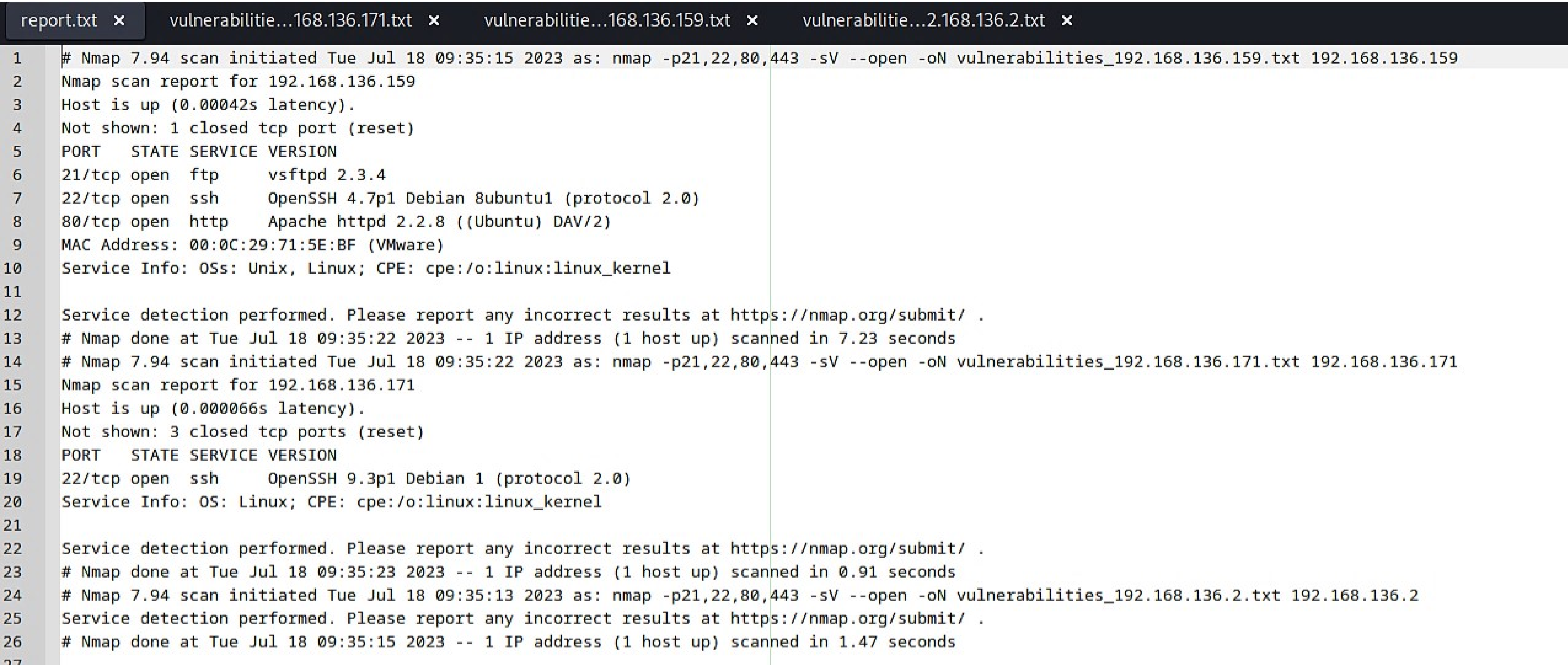


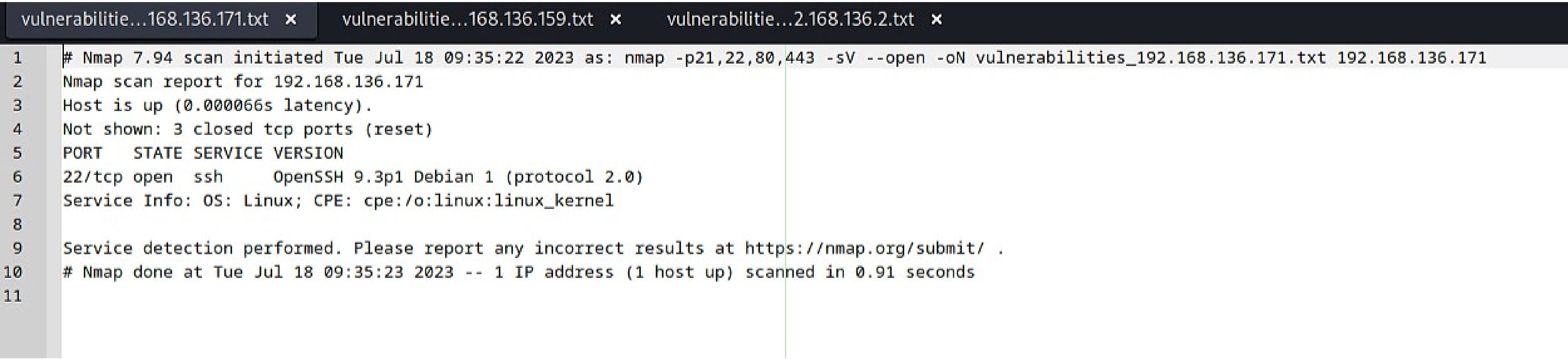
```
└─$ sudo bash lpl.sh
Scanning LAN ...
LAN scan completed.
Finding potential vulnerabilities ...
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 09:35 EDT
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.47 seconds
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 09:35 EDT
Nmap scan report for 192.168.136.159
Host is up (0.00042s latency).
Not shown: 1 closed tcp port (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:71:5E:BF (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.23 seconds
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-18 09:35 EDT
Nmap scan report for 192.168.136.171
Host is up (0.000066s latency).
Not shown: 3 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.91 seconds
Vulnerability scan completed.
Enter the path to the user list (Press Enter for default): (default: /usr/share/wordlists/nmap.lst):
Enter the path to the password list (Press Enter for default): (default: /usr/share/wordlists/john.lst):
No login service available.
Generating Metasploit Framework commands ...
Metasploit Framework commands generated.
[*] Processing /dev/stdin for ERB directives.
msf6 > Scan time: Tue Jul 18 09:36:20 AM EDT 2023
Number of found devices: 3
Saving results to report.txt ...
Results saved to report.txt.
Enter an IP address to display findings (Press Enter to skip) (default: ): 192.168.136.159
# Nmap 7.94 scan initiated Tue Jul 18 09:35:15 2023 as: nmap -p21,22,80,443 -sV --open -oN vulnerabilities_192.168.136.
159.txt 192.168.136.159
Nmap scan report for 192.168.136.159
```



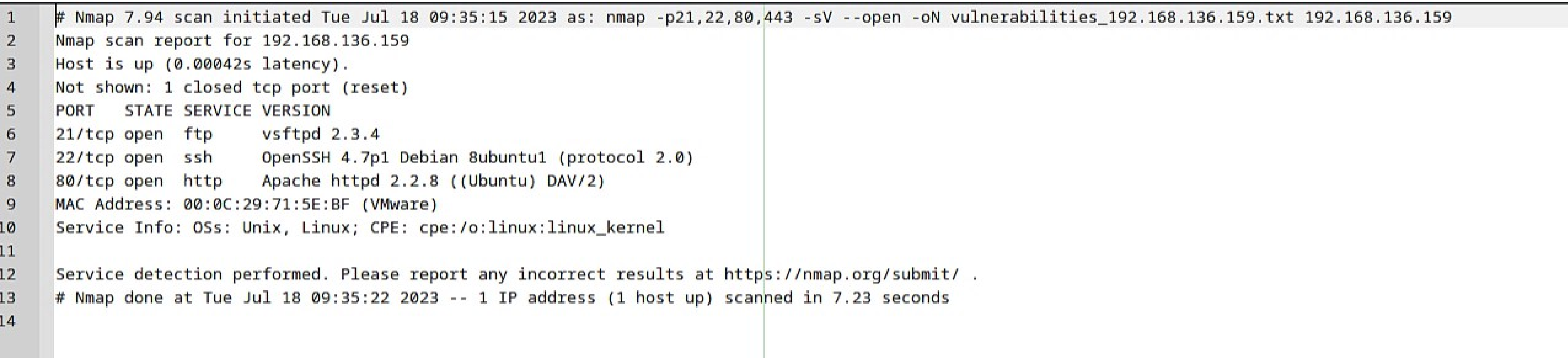
```
192.168.136.2
192.168.136.159
192.168.136.171
```


report.txt ×
vulnerabilitie…168.136.171.txt ×
vulnerabilitie…168.136.159.txt ×
vulnerabilitie…2.168.136.2.txt ×

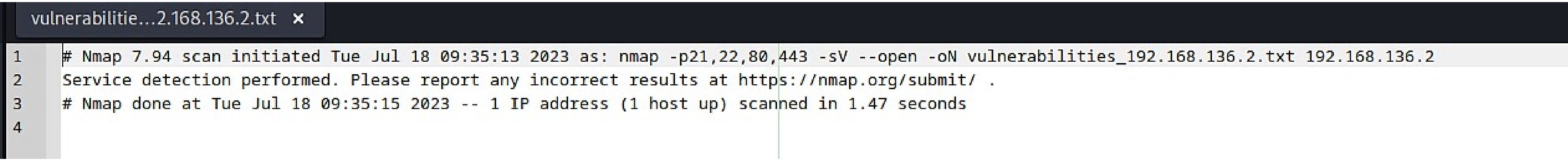
```
# Nmap 7.94 scan initiated Tue Jul 18 09:35:15 2023 as: nmap -p21,22,80,443 -sV --open -oN vulnerabilities_192.168.136.159.txt 192.168.136.159
Nmap scan report for 192.168.136.159
Host is up (0.00042s latency).
Not shown: 1 closed tcp port (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:71:5E:BF (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 18 09:35:22 2023 -- 1 IP address (1 host up) scanned in 7.23 seconds
# Nmap 7.94 scan initiated Tue Jul 18 09:35:22 2023 as: nmap -p21,22,80,443 -sV --open -oN vulnerabilities_192.168.136.171.txt 192.168.136.171
Nmap scan report for 192.168.136.171
Host is up (0.000066s latency).
Not shown: 3 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 18 09:35:23 2023 -- 1 IP address (1 host up) scanned in 0.91 seconds
# Nmap 7.94 scan initiated Tue Jul 18 09:35:13 2023 as: nmap -p21,22,80,443 -sV --open -oN vulnerabilities_192.168.136.2.txt 192.168.136.2
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 18 09:35:15 2023 -- 1 IP address (1 host up) scanned in 1.47 seconds
```


vulnerabilitie…168.136.171.txt ×
vulnerabilitie…168.136.159.txt ×
vulnerabilitie…2.168.136.2.txt ×

```
# Nmap 7.94 scan initiated Tue Jul 18 09:35:22 2023 as: nmap -p21,22,80,443 -sV --open -oN vulnerabilities_192.168.136.171.txt 192.168.136.171
Nmap scan report for 192.168.136.171
Host is up (0.000066s latency).
Not shown: 3 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.3p1 Debian 1 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 18 09:35:23 2023 -- 1 IP address (1 host up) scanned in 0.91 seconds
```



```
# Nmap 7.94 scan initiated Tue Jul 18 09:35:15 2023 as: nmap -p21,22,80,443 -sV --open -oN vulnerabilities_192.168.136.159.txt 192.168.136.159
Nmap scan report for 192.168.136.159
Host is up (0.00042s latency).
Not shown: 1 closed tcp port (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
22/tcp open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:71:5E:BF (VMware)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 18 09:35:22 2023 -- 1 IP address (1 host up) scanned in 7.23 seconds
```



```
# Nmap 7.94 scan initiated Tue Jul 18 09:35:13 2023 as: nmap -p21,22,80,443 -sV --open -oN vulnerabilities_192.168.136.2.txt 192.168.136.2
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Jul 18 09:35:15 2023 -- 1 IP address (1 host up) scanned in 1.47 seconds
```