

```
└─$ 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
```

lan_scan_result.txt		report.txt	vulnerabilite...168.136.171.txt
1	192.168.136.2		
2	192.168.136.159		
3	192.168.136.171		
4			

report.txt xvulnerabilitie...168.136.171.txt xvulnerabilitie...168.136.159.txt xvulnerabilitie...2.168.136.2.txt x

```
1 # 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
2 Nmap scan report for 192.168.136.159
3 Host is up (0.00042s latency).
4 Not shown: 1 closed tcp port (reset)
5 PORT      STATE SERVICE VERSION
6 21/tcp    open  ftp      vsftpd 2.3.4
7 22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
8 80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
9 MAC Address: 00:0C:29:71:5E:BF (VMware)
10 Service Info: OS: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
11
12 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
13 # Nmap done at Tue Jul 18 09:35:22 2023 -- 1 IP address (1 host up) scanned in 7.23 seconds
14 # 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
15 Nmap scan report for 192.168.136.171
16 Host is up (0.000066s latency).
17 Not shown: 3 closed tcp ports (reset)
18 PORT      STATE SERVICE VERSION
19 22/tcp    open  ssh      OpenSSH 9.3p1 Debian 1 (protocol 2.0)
20 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
21
22 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
23 # Nmap done at Tue Jul 18 09:35:23 2023 -- 1 IP address (1 host up) scanned in 0.91 seconds
24 # 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
25 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
26 # Nmap done at Tue Jul 18 09:35:15 2023 -- 1 IP address (1 host up) scanned in 1.47 seconds
27
```



vulnerabilitie...168.136.171.txt x

vulnerabilitie...168.136.159.txt x

vulnerabilitie...2.168.136.2.txt x

```
1 # 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
2 Nmap scan report for 192.168.136.171
3 Host is up (0.000066s latency).
4 Not shown: 3 closed tcp ports (reset)
5 PORT      STATE SERVICE VERSION
6 22/tcp    open  ssh      OpenSSH 9.3p1 Debian 1 (protocol 2.0)
7 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
8
9 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
10 # Nmap done at Tue Jul 18 09:35:23 2023 -- 1 IP address (1 host up) scanned in 0.91 seconds
11
```

```
1 # 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
2 Nmap scan report for 192.168.136.159
3 Host is up (0.00042s latency).
4 Not shown: 1 closed tcp port (reset)
5 PORT      STATE SERVICE VERSION
6 21/tcp    open  ftp      vsftpd 2.3.4
7 22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
8 80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
9 MAC Address: 00:0C:29:71:5E:BF (VMware)
10 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
11
12 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
13 # Nmap done at Tue Jul 18 09:35:22 2023 -- 1 IP address (1 host up) scanned in 7.23 seconds
14
```

vulnerabilitie...2.168.136.2.txt x

```
1 # 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
2 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
3 # Nmap done at Tue Jul 18 09:35:15 2023 -- 1 IP address (1 host up) scanned in 1.47 seconds
4
```