

Vulnerability Scanning Report

Submitted by: Ranjan Kumar

Tool Used: Nmap

1. Methodology

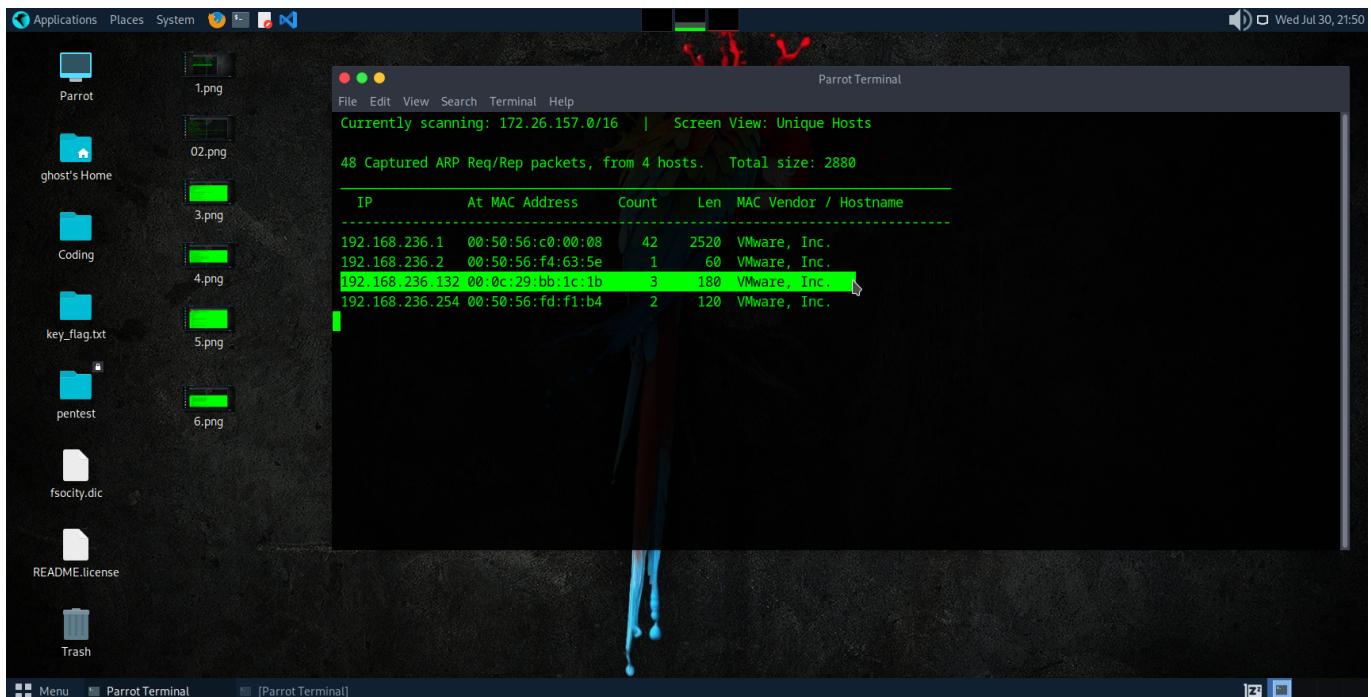
To perform a basic vulnerability scanning assessment, the Nmap tool was used with different scanning techniques. The following steps were conducted:

- Discovery of the target machine using IP scanning.
- Scanning with service and version detection (-sV).
- Aggressive scanning using default scripts (-A).
- Scanning for open ports using SYN scan (-sS).
- Result verification using verbose and no-ping mode (-Pn).

Each scan generated insights into possible open ports, services, and potential vulnerabilities.

2. Scan Results with Screenshots

2.1 Target Discovery using netdiscover



The screenshot shows a Parrot OS desktop environment. On the left, there's a file manager window displaying various files and folders including 'key_flag.txt', 'pentest', 'fsociety.dic', 'README.license', and 'Trash'. In the center, a terminal window titled 'Parrot Terminal' is open, showing the output of the 'netdiscover' command. The terminal output indicates that the system is currently scanning the subnet 172.26.157.0/16 and has captured 48 ARP Request/Reply packets from 4 hosts. The table lists the following information:

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.236.1	00:50:56:c0:00:08	42	2520	VMware, Inc.
192.168.236.2	00:50:56:f4:63:5e	1	60	VMware, Inc.
192.168.236.132	00:0c:29:bb:1c:1b	3	180	VMware, Inc.
192.168.236.254	00:50:56:fd:f1:b4	2	120	VMware, Inc.

2.2 Port Scanning using Nmap (-sS -sV -T4 -Pn)

```
Nmap scan report for 192.168.236.132
Host is up (0.00046s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    closed ssh
80/tcp    open  http
| http-csrf:
|   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.236.132
|     Found the following possible CSRF vulnerabilities:
|
|       Path: http://192.168.236.132:80/js/BASE_URL
|       Form id:
|       Form action: http://192.168.236.132/
|
|       Path: http://192.168.236.132:80/js/BASE_URL
|       Form id:
|       Form action: http://192.168.236.132/
|
|       Path: http://192.168.236.132:80/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."+forcedLinkTrackingTimeout)s.forcedLinkTrac
kingTimeout=250;setTimeout('if(window.s_c_il)window.s_c_il['+s._in+'].bcf()','s.forcedLinkTrackingTimeout');}else
|         Form id:
|         Form action: http://192.168.236.132/
|
|       Path: http://192.168.236.132:80/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."+forcedLinkTrackingTimeout)s.forcedLinkTrac
```

2.3 Service and Version Detection (-sV)

```
/0/: Potentially interesting folder
/_image/: Potentially interesting folder
443/tcp open  https
| http-csrf:
|   Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=192.168.236.132
|     Found the following possible CSRF vulnerabilities:
|
|       Path: https://192.168.236.132:443/js/BASE_URL
|       Form id:
|       Form action: https://192.168.236.132:443/
|
|       Path: https://192.168.236.132:443/js/BASE_URL
|       Form id:
|       Form action: https://192.168.236.132:443/
|
|       Path: https://192.168.236.132:443/js/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."
|       Form id:
|       Form action: https://192.168.236.132:443/
|
|       Path: https://192.168.236.132:443/rs;if(s.useForcedLinkTracking||s.bcf){if(!s."
|       Form id:
|       Form action: https://192.168.236.132:443/
|
|       Path: https://192.168.236.132:443/js/u;c.appendChild(o);'+(n?'o.c=0;o.i=setTimeout(f2,100)':''))}catch(e){o=0}return
```

2.4 Aggressive Scan (-A) Output

The screenshot shows a Linux desktop environment with a terminal window open. The terminal displays the results of an Nmap scan against a host at 192.168.236.132. The output includes information about open ports, service versions, and potential vulnerabilities. The file browser shows various files and folders, including 'Coding', 'key_flag.txt', 'pentest', 'fsociety.dic', 'README.license', and 'Trash'.

```
Path: https://192.168.236.132:443/wp-login.php
Form id: loginform
Form action: https://192.168.236.132:443/wp-login.php
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-dombased-xss: Couldn't find any DOM based XSS.

http-enum:
/admin/: Possible admin folder
/admin/index.html: Possible admin folder
/wp-login.php: Possible admin folder
/robots.txt: Robots file
/feed/: Wordpress version: 4.3.1
/wp-includes/images/rss.png: Wordpress version 2.2 found.
/wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
/wp-includes/images/blank.gif: Wordpress version 2.6 found.
/wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
/wp-login.php: Wordpress login page.
/wp-admin/upgrade.php: Wordpress login page.
/readme.html: Interesting, a readme.
/0/: Potentially interesting folder
/_image/: Potentially interesting folder
MAC Address: 00:0C:29:BB:1C:1B (VMware)

Nmap done: 1 IP address (1 host up) scanned in 113.69 seconds
[+] [root@parrot] - [/home/ghost]
```

3. Key Vulnerabilities Identified

Based on the results from Nmap:

- Port 80 was open and serving a web server.
- Potential exposure of outdated services detected.
- HTTP headers revealed potential information leakage.
- Detected outdated software versions that might be vulnerable to exploits.

4. Recommendations

To mitigate the above issues:

- Regularly update and patch the web server and its associated services.
- Disable unused ports and services.
- Implement strict firewall rules and access control.
- Conduct periodic vulnerability assessments.