

Warren's PT Project

Goal: To discover devices on the network and then run a scan to find open ports. User can then choose which network and port they would like to scan for vulnerabilities, and if a login service is available, brute force it. The results are then compiled into a report which can be view using the script.

Tools: netmask, nmap, hydra

Created by: Warren Justin Chan

Before starting..

```
(kali㉿kali)-[~/CFC3110/ProjectVuln]
$ ls
passwords.txt  usernames.txt  WarrenPTCFC3110.sh

(kali㉿kali)-[~/CFC3110/ProjectVuln]
$
```

Before we begin, we can see that there are only 3 files in the folder, after we run the script there will be created usernames, passwords, and report files created which will be viewed at the end of this document.

```
SYNOPSIS: 1. Start Vulnerability Scanner (Nmap) + Brute Force Attack (Hydra)
2. View Reports
3. Exit

Welcome. How would you like to start?
1. Start Vulnerability Scanner (Nmap) + Brute Force Attack (Hydra)
2. View Reports
3. Exit
```

The user is given 3 choices when starting the script.

Vulnerability Scanner

The expected output is as such:

The script will first ask for the users first IP Address in the network followed by the last IP Address and uses netmask to calculate the CIDR Range

```
28 2. View Reports
29 3. Exit
30
31 read mainmenu
32
33 Erase $mainmenu in
34
35
36
37 function vulnSCANATT
38 echo
39 echo
40
41 Your IP is: 192.168.211.128
42 Your Subnet Mask is: 255.255.255.0
43 Your Broadcast Address is: 192.168.211.255
44
45 Enter the first IP Address within your network: 192.168.211.0
46
47 Enter the last IP Address within your network: 192.168.211.255
48
49 Calculating CIDR Block..
50 Your LAN Range is: 192.168.211.0/24
51
52 Found IP addresses are:
53 192.168.211.2
54 192.168.211.128
55 192.168.211.132
```

The found IP Address are then put into a list file.

Vulnerability Scanner

```
Looking for open ports on each live host:

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 14:35 EDT
Nmap scan report for 192.168.211.12
Host is up (0.00057s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
53/tcp    open  tcpwrapped

Nmap scan report for me (192.168.211.128)
Host is up (0.00051s latency).
All 1000 scanned ports on me (192.168.211.128) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for msf (192.168.211.132)
Host is up (0.0020s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login    OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql    MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc       VNC (protocol 3.3)
6000/tcp  open  X11      (access denied)
6667/tcp  open  irc       UnrealIRCd
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 3 IP addresses (3 hosts up) scanned in 11.54 seconds

Results saved to: PTEnumReport
```

The script then takes the list of IP Addresses that were found in the network and automatically looks for open ports for each IP Address, the results are then saved into a file (PTEnumReport) which can be viewed later on.

Brute Force

```
Enter IP Address to scan for vulnerabilities:
192.168.211.132

Enter Port Number:
22

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 14:41 EDT
Nmap scan report for msf (192.168.211.132)
Host is up (0.00047s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
| cpe:/a:openbsd:openssh:4.7p1:
| SECURITYVULNS:VULN:8166 7.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
| CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
| CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
| SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
| CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
| CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
| CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
| CVE-2008-5161 2.6 https://vulners.com/cve/CVE-2008-5161
| CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
| CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
| SECURITYVULNS:VULN:9455 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
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 0.52 seconds

Results saved to file: 192.168.211.132

Attempting to brute force selected IP and Port...

Would you like to:
A) Use an existing Username and Password list
B) Create a new Username and Password list
```

The user is then prompted for a target IP and specific port. It is then run through a vulnerability checker script through nmap to find potential vulnerabilities for the open port. In this example port 22 (SSH) is used and the output for found vulnerabilities include CVE number, severity rating, and link to the CVE found.

Results of found vulnerabilities are then saved into a file with the name of the target IP in order to facilitate searching

Brute Force

```
Would you like to:
A) Use an existing Username and Password list
B) Create a new Username and Password list
a
Enter Username File:
usernames.txt
Using username file: usernames.txt
Enter Password File:
passwords.txt
Using password file: passwords.txt
Currently supported brute force services:
adam6500 afp asterisk cisco cisco-enable cvs firebird ftp ftps http[s]-{head|get|post}
http[s]-{get|post}-form http-proxy http-proxy-urlenum icq imap[s] irc ldap2[s]
ldap3[-{cram|digest|md5}[s] mssql mysql(v4) mysql5 ncp nntp oracle oracle-listener ora
cle-sid pcanywhere pcnfs pop3[s] postgres rdp radmin2 redis rexec rlogin rpcap rsh rtsp
s7-300 sapr3 sip smb smtp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s]
vmauthd vnc xmpp
Enter login service to brute force:
ssh
Selected login service is: ssh
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t
4
[22][ssh] host: 192.168.211.132 login: msfadmin password: msfadmin
Results saved to file: 192.168.211.132
Would you like to:
1. Run Vulnerability Scanner + Brute Force Attack again
2. Return to Main Menu
3. Exit
```

Users can choose to use a username and password file or to create their own

List of possible login services to brute force through Hydra

Results are saved into target IP file.

Users can then choose if they would like to run the script again or look at a report for the findings.

Brute Force

```
Would you like to:
A) Use an existing Username and Password list
B) Create a new Username and Password list
b
Creating Username List..
Enter minimum number of characters:
2
Enter maximum number of characters:
2
Do you want to specify A) Patterns or B) Symbols/Characters
a
Pattern list:
@ = lower case characters
, = upper case characters
% = numbers
^ = symbols
Enter Pattern:
@,
Crunch will now generate the following amount of data: 2028 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 676
crunch: 100% completed generating output
Username List saved to PTusernames.txt
```

Creating username and password list using crunch then to be used in the Hydra attack.

```
Creating Password List..
Enter minimum number of characters:
2
Enter maximum number of characters:
2
Do you want to specify A) Patterns or B) Symbols/Characters
b
Enter characters/symbols to use:
ad
Crunch will now generate the following amount of data: 12 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 4
crunch: 100% completed generating output
Password List saved to PTpasswords.txt
```


Viewing Reports

```
Select a report to view:  
(NOTE: If this script is being run for the first time, there won't be any reports to be viewed.)  
1. Enumerated LAN Network Report  
2. Vulnerability Scan + Brute Force Report  
█
```

Reports are broken down into two sections, the overall network scan results and the specific targeted IP results.

Enumerated LAN Network Report

```
Select a report to view:
(NOTE: If this script is being run for the first time, there won't be any reports to be viewed.)
1. Enumerated LAN Network Report
2. Vulnerability Scan + Brute Force Report
1
Mon May 8 03:15:02 PM EDT 2023 : Script started
Your LAN Range is: 192.168.211.0/24
Found IP addresses are:
192.168.211.2
192.168.211.128
192.168.211.132
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 15:15 EDT
Nmap scan report for 192.168.211.2
Host is up (0.00066s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped

Nmap scan report for me (192.168.211.128)
Host is up (0.00071s latency).
All 1000 scanned ports on me (192.168.211.128) are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for msf (192.168.211.132)
Host is up (0.0019s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped

1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
```

The Enumerated Report shows results of searches, including time & date of searches and the list of IP Addresses found within the network. This can be accessed to see previous searches as well.

Vulnerability + Brute Force Report

```
Select a report to view:
(NOTE: If this script is being run for the first time, there won't be any reports to be viewed.)
1. Enumerated LAN Network Report
2. Vulnerability Scan + Brute Force Report
2

Enter IP Address:
192.168.211.132
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-08 15:15 EDT
Nmap scan report for msf (192.168.211.132)
Host is up (0.00077s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
vulners:
| cpe:/a:openbsd:openssh:4.7p1:
| SECURITYVULNS:VULN:8166 7.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
| CVE-2010-4478 7.5 https://vulners.com/cve/CVE-2010-4478
| CVE-2008-1657 6.5 https://vulners.com/cve/CVE-2008-1657
| SSV:60656 5.0 https://vulners.com/seebug/SSV:60656 *EXPLOIT*
| CVE-2010-5107 5.0 https://vulners.com/cve/CVE-2010-5107
| CVE-2012-0814 3.5 https://vulners.com/cve/CVE-2012-0814
| CVE-2011-5000 3.5 https://vulners.com/cve/CVE-2011-5000
| CVE-2008-5161 2.6 https://vulners.com/cve/CVE-2008-5161
| CVE-2011-4327 2.1 https://vulners.com/cve/CVE-2011-4327
| CVE-2008-3259 1.2 https://vulners.com/cve/CVE-2008-3259
| SECURITYVULNS:VULN:9455 0.0 https://vulners.com/securityvulns/SECURITYVULNS:VULN:9455
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 0.54 seconds
Using username file: usernames.txt
Using password file: passwords.txt
Selected login service is: ssh
[22][ssh] host: 192.168.211.132 login: msfadmin password: msfadmin

Would you like to:
1. Return to Previous Menu
2. Return to Main Menu
3. Exit
```

Vulnerability scan report can be viewed via keying in the targeted IP Address.

Results of the Hydra attack are also recorded. If there are no results, that means the attack was unsuccessful.

Misc.

```
(kali㉿kali)-[~/CFC3110/ProjectVuln]
$ ls
192.168.211.132  PTEnumReport  PTpasswords.txt  usernames.txt
passwords.txt    PTiplist.lst  PTusernames.txt  WarrenPTCFC3110.sh

(kali㉿kali)-[~/CFC3110/ProjectVuln] [ $usrCrunchpattern = A ] || [ $
$
```

After running the script we can now see several files created to supplement the running of the script and the generated reports.