CFC Project 5 (Vulner)

CFC020823

Penetration testing

Zulkarnaen

S17

Table of contents

Introduction

Objectives of this project:

1. To automate the penetration testing of a network using 1 script.
2. Allow user to choose between 2 types of scan to run on the network.

- Basic: scans the network for TCP and UDP, including the service version and weak passwords.
- Full: include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.

3. Login services to be checked are SSH, FTP, Telnet and RDP.

- Provide a built in passwords list and allow user to use their own list.

4. Output the results and allow user to search within it and provide the user an option to zip it.

Methodology

1. Writing the script

1.1 Create a draft script using all functions.

1.2 Create all the functions needed for the script.

1.3 Research for solution if needed. Note down source for later reference.

1.4 Create built in passwords and username lists.

1.5 Create sections for user input.

2. Testing

2.1 Run script and fine tune where neccessary.

Writing the script

1. **Used geany as it is more efficient to write and check at the same time.**
2. **Able to organise script easily and for any user to understand with added comments.**
3. **Script organised in as follows:**

- Functions.
- IP input.
- Output directory input.
- Basic of Full scan.
- Used which passwords list.
- Allow user to search results.
- Allow user to zip results.

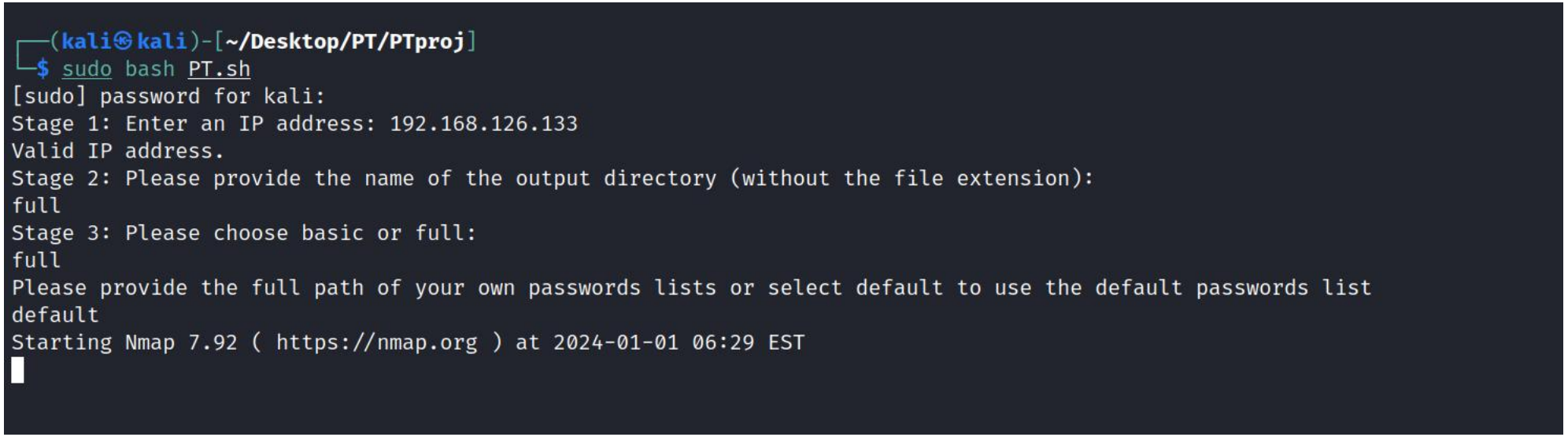
Writing the script

- Comments added to further explain the functions and commands

```
#!/bin/bash

#Functions----------------------

# Function for Basic scan.
# Basic: scans the network for TCP and UDP, including the service version and weak passwords.
# To scan the network for TCP ports and service version, used nmap $user_ip -sV -oN $direc.txt, this is the nmap the ip input by user with flag -sV for version ad -oN to output into the output directory by user.
# To scan for weak passwords, hydra was used for all 4 services (ssh, telnet, ftp and rdp), usernames list is provided, passwords list is provided if user selects default, or uses user's passwords list. flag -t 4 to use
# To scan for UDP ports, used masscan.
function Basic()
{
    nmap $user_ip -sV -oN $direc.txt
    hydra -L top-usernames-shortlist.txt -P $passlst $user_ip ssh >> $direc.txt -t 4 -T 2
    hydra -L top-usernames-shortlist.txt -P $passlst $user_ip telnet >> $direc.txt -t 4 -T 2
    hydra -L top-usernames-shortlist.txt -P $passlst $user_ip ftp >> $direc.txt -t 4 -T 2
    hydra -L top-usernames-shortlist.txt -P $passlst $user_ip rdp >> $direc.txt -t 4 -T 2

    sudo masscan $user_ip -pU:1-10000 >> $direc.txt

}



# Function for Full scan
# Full: include Nmap Scripting Engine (NSE), weak passwords, and vulnerability analysis.
# To scan the network for TCP ports and service version, used nmap $user_ip -sV -oN $direc.txt, this is the nmap the ip input by user with flag -sV for version ad -oN to output into the output directory by user.
# To scan for weak passwords for ssh, telnet, ftp, used brute NSEs with either default passwords list or user passwords list. Output to .txt file and .xml file.
# To scan for weak passwords for rdp, used hydra bruteforce, outpuut to user output directory.
# Used .xml file to automate searchsploit and append results into .txt file.
# To scan for UDP ports, used masscan.
# Used vulners script to access vulnerabilities.
function Full()
{
    nmap $user_ip --script ssh-brute,telnet-brute,ftp-brute,vulners --script-args ssh-brute.passdb=$passlst,telnet-brute.passdb=$passlst,ftp-brute.passdb=$passlst -sV -oN $direc.txt -oX $direc.xml

    hydra -L top-usernames-shortlist.txt -P $passlst $user_ip rdp >> $direc.txt
```

Output in terminal

- Script broken into stages for user reference.



Output in geany (searchable results)

- User able to use ctl+f to search for any part of the results in geany

PT.sh × full.txt ×

```
# Nmap 7.92 scan initiated Mon Jan  1 04:58:54 2024 as: nmap --script ssh-brute,telnet-brute,ftp-brute,vulners --script-args ssh-brute.passdb=darkweb2017-top100.txt,telnet-brute.passdb=darkweb2017-top
Nmap scan report for msf (192.168.126.133)
Host is up (0.0029s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| vulners:
|   cpe:/a:vsftpd:vsftpd:2.3.4:
|       PRION:CVE-2011-2523 10.0    https://vulners.com/prion/PRION:CVE-2011-2523
|       EDB-ID:49757    10.0    https://vulners.com/exploitdb/EDB-ID:49757  *EXPLOIT*
|_      1337DAY-ID-36095    10.0    https://vulners.com/zdt/1337DAY-ID-36095    *EXPLOIT*
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|   Statistics: Performed 16 guesses in 17 seconds, average tps: 0.9
|_  ERROR: The service seems to have failed or is heavily firewalled...
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:4.7p1:
|       SSV:78173   7.8 https://vulners.com/seebug/SSV:78173    *EXPLOIT*
|       SSV:69983   7.8 https://vulners.com/seebug/SSV:69983    *EXPLOIT*
|       EDB-ID:24450    7.8 https://vulners.com/exploitdb/EDB-ID:24450  *EXPLOIT*
|       SECURITYVULNS:VULN:8166 7.5 https://vulners.com/securityvulns/SECURITYVULNS:VULN:8166
|       PRION:CVE-2010-4478 7.5 https://vulners.com/prion/PRION:CVE-2010-4478
|       CVE-2010-4478   7.5 https://vulners.com/cve/CVE-2010-4478
|       SSV:20512   7.2 https://vulners.com/seebug/SSV:20512    *EXPLOIT*
|       PRION:CVE-2011-1013 7.2 https://vulners.com/prion/PRION:CVE-2011-1013
|       PRION:CVE-2008-1657 6.5 https://vulners.com/prion/PRION:CVE-2008-1657
|       CVE-2008-1657   6.5 https://vulners.com/cve/CVE-2008-1657
|       SSV:60656   5.0 https://vulners.com/seebug/SSV:60656    *EXPLOIT*
|       PRION:CVE-2011-2168 5.0 https://vulners.com/prion/PRION:CVE-2011-2168
|       PRION:CVE-2010-5107 5.0 https://vulners.com/prion/PRION:CVE-2010-5107
|       CVE-2010-5107   5.0 https://vulners.com/cve/CVE-2010-5107
|       PRION:CVE-2010-4755 4.0 https://vulners.com/prion/PRION:CVE-2010-4755
|       PRION:CVE-2010-4754 4.0 https://vulners.com/prion/PRION:CVE-2010-4754
|       PRION:CVE-2012-0814 3.5 https://vulners.com/prion/PRION:CVE-2012-0814
```

Output in terminal (zip or not)

- User able to use choose to zip the results.
- If yes, the zip folder name will be the same as the output name.
- If no, script will end.

```
[i] /usr/bin/searchsploit -t unrealircd
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2024-01-01 12:40:05 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [10000 ports/host]
Would you like to zip the results? y/n
y
Output directory name will be zip folder name.
  adding: full.txt (deflated 84%)
```

Discussion & Recommendations

Some pointers regarding this script:

1. Script requires sudo as masscan is used for UDP scanning.
2. Full scan is much faster at scanning compared to basic scan as it uses NSE scripts instead of hydra brute forcing.
3. Hydra brute forcing takes alot of time, shortening the list or reducing the number of services to be scanned may speed up this process.
4. To validate the user's input for IP address, I found the regular expression commonly used for IP addresses. (link in references page)

Conclusion

This script will automate pen testing for a network given by user, however, full scan would be a significantly faster scan and provides more information such as vulnerabilities through searchsploit and vulners NSE script.

References

- https://www.oreilly.com/library/view/regular-expressions-cookbook/9780596802837/ch07s16.html
- Regular expression link used in input validation for IP address