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 computor

    sudo apt install masscan #install masscan on the local computor

    sudo apt install hydra  #install hydra on the local computor

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

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 overrite if already present
     date1=$(date) #store date1 as date of current computor
      echo "Please enter ip for Nmap scan" #prompt user to key in IP
       read ipnmap #store variable for usage of ip when user key in the ip when prompted
        nmap "$ipnmap" -oG ~"$ipnmap"_NmapResult.scan #nmap command with user input of IP and stored output into a file
         printf "$date1: 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 overrite if already present
      date2=$(date) #store date2 as date of current computor
       echo "please enter ip for masscan" #prompt user to key in IP
        read massip #store variable for usage of ip when user key in the ip when prompted
         sudo masscan "$massip" -p 20-100 -oG massresult #masscan command , user need to key in sudo password
          printf "$date2: 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 overrite if already present
      date3=$(date) #store date2 as date of current computor
       echo "please enter username for hydra" #prompt user to key in username of the  victim
        read userH #store variable of the username  that the user key in
         echo "please enter password for hydra" #prompt user to key in password of the  victim
          read passH #store variable of the password that the user key in
           echo "please enter service for hydra" #prompt user to key in the service which the user would like to attack
            read serviceH # store variable of the service the user key in
             echo "please enter Ip address for Hydra" #prompt user to key in ip for the attack
              read ipH #store variable of the IP the user key in
               hydra -l "$userH" -p "$passH" "$serviceH"://"$ipH" -o hydraresult #hydra command after user has keyed in the infomation needed with all the variable
                printf "$date3: Hydra : $ipH\n" >> $HLOG  # printf to output/log stored to a file
                 socsa #repeat the function for continuous/resume
                  ;;
```

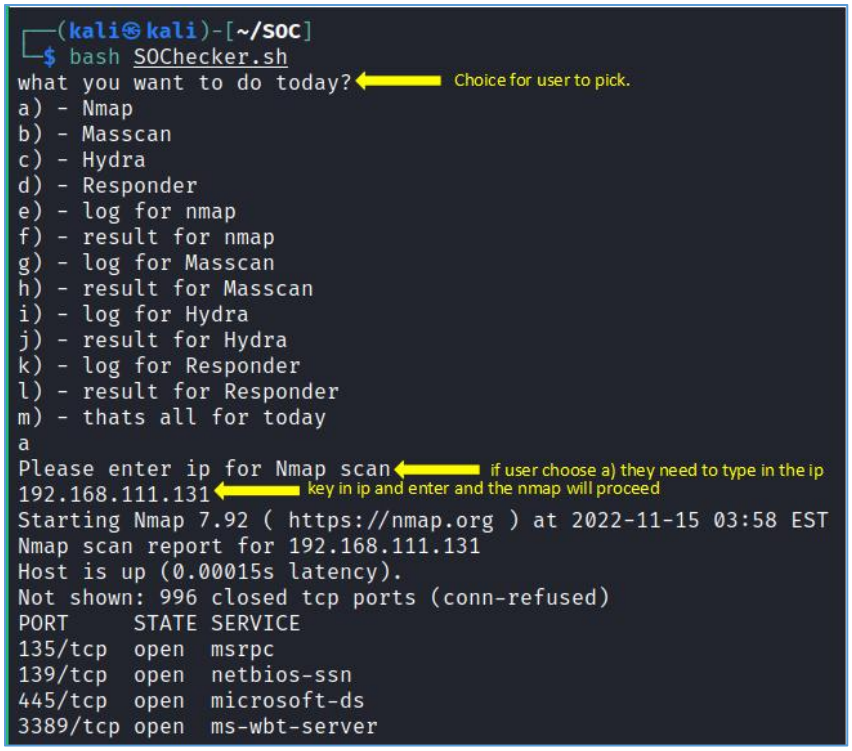
Above is the output of each choices the user can choose

```
d)
   RLOG=res_log # create log file or overrite if already present
    date4=$(date) #store date4 as date of current computor
     sudo responder -I eth0 >> res_result  # responder command , responder will start to listen at the victim machine so it will appear nothing. until theres a activities
      printf "$date4: responder : -I eth0\n" >> $RLOG # 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
     ;;
```

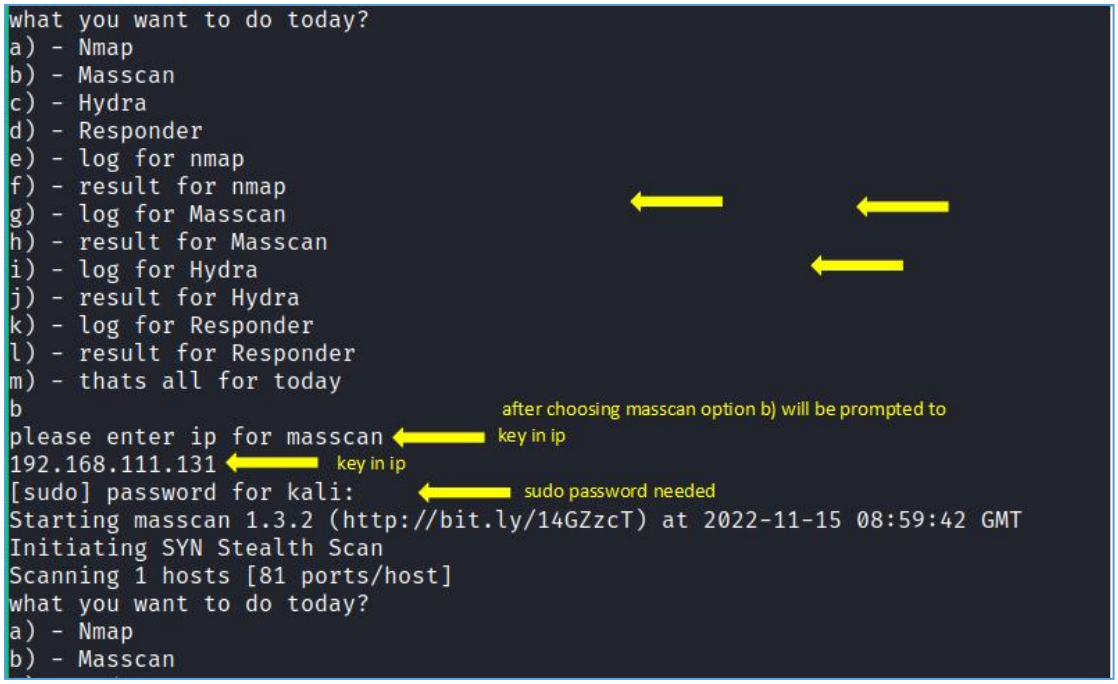
Above is the output of each choices the user can choose
User also can store attack and scan in to logs/file
etc. “e)” from above snapshot

```
      ;;

    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
```

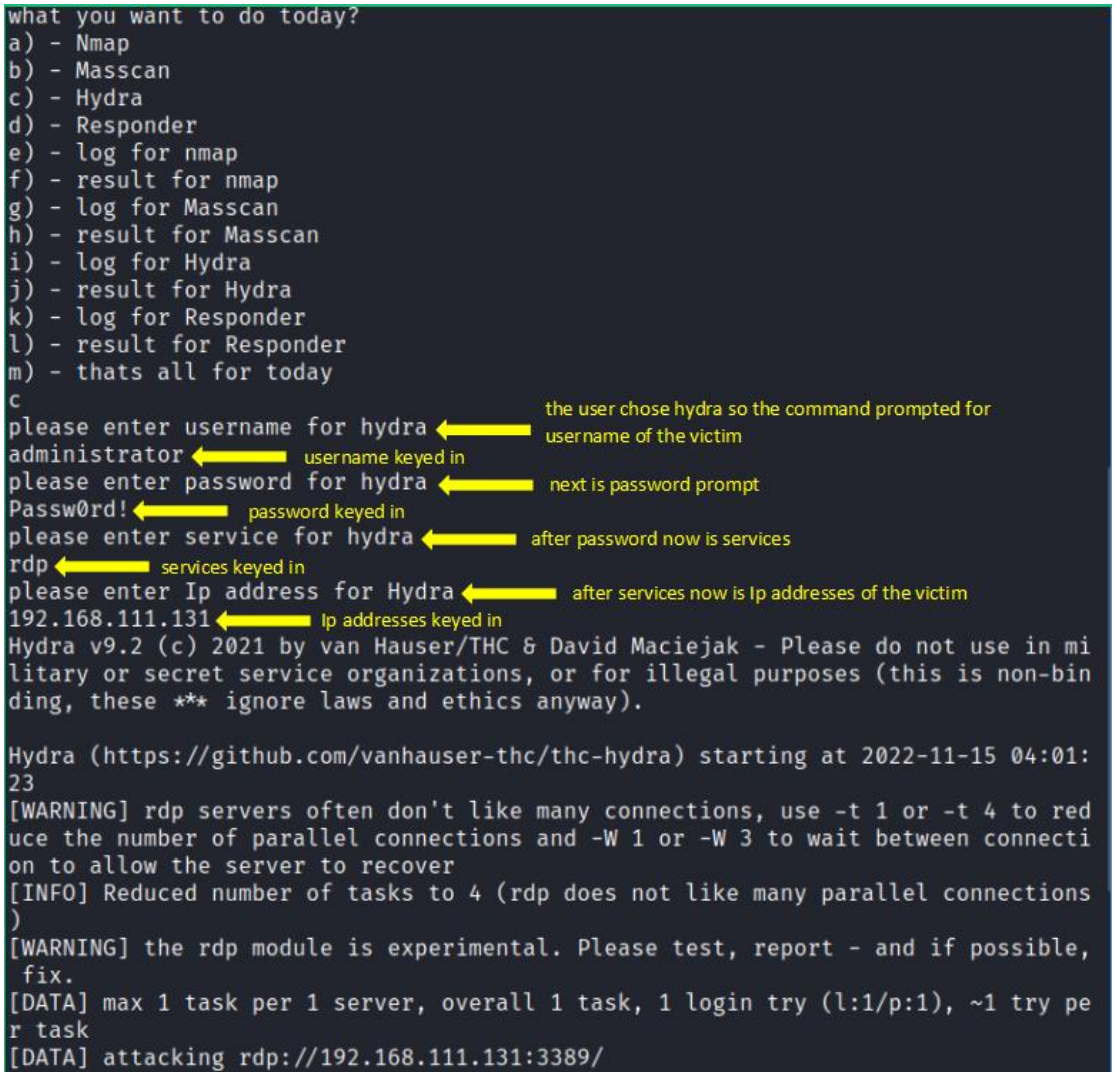
Continue on with the script user can also cat/open the file if they wish to
etc. “j)”



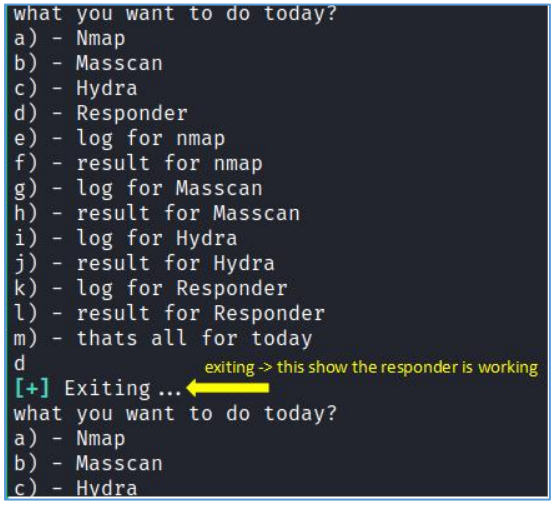
above snapshot show what happen when you select option for nmap
etc. Need to key in IP if prompted



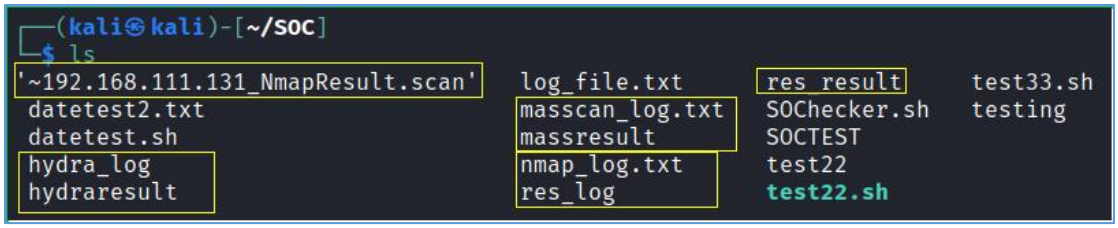
Above snapshot is a example of masscan was selected
need to key in ip and sudo password



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



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



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