Project 1: NIDS Rule Creation and Testing Lab 🕵️

Network Intrusion Detection System (NIDS) Rule Creation and Testing Lab

Problem Statement: Develop and test a robust set of custom rules for a Network Intrusion Detection System (NIDS) to identify and flag common cyber-attacks in real-time, reducing the mean time to detect threats within a network.

Abstract

A concise summary of what you built: a virtualised lab, Snort NIDS on Ubuntu, a Kali attacker, and a custom rule to detect brute-force attempts.

Use Case: Create a virtualized security lab where an open-source NIDS like Snort or Suricata is deployed to monitor network traffic. The system will be configured with custom rules designed to detect specific malicious activities, such as reconnaissance scans, brute-force login attempts, and known malware communication, providing immediate alerts to security analysts for investigation.

Tools & Technologies Used:

- NIDS Engine: Snort,
- Operating System: Kali Linux 2025 (Attacker Machine), Ubuntu Server 24.04.10 (Target Machine)
- Virtualization: VirtualBox
- Attack & Testing Tools: Hydra
- Scripting & Analysis: Bash, Wireshark

Focus Directory are

1. Target Machine (Ubuntu Server)

```
cybermonk@myLap:~ $ cd /etc/snort/rules/local.rules
cybermonk@myLap:~ $ cd /var/log/snort
```

2. Attacker Machine

This guide details how to set up Snort, a Network Intrusion Detection System (NIDS), to detect an SSH brute-force attack.

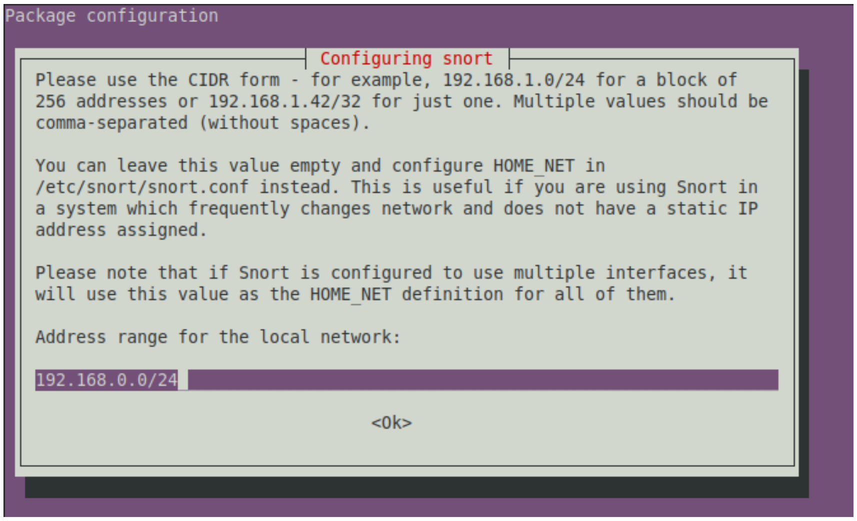
Step 1: Setup and Installation

a. **Install Ubuntu Server:** Use VirtualBox or VMware to create a new virtual machine. Install a minimal Ubuntu Server. Ensure the network adapter is set to "Bridged Mode" to get an IP address from your local network.

b. **Install Snor**t: Once the VM is running, update your package list and install Snort.

```
cybermonk@myLap:~ $sudo apt update
cybermonk@myLap:~ $sudo apt install -y snort
```

c. Configure Network Interface: During installation, you'll be prompted for the network interface to monitor. Enter the name of your primary interface (e.g., eth0 or enp0s3). You can find it by running the ip a command. Also, provide your local network range in CIDR notation (e.g., 192.168.0.0/24).



```
Package configuration

                          Configuring snort
 Please use the CIDR form - for example, 192.168.1.0/24 for a block of
 256 addresses or 192.168.1.42/32 for just one. Multiple values should be
 comma-separated (without spaces).

 You can leave this value empty and configure HOME_NET in
 /etc/snort/snort.conf instead. This is useful if you are using Snort in
 a system which frequently changes network and does not have a static IP
 address assigned.

 Please note that if Snort is configured to use multiple interfaces, it
 will use this value as the HOME_NET definition for all of them.

 Address range for the local network:

 192.168.0.0/24

                                <Ok>
```

Step 2: Create a Custom NIDS Rule

a. **Open the Rules File**: Snort's custom rules can be placed in /etc/snort/rules/local.rules. Open this file with a text editor like nano.

```
cybermonk@myLap:~ $sudo vim /etc/snort/rules/local.rules
```

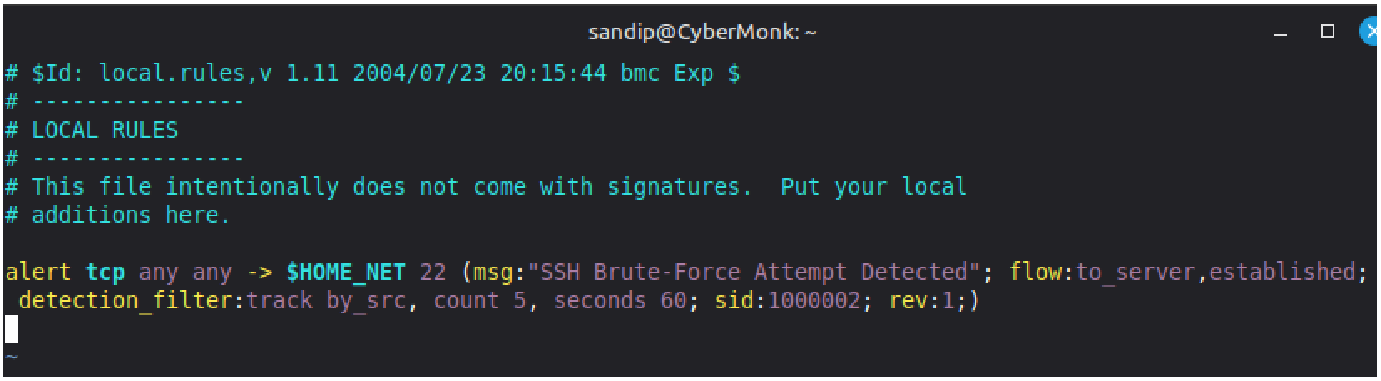
b. **Add a Brute-Force Rule:** Add the following rule to the bottom of the file. This rule alerts if it sees more than 5 connection attempts to the SSH port (22) from the same source IP within 60 seconds.

```
alert tcp any any -> $HOME_NET 22 (msg:"SSH Brute-Force Attempt Detected";
flow:to_server,established; detection_filter:track by_src, count 5, seconds 60;
sid:1000002; rev:1;)
```

Meaning in plain English:

*“Raise an alert if any external host makes 5 or more SSH (TCP/22) connection attempts to my home network within 60 seconds, as part of an established session.”*Meaning in plain English:

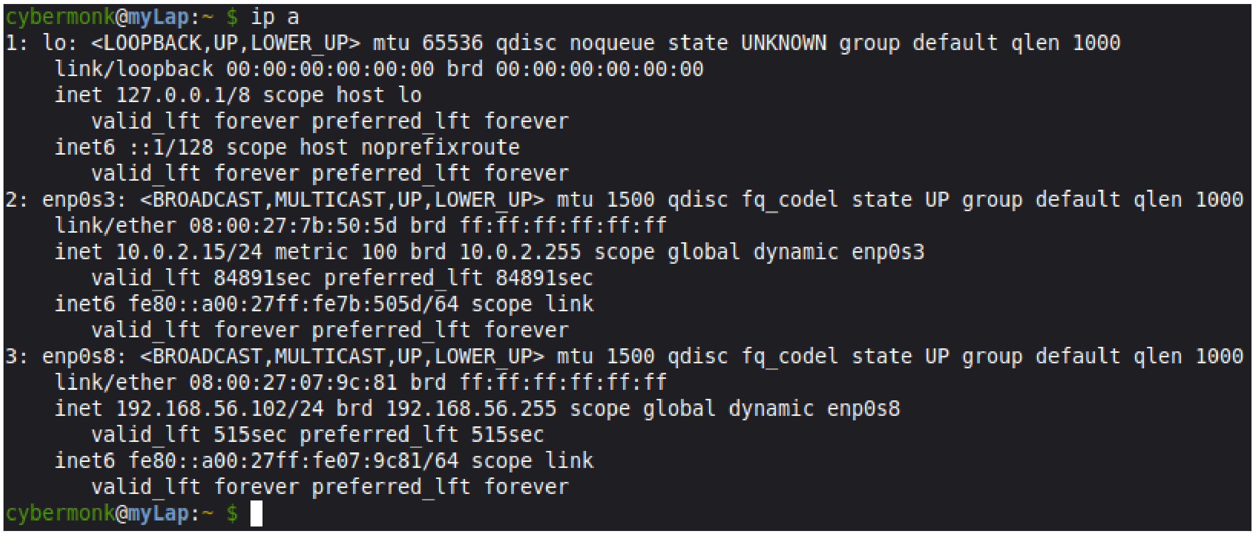
“Raise an alert if any external host makes 5 or more SSH (TCP/22) connection attempts to my home network within 60 seconds, as part of an established session.”



```
# $Id: local.rules,v 1.11 2004/07/23 20:15:44 bmc Exp $
# ----------------
# LOCAL RULES
# ----------------
# This file intentionally does not come with signatures.  Put your local
# additions here.

alert tcp any any -> $HOME_NET 22 (msg:"SSH Brute-Force Attempt Detected"; flow:to_server,established;
 detection_filter:track by_src, count 5, seconds 60; sid:1000002; rev:1;)

~
```

Step 3: Test the Rule

a. **Start Snort:** Run Snort in console mode to watch for alerts in real-time. Replace enp0s3 with your network interface.

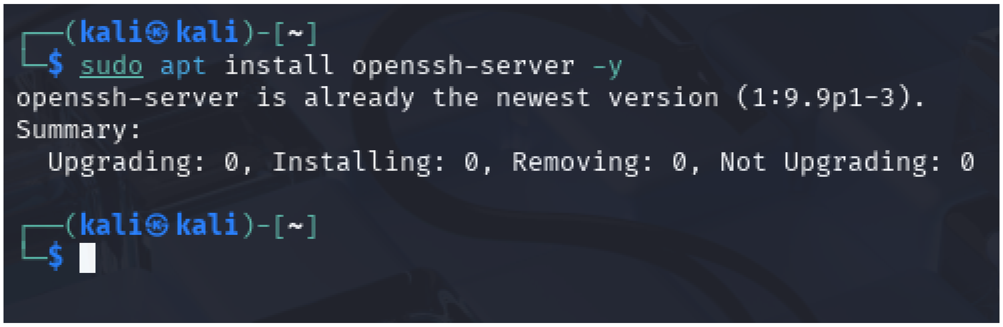


```
cybermonk@myLap:~ $ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:7b:50:5d brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 metric 100 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 84891sec preferred_lft 84891sec
    inet6 fe80::a00:27ff:fe7b:505d/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:07:9c:81 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.102/24 brd 192.168.56.255 scope global dynamic enp0s8
       valid_lft 515sec preferred_lft 515sec
    inet6 fe80::a00:27ff:fe07:9c81/64 scope link
       valid_lft forever preferred_lft forever
cybermonk@myLap:~ $ 
```

cybermonk@myLap:~ $*sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s8*

b**. Install an SSH Serve**r: To attack something, you need an SSH server running on your Snort VM.

kali@kali:~$*sudo apt install -y openssh-server*

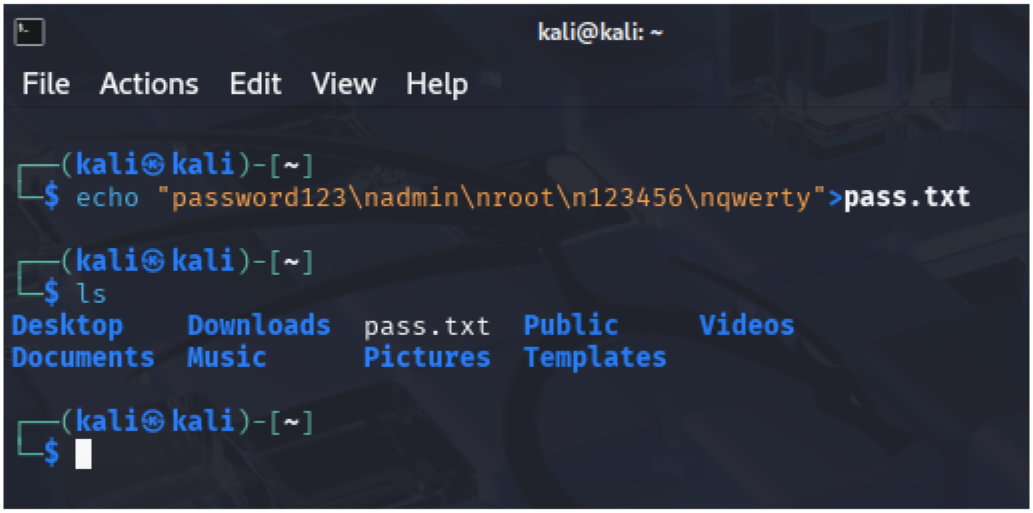


```
┌──(kali㉿kali)-[~]
└─$ sudo apt install openssh-server -y
openssh-server is already the newest version (1:9.9p1-3).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 0

┌──(kali㉿kali)-[~]
└─$ 
```

Step 4. Perform the Attack: From **another machine** on the same network (your host machine or another VM), use a tool like **Hydra** to simulate a brute-force attack. You'll need a dummy password list.

# Create a small password list

kali@kali:~$*echo "password123\nadmin\nroot\n123456\nqwerty" > pass.txt*



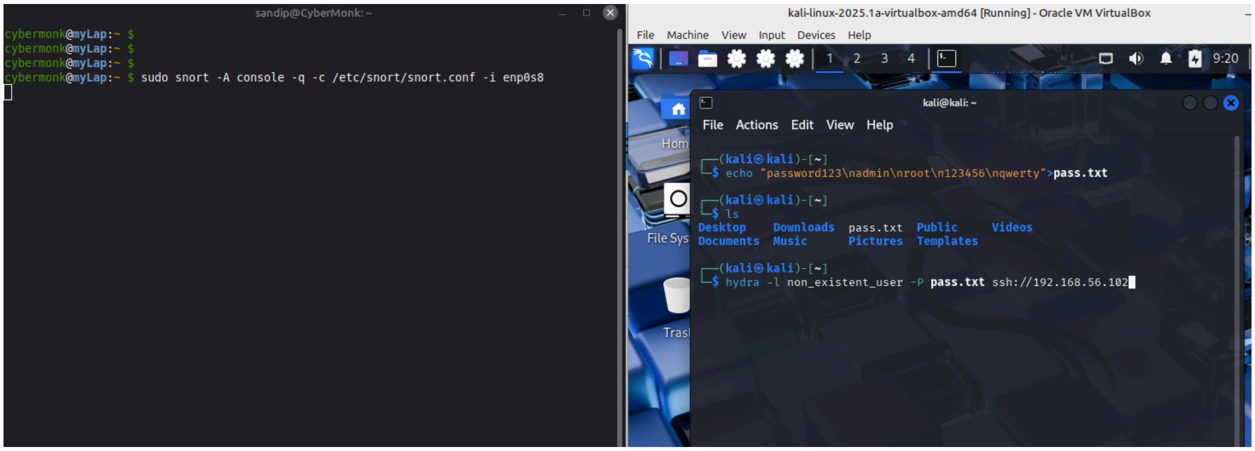
```
┌──(kali㉿kali)-[~]
└─$ echo "password123\nadmin\nroot\n123456\nqwerty">pass.txt

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  pass.txt  Public     Videos
Documents  Music      Pictures  Templates

┌──(kali㉿kali)-[~]
└─$ 
```

# Run Hydra (replace <VM_IP> with the Ubuntu VM's IP address)

kali@kali:~$hydra -l non_existent_user -P pass.txt ssh://<VM_IP>

So,

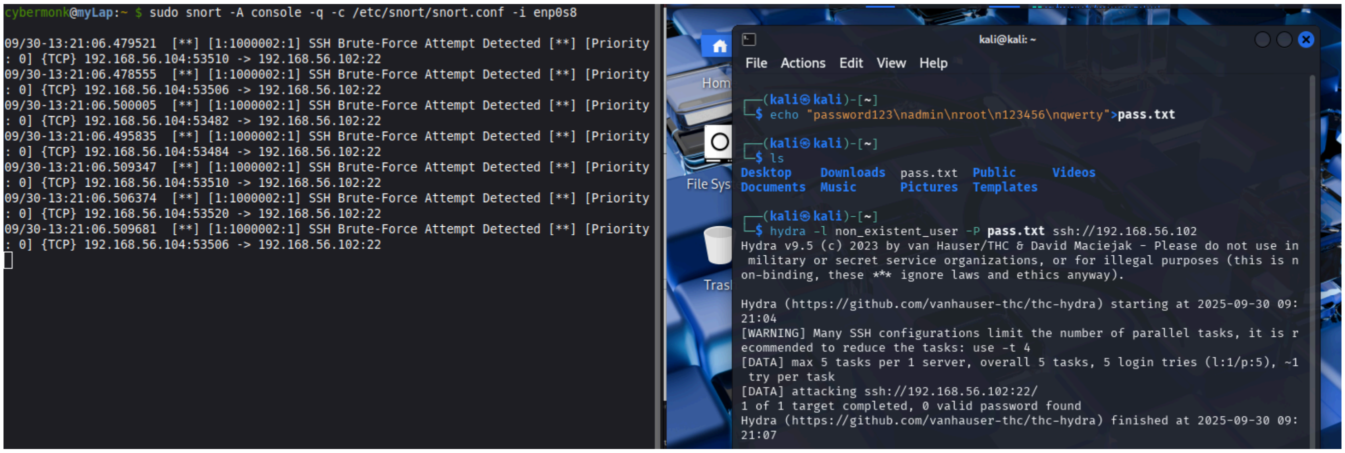
kali@kali:~$*hydra -l non_existent_user -P pass.txt ssh://192.168.56.102*


sandip@CyberMonk: ~
kali-linux-2025.1a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
9:20
Hom
File Sys
Tras
kali@kali: ~
File Actions Edit View Help

```
cybermonk@myLap:~ $
cybermonk@myLap:~ $
cybermonk@myLap:~ $
cybermonk@myLap:~ $ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s8
```

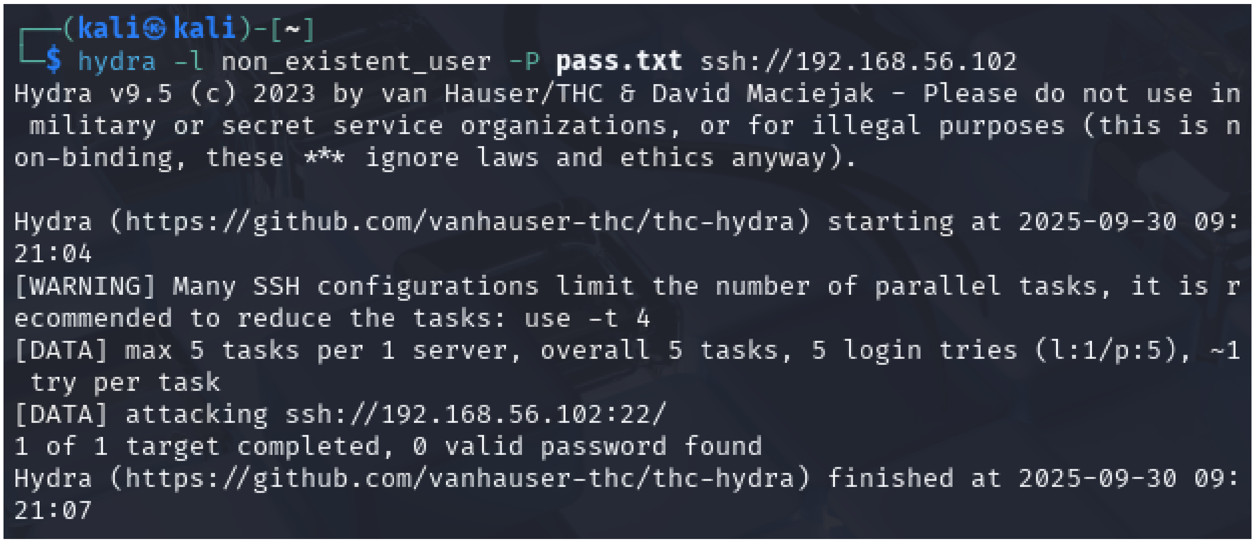
```
┌──(kali㉿kali)-[~]
└─$ echo "password123\nadmin\nroot\n123456\nqwerty">pass.txt

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  pass.txt  Public     Videos
Documents  Music      Pictures  Templates

┌──(kali㉿kali)-[~]
└─$ hydra -l non_existent_user -P pass.txt ssh://192.168.56.102
```

b. **Verify the Alert:** Watch the console where Snort is running. After a few seconds of the Hydra attack, you will see the alert message "**SSH Brute-Force Attempt Detected**" appear multiple times.



```
cybermonk@myLap:~ $ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s8

09/30-13:21:06.479521  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority
: 0] {TCP} 192.168.56.104:53510 -> 192.168.56.102:22
09/30-13:21:06.478555  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority
: 0] {TCP} 192.168.56.104:53506 -> 192.168.56.102:22
09/30-13:21:06.500005  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority
: 0] {TCP} 192.168.56.104:53482 -> 192.168.56.102:22
09/30-13:21:06.495835  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority
: 0] {TCP} 192.168.56.104:53484 -> 192.168.56.102:22
09/30-13:21:06.509347  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority
: 0] {TCP} 192.168.56.104:53510 -> 192.168.56.102:22
09/30-13:21:06.506374  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority
: 0] {TCP} 192.168.56.104:53520 -> 192.168.56.102:22
09/30-13:21:06.509681  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority
: 0] {TCP} 192.168.56.104:53506 -> 192.168.56.102:22
```

```
┌──(kali㉿kali)-[~]
└─$ echo "password123\nadmin\nroot\n123456\nqwerty">pass.txt

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads  pass.txt  Public     Videos
Documents  Music      Pictures  Templates

┌──(kali㉿kali)-[~]
└─$ hydra -l non_existent_user -P pass.txt ssh://192.168.56.102
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-30 09:
21:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1
 try per task
[DATA] attacking ssh://192.168.56.102:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-30 09:
21:07
```



```
┌──(kali㉿kali)-[~]
└─$ hydra -l non_existent_user -P pass.txt ssh://192.168.56.102
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-09-30 09:
21:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1
 try per task
[DATA] attacking ssh://192.168.56.102:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-30 09:
21:07
```

```
cybermonk@myLap:~ $ sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s8
10/03-21:41:35.967629  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0]
{TCP} 192.168.56.104:48994 -> 192.168.56.102:22
10/03-21:41:35.967313  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0]
{TCP} 192.168.56.104:48988 -> 192.168.56.102:22
10/03-21:41:35.990411  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0]
{TCP} 192.168.56.104:48960 -> 192.168.56.102:22
10/03-21:41:35.988153  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0]
{TCP} 192.168.56.104:48966 -> 192.168.56.102:22
10/03-21:41:36.008844  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0]
{TCP} 192.168.56.104:48972 -> 192.168.56.102:22
10/03-21:41:36.012344  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0]
{TCP} 192.168.56.104:48994 -> 192.168.56.102:22
10/03-21:41:36.013830  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0]
{TCP} 192.168.56.104:48988 -> 192.168.56.102:22
```

To View in the server Log

cybermonk@myLap:.../log/snort $ *ls*

```
snort.alert snort.alert.fast  snort.log  snort.log.1759238389  snort.log.1759527594
```

Step 5: Scripting & Analysis: snort.log.1759527594

To View in the server Log

cybermonk@myLap:.../log/snort $ *ls*

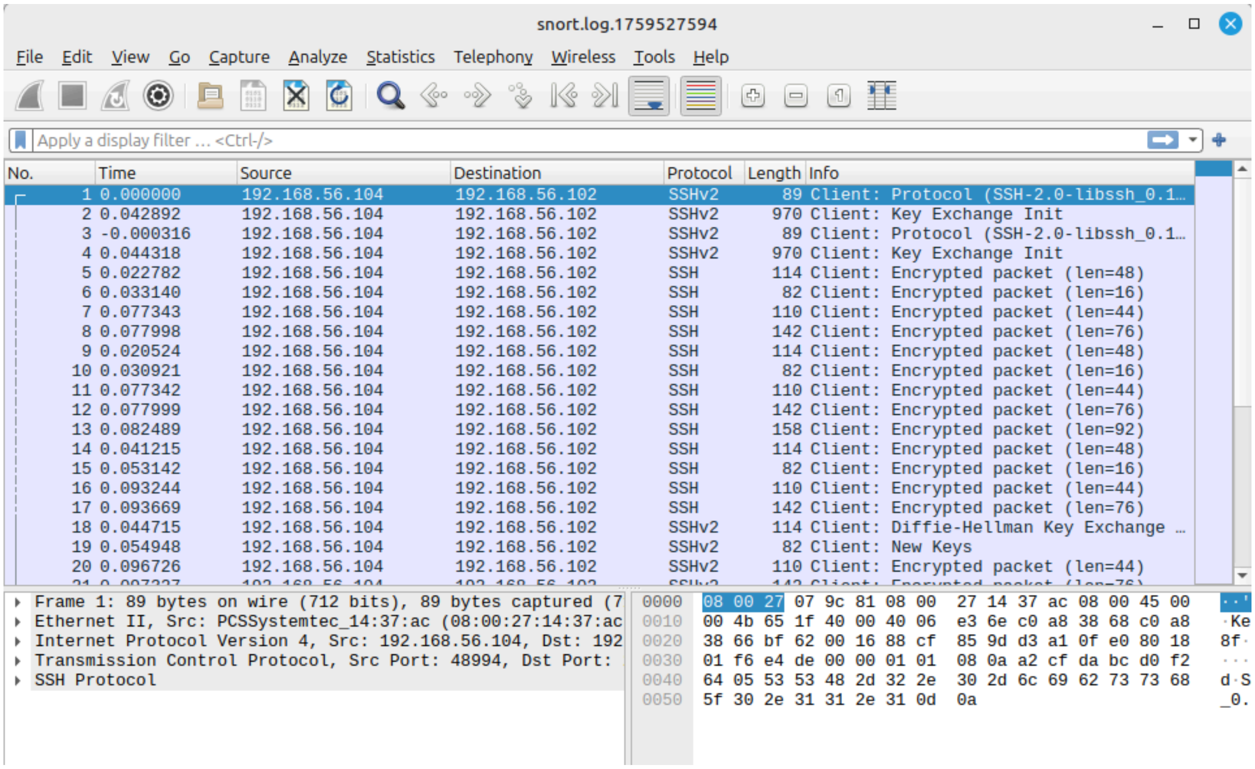
```
snort.alert snort.alert.fast  snort.log  snort.log.1759238389  snort.log.1759527594
```

a. Bash Command:

Since the file is not in a Human Readable so to be converted into a human-readable format

cybermonk@myLap:~ $ *sudo snort -r /var/log/snort/snort.log.1759527594 &> /home/cybermonk/snort-log.txt*

b. Wireshark packet analysis



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.56.104	192.168.56.102	SSHv2	89	Client: Protocol (SSH-2.0-libssh_0.1…
2	0.042892	192.168.56.104	192.168.56.102	SSHv2	970	Client: Key Exchange Init
3	-0.000316	192.168.56.104	192.168.56.102	SSHv2	89	Client: Protocol (SSH-2.0-libssh_0.1…
4	0.044318	192.168.56.104	192.168.56.102	SSHv2	970	Client: Key Exchange Init
5	0.022782	192.168.56.104	192.168.56.102	SSH	114	Client: Encrypted packet (len=48)
6	0.033140	192.168.56.104	192.168.56.102	SSH	82	Client: Encrypted packet (len=16)
7	0.077343	192.168.56.104	192.168.56.102	SSH	110	Client: Encrypted packet (len=44)
8	0.077998	192.168.56.104	192.168.56.102	SSH	142	Client: Encrypted packet (len=76)
9	0.020524	192.168.56.104	192.168.56.102	SSH	114	Client: Encrypted packet (len=48)
10	0.030921	192.168.56.104	192.168.56.102	SSH	82	Client: Encrypted packet (len=16)
11	0.077342	192.168.56.104	192.168.56.102	SSH	110	Client: Encrypted packet (len=44)
12	0.077999	192.168.56.104	192.168.56.102	SSH	142	Client: Encrypted packet (len=76)
13	0.082489	192.168.56.104	192.168.56.102	SSH	158	Client: Encrypted packet (len=92)
14	0.041215	192.168.56.104	192.168.56.102	SSH	114	Client: Encrypted packet (len=48)
15	0.053142	192.168.56.104	192.168.56.102	SSH	82	Client: Encrypted packet (len=16)
16	0.093244	192.168.56.104	192.168.56.102	SSH	110	Client: Encrypted packet (len=44)
17	0.093669	192.168.56.104	192.168.56.102	SSH	142	Client: Encrypted packet (len=76)
18	0.044715	192.168.56.104	192.168.56.102	SSHv2	114	Client: Diffie-Hellman Key Exchange …
19	0.054948	192.168.56.104	192.168.56.102	SSHv2	82	Client: New Keys
20	0.096726	192.168.56.104	192.168.56.102	SSHv2	110	Client: Encrypted packet (len=44)

```
▸ Frame 1: 89 bytes on wire (712 bits), 89 bytes captured (7
▸ Ethernet II, Src: PCSSystemtec_14:37:ac (08:00:27:14:37:ac
▸ Internet Protocol Version 4, Src: 192.168.56.104, Dst: 192
▸ Transmission Control Protocol, Src Port: 48994, Dst Port:
▸ SSH Protocol
```

```
0000  08 00 27 07 9c 81 08 00  27 14 37 ac 08 00 45 00   ··'
0010  00 4b 65 1f 40 00 40 06  e3 6e c0 a8 38 68 c0 a8   ·Ke
0020  38 66 bf 62 00 16 88 cf  85 9d d3 a1 0f e0 80 18   8f·
0030  01 f6 e4 de 00 00 01 01  08 0a a2 cf da bc d0 f2   ···
0040  64 05 53 53 48 2d 32 2e  30 2d 6c 69 62 73 73 68   d·S
0050  5f 30 2e 31 31 2e 31 0d  0a                        _0.
```

Reference

https://medium.com/@huglertomgaw/snort-tryhackme-fab9838b715b