Project 1: NIDS Rule Creation and Testing Lab

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

sudo apt update

sudo apt install -y snort

```
40 packages can be upgraded. Run 'apt list --upgradable' to see them.
harsh@harsh-VMware-Virtual-Platform:~$ sudo apt install -y snort
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 libpcre3 oinkmaster snort-common snort-common-libraries snort-rules-default
Suggested packages:
  snort-doc
The following NEW packages will be installed:
  libdaq2t64 libdumbnet1 libluajit-5.1-2 libluajit-5.1-common libnetfilter-queue1 libpcre3 oinkmaster snort snort-common snort-common-libraries
  snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 40 not upgraded.
Need to get 2,666 kB of archives.
After this operation, 11.4 MB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-common all 2.1.0+git20231223.c525bcb+dfsg-1 [49.2 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libluajit-5.1-2 amd64 2.1.0+git20231223.c525bcb+dfsg-1 [275 kB]
Get:3 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libpcre3 amd64 2:8.39-15build1 [248 kB]
Get:4 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common-libraries amd64 2.9.20-0+deb11u1ubuntu1 [899 kB]
Get:5 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-rules-default all 2.9.20-0+deb11u1ubuntu1 [144 kB]
Get:6 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort-common all 2.9.20-0+deb11u1ubuntu1 [47.7 kB]
Get:7 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdumbnet1 amd64 1.17.0-1ubuntu2 [30.7 kB]
Get:8 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libnetfilter-queue1 amd64 1.0.5-4build1 [15.1 kB]
Get:9 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 libdaq2t64 amd64 2.0.7-5.1build3 [92.9 kB]
Get:10 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 snort amd64 2.9.20-0+deb11u1ubuntu1 [791 kB]
Get:11 http://in.archive.ubuntu.com/ubuntu noble/universe amd64 oinkmaster all 2.0-4.2 [71.9 kB]
Fetched 2,666 kB in 2s (1,270 kB/s)
Preconfiguring packages ...
Snort configuration: interface default not set, using 'ens33'
```

Step 2: Create a Custom NIDS Rule

sudo nano /etc/snort/rules/local.rules

```
harsh@harsh-VMware-Virtual-Platform:~$ cd /etc/snort
harsh@harsh-VMware-Virtual-Platform:/etc/snort$ ls
attribute_table.dtd    community-sid-msg.map  gen-msg.map       rules       snort.debian.conf  unicode.map
classification.config  file_magic.conf        reference.config  snort.conf  threshold.conf
harsh@harsh-VMware-Virtual-Platform:/etc/snort$ cd rules
harsh@harsh-VMware-Virtual-Platform:/etc/snort/rules$ ls
attack-responses.rules   community-imap.rules          community-web-attacks.rules  experimental.rules  mysql.rules      rservices.rules   web-client.rules
backdoor.rules           community-inappropriate.rules community-web-cgi.rules     exploit.rules       netbios.rules    scan.rules        web-coldfusion.rules
bad-traffic.rules        community-mail-client.rules   community-web-client.rules   finger.rules        nntp.rules       shellcode.rules   web-frontpage.rules
chat.rules               community-misc.rules          community-web-dos.rules      ftp.rules           oracle.rules     smtp.rules        web-iis.rules
community-bot.rules      community-nntp.rules          community-web-iis.rules      icmp-info.rules     other-ids.rules  snmp.rules        web-misc.rules
community-deleted.rules  community-oracle.rules        community-web-misc.rules     icmp.rules          p2p.rules        sql.rules         web-php.rules
community-dos.rules      community-policy.rules        community-web-php.rules      imap.rules          policy.rules     telnet.rules      x11.rules
community-exploit.rules  community-sip.rules           ddos.rules                   info.rules          pop2.rules       tftp.rules
community-ftp.rules      community-smtp.rules          deleted.rules                local.rules         pop3.rules       virus.rules
community-game.rules     community-sql-injection.rules dns.rules                    misc.rules          porn.rules       web-attacks.rules
community-icmp.rules     community-virus.rules         dos.rules                    multimedia.rules    rpc.rules        web-cgi.rules
harsh@harsh-VMware-Virtual-Platform:/etc/snort/rules$
```

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.

Step 3: Test the Rule

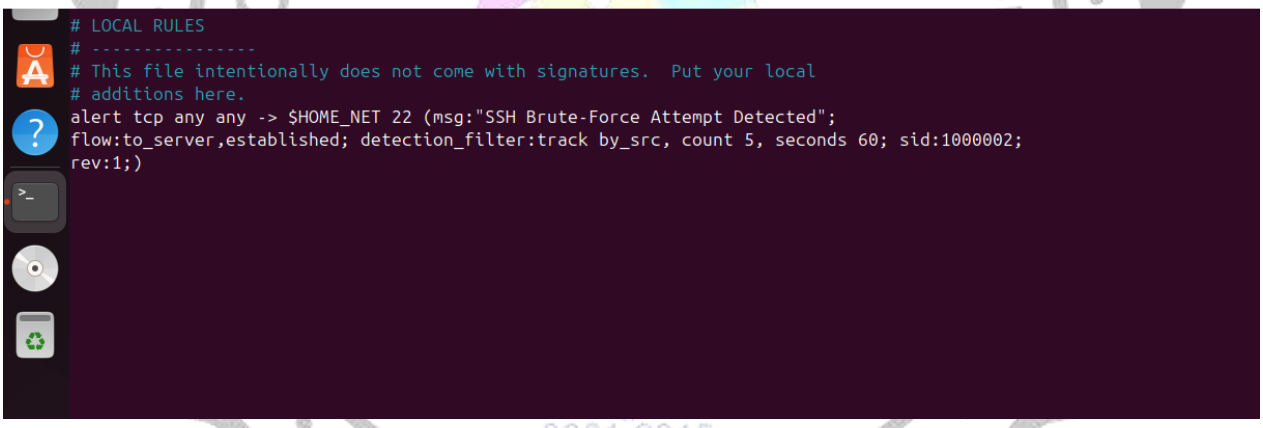
1. **Start Snort**: Run Snort in console mode to watch for alerts in real-time. Replace enp0s3 with your network interface.

sudo snort -A console -q -c /etc/snort/snort.conf -i enp0s3

2. **Install an SSH Server**: To attack something, you need an SSH server running on your Snort VM. *sudo apt install -y openssh-server*

3. **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

echo "password123\nadmin\nroot\n123456\nqwerty" > pass.txt



```
MaxRss at the end of detection rules:104760

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.10.4 (with TPACKET_V3)
           Using PCRE version: 8.39 2016-06-14
           Using ZLIB version: 1.3

           Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_S7COMMPLUS  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>

Total snort Fixed Memory Cost - MaxRss:104760
Snort successfully validated the configuration!
Snort exiting
harsh@harsh-VMware-Virtual-Platform:/etc/snort$
```

4. **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.

```
┌──(harsh㉿kali)-[~]
└─$ nmap -sV 192.168.1.7
tarting Nmap 7.95 ( https://nmap.org ) at 2025-08-30 14:11 EDT
map scan report for 192.168.1.7 (192.168.1.7)
ost is up (0.00039s latency).
ot shown: 999 closed tcp ports (reset)
ORT   STATE SERVICE VERSION
2/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.13 (Ubuntu Linux; protocol 2.0)
AC Address: 00:0C:29:29:BE:B0 (VMware)
ervice Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

ervice detection performed. Please report any incorrect results at https://nmap.org/submit/ .
map done: 1 IP address (1 host up) scanned in 1.96 seconds

┌──(harsh㉿kali)-[~]
└─$
```

```
┌──(harsh㉿kali)-[~]
└─$ hydra -l harsh -P pass.txt 192.168.1.7 ssh
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 2025-08-30 14:
09:33
[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://192.168.1.7:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-08-30 14:
09:37
```

```
etting up openssh-sftp-server (1:9.6p1-3ubuntu13.13) ...
etting up openssh-server (1:9.6p1-3ubuntu13.13) ...

reating config file /etc/ssh/sshd_config with new version
reated symlink /etc/systemd/system/sockets.target.wants/ssh.socket → /usr/lib/systemd/system/ssh.socket.
reated symlink /etc/systemd/system/ssh.service.requires/ssh.socket → /usr/lib/systemd/system/ssh.socket.
etting up ssh-import-id (5.11-0ubuntu2.24.04.1) ...
etting up ncurses-term (6.4+20240113-1ubuntu2) ...
rocessing triggers for man-db (2.12.0-4build2) ...
rocessing triggers for ufw (0.36.2-6) ...
arsh@harsh-VMware-Virtual-Platform:/etc/snort$ sudo snort -A console -q -c /etc/snort/snort.conf -i ens33
8/30-23:39:34.300481  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0] {TCP} 192.168.1.8:49818 -> 192.168.1.7:22
8/30-23:39:34.301254  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0] {TCP} 192.168.1.8:49824 -> 192.168.1.7:22
8/30-23:39:34.362372  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0] {TCP} 192.168.1.8:49804 -> 192.168.1.7:22
8/30-23:39:34.357922  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0] {TCP} 192.168.1.8:49788 -> 192.168.1.7:22
8/30-23:39:34.362378  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0] {TCP} 192.168.1.8:49814 -> 192.168.1.7:22
8/30-23:39:34.374474  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0] {TCP} 192.168.1.8:49818 -> 192.168.1.7:22
8/30-23:39:34.377799  [**] [1:1000002:1] SSH Brute-Force Attempt Detected [**] [Priority: 0] {TCP} 192.168.1.8:49824 -> 192.168.1.7:22
```