Step 1: Update Ubuntu and Install Required Packages

1. Update the package repository:
sudo apt update && sudo apt upgrade -y

2. Install security tools:
sudo apt install snort suricata nmap nikto hydra apache2 -y

3. Enable Apache web server:
sudo systemctl start apache2
sudo systemctl enable apache2

```
Setting up librte-net24:amd64 (23.11-1ubuntu0.1) ...
Setting up librte-ethdev24:amd64 (23.11-1ubuntu0.1) ...
Setting up librte-hash24:amd64 (23.11-1ubuntu0.1) ...
Setting up librte-ip-frag24:amd64 (23.11-1ubuntu0.1) ...
Setting up librte-net-bond24:amd64 (23.11-1ubuntu0.1) ...
Setting up suricata (1:7.0.3-1build3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/suricata.service → /usr/lib/systemd/system/suricata.service.
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.4) ...
student@student-VMware-Virtual-Platform:~$ sudo systemctl start apache2
sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
student@student-VMware-Virtual-Platform:~$
```

Part 1: Configuring Intrusion Detection Systems (IDS)

Step 2: Configure Snort IDS

1. Verify Snort Installation:
snort -V

2. Edit Snort Configuration File:
sudo nano /etc/snort/snort.conf

- Set the HOME_NET to match your network:
  ipvar HOME_NET 10.10.10.0/24
  preprocessor sfportscan: proto { all } scan_type { all } sense_level { low }
  output alert_fast: /var/log/snort/alert

3. Run Snort in IDS Mode:
sudo snort -A console -c /etc/snort/snort.conf -i eth0

(eth0: interface name, check ifconfig for the interface name and IP address)

```
4057 Snort rules read
    3383 detection rules
    0 decoder rules
    0 preprocessor rules
3383 Option Chains linked into 949 Chain Headers
+++++++++++++++++++++++++++++++++++++++++++++++++++

+-------------------[Rule Port Counts]-------------------------------------
|             tcp     udp    icmp      ip
|     src     151      18       0       0
|     dst    3306     126       0       0
|     any     383      48      52      22
|      nc      27       8      15      20
|     s+d      12       5       0       0
+--------------------------------------------------------------------------

+-----------------------[detection-filter-config]-----------------------------
| memory-cap : 1048576 bytes
+-----------------------[detection-filter-rules]------------------------------
| none
----------------------------------------------------------------------------

+-----------------------[rate-filter-config]----------------------------------
| memory-cap : 1048576 bytes
+-----------------------[rate-filter-rules]-----------------------------------
| none
----------------------------------------------------------------------------

+-----------------------[event-filter-config]---------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]---------------------------------
| none
+-----------------------[event-filter-local]----------------------------------
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=10
```

```
+-----------------------[event-filter-config]---------------------------------
| memory-cap : 1048576 bytes
+-----------------------[event-filter-global]---------------------------------
| none
+-----------------------[event-filter-local]----------------------------------
| gen-id=1      sig-id=2523       type=Both      tracking=dst count=10  seconds=10
| gen-id=1      sig-id=1991       type=Limit     tracking=src count=1   seconds=60
| gen-id=1      sig-id=2496       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=3273       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=3152       type=Threshold tracking=src count=5   seconds=2
| gen-id=1      sig-id=2495       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2494       type=Both      tracking=dst count=20  seconds=60
| gen-id=1      sig-id=2275       type=Threshold tracking=dst count=5   seconds=60
| gen-id=1      sig-id=2924       type=Threshold tracking=dst count=10  seconds=60
| gen-id=1      sig-id=2923       type=Threshold tracking=dst count=10  seconds=60
+-----------------------[suppression]----------------------------------------
| none
----------------------------------------------------------------------------
Rule application order: pass->drop->sdrop->reject->alert->log
Verifying Preprocessor Configurations!
WARNING: flowbits key 'ms_sql_seen_dns' is checked but not ever set.
WARNING: flowbits key 'smb.tree.create.lsarpc' is set but not ever checked.
33 out of 1024 flowbits in use.

[ Port Based Pattern Matching Memory ]
+- [ Aho-Corasick Summary ] -----------------------------------
| Storage Format    : Full-Q
| Finite Automaton  : DFA
| Alphabet Size     : 256 Chars
| Sizeof State      : Variable (1,2,4 bytes)
| Instances         : 215
|     1 byte states : 204
|     2 byte states : 11
|     4 byte states : 0
| Characters        : 64755
| States            : 31951
| Transitions       : 863868
| State Density     : 10.6%
| Patterns          : 5041
| Match States      : 3836
| Memory (MB)       : 16.90
|   Patterns        : 0.51
|   Match Lists     : 1.01
|   DFA
|     1 byte states : 1.02
|     2 byte states : 13.96
|     4 byte states : 0.00
+-------------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 1038 ]
pcap DAQ configured to passive.
Acquiring network traffic from "eth0".
Reload thread starting...
Reload thread started, thread 0x7486001bc6c0 (18289)
ERROR: Can't start DAQ (-1) - No such device exists!
Fatal Error, Quitting..
student@student-VMware-Virtual-Platform:~$
```

Part 2: Performing Vulnerability Analysis

Step 3: Scan for Open Ports Using Nmap

1. Identify the Target IP Address:
   ip a

2. Run Nmap Scan:
   nmap -sV -p- 10.10.10.6 (Check for your system IP address here)

```
student@student-VMware-Virtual-Platform:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state
    link/ether 00:0c:29:fb:09:ea brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.253.128/24 brd 192.168.253.255 scope global dynamic nopr
       valid_lft 1131sec preferred_lft 1131sec
    inet6 fe80::20c:29ff:fefb:9ea/64 scope link
       valid_lft forever preferred_lft forever
student@student-VMware-Virtual-Platform:~$ nmap -sV -p- 10.10.10.6
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-27 17:26 IST
Note: Host seems down. If it is really up, but blocking our ping probes,
Nmap done: 1 IP address (0 hosts up) scanned in 3.10 seconds
student@student-VMware-Virtual-Platform:~$ nmap -sV -p- 192.168.253.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-27 17:27 IST
Nmap scan report for student-VMware-Virtual-Platform (192.168.253.128)
Host is up (0.00011s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.58 ((Ubuntu))
443/tcp open  http    Apache httpd 2.4.58
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.81 seconds
student@student-VMware-Virtual-Platform:~$
```

```
student@student-VMware-Virtual-Platform: ~
+ ERROR: Invalid IP '10.10.10.'

+ 0 host(s) tested
student@student-VMware-Virtual-Platform:~$ nikto -h http://192.168.253.128
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          192.168.253.128
+ Target Hostname:    192.168.253.128
+ Target Port:        80
+ Start Time:         2025-03-27 17:27:52 (GMT5.5)
---------------------------------------------------------------------------
+ Server: Apache/2.4.58 (Ubuntu)
+ Server leaks inodes via ETags, header found with file /, fields: 0x29af 0x6315
150d4dc60
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Allowed HTTP Methods: OPTIONS, HEAD, GET, POST
+ OSVDB-561: /server-status: This reveals Apache information. Comment out approp
riate line in httpd.conf or restrict access to allowed hosts.
+ 6544 items checked: 0 error(s) and 4 item(s) reported on remote host
+ End Time:           2025-03-27 17:28:03 (GMT5.5) (11 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
student@student-VMware-Virtual-Platform:~$
```

Step 4: Web Vulnerability Scan Using Nikto

1. Run Nikto Scan:
   nikto -h http://10.10.10.6 (Check for your system IP address here)

```
student@student-VMware-Virtual-Platform:~$ nmap -A 192.168.253.128
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-27 17:29 IST
Nmap scan report for student-VMware-Virtual-Platform (192.168.253.128)
Host is up (0.00017s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT    STATE SERVICE VERSION
80/tcp  open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
443/tcp open  http    Apache httpd 2.4.58
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.58 (Ubuntu)
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.30 seconds
student@student-VMware-Virtual-Platform:~$ sudo cat /var/log/snort/alert
cat: /var/log/snort/alert: No such file or directory
student@student-VMware-Virtual-Platform:~$
```

Part 3: Performing Vulnerability Analysis

Step 5: Simulate Port Scanning Attack

1. Run an aggressive Nmap scan:
   nmap -A 10.10.10.6 (Check for your system IP address here)

2. Check Snort Logs:
sudo cat /var/log/snort/alert

```
student@student-VMware-Virtual-Platform:~$ sudo nano /etc/snort/snort.conf
student@student-VMware-Virtual-Platform:~$ sudo nano /etc/snort/rules/local.rule
student@student-VMware-Virtual-Platform:~$ sudo nano /etc/snort/rules/local.rule
student@student-VMware-Virtual-Platform:~$ sudo cat /var/log/snort/alert
cat: /var/log/snort/alert: No such file or directory
student@student-VMware-Virtual-Platform:~$ sudo cat /var/log/snort/alert
cat: /var/log/snort/alert: No such file or directory
student@student-VMware-Virtual-Platform:~$
```

Step 6: Simulate Port Scanning Attack

1. Run Hydra Brute-Force Attack on SSH:
hydra -L users.txt -P passwords.txt ssh://10.10.10.6

(Please create the user.txt and passwords.txt file by using mkdir command then Add some sample user as “test” and password as “toor” on the 10.10.10.6 system. Perform this attack from another VM like Kali Linux with ip as 10.10.10.4. Please remember all the IPs given may vary from system to system)

2. Check Snort Rules:
sudo nano /etc/snort/snort.conf

include $RULE_PATH/local.rules (Look for this line in the configuration file)

sudo nano /etc/snort/rules/local.rules (Edit this file)

alert tcp any any -> $HOME_NET any (msg:"Port scan detected"; flags:S; threshold: type threshold, track by_src, count 10, seconds 60; sid:1000001; rev:1;)

alert tcp any any -> $HOME_NET 22 (msg:"SSH brute force attack detected"; flow:to_server,established; detection_filter:track by_src, count 5, seconds 30; sid:1000002; rev:1;)

(Add these 2 rules in the local.rules file)

3. Check Snort Logs:
sudo cat /var/log/snort/alert

```
student@student-VMware-Virtual-Platform:~$ sudo tail -f /var/log/snort/alert
tail: cannot open '/var/log/snort/alert' for reading: No such file or directory
tail: no files remaining
student@student-VMware-Virtual-Platform:~$
```

Part 4: Intrusion Analysis and Prevention

Step 7: Analyze IDS Logs

1. View Snort Alerts:
sudo tail -f /var/log/snort/alert

Step 8: Mitigate Vulnerabilities

1. Block Attacker's IP Address:
sudo ufw deny from 10.10.10.4

2. Harden SSH Configuration:
sudo nano /etc/ssh/sshd_config (Please change the following in the file)

PermitRootLogin no
AllowUsers test

3. Restart SSH:
sudo systemctl restart ssh

```
student@student-VMware-Virtual-Platform:~$ sudo ufw deny from 10.10.10.4
Rules updated
student@student-VMware-Virtual-Platform:~$ sudo nano /etc/ssh/sshd_config
student@student-VMware-Virtual-Platform:~$ sudo systemctl restart ssh
Failed to restart ssh.service: Unit ssh.service not found.
student@student-VMware-Virtual-Platform:~$
```