# Dependencies For Setting up Network Honeypot Environment

Setting up a network honeypot environment requires several dependencies to ensure its functionality and security. Here are some of the key dependencies you'll need:

1. Operating System: Choose a suitable operating system for your honeypot environment. Common choices include Linux distributions like Ubuntu, Debian, or CentOS.

2. Virtualization Software: You'll need virtualization software to create and manage virtual machines (VMs) for your honeypot environment. Popular options include VirtualBox, VMware, or KVM.

3. Network Monitoring Tools: To capture network traffic and analyze the activities of potential attackers, you'll need network monitoring tools like Wireshark, snort, tcpdump, or Suricata. These tools help you gain insights into the activities targeting your honeypot.

4. Honeypot Software: Select a honeypot software or framework that suits your needs. There are various options available, each with its own strengths and weaknesses. Some popular choices are:

Honeyd: A low-interaction honeypot that simulates multiple virtual hosts on a network.
Kippo: A SSH honeypot that emulates a vulnerable SSH service to capture and log attacker activities.
Cowrie: A fork of Kippo with added features and improvements.
Dionaea: A honeypot that specializes in capturing and analyzing attacks targeting services like SMB, FTP, HTTP, etc.

Glastopf: A web application honeypot designed to attract and capture attacks targeting web services.

5. Firewall and Network Configuration: Configure your network and firewall rules to ensure that the honeypot environment is isolated from your production network. This prevents any potential compromises from affecting your live systems.

6. Logging and Monitoring: Implement robust logging and monitoring mechanisms to record and analyze the activities within your honeypot environment. Tools like ELK Stack (Elasticsearch, Logstash, Kibana) or Splunk can help you collect, analyze, and visualize logs effectively.

7. Security Updates and Patch Management: Regularly update and patch the software and operating systems in your honeypot environment to address any vulnerabilities or security flaws. This helps maintain the integrity and security of your honeypot setup.

8. Network Segmentation: Consider segmenting your honeypot environment from your internal network to limit the potential impact of any successful attacks. This adds an extra layer of security and reduces the risk of compromising your production systems.

9. Legal Considerations: Be aware of the legal implications of running a honeypot environment. Understand the laws and regulations in your jurisdiction and ensure that you're operating within the legal boundaries.

10. Documentation and Analysis Tools: Establish a process to document and analyze the data collected from your honeypot environment. This can include tools for data analysis, visualization, and reporting to gain insights into the attackers' techniques and motives.

Remember, setting up and maintaining a honeypot environment requires expertise and careful consideration of security risks. It's essential to continuously monitor and update

your honeypot environment to ensure its effectiveness and minimize any potential risks to your infrastructure.

## Configuration Of Network Honeypot

"To configure a network honeypot, you'll need to follow these general steps:

1. Determine your objectives: Clearly define your goals for setting up a honeypot, such as monitoring specific network services or capturing certain types of attacks.

2. Select a suitable honeypot software: Choose a honeypot software or framework that aligns with your objectives. Some popular options include Honeyd, Kippo, Cowrie, Dionaea, and Glastopf. Each honeypot has its own strengths and weaknesses, so choose the one that best suits your needs.

3. Choose an operating system: Select a compatible operating system for your honeypot environment, such as Ubuntu, Debian, or CentOS. Ensure that the chosen OS is supported by the honeypot software you've chosen.

4. Set up virtualization: Install a virtualization software like VirtualBox, VMware, or KVM to create virtual machines (VMs) for your honeypot environment. This allows you to isolate and monitor the activities within the honeypot.

5. Network configuration: Configure your network and firewall settings to isolate the honeypot environment from your production network. This prevents any potential compromises from affecting your live systems. Consider network segmentation for added security.

6. Install and configure the honeypot software: Follow the installation instructions provided by the chosen honeypot software. Configure the software to simulate the desired network services and vulnerabilities.

7. Implement logging and monitoring: Set up robust logging and monitoring mechanisms to capture and analyze the activities within the honeypot environment. Tools like Wireshark, snort, tcpdump, or Suricata can help you capture network traffic and gain insights into attacker activities.

8. Regularly update and patch: Keep the software and operating system in your honeypot environment up to date with the latest security updates and patches. This ensures that any vulnerabilities are addressed promptly.

9. Document and analyze: Establish a process to document and analyze the data collected from your honeypot environment. This can involve using tools like ELK Stack (Elasticsearch, Logstash, Kibana) or Splunk to collect, analyze, and visualize logs effectively.

Remember to consider legal implications and ensure compliance with relevant laws and regulations when running a honeypot environment. It's also crucial to continuously monitor and update your honeypot setup to maintain its effectiveness and minimize potential risks.

# Now lets Create a Simple Network Honeypot

NOTE: I'm not going to use any honeypot software or vulnerable os , i'm just showing you how you can create a customizable honeypot.

I'm going to create a SSH Network Honeypot,

Requirement:

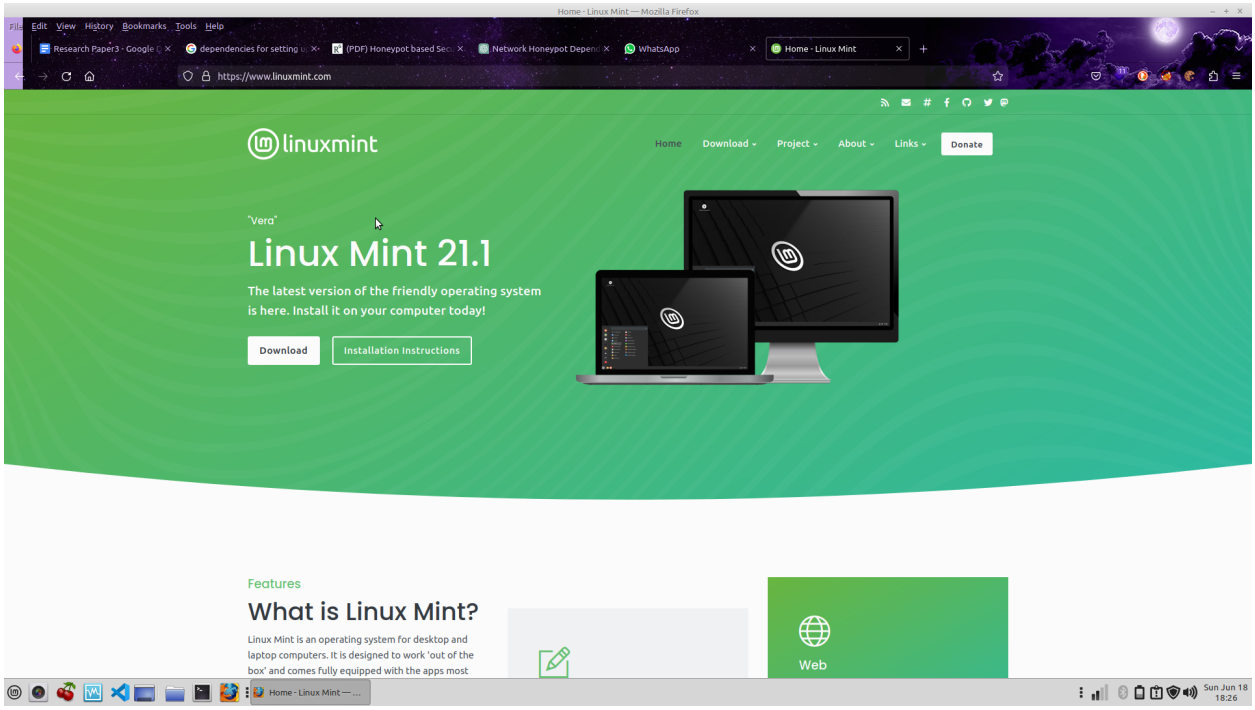
1. Linux/Ubuntu Os,
2. VM
3. Monitoring Tool (i'm going to use snort)

**Step1**

Lets Install Linux Mint (You can install any ubuntu os)

Visit below link

https://www.linuxmint.com/

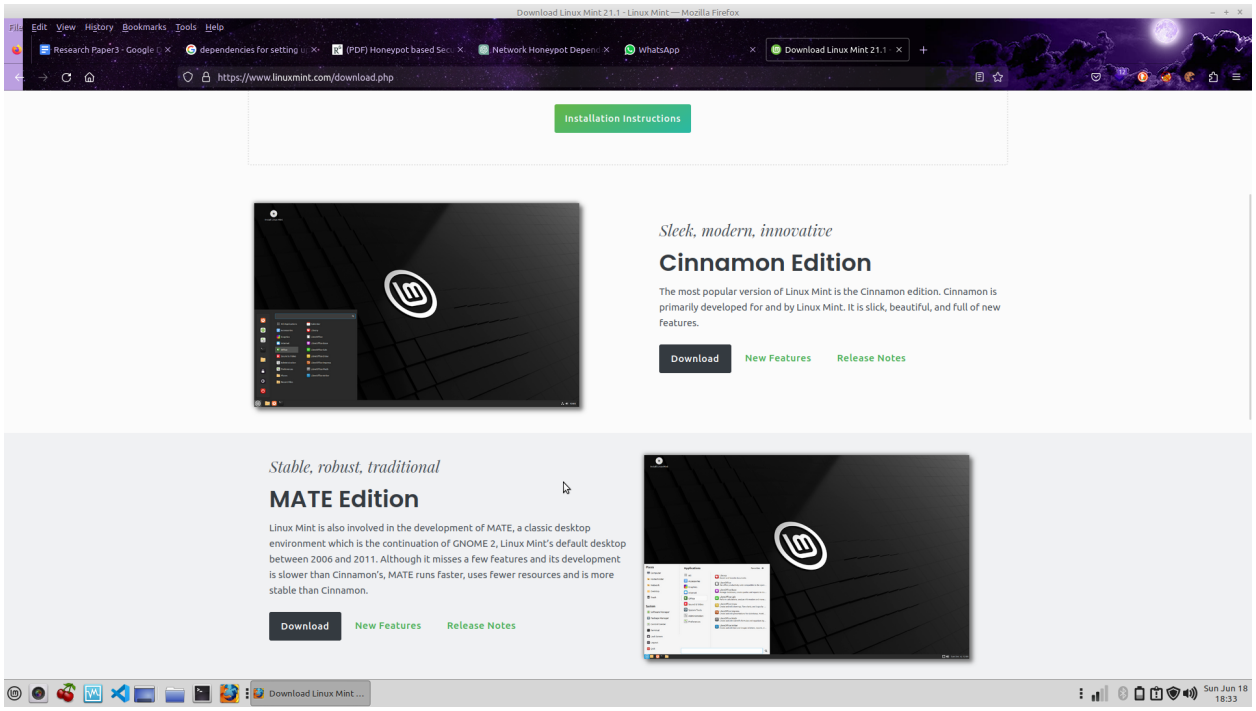



Linux Mint have three flavor/Edition

Cinnamon Edition ,

Mate Edition ,

Xfce Edition




## Cinnamon Edition

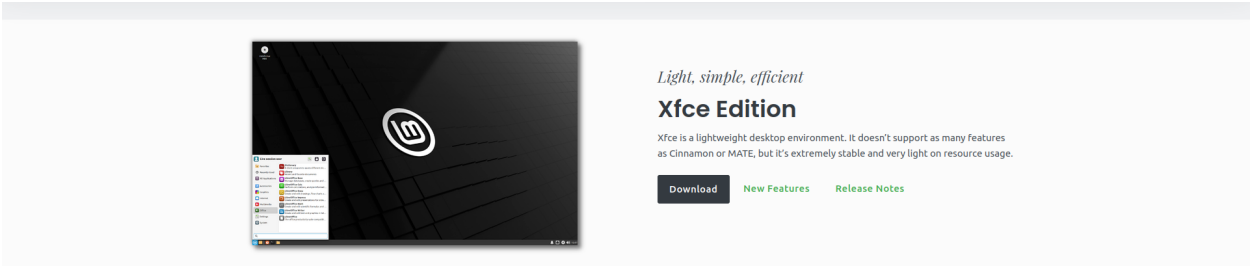
The most popular version of Linux Mint is the Cinnamon edition. Cinnamon is primarily developed for and by Linux Mint. It is slick, beautiful, and full of new features.

Sleek, modern, innovative

## MATE Edition

Linux Mint is also involved in the development of MATE, a classic desktop environment which is the continuation of GNOME 2, Linux Mint's default desktop between 2006 and 2011. Although it misses a few features and its development is slower than Cinnamon's, MATE runs faster, uses fewer resources and is more stable than Cinnamon.

Stable, robust, traditional




## Xfce Edition

Xfce is a lightweight desktop environment. It doesn't support as many features as Cinnamon or MATE, but it's extremely stable and very light on resource usage.

Light, simple, efficient

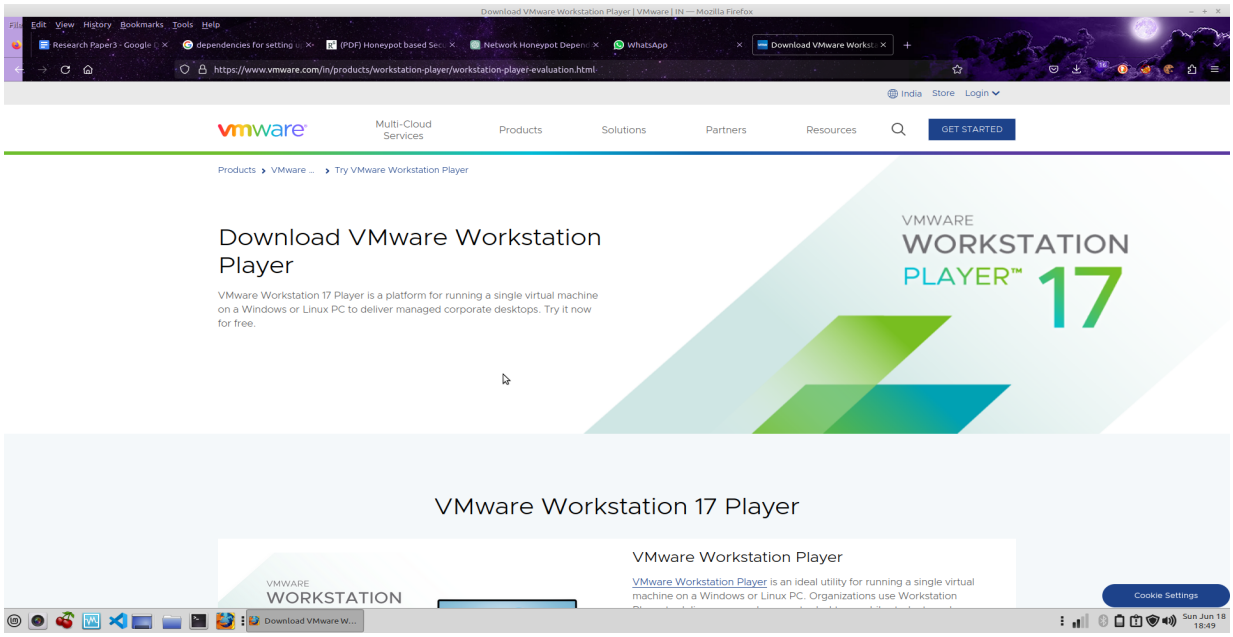
But I suggest the Mate Edition is Good , because I've been using it for 2 years and my experience is good with it.

Install any edition which you want.

**Step2**

install any VMs (Virtual box/ Vmware workstation)

Vmware



Virtual-Box


**Step3**

Let's install a Monitoring Tool. There are many but I'm going to use SNORT. It is simple to use.

## snort installation in linux mint,

**step1**

update your system before installing snort

command: apt-get update && upgrade

```
apt-get update && upgrade
```

Step2

install snort 2 (there are two version of snort available ,

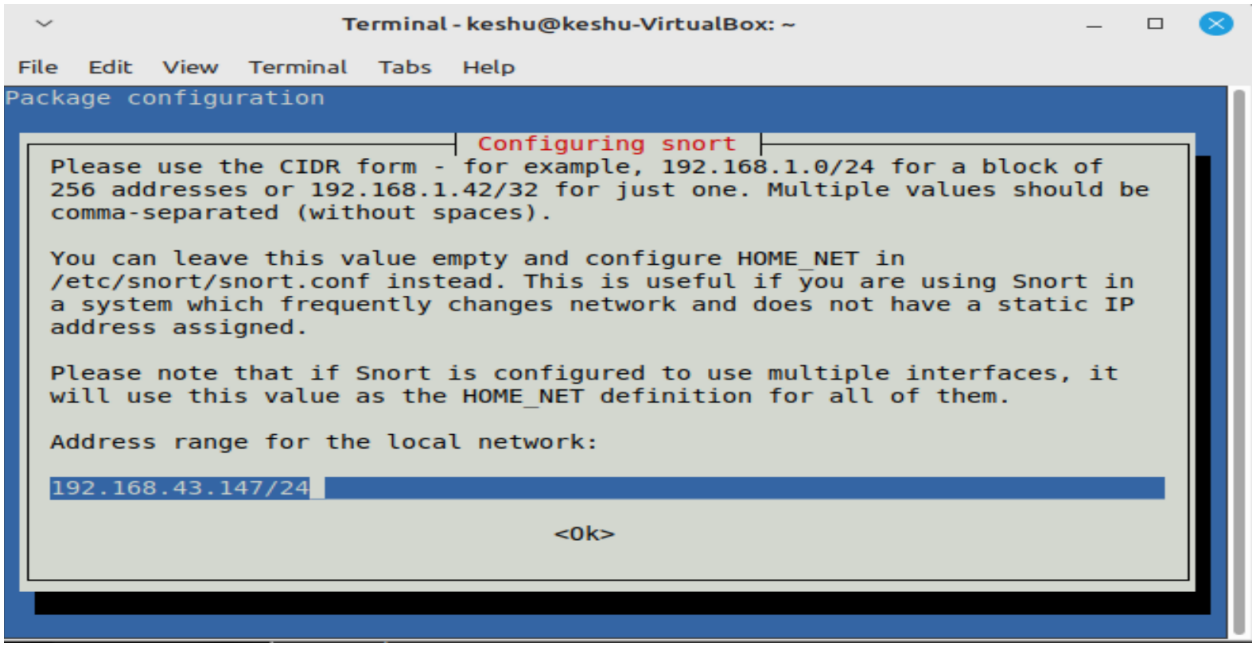
(snort2, snort3), we are going to use snort2)

command: apt install snort

```
sudo apt install snort
```

Step3

when installation completed you get this below screen




If you get this above screen then, type your ip address with CIDR notation .

NOTE: before this above screen , snort may ask you for your interface name.

**IF YOU GET ANY ISSUE IN INSTALLING SNORT, USE REFERENCE VIDEO**

Type this below command to getting your interface id name,and your IP address with CIDR notation.

Command: ip a

```
keshu@keshu-VirtualBox:~$ ip a s
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 100
0
    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
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defaul
t qlen 1000
    link/ether 08:00:27:6c:a8:13 brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.147/24 brd 192.168.43.255 scope global dynamic noprefixroute enp0s3
       valid_lft 2628sec preferred_lft 2628sec
    inet6 2409:4064:4b95:f36e:24a4:7cf2:5cd9:253c/64 scope global temporary dynamic
       valid_lft 3349sec preferred_lft 3349sec
    inet6 2409:4064:4b95:f36e:b83f:649c:6cb4:5b2d/64 scope global dynamic mngtmpaddr nopre
fixroute
       valid_lft 3349sec preferred_lft 3349sec
    inet6 fe80::98ba:df9f:7833:736d/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
keshu@keshu-VirtualBox:~$
```

enp0s3: is the interface name of my machine, 192.168.43.147/24:IP with CIDR.

**NOTE: in your case it may be different.**

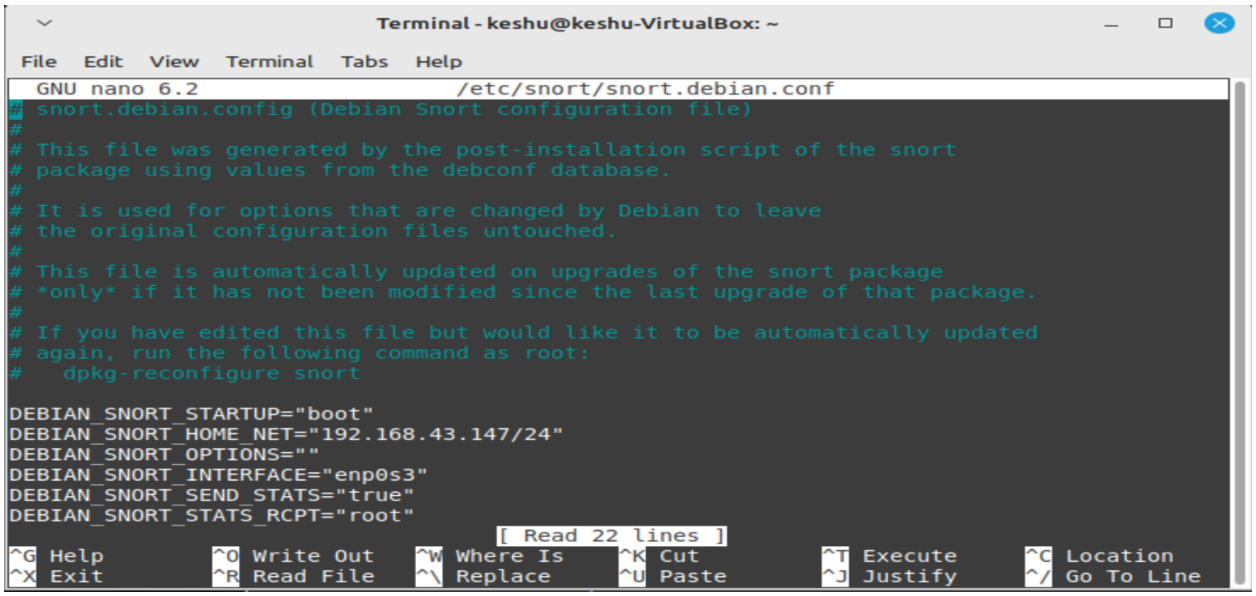
Step4
When snort installed, notice this below sentence,

```
Setting up snort (2.9.15.1-6build1) ...
Snort configuration: interface default not set, using 'enp0s3'
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
keshu@keshu-VirtualBox:~$
```

Snort configuration: interface default not set, using ‘enp0s3’

Let's verify if our interface name / IP with CIDR value is set correctly or not,

Use this below command to open your **snort.debian.conf** file, you can locate this file in /etc/snort/snort.debian.conf , open with any text editor.
**command:sudo nano /etc/snort/snort.debian.conf**



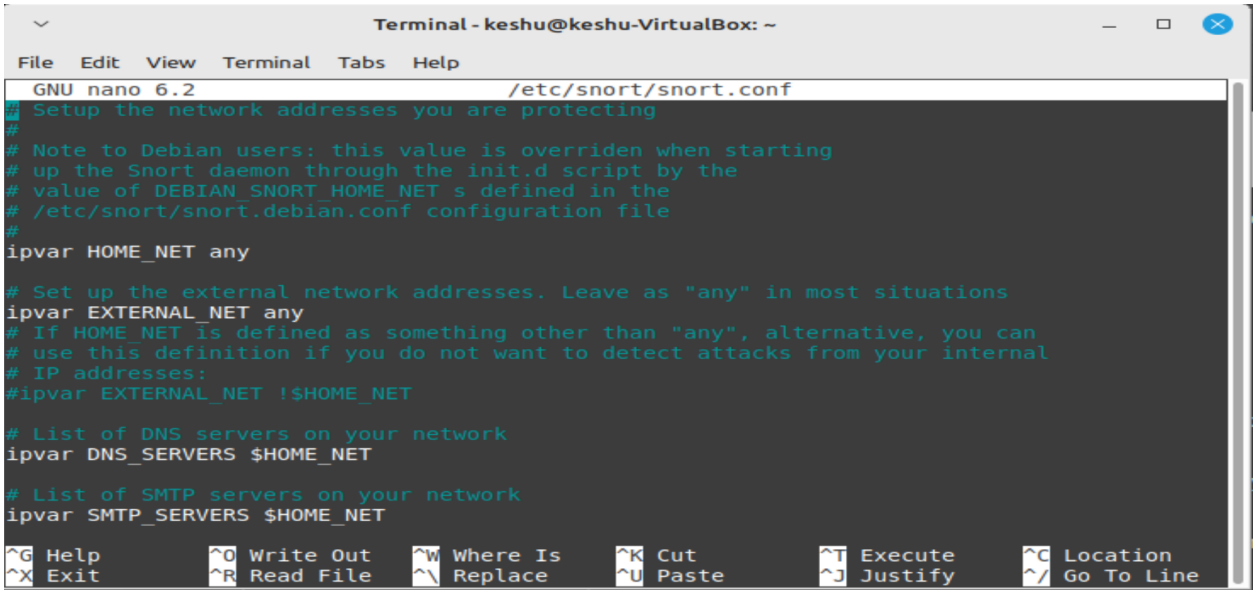

if it's not correct, correct it with the above interface name,

if correct then just verify it.

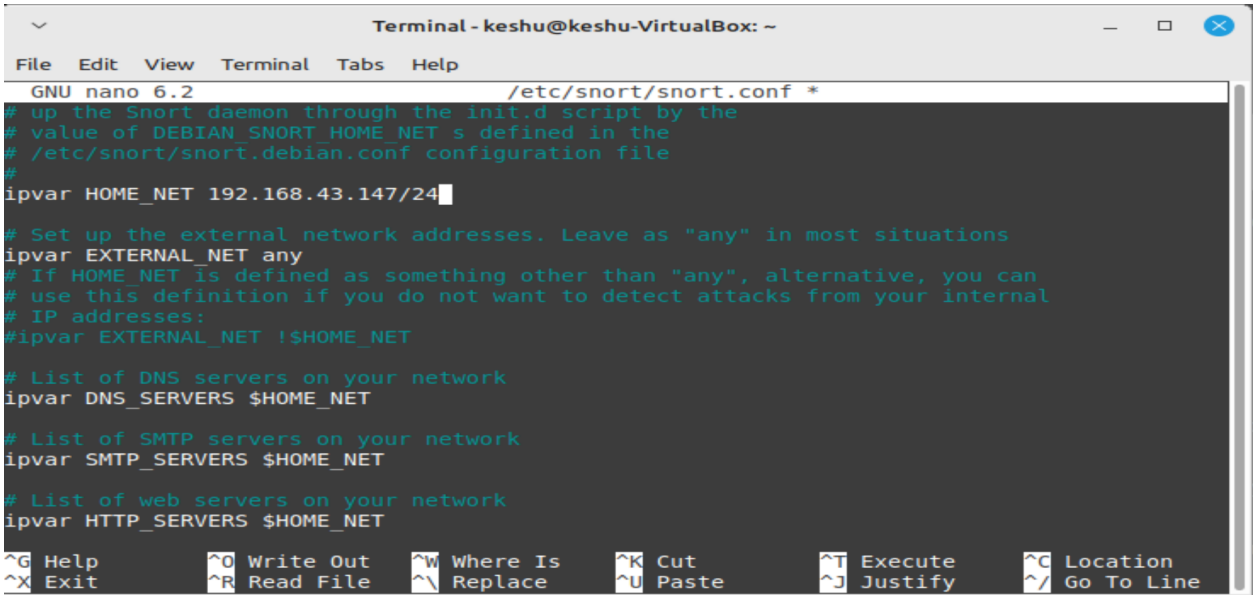
**Step5**

Now all set , Let's play with the snort config file, use this below command to open snort.conf file. Remember: You can use any text editor.

```
sudo vim /etc/snort/snort.conf
```




change the HOME_NET Value, it should be your ip address with its range.




After changing, save it.

## Step6

Now all set , only one thing is left , Snort Rule section left,
Snort has pre written Rules , Let's use it .

If you want to write/use your custom rules then , write your all rules in **local.rules** folder, use below command to open local.rules folder

Open rule file of snort, use this below command

```
sudo vim /etc/snort/rules/local.rules
```

Step7
Run Snort
Use below command to Run Snort

```
:~$ sudo snort -q -i <your network interface name> -A console -c /etc/snort/snort.conf
```

Use This Above Command To Run Snort With Pre Written Rules.

You can use this below command to run snort with your custom rules,

```
~$ sudo snort -q -i <interface-name> -A console -c /etc/snort/rules/local.rules
```

Lets See Simple Result Of Snort

```
keshav@inquisitive:~$ sudo snort -q -i wlo1  -A console -c /etc/snort/snort.conf
06/20-11:45:34.940634  [**] [1:2001219:4] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 192.168.43.147:42612 -> 192.168.43.4:22
06/20-11:45:42.250253  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::98ba:df9f:7833:736d -> fe80::bac7:4aff:feae:1545
06/20-11:45:42.268894  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> fe80::98ba:df9f:7833:736d
06/20-11:45:42.579573  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> 2409:4064:4e11:e97b:17e:3e0d:50b9:8635
06/20-11:45:42.580040  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} 2409:4064:4e11:e97b:17e:3e0d:50b9:8635 -> fe80::bac7:4aff:feae:1545
06/20-11:45:45.241694  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> 2409:4064:4e11:e97b:d81f:6285:a08c:e693
06/20-11:45:45.241758  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} 2409:4064:4e11:e97b:d81f:6285:a08c:e693 -> fe80::bac7:4aff:feae:1545
06/20-11:45:47.494687  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::bac7:4aff:feae:1545 -> fe80::98ba:df9f:7833:736d
06/20-11:45:47.495160  [**] [1:100001:1] ICMP Ping Detected [**] [Priority: 0] {IPV6-ICMP} fe80::98ba:df9f:7833:736d -> fe80::bac7:4aff:feae:1545
06/20-11:45:55.175511  [**] [1:2001219:4] Potential SSH Brute Force Attack [**] [Classification: Attempted Denial of Service] [Priority: 2] {TCP} 192.168.43.147:44152 -> 192.168.43.4:22
^C*** Caught Int-Signal
keshav@inquisitive:~$ sudo snort -q -i <your network interface name> -A console -c /etc/snort/snort.conf
```

In Above Result Snort Detected Two Time Brute-Force Attack On This Machine.

If the above figure is not clear, then run your snort and check it by yourself, and you can check log also.

You can locate your snort log in below folder,

```
cd /var/log/snort
```

# NOTE

**If you want a snort drop down ssh login attempt, after 3 attempts then go and learn deep about writing snort rules. It will help to write advanced rules.**

## How To Choose Right Network Honeypot Software For Different Network Topology

*The size and complexity of your network:** If you have a large and complex network, you will need a honeypot software that can scale to meet your needs. This means that the honeypot software should be able to handle a large number of connections and should be able to collect data from a variety of sources.
**The types of attacks you are most susceptible to:** If you are most susceptible to simple bot attacks, you may be able to get away with using a low-interaction honeypot. However, if you are worried about more sophisticated attacks, you will need a honeypot that can interact with attackers and collect more detailed information.
**Your budget:** Honeypot software can range in price from free to thousands of dollars. You will need to choose a honeypot that fits your budget and your needs.

Here is a more detailed explanation of some of the most popular honeypot software options:

**Honeypot-NG:** This is a free and open-source honeypot software that is easy to set up and use. It is a good option for small networks that are susceptible to simple bot attacks. Honeypot-NG is a good option for organizations that want to get started with honeypotting without a large investment. It is easy to set up and use, and it can be used to collect data on a variety of attacks.

**The Honeynet Project:** This is a non-profit organization that provides a variety of honeypot software options, including high-interaction honeypots. It is a good option for organizations that are worried about sophisticated attacks. The Honeynet Project is a good option for organizations that want to collect detailed information about attacks. They offer a variety of honeypot software options, including high-interaction honeypots that can interact with attackers and collect more detailed information.
**Snort:** This is a network intrusion detection system (IDS) that can also be used as a honeypot. It is a good option for organizations that want to collect detailed information about attacks. Snort is a popular network IDS that can also be used as a honeypot. It is a good option for organizations that want to collect detailed information about attacks.

Here are some additional tips for choosing the right network honeypot software:

**Consider your security goals:** What do you hope to achieve by deploying a honeypot? Do you want to collect information about attackers, or do you want to deter attacks?
**Evaluate your network infrastructure:** What kind of network do you have? How many hosts are on your network? What is your budget?
Research different honeypot software options:** There are many different honeypot software options available. Do some research to find the best option for your needs.
**Get help from a security expert:** If you are not sure how to choose or deploy a honeypot, consider getting help from a security expert.

---

MORE DETAIL INFORMATION:

---

1. Types of Network Honeypots:
Network honeypots can be categorized into two main types:

a. Low-Interaction Honeypots: These honeypots simulate a limited number of network services and provide minimal interaction with potential attackers. They are lightweight and consume fewer resources. Examples include Honeyd and Tiny Honeypot.

b. High-Interaction Honeypots: These honeypots emulate complete operating systems and services, allowing attackers to interact with them extensively. They provide a more realistic environment but require additional resources and expertise to set up and maintain. Examples include Kippo, Cowrie, and Dionaea.

When choosing a network honeypot software, consider the level of interaction required, the available resources, and the expertise available to manage it effectively.

2. Network Topology Considerations:

Network topology refers to the arrangement and structure of the network components. Here are a few common network topologies and their considerations:

a. Flat Network: In a flat network, all devices are connected to a single network segment without any segmentation. In this case, a honeypot can be directly placed within the network, monitoring all incoming traffic. High-interaction honeypots can be used to capture detailed attacker interactions.

b. Segmented Network: A segmented network is divided into multiple network segments or VLANs, usually based on different departments or security zones. In this case, you can deploy honeypots in each segment or VLAN to monitor and capture attacks specific to that segment. Low-interaction honeypots like Honeyd can be useful in this scenario.

c. DMZ (Demilitarized Zone): A DMZ is a separate network zone between the internal network and the external/internet-facing network. Deploying honeypots in the DMZ allows you to monitor and analyze attacks specifically targeting externally-facing services like web servers, mail servers, or DNS servers.

d. Virtualized Network: In virtualized environments, such as cloud-based deployments or virtual private networks (VPNs), you can set up honeypots as virtual machines within the virtualized network. Consider using virtualization-aware honeypot software that can integrate well with the underlying virtualization infrastructure.

Consider the network topology and the specific areas you want to monitor when choosing the placement and type of honeypot software.

3. Features and Capabilities:

Different honeypot software offer varying features and capabilities. Consider the following factors:

a. Simulated Services: Determine which network services the honeypot software can emulate. For example, if you want to monitor attacks targeting SSH, consider honeypots like Kippo or Cowrie, which specialize in simulating vulnerable SSH services.

b. Logging and Monitoring: Look for honeypot software that provides robust logging and monitoring capabilities. This includes features such as capturing network traffic, logging attacker interactions, generating alerts, and integrating with log management or SIEM systems.

c. Attack Analysis: Some honeypot software offer built-in analysis tools or integration with external analysis platforms. Consider the capabilities for analyzing captured attack data, generating reports, and extracting insights from the collected information.

d. Ease of Use: Evaluate the user-friendliness and ease of configuration of the honeypot software. Consider the available documentation, community support, and the level of technical expertise required to set up and manage the honeypot effectively.

e. Customization and Flexibility: Assess the software's ability to customize the honeypot environment and tailor it to specific requirements. This can include modifying banners, emulating different software versions, or adding custom vulnerabilities.

4. Community Support and Updates:

Check the availability of community support, active development, and regular updates for the honeypot software you're considering. Look for an engaged user community, forums, and mailing lists where you can seek help, share experiences, and stay updated on the latest developments and security patches.

5. Integration with Existing Infrastructure:

Consider how well the honeypot software integrates with your existing infrastructure, such as logging and monitoring systems, SIEM solutions, or threat intelligence platforms. Integration capabilities can streamline data collection, analysis, and incident response processes.

6. Legal and Ethical Considerations:

Be aware of legal and ethical considerations when deploying a honeypot. Ensure that the chosen honeypot software complies with relevant laws and regulations in your jurisdiction. Understand the potential risks and liabilities associated with operating a honeypot environment and take appropriate measures to mitigate them.

Ultimately, the right honeypot software for your network topology depends on your specific goals, available resources, technical expertise, and the level of interaction and monitoring you require. Conduct thorough research, consider the factors mentioned above, and test different honeypot solutions in a controlled environment before deploying them in production.

By following these tips, you can choose the right network honeypot software for your network topology and security goals.

## Tools For Network Security Testing And Analysis


**#1 Nmap: Discovering Networks and Auditing Security**

**Creator:** Gordon Fyodor Lyon

**Why We Like It:** The most fitting way to kick off is with arguably the most valuable of all network pen testing tools: Nmap AKA Network Mapper, this is an extremely flexible pen testing tool that can be used to scan both large and small networks on a wide range of operating systems. Nmap is versatile and easy to use, and provides a quick, simple way to uncover information.

Go to the Tool >>

**#2 Pompem: Finding Exploits and Vulnerabilities**

**Creator**: Rafael Francischini

**Why We Like It**: Because Pompem was developed in Python, it can perform advanced searches in a variety of databases. It helps to alleviate the more manual work that pen testers and ethical hackers do to find vulnerabilities and exploits in their respective databases, saving time and energy.

Go to the Tool >>

**#3 NP**: **Combining Different Pen Testing Tools**

**Creator:** Liam Somerville

**Why We Like It:** This open-source tool makes it easy to summarize and query the output of multiple different port scanners so you can spend more time hacking and less time grepping. And as a bonus – the creator is one of Bishop Fox's own!

Go to the Tool >>

**#4 Arp-Scan: Scanning for IP Hosts**

**Creator: Roy Hills**

**Why We Like It:** Arp-Scan is a command line tool that makes discovering and detecting the characteristics of IP hosts much more accessible. The main benefits of using Arp-Scan according to the Kali Team include discovery of all IPV4 connected devices, its quick identification and mapping of IP addresses to MAC addresses, identification of duplicate IP addresses, isolation and location of rogue devices, and device identification by NIC vendor. Additionally, Arp-Scan works well in tandem with the other tools that the Kali Team has created, like Arpwatch.

Go to the Tool >>

**#5 Wifite2: Auditing Encrypted Wireless Networks**

**Creator:** derv82

**Why We Like It:** This tool is a rewrite of the network pen testing tool Wifite. Use Wifite2 to retrieve a router's password via several different methods, such as by way of Offline Pixie-Dust

attacks or the Online Brute-Force PIN attacks. Compared to the (slightly) older Wifite, this iteration offers less bugs, better speed, and increased accuracy.

Go to the Tool >>

**#6 Aireplay-ng and Aircrack-ng: Leveraging This Tool Duo**

**Creators**: Aireplay-ng / Aircrack-ng

**Why We Like It:** These wireless network pen testing tools go together like two peas in a pod. The aireplay tool works to generate traffic that the aircrack tool can later use to discover any network insecurities as well as to craft APR injections.

Go to the Tools >>

**#7 Evilgophish: Building Upon Previous Resources**

**Creator**: Dylan Evans

**Creators of Previous Resources:** Kuba Gretzky and Jordan Wright

**Why We Like It**: Dylan Evans had the spectacular idea to combine the best of both worlds in Evilgophish. Evilginx is a tool by Kuba Gretzky and GoPhish is a toolkit currently maintained by Jordan Wright (equally amazing tools in their own right). Both tools serve different and highly useful purposes; Evilginx is a proxy man-in-the-middle framework that can be used to circumvent 2FA. Meanwhile, GoPhish is a popular open-source social engineering framework. When they are together as Evilgophish, you can truly elevate your red teaming or pen testing engagements! Unlike the OG GoPhish, Evilgophish has SMS phishing capabilities and comes with a blacklist that contains IP addresses/blocks owned by the likes of ProofPoint, Microsoft, and Trend Micro.

Go to the Tool >>

**#8 CloudFox: Automating the Enumeration Process for Cloud Pen Tests**

**Creators**: Seth Art and Carlos Vendramini

**Why We** Like It: This tool straight from the Fox Den – inspired by existing tools like PowerView – helps hackers find attack paths in cloud environments that would otherwise be difficult to

navigate. We love that this tool provides a different service than other popular tools that analyze cloud environments. Watch the creators themselves demo CloudFox in our Tool Talk recording from September 2022!

Go to the Tool >>

## List of 10 Best Network Security Testing Tools

1. Astra Security
2. NMAP
3. Wireshark
4. OpenVAS
5. Metasploit
6. Nikto
7. PRTG Network Monitor
8. Snort
9. Intruder
10. Syxsense

---

### 1. Wireshark

Wireshark is an open-source network protocol analyzer that helps organizations capture real-time data and track, manage, and analyze network traffic even with minute details.

It allows users to view the TCP session rebuilt streams. It helps to analyze incoming and outgoing traffic to troubleshoot network problems.

**Features**

- Deep inspection of hundreds of protocols
- Capture real-time data and offline analysis
- It runs on multiple operating systems like Windows, Linux, macOS, etc.
- **It provides color codes to each packet for quick analysis.**

**Pros**

- Supports multiple operating systems like Windows, Linux, etc
- Easily integrates with third-party applications

**Cons**

- Steep learning curve
- Difficult to read the encrypted network traffic
- Lack of support

## 2. Nexpose

Nexpose is a network security software that provides real-time information about vulnerabilities and reduces the threats in a network. In addition, Nexpose permits the users to allot a risk score to the detected vulnerabilities so that they may be prioritized as per the security levels.

Nexpose helps IT teams to get real-time scanning of the network and detect network vulnerabilities. It also continuously refreshes and adapts to new threats in software and data.

Features

- Nexpose provides real-time network traffic.
- It provides a risk score and helps IT teams prioritize the risk as per the security levels.
- It shows the  IT teams different actions they can take immediately to reduce the risk.

Pros

- Easy to use
- In-depth scanning of network vulnerabilities.

Cons

- No domain-based authentication for Linux devices
- Lack of customer support

## 3. Splunk

Splunk is used for monitoring network security. It provides both real-time data analysis and historical data searches.

It is a cloud-based platform that provides insights for petabyte-scale data analytics across the hybrid cloud.

Splunk's search function makes application monitoring easy and user-friendly.

It contains a user interface to catch, index, and assemble data and generate alerts, reports, dashboards, and graphs in real-time.

**Features**

- Splunk attributes risk to users and systems and maps alerts to cybersecurity frameworks, and trigger alerts when the risk exceeds the threshold.
- It helps in prioritizing alerts and accelerating investigations with built-in threat intelligence.
- It helps to get automatic security content updates to stay updated with the emerging threats.

**Pros**

- The indexing of data is easy
- Easy to use

**Cons**

- Steep learning curve

## 4. Nagios

Nagios is a network security tool that helps to monitor hosts, systems, and networks. It sends alerts in real-time. You can select which specific notifications you would like to receive.

It can track network resources like HTTP, NNTP, ICMP, POP3, and SMTP. It is a free tool.

**Features**

- Nagios help to monitor IT infrastructure components, including system metrics, network protocols, application services, servers, and network infrastructure.
- It sends alerts when an unauthorized network is detected and provides IT admin with notice of important events.
- It provides reports which show the history of events, notifications, and alert responses for later review.

**Pros**

- Great tool for live monitoring
- User friendly
- Data monitoring can be tracked easily

**Cons**

- Limited reporting capabilities
- The system slows down while monitoring the data

## 5. Tor

Tor is a network security tool that ensures the privacy of users while using the internet. It helps in preventing cybersecurity threats and is useful in safeguarding information security.

Tor works on the concept of onion routing, and the layers are layered one over the other similar to the onion. All the layers function smartly so that there is no need to reveal any IP and geographical location of the user. Therefore, limiting the visibility of any sites, you are visiting.

**Features**

- Tor software is available for Linux, Windows, as well as Mac
- It helps to block the third-party trackers, and ads can't follow you
- It prevents third-party watching your connection from knowing what websites you visit
- It aims to make all users look the same and is difficult for trackers

**Pros**

- It protects the online identity
- Provides a high-level privacy
- User-friendly interface

**Cons**

- The system gets slower during navigation
- Starting and  browsing time is high

## 6. Nessus Professional

Nessus professional is a network security software that can detect vulnerabilities like software bugs and general security problems in software applications, IT devices, and operating systems and manage them appropriately.

Users can access a variety of security plug-ins as well as develop their own and scan individual computers as well as networks.

**Features**

- It provides customization of reports by vulnerability or hosts and creates a summary for the users.
- Sends email notifications of the scan results
- It helps meet government, regulatory, and corporate requirements
- It scans cloud applications and prevents your organization from cybersecurity threats

**Pros**

- It offers flexibility for developing custom solutions
- Nessus VA scan covers all standard network devices like endpoints, servers, network devices, etc.
- Provide plug-ins for many vulnerabilities

**Cons**

- The software slows down when you scan a large scope
- Poor customer support

## 7. Metasploit

Metasploit is security software that contains various tools for executing penetrating testing services. IT professionals use this tool to reach security goals such as vulnerabilities in the system, improving the computer system security, cyber defense strategies and maintaining complete security assessments.

The penetration testing tools can examine various security systems, including web-based apps, servers, networks, etc.

It allows the organization to perform security assessments and improve its overall network defenses and make them more responsive.

**Features**

- The tools are used to take advantage of system weaknesses
- The module encoders are used to convert codes or information
- Metasploit allows a clean exit from the target system. It has compromised

**Pros**

- Good support for penetration testing
- Useful to learn and understand vulnerabilities that exist in the system
- Freely available and includes all penetration testing tools

**Cons**

- Software updates are less frequent
- Steep learning curve

## 8. Kali Linux

Kali Linux is a penetration testing tool used to scan IT systems and network vulnerabilities. The organization can monitor and maintain its network security systems on just one platform.

It offers a security auditing operating system and tools with more than 300 techniques to make sure that your sites and Linux servers stay safe.

Kali Linux is used by professional penetration testers, ethical hackers, cybersecurity experts, and individuals who understand the usage and value of this software.

**Features**

- Kali Linux comes with pre-installed tools like Nmap, Aircrack-ng, Wireshark, etc., to help with information security tasks.
- It provides multi-language support.
- It helps to generate the customized version of Kali Linux.

**Pros**

- Pre-installed tools are ready to use
- Simple and user-friendly interface

**Cons**

- Limited customization
- The installation process is complicated

## 9. Snort

Snort is an open-source network security tool used to scan networks and prevent any unauthorized activity in the network. IT professionals use it to track, monitor, and analyze network traffic. It helps to discover any signs of theft, unauthorized access, etc. After detection, the tool will help send alerts to the users.

Additionally, Snort is used to perform protocol analysis, detect frequent attacks on a system, look for data captured from traffic, etc.

**Features**

- Snort provides a real-time traffic monitor
- It provides protocol analysis
- It can be installed in any network environment

**Pros**

- Good for monitoring network traffic
- Good for detecting any network intrusions

**Cons**

- Complicated settings and configuration
- Steep learning curve

## 10. Forcepoint

Forcepoint is a cloud-based security solution and is used to define network security, restrict users from accessing specific content and block various attempts to hack or get your organization's information.

The IT admin can customize Forcepoint to monitor and detect any unauthorized acts in a network and can take the appropriate action required. It adds an extra level of security for critical threats.

Forcepoint is majorly for the organizations working in the cloud, and it will be able to block or provide warnings about any risky cloud servers.

**Features**

- Forcepoint helps in monitoring any unusual cloud activities.
- It provides tracking of any suspicious behavior and sends alerts to the IT admins.
- It protects and secures data.
- It helps to limit the access of your employees within the scope of your organization.

**Pros**

- Good support
- Easy to set up and user-friendly interface

**Cons**

- Creating reports is difficult
- Less flexibility in real-time screen monitoring

==========

1. OWASP (Open Web Application Security Project): OWASP provides a wealth of information and resources related to web application security. They have a

dedicated section on their website that covers various security tools and technologies: https://owasp.org/

2. SANS Institute: SANS offers a wide range of training courses and resources on network security, including tools and techniques. Their website provides valuable insights and educational materials: https://www.sans.org/
3. Network Security Tools on GitHub: GitHub hosts numerous open-source network security tools. You can explore repositories and projects related to network security tools and their source code here: https://github.com/topics/network-security
4. Cybersecurity and Infrastructure Security Agency (CISA): CISA provides guidance, best practices, and resources on network security. Their website offers insights into various security tools and technologies: https://www.cisa.gov/cybersecurity-tools
5. Network Security Tools on SecurityFocus: SecurityFocus is a comprehensive security resource that covers various aspects of network security. They have a section dedicated to network security tools, where you can find articles, discussions, and information: https://www.securityfocus.com/tools
6. Network Security Tools on TechTarget: TechTarget is an online platform that provides resources and insights into technology-related topics. Their network security tools section covers articles, tutorials, and reviews of different security tools: https://searchsecurity.techtarget.com/network-security-tools

These resources should provide you with a good starting point to explore and learn about network security tools. Remember to refer to reputable sources, documentation, and user guides for each specific tool you're interested in.

**There are many more tools , dont stop your research here.**

## Reference

### Windows Honeypot

https://resources.infosecinstitute.com/topic/ghost-usb-honeypot-part-2/ ,

Design and Implementation of a Real-Time Honeypot System for the Detection and Prevention of Systems Attacks .

Tool for network security

https://bishopfox.com/blog/8-network-pen-testing-tools ,
https://www.getastra.com/blog/security-audit/network-security-testing-tools/ ,
https://www.zluri.com/blog/network-security-tools/ ,

### Honeypot strategies

Don't forget to try AI Website,

https://www.comparitech.com/net-admin/how-to-establish-a-honeypot-on-your-network/