PROJECT REPORT

INT 301 : OPEN SOURCE TECHNOLOGIES

Topic: Use any open source software to generate a daily report of internet usage from 9pm-7am in your hostel/home.

Submitted in partial fulfillment of the requirements for the award of degree

B. Tech. (Computer Science & Engineering)

Submitted to

LOVELY PROFESSIONAL UNIVERSITY

PHAGWARA, PUNJAB

SUBMITTED BY

Name of student: Nishant

Registration Number: 11916991

INTRODUCTION

Objective: The objective of this project is to implement ntop, an open-source network monitoring tool, to effectively monitor and analyze internet usage in order to gain insights into network traffic patterns, identify potential bandwidth bottlenecks, detect suspicious or malicious activities, and optimize network performance.

Specifically, the project aims to achieve the following objectives:

1. Network Traffic Analysis: Utilize ntop to collect and analyze network traffic data, including protocols, sources, destinations, and volumes, to gain a comprehensive understanding of the internet usage patterns within the network.

2. Bandwidth Monitoring: Monitor bandwidth usage in real-time using ntop's graphical interface, reports, and alerts to identify applications, devices, or users consuming excessive bandwidth and take appropriate actions to optimize network resources.

3. Anomaly Detection: Leverage ntop's built-in anomaly detection capabilities to identify and alert on abnormal network behavior, such as sudden spikes in traffic, unusual communication patterns, or potential security threats, allowing for timely response and mitigation.

4. Reporting and Visualization: Utilize ntop's reporting and visualization features to generate comprehensive reports and visual representations of network usage trends, top talkers, and key performance indicators (KPIs), providing meaningful insights for network troubleshooting, capacity planning, and policy enforcement.

5. Network Optimization: Utilize the insights obtained from ntop's analysis to optimize network performance, such as identifying and addressing network bottlenecks, optimizing network configurations, and improving Quality of Service (QoS) policies to ensure optimal internet usage and efficient utilization of network resources.

By achieving these objectives, the project aims to improve network visibility, enhance network performance, detect and mitigate security threats, and optimize internet usage, leading to a more efficient, secure, and reliable network infrastructure.

Description: The project involves implementing ntop, an open-source network monitoring tool, to monitor and analyze internet usage within a network environment. With the increasing reliance on the internet for communication, collaboration, and data exchange, it has become crucial for organizations to gain insights into their network traffic patterns, optimize bandwidth utilization, detect anomalies, and ensure efficient internet usage.[3]

The project will begin with the installation and configuration of ntop on the network infrastructure, which may include setting up ntop on a dedicated server or deploying it as a virtual machine. Once ntop is up and running, it will be configured to capture and analyze network traffic data in real-time from various sources, including routers, switches, or other network devices.

The project will utilize ntop's rich set of features to monitor and analyze internet usage. This may include generating reports and visualizations to gain insights into network traffic patterns, identifying top talkers, monitoring bandwidth usage in real-time, and setting up alerts for anomalous behaviors or security threats. The project will also leverage ntop's anomaly detection capabilities to detect unusual network behaviors, such as sudden spikes in traffic, excessive bandwidth consumption, or suspicious communication patterns, and take appropriate actions to mitigate potential risks.

In addition, the project will utilize ntop's reporting and visualization capabilities to generate comprehensive reports and visual representations of network usage trends, top applications or protocols, and key performance indicators (KPIs). These reports will provide valuable insights for network troubleshooting, capacity planning, and policy enforcement, enabling to optimize network performance and ensure efficient internet usage.

Overall, the project aims to leverage ntop's capabilities to enhance network visibility, optimize bandwidth utilization, detect and mitigate security threats, and ensure efficient internet usage, leading to a more reliable, secure, and performant network infrastructure.

Scope: The scope of the project using ntop to monitor internet usage will encompass the following:

1. Implementation of ntop: The project will involve the installation, configuration, and deployment of ntop on the network infrastructure. This may include setting up ntop on a dedicated server or virtual machine, configuring it to capture network traffic data from various sources, and integrating it with the existing network environment.
2. Network Traffic Analysis: The project will utilize ntop's features to collect and analyze network traffic data in real-time, including protocols, sources, destinations, and volumes, to gain insights into internet usage patterns within the network. The scope will include monitoring and analyzing network traffic data to identify top applications, protocols,

devices, or users consuming bandwidth, and generating reports and visualizations to interpret the data effectively.

3. Bandwidth Monitoring: The project will involve using ntop's capabilities to monitor bandwidth usage in real-time, including setting up alerts for excessive bandwidth consumption, identifying bandwidth bottlenecks, and optimizing network resources. The scope may also include monitoring Quality of Service (QoS) policies and analyzing bandwidth usage trends over time to optimize network performance.

4. Anomaly Detection: The project will utilize ntop's built-in anomaly detection capabilities to detect and alert on abnormal network behavior, such as sudden spikes in traffic, unusual communication patterns, or potential security threats. The scope may include setting up thresholds, rules, and filters to trigger alerts for anomalies, and taking appropriate actions to investigate and mitigate risks.

5. Reporting and Visualization: The project will involve utilizing ntop's reporting and visualization features to generate comprehensive reports and visual representations of network usage trends, top talkers, and key performance indicators (KPIs). The scope may include customizing reports, creating dashboards, and interpreting visualizations to gain meaningful insights into network traffic patterns and usage.

6. Network Optimization: The project will encompass utilizing the insights obtained from ntop's analysis to optimize network performance. This may include identifying and addressing network bottlenecks, optimizing network configurations, and improving QoS policies to ensure efficient internet usage and optimal network performance.

The project scope will be defined in collaboration with relevant stakeholders and may be refined or expanded based on the organization's specific requirements, resources, and constraints. The project will work closely with network administrators, IT, and security teams to ensure successful implementation and utilization of ntop for monitoring internet usage within the defined scope.

Dependencies for performing the project using ntop to monitor internet usage may include:

1. Network Infrastructure: The project will require a stable and functional network infrastructure, including routers, switches, and other networking devices, that can capture and forward network traffic data to ntop for analysis.[2]

2. ntop Software: The project will depend on the availability and proper installation of ntop software, which includes downloading and installing the appropriate version of ntop for the specific operating system or platform being used. This may also include configuring ntop with the necessary settings and parameters for capturing and analyzing network traffic data.

3. Hardware Resources: The project may require dedicated server or virtual machine resources to host ntop, including sufficient CPU, memory, and storage capacity to handle the network traffic data and analysis requirements.
4. Access to Network Devices: The project will need appropriate access and permissions to the network devices, such as routers, switches, or other devices, to configure them to forward network traffic data to ntop for analysis.
5. Access to Network Traffic Data: The project will depend on the availability of network traffic data for analysis. This may require permissions and access to capture network traffic data from various sources, such as routers, switches, or other network devices.
6. Documentation and Resources: The project may rely on documentation, online resources, tutorials, and other references to properly configure, utilize, and troubleshoot ntop for monitoring internet usage. This may include ntop's official documentation, user guides, forums, and other online resources.

It's important to identify and ensure that all the necessary dependencies are available and properly addressed to ensure a successful implementation of the project using ntop for monitoring internet usage. Regular communication and collaboration with relevant stakeholders, including network administrators, IT personnel, and security teams, will be essential to ensure smooth progress and completion of the project.

Step-by-step Installation:

Step 1: Enter in root user and run these commands:

```
sudo su -
apt-get update
apt-get upgrade
apt-get install software-properties-common wget
```

Step 2: Now, We will add the repository which contains the ntopng program[1]

```
add-apt-repository universe
```

Step 3: Next, we have to install the package

```
apt install ntopng
```

To start it, use the command

```
systemctl start ntopng
```

Configuration File

To view the configuration file,

```
cat /etc/ntopng/ntopng.conf
```

To choose the port use “–http-port” or “-w” option as

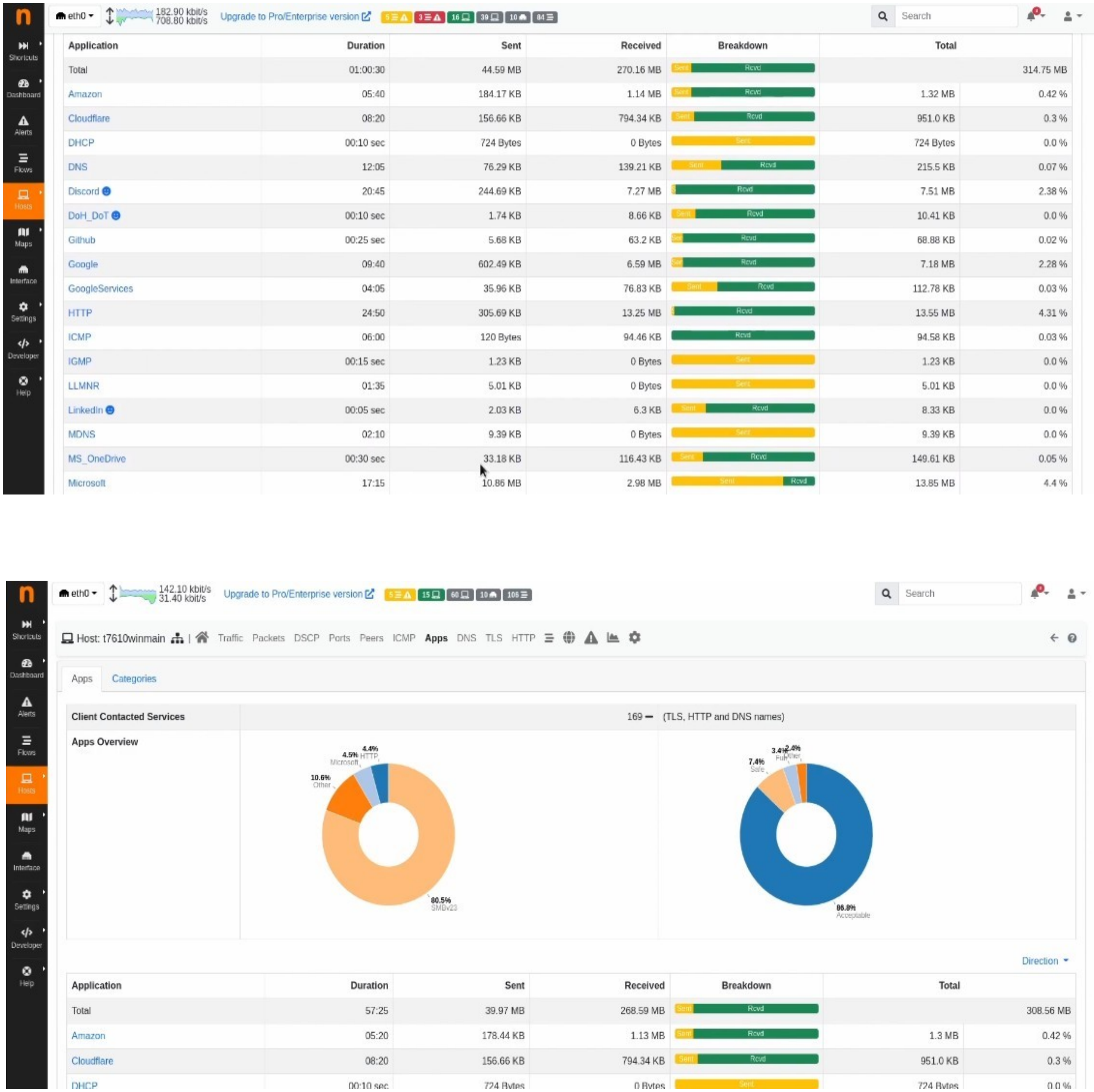
```
--http-port=:3000
```

To run ntopng or to start the ntopng[4]

```
ntopng
```

This will run ntopng and view it use the URL in your browser

```
http://<ntopng IP Address>:<port>/
```

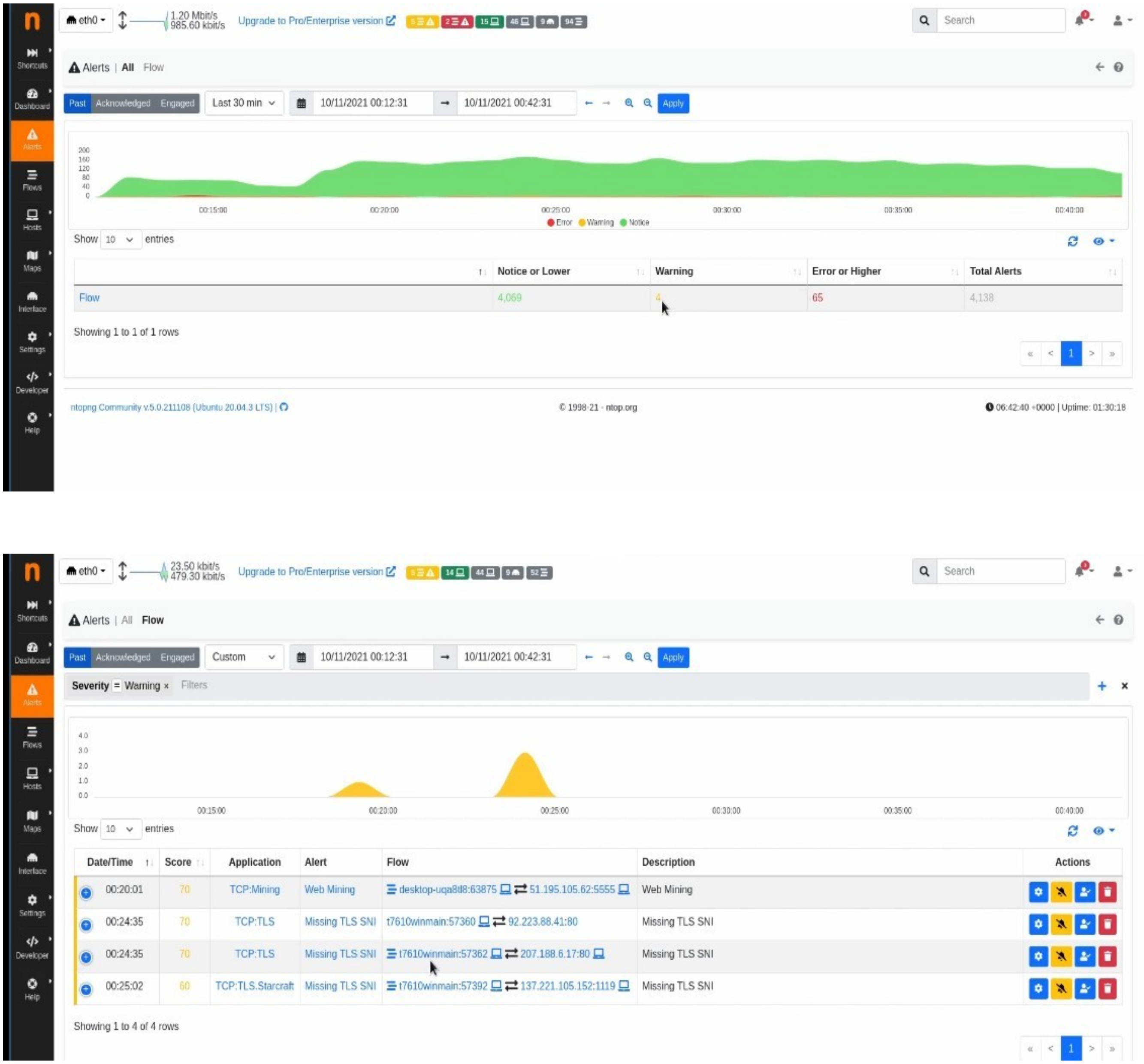


Application	Duration	Sent	Received	Breakdown	Total	
Total	01:00:30	44.59 MB	270.16 MB	Sent Rcvd		314.75 MB
Amazon	05:40	184.17 KB	1.14 MB	Sent Rcvd	1.32 MB	0.42 %
Cloudflare	08:20	156.66 KB	794.34 KB	Sent Rcvd	951.0 KB	0.3 %
DHCP	00:10 sec	724 Bytes	0 Bytes	Sent	724 Bytes	0.0 %
DNS	12:05	76.29 KB	139.21 KB	Sent Rcvd	215.5 KB	0.07 %
Discord	20:45	244.69 KB	7.27 MB	Rcvd	7.51 MB	2.38 %
DoH_DoT	00:10 sec	1.74 KB	8.66 KB	Sent Rcvd	10.41 KB	0.0 %
Github	00:25 sec	5.68 KB	63.2 KB	Sent Rcvd	68.88 KB	0.02 %
Google	09:40	602.49 KB	6.59 MB	Sent Rcvd	7.18 MB	2.28 %
GoogleServices	04:05	35.96 KB	76.83 KB	Sent Rcvd	112.78 KB	0.03 %
HTTP	24:50	305.69 KB	13.25 MB	Rcvd	13.55 MB	4.31 %
ICMP	06:00	120 Bytes	94.46 KB	Rcvd	94.58 KB	0.03 %
IGMP	00:15 sec	1.23 KB	0 Bytes	Sent	1.23 KB	0.0 %
LLMNR	01:35	5.01 KB	0 Bytes	Sent	5.01 KB	0.0 %
LinkedIn	00:05 sec	2.03 KB	6.3 KB	Sent Rcvd	8.33 KB	0.0 %
MDNS	02:10	9.39 KB	0 Bytes	Sent	9.39 KB	0.0 %
MS_OneDrive	00:30 sec	33.18 KB	116.43 KB	Sent Rcvd	149.61 KB	0.05 %
Microsoft	17:15	10.86 MB	2.98 MB	Sent Rcvd	13.85 MB	4.4 %

Client Contacted Services	169 — (TLS, HTTP and DNS names)
Apps Overview	

Application	Duration	Sent	Received	Breakdown	Total	
Total	57:25	39.97 MB	268.59 MB	Sent Rcvd		308.56 MB
Amazon	05:20	178.44 KB	1.13 MB	Sent Rcvd	1.3 MB	0.42 %
Cloudflare	08:20	156.66 KB	794.34 KB	Sent Rcvd	951.0 KB	0.3 %
DHCP	00:10 sec	724 Bytes	0 Bytes	Sent	724 Bytes	0.0 %

Fig. : Usage indicator



eth0 1.20 Mbit/s 985.60 kbit/s

Alerts | All Flow

Last 30 min 10/11/2021 00:12:31 → 10/11/2021 00:42:31

Show 10 entries

	Notice or Lower	Warning	Error or Higher	Total Alerts
Flow	4,069	4	65	4,138

Showing 1 to 1 of 1 rows

ntopng Community v.5.0.211108 (Ubuntu 20.04.3 LTS) | © 1998-21 - ntop.org 06:42:40 +0000 | Uptime: 01:30:18

eth0 23.50 kbit/s 479.30 kbit/s

Alerts | All Flow

Custom 10/11/2021 00:12:31 → 10/11/2021 00:42:31

Severity = Warning ×

Show 10 entries

Date/Time	Score	Application	Alert	Flow	Description	Actions
00:20:01	70	TCP:Mining	Web Mining	desktop-uqa8d8:63875 ⇄ 51.195.105.62:5555	Web Mining	
00:24:35	70	TCP:TLS	Missing TLS SNI	t7610winmain:57360 ⇄ 92.223.88.41:80	Missing TLS SNI	
00:24:35	70	TCP:TLS	Missing TLS SNI	t7610winmain:57362 ⇄ 207.188.6.17:80	Missing TLS SNI	
00:25:02	60	TCP:TLS.Starcraft	Missing TLS SNI	t7610winmain:57392 ⇄ 137.221.105.152:1119	Missing TLS SNI	

Showing 1 to 4 of 4 rows

Fig. : Ntopng application UI

REFERENCES

[1] https://www.geeksforgeeks.org/how-to-install-ntopng-in-linux/

[2] https://www.ntop.org/products/traffic-analysis/ntop/

[3] https://help.ubuntu.com/community/Ntop

[4] https://linuxhostsupport.com/blog/how-to-install-ntopng-on-debian-11/

[5] https://thewatch.centreon.com/product-how-to-21/