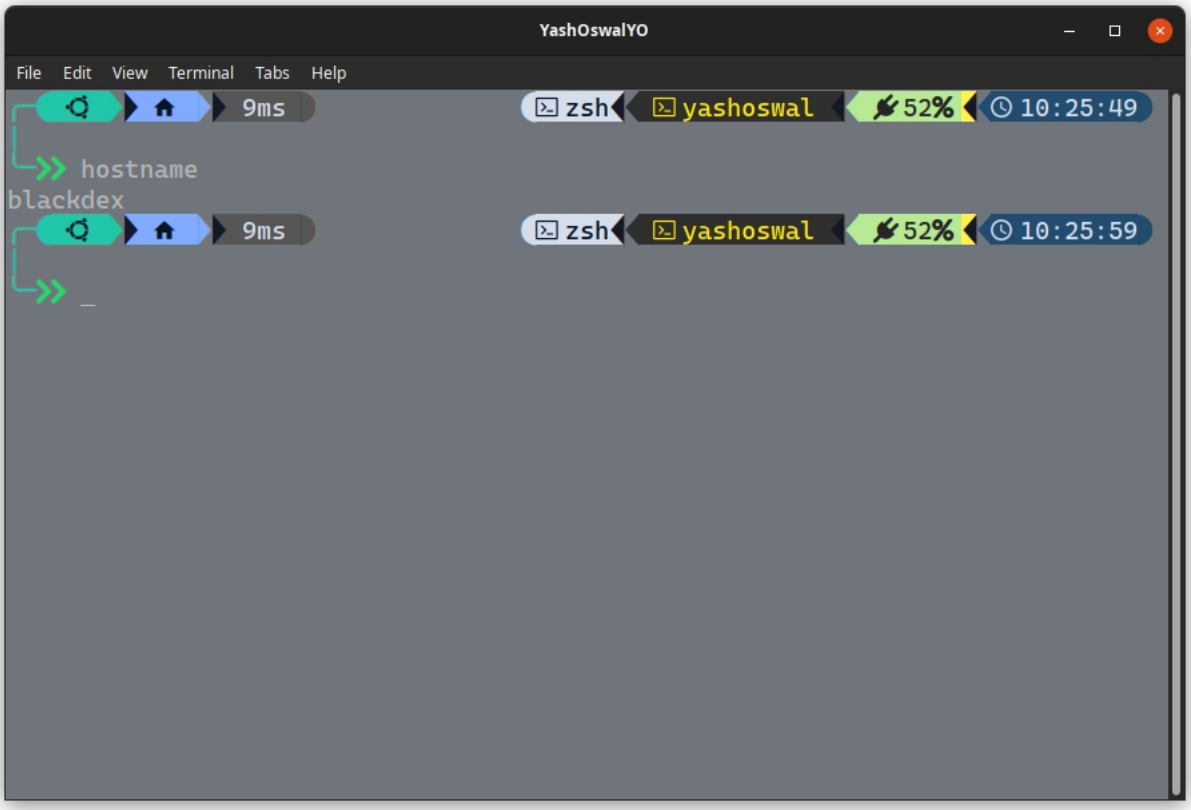
Practical – 1

Aim- Implement different basic Networking commands

Command: hostname

Description: Shows us the Host's name

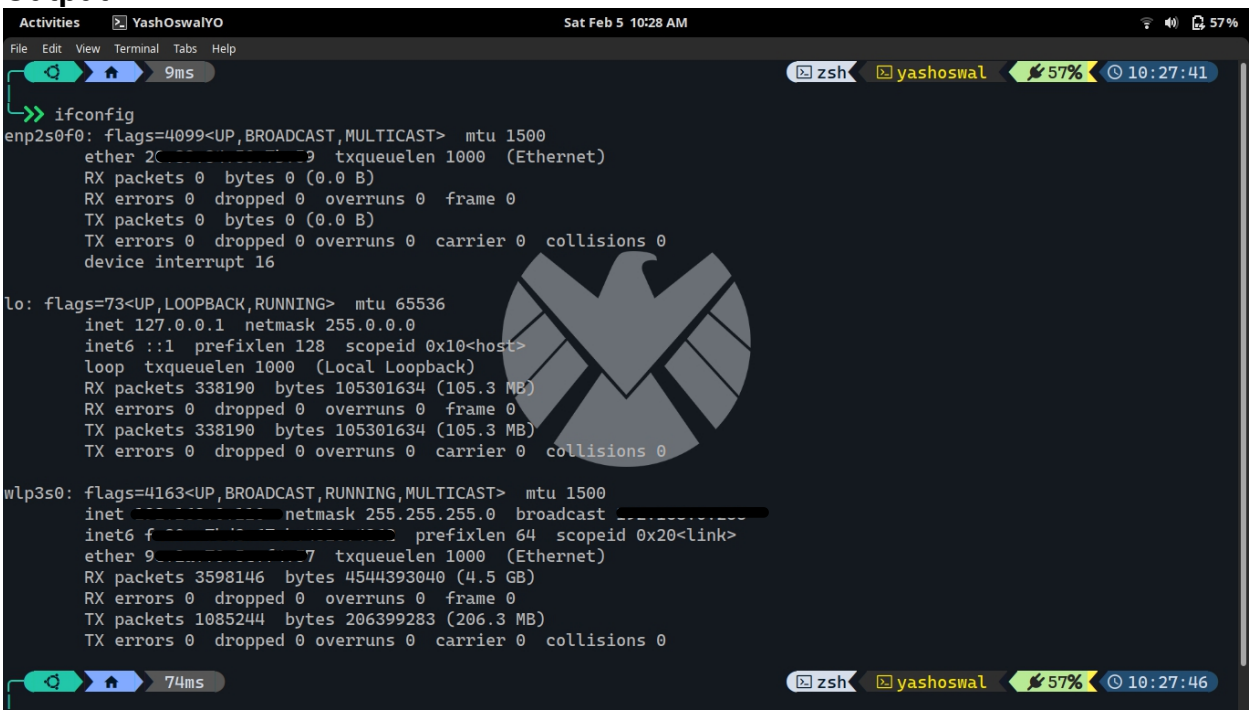
Output:



Command: ifconfig

Description: “ifconfig” Displays all current TCP/IP network configuration values and refreshes Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. If we used command without parameters, ipconfig displays Internet Protocol version 4 (IPv4) and IPv6 addresses, subnet mask, and default gateway for all adapters.

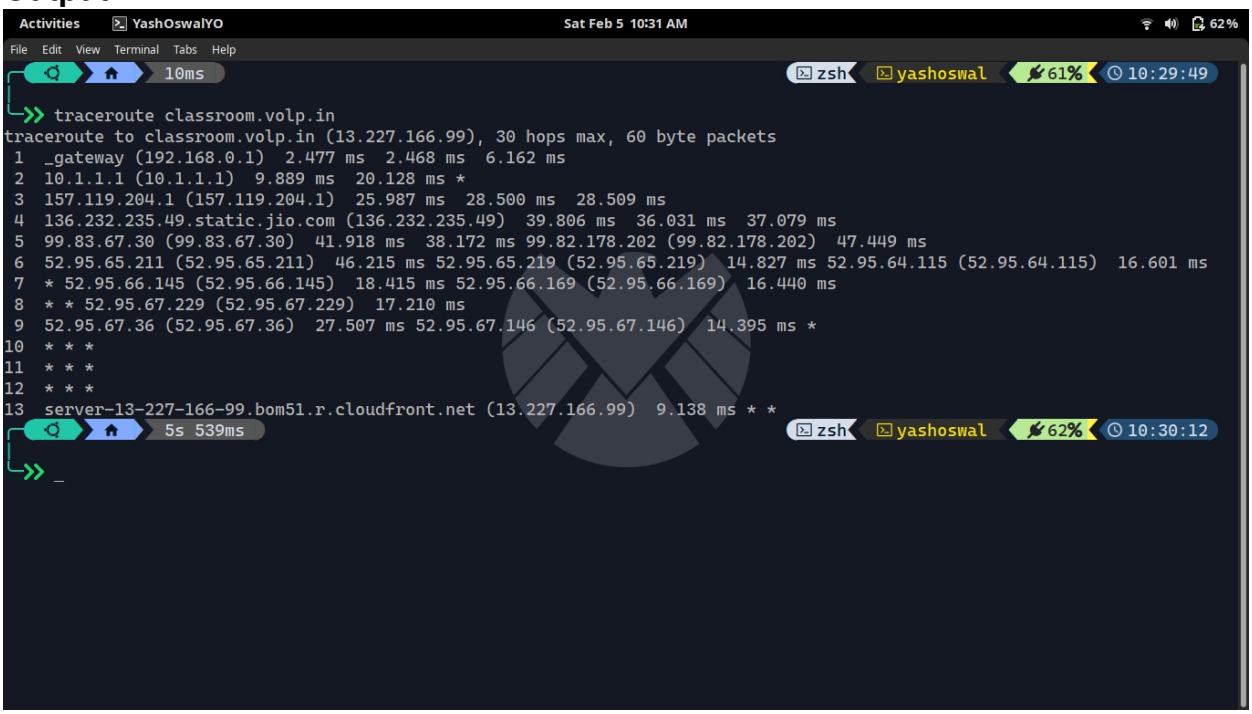
Output:



Command: traceroute <hostname>

Description: In computing, traceroute and tracert are computer network diagnostic commands for displaying possible routes and measuring transit delays of packets across an Internet Protocol network.

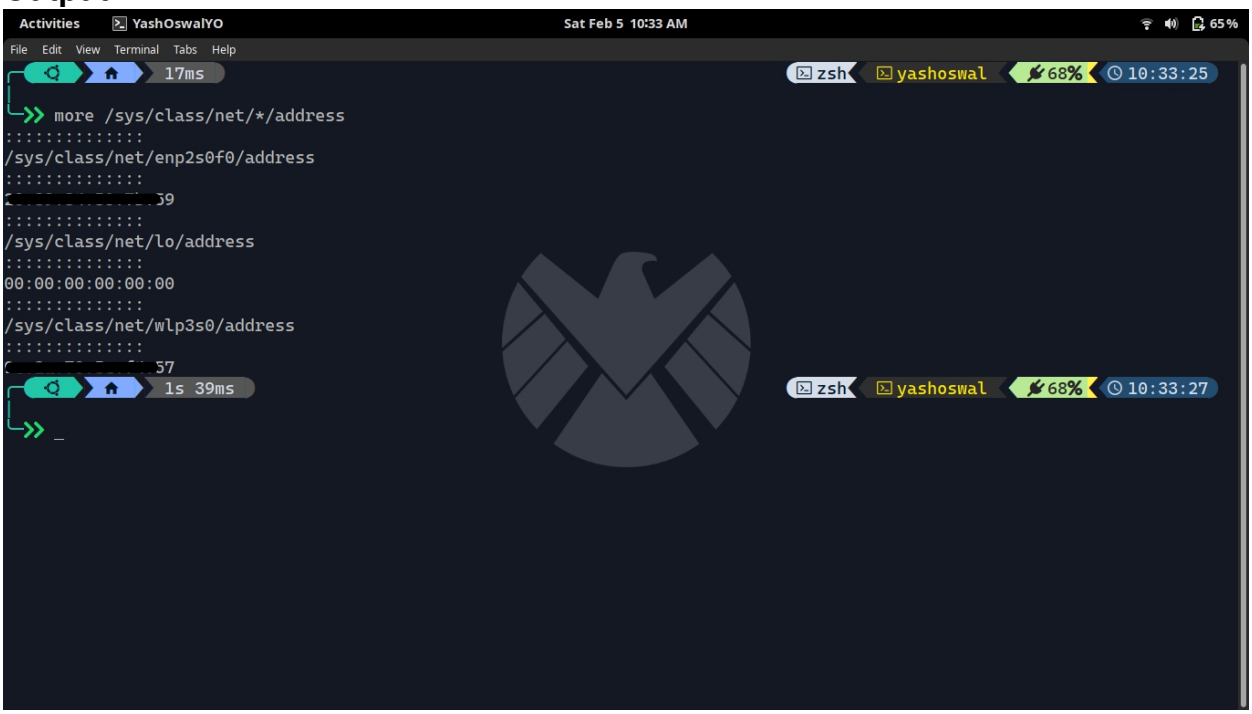
Output:



Command: more /sys/class/net/*/address

Description: Outputs mac address of all devices

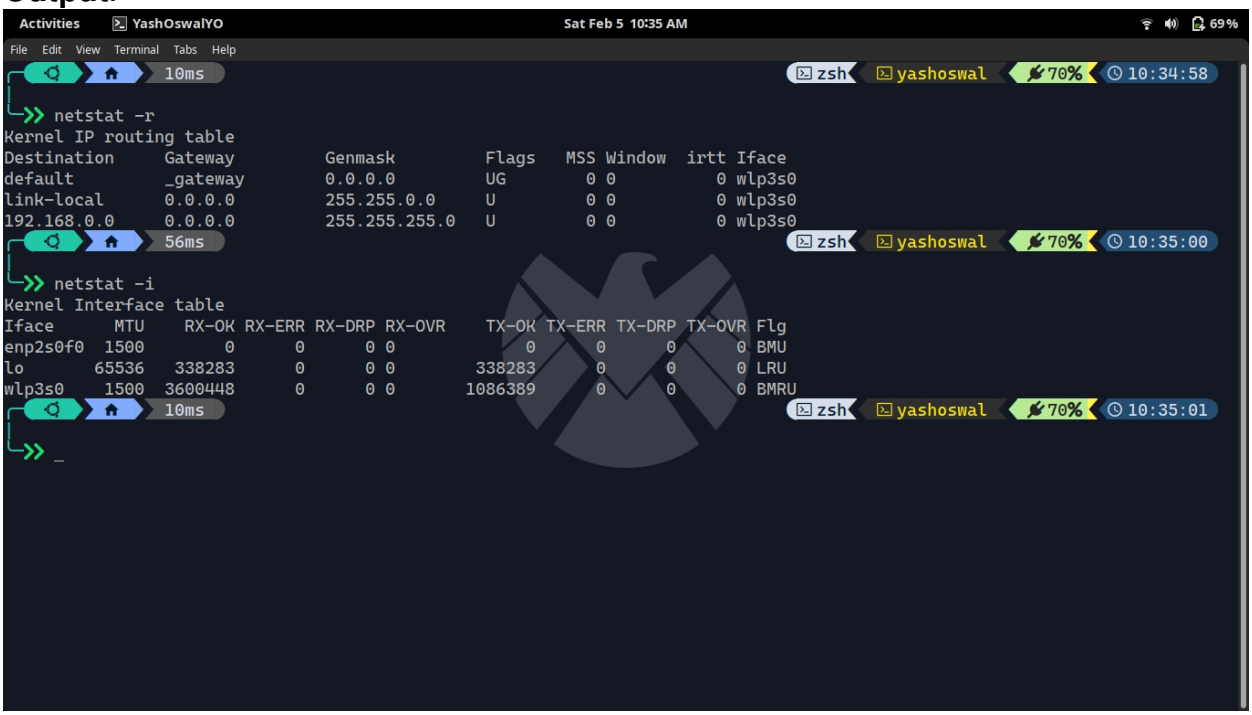
Output:



Command: netstat

Description: Print network connections, routing tables, interface statistics, masquerade connections, and multicast memberships

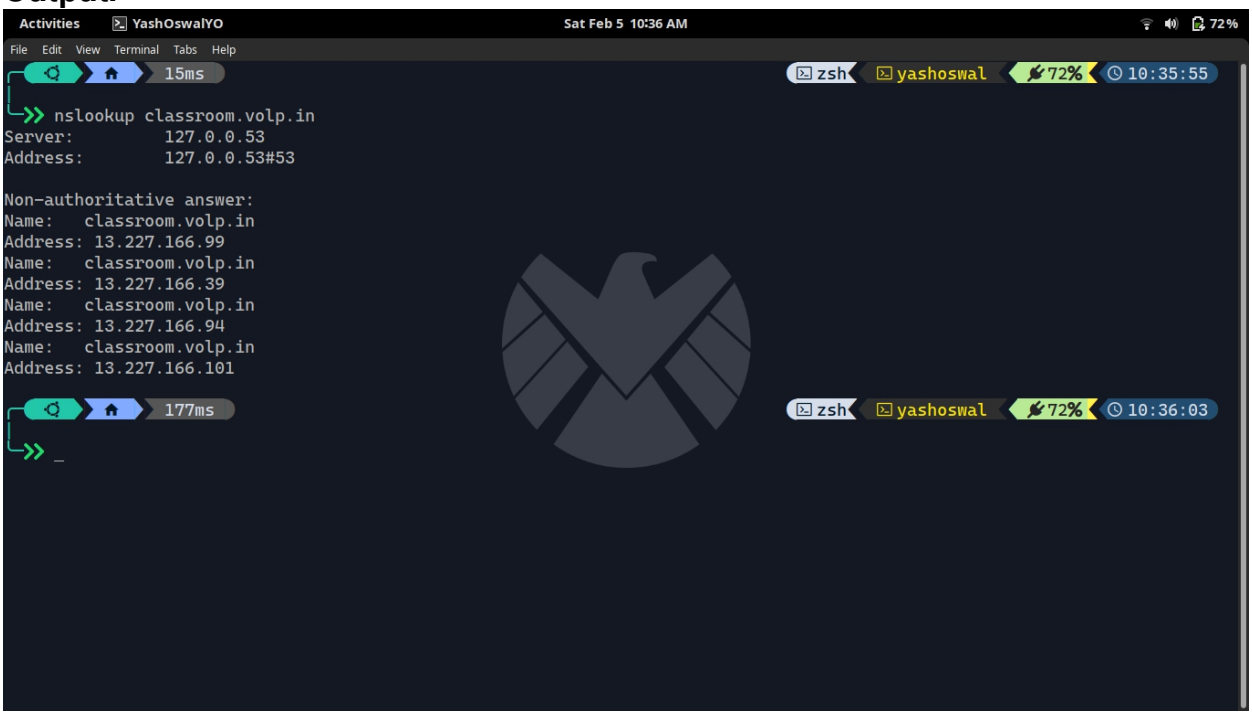
Output:



Command: nslookup <hostname>

Description: nslookup is a network administration command-line tool for querying the Domain Name System to obtain the mapping between domain name and IP address, or other DNS records

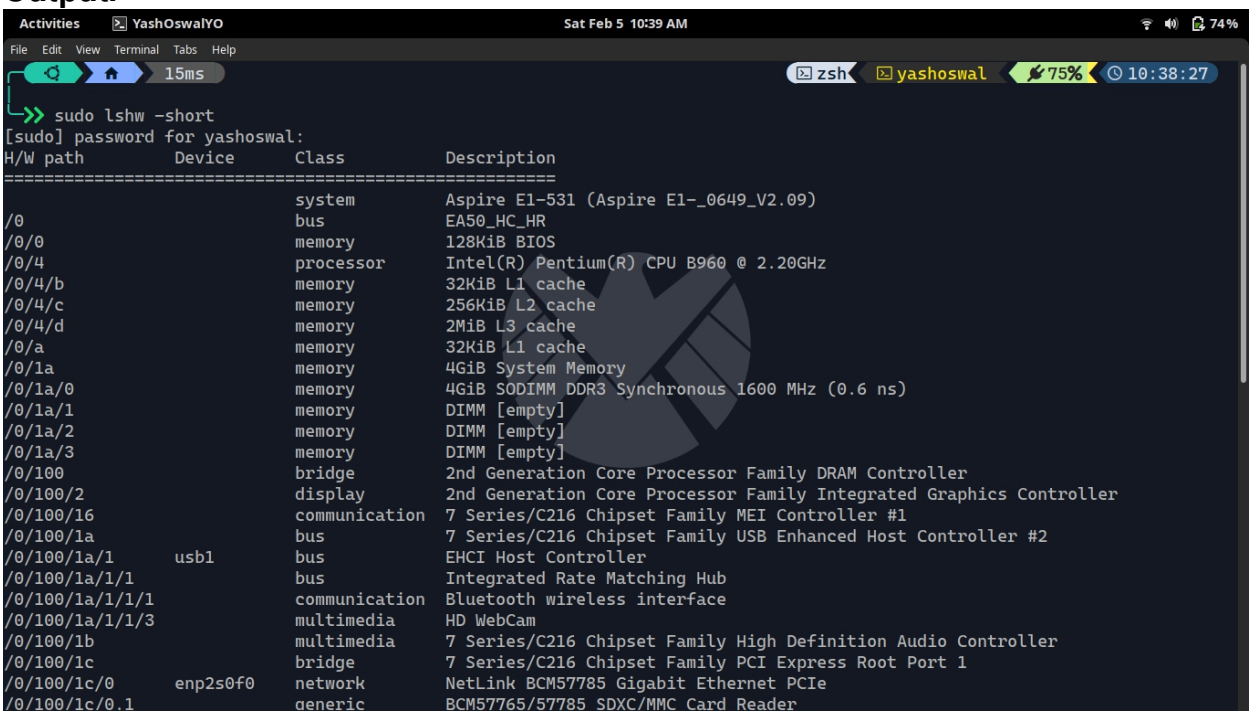
Output:



Command: sudo lshw -short

Description: lshw(list hardware) is a small Linux/Unix tool which is used to generate the detailed information of the system's hardware configuration from various files in the /proc directory.

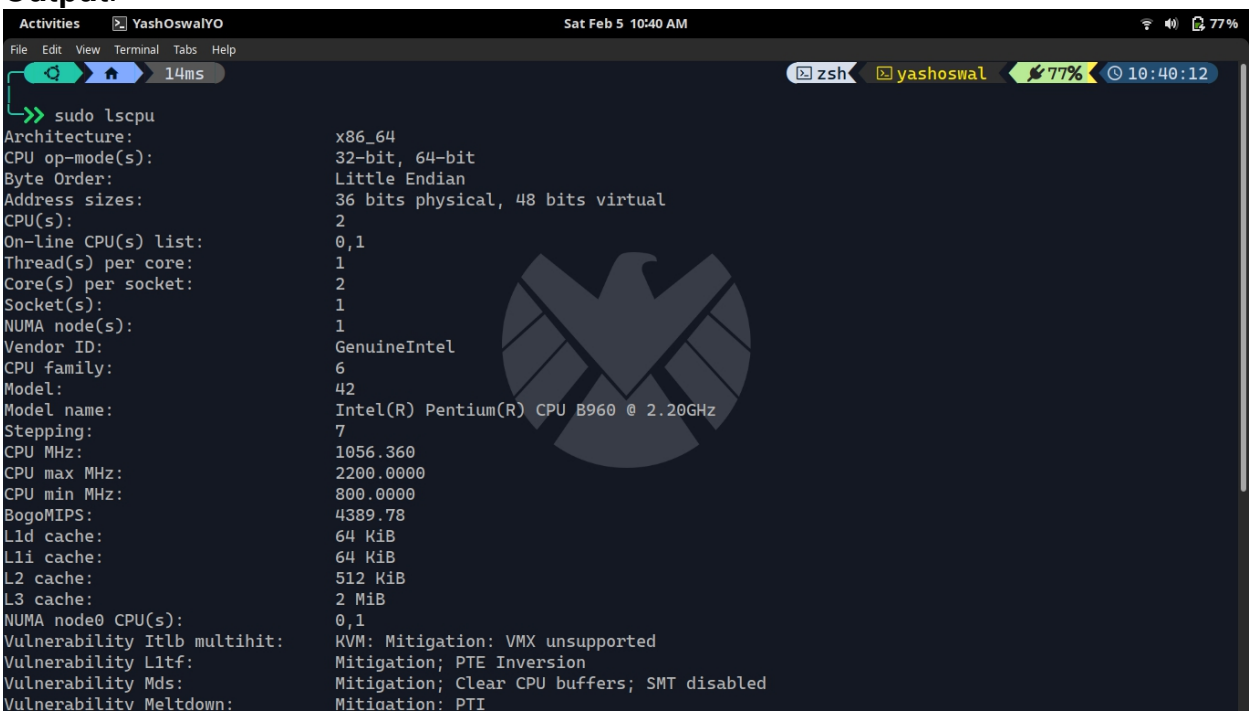
Output:



Command: sudo lscpu

Description:A command-line utility “lscpu” in Linux is used to get CPU information of the system. The “lscpu” command fetches the CPU architecture information from the “sysfs” and /proc/cpuinfo files and displays it in a terminal.

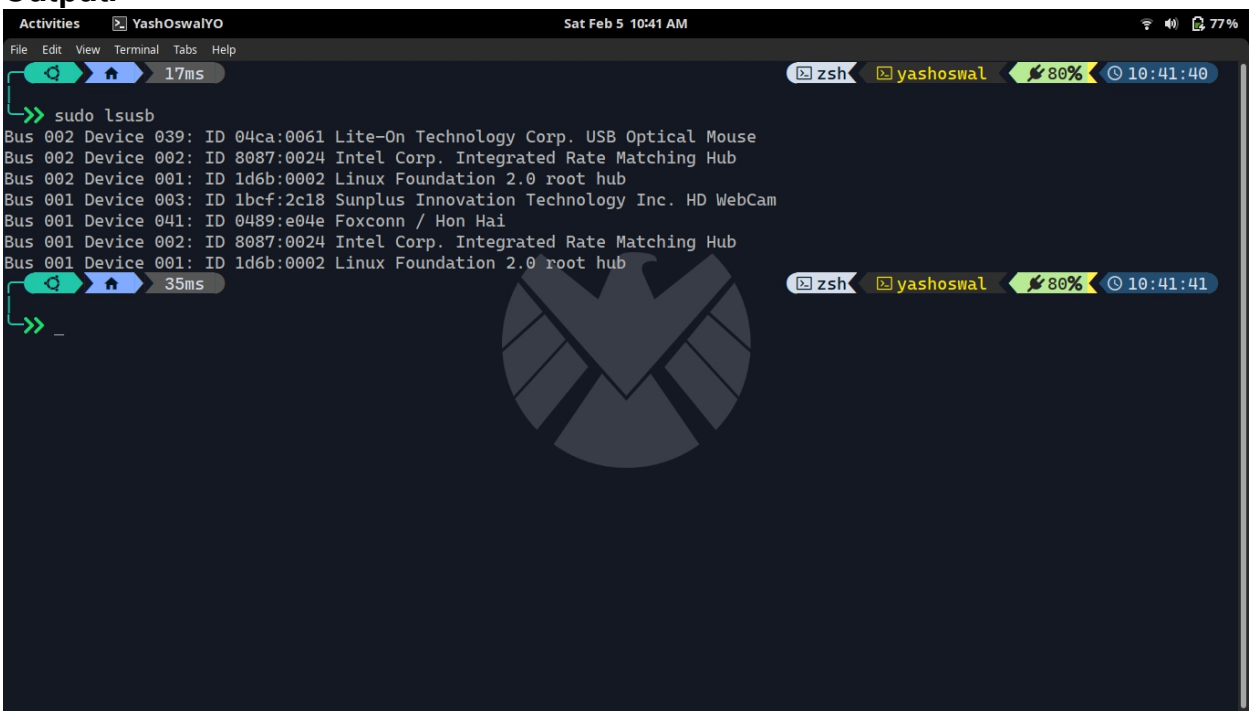
Output:



Command: sudo lsusb

Description: lsusb is a utility for displaying information about USB buses in the system and the devices connected to them.

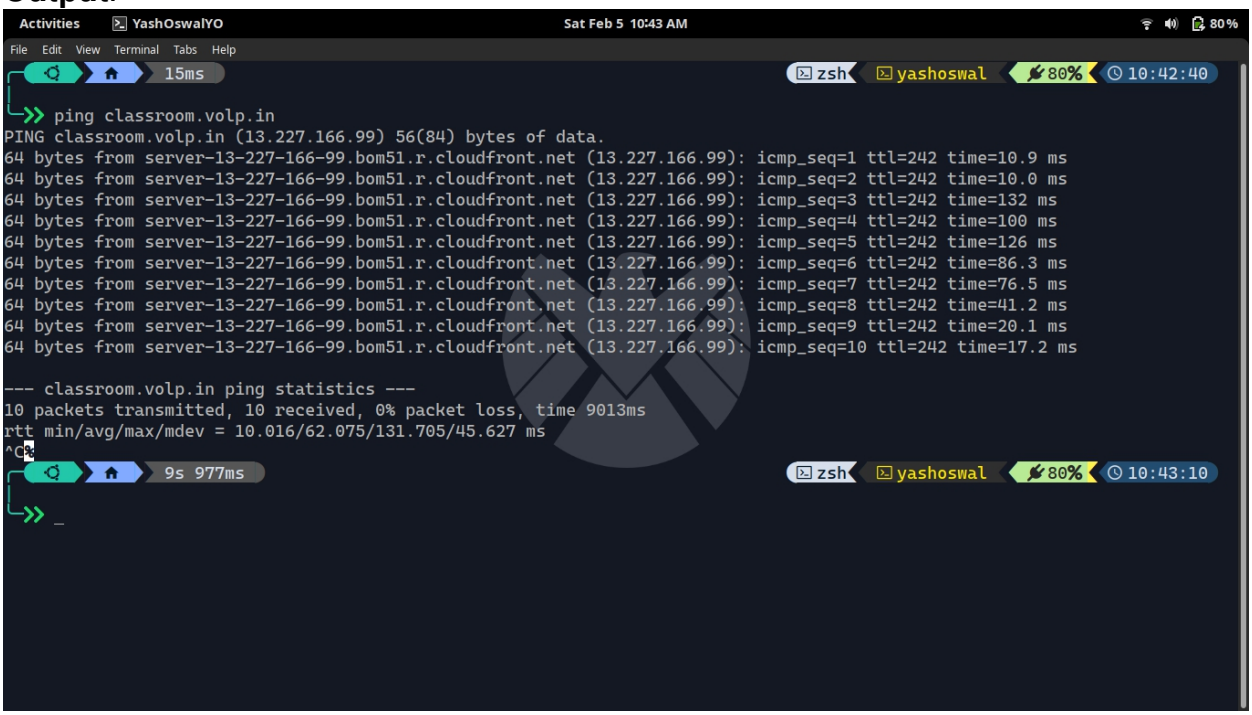
Output:



Command: ping <hostname>

Description: Ping is a command-line utility, available on virtually any operating system with network connectivity, that acts as a test to see if a networked device is reachable. The ping command sends a request over the network to a specific device.

Output:



Command: arp -a

Description: This command displays the ARP table of the active NIC. If multiple NICs are installed on the computer, we can use the -a option with this command. If the -a option is used, the ARP command displays all ARP tables.

Output:

Practical – 2

Aim- Illustrate different data protection mechanisms

Introduction: Data protection is the process of safeguarding important data from corruption, compromise or loss and providing the capability to restore the data to a functional state should something happen to render the data inaccessible or unusable.

Mechanisms:

1) Data Encryption:

Data encryption translates data into another form, or code, so that only people with access to a secret key (formally called a decryption key) or password can read it. Currently, encryption is one of the most popular and effective data security methods used by organizations. Two main types of data encryption exist - asymmetric encryption, also known as public-key encryption, and symmetric encryption.

The purpose of data encryption is to protect digital data confidentiality as it is stored on computer systems and transmitted using the internet or other computer networks. The outdated data encryption standard (DES) has been replaced by modern encryption algorithms that play a critical role in the security of IT systems and communications.

2) Data Backup to the Cloud:

Backing up your data to the cloud is one of the best ways to guard against data loss. Cloud data backup should be done on a frequent and regular basis; this is especially important for mission-critical data whose loss or corruption can severely damage normal business processes and operations. Backing up our data to the cloud allows for easy scalability; the size of our cloud data storage can be readily expanded to accommodate your data storage needs.

3) Password Protection:

Password control is the primary line of defense in safeguarding the data within your network. Sensitive information should be password protected such that only users who know the password can access the data. The password that is used to secure the data should not be used for other applications or tools; it should be strong, with a combination of letter, numbers, and special characters, as well as unique. In addition, the password should be provided only to individuals who need access to the data to carry out their job duties. Furthermore, the password should be changed on a regular basis.

4) Identity and Access Management (IAM):

One of the major ways to secure your data is to regulate the users that have access to your network, and by extension, your data. Access to your network should only be granted to individuals who need the relevant data to carry out their job duties; access should be terminated as soon as the data in your network is no longer needed. In addition, each user should have an individual user account; the use of shared accounts should be minimized as much as possible. Furthermore, for users with access to your network, only the minimum rights needed to carry out their job responsibilities should be provided; this is known as the principle of least privilege

5) Intrusion Detection and Prevention Software:

Part of keeping your data secure is monitoring and regulating the traffic in and out of your network. Prompt identification of network threats allow for necessary measures to be implemented before any significant data corruption or data loss occurs. Intrusion detection and prevention software are applications that constantly monitor network traffic for well-known threats. These applications can be configured to carry out a host of actions to neutralize any recognized network threats

Practical – 3

Aim- Inspect Wireshark Packets

Wireshark:

Wireshark is a data capturing program that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports.

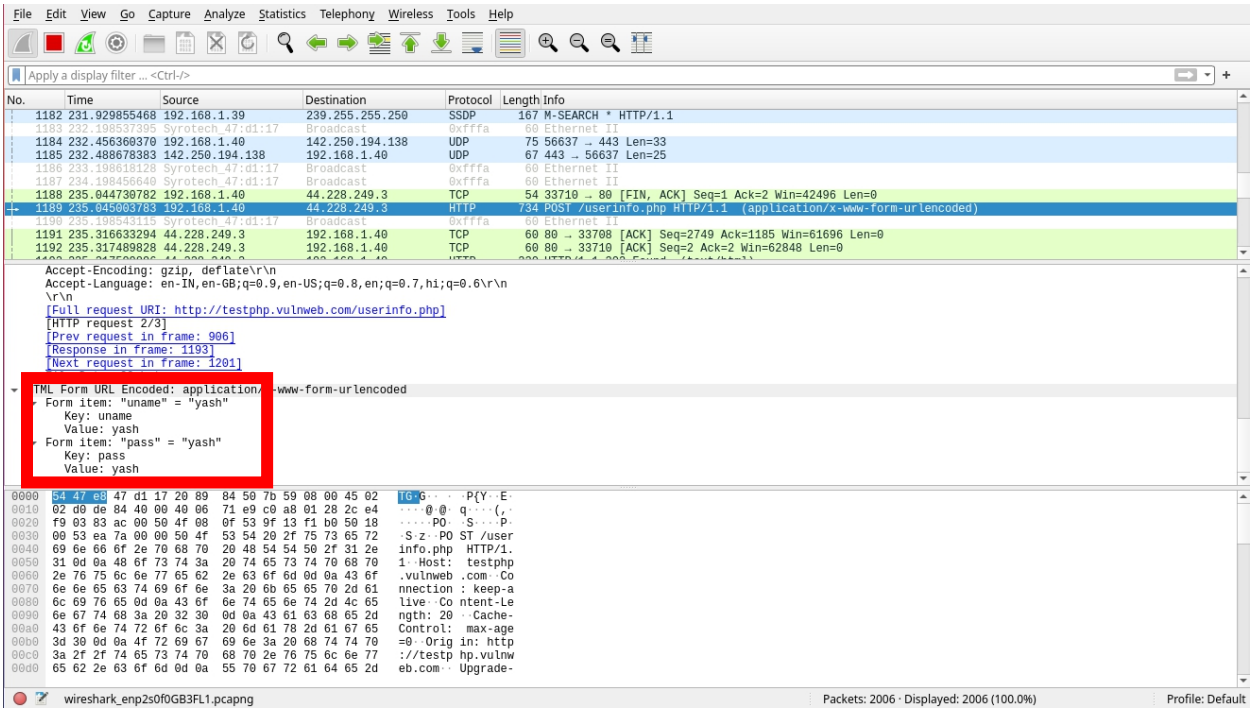
- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.
- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.
- Data display can be refined using a display filter.
- Plug-ins can be created for dissecting new protocols.[22]
- VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.
- Raw USB traffic can be captured.[23]
- Wireless connections can also be filtered as long as they traverse the monitored Ethernet.[clarification needed]
- Various settings, timers, and filters can be set to provide the facility of filtering the output of the captured traffic.

Wireshark's native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor.

Name:-Yash Oswal
Enrollment No:- 201901226

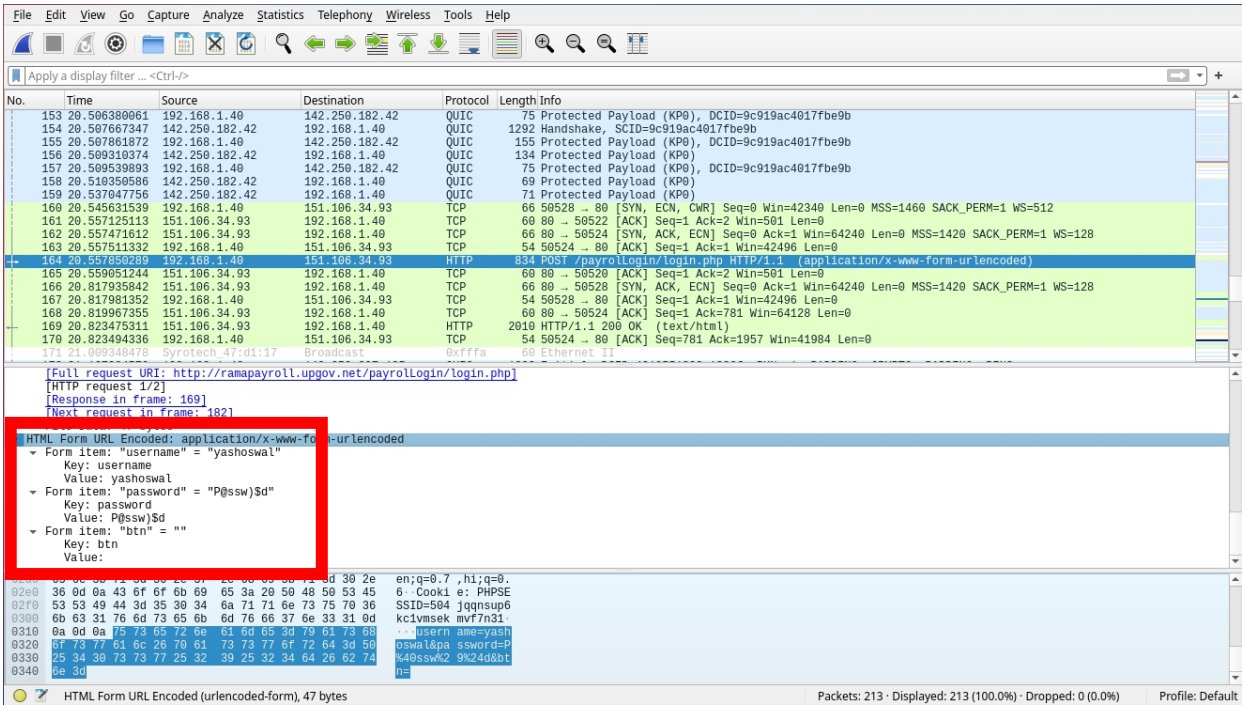
Site: http://testphp.vulnweb.com/login.php

Form data in plain text



Site: http://ramapayroll.upgov.net/payrolLogin/login.php

Username and password transferred in plain text



VISHWAKARMA UNIVERSITY
Maximising Human Potential

Practical – 5

Aim- PRTG Scanner

Introduction:

Monitor all the systems, devices, traffic, and applications in your IT infrastructure.

Everything is included with PRTG; there is no need for additional plugins or downloads.

PRTG is a powerful and easy-to-use solution, which is suitable for businesses of all sizes.

Bandwidth

Determine how much bandwidth your devices and applications are using and identify the source of bottlenecks.

Learn more

Database

Monitor specific datasets from your databases with individually-configured PRTG sensors and SQL queries.

Learn more

Application

Manage all your applications and get detailed statistics about every application running in your network.

Learn more

Name:-Yash Oswal
Enrollment No:- 201901226

Cloud

Centrally monitor and manage all your cloud computing services from anywhere.

Learn more

Server

Monitor all types of servers in real time with regard to availability, accessibility, capacity, and overall reliability.

Learn more

LAN

Keep track of your entire local network, including your workstations, routers, switches, servers, and printers.

Learn more

SNMP

Monitor a diverse range of devices using the SNMP functionality of PRTG.

Learn more

Report

Name:-Yash Oswal
Enrollment No:- 201901226

PRTG NETWORK MONITOR

Summary report for all sensors (13-04-2022 00:00:00 - 20-04-2022 00:00:00 24 / 7)

Results

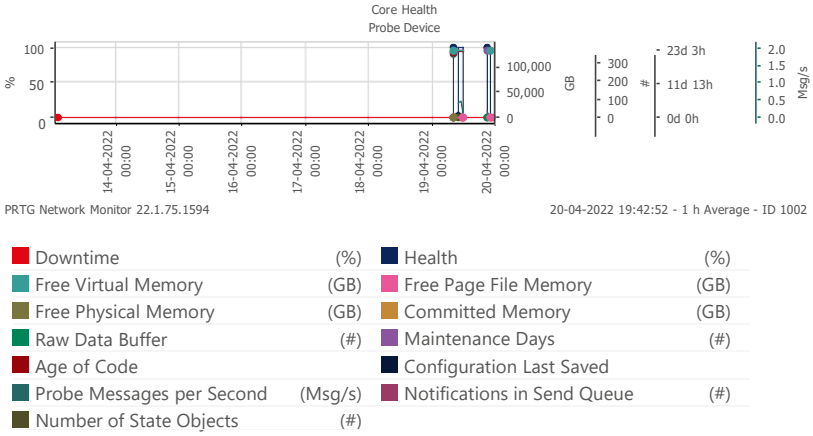
Sensor: Core Health

Local Probe (Local Probe) »

Probe, Group, Device: Probe Device

Average (Health): 100 %

Up:	100 %	[02h 12m 14s]
Down:	0 %	[00s]
Good:	100 %	[137]
Failed:	0 %	[0]



Downtime	(%)	Health	(%)
Free Virtual Memory	(GB)	Free Page File Memory	(GB)
Free Physical Memory	(GB)	Committed Memory	(GB)
Raw Data Buffer	(#)	Maintenance Days	(#)
Age of Code		Configuration Last Saved	
Probe Messages per Second	(Msg/s)	Notifications in Send Queue	(#)
Number of State Objects	(#)		

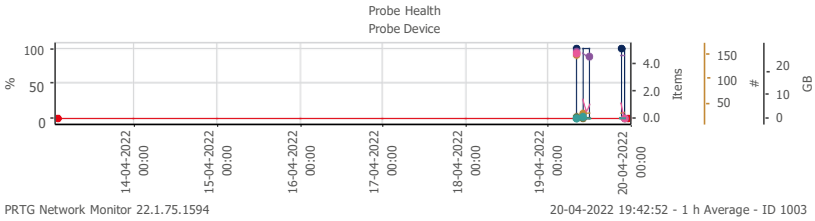
Sensor: Probe Health

Local Probe (Local Probe) »

Probe, Group, Device: Probe Device

Average (Health): 100 %

Up:	100 %	[02h 12m 14s]
Down:	0 %	[00s]
Good:	100 %	[137]
Failed:	0 %	[0]



Downtime	(%)	Health	(%)
Message Queue	(Items)	Open Requests	(Items)
Probe Process CPU Load	(%)	Threads	(#)
Memory Usage	(GB)	Data Storage Free	(GB)

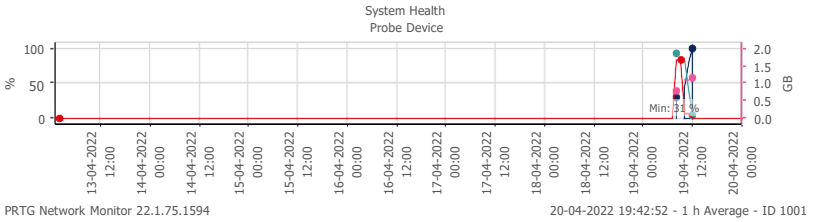
Sensor: System Health

Local Probe (Local Probe) »

Probe, Group, Device: Probe Device

Average (Health): 75 %

Up:	85 %	[01h 17m 47s]
Down:	15 %	[13m 20s]
Good:	73 %	[70]
Failed:	27 %	[26]



Downtime	(%)	Health	(%)
System CPU Load	(%)	Available Memory	(GB)

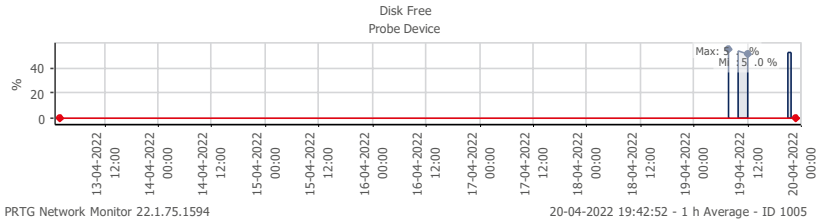
Sensor: Disk Free

Local Probe (Local Probe) »

Probe, Group, Device: Probe Device

Average (Free Space C:): 53 %

Up:	100 %	[02h 13m 14s]
Down:	0 %	[00s]
Good:	100 %	[138]
Failed:	0 %	[0]



Downtime	(%)	Free Space C:	(%)

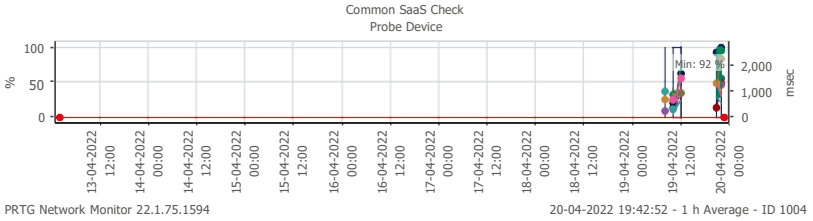
Sensor: Common SaaS Check

Local Probe (Local Probe) »

Probe, Group, Device: Probe Device

Average (Available Services): 98 %

Up:	100 %	[01h 45m 13s]
Down:	0 %	[00s]
Good:	100 %	[12]



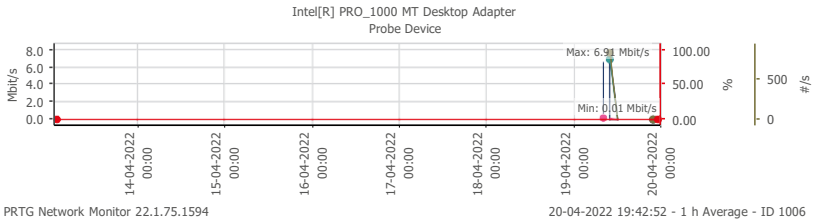
Failed:	0 %	[0]

Downtime (%) | Available Services (%)
Office 365 (msec) | Bing (msec)
Google Apps (msec) | Dropbox (msec)
Salesforce (msec) | GitHub (msec)
Facebook (msec) | Twitter (msec)
Youtube (msec)

Sensor: Intel[R] PRO_1000 MT Desktop Adapter

Local Probe (Local Probe) »
Probe, Group, Device: Probe Device

Average (Total):	2.51 Mbit/s	
Total (Total):	2,369 MB	
Up:	100 %	[02h 09m 11s]
Down:	0 %	[00s]
Good:	100 %	[134]
Failed:	0 %	[0]

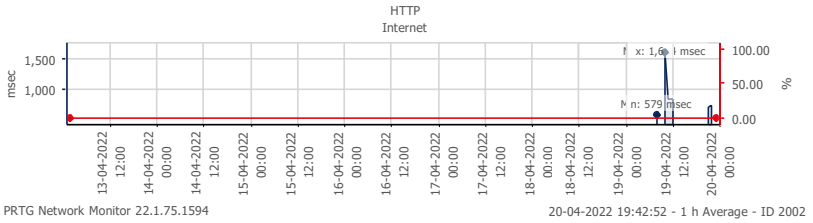


Downtime (%) | Total (Mbit/s)
Traffic in (Mbit/s) | Traffic out (Mbit/s)
Packets (#/s)

Sensor: HTTP

Local Probe (Local Probe) »
Network Infrastructure »
Probe, Group, Device: Internet

Average (Loading time):	891 msec	
Up:	100 %	[02h 11m 14s]
Down:	0 %	[00s]
Good:	98.529 %	[134]
Failed:	1.471 %	[2]

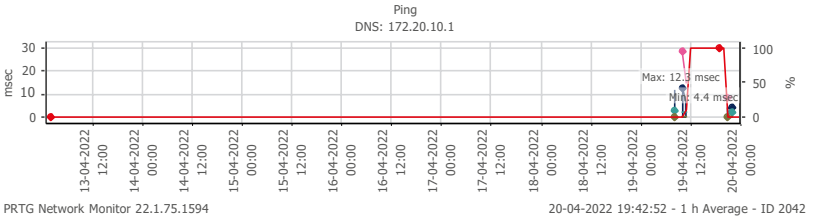


Downtime (%) | Loading time (msec)

Sensor: Ping

Local Probe (Local Probe) »
Network Infrastructure »
Probe, Group, Device: DNS: 172.20.10.1

Average (Ping Time):	7 msec	
Up:	87 %	[01h 55m 14s]
Down:	13 %	[16m 30s]
Good:	86 %	[231]
Failed:	14 %	[39]

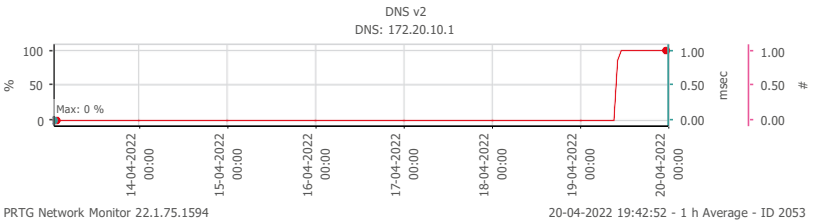


Downtime (%) | Ping Time (msec)
Minimum (msec) | Maximum (msec)
Packet Loss (%)

Sensor: DNS v2

Local Probe (Local Probe) »
Network Infrastructure »
Probe, Group, Device: DNS: 172.20.10.1

Average (Records Resolved):	No data	
Up:	1.58 %	[02m 00s]
Down:	98.42 %	[02h 04m 34s]
Good:	0 %	[0]
Failed:	100 %	[129]

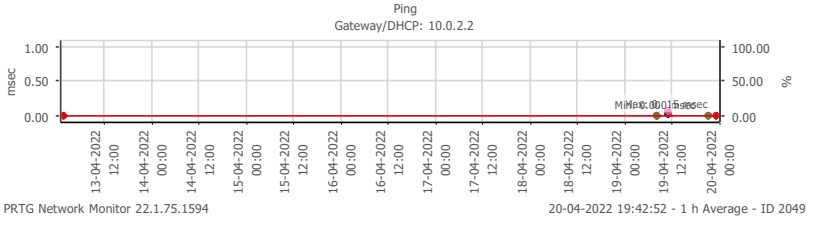


Downtime (%) | Records Resolved
Response Time (msec) | Record Count (#)

Sensor: Ping

Local Probe (Local Probe) »
Network Infrastructure »
Probe, Group, Device: Gateway/DHCP: 10.0.2.2

Average (Ping Time):	0 msec	
Up:	100 %	[02h 10m 43s]
Down:	0 %	[00s]
Good:	100 %	[266]
Failed:	0 %	[0]



Downtime (%) | Ping Time (msec)
Minimum (msec) | Maximum (msec)
Packet Loss (%)

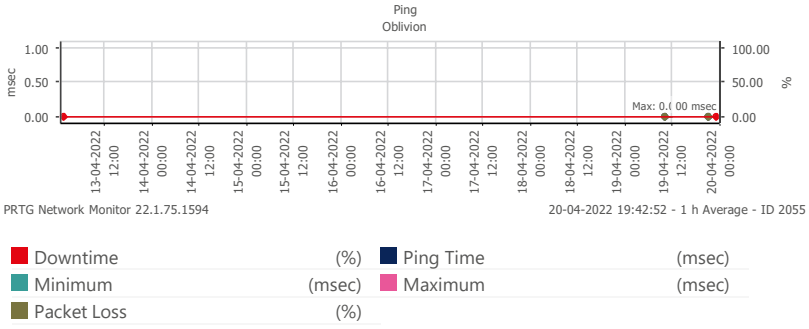
Sensor: Ping

Local Probe (Local Probe) »
Clients »

Probe, Group, Device: Oblivion

Average (Ping Time): 0 msec

Up:	100 %	[01h 56m 49s]
Down:	0 %	[00s]
Good:	100 %	[120]
Failed:	0 %	[0]



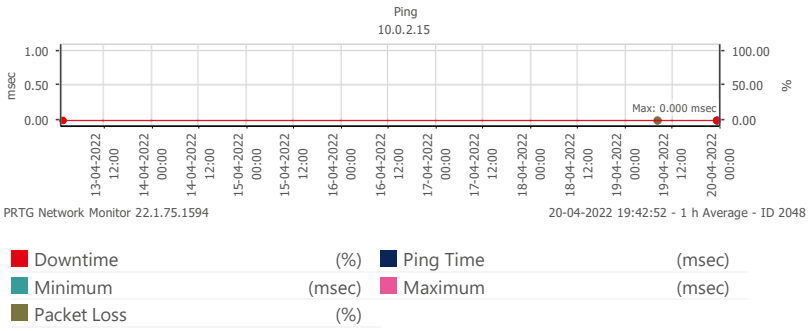
Sensor: Ping

Local Probe (Local Probe) »
Subnet 10.0.2 »

Probe, Group, Device: 10.0.2.15

Average (Ping Time): 0 msec

Up:	100 %	[03m 01s]
Down:	0 %	[00s]
Good:	100 %	[10]
Failed:	0 %	[0]



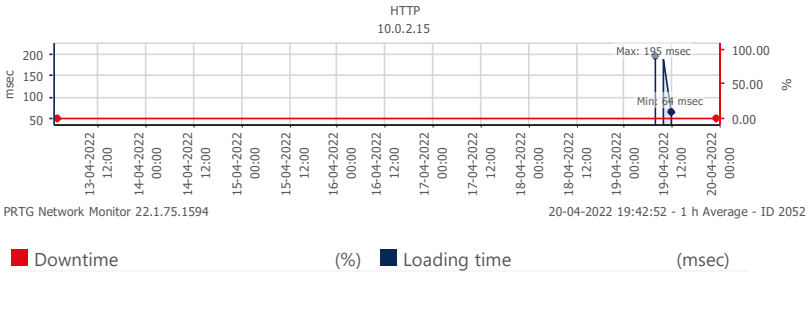
Sensor: HTTP

Local Probe (Local Probe) »
Subnet 10.0.2 »

Probe, Group, Device: 10.0.2.15

Average (Loading time): 124 msec

Up:	100 %	[01h 26m 06s]
Down:	0 %	[00s]
Good:	100 %	[90]
Failed:	0 %	[0]



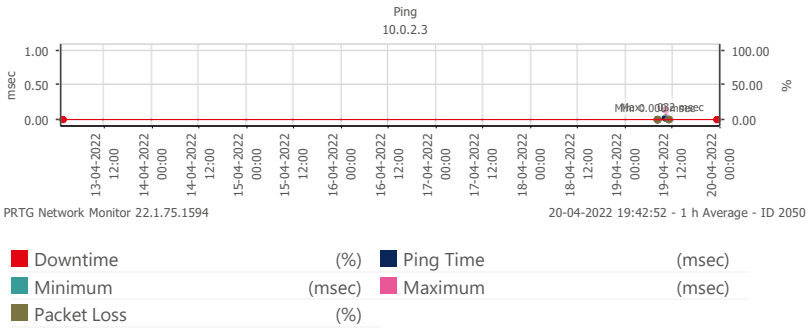
Sensor: Ping

Local Probe (Local Probe) »
Subnet 10.0.2 »

Probe, Group, Device: 10.0.2.3

Average (Ping Time): 0 msec

Up:	100 %	[01h 28m 06s]
Down:	0 %	[00s]
Good:	100 %	[180]
Failed:	0 %	[0]



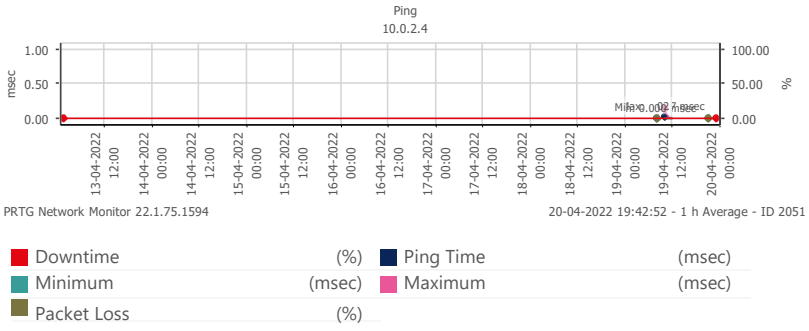
Sensor: Ping

Local Probe (Local Probe) »
Subnet 10.0.2 »

Probe, Group, Device: 10.0.2.4

Average (Ping Time): 0 msec

Up:	100 %	[02h 10m 44s]
Down:	0 %	[00s]
Good:	100 %	[265]
Failed:	0 %	[0]



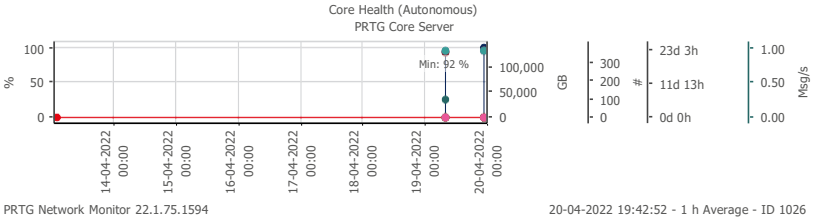
Sensor: Core Health (Autonomous)

Probe, Group, Device: PRTG Core Server

Average (Health): 94 %

Up:	100 %	[06m 05s]

Down:	0 %	[00s]
Good:	100 %	[11]
Failed:	0 %	[0]



Downtime	(%)	Health	(%)
Free Virtual Memory	(GB)	Free Page File Memory	(GB)
Free Physical Memory	(GB)	Committed Memory	(GB)
Raw Data Buffer	(#)	Maintenance Days	(#)
Age of Code		Configuration Last Saved	
Probe Messages per Second	(Msg/s)	Notifications in Send Queue	(#)
Number of State Objects	(#)		

Practical – 6

Aim- Nessus Report

What is Nessus?

Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Who would use a tool like this?

If you are an administrator in charge of any computer (or group of computers) connected to the internet, Nessus is a great tool help keep their domains free of the easy vulnerabilities that hackers and viruses commonly look to exploit.

What Nessus is NOT

Nessus is not a complete security solution, rather it is one small part of a good security strategy. Nessus does not actively prevent attacks, it is only a tool that checks your computers to find vulnerabilities that hackers COULD exploit. IT IS UP TO THE SYSTEM ADMINISTRATOR TO PATCH THESE VULNERABILITIES IN ORDER TO CREATE A SECURITY SOLUTION.

Why Nessus?

If you are familiar with other network vulnerability scanners, you might be wondering what advantages Nessus has over them. Key points include:

- Unlike other scanners, Nessus does not make assumptions about your server configuration (such as assuming that port 80 must be the only web server) that can cause other scanners to miss real vulnerabilities.

- Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. Its also provides a plug-in interface, and many free plug-ins are available from the Nessus plug-in site. These plugs are often specific to detecting a common virus or vulnerability.

- Up to date information about new vulnerabilities and attacks. The Nessus team updates the list of what vulnerabilities to check for on a daily basis in order to minimize

the window between an exploit appearing in the wild, and you being able to detect it with Nessus

- Open-source. Nessus is open source, meaning it costs nothing, and you are free to see and modify the source as you wish.

- Patching Assistance: When Nessus detects a vulnerability, it is also most often able to suggest the best way you can mitigate the vulnerability.

For other advantages/features of Nessus, see: http://www.nessus.org/features.html

How Nessus Works

To learn how Nessus and other port-scanning security tools work, it is necessary to understand different services (such as a web server, SMTP server, FTP server, etc) are accessed on a remote server. Most high-level network traffic, such as email, web pages, etc reach a server via a high-level protocol that is transmitted reliably by a TCP stream. To keep different streams from interfering with each other, a computer divides its physical connection to the network into thousands of logical paths, called ports. So if you want to talk to a web server on a given machine, you would connect to port #80 (the standard HTTP port), but if you wanted to connect to an SMTP server on that same machine you would instead connect to port #25.

Each computer has thousands of ports, all of which may or may not have services (ie: a server for a specific high-level protocol) listening on them. Nessus works by testing each port on a computer, determining what service it is running, and then testing this service to make sure there are no vulnerabilities in it that could be used by a hacker to carry out a malicious attack. Nessus is called a "remote scanner" because it does not need to be installed on a computer for it to test that computer. Instead, you can install it on only one computer and test as many computers as you would like.

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

ppup.ac.in

Vulnerabilities Total: 62

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRITICAL	10.0	58987	PHP Unsupported Version Detection
HIGH	7.5	142591	PHP < 7.3.24 Multiple Vulnerabilities
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.9	31705	SSL Anonymous Cipher Suites Supported
MEDIUM	5.9	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
MEDIUM	5.3	152853	PHP < 7.3.28 Email Header Injection
MEDIUM	5.3	15901	SSL Certificate Expiry
MEDIUM	5.3	45411	SSL Certificate with Wrong Hostname
MEDIUM	6.4*	57582	SSL Self-Signed Certificate
LOW	2.6*	15855	POP3 Cleartext Logins Permitted
LOW	2.6*	54582	SMTP Service Cleartext Login Permitted
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	39520	Backported Security Patch Detection (SSH)
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type

INFO	N/A	10092	FTP Server Detection
INFO	N/A	42149	FTP Service AUTH TLS Command Support
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	85805	HTTP/2 Cleartext Detection
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11414	IMAP Service Banner Retrieval
INFO	N/A	42085	IMAP Service STARTTLS Command Support
INFO	N/A	10719	MySQL Server Detection
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	11936	OS Identification
INFO	N/A	117886	OS Security Patch Assessment Not Available
INFO	N/A	10919	Open Port Re-check
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	10185	POP Server Detection
INFO	N/A	42087	POP3 Service STLS Command Support
INFO	N/A	54580	SMTP Authentication Methods
INFO	N/A	10263	SMTP Server Detection
INFO	N/A	42088	SMTP Service STARTTLS Command Support
INFO	N/A	10267	SSH Server Type and Version Information
INFO	N/A	56984	SSL / TLS Versions Supported

INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	22964	Service Detection
INFO	N/A	11153	Service Detection (HELP Request)
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	10287	Traceroute Information
INFO	N/A	100669	Web Application Cookies Are Expired
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	11424	WebDAV Detection

* indicates the v3.0 score was not available; the v2.0 score is shown