

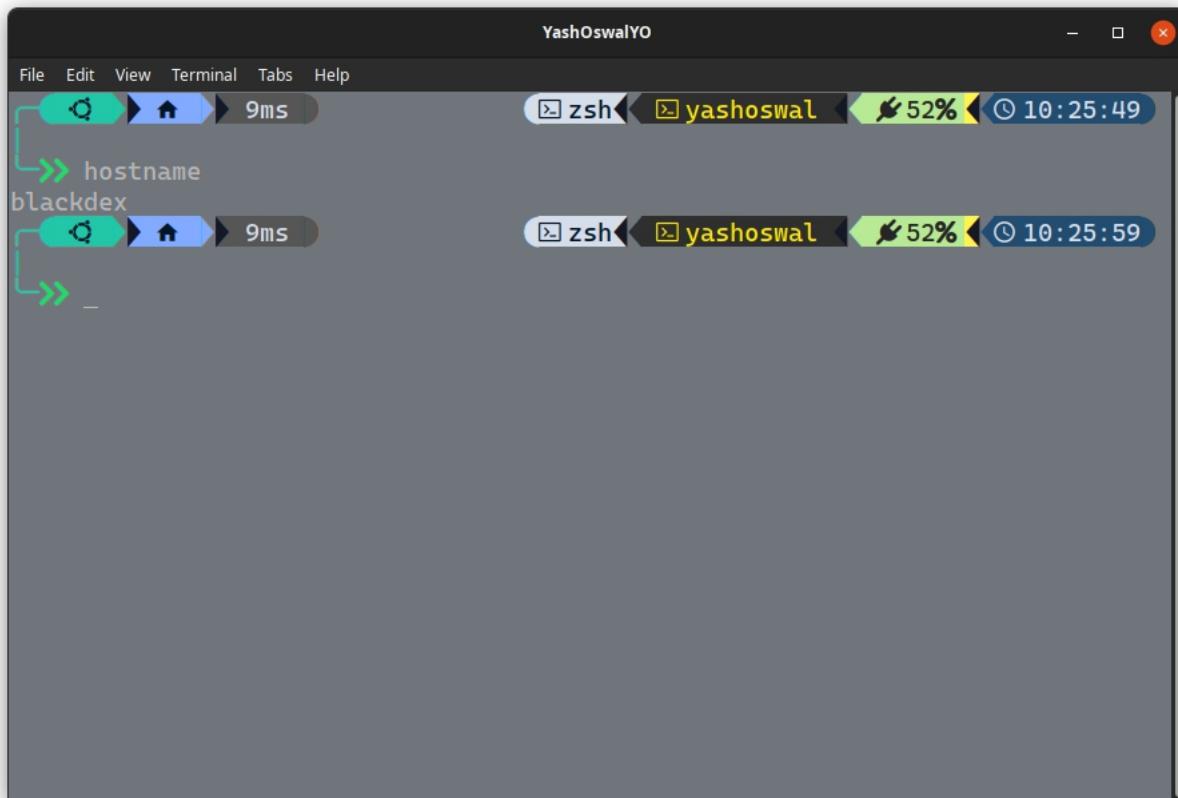
## Practical – 1

**Aim-** Implement different basic Networking commands

**Command:** hostname

**Description:** Shows us the Host's name

**Output:**

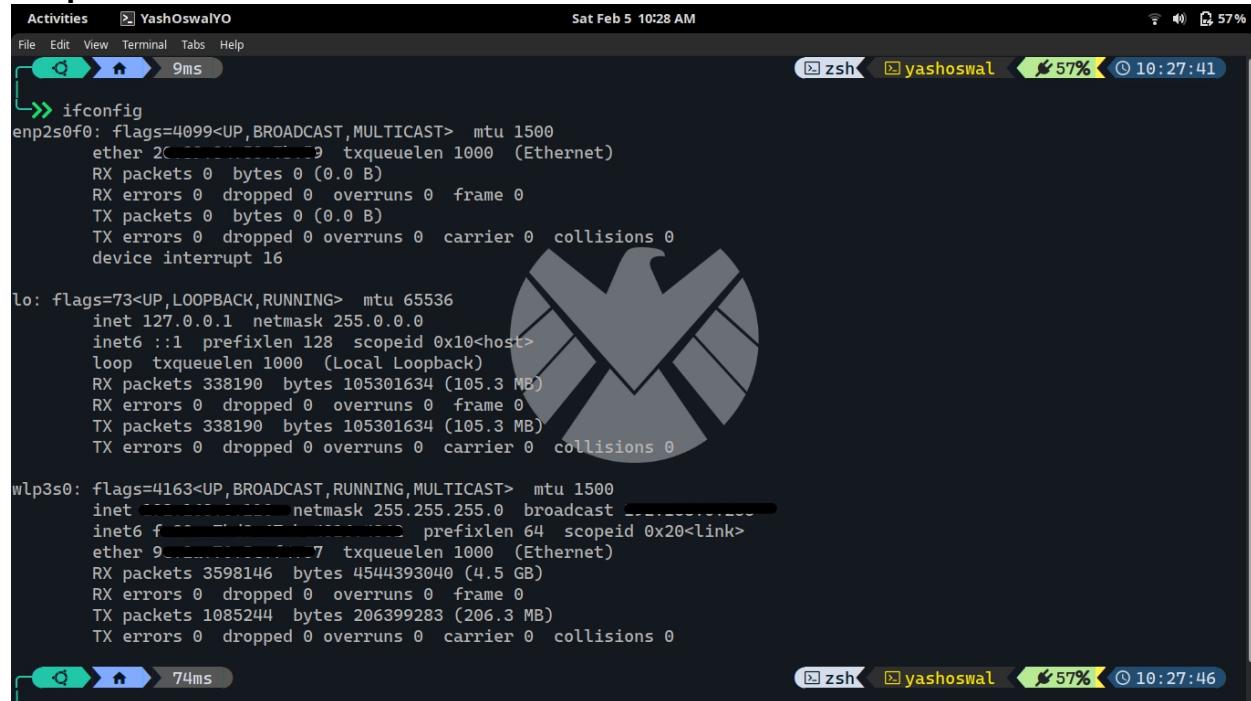


The screenshot shows a terminal window titled "YashOswalYO". The window has a dark theme with light-colored text. At the top, there is a menu bar with options: File, Edit, View, Terminal, Tabs, Help. Below the menu is a toolbar with icons for search, home, and refresh, followed by the text "9ms". On the right side of the window, there is a system tray showing a zsh icon, a user icon "yashoswal", a battery icon at 52%, and a clock icon showing the time as 10:25:49. The main area of the terminal displays the command "hostname" and its output "blackdex". Below this, there is another prompt "blackdex" and a blank line. The bottom of the window shows a footer with the text "zsh" and "yashoswal" again, along with the battery and clock icons.

## 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:



```

Activities  YashOswalYO
File Edit View Terminal Tabs Help
Sat Feb 5 10:28 AM
File Edit View Terminal Tabs Help
zsh  yashoswal  57%  10:27:41

>> ifconfig
enp2s0f0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 2C:...:9 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 16

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
        loop txqueuelen 1000 (Local Loopback)
        RX packets 338190 bytes 105301634 (105.3 MB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 338190 bytes 105301634 (105.3 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlp3s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet ... netmask 255.255.255.0 broadcast ...
    inet6 f... prefixlen 64 scopeid 0x20<link>
        ether 9... txqueuelen 1000 (Ethernet)
        RX packets 3598146 bytes 4544393040 (4.5 GB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1085244 bytes 206399283 (206.3 MB)
        TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

**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:**



The screenshot shows a terminal window titled "Activities" with the user "YashOswalYO". The terminal is running on "zsh" and shows the command "traceroute classroom.volp.in" being executed. The output of the traceroute command is displayed, showing the path from the user's machine to the destination server. The terminal window has a dark background with light-colored text. The status bar at the bottom right shows battery level (62%), signal strength, and the current time (10:29:49).

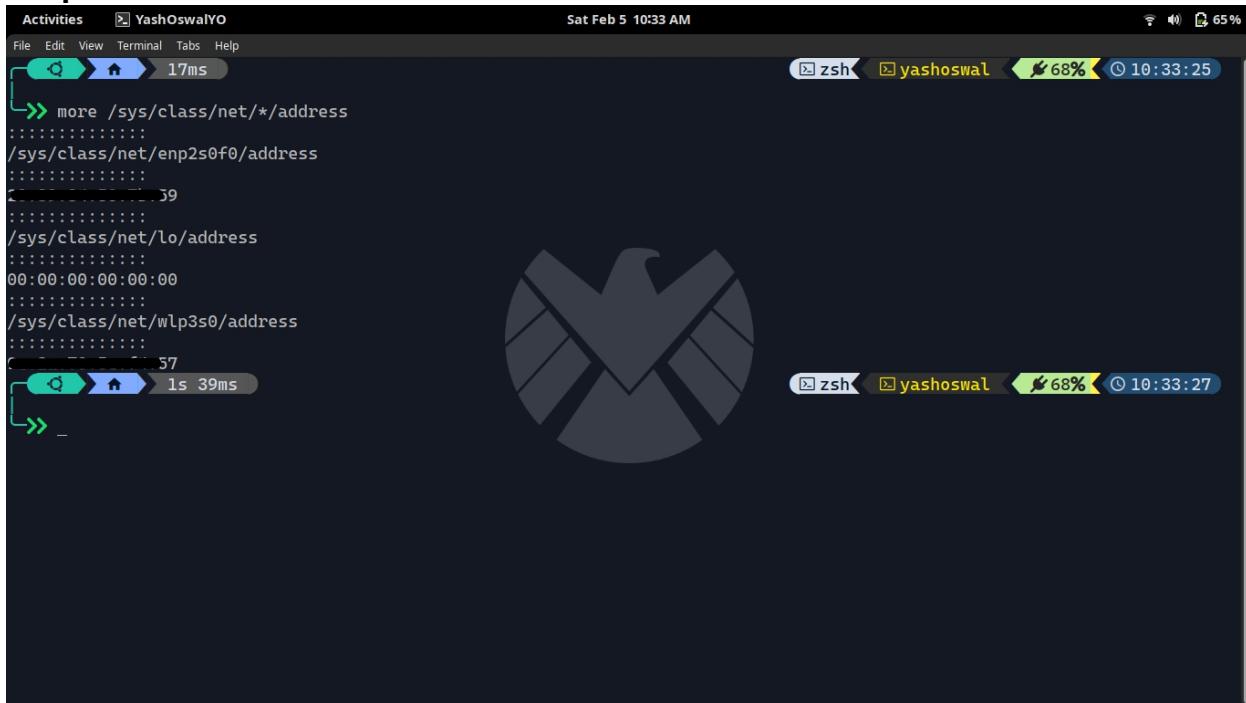
```
Activities [YashOswalYO]
File Edit View Terminal Tabs Help Sat Feb 5 10:31 AM
File Edit View Terminal Tabs Help zsh yashoswal 61% 10:29:49
traceroute to classroom.volp.in (13.227.166.99), 30 hops max, 60 byte packets
1 _gateway (192.168.0.1) 2.477 ms 2.468 ms 6.162 ms
2 10.1.1.1 (10.1.1.1) 9.889 ms 20.128 ms *
3 157.119.204.1 (157.119.204.1) 25.987 ms 28.500 ms 28.509 ms
4 136.232.235.49.static.jio.com (136.232.235.49) 39.806 ms 36.031 ms 37.079 ms
5 99.83.67.30 (99.83.67.30) 41.918 ms 38.172 ms 99.82.178.202 (99.82.178.202) 47.449 ms
6 52.95.65.211 (52.95.65.211) 46.215 ms 52.95.65.219 (52.95.65.219) 14.827 ms 52.95.64.115 (52.95.64.115) 16.601 ms
7 * 52.95.66.145 (52.95.66.145) 18.415 ms 52.95.66.169 (52.95.66.169) 16.440 ms
8 * 52.95.67.229 (52.95.67.229) 17.210 ms
9 52.95.67.36 (52.95.67.36) 27.507 ms 52.95.67.146 (52.95.67.146) 14.395 ms *
10 * * *
11 * * *
12 * * *
13 server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99) 9.138 ms * *
zsh yashoswal 62% 10:30:12

```

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

**Description:** Outputs mac address of all devices

**Output:**

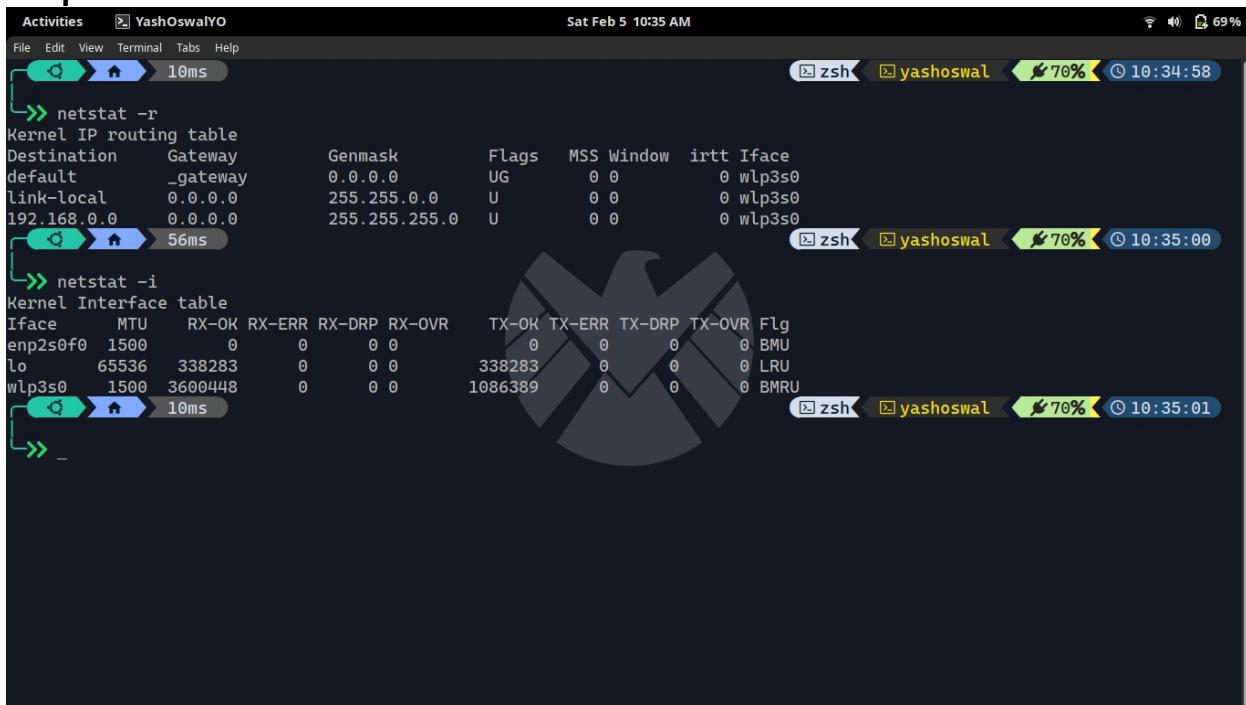


```
Activities YashOswalYO Sat Feb 5 10:33 AM zsh yashoswal 68% 10:33:25
File Edit View Terminal Tabs Help
>> more /sys/class/net/*/*address
:::::::
/sys/class/net/enp2s0f0/address
:::::::
:::39
:::::::
/sys/class/net/lo/address
:::::::
00:00:00:00:00:00
:::::::
/sys/class/net/wlp3s0/address
:::::::
:::37
>> _
```

## Command: netstat

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

### Output:



The screenshot shows a terminal window titled "Activities" with the session name "YashOswalYO". The terminal is running on a system with the date and time "Sat Feb 5 10:35 AM". The window title bar also displays "zsh" and the user "yashoswal" with a battery icon at 70% and a timestamp of "10:34:58". The terminal content shows the execution of the "netstat" command with the "-r" and "-i" options. The output for "netstat -r" displays the Kernel IP routing table with columns for Destination, Gateway, Genmask, Flags, MSS, Window,irtt, and Iface. The output for "netstat -i" displays the Kernel Interface table with columns for Iface, MTU, RX-OK, RX-ERR, RX-DRP, RX-OVR, TX-OK, TX-ERR, TX-DRP, TX-OVR, and Flg. The terminal prompt ends with "» \_".

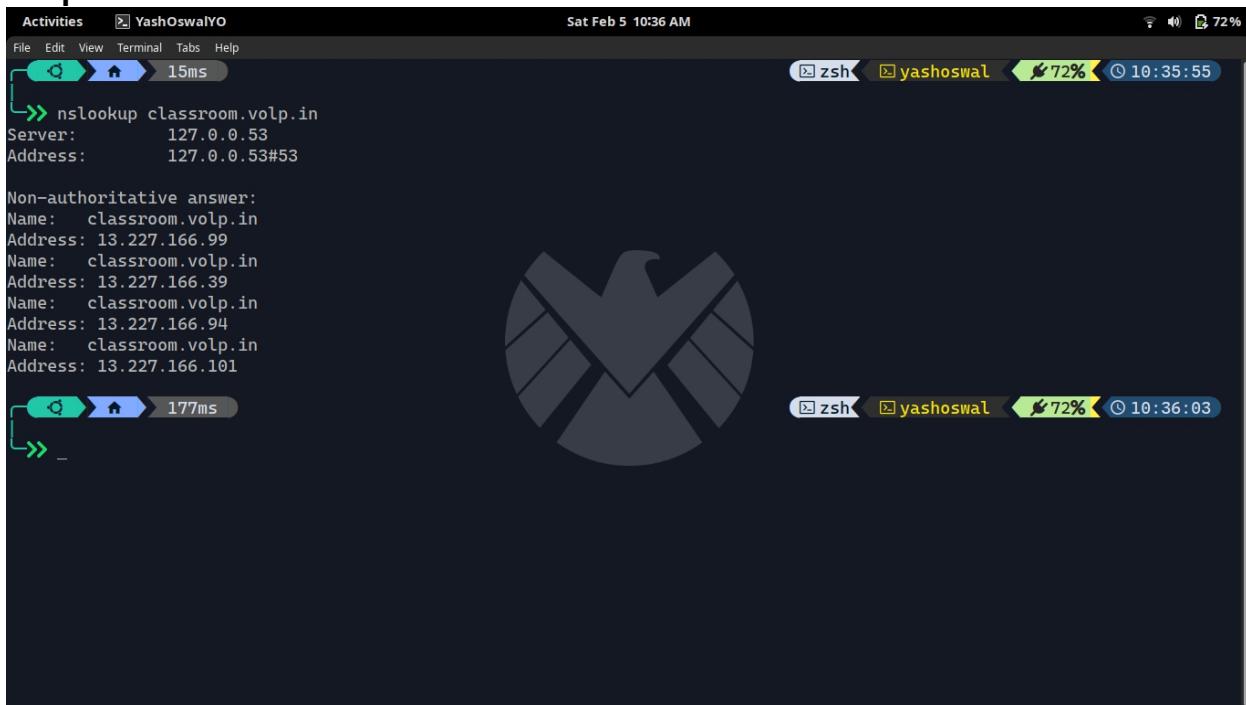
```
Activities YashOswalYO
File Edit View Terminal Tabs Help
Sat Feb 5 10:35 AM
zsh yashoswal 70% 10:34:58

» netstat -r
Kernel IP routing table
Destination     Gateway         Genmask        Flags   MSS Window irtt Iface
default         _gateway       0.0.0.0        UG      0 0          0 wlp3s0
link-local      0.0.0.0        255.255.0.0   U        0 0          0 wlp3s0
192.168.0.0    0.0.0.0        255.255.255.0 U        0 0          0 wlp3s0
» netstat -i
Kernel Interface table
Iface      MTU     RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp2s0f0    1500      0     0     0     0        0     0     0     0 BMU
lo        65536  338283      0     0     0  338283      0     0     0 LRU
wlp3s0    1500  3600448      0     0     0  1086389      0     0     0 BMRU
» _
```

**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:**



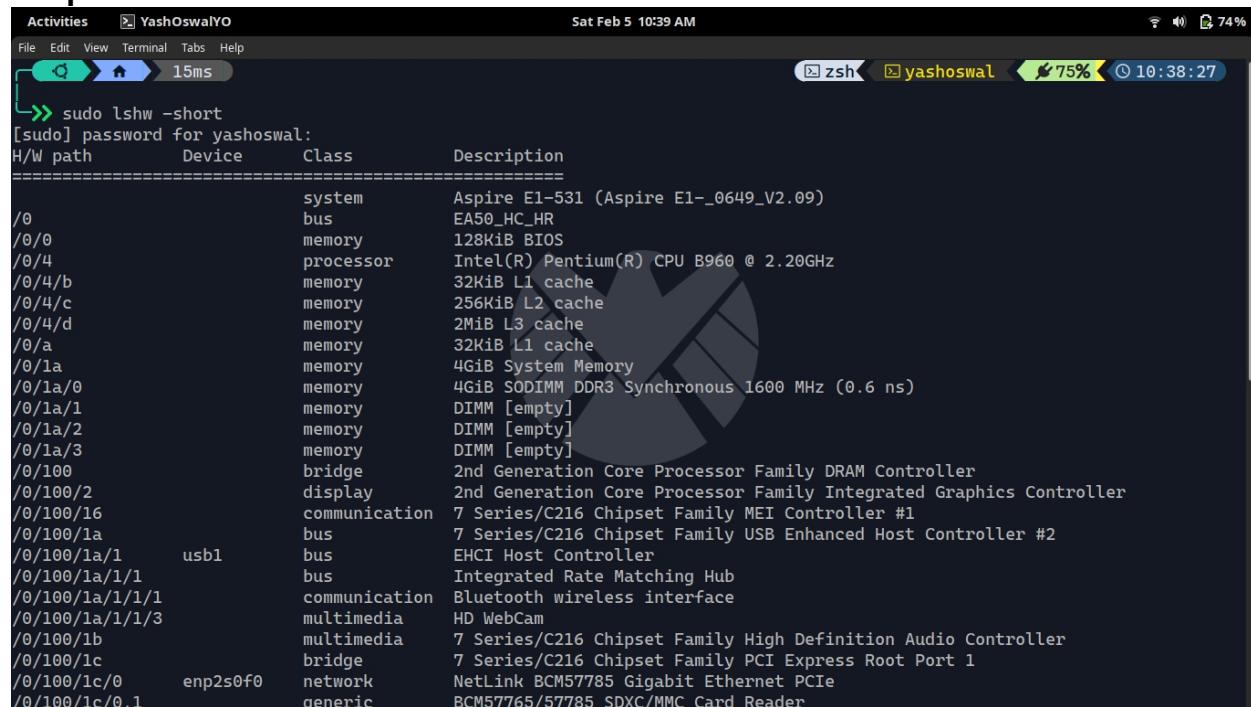
```
Activities YashOswalYO Sat Feb 5 10:36 AM zsh 72% 10:35:55
File Edit View Terminal Help
>> nslookup classroom.volp.in
Server: 127.0.0.53
Address: 127.0.0.53#53

Non-authoritative answer:
Name: classroom.volp.in
Address: 13.227.166.99
Name: classroom.volp.in
Address: 13.227.166.39
Name: classroom.volp.in
Address: 13.227.166.94
Name: classroom.volp.in
Address: 13.227.166.101
>> _
```

**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:**



```

Activities  YashOswalYO
File Edit View Terminal Tabs Help
Sat Feb 5 10:39 AM
File Edit View Terminal Tabs Help
zsh  yashoswal  75%  10:38:27

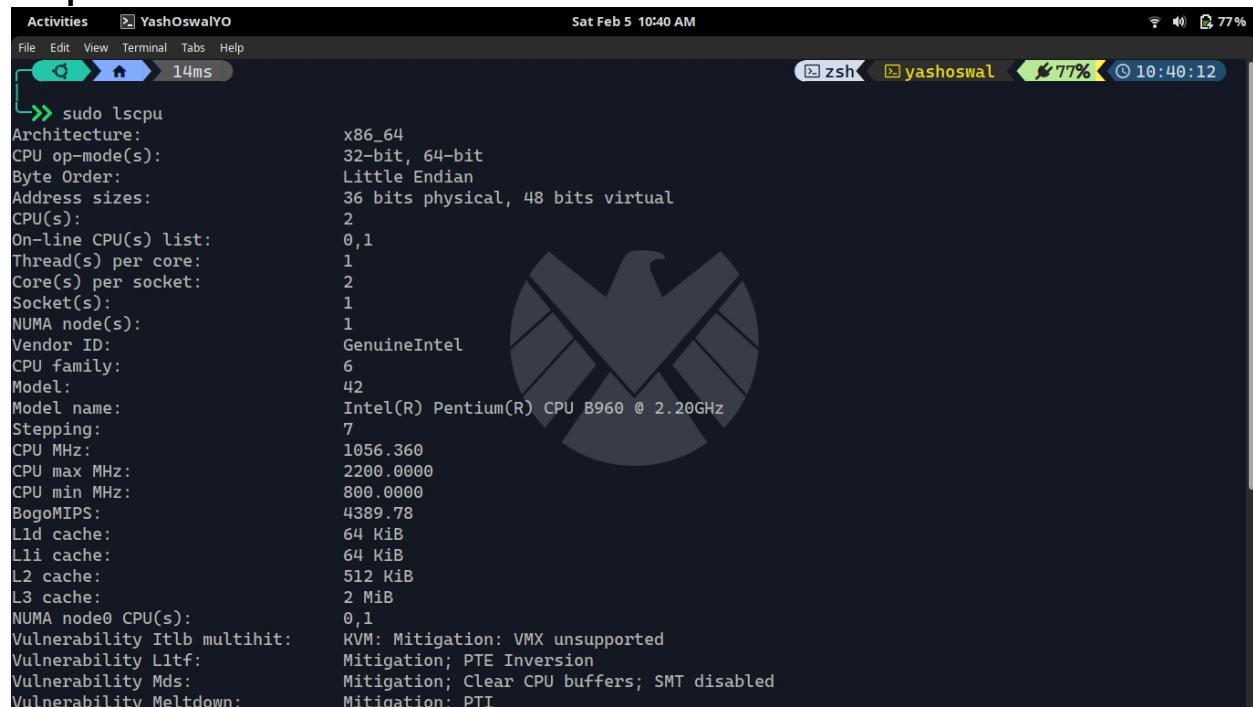
>> sudo lshw -short
[sudo] password for yashoswal:
H/W path        Device      Class      Description
=====
/0              system      Aspire E1-531 (Aspire E1-_0649_V2.09)
/0/0             bus         EA50_HC_HR
/0/4             memory     128KiB BIOS
/0/4/b            processor   Intel(R) Pentium(R) CPU B960 @ 2.20GHz
/0/4/c            memory     32KiB L1 cache
/0/4/d            memory     256KiB L2 cache
/0/a              memory     2MiB L3 cache
/0/1a             memory     32KiB L1 cache
/0/1a/0            memory     4GiB System Memory
/0/1a/1            memory     4GiB SODIMM DDR3 Synchronous 1600 MHz (0.6 ns)
/0/1a/2            memory     DIMM [empty]
/0/1a/3            memory     DIMM [empty]
/0/100            bridge      2nd Generation Core Processor Family DRAM Controller
/0/100/2           display     2nd Generation Core Processor Family Integrated Graphics Controller
/0/100/16          communication 7 Series/C216 Chipset Family MEI Controller #1
/0/100/1a          bus         7 Series/C216 Chipset Family USB Enhanced Host Controller #2
/0/100/1a/1         usbl       bus         EHCI Host Controller
/0/100/1a/1/1       bus         bus         Integrated Rate Matching Hub
/0/100/1a/1/1/1     communication Bluetooth wireless interface
/0/100/1a/1/1/3     multimedia  HD WebCam
/0/100/1b            multimedia  7 Series/C216 Chipset Family High Definition Audio Controller
/0/100/1c            bridge      7 Series/C216 Chipset Family PCI Express Root Port 1
/0/100/1c/0          network     NetLink BCM57785 Gigabit Ethernet PCIe
/0/100/1c/0.1        generic    BCM57765/57785 SDXC/MMC Card Reader

```

**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:**



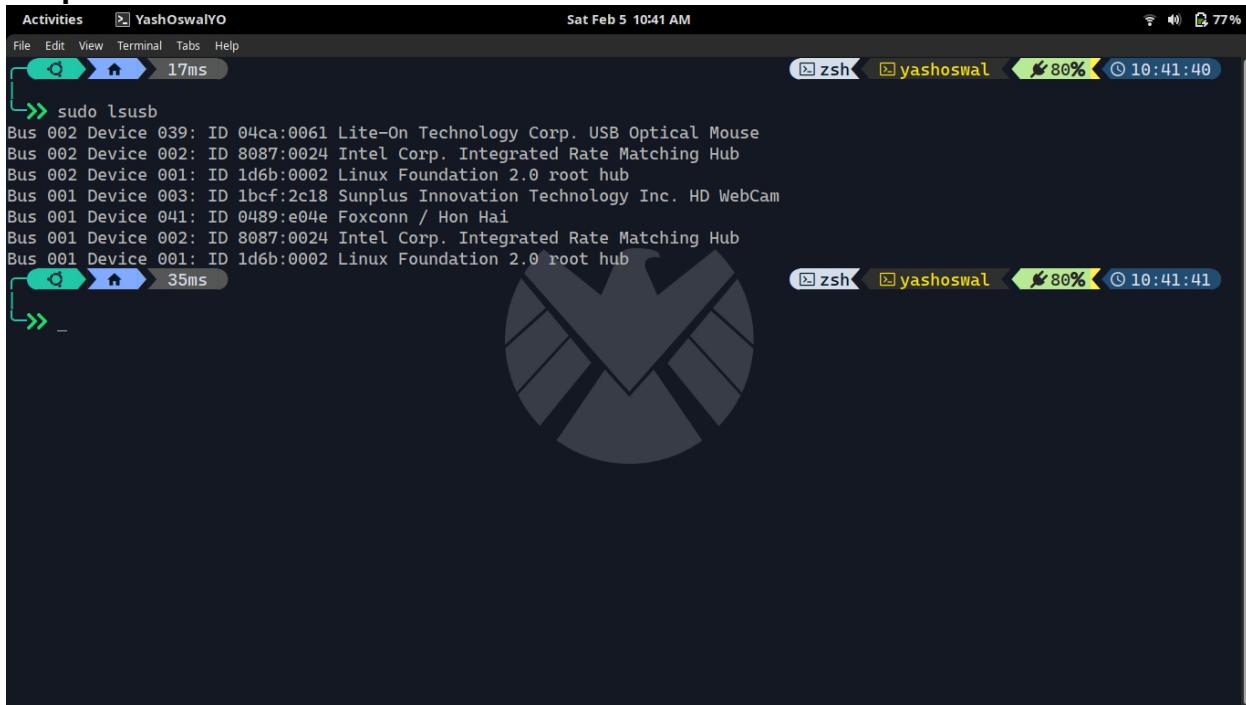
```
Activities YashOswalYO
File Edit View Terminal Tabs Help
Sat Feb 5 10:40 AM
File Edit View Terminal Tabs Help
zsh yashoswal 77% 10:40:12

>> sudo lscpu
Architecture: x86_64
CPU op-mode(s): 32-bit, 64-bit
Byte Order: Little Endian
Address sizes: 36 bits physical, 48 bits virtual
CPU(s): 2
On-line CPU(s) list: 0,1
Thread(s) per core: 1
Core(s) per socket: 2
Socket(s): 1
NUMA node(s): 1
Vendor ID: GenuineIntel
CPU family: 6
Model: 42
Model name: Intel(R) Pentium(R) CPU B960 @ 2.20GHz
Stepping: 7
CPU MHz: 1056.360
CPU max MHz: 2200.0000
CPU min MHz: 800.0000
BogoMIPS: 4389.78
L1d cache: 64 KiB
L1i cache: 64 KiB
L2 cache: 512 KiB
L3 cache: 2 MiB
NUMA node0 CPU(s): 0,1
Vulnerability Itlb multihit: KVM: Mitigation: VMX unsupported
Vulnerability L1tf: Mitigation: PTE Inversion
Vulnerability Mds: Mitigation: Clear CPU buffers; SMT disabled
Vulnerability Meltdown: Mitigation: PTI
```

**Command:** sudo lsusb

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

**Output:**



The screenshot shows a terminal window titled "YashOswalYO" running on a Linux desktop. The terminal displays the output of the "sudo lsusb" command. The output lists several USB devices connected to the system, including a Lite-On Technology Corp. USB Optical Mouse, an Intel Corp. Integrated Rate Matching Hub, a Linux Foundation 2.0 root hub, a Sunplus Innovation Technology Inc. HD WebCam, a Foxconn / Hon Hai device, another Intel Corp. Integrated Rate Matching Hub, and a Linux Foundation 2.0 root hub. The terminal interface includes a navigation bar at the top with "Activities", "File", "Edit", "View", "Terminal", "Tabs", and "Help". The status bar at the bottom shows "zsh", the user "yashoswal", battery level at 80%, and the time "10:41:40". A large circular logo is visible in the center of the terminal window.

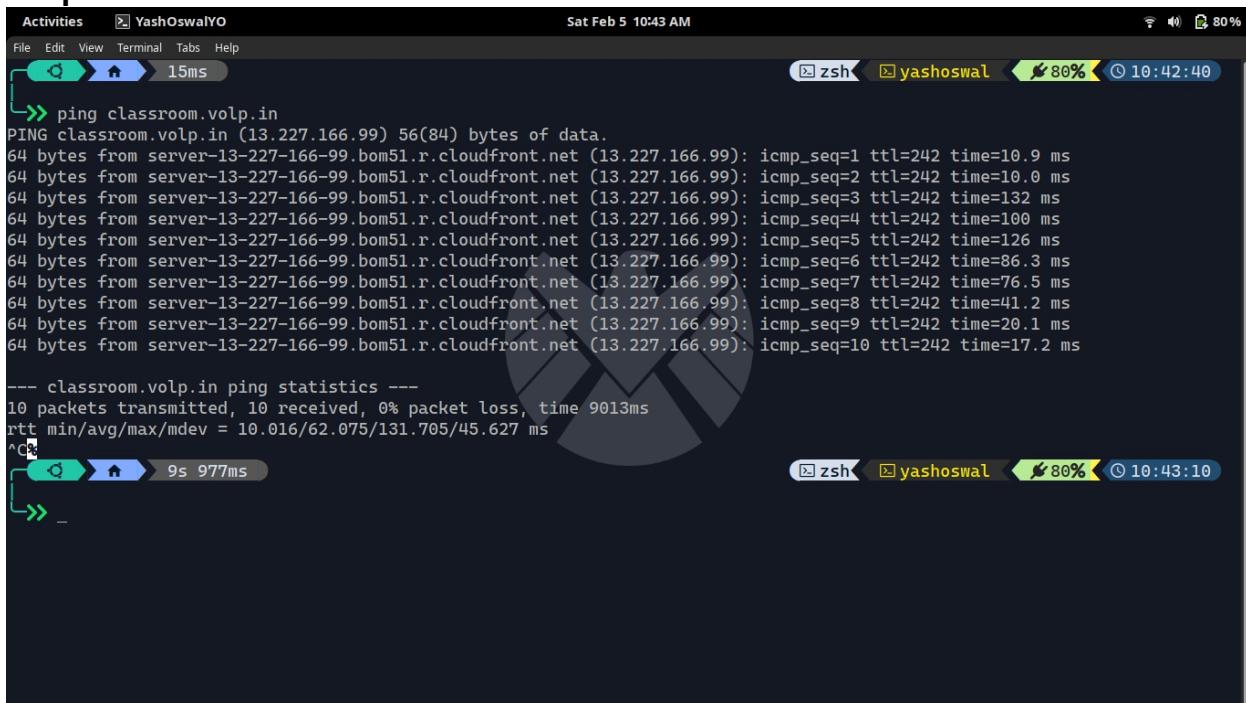
```
Activities YashOswalYO
File Edit View Terminal Tabs Help
Sat Feb 5 10:41 AM
zsh yashoswal 80% 10:41:40

>> sudo lsusb
Bus 002 Device 039: ID 04ca:0061 Lite-On Technology Corp. USB Optical Mouse
Bus 002 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 002 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 001 Device 003: ID 1bcf:2c18 Sunplus Innovation Technology Inc. HD WebCam
Bus 001 Device 041: ID 0489:e04e Foxconn / Hon Hai
Bus 001 Device 002: ID 8087:0024 Intel Corp. Integrated Rate Matching Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
>> _
```

**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:**



The screenshot shows a terminal window titled 'YashOswalYO' running on a Zsh shell. The terminal displays the results of a ping command to 'classroom.volp.in'. The output includes 10 successful echo replies from the server, each showing the source IP, sequence number, TTL, time taken, and the path to the destination. Below this, ping statistics are provided, indicating 10 packets transmitted, 10 received, 0% packet loss, and a round-trip time of 9013ms. The terminal interface includes a top bar with file, edit, view, terminal, tabs, and help options, and a bottom status bar showing battery level at 80% and the current date and time.

```
Activities YashOswalYO
File Edit View Terminal Tabs Help
Sat Feb 5 10:43 AM
File Edit View Terminal Tabs Help
zsh yashoswal 80% 10:42:40
>> ping classroom.volp.in
PING classroom.volp.in (13.227.166.99) 56(84) bytes of data.
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=1 ttl=242 time=10.9 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=2 ttl=242 time=10.0 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=3 ttl=242 time=132 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=4 ttl=242 time=100 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=5 ttl=242 time=126 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=6 ttl=242 time=86.3 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=7 ttl=242 time=76.5 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=8 ttl=242 time=41.2 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=9 ttl=242 time=20.1 ms
64 bytes from server-13-227-166-99.bom51.r.cloudfront.net (13.227.166.99): icmp_seq=10 ttl=242 time=17.2 ms
--- classroom.volp.in ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 9013ms
rtt min/avg/max/mdev = 10.016/62.075/131.705/45.627 ms
^C
>> _
```

**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:**



```
Activities YashOswalYO
File Edit View Terminal Help Sat Feb 5 10:44 AM
File Terminal Help zsh yashoswal 81% 10:43:54
arp -a
_gateway (192.168.0.1) at 00:0c:29:00:7e [ether] on wlp3s0
zsh yashoswal 81% 10:43:56
_
```

## 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.

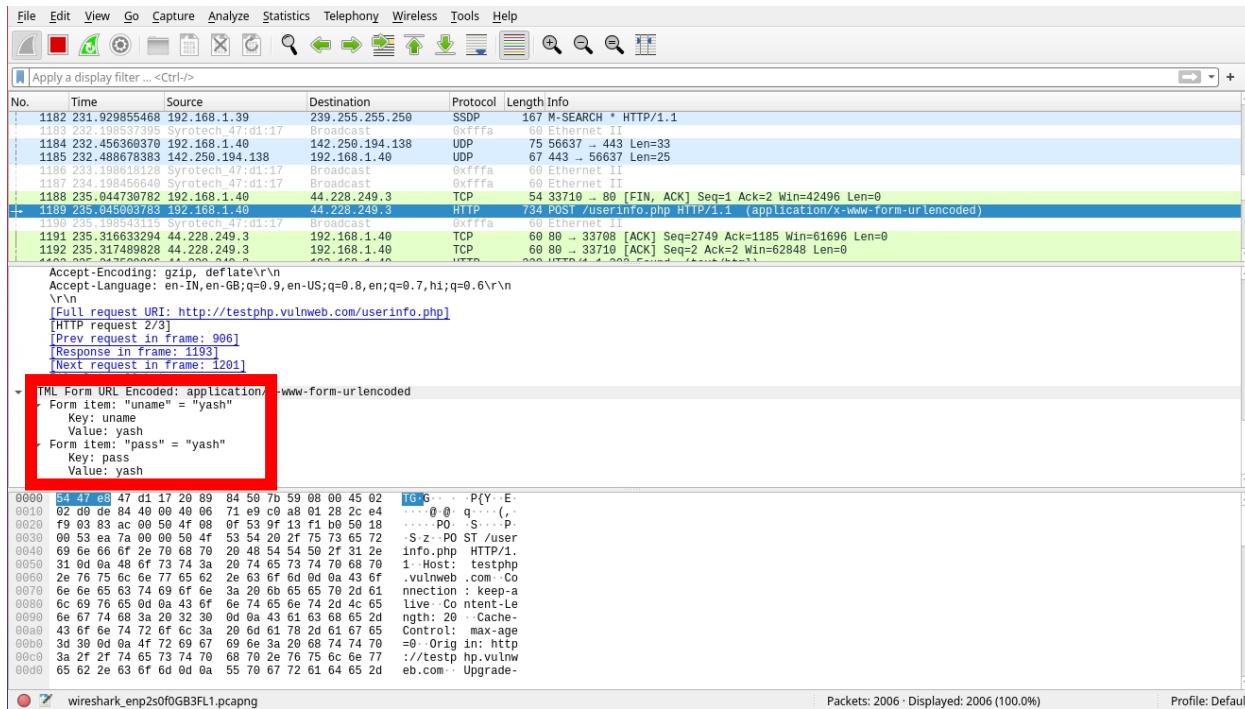
- Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.
- Live data can be read from different types of networks, including Ethernet, IEEE 802.11, PPP, and loopback.
- Captured network data can be browsed via a GUI, or via the terminal (command 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.

---

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

### Form data in plain text



The screenshot shows a Wireshark capture of a network traffic. A POST request is sent from IP 192.168.1.40 to 192.168.1.40 at port 80. The request contains the following data:

```

Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-IN, en-GB;q=0.9, en-US;q=0.8, en;q=0.7, hi;q=0.6\r\n
\r\n
[Full request URI: http://testphp.vulnweb.com/userinfo.php]
[HTTP request 2/3]
[Prev request in frame: 906]
[Response in frame: 4193]
[Next request in frame: 1201]

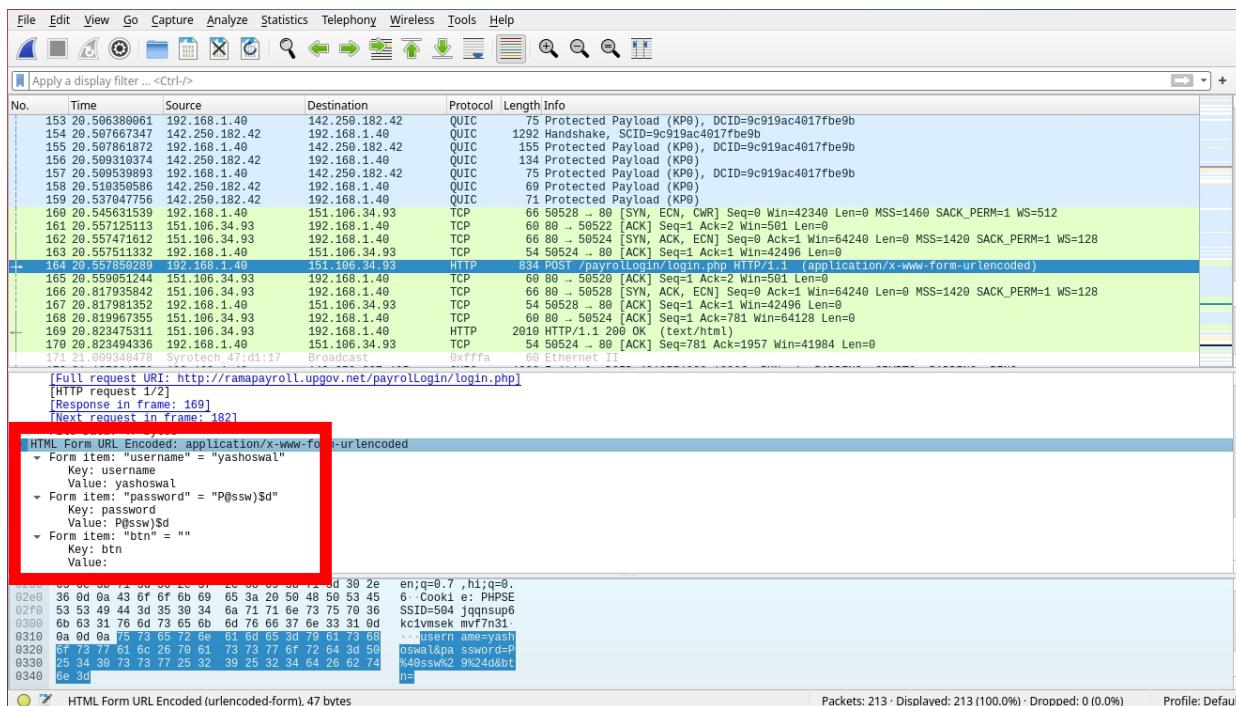
HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "uname" = "yash"
    Key: uname
    Value: yash
  - Form item: "pass" = "yash"
    Key: pass
    Value: yash

```

The captured data also includes the raw hex and ASCII representations of the packet.

Site: <http://ramapayroll.upgov.net/payrollLogin/login.php>

### Username and password transferred in plain text



The screenshot shows a Wireshark capture of a network traffic. A POST request is sent from IP 192.168.1.40 to 192.168.1.40 at port 80. The request contains the following data:

```

[Full request URI: http://ramapayroll.upgov.net/payrollLogin/login.php]
[HTTP request 1/2]
[Response in frame: 169]
[Next request in frame: 182]

HTML Form URL Encoded: application/x-www-form-urlencoded
  - Form item: "username" = "yashoswal"
    Key: username
    Value: yashoswal
  - Form item: "password" = "P@ssw0rd"
    Key: password
    Value: P@ssw0rd
  - Form item: "btn" = ""
    Key: btn
    Value:

```

The captured data also includes the raw hex and ASCII representations of the packet.

## 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](#)

## 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.

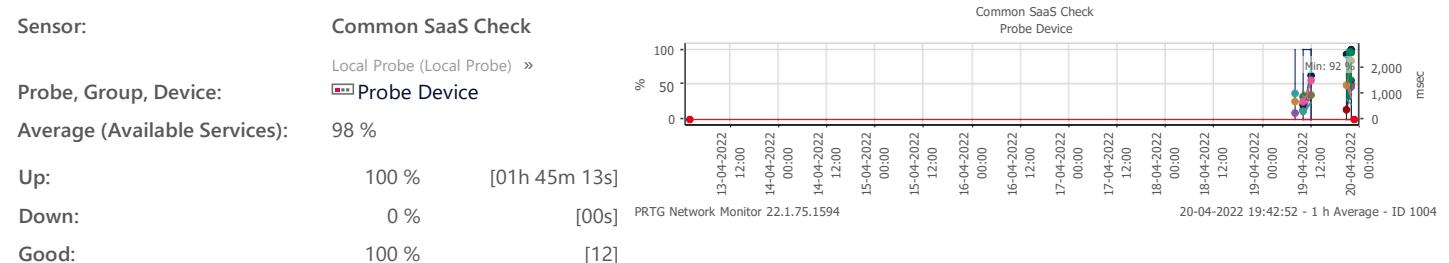
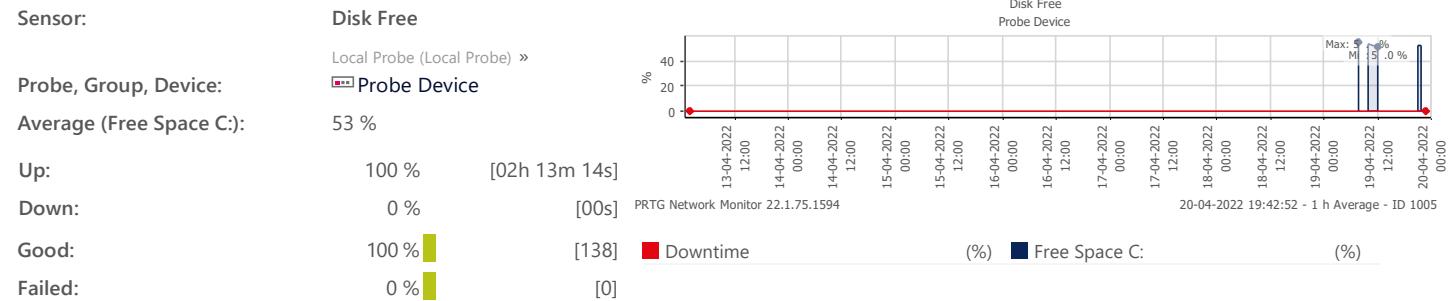
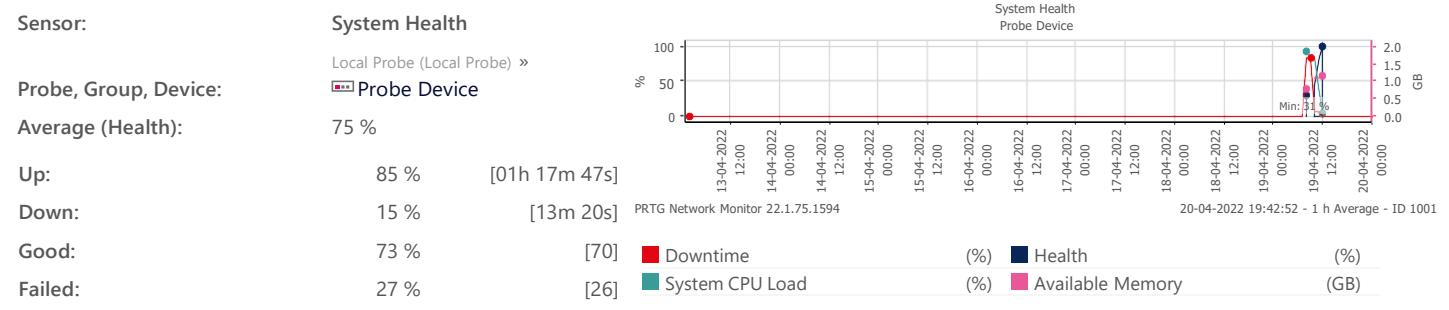
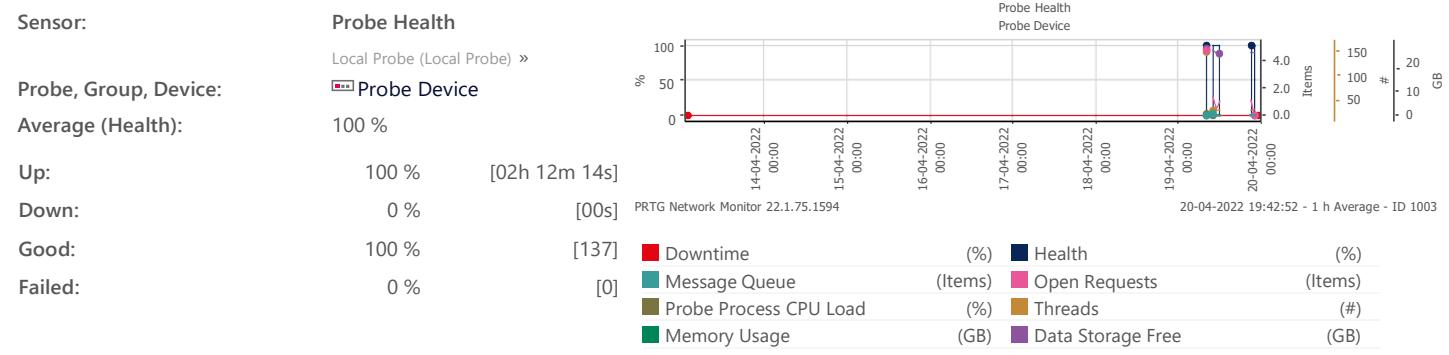
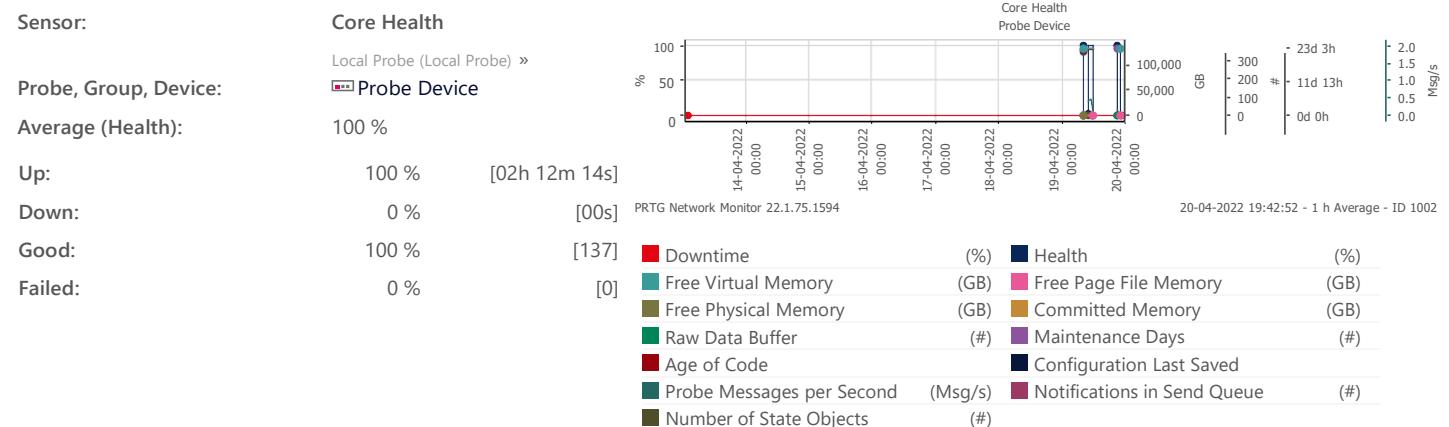
[Learn more](#)

Report

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

## Results

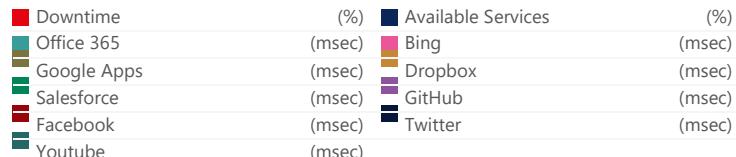
## Graph



Failed:

0 %

[0]



Sensor:

**Intel[R] PRO\_1000 MT Desktop Adapter**

Local Probe (Local Probe) »

Probe Device

Probe, Group, Device:

Average (Total):

2.51 Mbit/s

Total (Total):

2,369 MB

Up:

100 % [02h 09m 11s]

Down:

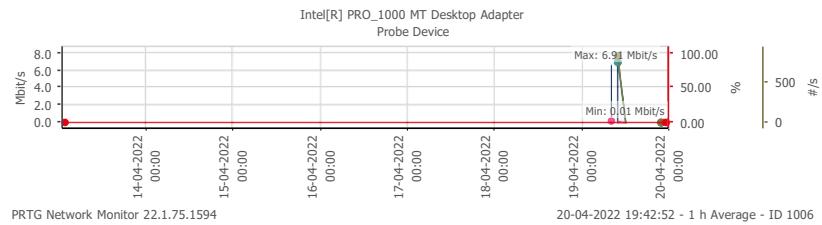
0 % [00s]

Good:

100 % [134]

Failed:

0 % [0]



Sensor:

**HTTP**

Local Probe (Local Probe) »

Network Infrastructure »

Internet

Probe, Group, Device:

Average (Loading time):

891 msec

Up:

100 % [02h 11m 14s]

Down:

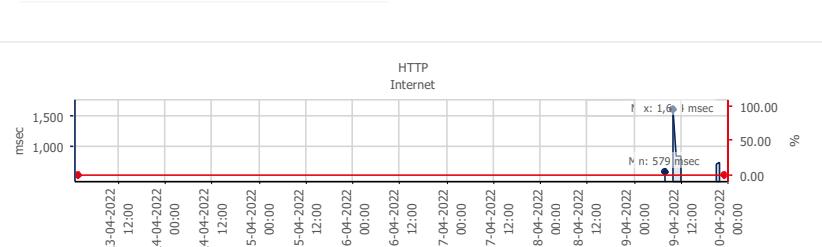
0 % [00s]

Good:

98.529 % [134]

Failed:

1.471 % [2]



Sensor:

**Ping**

Local Probe (Local Probe) »

Network Infrastructure »

DNS: 172.20.10.1

Probe, Group, Device:

Average (Ping Time):

7 msec

Up:

87 % [01h 55m 14s]

Down:

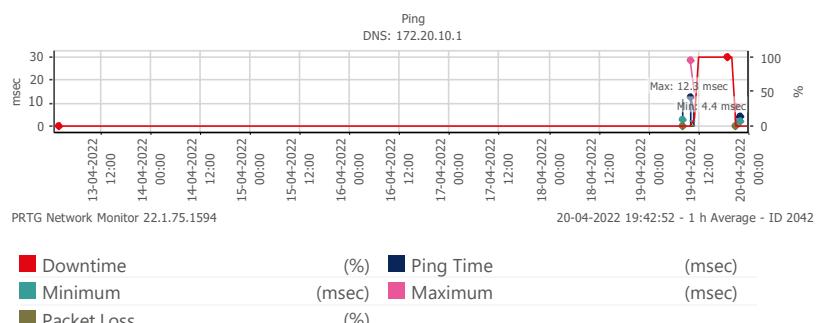
13 % [16m 30s]

Good:

86 % [231]

Failed:

14 % [39]



Sensor:

**DNS v2**

Local Probe (Local Probe) »

Network Infrastructure »

DNS: 172.20.10.1

Probe, Group, Device:

Average (Records Resolved):

No data

Up:

1.58 % [02m 00s]

Down:

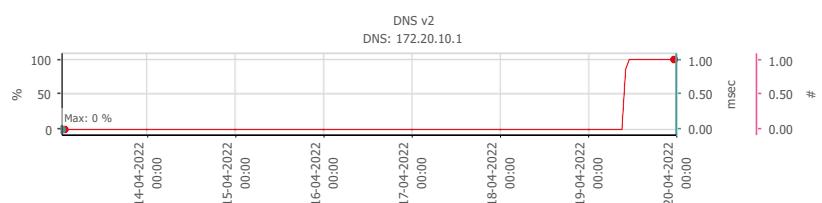
98.42 % [02h 04m 34s]

Good:

0 % [0]

Failed:

100 % [129]



Sensor:

**Ping**

Local Probe (Local Probe) »

Network Infrastructure »

Gateway/DHCP: 10.0.2.2

Probe, Group, Device:

Average (Ping Time):

0 msec

Up:

100 % [02h 10m 43s]

Down:

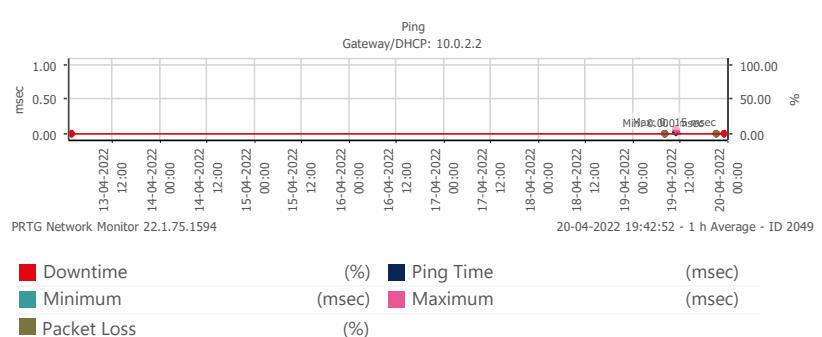
0 % [00s]

Good:

100 % [266]

Failed:

0 % [0]

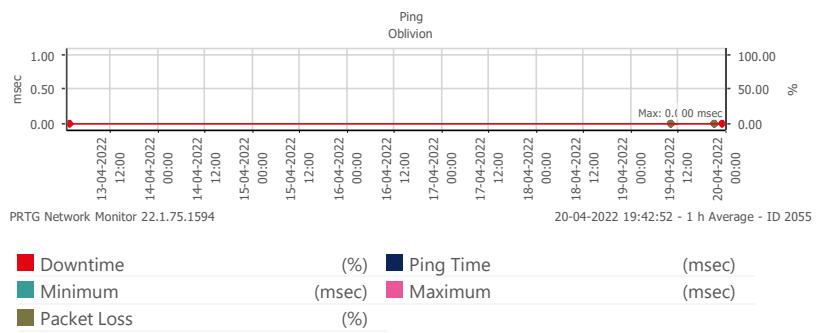


**Sensor:****Ping**

Local Probe (Local Probe) »

Clients »

■ Oblivion

**Probe, Group, Device:****Average (Ping Time):**

0 msec

**Up:**

100 %

[01h 56m 49s]

PRTG Network Monitor 22.1.75.1594

**Down:**

0 %

[00s]

PRTG Network Monitor 22.1.75.1594

**Good:**

100 %

[120]

PRTG Network Monitor 22.1.75.1594

**Failed:**

0 %

[0]

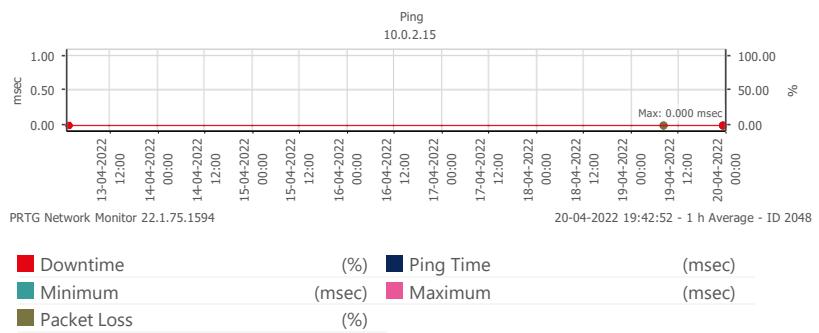
PRTG Network Monitor 22.1.75.1594

**Sensor:****Ping**

Local Probe (Local Probe) »

Subnet 10.0.2 »

■ 10.0.2.15

**Probe, Group, Device:****Average (Ping Time):**

0 msec

**Up:**

100 %

[03m 01s]

PRTG Network Monitor 22.1.75.1594

**Down:**

0 %

[00s]

PRTG Network Monitor 22.1.75.1594

**Good:**

100 %

[10]

PRTG Network Monitor 22.1.75.1594

**Failed:**

0 %

[0]

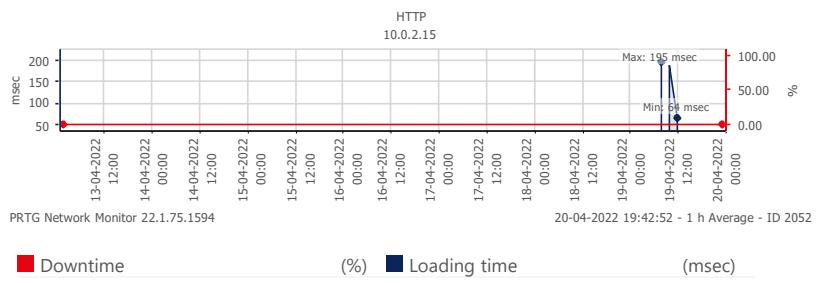
PRTG Network Monitor 22.1.75.1594

**Sensor:****HTTP**

Local Probe (Local Probe) »

Subnet 10.0.2 »

■ 10.0.2.15

**Probe, Group, Device:****Average (Loading time):**

124 msec

**Up:**

100 %

[01h 26m 06s]

PRTG Network Monitor 22.1.75.1594

**Down:**

0 %

[00s]

PRTG Network Monitor 22.1.75.1594

**Good:**

100 %

[90]

PRTG Network Monitor 22.1.75.1594

**Failed:**

0 %

[0]

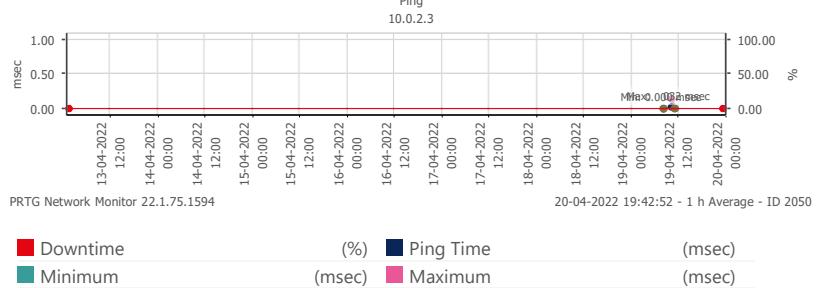
PRTG Network Monitor 22.1.75.1594

**Sensor:****Ping**

Local Probe (Local Probe) »

Subnet 10.0.2 »

■ 10.0.2.3

**Probe, Group, Device:****Average (Ping Time):**

0 msec

**Up:**

100 %

[01h 28m 06s]

PRTG Network Monitor 22.1.75.1594

**Down:**

0 %

[00s]

PRTG Network Monitor 22.1.75.1594

**Good:**

100 %

[180]

PRTG Network Monitor 22.1.75.1594

**Failed:**

0 %

[0]

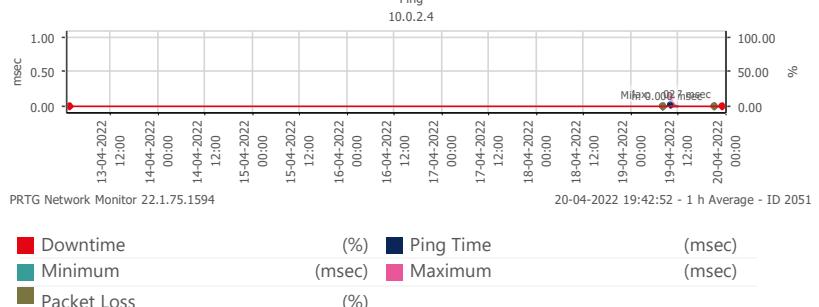
PRTG Network Monitor 22.1.75.1594

**Sensor:****Ping**

Local Probe (Local Probe) »

Subnet 10.0.2 »

■ 10.0.2.4

**Probe, Group, Device:****Average (Ping Time):**

0 msec

**Up:**

100 %

[02h 10m 44s]

PRTG Network Monitor 22.1.75.1594

**Down:**

0 %

[00s]

PRTG Network Monitor 22.1.75.1594

**Good:**

100 %

[265]

PRTG Network Monitor 22.1.75.1594

**Failed:**

0 %

[0]

PRTG Network Monitor 22.1.75.1594

**Sensor:****Core Health (Autonomous)****Probe, Group, Device:**

■ PRTG Core Server

**Average (Health):**

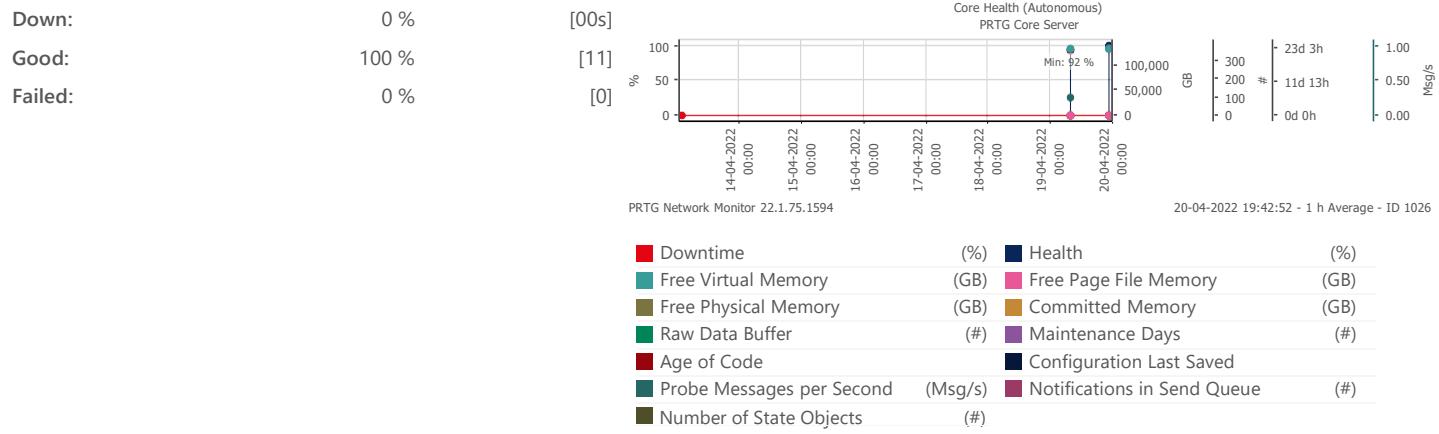
94 %

**Up:**

100 %

[06m 05s]

PRTG Network Monitor 22.1.75.1594



PAESSLER 22.1.75.1594+ • 20-04-2022 19:42:51

## 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

- ppup.ac.in..... 4

---

## **Vulnerabilities by Host**

---

# ppup.ac.in



## Vulnerabilities

Total: 62

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

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

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

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