

CYBERSECURITY

Cybersecurity focuses on the protection of computer systems from unauthorized access from unauthorized personnel.

WEEK 1:

Deploying of a networked Sandbox: In computer security and architecture A sandboxed network is a network environment that is isolated from the rest of the network and is often used for testing, running potentially malicious code, or conducting experiments without risking harm to the main network or systems. Machines needed for this task are *Ubuntu gateway 22.04*, *Ubuntu WordPress 14.04 and 22.04*, *kali linux* and *windows Iso file*. All these machines will be deployed in a virtual box (An popular open-source virtualization software developed by Oracle that allows you to create and run virtual machines (VMs) on your computer) in order to achieve the image below

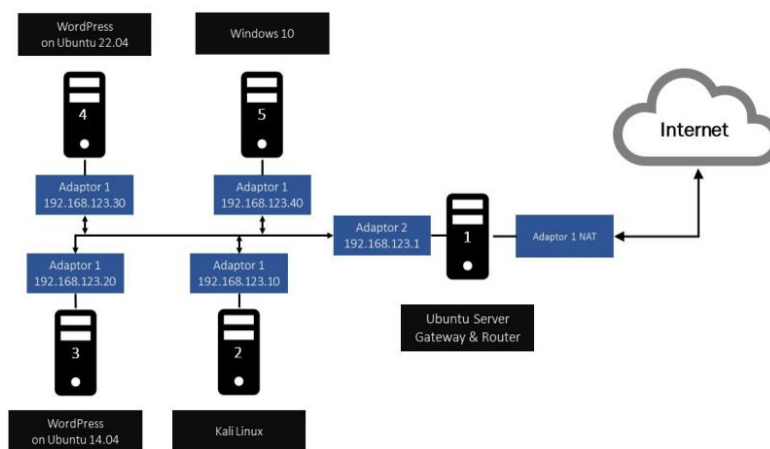
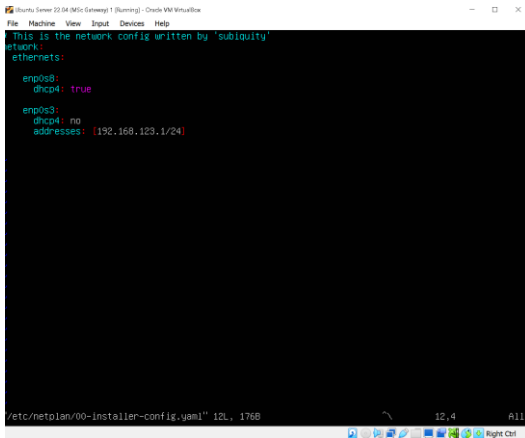


Figure 1: Sandboxed Network Diagram

Configuring Ubuntu Gateway:

Ubuntu gateway is simply the Router within this network. To configure it, I started by installing all the machines and clicked on Ubuntu gateway, after logging in, I set the adapters and configured the Ubuntu 22.04 gateway settings using (`sudo vi 00-installer-config.yaml`) and change the IP details and interface name to my environment then apply with `$ sudo netplan apply`.

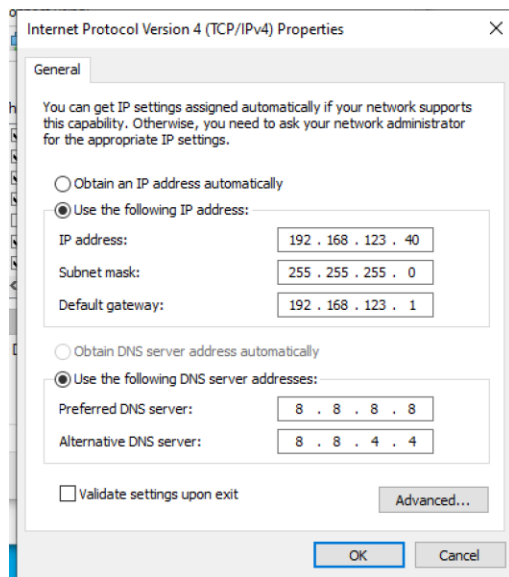
Problem: I had issues configuring my Ubuntu gateway server, I had to use the vi instead of nano



```
This is the network config written by 'subiquity'
network:
  ethernet0:
    dhcp4: true
    dhcp3: no
    addresses: (192.168.123.1/24)
```

Windows

Next, install windows iso file and set the ram to 4096, the storage to 70gb and click finish. When it is running, edit the ethernet setting and configure the ip address to 192.168.123.40. I also set the network adapter to internal network, disabling all other other adapters.



DEPLOYMENT OF SANDBOXED NETWORK

After starting all my virtual machines, I set all adapters to internal network as they use single adapters except for Ubuntu gateway 22.04. I made sure Kali Linux can browse word press servers. As seen on fig 1 and 2.

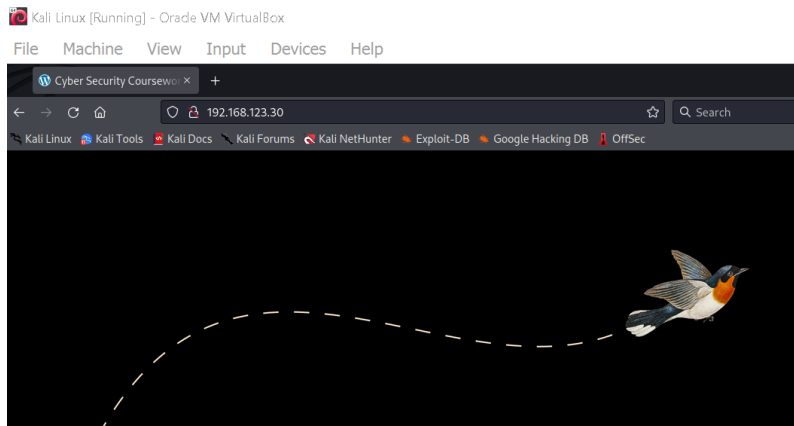


fig.1

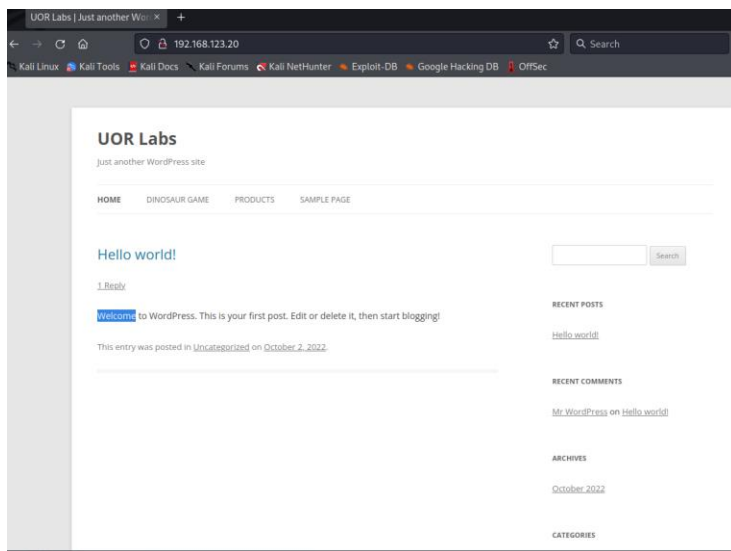


Fig.2

RENAMING THE HOSTNAMES.

I renamed the hostnames of all machines to various names.

```

--- 192.168.123.40 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2012ms
rtt min/avg/max/mdev = 0.651/1.295/1.623/0.455 ms
student@Nwaka:~$ 192.168.123.20
192.168.123.20: command not found
student@Nwaka:~$ ping 192.168.123.20
PING 192.168.123.20 (192.168.123.20) 56(84) bytes of data.
64 bytes from 192.168.123.20: icmp_seq=1 ttl=64 time=0.637 ms
64 bytes from 192.168.123.20: icmp_seq=2 ttl=64 time=0.580 ms
64 bytes from 192.168.123.20: icmp_seq=3 ttl=64 time=0.529 ms
^C
--- 192.168.123.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.529/0.582/0.637/0.044 ms
student@Nwaka:~$ ping 192.168.123.10
PING 192.168.123.10 (192.168.123.10) 56(84) bytes of data.
64 bytes from 192.168.123.10: icmp_seq=1 ttl=64 time=0.754 ms
64 bytes from 192.168.123.10: icmp_seq=2 ttl=64 time=0.691 ms
64 bytes from 192.168.123.10: icmp_seq=3 ttl=64 time=0.731 ms
^C
--- 192.168.123.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.691/0.725/0.754/0.026 ms
student@Nwaka:~$ ping 192.168.123.30
PING 192.168.123.30 (192.168.123.30) 56(84) bytes of data.
64 bytes from 192.168.123.30: icmp_seq=1 ttl=64 time=0.019 ms
64 bytes from 192.168.123.30: icmp_seq=2 ttl=64 time=0.024 ms
64 bytes from 192.168.123.30: icmp_seq=3 ttl=64 time=0.023 ms
^C
--- 192.168.123.30 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.019/0.022/0.024/0.002 ms
student@Nwaka:~$

```

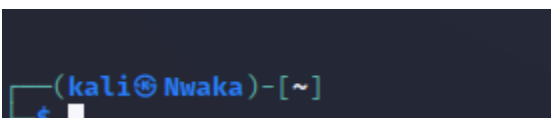
Ubuntu server 22.04(wordpress)

[see details in windows security](#)

Device specifications

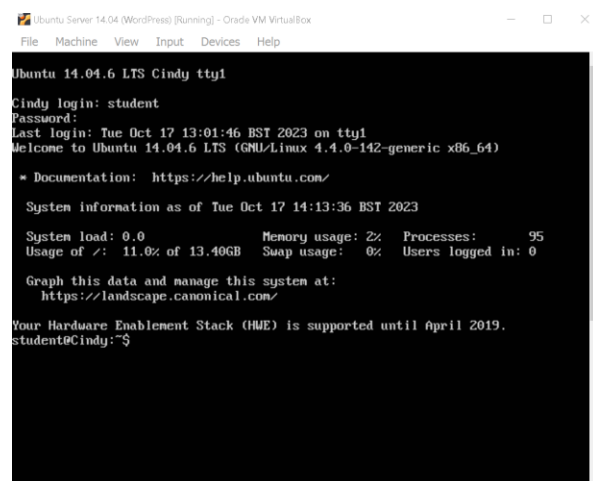
Device name	CINDY
Processor	Intel(R) Core(TM) i7-10700K CPU @ 3.80GHz 3.79 GHz
Installed RAM	4.00 GB

Windows



Kali linux hostname

```
udent@student:~$ hostnamectl
static hostname: nwaka
        Icon name: computer-vm
        Chassis: vm
        Machine ID: 5ac450d95b2e475eb0a2d14034b
        Boot ID: 3e7a8a824718492385f6c1d5d62
Virtualization: oracle
Operating System: Ubuntu 22.04.1 LTS
        Kernel: Linux 5.15.0-60-generic
        Architecture: x86-64
Hardware Vendor: innotek GmbH
Hardware Model: VirtualBox
udent@student:~$
```



```
Ubuntu Server 14.04 (WordPress) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu 14.04.6 LTS Cindy tty1
Cindy login: student
Password:
Last login: Tue Oct 17 13:01:46 BST 2023 on tty1
Welcome to Ubuntu 14.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Tue Oct 17 14:13:36 BST 2023

System load: 0.0          Memory usage: 2%    Processes:    95
Usage of /:  11.0% of 13.40GB  Swap usage:  0%    Users logged in: 0

Graph this data and manage this system at:
https://landscape.canonical.com/

Your Hardware Enablement Stack (HWE) is supported until April 2019.
student@Cindy:~$
```

Ubuntu 14.01 Wordpress

PING TEST

Ping test is a network utility used to test the reachability of a host (a device or computer) on an Internet Protocol (IP) network and measure the round-trip time it takes for data packets to travel to the destination and back to the source.

```
Windows 10 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Select Command Prompt
C:\Users\vboxuser>ping 192.168.123.30

Pinging 192.168.123.30 with 32 bytes of data:
Reply from 192.168.123.30: bytes=32 time<1ms TTL=64
Reply from 192.168.123.30: bytes=32 time<1ms TTL=64
Reply from 192.168.123.30: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.123.30:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\vboxuser>ping 192.168.123.20

Pinging 192.168.123.20 with 32 bytes of data:
Reply from 192.168.123.20: bytes=32 time<1ms TTL=64
Reply from 192.168.123.20: bytes=32 time<1ms TTL=64
Reply from 192.168.123.20: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.123.20:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\vboxuser>ping 192.168.123.10

Pinging 192.168.123.10 with 32 bytes of data:
Reply from 192.168.123.10: bytes=32 time<1ms TTL=64
Reply from 192.168.123.10: bytes=32 time<1ms TTL=64
Reply from 192.168.123.10: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.123.10:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
Control-C
^C
C:\Users\vboxuser>ping 192.168.123.40

Pinging 192.168.123.40 with 32 bytes of data:
Reply from 192.168.123.40: bytes=32 time<1ms TTL=128
Reply from 192.168.123.40: bytes=32 time<1ms TTL=128
```

Windows Ping Test.

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
kali@kali: ~
File Actions Edit View Help
kali@kali:~$ ping 192.168.123.30
PING 192.168.123.30 (192.168.123.30) 56(84) bytes of data.
64 bytes from 192.168.123.30: icmp_seq=1 ttl=64 time=1.22 ms
64 bytes from 192.168.123.30: icmp_seq=2 ttl=64 time=0.610 ms
64 bytes from 192.168.123.30: icmp_seq=3 ttl=64 time=0.653 ms
^C
--- 192.168.123.30 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 0.610/0.828/1.221/0.278 ms

kali@kali:~$ ping 192.168.123.20
PING 192.168.123.20 (192.168.123.20) 56(84) bytes of data.
64 bytes from 192.168.123.20: icmp_seq=1 ttl=64 time=0.018 ms
64 bytes from 192.168.123.20: icmp_seq=2 ttl=64 time=0.021 ms
64 bytes from 192.168.123.20: icmp_seq=3 ttl=64 time=0.019 ms
^C
--- 192.168.123.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2024ms
rtt min/avg/max/mdev = 0.018/0.019/0.021/0.001 ms

kali@kali:~$ ping 192.168.123.40
PING 192.168.123.40 (192.168.123.40) 56(84) bytes of data.
64 bytes from 192.168.123.40: icmp_seq=1 ttl=128 time=1.21 ms
64 bytes from 192.168.123.40: icmp_seq=2 ttl=128 time=0.553 ms
64 bytes from 192.168.123.40: icmp_seq=3 ttl=128 time=0.568 ms
64 bytes from 192.168.123.40: icmp_seq=4 ttl=128 time=0.568 ms
^C
--- 192.168.123.40 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3026ms
rtt min/avg/max/mdev = 0.553/0.725/1.211/0.280 ms

kali@kali:~$ ping 192.168.123.1
PING 192.168.123.1 (192.168.123.1) 56(84) bytes of data.
64 bytes from 192.168.123.1: icmp_seq=1 ttl=64 time=0.597 ms
64 bytes from 192.168.123.1: icmp_seq=2 ttl=64 time=0.571 ms
64 bytes from 192.168.123.1: icmp_seq=3 ttl=64 time=0.597 ms
64 bytes from 192.168.123.1: icmp_seq=4 ttl=64 time=0.550 ms
^C
--- 192.168.123.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3077ms
rtt min/avg/max/mdev = 0.550/0.578/0.597/0.019 ms
```

Kali Linux ping test.

```
System load: 0.0      Memory usage: 2%    Processes:    95
Usage of /: 11.0% of 13.40GB  Swap usage:  0%    Users logged in: 0
```

Graph this data and manage this system at:
<https://landscape.canonical.com/>

Your Hardware Enablement Stack (HWE) is supported until April 2019.

```
student@Cindy:~$ ping 192.168.123.40
PING 192.168.123.40 (192.168.123.40) 56(84) bytes of data.
64 bytes from 192.168.123.40: icmp_seq=1 ttl=128 time=1.68 ms
64 bytes from 192.168.123.40: icmp_seq=2 ttl=128 time=0.583 ms
64 bytes from 192.168.123.40: icmp_seq=3 ttl=128 time=0.513 ms
64 bytes from 192.168.123.40: icmp_seq=4 ttl=128 time=0.524 ms
64 bytes from 192.168.123.40: icmp_seq=5 ttl=128 time=0.602 ms
^C
```

```
--- 192.168.123.40 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4047ms
rtt min/avg/max/mdev = 0.513/0.780/1.680/0.451 ms
```

```
student@Cindy:~$ ping 192.168.123.20
PING 192.168.123.20 (192.168.123.20) 56(84) bytes of data.
64 bytes from 192.168.123.20: icmp_seq=1 ttl=64 time=0.016 ms
64 bytes from 192.168.123.20: icmp_seq=2 ttl=64 time=0.018 ms
64 bytes from 192.168.123.20: icmp_seq=3 ttl=64 time=0.017 ms
^C
```

```
--- 192.168.123.20 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2064ms
rtt min/avg/max/mdev = 0.016/0.017/0.018/0.000 ms
```

```
student@Cindy:~$ ping 192.168.123.1
PING 192.168.123.1 (192.168.123.1) 56(84) bytes of data.
```

Ubuntu server 14.04

GATEWAY INTERNET ACCESS TEST.

To test the internet gateway access, I used “nslookup bbc.co.uk” and they were all responding.

```
student@Cindy:~$ nslookup bbc.co.uk
Server:      8.8.8.8
Address:     8.8.8.8#53
```

Non-authoritative answer:

```
Name:   bbc.co.uk
Address: 151.101.0.81
Name:   bbc.co.uk
Address: 151.101.64.81
Name:   bbc.co.uk
Address: 151.101.128.81
Name:   bbc.co.uk
Address: 151.101.192.81
```

```
student@Nwaka:~$ nslookup bbc.co.uk
Server:      127.0.0.53
Address:     127.0.0.53#53

Non-authoritative answer:
Name:   bbc.co.uk
Address: 151.101.0.81
Name:   bbc.co.uk
Address: 151.101.64.81
Name:   bbc.co.uk
Address: 151.101.128.81
Name:   bbc.co.uk
Address: 151.101.192.81
Name:   bbc.co.uk
```

```
~$ nslookup bbc.co.uk
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   bbc.co.uk
Address: 151.101.0.81
Name:   bbc.co.uk
Address: 151.101.64.81
Name:   bbc.co.uk
Address: 151.101.128.81
Name:   bbc.co.uk
Address: 151.101.192.81
Name:   bbc.co.uk
Address: 2a04:4e42::81
Name:   bbc.co.uk
Address: 2a04:4e42:200::81
Name:   bbc.co.uk
Address: 2a04:4e42:400::81
Name:   bbc.co.uk
Address: 2a04:4e42:600::81
```

```
—(kali@Nwaka)~[~]
~$
```

Back Up of Sandboxed Network:

Export your VMs as OVA files from VirtualBox and back the OVA files to OneDrive, Google Drive, Drop Box etc