

Network Operating Systems and Services (ACCA5023)

Worksheet 1: Building a virtual LAN using type 2 hypervisor software.

(Practical Tasks)

STUDENT NUMBER: 1810613

Task 1: VM creation and Operating System installations

Virtual Machine creation

Machines created with specs listed below.

Server 1

Oracle VM VirtualBox Manager

File Machine Help

Tools

Server1 2019 Powered Off

Server2 2019 Powered Off

Client1 10 Powered Off

Client2 10 Powered Off

New Settings Discard Start

General

Name: Server1
Operating System: Windows 2019 (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Server1.vdi (Normal, 25.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

Server 2

Oracle VM VirtualBox Manager

File Machine Help

Tools

Server1 2019 Powered Off

Server2 2019 Powered Off

Client1 10 Powered Off

Client2 10 Powered Off

New Settings Discard Start

General

Name: Server2
Operating System: Windows 2019 (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Server2.vdi (Normal, 25.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 1, PRACTICAL TASKS

Client 1

Oracle VM VirtualBox Manager

File Machine Help

Tools

Server1 2019 Powered Off

Server2 2019 Powered Off

Client1 10 Powered Off

Client2 10 Powered Off

New Settings Discard Start

General

Name: Client1
Operating System: Windows 10 (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Client1.vdi (Normal, 20.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

Description

None

Client 2

Oracle VM VirtualBox Manager

File Machine Help

Tools

Server1 2019 Powered Off

Server2 2019 Powered Off

Client1 10 Powered Off

Client2 10 Powered Off

New Settings Discard Start

General

Name: Client2
Operating System: Windows 10 (64-bit)

System

Base Memory: 4096 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization

Display

Video Memory: 128 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled

Storage

Controller: SATA
SATA Port 0: Client2.vdi (Normal, 20.00 GB)
SATA Port 1: [Optical Drive] Empty

Audio

Host Driver: Windows DirectSound
Controller: Intel HD Audio

Network

Adapter 1: Intel PRO/1000 MT Desktop (NAT)

USB

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

None

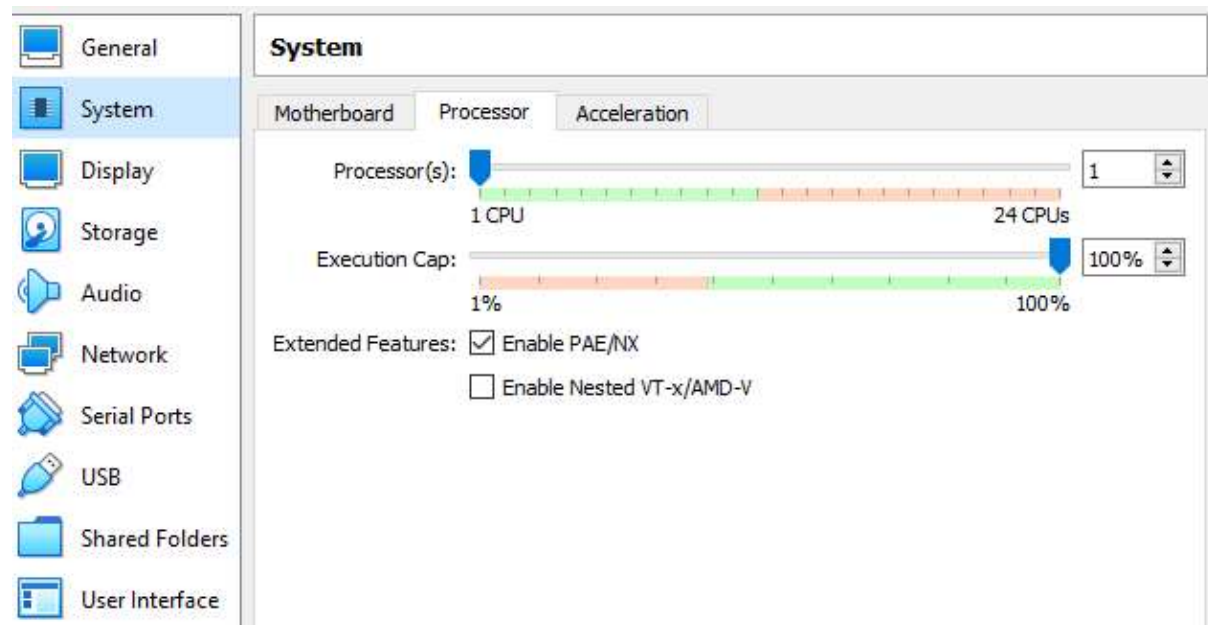
Description

None

Operating system installation and optimisation

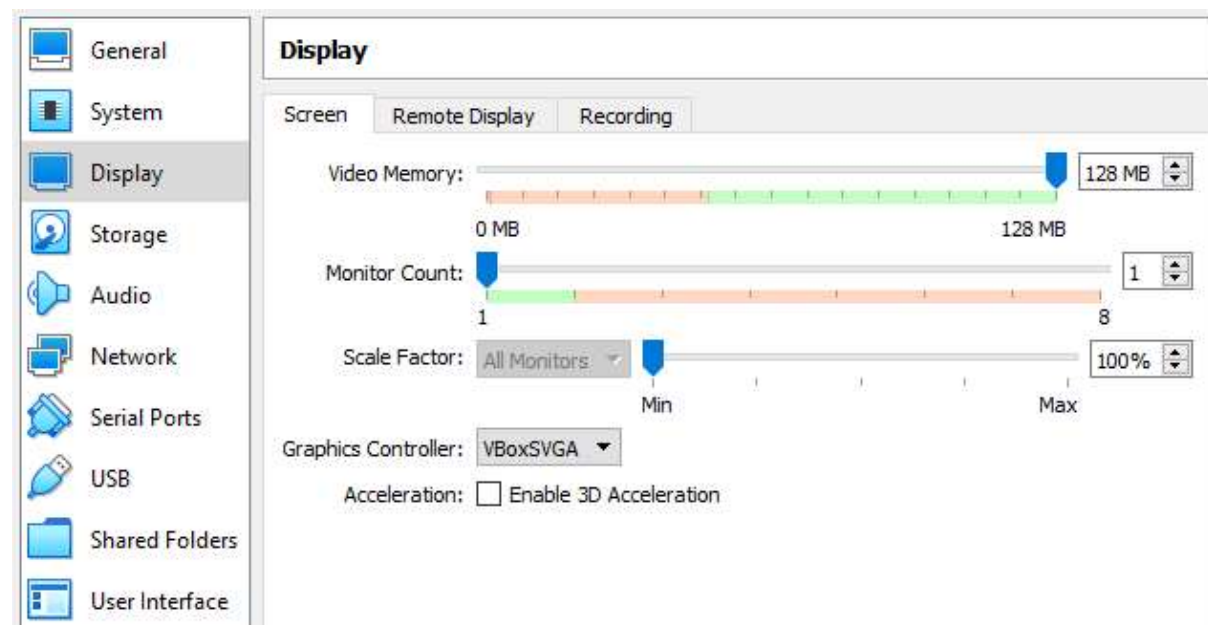
Optimisation 1

PAE/NX enabled across all machines to ensure that the Host system CPU is more readily accessible. This was applied to all VMs using the method captured in the screenshot below:



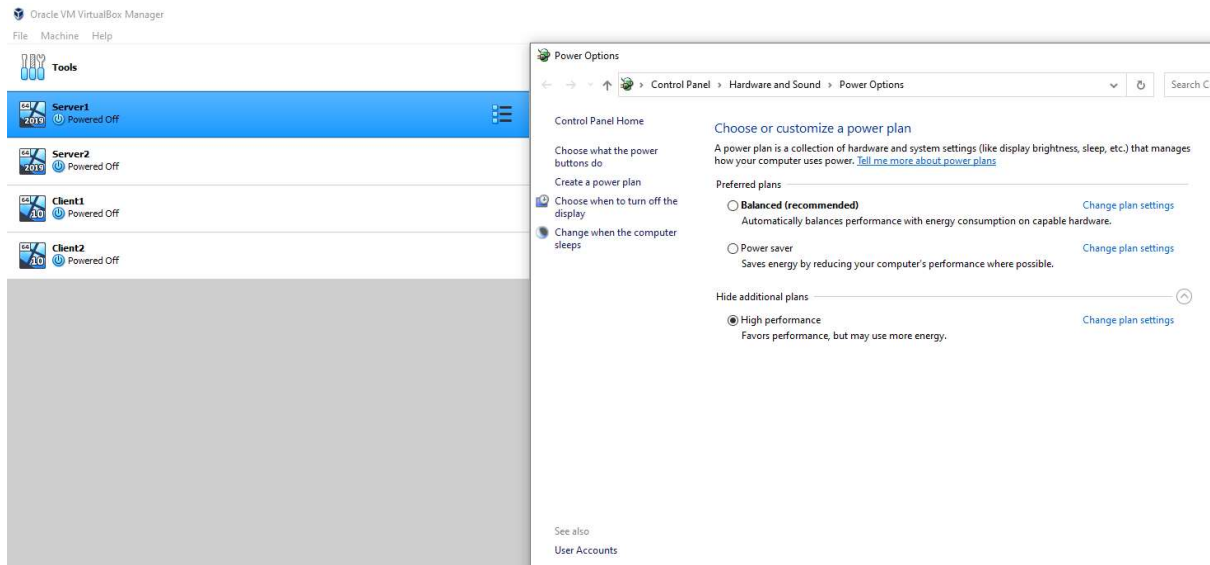
Optimisation 2

128MB video memory allocated to each machine.



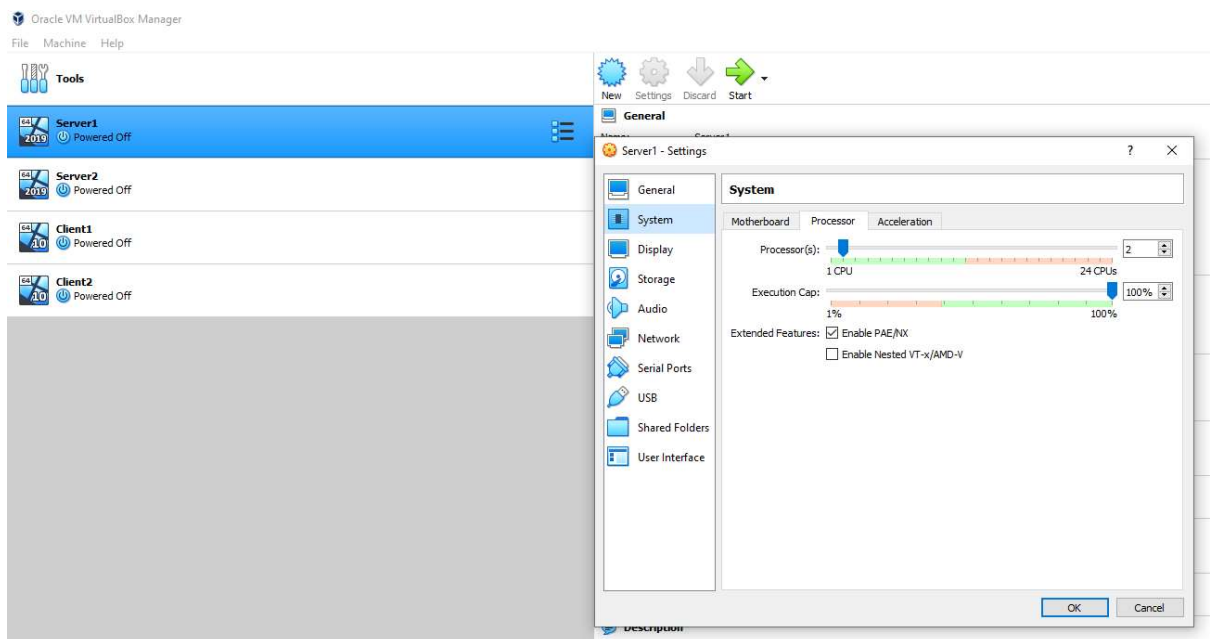
Optimisation 3

Set the host machine power plan to “performance” to ensure the hosts machines components are receiving optimal power which may not always be the case on the more energy conservative “balanced” plan.



Optimisation 4

CPU cores have been increased to 2. This will increase the processing speed of the VMs while taking little away from the host which is running an AMD Ryzen 3900X which supports multithreading on 12 cores.



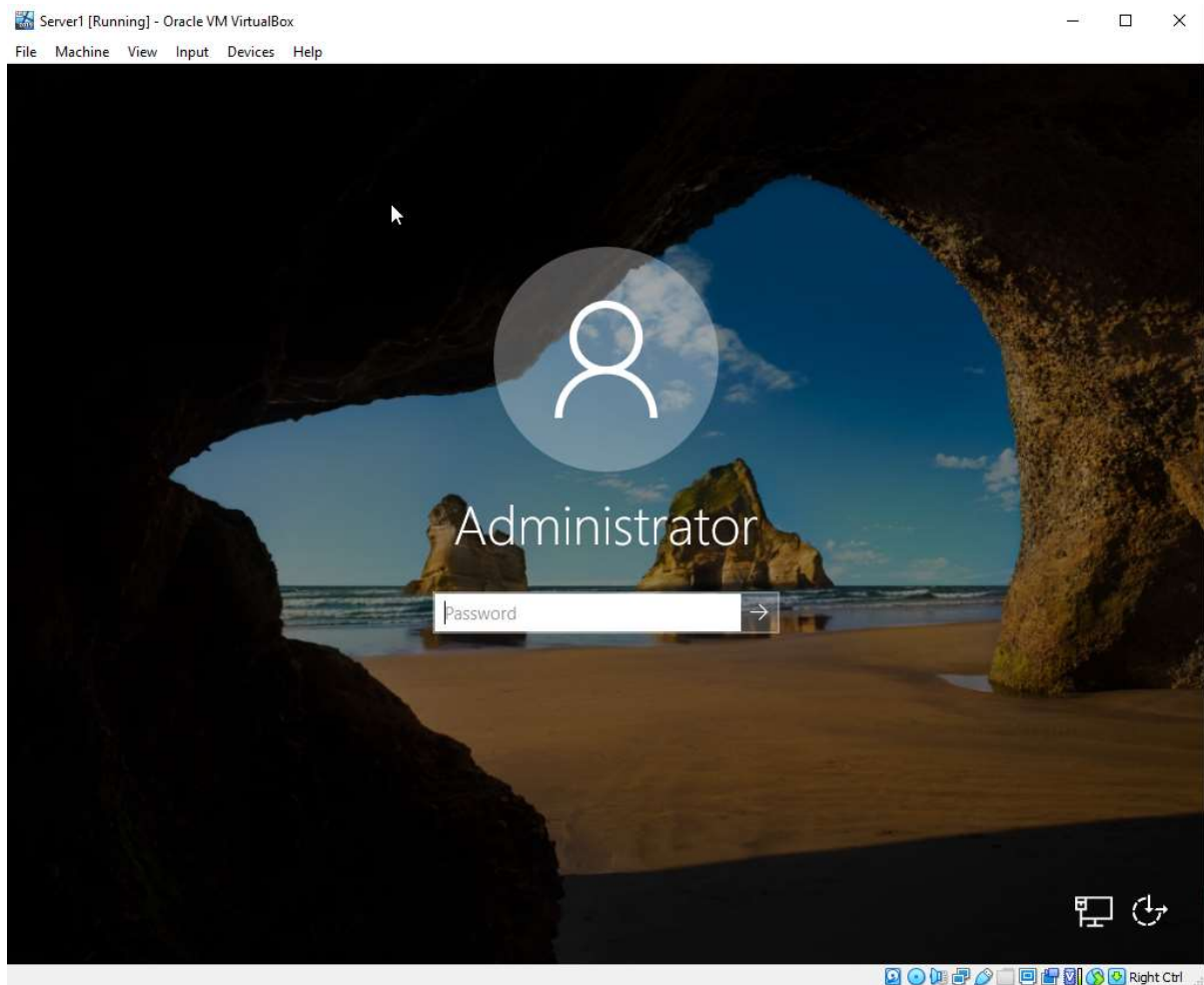
Optimisation Observations:

The host is using a single dedicated GPU and the motherboard does not feature on-board graphical processing. This leaves no option to run the VM using the graphics processor; the system would need more than 1 GPU unit to implement this optimisation.

The host machine is using 32GB of ram, so while it is more than viable to dedicate 8GB of RAM to the VMs as opposed to the default 4GB - there is no benefit to be gained given the use case of the machines.

Windows Installation

Windows server 2019 installed on server 1. The login password for the Administrator account has been set to "P@ssw0rd".

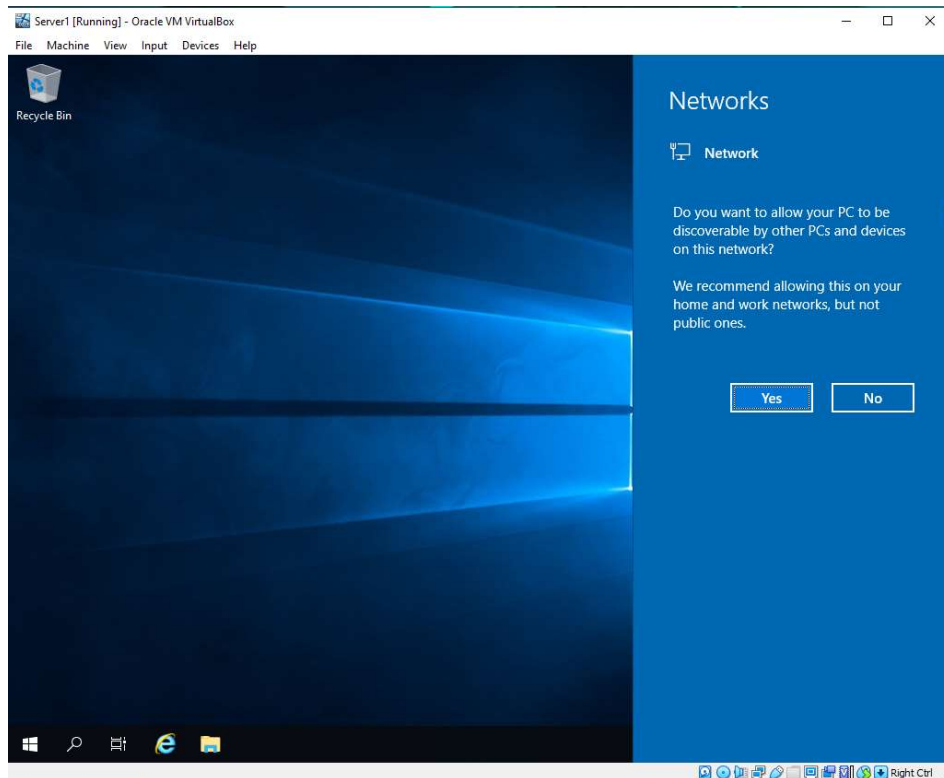


STUDENT NUMBER: 1810613

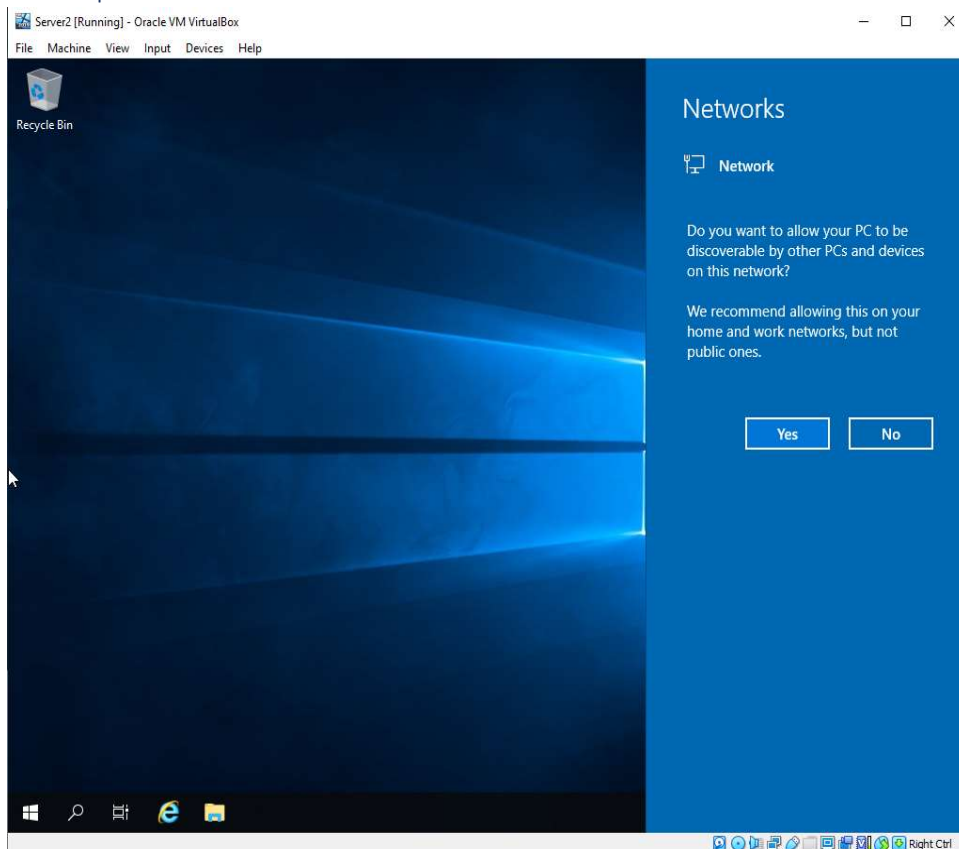
ACCA5023: WORKSHEET 1, PRACTICAL TASKS

Windows Installation Complete

Desktop view server 1



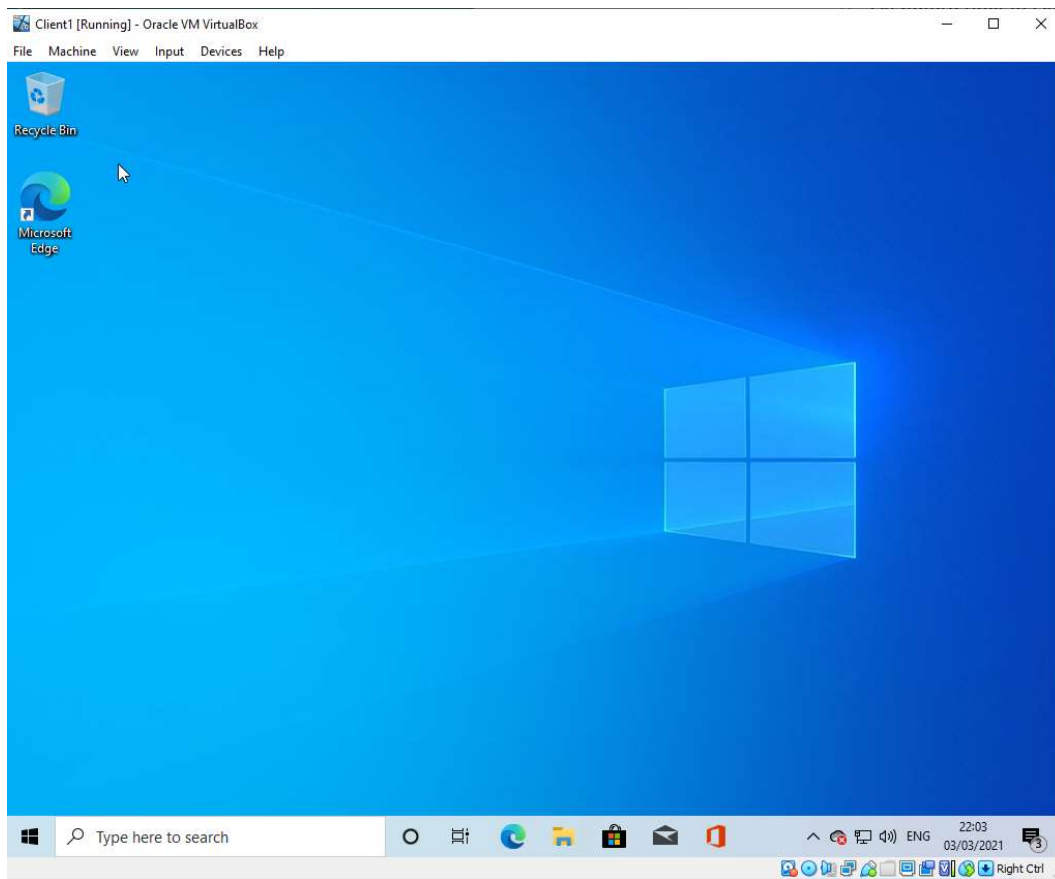
Desktop view server 2



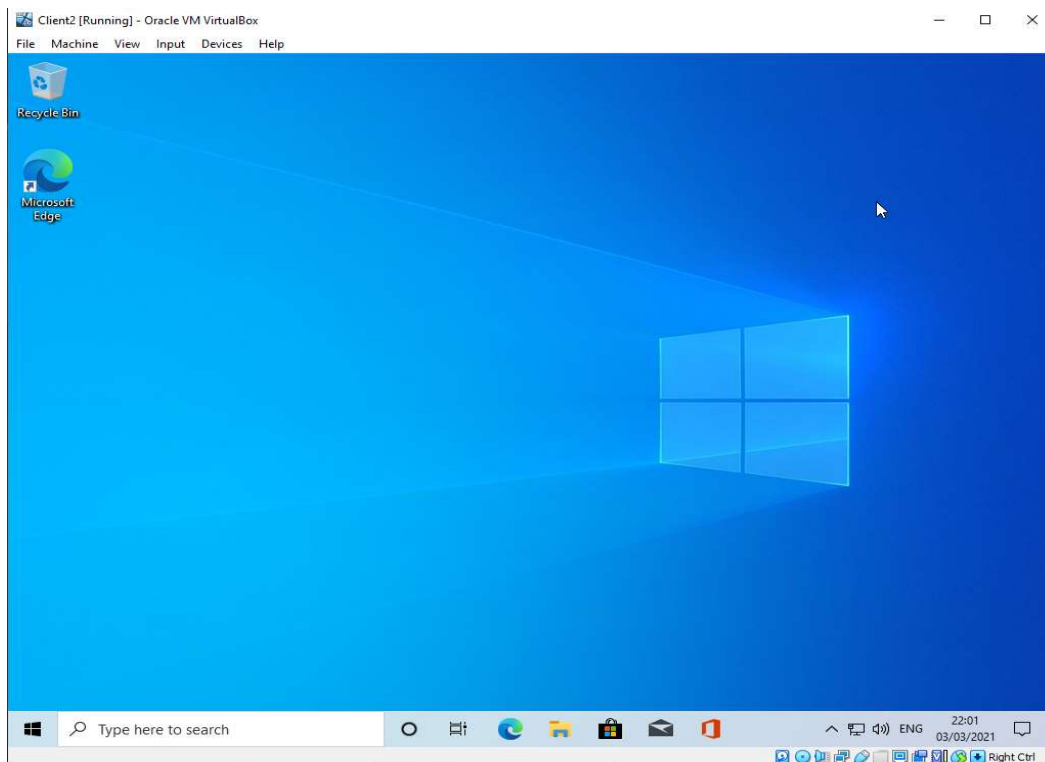
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 1, PRACTICAL TASKS

Desktop view client 1

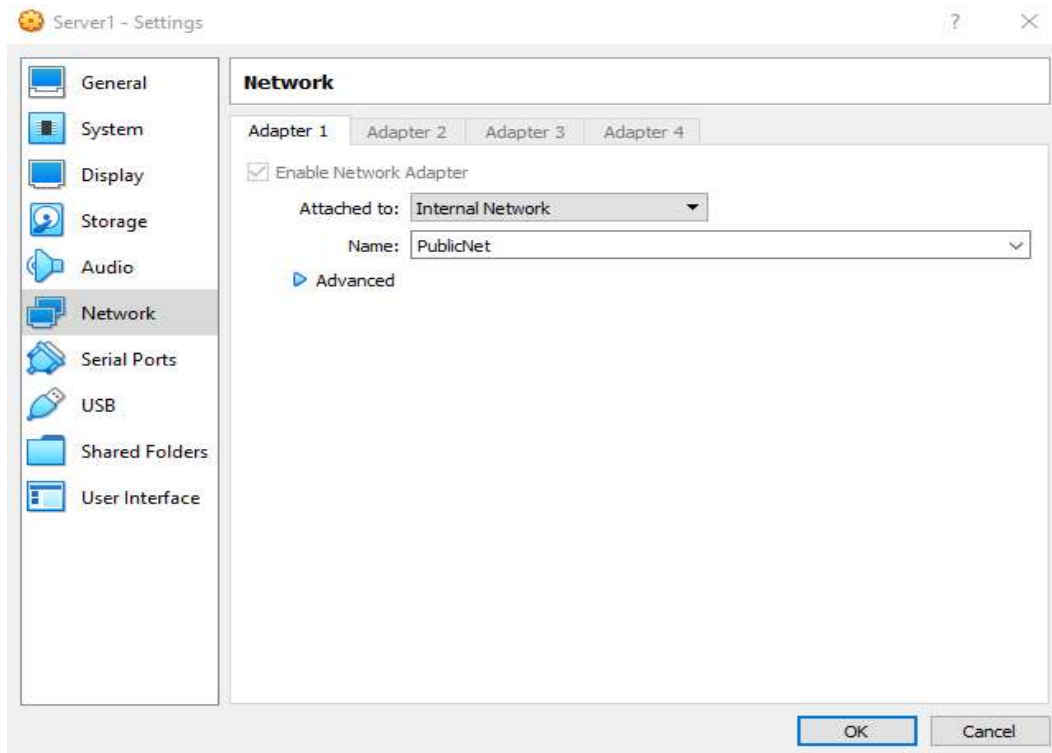


Desktop view client 2

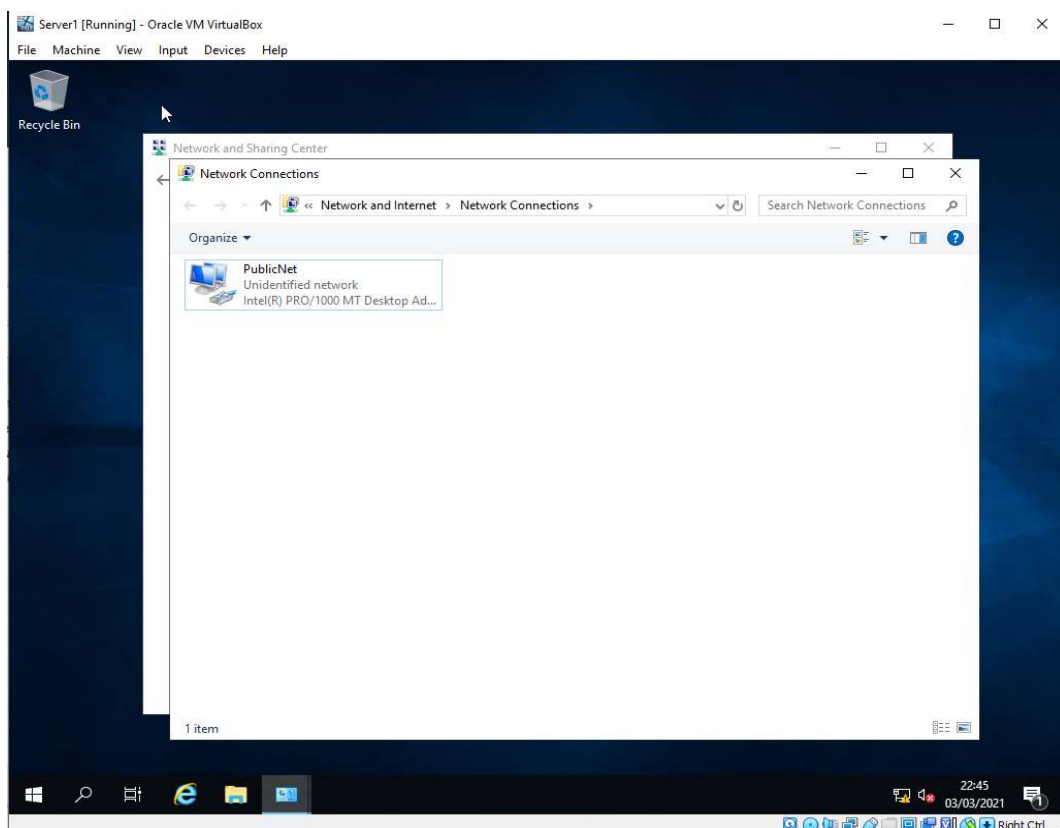


Task 2: Virtual Network configurations

Virtual network adapter set to internal network. The LAN name has been specified as 'PublicNet'.



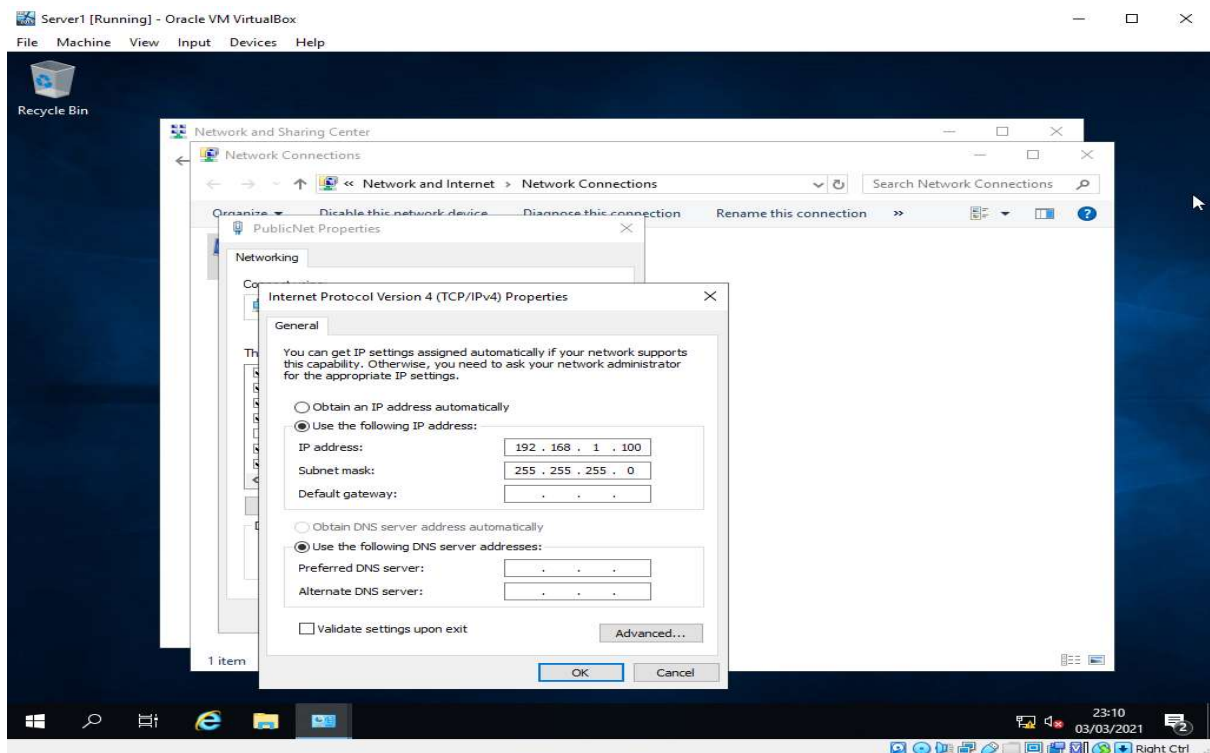
Server1 network connection has been renamed to 'PublicNet'.



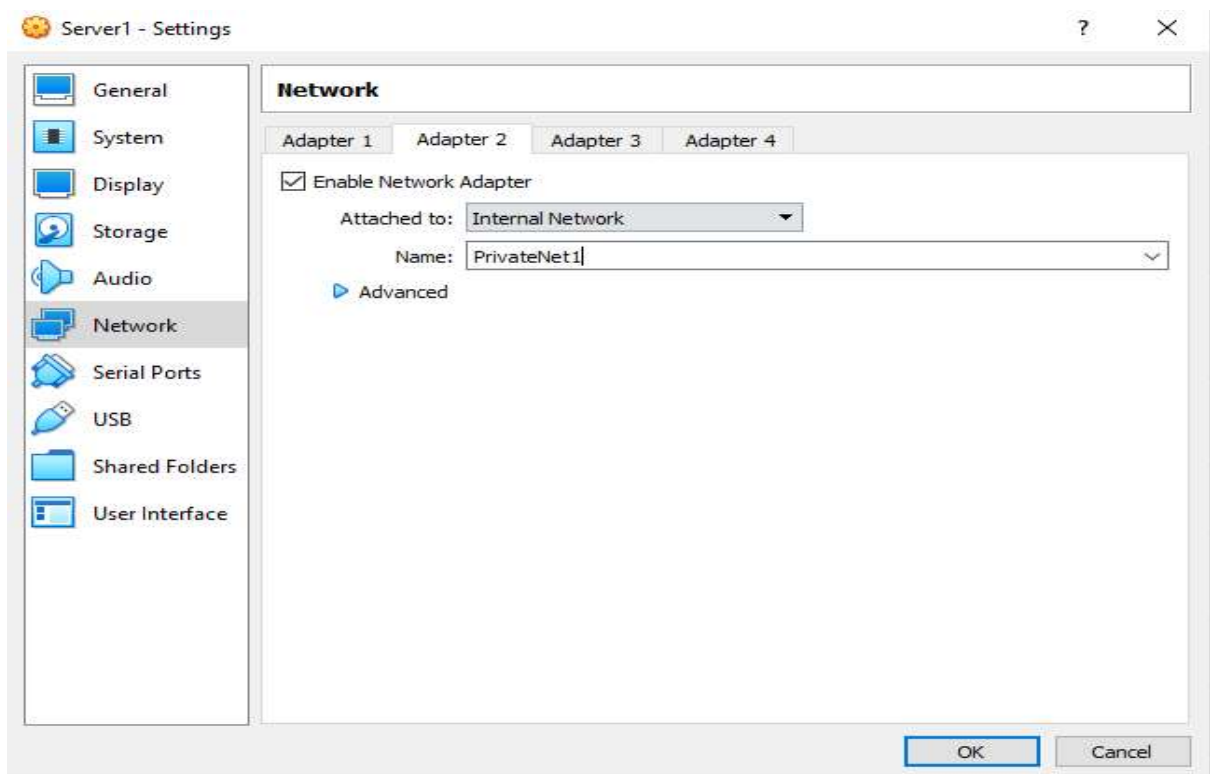
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 1, PRACTICAL TASKS

IP and subnet mask configured for server 1.



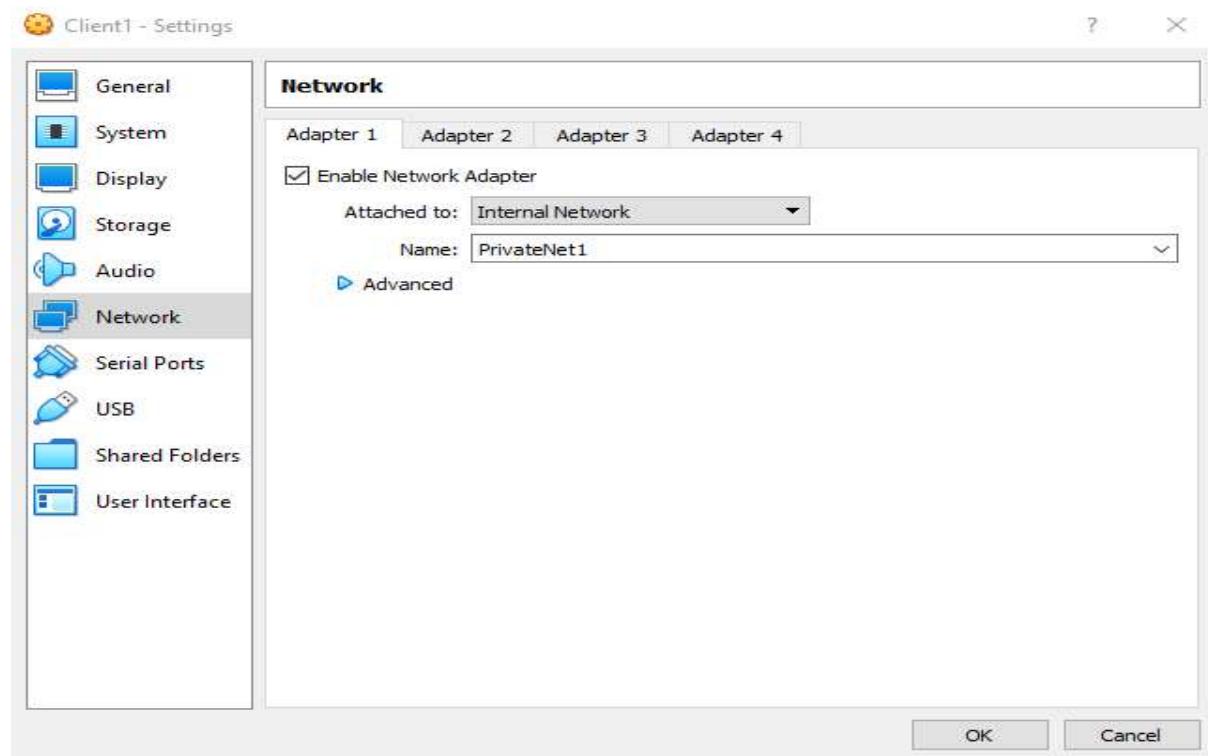
A second virtual network adapter has been configured on a different LAN which has been specified as PrivateNet1.



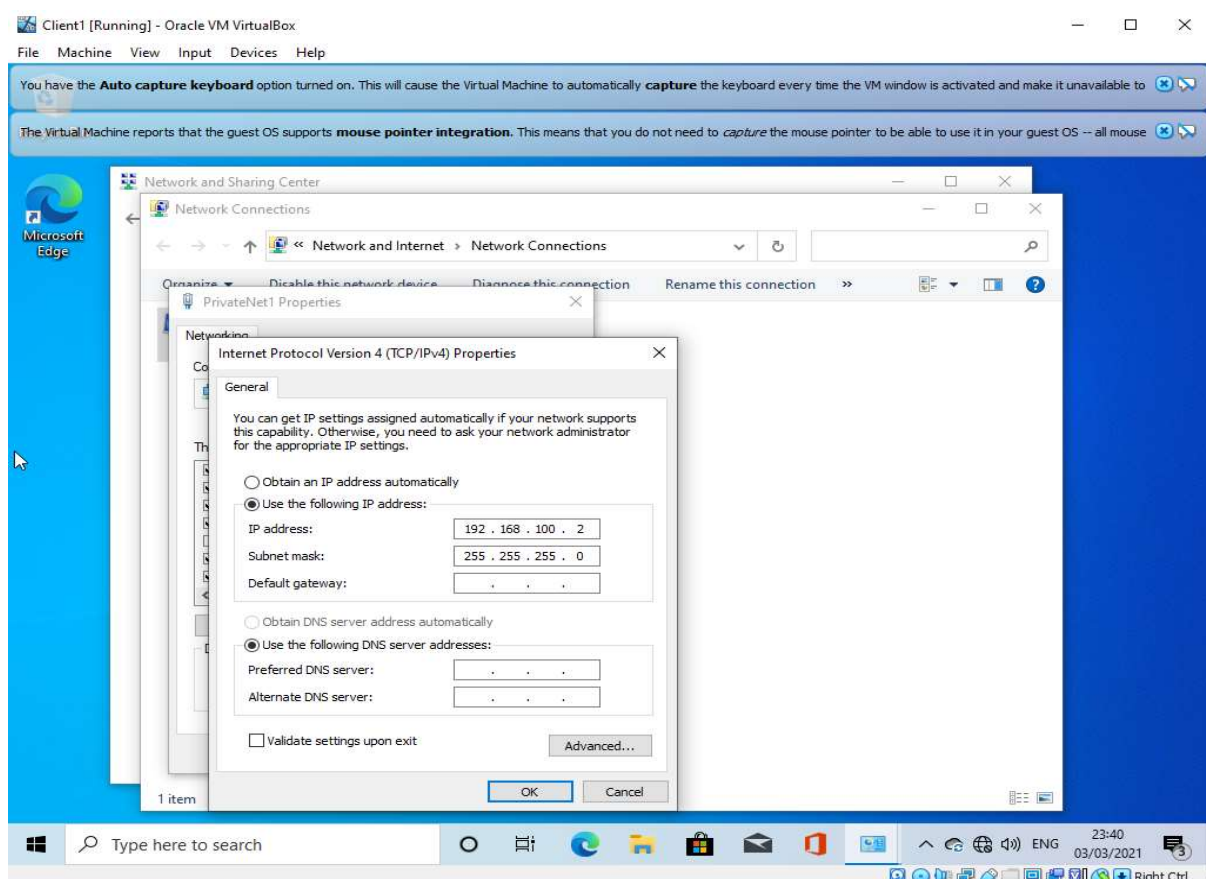
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 1, PRACTICAL TASKS

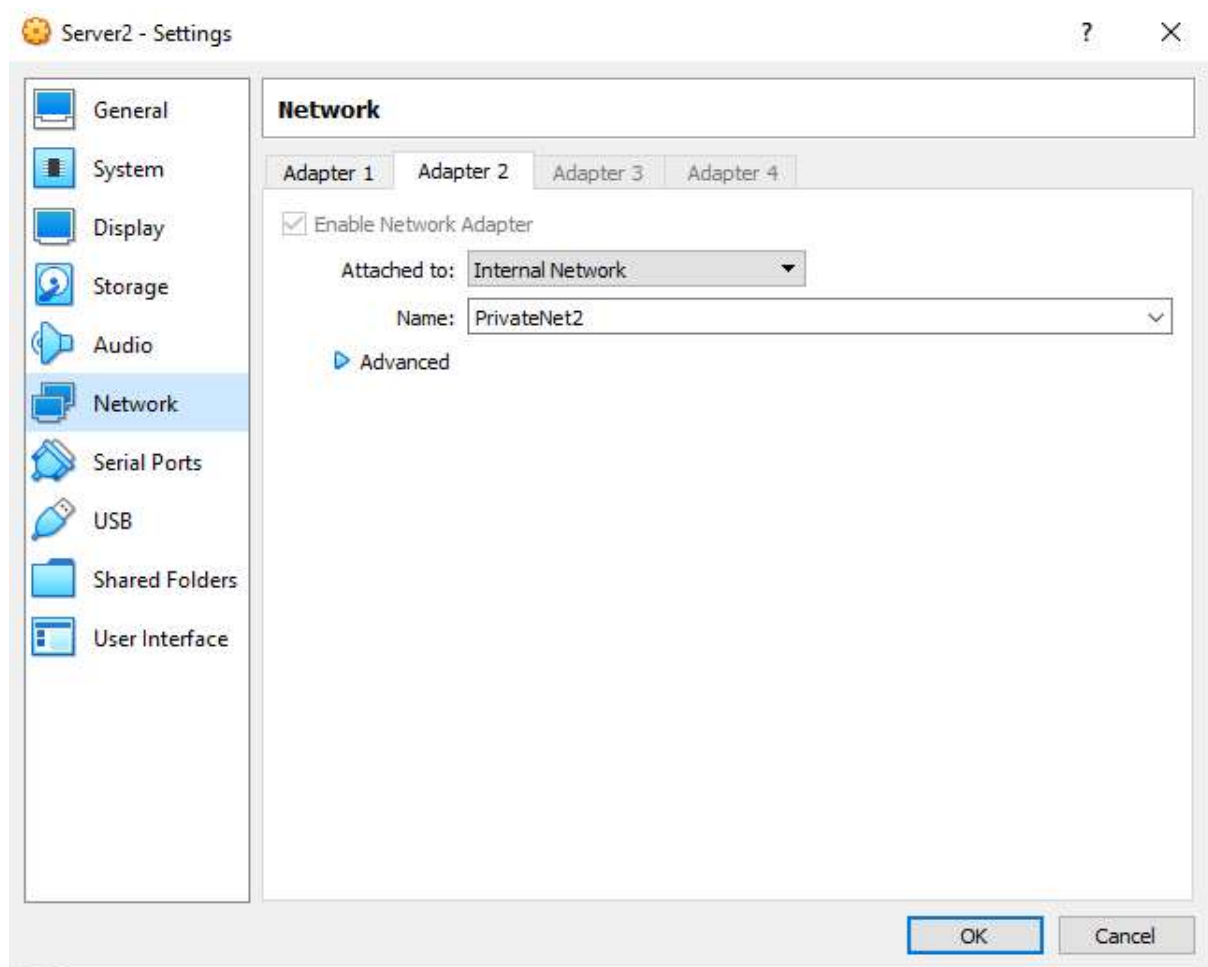
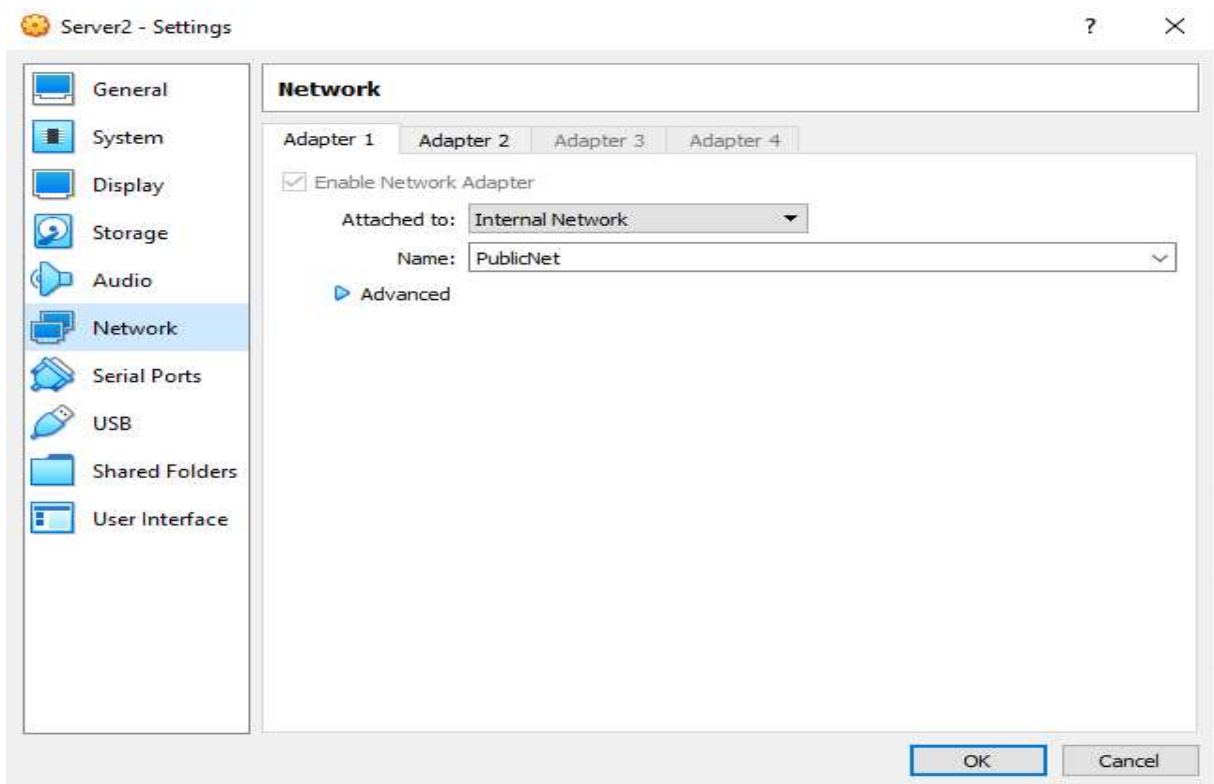
Client 1 has been given the adapter "PrivateNet1"



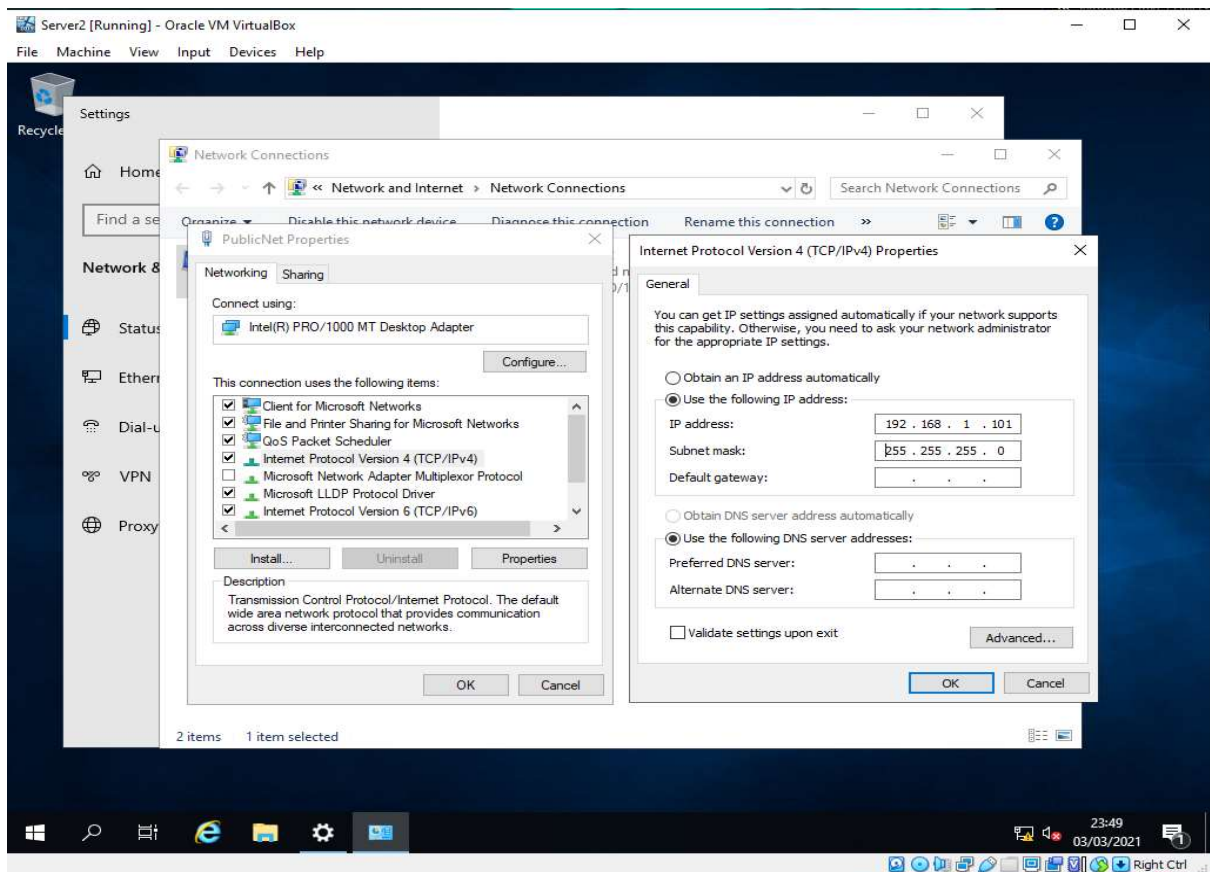
Client 1 IP and subnet mask set for the PrivateNet1 adapter.



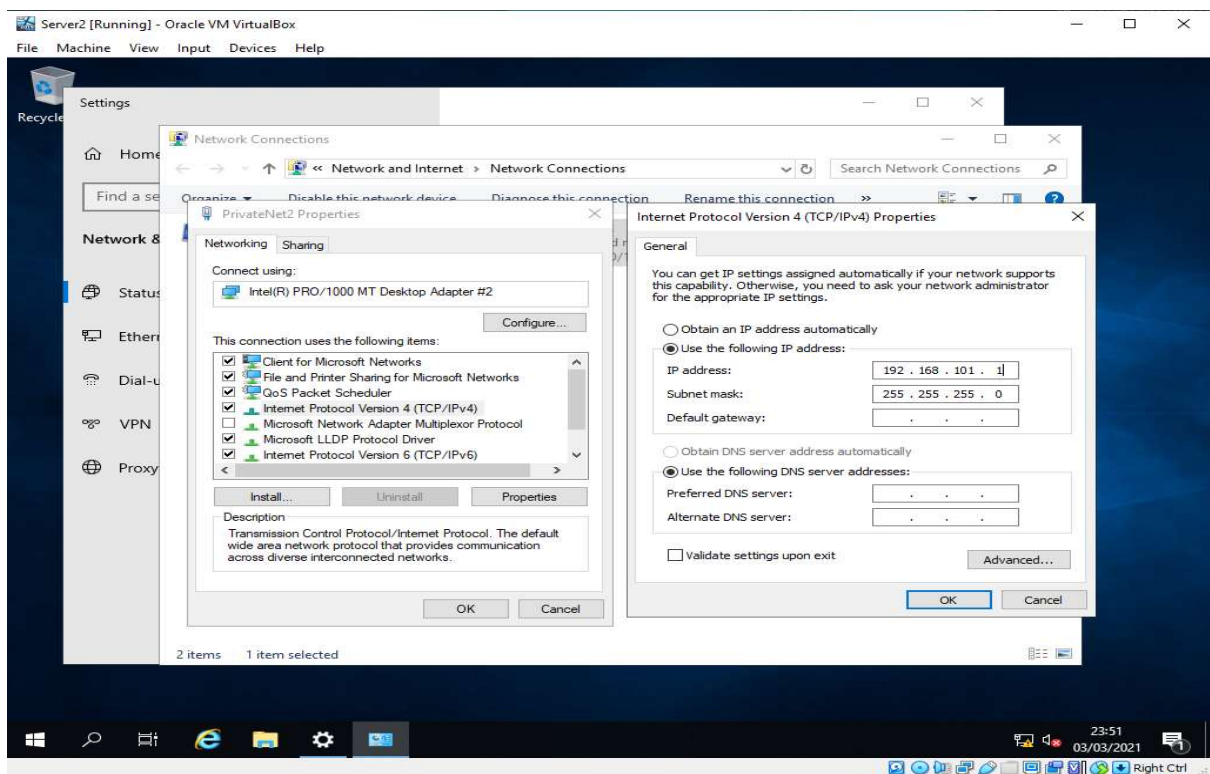
Server2 has both PublicNet and PrivateNet2 adapters configured.



IP and subnet configured for the PublicNet adapter on Server2



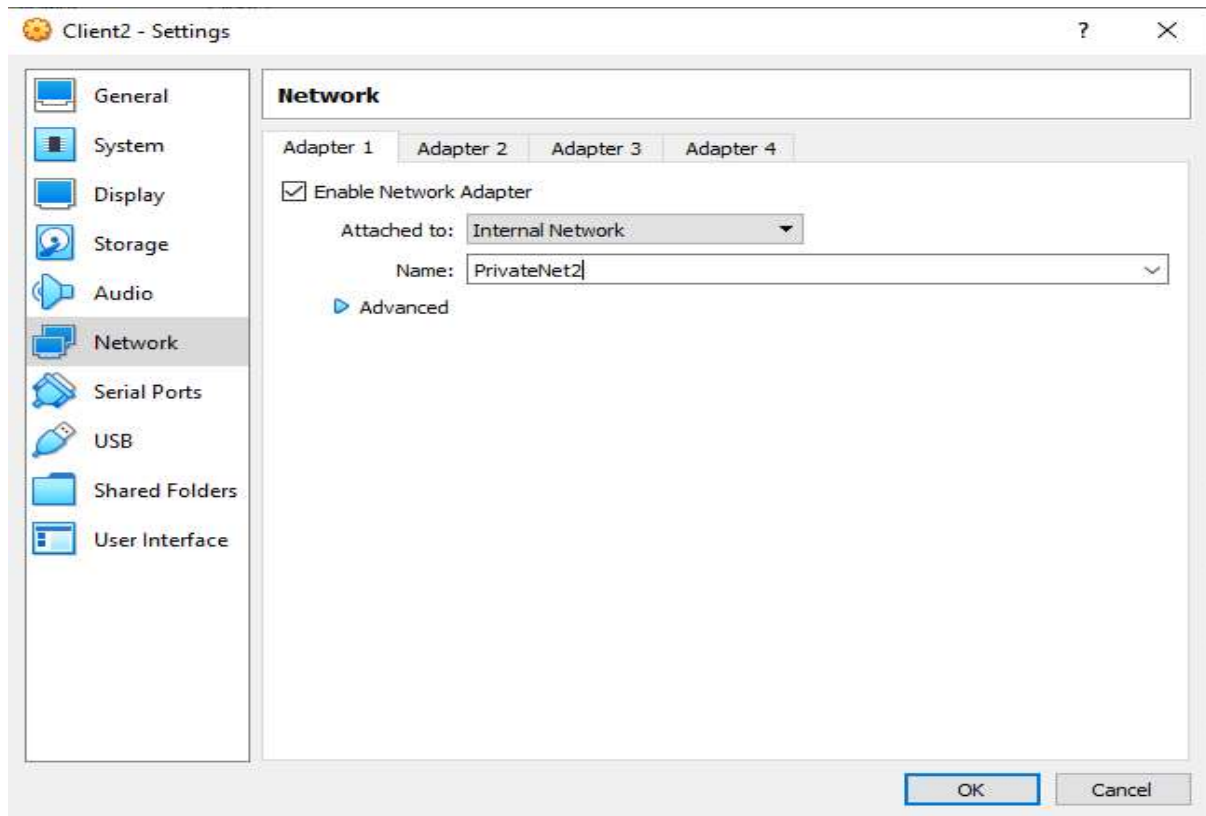
IP and subnet configured for the PrivateNet2 adapter on Server2



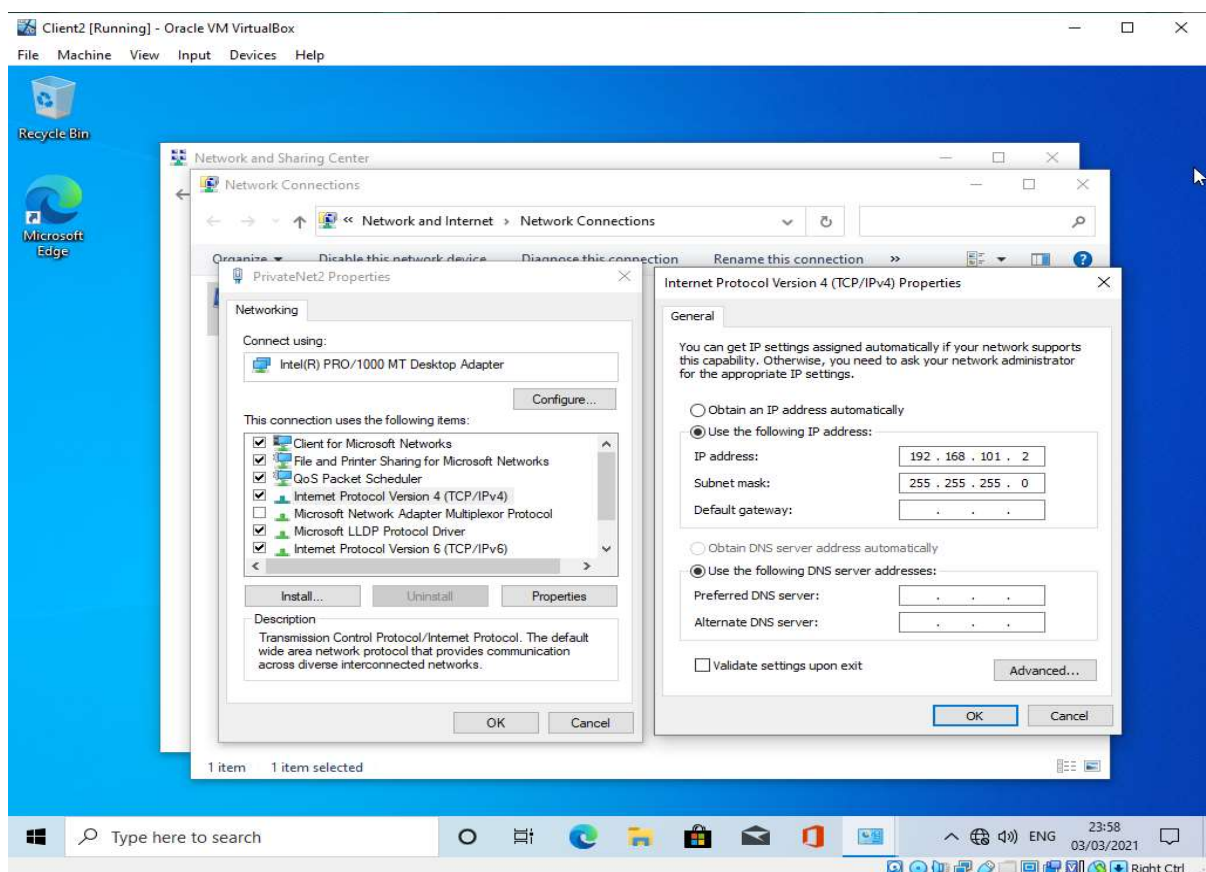
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 1, PRACTICAL TASKS

Client 2 network adapter set to connect to PrivateNet2.



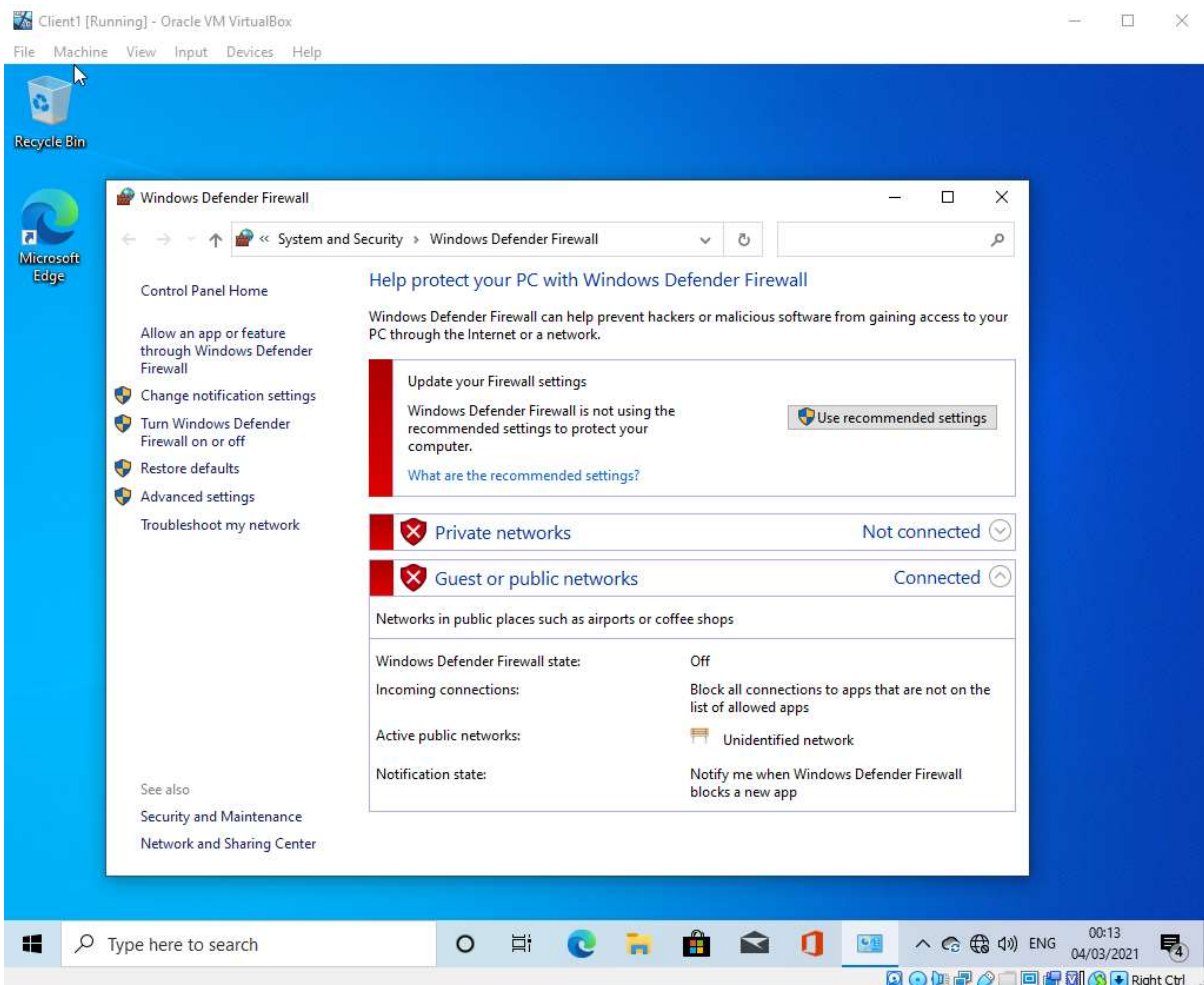
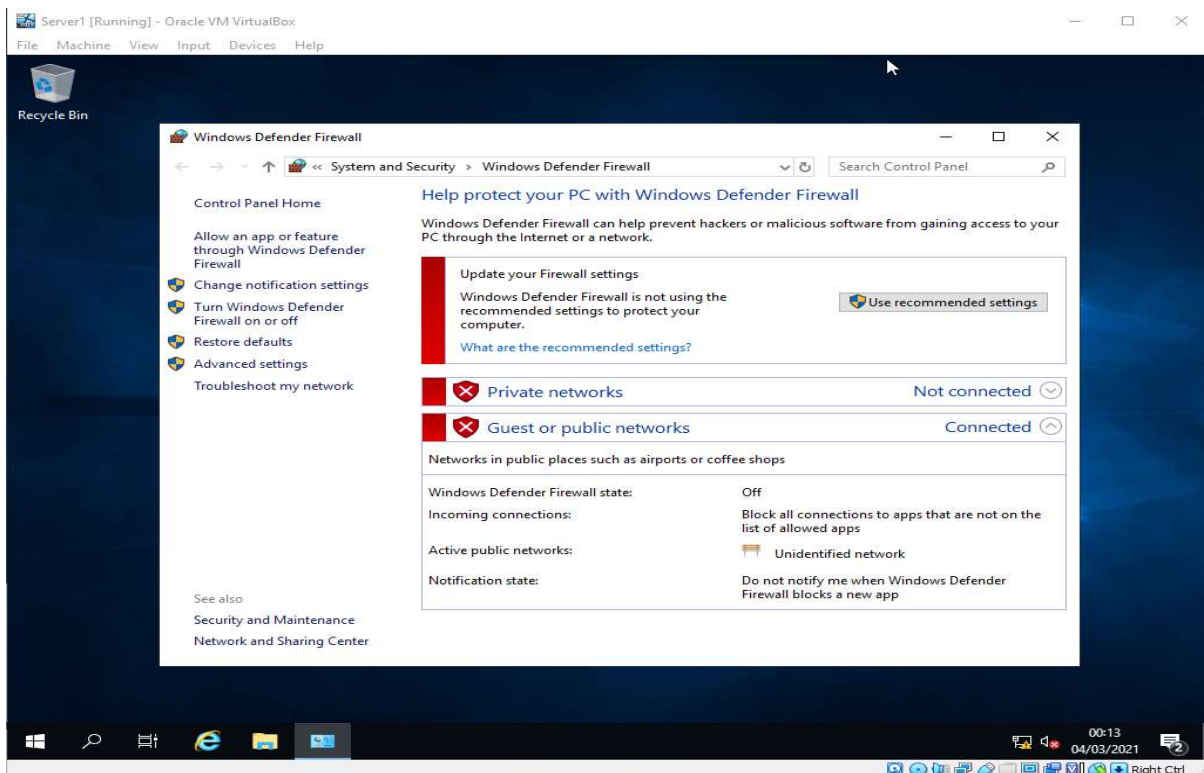
IP and subnet mask configured for PrivateNet2 adapter on Client 2.



STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 1, PRACTICAL TASKS

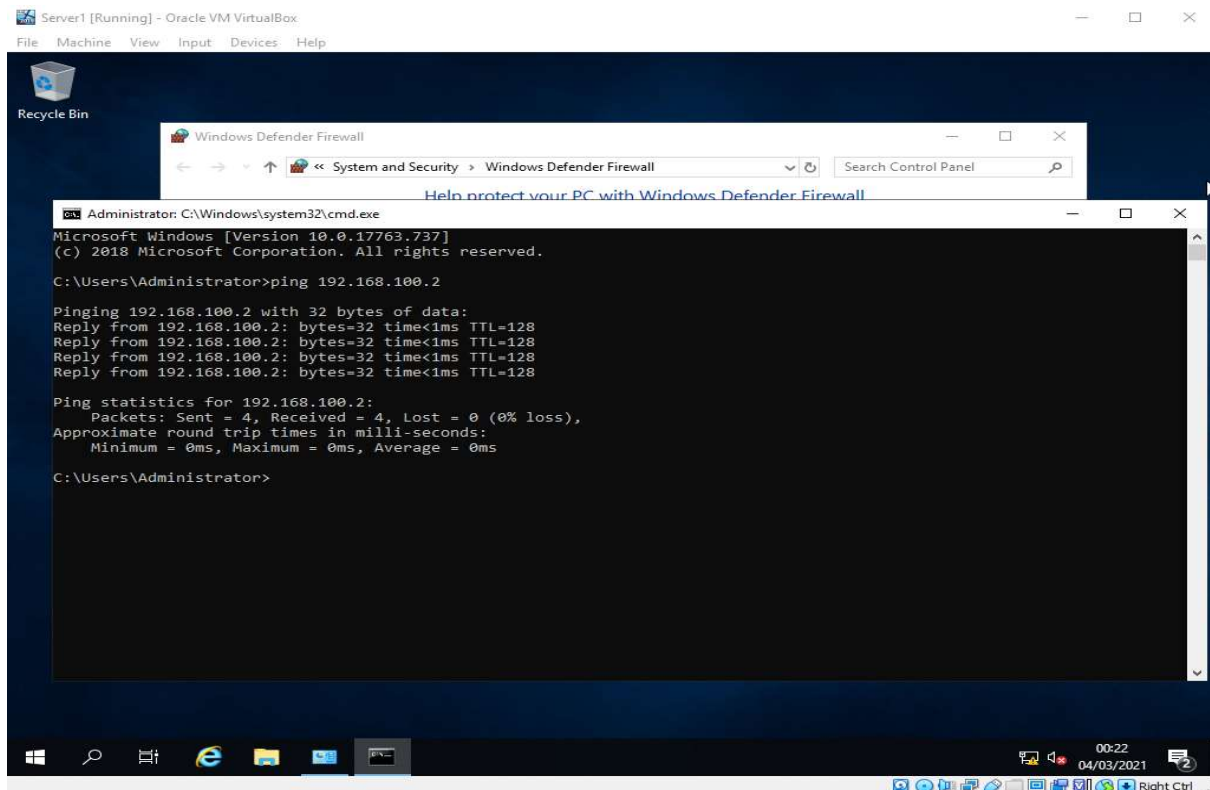
Firewall disabled on both server 1 and Client 1.



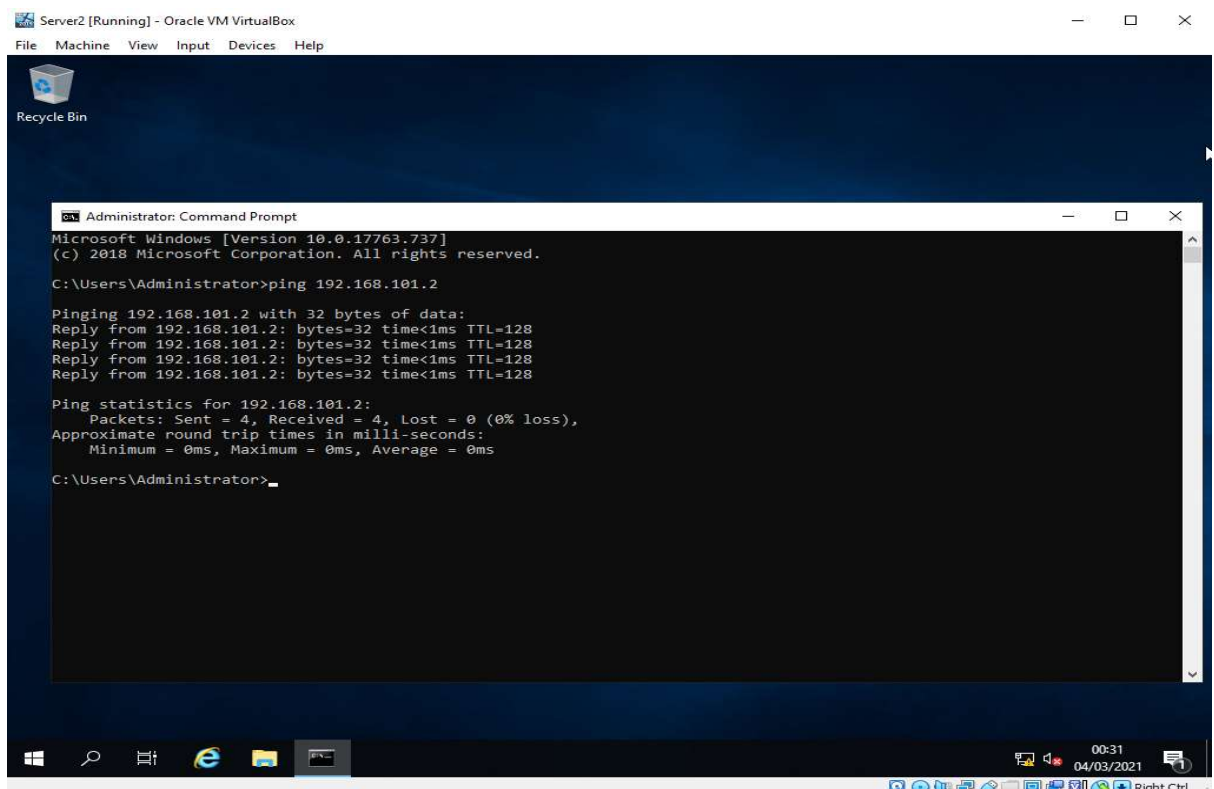
STUDENT NUMBER: 1810613

ACCA5023: WORKSHEET 1, PRACTICAL TASKS

Evidence of connectivity when ping client 1 from server 1



Evidence of connectivity when ping client 2 from server 2 (note that firewall has been disabled on both server 2 and client 2)



Network Operating Systems and Services (ACCA5023)

Worksheet 1: Building a virtual LAN using type 2 hypervisor software.

(Observational Tasks)

STUDENT NUMBER: 1810613

Task 3: Observational Tasks

NB: You should use a proper referencing style here when submitting your answers.

3 a) Describe the main differences between Type 1 and Type 2 Hypervisors. Identify benefits and drawbacks of both and provide some example Vendors.

Type 1 Hypervisors

Type 1 hypervisors are known as “Bare-metal” or “Native” hypervisors (1). They do not require an underlying operating system in order to run. They are run directly on the physical hardware (2) and therefore are not impeded by the “middle layer” of OS or other software. Type 1 hypervisors act as a basic operating system and can control the hardware directly. A machine that is running a type 1 hypervisor cannot be used simultaneously for non-virtualisation purposes, because the hypervisor is acting as an OS itself (3). A management console on another machine is necessary to set up and manage type 1 hypervisors (3).

Type 2 Hypervisors

Type 2 hypervisors are known as “Hosted” hypervisors (2). They do require a pre-existing OS installed on the physical machine in order to run and control the hardware, unlike type 1 hypervisors. This creates an extra layer of software compared with a type 1 hypervisor, as any action performed by either the hypervisor or a virtual machine will be passed through the OS (1). A machine that is running a type 2 hypervisor does not require a separate machine to set up or manage the hypervisor: the virtual machine is launched as an application within the operating system, and all tasks can be performed on the host machine (3).

Comparison of hypervisor types

Type 1 hypervisors are most commonly used in large organisations and enterprises (1). This is because of the increased efficiency over type 2 hypervisors: they do not have a “middle – layer” of software (the OS) draining system resources and increasing latency which results in higher-performance capabilities compared with a type 2 hypervisor (2). This is beneficial in enterprise where the efficient allocation of resources by type 1 hypervisors are an important contributor to economies of scale, or for facilitating data-intensive workloads. Common type 1 hypervisors are scalable allowing expansion and flexibility, which is beneficial when adding, replacing, or removing physical hardware, or working around hardware failure (1).

The independence of type 1 hypervisors from the host operating system means that they are also intrinsically more secure. As the type 1 hypervisor is not reliant on an operating system to function, it is also not as vulnerable to attacks on security flaws that exist within an OS. Any successful attack would be isolated to the OS running on an individual virtual machine (VM) (2). Conversely, an attack on the operating system of the machine hosting type 2 hypervisors could jeopardise all virtual machines running on it, another important consideration for enterprise datacentres.

Licensing fees for type 1 hypervisors are usually out of the reach of smaller organisations and individuals (3). Type 2 hypervisors are usually more affordable, and their downsides (less secure and efficient) are less of a concern for these kinds of users. The fact that a type 2 hypervisor does not prevent a machine from performing other tasks and does not require an additional machine to set it up or manage it makes it more accessible. Type 2 hypervisors are commonly used as test environments, for example, to test software prior to release (2).

Example Vendors

- Type 1 Hypervisor Vendors
 - VMWare vSphere
 - Kernel-Based Virtual Machine (KVM)
 - Microsoft Hyper-V
- Type 2 Hypervisor Vendors
 - Oracle VM VirtualBox
 - VMWare Workstation Pro
 - Windows Virtual PC

3 b) What is the significance of the subnet mask in IPv4 addressing?

To understand why subnet masks are used it is important to consider the routine of dividing or 'subnetting' a network into different chunks or 'sub-networks' – a function carried out by a network administrator to help manage network congestion and improve performance (4).

An important part of IPv4 subnetting is a concept known as the 'subnet mask'. The subnet mask is a 32-bit number which is created by separating the IP address into the network and host addresses. This is achieved by by setting all host bits to 0 and all network bits to 1 (5).

Depending on the type of network class, (A,B OR C) a different default subnet mask is given to identify the network and host portions of an IPv4 address. The subnet mask is compared to the IPv4 address bit for bit, from left to right.

Class A: 255.0.0.0 – The subnet mask is used for the first network portion of the address, with octets 2, 3, and 4 left for the network administrator to distribute into subnets or hosts as required.

Class B: 255.255.0.0 – The subnet mask is used for the first two octets of the network, with octets 3 and 4 left for the network administrator to distribute into subnets or hosts.

Class C: 255.255.255.0 - The first three octets are the network portion in type C addresses, with just octet 4 remaining for the network administrator to divide into subnets or hosts.

This significance of the subnet mask is that is used to determine whether a host is on the local subnet or on a remote network. This is important: as hosts can talk directly to other hosts on the same network, but for external networks, they would need the use of a router to talk to the external hosts (6).

3 c) Cloud computing has revolutionised the way that enterprise networks are hosted. Describe the use of cloud computing including its benefits and drawbacks and identify example vendors within the industry.

Enterprise networks facilitate the movement of data across servers, user PCs and other services. Users can typically access a host datacentre through a Local Area Network (LAN) or VPN for users outside of the local area (7). Previously, an organisation would require a large initial outlay in setting up a network: there are both hardware and implementation costs (8). Once an organisation has surpassed this barrier, they are then faced with the logistical challenges of maintaining a reliable, secure, efficient network: equipment failure, data loss, security challenges, and futureproofing their infrastructure (7). A company may be limited in how quickly they can react to fluctuations in demand (i.e. maintaining unnecessary infrastructure or expanding current infrastructure capabilities) (9). The high set up costs of developing and maintaining enterprise networks is often considered a significant barrier to entry for new companies and a limiting factor for existing companies.

Cloud Computing is where resources such as servers, networks and software applications are accessed over the internet instead of being owned and managed by an organisation on its own premises (9). Infrastructure as a Service (IaaS) is a type of cloud computing that allows an organisation to use network resources over the internet on a pay-as-you-go basis (8). An IaaS service provider will offer use of its physical data centres, without the need for end users to access them physically. The service provider will undertake all maintenance and security associated with their upkeep, and manage hypervisors for the end users. The end users will be able to use CPUs, GPUs, memory and storage on-demand, supplied by the service provider, over the internet (8). The user can implement their own OS, applications and data in the same way they would using traditional infrastructure. The user can scale their requirements rapidly, according to their needs, an advantage over traditional enterprise networks. This has also reduced the barriers to entry for smaller organisations: they can now compete with more established companies, without the logistical challenges of setting up and maintaining their own enterprise network.

Example Vendors

- Amazon Web Services (largest provider)
- Microsoft Azure
- Google Cloud Platform
- IBM

3 d) Give an in-detail description about the different terminologies and its purposes (like (not limited to) Ping, Server Management, Firewall, PAE/NX, OOBE etc) you came across during the Task 1 and Task 2. Compare your list of terminologies in the aspect of their operations/functionality with other Network Operating Systems. *(For example: If you select Windows Firewall and describe the operations/functionality of Windows Server 2019 Firewall, you have to compare these features with the operations/functionality of other Network Operating Systems like Linux, Mac)*

Ping

The Ping tool measures the amount of time it takes to send a packet to a destination computer and be returned. It is a test that is used to ensure the host address is reachable before a payload is sent across the IP Network. The Ping tool sends a number of echo request packets (typically four or five) of a known size to an IP address and a “Pong” response from the destination returns an echo reply packet (10). The time between these responses in milliseconds demonstrates the latency, and the number and size of the packets is recorded to demonstrate that there are no network errors. It will time out if no response is received (10). The packets time-to-live (TTL) is calculated, which indicates how many further “hops” a packet can make before it is disregarded. This is known as a “hop limit” in IPv6, and all packets have this value specified as it is a requirement of the Internet Protocol.

The Ping tool can be used as a troubleshooting tool: for example, checking that the local computer is added to the network by Pinging it's IP address (11).

Server Management

Essential elements of server management include monitoring hardware and components to ensure that servers perform adequately; ensuring that all software is kept updated; ensuring that data is kept backed-up, with an adequate plan for its recovery should something go wrong; and ensuring the security of the server by implementing suitable firewalls, encryption and access controls. These are discussed in more detail below:

- Hardware
 - Hardware should be specified in line with the requirements of the organisation:
 - hardware that is insufficient for the needs of the organisation will affect the performance of the server and require expansion prematurely, wasting time and money
 - hardware vastly in excess of what is required will increase costs, both in initial outlay and running costs
 - Monitoring the CPU, hard drive, RAM and other components, and replacing or upgrading them when they are nearing capacity or end-of-life to maintain optimum performance
 - Ensuring that the physical server environment is appropriate
 - The server room conditions should be carefully controlled to avoid spikes in temperature or humidity
 - There should be appropriate airflow in the server room

- Hot aisles and cold aisles, with sealed racks of servers can optimise cooling efficiency (12)
 - Ensuring that an Uninterruptable Power Supply (UPS) and backup generator are available in case of power outage in order to prevent data loss
- Software
 - Ensuring that all software on the servers is up to date to ensure optimum performance and prevent vulnerabilities in out of date software being exploited
- Backups
 - Whole-system or incremental backups may be appropriate depending on the types of data that is being backed up
 - Disc images (golden image?)
- Security
 - Ensuring that the servers are adequately protected from security threats, for example, implementing firewalls, user access management, etc.

Firewall

A firewall is the first line of defence for a network against external security threats. It monitors all traffic on the network and can allow or block traffic according to set security rules, protecting the internal network from external threats. Firewalls filter traffic by only allowing packets which meet pre-defined criteria to pass through. Five types of firewall are: packet filtering firewalls, which compare packets against access control lists; circuit-level gateways, which monitor TCP handshakes to determine whether requested transactions are from a trusted, legitimate source; application-level gateways (also known as a proxy firewall) which monitors all data exchanges, and can also be used to prevent users accessing restricted websites (13); stateful inspection firewalls, which not only monitors individual packets, but considers packets in context of the connection in order to detect unusual or suspicious patterns (14); and next-generation firewalls, which combine stateful inspection and deep packet inspection with functions such as antivirus and antimalware (15).

The two main methods of deploying a firewall are network-based firewalls, which are hardware-based and filters traffic between a secured LAN or intranet and the internet, and host-based firewalls, which are software-based and placed on a host computer (16). Most commonly, a network-based firewall is used as a barrier to protect an enterprise network from internet-based threats. It cannot be disabled remotely because it is hardware based, with separate ports for the internal network, and separate ports for the internet (16). It therefore does not affect the performance of the network. The configuration of the network ports control access to areas of the network (e.g. between the host and a web server, or between a host and the internet). Should a security threat bypass the firewall, it will not be able to compromise other areas of the network. Their use is generally limited to larger organisations, due to the increased difficulty of implementing and configuring them correctly (15). A host-based firewall is used to add a second layer of defence should a threat

bypass the network-based firewall. It can also be used in isolation, but this is usually limited to home and personal use where network-based firewalls would be excessive. It monitors and controls traffic entering and leaving the host PC. It can additionally provide protection from malware, as it is connected to processes that are running on the host computer (16). They are easy to implement and are commonly included with an OS on installation. However, as it is running on the host system, it can be turned off remotely in a successful security breach.

PAE/NX

Physical Address Extension (PAE) is a feature that allows more room for the physical page address in the page table entry by enlarging the page table entry from 32 bits to 64 bits on compatible CPUs. This allows the CPU to access a larger address space, and thus supports more than 4gb of addressed memory (17). The NX-bit marks an area of memory as non-executable to dedicate them to either code or storage. It does so by marking bit 63 to **1** to prevent code execution, or **0** to allow it. By preventing areas of memory from being executable, it prevents buffer overflow attacks, an exploit that purposely attempts to exceed the storage capacity of the memory buffer to insert additional code and breach a systems security (18). Enabling this feature when setting up a hypervisor, virtual machine, or operating system will both prevent some memory errors and buffer overflow attacks. Some OSes, such as Ubuntu Server must have PAE enabled as a requirement for function (17).

OOBE

Out of the Box Experience (OOBE) refers to the starting screens that a user will see on starting an OS on their PC for the first time. For these tasks, the operating system used was Windows 10, and so this section will discuss the Windows 10 OOBE. The OOBE ensures that common features and settings are suitably configured before first use. When starting the system, the user is required to accept the licence agreement, select a language and region and set up an internet connection etc (19).

Bibliography

1. **Taylor, K.** Type 1 vs Type 2 Hypervisors. *HiTechNectar*. [Online] [Cited: 28 02 2021.] <https://www.hitechnectar.com/blogs/hypervisor-type-1-vs-type-2/>.
2. **Bigelow, SJ & Kirsch, B.** What's the difference between Type 1 vs. Type 2 hypervisor? *SearchServerVirtualization.com*. [Online] 13 01 2021. <https://searchservvirtualization.techtarget.com/feature/Whats-the-difference-between-Type-1-and-Type-2-hypervisors>.
3. **Simic, S.** What is a Hypervisor? Types of Hypervisors 1&2. *phoenixNAP Global IT Services*. [Online] 24 01 2019. [Cited: 28 02 2021.] <https://phoenixnap.com/kb/what-is-hypervisor-type-1-2>.
4. **Field Engineer.** Subnetting. *Field Engineer*. [Online] [Cited: 01 03 2020.] <https://www.fieldengineer.com/skills/subnetting>.
5. **AVI Networks.** Subnet Mask Definition. *AVI Networks*. [Online] [Cited: 01 03 2021.] <https://avinetworks.com/glossary/subnet-mask/>.
6. **Microsoft.** Understand TCP/IP addressing and subnetting basics. *Microsoft*. [Online] 21 09 2020. [Cited: 01 03 2021.] <https://docs.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-addressing-and-subnetting>.
7. **VMWare.** Enterprise Networking. *vmware*. [Online] [Cited: 01 03 2021.] <https://www.vmware.com/topics/glossary/content/enterprise-networking>.
8. **IBM Cloud Education.** IaaS (Infrastructure-as-a-Service). *IBM*. [Online] 12 07 2019. [Cited: 01 03 2021.] <https://www.ibm.com/cloud/learn/iaas#toc-what-is-ia-k7Negcdh>.
9. **IBM.** Cloud computing: A complete guide. *IBM*. [Online] [Cited: 28 02 2021.] <https://www.ibm.com/cloud/learn/cloud-computing-gbl>.
10. **PAESSLER AG.** IT Explained: Ping. *PAESSLER The Monitoring Experts*. [Online] [Cited: 02 03 2021.] <https://www.paessler.com/it-explained/ping>.
11. **Microsoft.** Using the Ping Command. *Microsoft*. [Online] 07 03 2012. [Cited: 02 03 2021.] [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732509\(v=ws.10\)?redirectedfrom=MSDN](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732509(v=ws.10)?redirectedfrom=MSDN).
12. **Vaughan-Nichols, SJ.** The best ways to manage data center airflow. *TechBeacon*. [Online] [Cited: 02 03 2021.] <https://techbeacon.com/enterprise-it/best-ways-manage-data-center-airflow>.
13. **The Open University.** Network Security. *OpenLearn*. [Online] [Cited: 04 03 2021.] <https://www.open.edu/openlearn/science-maths-technology/computing-and-ict/systems-computer/network-security/content-section-9.5>.

14. **Fortinet.** Stateful vs. Stateless Firewalls. *Fortinet*. [Online] [Cited: 04 03 2021.] <https://www.fortinet.com/resources/cyberglossary/stateful-vs-stateless-firewall>.
15. **DeCarlo AL & Ferrell, RG.** The 5 different types of firewalls explained. *TechTarget*. [Online] 01 2021. [Cited: 04 03 2021.] <https://searchsecurity.techtarget.com/feature/The-five-different-types-of-firewalls>.
16. **Andrea, H.** Network based Firewall vs Host based Firewall-Discussion and Comparison. *Networks Training*. [Online] [Cited: 02 03 2020.] <https://www.networkstraining.com/network-based-firewall-vs-host-based-firewall-discussion-and-comparison/>.
17. **Virtual Box.** Chapter 3. Configuring Virtual Machines. *Virtual Box*. [Online] [Cited: 04 03 2021.] <https://www.virtualbox.org/manual/ch03.html>.
18. **imperva.** Buffer Overflow Attack. *imperva*. [Online] [Cited: 05 03 2021.] <https://www.imperva.com/learn/application-security/buffer-overflow/>.
19. **Windows Hardware Developer.** Customize the Out of Box Experience (OOBE). *Microsoft*. [Online] 09 07 2018. [Cited: 05 03 2021.] <https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/customize-oobe>.