Journal

Mohammed Bin Ali

COIT20246 Networking & Cyber Security
Student ID - 12227071

Submitted to
Unit Cordinator - Steven Gordon
Tutor - Tarek Elwan

Week 4

Task 1. View Routing Table

ifIndex	DestinationPrefix	NextHop	RouteMetric	ifMetric	PolicyStore
1	255.255.255.255/32	0.0.0.0	256	75	ActiveStore
1	224.0.0.0/4	0.0.0.0	256	75	ActiveStore
1	127.255.255.255/32	0.0.0.0	256	75	ActiveStore
1	127.0.0.1/32	0.0.0.0	256	75	ActiveStore
1	127.0.0.0/8	0.0.0.0	256	75	ActiveStore
1	ff00::/8	::	256	75	ActiveStore
1	::1/128	::	256	75	ActiveStore

- The DestinationPrefix column shows the network address or prefix of the destination network that the route applies to. For example, "0.0.0.0/0" means the default route, which is used for all destinations that don't match any more specific route.

- The NextHop column shows the IP address of the next hop or gateway that the computer should use to reach the destination network. For example, if the destination network is on a different subnet, the next hop might be the router that connects the two subnets.

- The RouteMetric column shows the cost or priority of the route. Lower values indicate a more preferred route.

- The InterfaceAlias column shows the name of the network interface that the route applies to. This can be useful for troubleshooting connectivity issues on specific interfaces.

- The AddressFamily column shows whether the route is for IPv4 or IPv6.

- The Protocol column shows the routing protocol that created the route. Different protocols have different behaviors and priorities, and may be used in different network topologies.

- The PolicyStore column shows where the route is stored. Routes can be stored in the active routing table, the persistent routing table, or other policy stores, depending on how they were created or modified.

Task 2. IP Network Design

a) IP Address Assignment:

For the first LAN : Configuring based on last 4 digits of my Student ID : 1222**7071**

| Device/Interface | IP Address | Subnet Mask | Default Gateway |

PC1	**70.71.**56.1	255.255.255.0	**70.71.**56.254
PC2	**70.71.**56.2	255.255.255.0	**70.71.**56.254
PC3	**70.71.**56.3	255.255.255.0	**70.71.**56.254
Switch1 Port1	**70.71**.56.254	255.255.255.0	N/A

For the second LAN (based on your partner's last four digits of their student ID): 1222**2522**

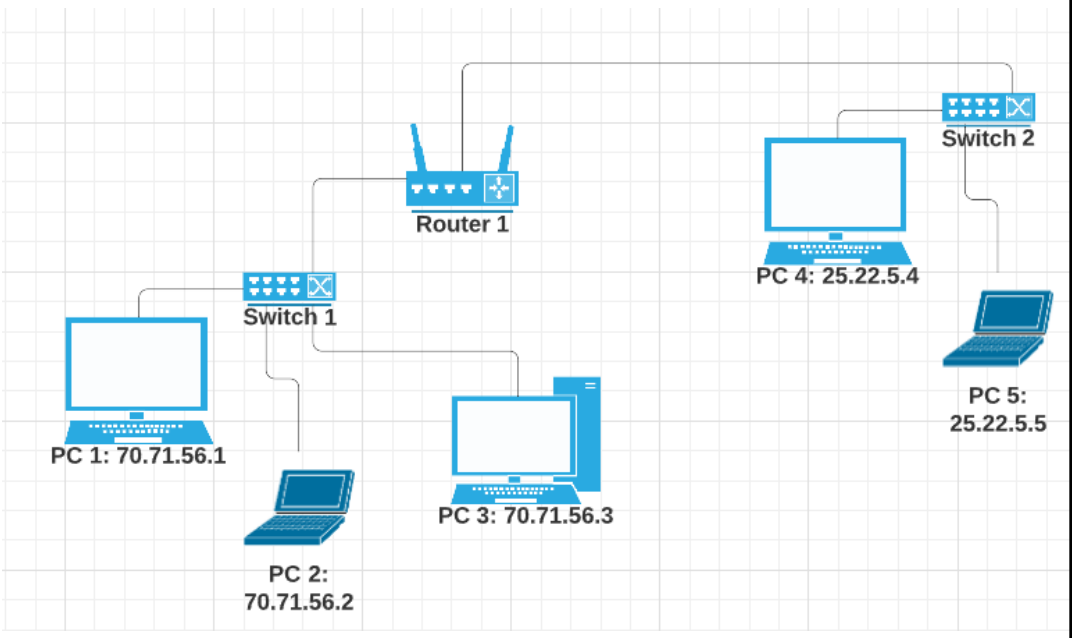
| Device/Interface | IP Address | Subnet Mask | Default Gateway |

PC4	**25.22.**5.4	255.255.255.0	**25.22.**.5.254
PC5	**25.22.**5.5	255.255.255.0	**25.22.**5.254
Switch2 Port1	**25.22.**5.254	255.255.255.0	N/A

For the WAN link:

| Device/Interface | IP Address | Subnet Mask | Default Gateway |
| Router1 Interface1 | **70.71.**57.1 | 255.255.255.252 | N/A |

b) Network Diagram:



c)RoutingTables:

Router1:

Destination|Next

Switch1(NetworkA)|DirectS

witch2(NetworkB)|Direct

***|Router**

d)PacketICMP/IPDiagram:

[PC1](**70.71.**56.1)>(**70.71.**56.254)[Switch1Port1]<WANLink>[Switch2Port1]
(**25.22.**5.254) < (**25.22.**5.5) [PC5]

IntheEthernetframeofthepacket,thesourceMACaddresswouldbe the MAC address of the network interface of the sender PC, and the destination MAC address would be the MAC address of the network interface of the next hop

Task 3. IP Address Lookup

When you ask "what is my IP address?", the website or service providing the answer will usually display the public IP address assigned to your network by your Internet Service Provider (ISP). This IP address is unique to your network and is used to identify your location on the internet.

The accuracy of the identified location will vary depending on the method used to determine the location. Some services may use your IP address to estimate your general geographic location, while others may use more sophisticated methods such as GPS, Wi-Fi triangulation, or cell tower location data.

When you try this from different networks, such as on-campus and home, or via home internet and mobile phone, the identified IP address and location will likely be different. This is because each network has a different public IP address assigned to it by the ISP. The location accuracy may also vary based on the methods used to determine the location and the availability of location data.

In general, the IP address itself does not reveal personal information about you, such as your name or physical address. However, it can be used to identify your ISP and general location. It is important to be cautious when sharing your IP address online, especially if you are accessing sensitive information or using public Wi-Fi networks.

Task 4. IP Addresses, VPNs and Contract Cheating

a) Reasons for bypassing geolocation services with a VPN include accessing geo-restricted content, maintaining online privacy and security, and bypassing censorship. However, there are also reasons against using a VPN to bypass geolocation, such as potentially breaking the terms of service for certain websites or services, and potentially committing illegal acts if the VPN is used for illegal activities.

b) Reasons for a university using IP addresses to identify possible contract cheating include detecting potential academic misconduct and maintaining academic integrity. However, there are also potential downsides, such as false positives (where a student may have legitimately submitted an assessment from a different location) and the possibility of discriminating against international students.

c) My advice to future students would be to use a VPN with caution and to make sure to read the terms of service for any websites or services they are accessing. If a VPN is used to bypass geolocation, it is important to understand the potential risks and to use it responsibly.

Additionally, students should make sure to follow their university's policies and guidelines regarding academic integrity and assessment submission.

Overall, the use of VPNs and IP addresses in relation to geolocation and academic integrity raise important social and ethical issues related to privacy, security, and fairness. It is important to weigh the potential benefits and risks of using these technologies and to use them responsibly and in accordance with relevant laws and regulations.

Week 5

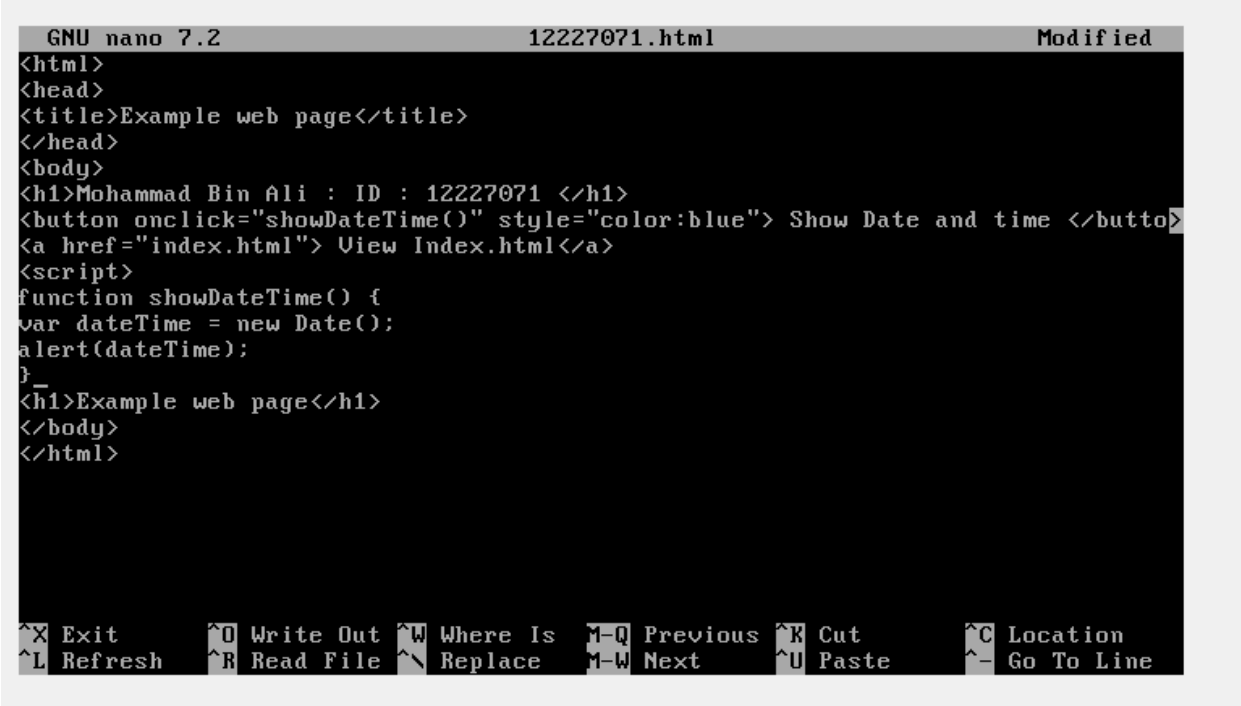
Task 1. Create Web Pages in OpenWRT

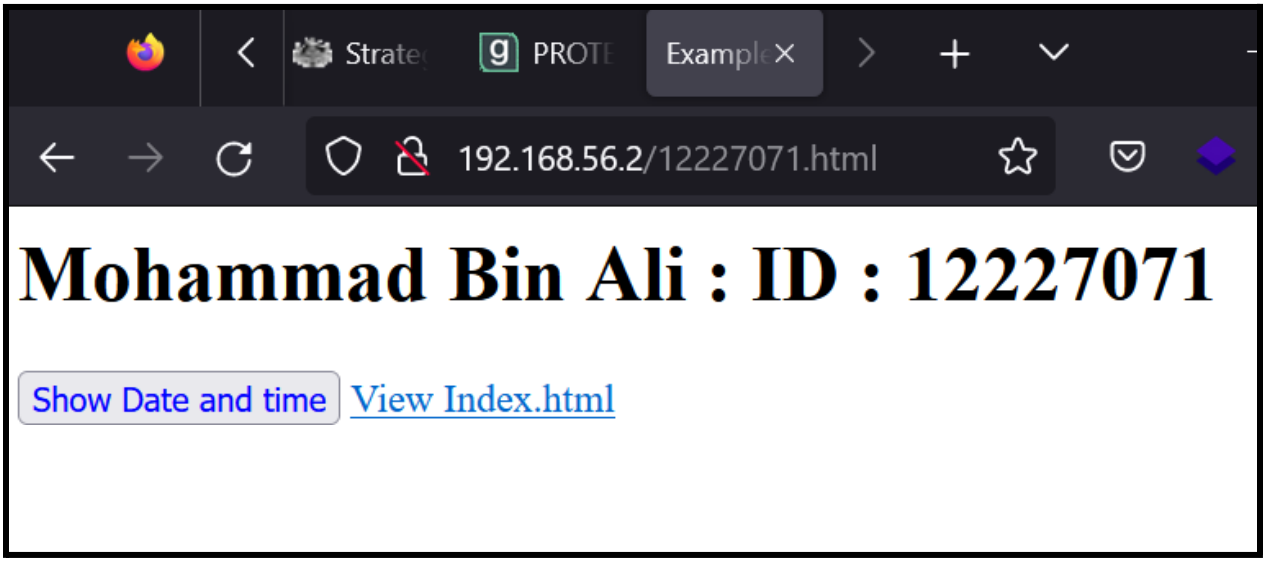
a) Copy the index.html file to a new HTML file named by your student ID, e.g., 12345678.html.

b) Add a link in index.html to the new HTML file.

c) Edit the new file to include your details (e.g., name, ID), to display the date/time when a button is clicked, and to use a new CSS file

d) Create and edit the CSS file to change the color of some text.





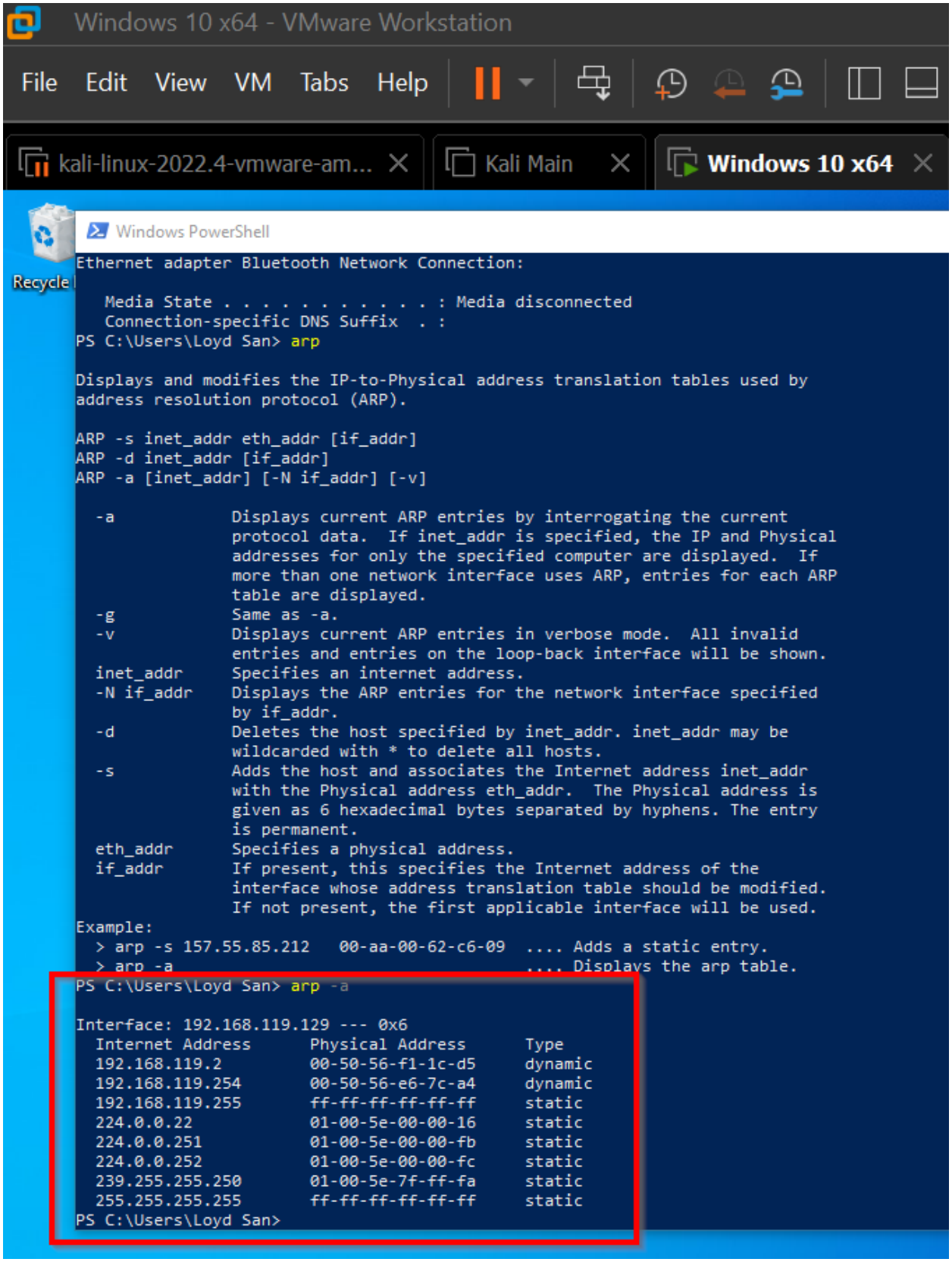

```
<!DOCTYPEhtml>
<html>
<head>
        <title>MyPage</title>
</head>
<body>
        <h1>MohammadBinAliID:12227071</h1>

        <buttononclick="showDateTime()"style="color:blue">ShowdateandTime</button>
        <ahref="index.html">Viewindex.html</a>

        <script>
                functionshowDateTime(){
                        vardateTime=newDate();aler
                        t(dateTime);
                }
         </script>
</body>
</html>
```

Html Code:

Task 2. Capture HTTP Packets

```
<button onclick="showDateTime()" style="color:blue"> Show Date and time </butto>
<a href="index.html"> View Index.html</a>
<script>
function showDateTime() {
var dateTime = new Date();
alert(dateTime);
}
<h1>Example web page</h1>
</body>
</html>



root@OpenWrt:/srv/www# tcpdump -i eth0 -n -w http-12227071.pcap 'not tcp port 22
'
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 byt
^C47 packets captured
47 packets received by filter
0 packets dropped by kernel
root@OpenWrt:/srv/www# _
```

```
root@OpenWrt:/srv/www# ls
12227071.html       http-12227071.pcap  index.html
root@OpenWrt:/srv/www# _
```


Windows 10 x64 - VMware Workstation
File Edit View VM Tabs Help
kali-linux-2022.4-vmware-am...
Kali Main
Windows 10 x64
Recycle
Windows PowerShell
Ethernet adapter Bluetooth Network Connection:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
PS C:\Users\Loyd San> arp
Displays and modifies the IP-to-Physical address translation tables used by
address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]
-a Displays current ARP entries by interrogating the current
protocol data. If inet_addr is specified, the IP and Physical
addresses for only the specified computer are displayed. If
more than one network interface uses ARP, entries for each ARP
table are displayed.
-g Same as -a.
-v Displays current ARP entries in verbose mode. All invalid
entries and entries on the loop-back interface will be shown.
inet_addr Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface specified
by if_addr.
-d Deletes the host specified by inet_addr. inet_addr may be
wildcarded with * to delete all hosts.
-s Adds the host and associates the Internet address inet_addr
with the Physical address eth_addr. The Physical address is
given as 6 hexadecimal bytes separated by hyphens. The entry
is permanent.
eth_addr Specifies a physical address.
if_addr If present, this specifies the Internet address of the
interface whose address translation table should be modified.
If not present, the first applicable interface will be used.
Example:
> arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a .... Displays the arp table.
PS C:\Users\Loyd San> arp -a
Interface: 192.168.119.129 --- 0x6
Internet Address Physical Address Type
192.168.119.2 00-50-56-f1-1c-d5 dynamic
192.168.119.254 00-50-56-e6-7c-a4 dynamic
192.168.119.255 ff-ff-ff-ff-ff-ff static
224.0.0.22 01-00-5e-00-00-16 static
224.0.0.251 01-00-5e-00-00-fb static
224.0.0.252 01-00-5e-00-00-fc static
239.255.255.250 01-00-5e-7f-ff-fa static
255.255.255.255 ff-ff-ff-ff-ff-ff static
PS C:\Users\Loyd San>

Task 3 Analyze HTTP Packet Capture

a)For each HTTP request/response, provide a short explanation of: what triggered the request, what was requested and what was the response. For example: “The user clicked on the link … which caused the browser to send a HTTP Request for /page.html. The server did not have that page so responded with … “.

Ans. Everytime we request some content on the web browser, it is sent via http - GET Method. Simple searching for the url, triggered the request. Entering the URL in the browser,i.e ip of our OPENWRT Machine, asks the server to serve the file requested, index.html is by default.

b) For the first HTTP request/response, list the five (5) address values that identify the host, transport protocol and application.

Host: This is the domain name or IP address of her web server to send requests to. Identifies the target host for the request.

Protocol: This specifies the transport protocol used for requests/responses. For HTTP, the protocol is usually "HTTP/1.1" or "HTTP/2".

Port: This identifies the port number used for requests/responses. For HTTP, the default port is 80 for unencrypted requests and 443 for encrypted requests (using HTTPS).

Method: It specifies the HTTP method used for the request. B. GET, POST, PUT, DELETE, etc. A method specifies the type of action the client wishes to perform on the server.

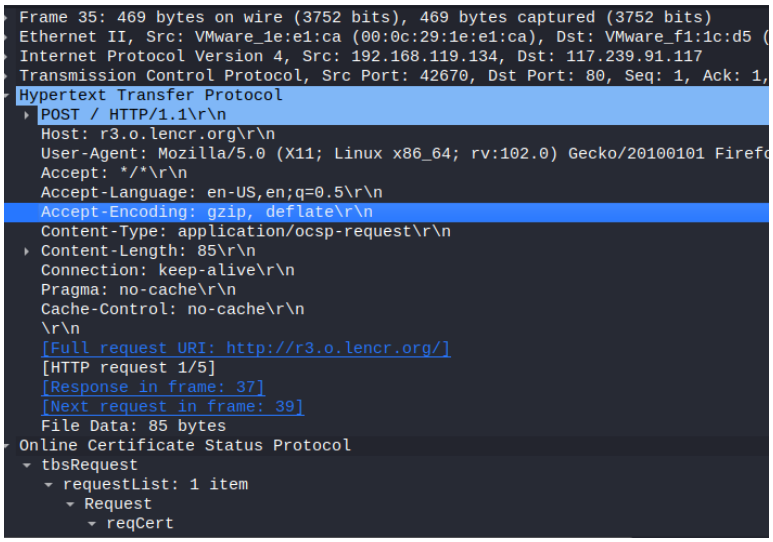
User agent: This identifies the application making the request. It usually contains information about the web browser or other client software being used. B. Version number and operating system.

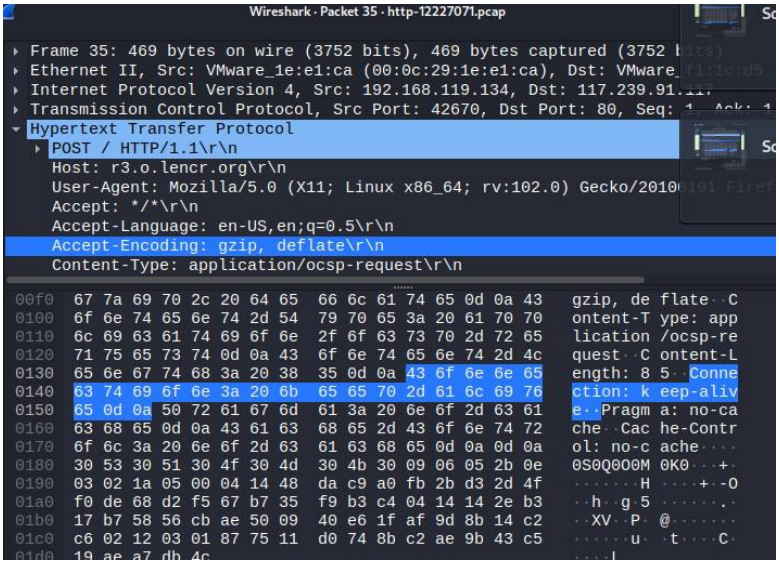
c) When you clicked on the button to show the date and time, did your browser send a request to the web server? Why or why not?

No, the browser does not send a request to the web server to display the date and time when the button is clicked. This is because the date and time display functionality is implemented using client-side scripting, specifically JavaScript executed by the client-side browser. This script gets the current date and time from the user's device and manipulates an HTML document to display the date and time. Requests are therefore handled entirely on the client side and do not require communication with the web server.

d) One of the HTTP request/responses was for your newly created web page (e.g., 12345678.html). Draw a packet diagram for the request, and include the following information: - Size, in Bytes, of each header and of the entire HTTP request

- Addresses included in each header and/or HTTP request





e) For the HTTP request from part (d), what is the value of the referrer? What does it identify? How can web servers use this information?

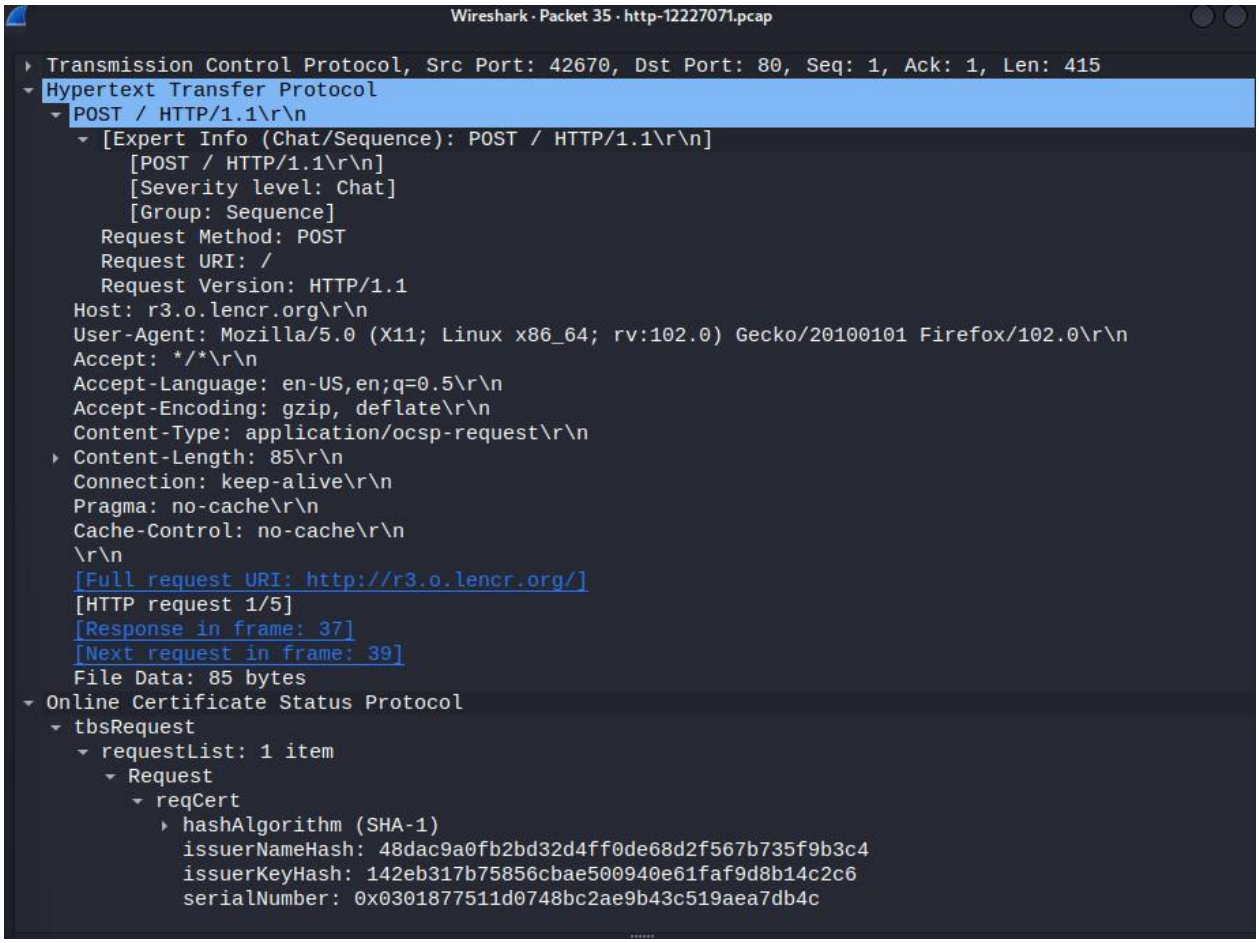
A "referrer" is an HTTP header that specifies the URL of the web page the user was visiting before clicking a link or submitting a form to get to the current page. It is also sometimes spelled

"Referer" (without the second "r"), a misspelling introduced into the HTTP specification for historical reasons.

A referrer can identify which page a user came from and provide useful information to the web server and her web application. For example, it can be used to track the effectiveness of advertising campaigns, see which search engines and other websites are sending traffic to a particular website. It can also be used to implement security measures. B. To prevent cross-site request forgery (CSRF) attacks.

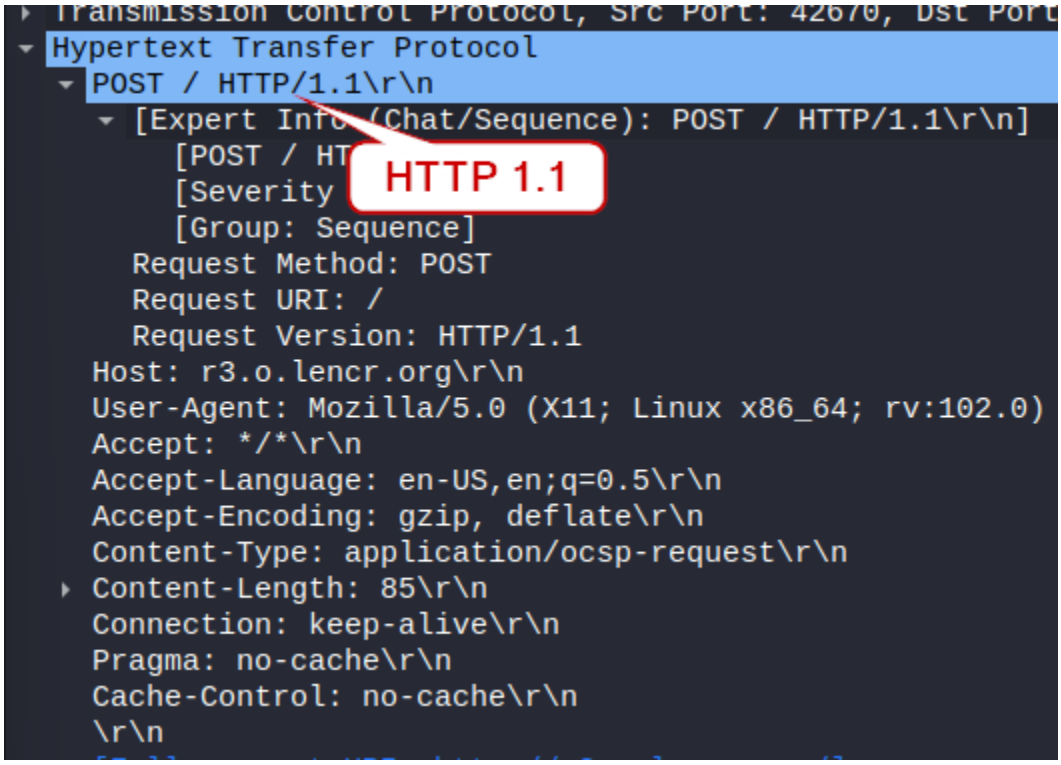
Web servers can use referrer information in a variety of ways, depending on their particular needs and configuration. For example, referrers can be used by web analytics tools to track the source of website traffic, and e-commerce sites can use them to track the effectiveness of their marketing campaigns. Some web servers and web applications use referrer information for access control or other purposes by verifying that requests are from a trusted source (such as the same domain or subdomain as the current page). implement security measures.

f) For the HTTP request from part (d), what information did the server learn about the web browser (e.g., name, version)?



g) What version of HTTP is used and what transport protocol is used?

HTTP 1.1



h) A connection-oriented service involves setting up a connection before any data transfer, as well as acknowledgements that are used to provide reliability. Identify the packets involved in connection setup (e.g., the packet numbers). How long did it take between the start of connection setup and the data transfer starting?

Sync: The initiating device sends a SYN packet to the receiving device requesting connection establishment. This packet has a sequence number (SYN sequence number) and a randomly generated initial sequence number (ISN).

Sync confirmation: The receiving device acknowledges the connection establishment request by responding with a SYN-ACK packet. This packet contains a SYN sequence number and an acknowledgment number (ACK number) that is the SYN sequence number + 1. The package also contains a randomly generated ISN. confirmation:

The initiating device sends her ACK packet, acknowledging receipt of the SYN-ACK packet. This packet contains her ACK number which is her ISN + 1 on the receiving device.

Data transfer can begin as soon as a connection is established.

i) Identify the acknowledgements. When is an acknowledgement typically sent?

In connection-oriented protocols like TCP, the receiving device sends an acknowledgment (ACK) to confirm that it has received and successfully processed the data packet sent by the sending device.An acknowledgment is usually sent after one device receives a data packet from the other device. The acknowledgment contains the next sequence number that the receiving device expects to receive from the sending device. The sending device then uses this information to determine if packets that were not received by the receiving device should be resent.

The ACK packet has a sequence number that corresponds to the next expected sequence number of the data from the other side.

Task 4 View Your Cookies

Cookies are small text files that are stored on a user's device by a website when they visit it. They are commonly used to store information such as login details, user preferences, and shopping cart contents. Cookies can also store information about the user's browsing behavior, such as which pages they have visited or how long they spent on a particular website.

Cookies can be categorized based on their lifespan and the domain that they belong to. Session cookies are temporary cookies that are erased when the user closes their web browser. Persistent cookies, on the other hand, remain on the user's device until they expire or are manually deleted by the user.

First-party cookies are created by the website that the user is visiting, while third-party cookies are created by a domain other than the one that the user is currently visiting. Third-party cookies are often used for advertising and tracking purposes, which can potentially compromise the user's privacy.

Week 6

 # Task 1. View Wi-Fi Details

In your journal include a screenshot of details of at least one AP, as well as list of information you found.

SSID: Thinkware_7A

BSSID: 04:32:F4:69:5B:7A

First Time: 2022-09-08T21:00:00.000Z

Last Time: 2023-03-15T19:00:00.000Z

Channel: 6

Encryption: wpa2

Quality of Signal:

2

SSID: HUAWEI-E5730-

90C9 BSSID:

38:F8:89:4D:90:C9

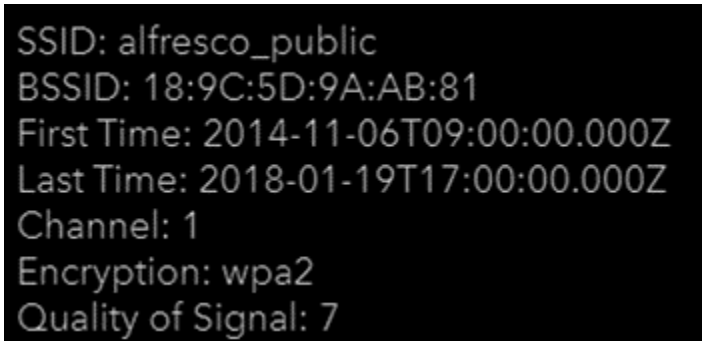
First Time: 2016-11-14T13:00:00.000Z

Last Time: 2016-11-16T23:00:00.000Z

Channel: 11

Encryption: wpa2

Quality of Signal:



0

 # Task 2. Use Wi-Fi Access Point

What are the important settings that you should consider when designing a Wi-Fi network? (Do not simply list all settings; rather select some important settings and discuss what you would consider changing them to and why).

SECURITY	
WiFi Encryption	WPA WPA2 WPA3 WPA/WPA2-Enterprise (802.1x)
Network Security	SPI Firewall Access Control IP & MAC Binding Application Layer Gateway
Guest Network	1× 5 GHz Guest Network 1× 2.4 GHz Guest Network

Quality of Service	QoS by Device
Cloud Service	OTA Firmware Upgrade TP-Link ID DDNS
NAT Forwarding	Port Forwarding Port Triggering DMZ UPnP
IPTV	IGMP Proxy IGMP Snooping Bridge Tag VLAN
DHCP	Address Reservation DHCP Client List Server
DDNS	TP-Link NO-IP DynDNS

SSID (Service Set Identifier): This is the name of your Wi-Fi network, and it's important to choose a unique and easy-to-remember name that is not shared with neighbouring networks. It's also recommended to disable SSID broadcasting, which makes the network invisible to devices that are not configured to connect to it.

Security: It's crucial to set up appropriate security measures to protect your network from unauthorized access. This can be done by enabling WPA2 encryption and using a strong password. You can also restrict access to specific devices by enabling MAC address filtering.

Channel and frequency: Wi-Fi operates on different channels and frequencies, and it's important to choose the best channel and frequency that minimizes interference from other nearby networks. You can use tools like Wi-Fi Analyzer to determine the least congested channel and frequency.

Quality of Service (QoS): QoS settings prioritize traffic on your network, which can improve the performance of specific applications or devices. You can assign priority levels to different applications or devices based on their bandwidth requirements.

Guest network: If you have guests who need Wi-Fi access, it's a good idea to set up a separate guest network that is isolated from your main network. This can be done by configuring a separate SSID with its own security settings.

When configuring these settings, it's important to strike a balance between security, performance, and usability.

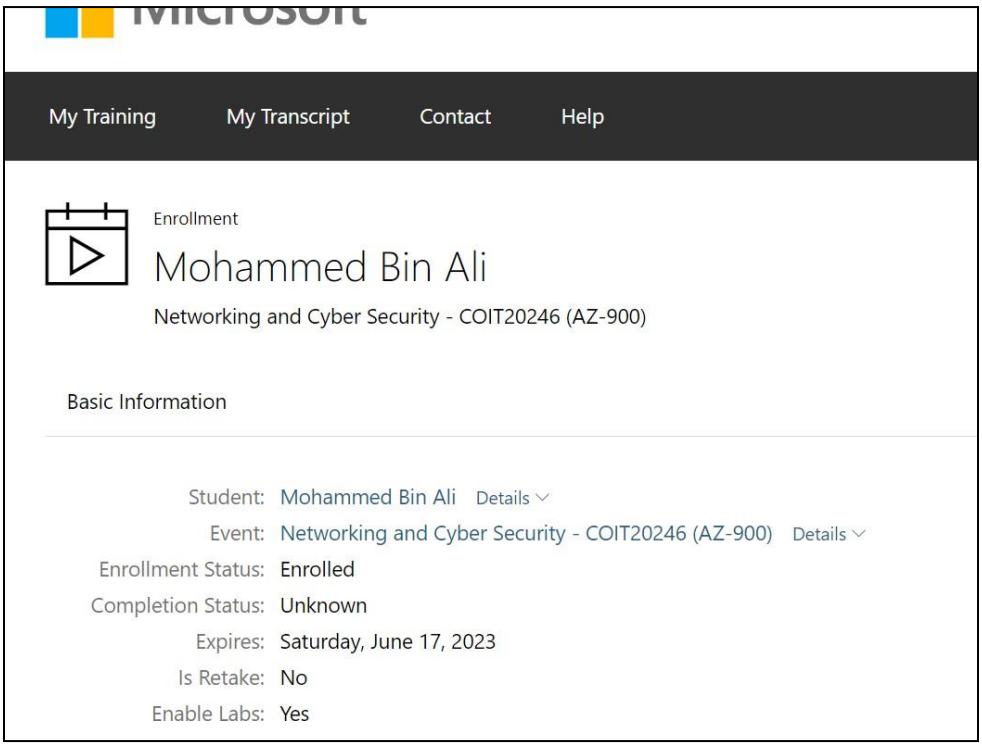
 # Task 3. Continue Your Project

Week 7

Task 1 Login to Microsoft Learn on Demand

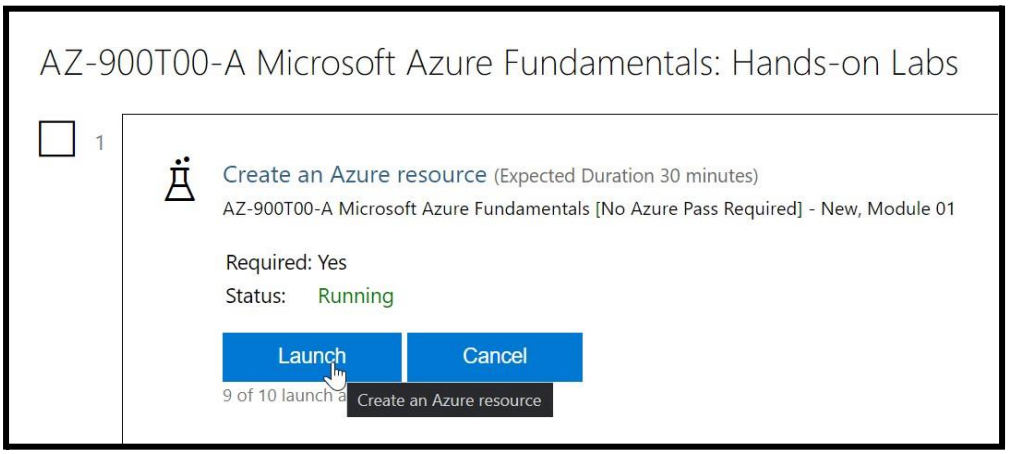
Creating an account on https://msle.learnondemand.net/ with a Skillable account, with Registration Key, on Moodle.

After Successful, registration, we are able to Launch modules for each lab,

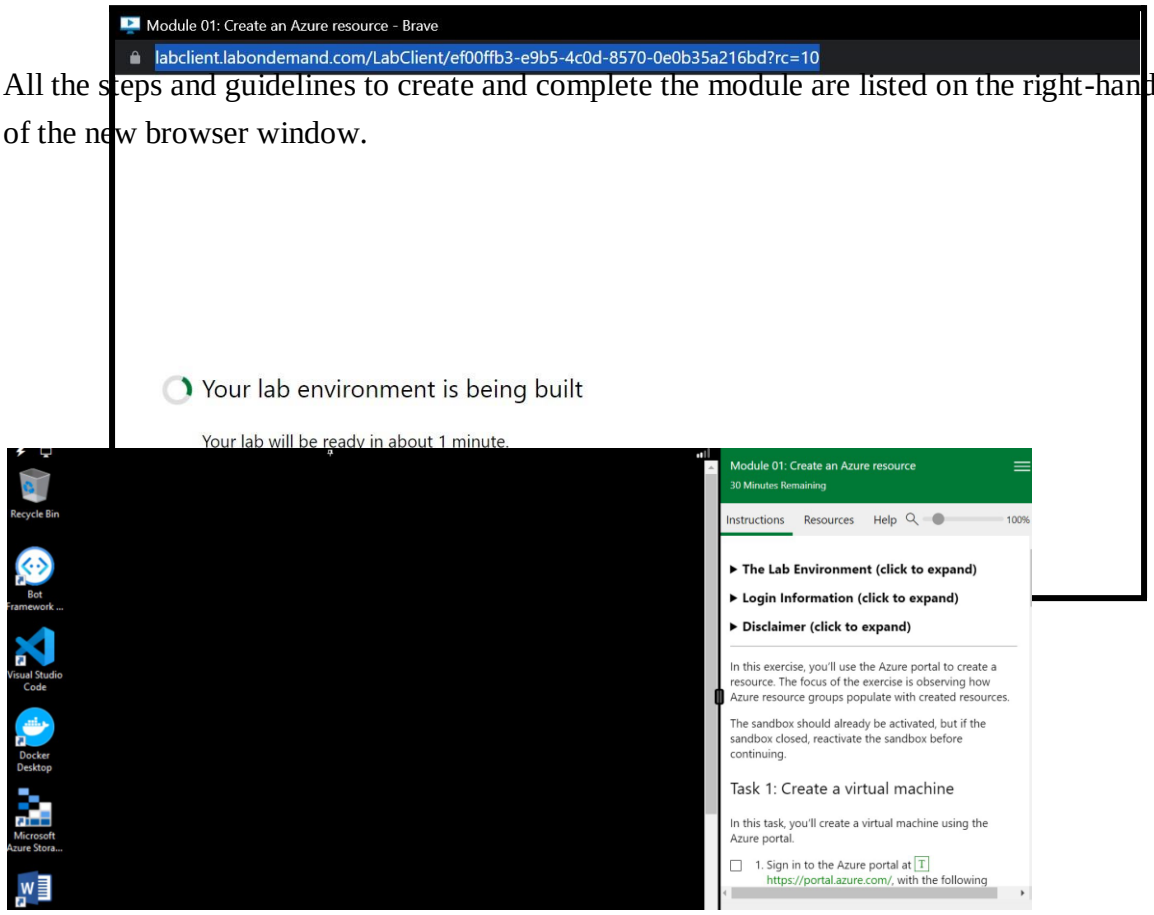


##Task 2 Creating an Azure Resource

Opening the lab by clicking on Launch Button.

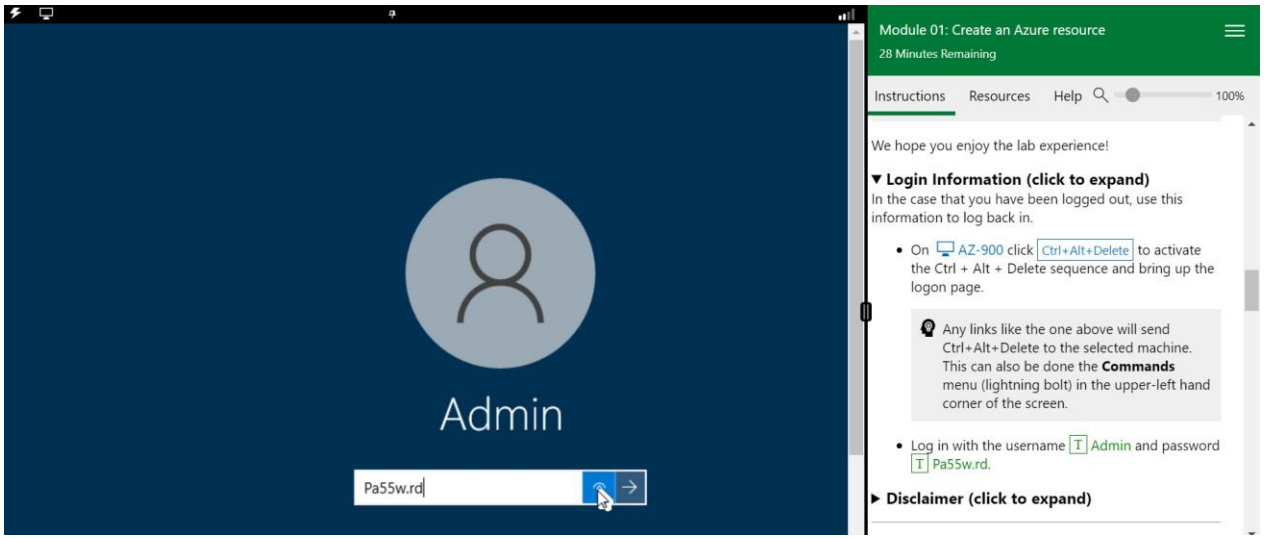


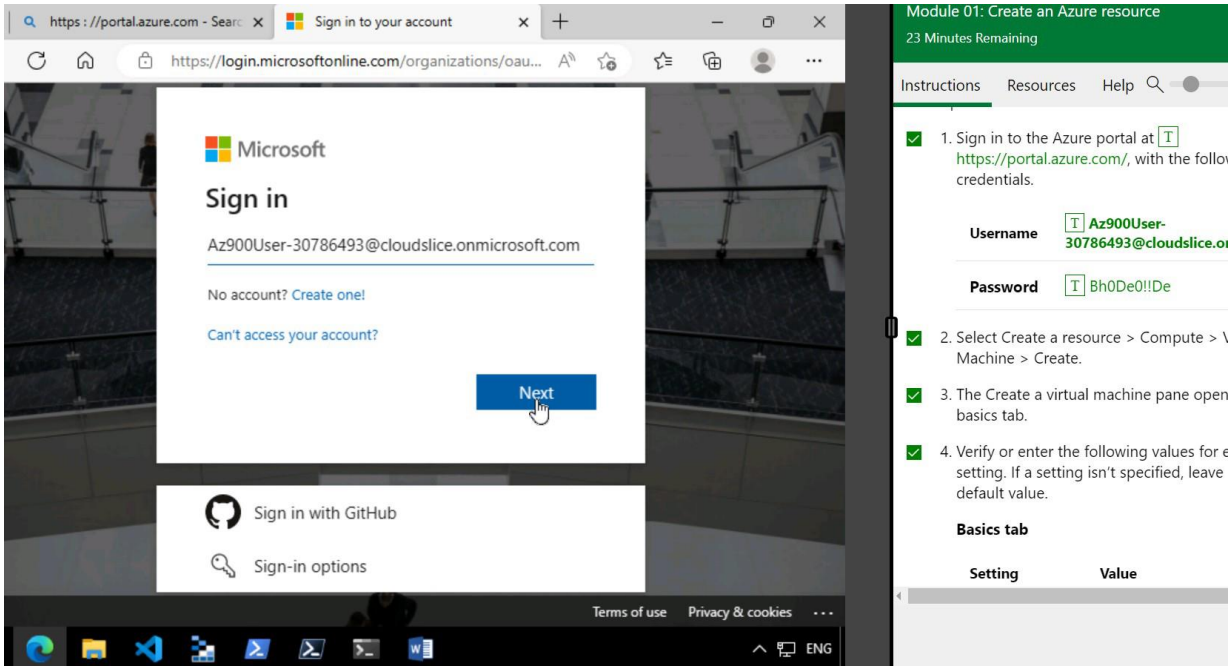
The lab opens up a new browser window, it is a cloud based Virtual Machine (Windows VM).

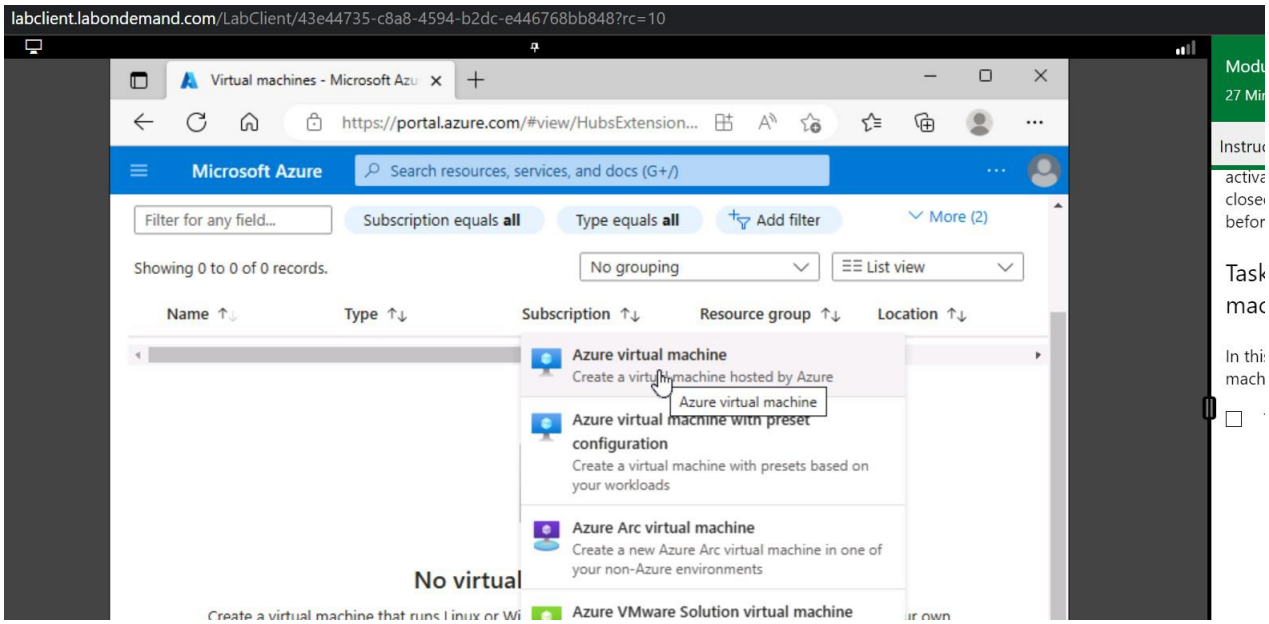


All the steps and guidelines to create and complete the module are listed on the right-hand-side of the new browser window.

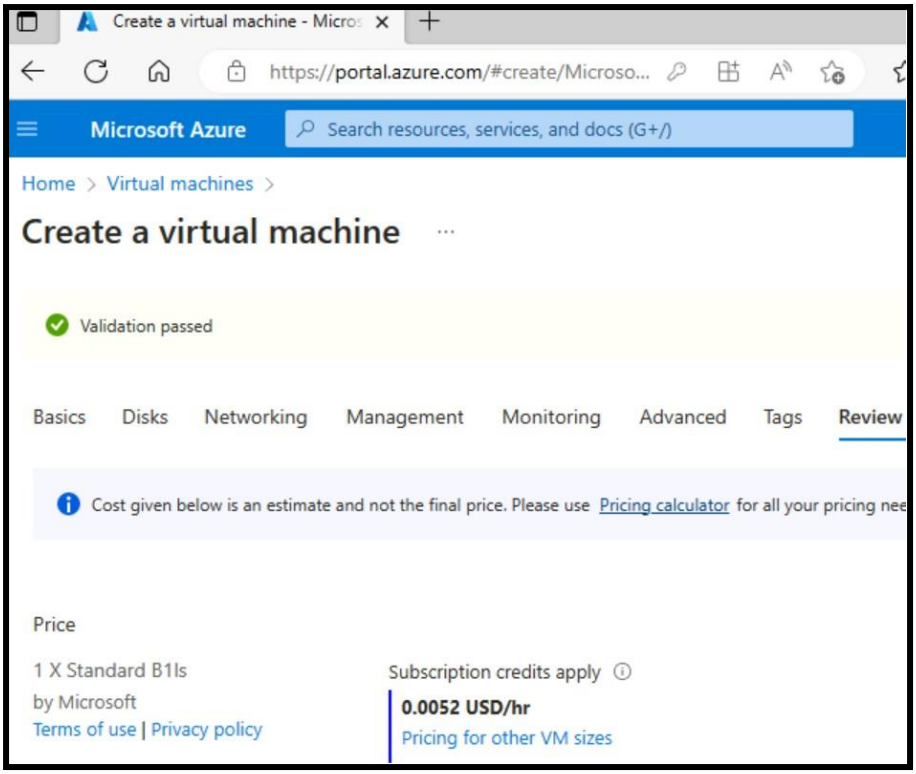
Here are the screen captures following each step taken to proceed with the Module.

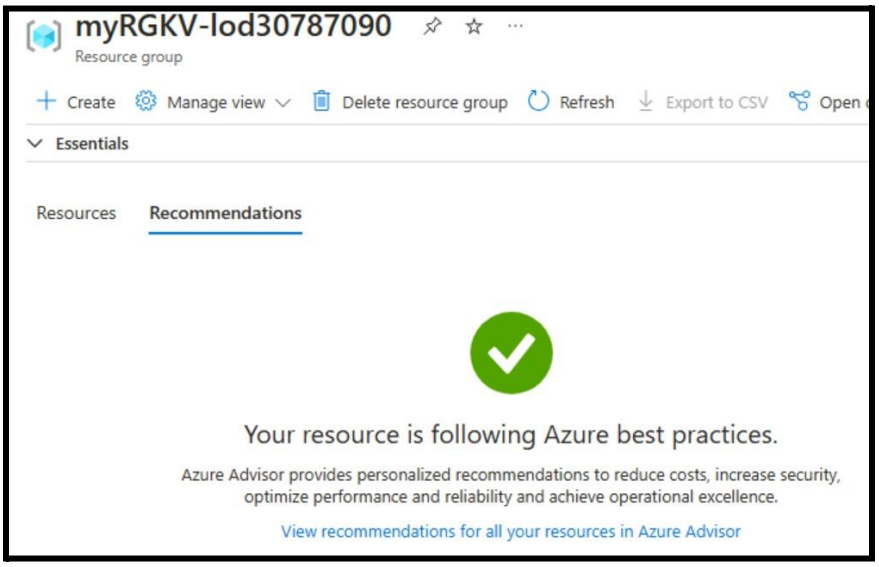

Admin
Pa55w.rd
Module 01: Create an Azure resource
28 Minutes Remaining
Instructions
Resources
Help
100%
We hope you enjoy the lab experience!
Login Information (click to expand)
In the case that you have been logged out, use this information to log back in.
On AZ-900 click Ctrl+Alt+Delete to activate the Ctrl + Alt + Delete sequence and bring up the logon page.
Any links like the one above will send Ctrl+Alt+Delete to the selected machine. This can also be done the Commands menu (lightning bolt) in the upper-left hand corner of the screen.
Log in with the username Admin and password Pa55w.rd.
Disclaimer (click to expand)


Sign in to your account
https://login.microsoftonline.com/organizations/oau...
Microsoft
Sign in
Az900User-30786493@cloudslice.onmicrosoft.com
No account? Create one!
Can't access your account?
Next
Sign in with GitHub
Sign-in options
Terms of use
Privacy & cookies
ENG
Module 01: Create an Azure resource
23 Minutes Remaining
Instructions
Resources
Help
1. Sign in to the Azure portal at https://portal.azure.com/, with the follo credentials.
Username
Az900User-30786493@cloudslice.o
Password
Bh0De0!!De
2. Select Create a resource > Compute > \ Machine > Create.
3. The Create a virtual machine pane open basics tab.
4. Verify or enter the following values for e setting. If a setting isn't specified, leave default value.
Basics tab
Setting
Value



Here is how the final virtual machine was created with all validations passed.





 # List the resources that were created and give a short explanation of what each resource is for.

Virtual machine:

This resource allows you to create VM instances in the cloud. You can choose the operating system, hardware, and memory configuration of your virtual machine.

Virtual network:

This resource allows you to create a virtual network in your cloud. You can use this network to securely connect virtual machines and other cloud resources.

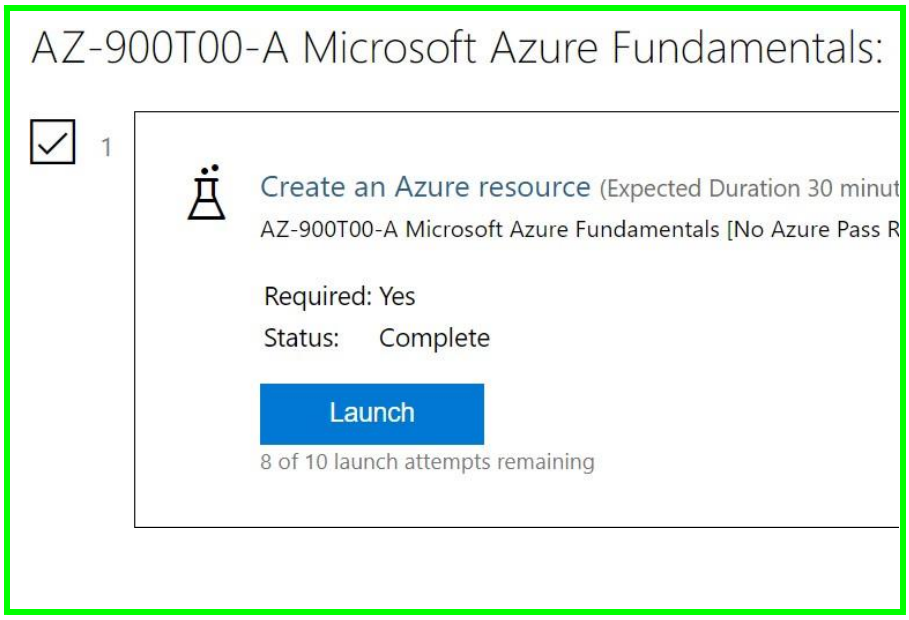
SQL database:

This resource allows you to create a managed relational database in the cloud. You can choose the performance level, memory, and other configuration settings for your database.

Storage account:

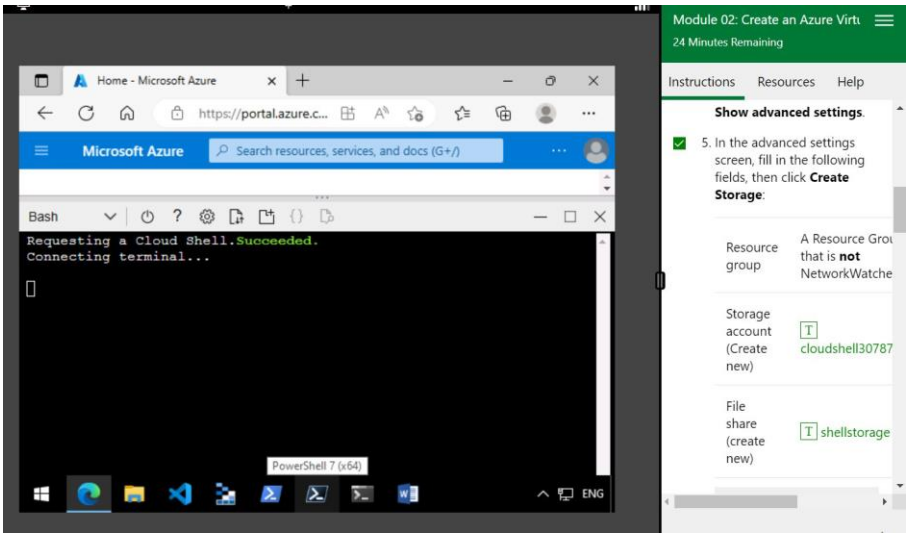
This resource allows you to create a storage account in the cloud. You can use this account to store files, blobs, tables, and queues.

This marks the Lab 1 complete.



Task 3: Create an Azure Virtual Machine.

Starting the lab, after navigating to **cloud cli**, we proceed with the mentioned commands. A screenshot for each and every step has been maintained to show stepwise proceedings.



 # Commands used to Create the Virtual Machine, Nginx , and to edit the index.html page

```
az vm create \
```

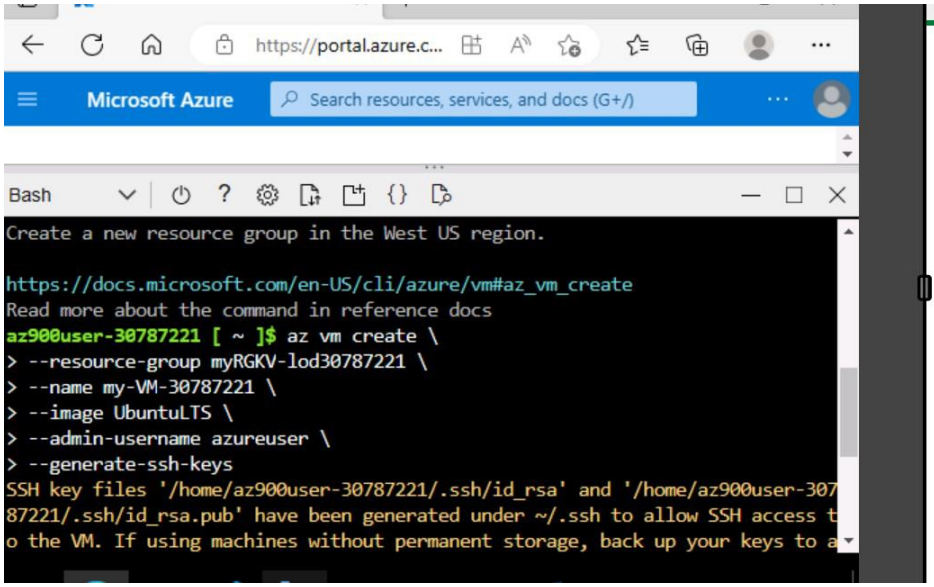
```
--resource-group myRGKV-lod30787221 \
```

--name my-VM-30787221 \

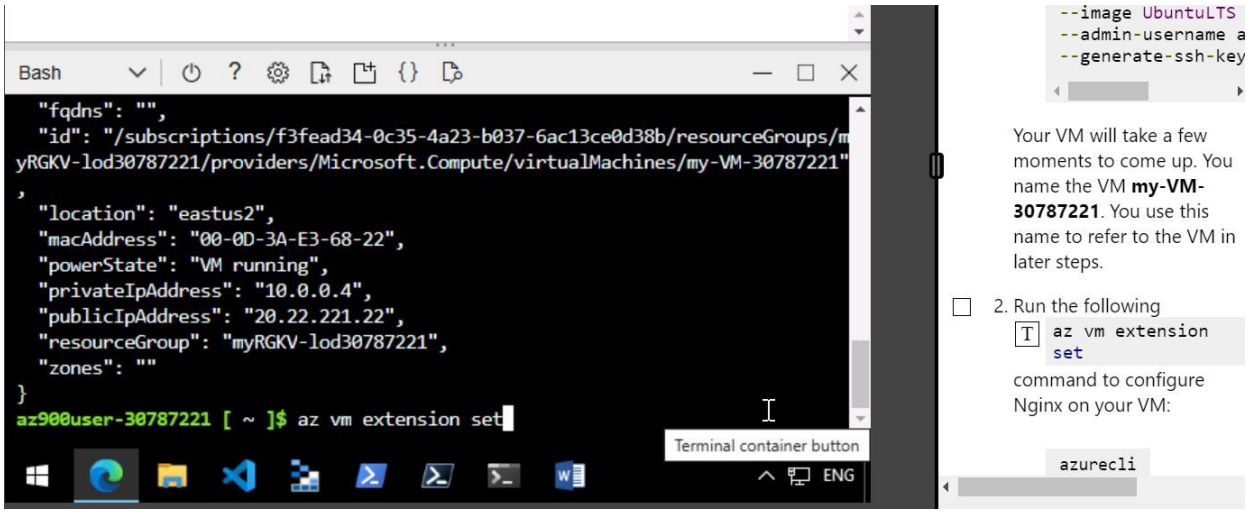
--image UbuntuLTS \

--admin-username azureuser \

--generate-ssh-keys



az vm extension set



az vm extension set \

```
--resource-group myRGKV-lod30787221 \
```

--vm-name my-VM-30787221 \

--name customScript \

--publisher Microsoft.Azure.Extensions \

--version 2.1 \

--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-wel come-to-azure/master/configure-nginx.sh"]}' \

--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

SSH into the VM created:

Ssh -l <username> <ip_address>

#note: for checking the public ip of the created VM, check resource groups, and the name of VM created from the azure cli.

You will get the ip address(public), then proceed with the below mentioned commands.

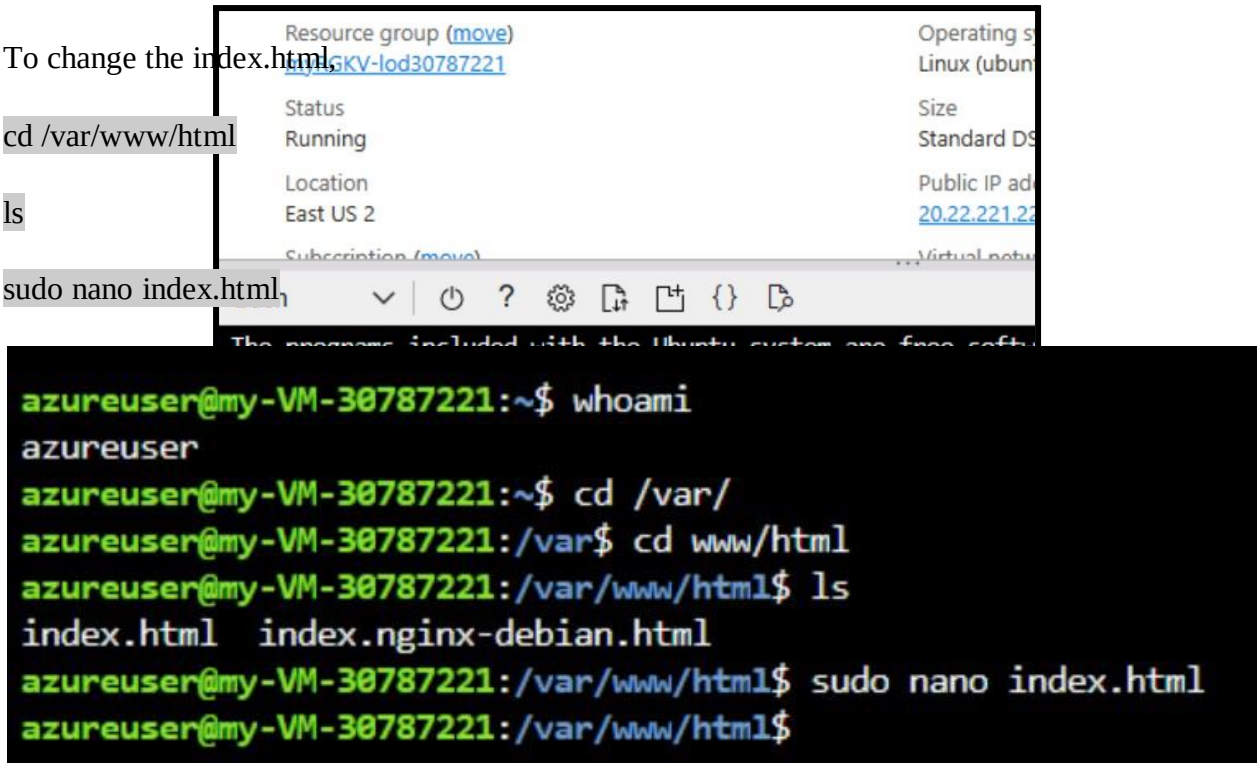
 # Here is the Public Ip Address of The Virtual Machine Created.

ssh -l azureuser 20.22.221.22

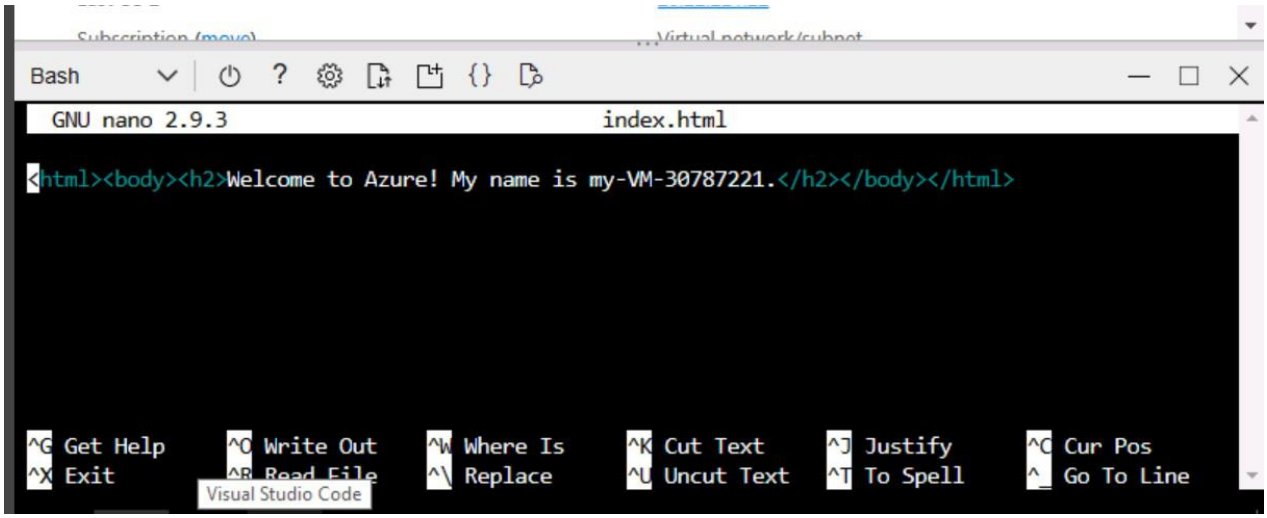
You can check for a successful ssh by typing command **whoami**

To change the index.html,

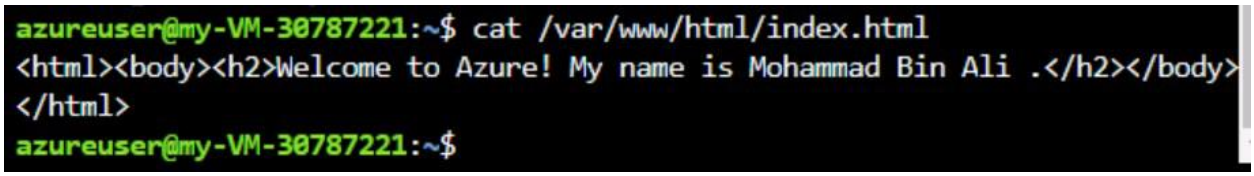
```
cd /var/www/html

ls

sudo nano index.html
```



It will open the file in a text editor: make necessary changes.



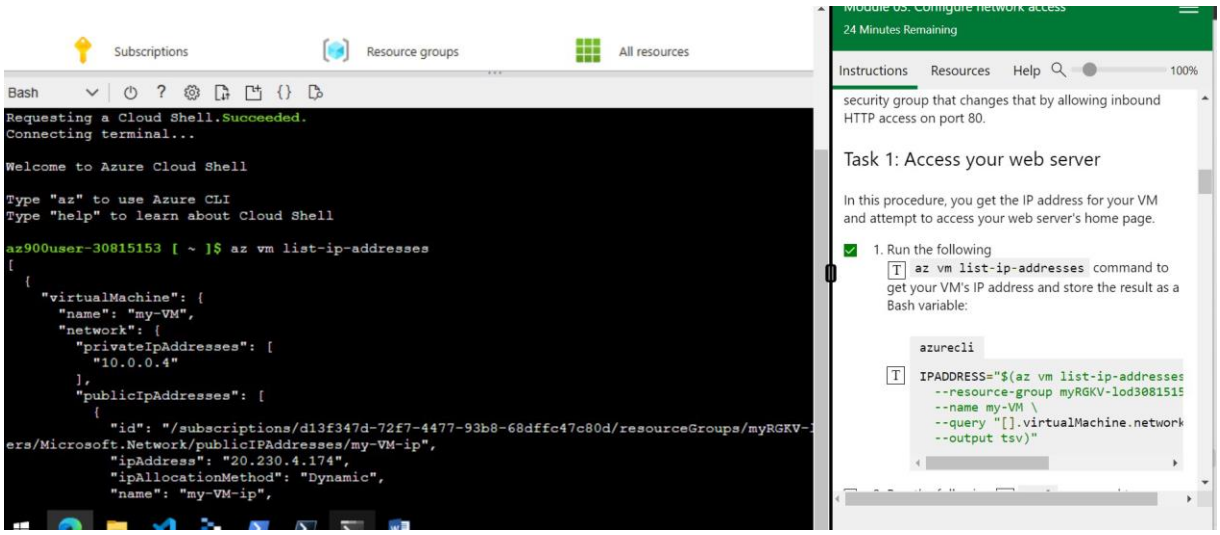
Updated index.html file.



Task 4 Configure Network Access to VM

Module 03: Configure network access

az vm list-ip-addresses command to get your VM's IP address and store the result as a Bash variable:

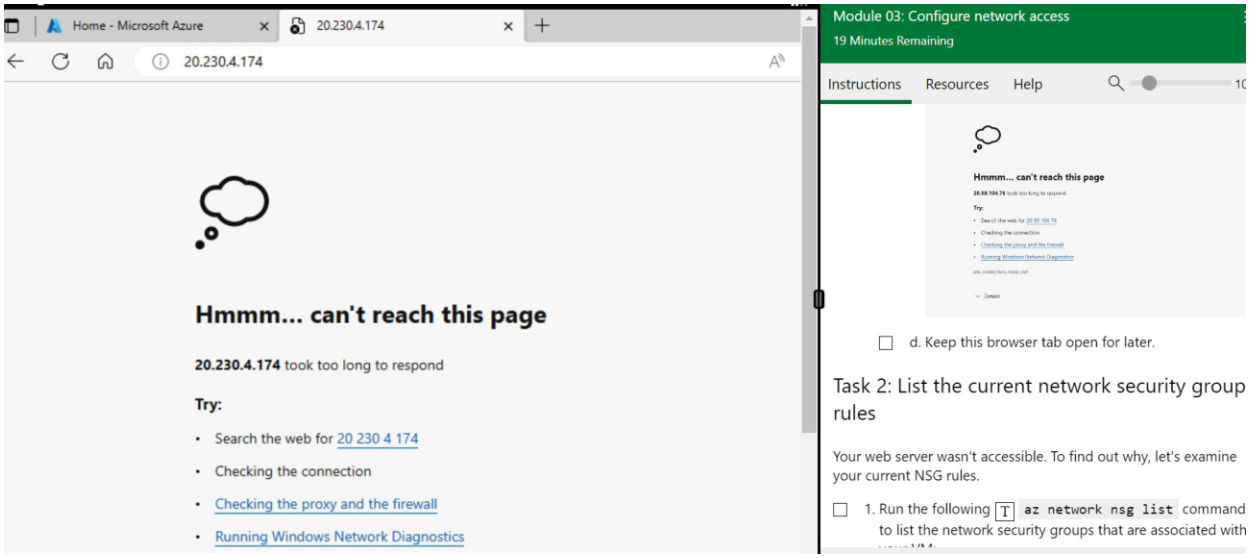


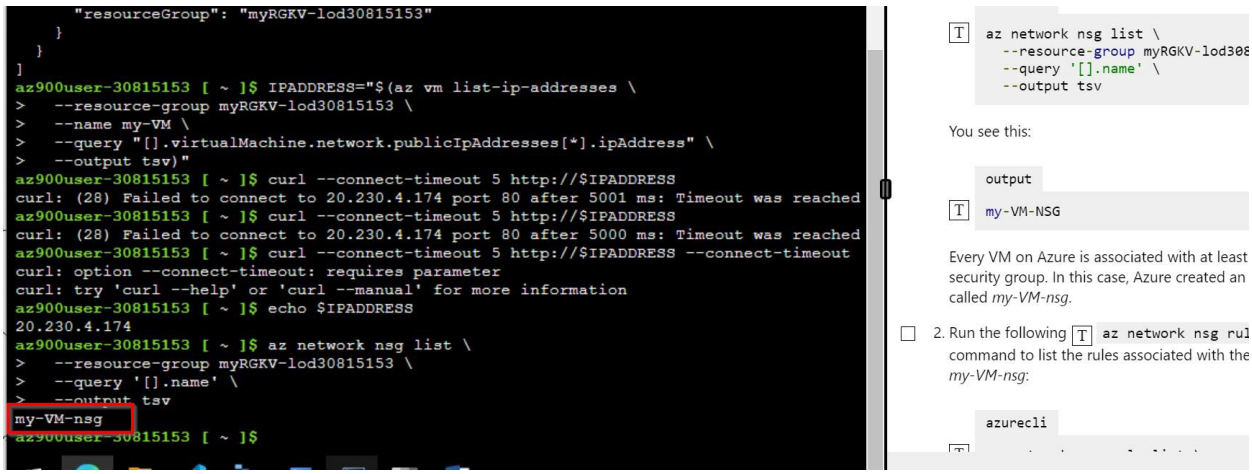
azurecli

```
IPADDRESS="$(az vm list-ip-addresses \
 --resource-group myRGKV-lod30815153 \
 --name my-VM \
 --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
    --output tsv)"
```

Command to download the home page:

```
curl --connect-timeout 5 http://$IPADDRESS
```





 # Commands

```
azurecli
IPADDRESS="$(az vm list-ip-addresses \
  --resource-group myRGKV-lod30815153 \
  --name my-VM \
  --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
      --output tsv)"
bash
     curl --connect-timeout 5 http://$IPADDRESS

     echo $IPADDRESS
azurecli
az network nsg list \
  --resource-group myRGKV-lod30815153 \
  --query '[].name' \
      --output tsv

az network nsg rule list \
  --resource-group myRGKV-lod30815153 \
  --nsg-name my-VM-nsg

az network nsg rule list \
  --resource-group myRGKV-lod30815153 \
  --nsg-name my-VM-nsg

azurecli
az network nsg rule create \
  --resource-group myRGKV-lod30815153 \
  --nsg-name my-VM-nsg \
  --name allow-http \
    --protocol tcp\
    --priority100\
  --destination-port-range 80 \
      --access Allow


azurecli
az network nsg rule list \
  --resource-group myRGKV-lod30815153 \
  --nsg-name my-VM-nsg \
  --query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \
      --output table
```

curl --connect-timeout 5 http://$IPADDRESS

 # Curl Successfully Accessing the website

```
az900user-30815153 [ ~ ]$ curl --connect-timeout 5 http://$IPADDRESS
<html><body><h2>Welcome to Azure! My name is my-VM.</h2></body></html>
```

***Note**:IhadtoredotheLab2formakingchangestotheindex.htmlfiletoshowmyNameonthewebpage. Aftermakingnecessarychanges,bygeneratingsshkeysfothenewVMandbysshingintotheVM,I WAS ABLE TO CHANGE THE NAME*

Explanation:

 # There are two network security rules that allow access to your VM. For each rule, give the port number and explain what that rule allows (e.g., what applications or protocols).

```
az network nsg rule create \
  --resource-group myRGKV-lod30815153 \
  --nsg-name my-VM-nsg \
  --name allow-http \
    --protocol tcp\
    --priority100\
  --destination-port-range 80 \
      --access Allow
```

Here the port 80 is for HTTP protocol, by allowing this port number, we are accepting http requests to our machine. It is allowing incoming HTTP traffic to Our created VM. One can access it using

the VM’s Public Ip and a browser.

To summarize:

Rule 1: Port 22 - This rule allows SSH access to the VM, which allows users to remotely connect to the VM using the SSH protocol. It is a network protocol again, allowing incoming SSH traffic to the VM.

Rule 2: Port 80 - This rule allows HTTP traffic to reach the VM, which is required to serve web pages using Nginx.

 # Advice for a small business on transitioning to cloud services:

Dependence on internet connectivity - Cloud services require reliable and stable internet connectivity to function properly. Any disruptions to internet service can negatively impact the business's ability to use cloud services effectively.

Data security and privacy - Storing sensitive business data on third-party servers can pose security and privacy risks. It's important to carefully consider the cloud provider's security measures and compliance certifications before migrating sensitive data to the cloud.

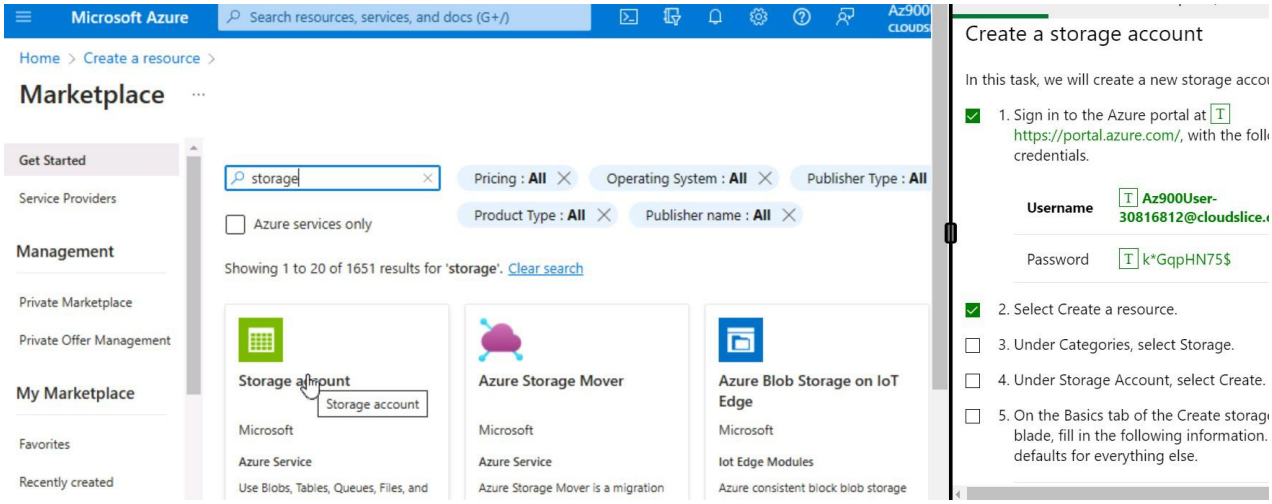
Training and support - Transitioning to cloud services often requires significant changes in workflows and processes. Adequate training and support may be required to ensure that employees can effectively use cloud services and minimize disruptions to business operations.

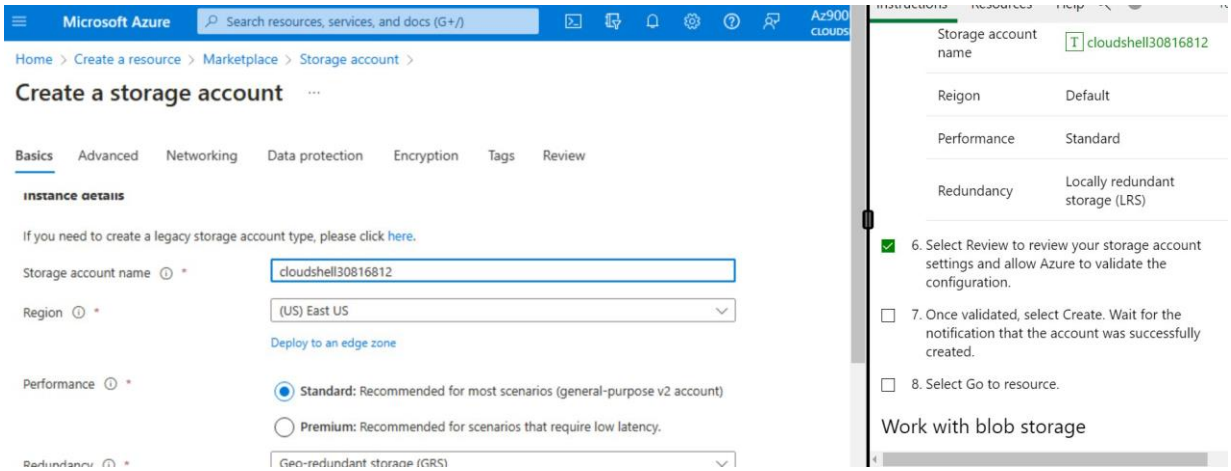
Vendor lock-in - Transitioning to a particular cloud provider can create a dependence on that provider's services and infrastructure. This can make it difficult to switch to a different provider or migrate away from cloud services altogether if necessary.

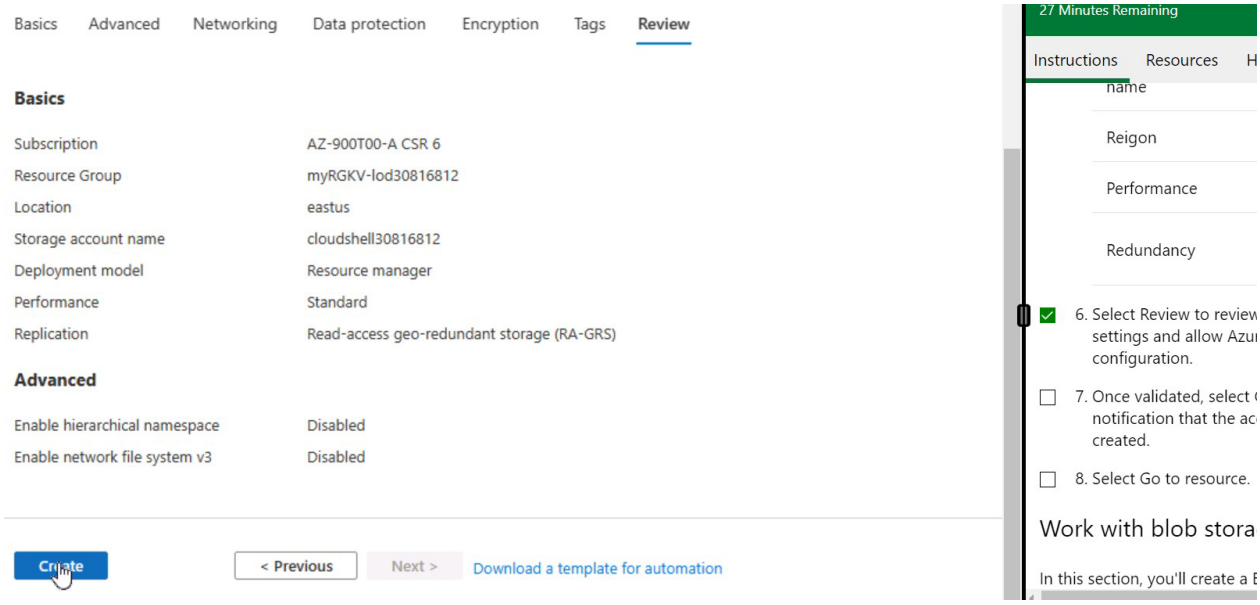
Cost - While cloud services can offer cost savings in some areas, it's important to carefully consider the total cost of ownership, including any additional costs for training, support, and customization. Cloud services may not always be the most cost-effective solution for every business.

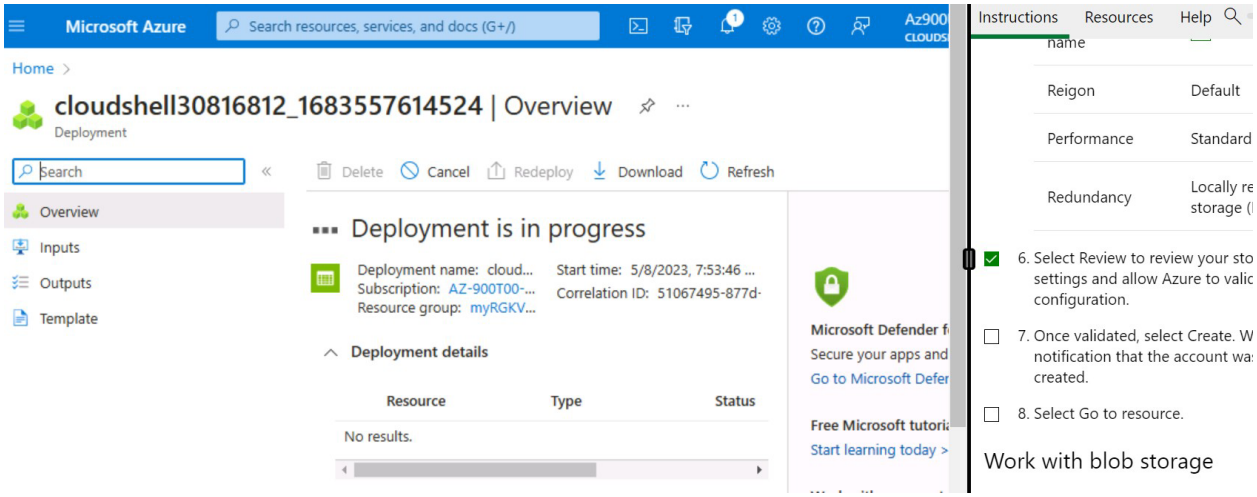
Task 5. Create a Storage Blob in Azure

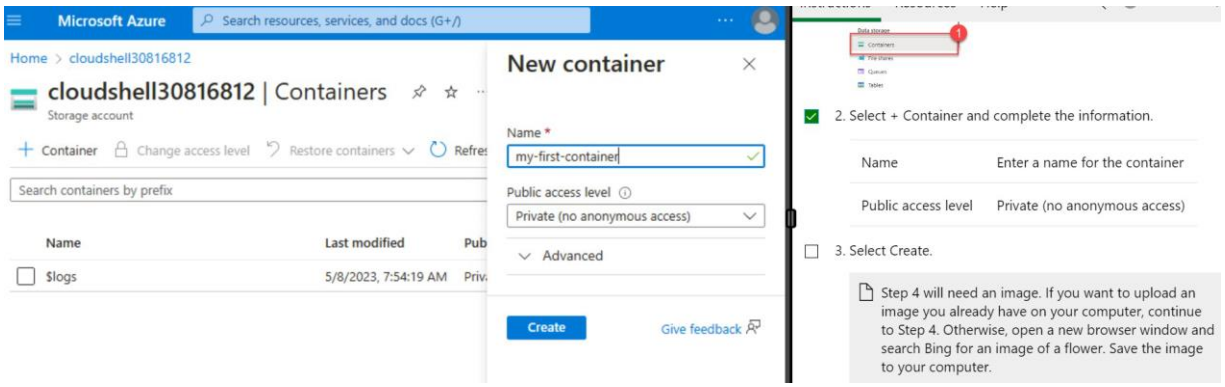
 # Complete Module 04: Create a storage blob. Follow the instructions in Microsoft Learn On Demand

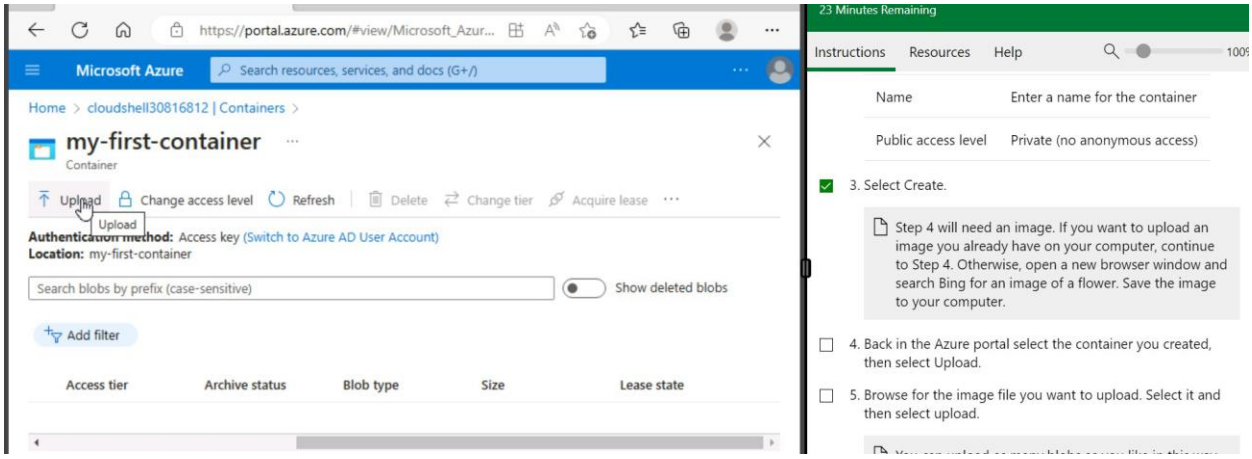

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource >
Marketplace
Get Started
Service Providers
Management
Private Marketplace
Private Offer Management
My Marketplace
Favorites
Recently created
storage
Pricing : All
Operating System : All
Publisher Type : All
Product Type : All
Publisher name : All
Azure services only
Showing 1 to 20 of 1651 results for 'storage'. Clear search
Storage account
Storage account
Microsoft
Azure Service
Use Blobs, Tables, Queues, Files, and
Azure Storage Mover
Microsoft
Azure Service
Azure Storage Mover is a migration
Azure Blob Storage on IoT Edge
Microsoft
Iot Edge Modules
Azure consistent block blob storage
Create a storage account
In this task, we will create a new storage accou
1. Sign in to the Azure portal at https://portal.azure.com/, with the foll credentials.
Username
Az900User-30816812@cloudslice.
Password
k*GqpHN75$
2. Select Create a resource.
3. Under Categories, select Storage.
4. Under Storage Account, select Create.
5. On the Basics tab of the Create storag blade, fill in the following information. defaults for everything else.

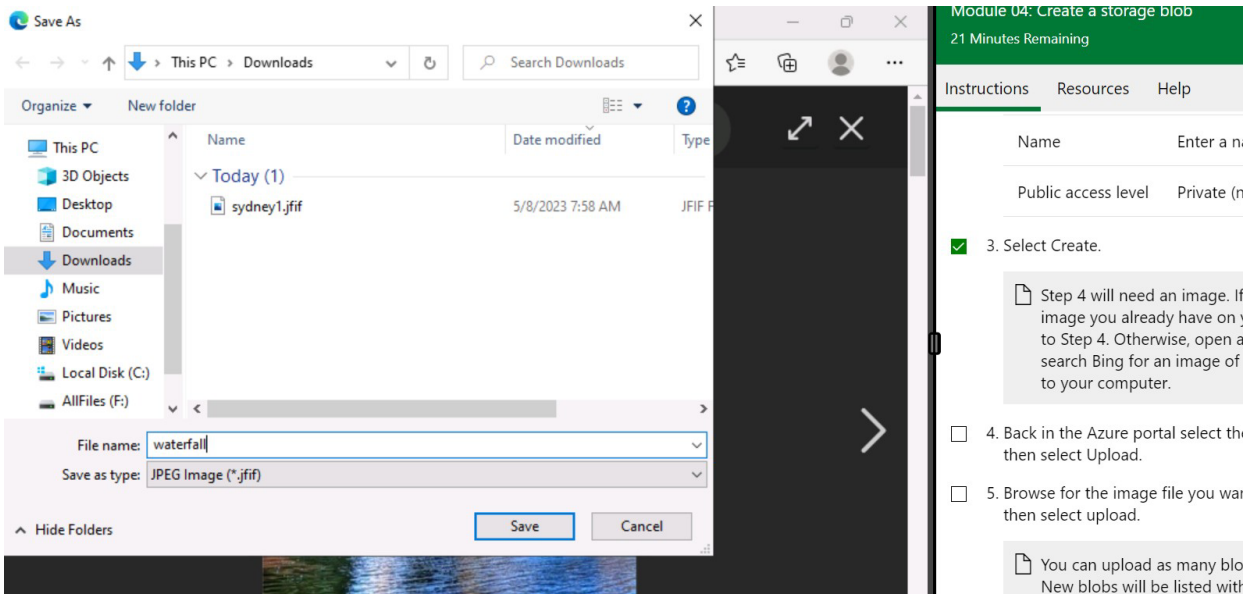

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace > Storage account >
Create a storage account
Basics
Advanced
Networking
Data protection
Encryption
Tags
Review
Instance details
If you need to create a legacy storage account type, please click here.
Storage account name
cloudshell30816812
Region
(US) East US
Deploy to an edge zone
Performance
Standard: Recommended for most scenarios (general-purpose v2 account)
Premium: Recommended for scenarios that require low latency.
Storage account name
cloudshell30816812
Reigon
Default
Performance
Standard
Redundancy
Locally redundant storage (LRS)
6. Select Review to review your storage account settings and allow Azure to validate the configuration.
7. Once validated, select Create. Wait for the notification that the account was successfully created.
8. Select Go to resource.
Work with blob storage

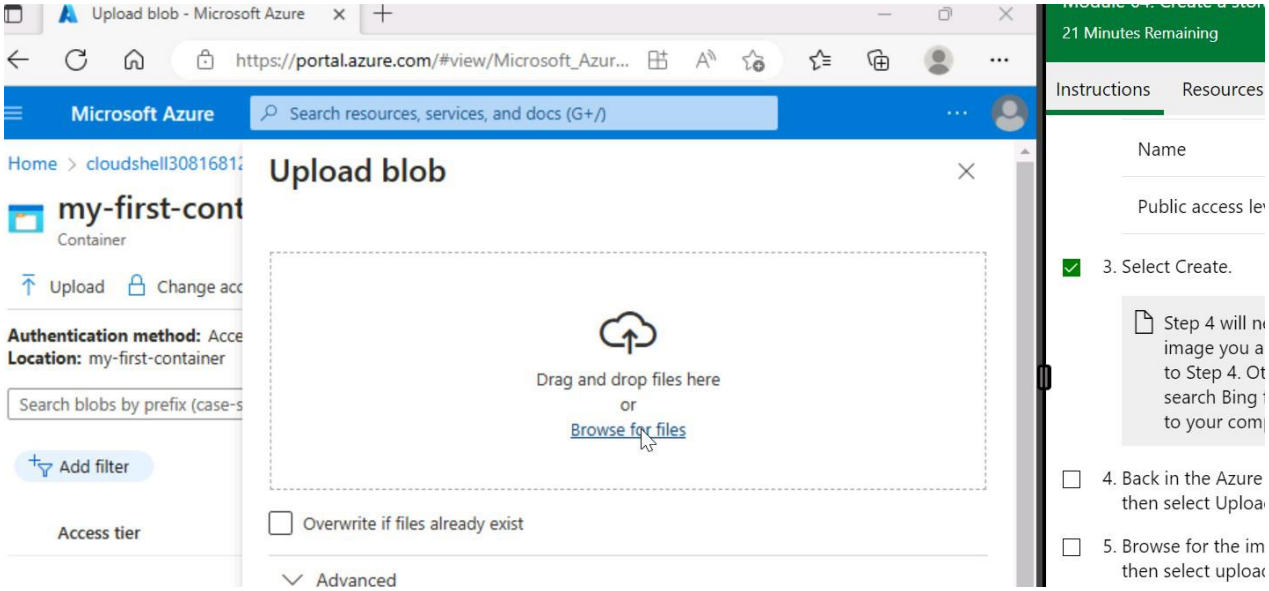

Basics
Advanced
Networking
Data protection
Encryption
Tags
Review
Basics
Subscription
AZ-900T00-A CSR 6
Resource Group
myRGKV-lod30816812
Location
eastus
Storage account name
cloudshell30816812
Deployment model
Resource manager
Performance
Standard
Replication
Read-access geo-redundant storage (RA-GRS)
Advanced
Enable hierarchical namespace
Disabled
Enable network file system v3
Disabled
Create
< Previous
Next >
Download a template for automation
27 Minutes Remaining
Instructions
Resources
Reigon
Performance
Redundancy
6. Select Review to review
settings and allow Azu
configuration.
7. Once validated, select
notification that the ac
created.
8. Select Go to resource.
Work with blob stora
In this section, you'll create a

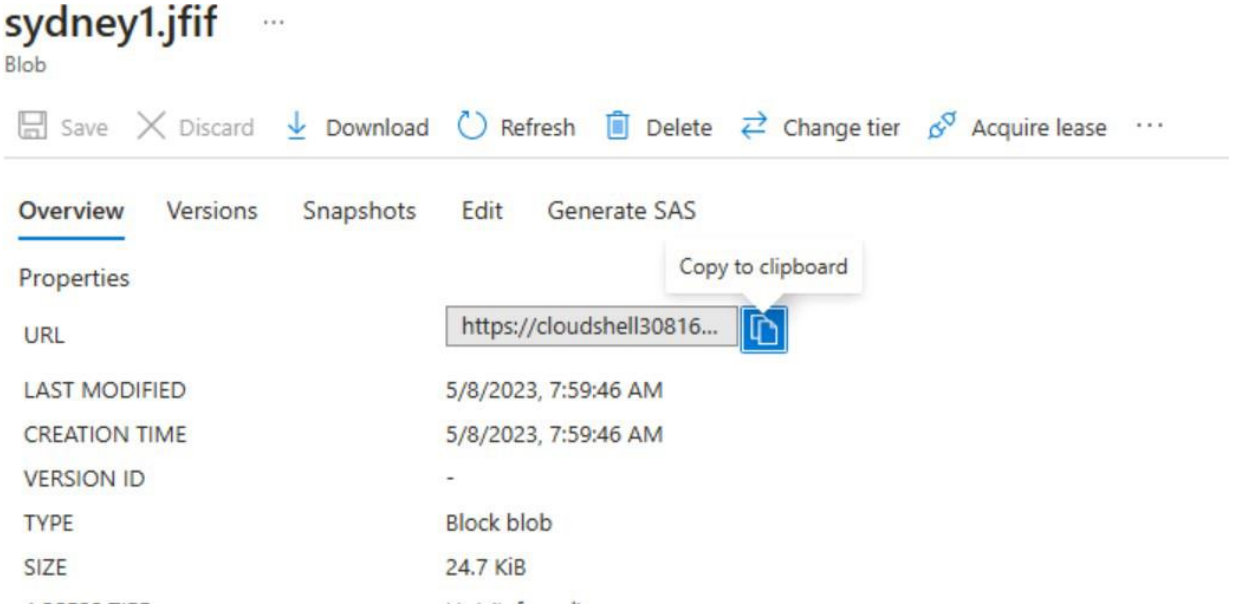

Microsoft Azure
Search resources, services, and docs (G+/)
Home
cloudshell30816812_1683557614524 | Overview
Deployment
Search
Overview
Inputs
Outputs
Template
Delete
Cancel
Redeploy
Download
Refresh
Deployment is in progress
Deployment name: cloud...
Subscription: AZ-900T00-...
Resource group: myRGKV...
Start time: 5/8/2023, 7:53:46 ...
Correlation ID: 51067495-877d-
Deployment details
Resource
Type
Status
No results.
Microsoft Defender f
Secure your apps and
Go to Microsoft Defer
Free Microsoft tutori
Start learning today >
Instructions
Resources
Help
Reigon
Default
Performance
Standard
Redundancy
Locally re
storage
6. Select Review to review your sto
settings and allow Azure to valic
configuration.
7. Once validated, select Create. W
notification that the account wa
created.
8. Select Go to resource.
Work with blob storage


Microsoft Azure
Search resources, services, and docs (G+/)
Home
cloudshell30816812
cloudshell30816812 | Containers
Storage account
Container
Change access level
Restore containers
Search containers by prefix
Name
Last modified
$logs
5/8/2023, 7:54:19 AM
New container
Name *
my-first-container
Public access level
Private (no anonymous access)
Advanced
Create
Give feedback
2. Select + Container and complete the information.
Name
Enter a name for the container
Public access level
Private (no anonymous access)
3. Select Create.
Step 4 will need an image. If you want to upload an image you already have on your computer, continue to Step 4. Otherwise, open a new browser window and search Bing for an image of a flower. Save the image to your computer.


Microsoft Azure
Search resources, services, and docs (G+/)
Home > cloudshell30816812 | Containers >
my-first-container
Container
Upload
Change access level
Refresh
Delete
Change tier
Acquire lease
Authentication method: Access key (Switch to Azure AD User Account)
Location: my-first-container
Search blobs by prefix (case-sensitive)
Show deleted blobs
Add filter
Access tier
Archive status
Blob type
Size
Lease state
23 Minutes Remaining
Instructions
Resources
Help
Name
Enter a name for the container
Public access level
Private (no anonymous access)
3. Select Create.
Step 4 will need an image. If you want to upload an image you already have on your computer, continue to Step 4. Otherwise, open a new browser window and search Bing for an image of a flower. Save the image to your computer.
4. Back in the Azure portal select the container you created, then select Upload.
5. Browse for the image file you want to upload. Select it and then select upload.


Save As
This PC > Downloads
Search Downloads
Organize
New folder
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
AllFiles (F:)
Name
Date modified
Type
Today (1)
sydney1.jfif
5/8/2023 7:58 AM
File name: waterfall
Save as type: JPEG Image (*.jfif)
Hide Folders
Save
Cancel
Module 04: Create a storage blob
21 Minutes Remaining
Instructions
Resources
Help
Public access level
3. Select Create.
4. Back in the Azure portal select th
then select Upload.
5. Browse for the image file you wa
then select upload.
You can upload as many blo
New blobs will be listed with


Upload blob - Microsoft Azure
https://portal.azure.com/#view/Microsoft_Azur...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > cloudshell30816812
my-first-cont
Container
Upload
Change acc
Authentication method: Acce
Location: my-first-container
Search blobs by prefix (case-s
Add filter
Access tier
Upload blob
Drag and drop files here
or
Browse for files
Overwrite if files already exist
Advanced
21 Minutes Remaining
Instructions
Resources
Name
Public access le
3. Select Create.
Step 4 will n
image you a
to Step 4. Ot
search Bing
to your com
4. Back in the Azure
then select Uploa
5. Browse for the im
then select uploa


sydney1.jfif
Blob
Save
Discard
Download
Refresh
Delete
Change tier
Acquire lease
Overview
Versions
Snapshots
Edit
Generate SAS
Properties
Copy to clipboard
URL
https://cloudshell30816...
LAST MODIFIED
5/8/2023, 7:59:46 AM
CREATION TIME
5/8/2023, 7:59:46 AM
VERSION ID
-
TYPE
Block blob
SIZE
24.7 KiB

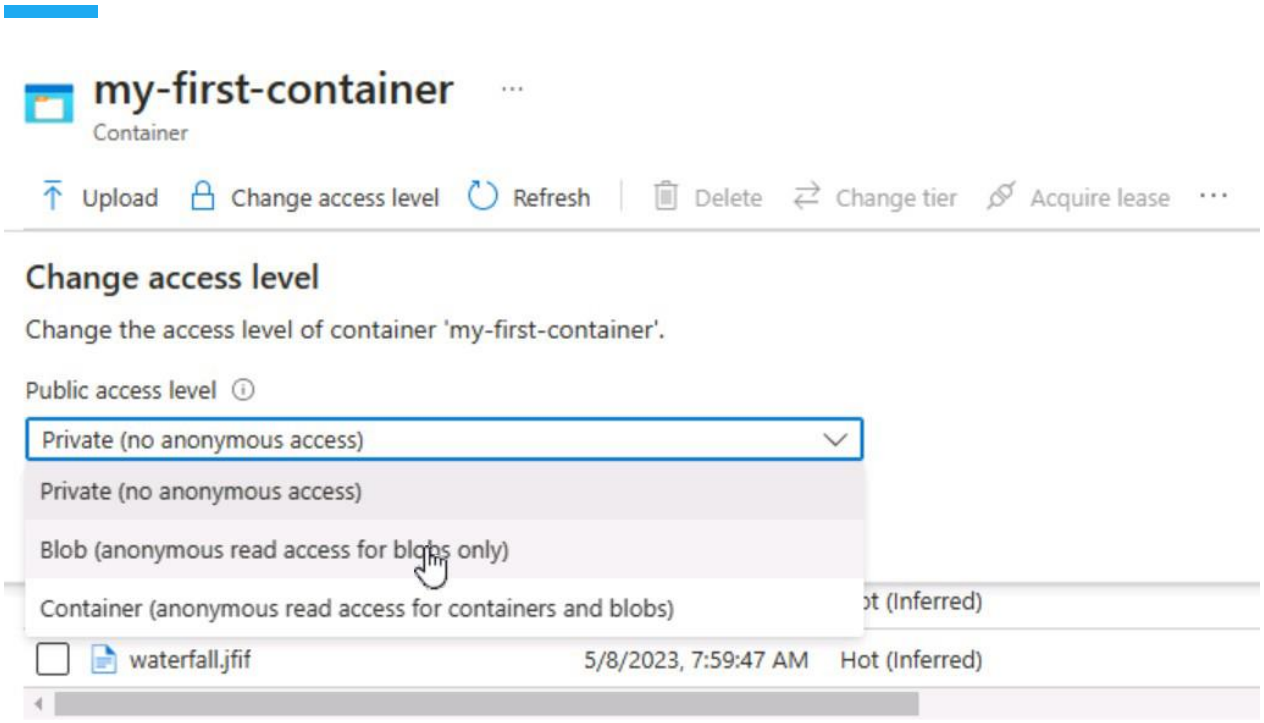
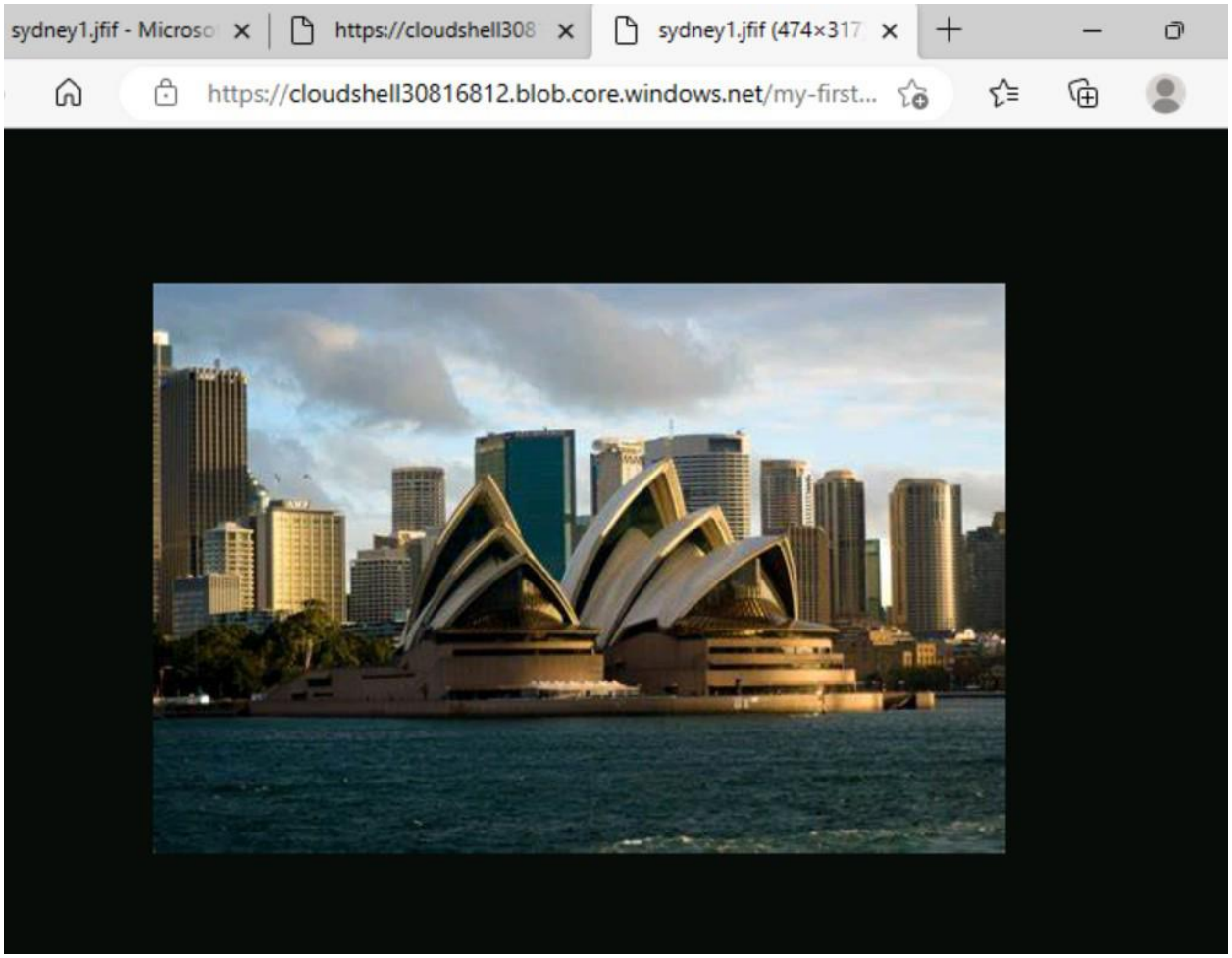


Image being able to be viewed.

 # Include a screenshot that shows one of the images and the full URL to access the image. • Include a screenshot of your Azure Portal resources that show the container(s).

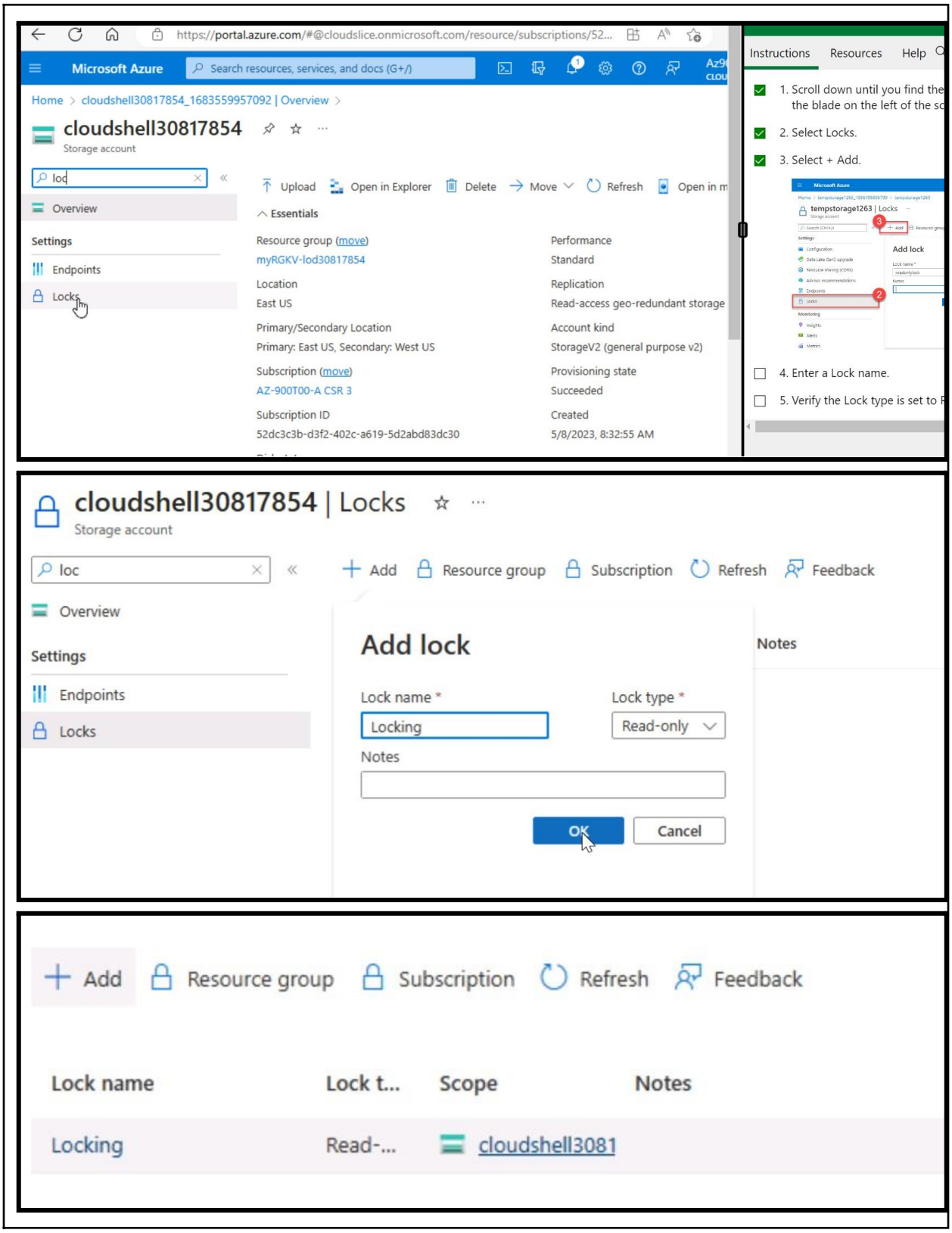


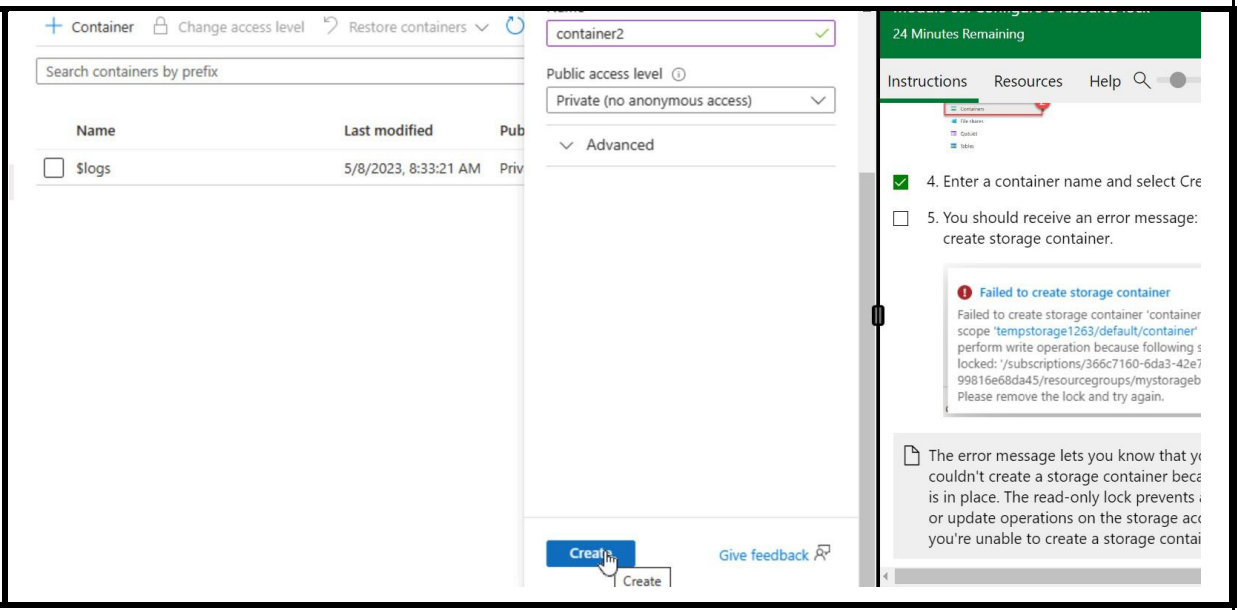
Task 6. Create a Resource Lock

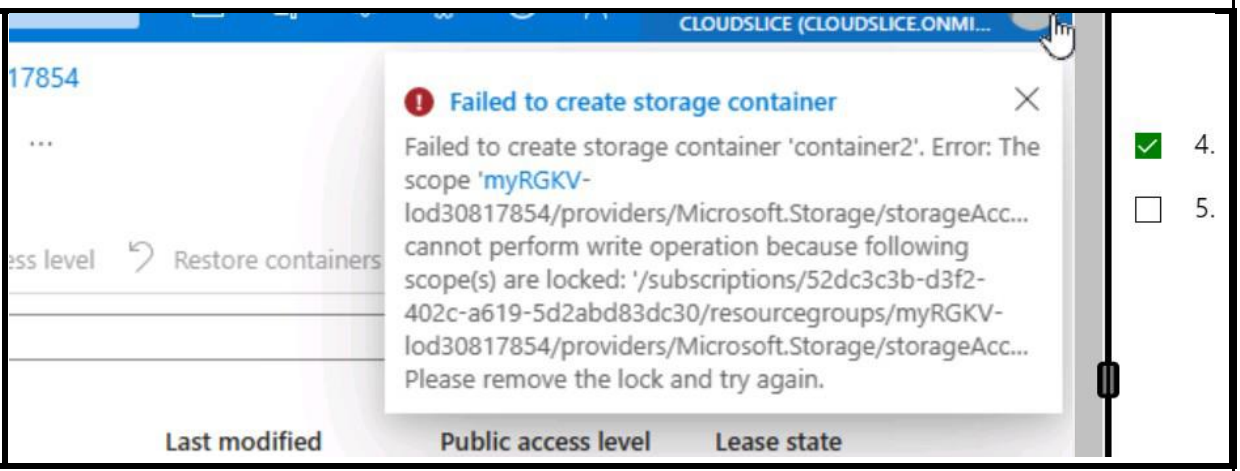
In Azure, resource locks can be applied to resource groups, subscriptions, or individual resources. Locks can be used to prevent deletion or modification of resources. There are two types of locks in Azure. Read-only lock and delete lock.

As the name suggests, read-only locks prevent modifications to resources, but not deletion of resources. A read-only lock allows a user to view a resource and perform operations that do not modify the resource, such as: B. Start or stop virtual machines, but cannot change resources. B. Adding or Deleting Components. Deletion locks, on the other hand, prevent the resource from being deleted or modified. This is a more restrictive lock type that prevents accidental deletion of critical resources. A delete lock prevents users from modifying or deleting resources, even if they have owner or contributor permissions.

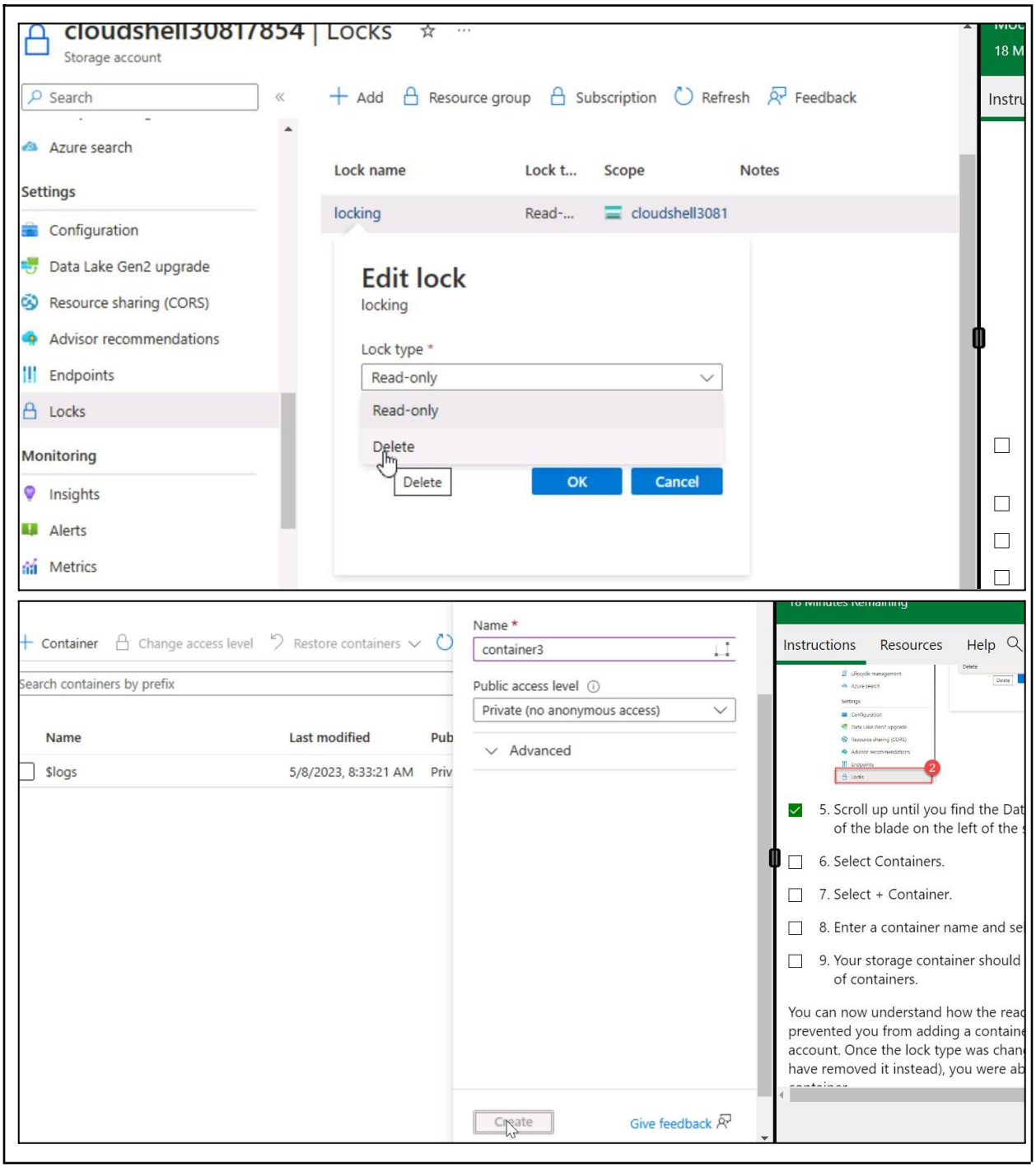
Lab 5 Completion Screenshots.

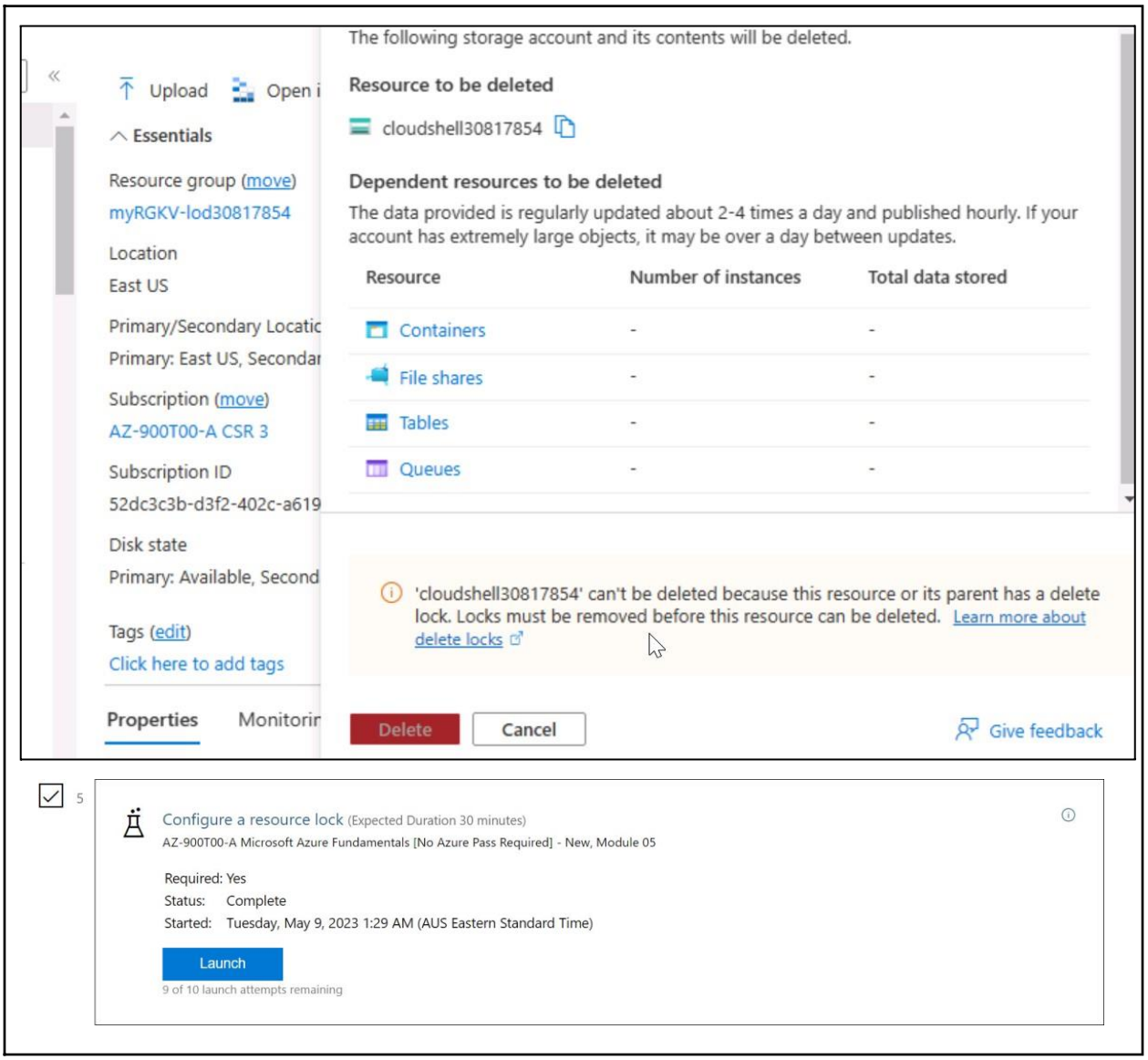

https://portal.azure.com/#@cloudslice.onmicrosoft.com/resource/subscriptions/52...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > cloudshell30817854_1683559957092 | Overview >
cloudshell30817854
Storage account
loc
Overview
Settings
Endpoints
Locks
Upload
Open in Explorer
Delete
Move
Refresh
Essentials
Resource group (move)
myRGKV-lod30817854
Location
East US
Primary/Secondary Location
Primary: East US, Secondary: West US
Subscription (move)
AZ-900T00-A CSR 3
Subscription ID
52dc3c3b-d3f2-402c-a619-5d2abd83dc30
Performance
Standard
Replication
Read-access geo-redundant storage
Account kind
StorageV2 (general purpose v2)
Provisioning state
Succeeded
Created
5/8/2023, 8:32:55 AM
Instructions
Resources
Help
1. Scroll down until you find the
the blade on the left of the sc
2. Select Locks.
3. Select + Add.
4. Enter a Lock name.
5. Verify the Lock type is set to
cloudshell30817854 | Locks
Storage account
loc
Add
Resource group
Subscription
Refresh
Feedback
Overview
Settings
Endpoints
Locks
Add lock
Lock name *
Locking
Lock type *
Read-only
Notes
OK
Cancel
Notes
Add
Resource group
Subscription
Refresh
Feedback
Lock name
Lock t...
Scope
Notes
Locking
Read-...
cloudshell3081





The error message lets you know that you couldn't create a storage container because a lock is in place. The read-only lock prevents any create or update operations on the storage account, so you're unable to create a storage container.


cloudshell30817854 | Locks
Storage account
Search
Add
Resource group
Subscription
Refresh
Feedback
Azure search
Settings
Configuration
Data Lake Gen2 upgrade
Resource sharing (CORS)
Advisor recommendations
Endpoints
Locks
Monitoring
Insights
Alerts
Metrics
Lock name
Lock t...
Scope
Notes
locking
Read-...
cloudshell3081
Edit lock
locking
Lock type *
Read-only
Read-only
Delete
Delete
OK
Cancel
Container
Change access level
Restore containers
Search containers by prefix
Name
Last modified
$logs
5/8/2023, 8:33:21 AM
Name *
container3
Public access level
Private (no anonymous access)
Advanced
Create
Give feedback
Instructions
Resources
Help
5. Scroll up until you find the Dat
of the blade on the left of the
6. Select Containers.
7. Select + Container.
8. Enter a container name and se
9. Your storage container should
of containers.
You can now understand how the read
prevented you from adding a containe
account. Once the lock type was chan
have removed it instead), you were ab



Task 7. Compare Cloud vs On-premise Costs

<u>Consumer desktop PC:</u>

Dell XPS 8940 Desktop:

- Processor: 11th Gen Intel Core i7-11700

- Memory: 16GB DDR4 2933MHz

- Storage: 512GB M.2 PCIe NVMe SSD

- Graphics: NVIDIA GeForce GTX 1650 4GB GDDR5

- Price: $1,249.99 (as of May

2023) Server:

HP ProLiant DL360 Gen10:

- Processor: Intel Xeon Silver 4210 2.2 GHz 10-core

- Memory: 32GB DDR4 2666MHz

- Storage: None included

- Graphics: None included

- Price: $4,385.00 (as of May 2023)

Cloud virtual machine:

Azure VM Standard B2s:

- Processor: 2 vCPUs, Intel Xeon E5-2673 v4 2.3GHz

- Memory: 4GB RAM

- Storage: 8GB temporary storage

- Graphics: None included

- Price: $0.082/hour (as of May

2023) Consumer Desktop PC:

CPU: Intel Core i7-11700K 3.6

GHz RAM: 16 GB DDR4

Storage: 512 GB NVMe SSD

GPU: NVIDIA GeForce GTX 1660 SUPER

OS: Windows 10

Home Cost: $1,299

Server:

CPU: Intel Xeon E-2278G 3.4

GHz RAM: 16 GB DDR4 ECC

Storage: 1 TB SATA HDD

RAID: RAID 1

OS: Windows Server 2019 Standard

Cost: $1,899

Azure VM:

CPU: 4 vCPUs (Intel Xeon Platinum 8272CL, 2.5 GHz)

RAM: 16 GB DDR4

Storage: 256 GB Premium SSD

OS: Windows Server 2019 Datacenter

Cost: $139.53/month or $1,662.36/year

Note:

The Azure VM cost is based on the pricing for a D4s v4 instance running Windows Server in the East US 2 region, with pay-as-you-go pricing.

When it comes to upfront cost, the consumer desktop PC is the cheapest option. However, it is important to note that this cost does not include peripherals such as a monitor, keyboard, and mouse. The server is the most expensive upfront option, but it also comes with features that are designed specifically for running applications and services in a business environment, such as RAID. The Azure VM has a moderate upfront cost, but its main advantage is that it is a flexible, scalable option that can be easily adjusted to meet changing needs. In terms of running costs, both consumer desktop PCs and servers require ongoing maintenance, including: B. Hardware upgrades, software updates, electricity bills. Azure VMs, on the other hand, have a predictable monthly cost that includes everything from hardware to software licenses.

Another trade-off to consider is the level of control and customization each option offers.

Consumer desktop PCs give the user complete control over the hardware and software, allowing for maximum customization. Servers give users less control over the physical hardware, but allow

them to customize the software to meet their specific needs. Azure VMs give users even less control over the physical hardware, but give them access to a variety of pre-configured software, making it easy to scale resources up or down as needed.

Week 8

Task 1. CIA Protections

List the assets, and for each asset, give the protection and reason.

1. Servers

Protection: confidentiality, integrity, availability

Reason: servers store sensitive information and are critical to the functioning of the network

2. User data

Protection: confidentiality, integrity

Reason: user data may contain personal or sensitive information that should not be accessible or tampered with by unauthorized parties

3. Network switches/routers

Protection: availability,

integrity

Reason: if switches or routers go down or are compromised, network traffic may not be able to reach its intended destination or may be intercepted

4. Firewalls

Protection: confidentiality, integrity

Reason: firewalls help prevent unauthorized access to the network and can help detect and block malicious activity

5. Backup data

Protection: availability, integrity

Reason: backup data is critical in the event of data loss or corruption, so it must be accessible and accurate

6. End-user devices (e.g. laptops, desktops, mobile

devices) Protection: confidentiality, integrity

Reason: these devices may contain sensitive information and may be used to access the network, so they should be protected from unauthorized access or tampering

7. Printers/scanners

Protection: availability, integrity

Reason: if printers or scanners go down, important documents may not be able to be printed or scanned, and if they are compromised, sensitive information may be leaked

8. Security cameras

Protection: availability,

integrity

Reason: if security cameras are down or compromised, there may be a gap in surveillance coverage and important footage may not be available in the event of an incident

9. Customer database

Protection:

Confidentiality

Reason: Personal information such as names, addresses, and payment details should only be accessed by authorized personnel and not shared with unauthorized parties.

10. Email server

Protection:

Integrity

Reason: Emails must not be altered or modified without authorization, as this could result in important information being lost or miscommunicated.

11.Web server

Protection:

Availability

Reason: A web server must be available to provide uninterrupted access to a company's website and web-based services.

12. File server

Protection: Confidentiality

Reason: Sensitive company information stored on a file server should only be accessible to authorized personnel, as it could be damaging if it falls into the wrong hands.

13. Backup system

Protection:

Availability

Reason: A backup system must be available to ensure that important data can be restored in case of a data loss event such as a cyberattack, hardware failure, or natural disaster.

14. Firewall

Protection:

Integrity

Reason: A firewall must be configured and maintained correctly to ensure that it is providing the intended protection and not being bypassed or manipulated by attackers.

15. Wireless network

Protection:

Confidentiality

Reason: Wireless networks must be secured to prevent unauthorized access to sensitive data transmitted over the network.

16. VPN (Virtual Private

Network) Protection:

Confidentiality

Reason: VPNs must be secured to ensure that data transmitted over the network is protected from eavesdropping and interception by unauthorized parties.

Task 2. Threat Sources and Motivation

List the threat sources, and for each threat source, give the motivation.

Threat Source 1: hacktivist

- Motivation: Spread a political or social message or raise awareness of a cause.

- Threat Source 2: cyber criminal

- Motivation: Obtaining money through theft, extortion, or other illegal activity.

- Threat Source 3: nation state

o Motivation: To gain strategic advantage or espionage, or to interfere with the operations of another country.

• Threat Source 4: Insider threats

o Motivation: Steal confidential information or intellectual property, interfere with operations, or retaliate for perceived fraud.

• Threat Source 5: business competitor(s)

o Motivation: Stealing intellectual property, trade secrets, or other confidential information to gain a competitive advantage.

• Threat Source 6: script kiddie(s)

o Motivation: To gain notoriety or cause harm without necessarily having a specific goal or agenda.

• Threat Source 7: state-sponsored hackers

o Motivation: Espionage, sabotaging another country's operations, or gaining strategic advantage in areas such as military, economic, or political.

• Threat Source 8: Gangster

o Motivation: Obtaining money through activities such as theft, extortion or fraud, or engaging in activities such as trafficking or drug smuggling.

Task 3. Explore Vulnerabilities

Include the details for the critical, high and medium CVE.

1.CVE-2021-33742

CVE Description: Log files in versions of McAfee Data Center Security Suite for Windows prior to
6.5.0 do not store sensitive information securely, allowing a local user to read the log files and gain unauthorized access to sensitive data.

Date: 2021-05-04

CVSS version 3 score: 7.8 (high)

Impact on Confidentiality, Integrity and Availability: Confidentiality (High), Integrity (Low), Availability (Low)

CWE: CWE-532: Injecting Sensitive Information into Log

Files Company: McAfee

Product Description: McAfee Data Center Security Suite for Windows is antivirus and malware detection software for Windows servers.

Vulnerability description: Sensitive information was stored in system log files without proper encryption or access controls, allowing local users to view sensitive data.

Detection and mitigation techniques: Update to version 6.5.0 or later.

2. CVE-2021-22986

CVE Description: Remote Code Execution for F5 BIG-IP versions 16.0.0-16.0.1.1, 15.1.0-15.1.2.1,
14.1.0-14.1.4, 13.1.0-13.1.3.6, and 12.1.0-12.1.5.3 An attacker executing arbitrary code through specially crafted requests to the Vulnerability Traffic Management User Interface (TMUI).

Date: 2021-03-10

CVSS Version 3 Score: 9.8 (Critical)

Impact on Confidentiality, Integrity, and Availability: Confidentiality (High), Integrity (High), Availability (High)

CWE: CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

Company: F5 Networks

Product Description: F5 BIG-IP is a traffic management software used by enterprise networks.

Explanation of Vulnerability: The vulnerability allowed an attacker to execute arbitrary code remotely by sending a specially crafted request to the Traffic Management User Interface (TMUI).

Detection and Mitigation Techniques: Upgrade to a fixed version (16.0.1.2, 15.1.2.2, 14.1.4.6, 13.1.3.4, or 12.1.5.3), or use recommended mitigations until an upgrade can be performed.

3. CVE-2022-39881

CVE Description: Use-after-free vulnerability in Microsoft Windows versions prior to Windows

11 and Windows Server 2022 allows a remote attacker to execute arbitrary code via a specially crafted document.

Date: 2022-03-08

CVSS Version 3 Score: 6.8 (Medium)

Impact on Confidentiality, Integrity, and Availability: Confidentiality (High), Integrity (High), Availability (Low)

CWE: CWE-416: Use After Free

Company: Microsoft

Product Description: Microsoft Windows is an operating system used by many computers worldwide.

Vulnerability description: This vulnerability allowed an attacker to send a specially crafted document to the system to execute arbitrary code and trigger a use-after-free condition.

Detection and mitigation techniques: Apply the latest security updates from Microsoft.

Task 4. Vulnerability Disclosures

Write up your own viewpoint that discusses the issues with vulnerability disclosure.

Vendors can take a long time to disclose vulnerabilities for a variety of reasons. A common reason is that vendors need time to research and develop before releasing patches to fix vulnerabilities. Additionally, the vendor may need to coordinate with other organizations or vendors affected by the vulnerability to develop a comprehensive solution. Legal or contractual considerations may also need to be considered before a vulnerability is disclosed.

The time it takes for a vendor to disclose a vulnerability depends on the severity of the vulnerability and the complexity of the required solution. In general, 90 days from disclosure of the vulnerability is a reasonable period of time for the vendor to notify MITER and the public of the vulnerability. This period is often referred to as the "cooperative disclosure" or "responsible disclosure" period.

If the vendor does not disclose the vulnerability within a reasonable timeframe, security researchers may consider doing so without the vendor's consent. However, researchers should carefully consider the potential implications of such an approach. B. Liability or negative publicity of the organization concerned. In some cases, it may be better to continue working with the vendor to resolve the issue privately or disclose the vulnerability to a trusted third party to enable responsible disclosure.

Week 9

Task 1. Select Security Objectives

For each of the selected sub-categories, give the function, category and sub-category, and then explain why it is important and explain an attack/vulnerability it may mitigate.

CSF : Cyber Security Framework

The CSF is organized around five core functions: Identify, Protect, Detect, Respond, and Recover.

Function: Protect; Category: Data Security; Sub-category: Information Protection Processes and Procedures (PR.DS-2)

Reason for importance: Information protection processes and procedures are important for ensuring that sensitive information is properly protected from unauthorized access, modification, or destruction. By implementing effective processes and procedures for protecting information, organizations can prevent data breaches, insider threats, and other types of cyber attacks.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as data breaches, insider threats, and social engineering attacks by ensuring that proper controls are in place for protecting sensitive information.

Function: Protect; Category: Risk Management; Sub-category: Risk Assessment (PR.RA-3)

Reason for importance: Risk assessments are important for identifying potential threats and vulnerabilities that could be exploited by cyber attackers. By conducting regular risk assessments, organizations can identify and prioritize potential threats, and develop effective strategies for mitigating those threats.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as malware infections, phishing attacks, and data breaches by identifying potential vulnerabilities and implementing effective controls to mitigate those vulnerabilities.

Function: Detect; Category: Anomalies and Events; Sub-category: Security Information and Event Management (SIEM) (DE.AE-3)

Reason for importance: Security information and event management (SIEM) is important for monitoring and analyzing security events and alerts, and for identifying potential cyber threats in

real-time. By implementing effective SIEM controls, organizations can quickly detect and respond to potential cyber threats.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as advanced persistent threats (APTs), insider threats, and ransomware attacks by continuously monitoring and analyzing security events and alerts.

Function: Detect; Category: Response Planning; Sub-category: Communications (DE.CM-1)

Reason for importance: Communications planning is critical for ensuring that all stakeholders are informed and involved in the incident response process in the event of a cyber attack. By developing effective communication plans, organizations can ensure that everyone is on the same page and can work together to mitigate the attack.

Mitigated attack/vulnerability: This sub-category can mitigate attacks such as data breaches, network intrusions, and ransomware attacks by ensuring that all stakeholders are informed and involved in the incident response process.

Create Asset Inventory

Tables of assets for the six (6) asset types, ensuring the Data assets also are classified.

Data Assets:

Asset Name	Classification	CIA Protections
Customer database	Confidential	Confidentiality
Financial records	Sensitive	Confidentiality, Integrity
Intellectual property	Critical	Confidentiality, Integrity
Personnel records	Confidential	Confidentiality
Marketing plans	Sensitive	Confidentiality, Integrity
Product designs	Critical	Confidentiality, Integrity
Legal documents	Confidential	Confidentiality

Hardware Assets:

Asset Name	Identification Information	CIA Protections
Servers	IP addresses, serial numbers	Availability, Confidentiality, Integrity
Routers	MAC addresses, serial numbers	Availability, Confidentiality, Integrity
Firewalls	IP addresses, firmware versions	Availability, Confidentiality, Integrity
Switches	MAC addresses, port configurations	Availability, Confidentiality, Integrity
Workstat i ons	Asset tags, user names	Availability, Confidentiality, Integrity
Laptops	Asset tags, serial numbers	Availability, Confidentiality, Integrity

Software Assets:

Asset Name	Vendor	CIA Protections
Operating system	Microsoft, Apple, Linux	Availability, Confidentiality, Integrity
Antivirus software	Symantec, McAfee, Kaspersky	Availability, Confidentiality, Integrity
Office productivity suite	Microsoft Office, Google Workspace	Availability, Confidentiality, Integrity
Web browser	Google Chrome, Mozilla Firefox	Availability, Confidentiality, Integrity

Email client	Microsoft Outlook, Gmail	Availability, Confidentiality, Integrity
Database management system	Oracle, Microsoft SQL Server	Availability, Confidentiality, Integrity

Physical Assets:

Asset Name	Location	CIA Protections
Building	Street address, floor plan	Availability, Confidentiality
Data center	Street address, access control list	Availability, Confidentiality, Integrity
Backup tapes	Offsite storage facility	Confidentiality, Integrity
Locks	Manufacturer, key code	Availability, Confidentiality
Security cameras	Location, manufacturer	Availability, Confidentiality

Personnel Assets:

Asset Name	Position	CIA Protections
CEO	Chief executive officer	Confidentiality
IT manager	Information technology manager	Availability, Confidentiality, Integrity
Database administrator	Database administrator	Confidentiality, Integrity
Sales representative	Sales representative	Availability, Confidentiality

Human resources manager	Human resources manager	Confidentiality

Network Assets:

Asset Name	Description	CIA Protections
Wireless access point	Model, encryption method	Availability, Confidentiality
Virtual private network	VPN gateway IP address, encryption protocol	Confidentiality
Domain name system	DNS server IP addresses, domain names	Availability, Confidentiality, Integrity
Network attached storage	Storage capacity, access control list	Availability, Confidentiality, Integrity
Intrusion detection system	IDS sensor IP addresses, alerting thresholds	Availability, Confidentiality, Integrity

Task 3. Information Flow Check

Diagrams of information flows for two (2) important assets

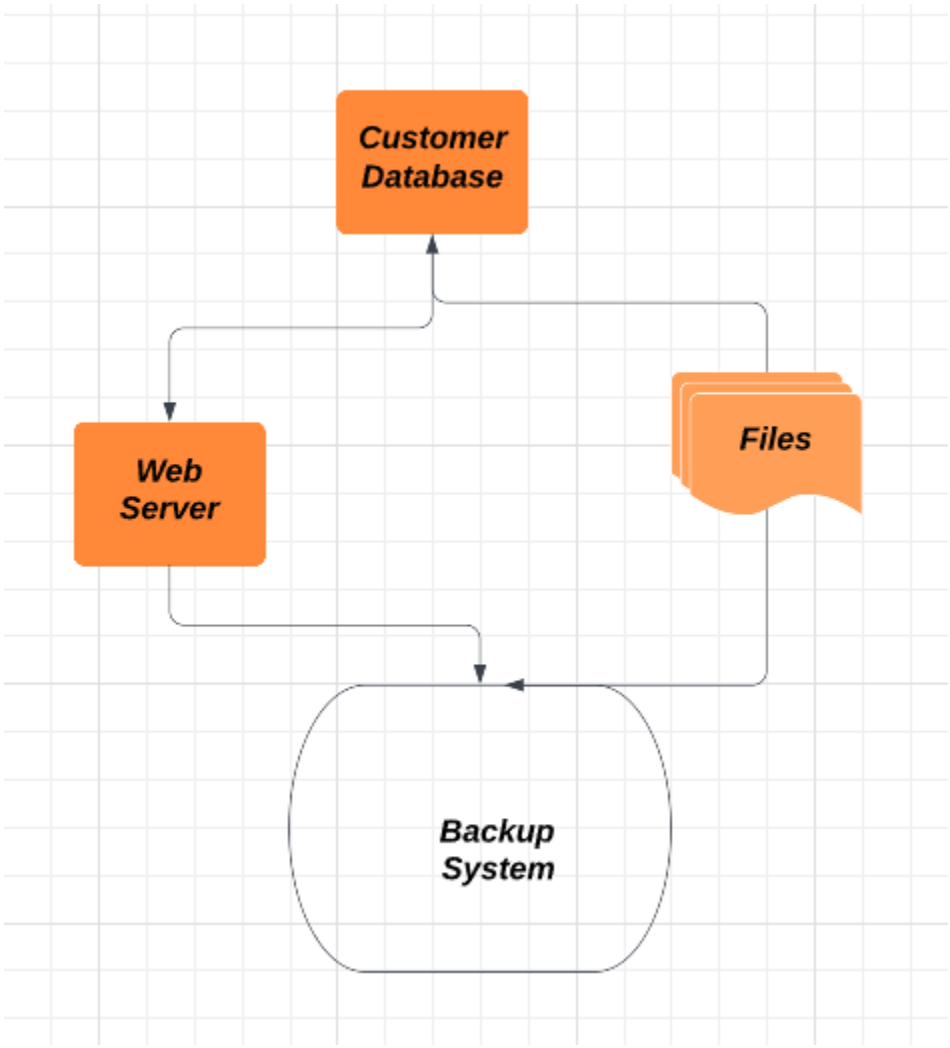
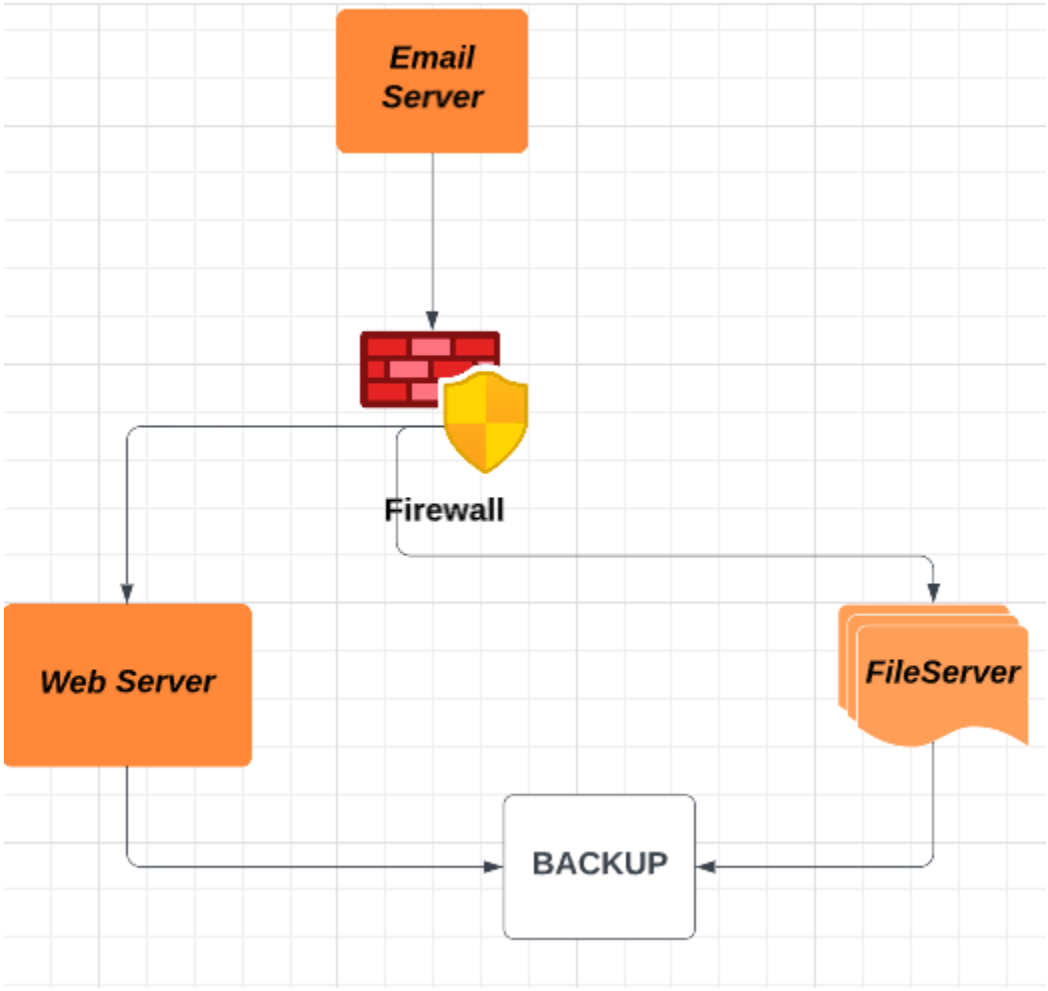


Diagram 2



Task 4. Conduct a Risk Analysis

There is no need to include this in your journal, as it will be in your project submission.

Week 10

Task 1. Essential Eight Mitigation Strategies

For each of the selected strategies, a description of how it is applied for your Project.

• Reasons why you selected these strategies (and not the other of the Essential Eight).

1. Essential → Application Control from 'Prevent Malware Delivery and Execution'

Reason : In a corporate environment, there is an undeniable need and usage of working with multiple options, there may be alternatives to applications, scammed applications etc. Point is that the applications used for specific utility also serve as great attack vectors.

Solution strategy? Having control over execution. To control applications that are untested, unapproved and have unjustifiable execution of scripts/dll etc.

Example & Description: Our Project is based on Protection and Detection. And having a thorough application control will aid our plan. For example, the Test network System will have minimal access in downloading and installation of applications, It will be password or protected with either mechanisms and would require Admin's consent and notice before installation of any application.

2. Essential → Restricted Administrative Privileges from 'Limit the Extent of Cyber Security Incidents'

   Reason : Limited Privileges has always been a great approach . We do not need high privileges to run every day tasks. This could help in reduction of possible attack scenarios. It may also ensure that even if an employee account gets compromised through thoroughly sorted Social engineering attacks, the risks will be comparatively low.

   Example & Description: Unnecessary extra privileges may lead to multiple accounts being at risk. Social Engineering attacks are nothing unheard of, a recent example being of UBER. Let's limit the privileges or construct accounts with dual consent for operation.

3. Excellent→ Network Segmentation from 'Limit the Extent of Cyber Security Incidents'

   Reason : A common strategy of Malwares or any attack vector to propagate in a compromised system is to check for linked networks. The wise strategy is to separate networks and restrict traffic between computers unless required. Limit access to network drives, databases and other configuration files based on user defined duties.

   Example & Description: The test network will be kept and maintained separately. It will have internal firewalls or security controls to allow specific or no internetwork traffic to reduce the compromise scale.

4. Excellent→ Continuous Incident detection and response from 'Detect Cyber

Security Incidents and Respond’

Reason : Attackers are never off the clock, thus it is necessary to implement strategies that could keep a track of malicious activities at all the time. This calls for a continuous

MONITORING and real time detection schemes/softwares or a dedicated team of professionals .

Example & Description: To put some good examples, on our test network or test assets, SIEM tools and a dedicated SOC team shall be deployed. Objective is to provide continuous monitoring and real time detection of malicious activities.

Task 2. Explore and Select NIST Controls

For each of the selected controls, an explanation of its relevance and description of how it is applied for your Project.

AU-14 Session Audit : This control is crucial because it makes sure that every user action within a system is tracked and logged. Organizations can recognise suspicious behavior and spot potential security breaches by keeping track of user behaviors. This control might be put into place on a secure network by installing audit settings on all pertinent systems and making sure that logs are kept for a long enough time. An organization may, for instance, set the retention duration to 90 days and arrange their Windows servers to audit user behavior.

AT-3 Role Based Training : This control is crucial because it guarantees that users possess the knowledge and abilities required to securely carry out their given tasks. Organizations can lower the risk of human error and lessen the chance of security incidents by offering training that is specific to each user's position within the company. This control could be accomplished in a safe network by creating role-based training courses and making sure that every user receives the right instruction for their position. For instance, a company might create a security awareness training course including modules for executives, IT personnel, and non-technical staff that are based on roles.

AT-1 Policies and Procedures : This control is crucial since it guarantees that everyone using the system is aware of the organization's security policies and practices. Organizations may foster a culture of security and reduce the risk of unintentional or purposeful security breaches by clearly defining and communicating security requirements. This control could be put into place in a secure network by creating thorough security policies and procedures and making sure that all users are trained in them. In order to ensure that all users are aware of the policy, training could be given once an organization develops a password policy that mandates users set secure passwords and change them frequently.

CM-7 Least Functionality : This control is crucial because it guarantees that systems are set up to

grant only the minimal amount of access required for them to function as intended. Organizations can restrict the attack surface and lower the risk of unauthorized access or data loss by limiting

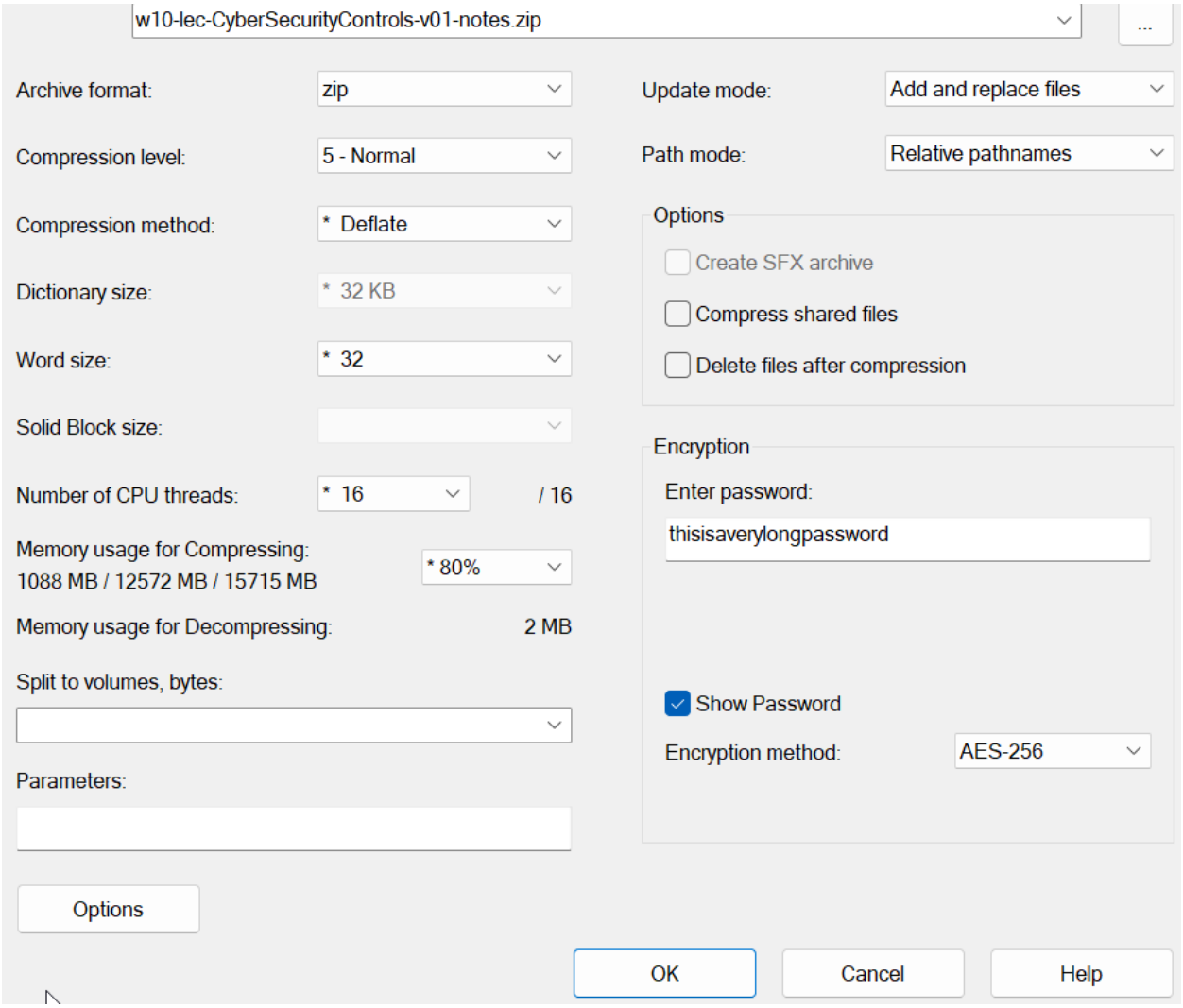
the functionality of systems and apps. This control might be put into place in a secure network by doing routine vulnerability assessments and penetration tests to find pointless services and functionality, and then turning them off or eliminating them. For instance, a company could examine the web application's vulnerabilities and find that the FTP service is being used needlessly. The FTP service might then be turned off to lessen the attack surface.

CA -7 Continuous Monitoring : This control is crucial because it guarantees that networks and systems are continuously checked for security-related accidents and events. Organizations may notice and respond to security breaches more rapidly by continually monitoring their systems, which lowers the impact and lowers the chance of data loss or theft. This control could be applied in a secure network by utilizing security monitoring solutions that offer real-time alerts and reporting. An organization might, for instance, install an intrusion detection system (IDS) that keeps track of network traffic and notifies security personnel of any unusual behavior.

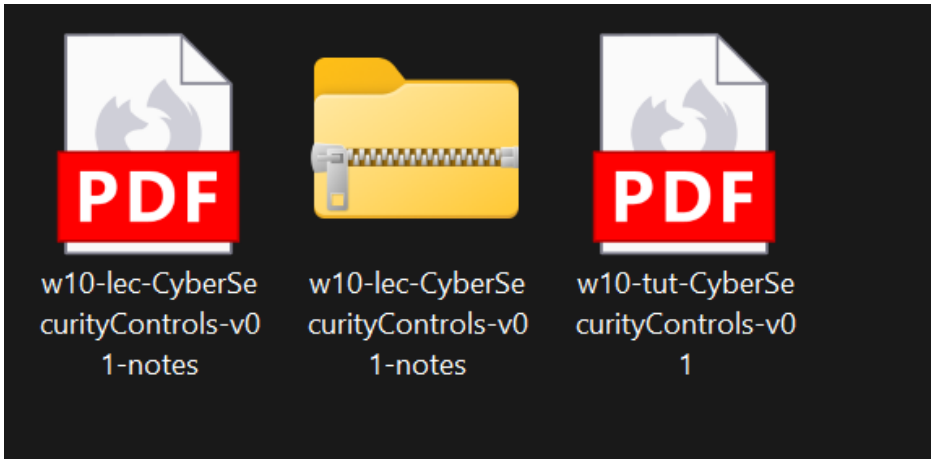
CA-8 Penetration Testing : This control is crucial because it guarantees that networks and systems are examined for flaws and vulnerabilities by mimicking actual attacks. Organizations can find security flaws and fix them before attackers take advantage of them by conducting frequent penetration tests. This control could be put into place in a safe network by conducting routine penetration tests on important networks and systems. An organization might, for instance, contract with an outside security company to conduct a penetration test on its online application in order to find vulnerabilities and offer suggestions for fixing them.

Task 3. Encrypt a File

Screenshot of the settings used to encrypt the file.



After completion, we got our zip file.



• Discuss how you shared the secret key, the limitations of that approach, and recommendations for more secure ways to share a secret key.

I shared the secret pass key via an email. It could also be sent through a chat application or in Person.

Limitation to this approach and the possible solutions :

- If the transmission method is insecure (for instance, if you share the password over email), the password may be intercepted or compromised while in transit.
- The recipient could easily forget the password, in which case it would be difficult to decrypt the file.

Some other useful measures than the general ones.

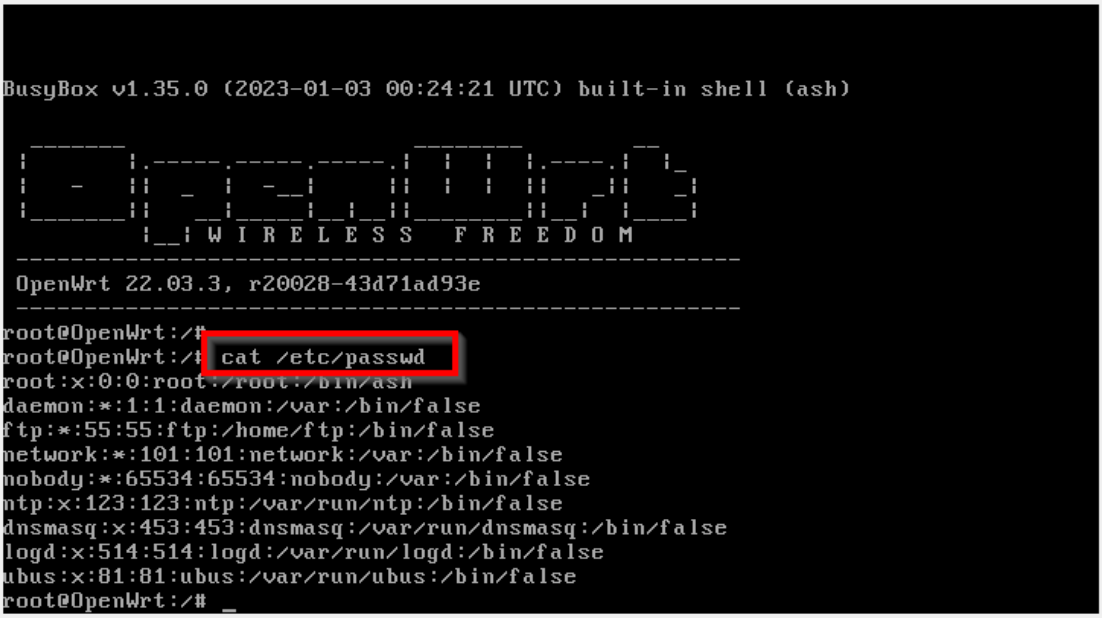
Using a secure file sharing service: You can use a secure file sharing service that enables you to encrypt the file and share the password in a secure manner rather than sharing the encrypted file and password individually. OneDrive, Google Drive, and Dropbox are a few examples of these services.

Using a secure messaging app: You can use a secure messaging app that enables end-to-end encryption, such as Signal or WhatsApp, in place of sending the password by email or text message.

Using a key management system: You can use a key management system to securely store and share the password with authorized users rather than disclosing it to them directly. LastPass and KeePass are a couple of examples of these solutions.

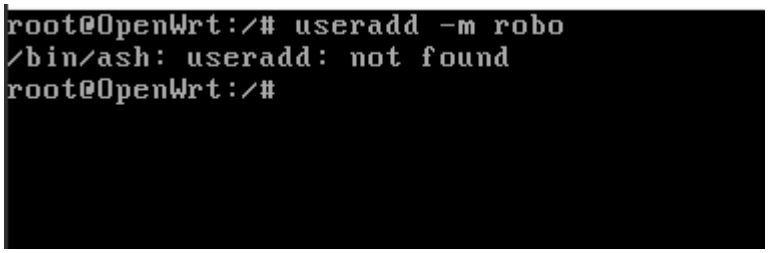
Task 4. View Password Information Stored in Linux

Screenshot or copy-and-paste of the /etc/shadow file entries that show your new user and password information.

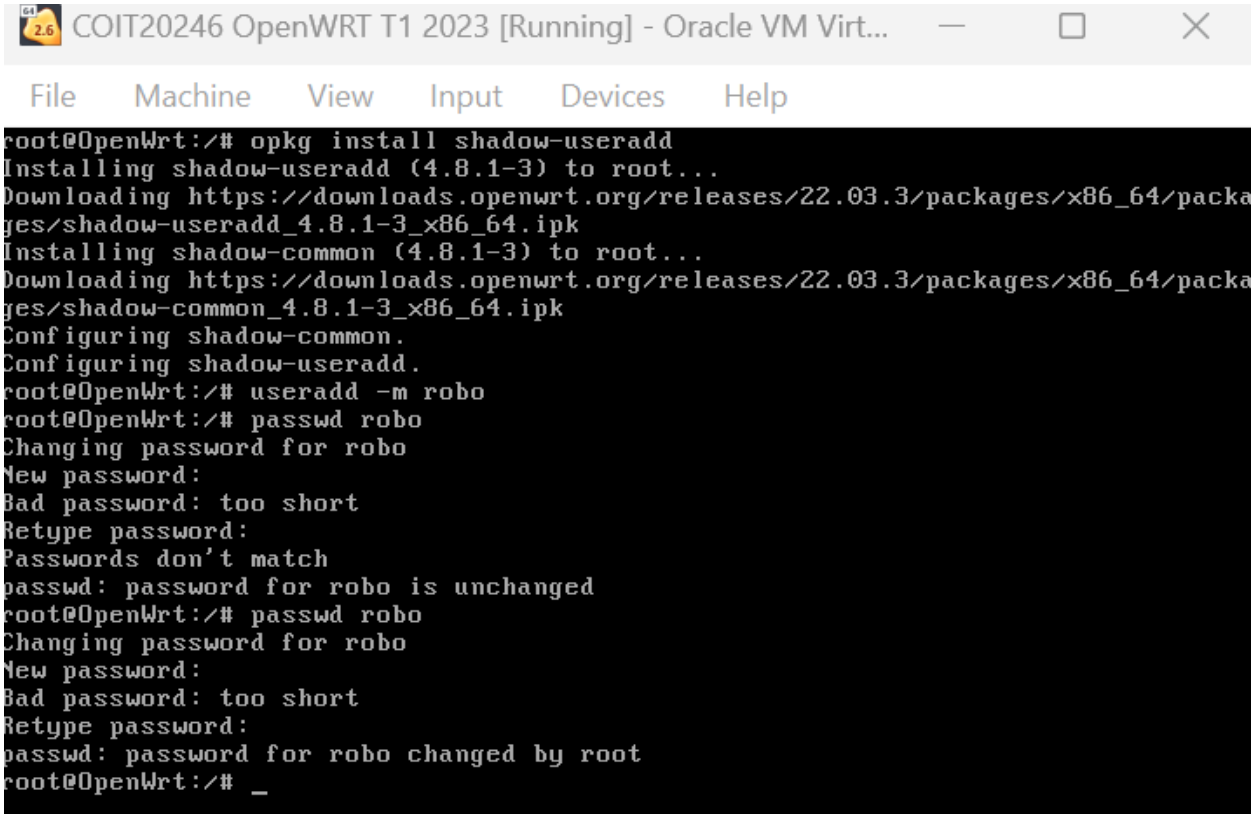


To add as new user, I tried the standard linux command **useradd -m <username>**

But I got error,



After checking with the video tutorial, I came back and updated my system, **opkg update, → opkg install shadow-useradd**



Commands used :

opkg update

opkg install shadow-useradd useradd -m <name_of_user> passwd <name_of_user>

To confirm new user added, we can once again go back and check the passwd file byu command

cat /etc/passwd

```
root@OpenWrt:/# passwd robo
Changing password for robo
New password:
Bad password: too short
Retype password:
Passwords don't match
passwd: password for robo is unchanged
root@OpenWrt:/# passwd robo
Changing password for robo
New password:
Bad password: too short
Retype password:
passwd: password for robo changed by root
root@OpenWrt:/# cat /etc/passwd
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
ntp:x:123:123:ntp:/var/run/ntp:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
logd:x:514:514:logd:/var/run/logd:/bin/false
ubus:x:81:81:ubus:/var/run/ubus:/bin/false
robo:x:1000:1000::/home/robo:
root@OpenWrt:/#
```

We can see details of the new user **robo** now.

We will do a couple of more things, we will edit our /etc/passwd file to allow putty login. We can do this by adding **/bin/ash** at the end of the new line created for the new user. Save and exit the nano editor.

```
root:x:0:0:root:/root:/bin/ash
daemon:*:1:1:daemon:/var:/bin/false
ftp:*:55:55:ftp:/home/ftp:/bin/false
network:*:101:101:network:/var:/bin/false
nobody:*:65534:65534:nobody:/var:/bin/false
ntp:x:123:123:ntp:/var/run/ntp:/bin/false
dnsmasq:x:453:453:dnsmasq:/var/run/dnsmasq:/bin/false
logd:x:514:514:logd:/var/run/logd:/bin/false
ubus:x:81:81:ubus:/var/run/ubus:/bin/false
robo:x:1000:1000::/home/robo:/bin/ash
```

Explanation of the password information stored in /etc/shadow, and why the actual password is not stored.

Only ‘Root’ user account or the one’s listed in the Sudoers List can view/do changes to the etc/passwd file.

The multiple field present in the /etc/passwd file are

Username: The name of the user.

Password: The encrypted password of the user.

Last password change: The number of days since the password was last changed.

Minimum password age: The number of days that must pass before the password can be changed again.

Maximum password age: The maximum number of days that a password can be used before it must be changed.

Warning period: The number of days before the password expires that the user is warned.

Inactivity period: The number of days after the password expires that the account is disabled.

Expiration date: The date on which the password will expire.

Reserved field: This field is not currently used.

The reason why the actual password is not stored in the /etc/shadow file is for security reasons. Storing the actual password in plain text would make it much easier for an attacker to gain unauthorized access to the system, as they could simply read the password from the /etc/shadow file. However, by storing only the encrypted hash, an attacker would need to crack the encryption to discover the password. This is a much more difficult and time-consuming process, particularly if the password is strong and complex.

Task 5. Setup Key-Based Authentication

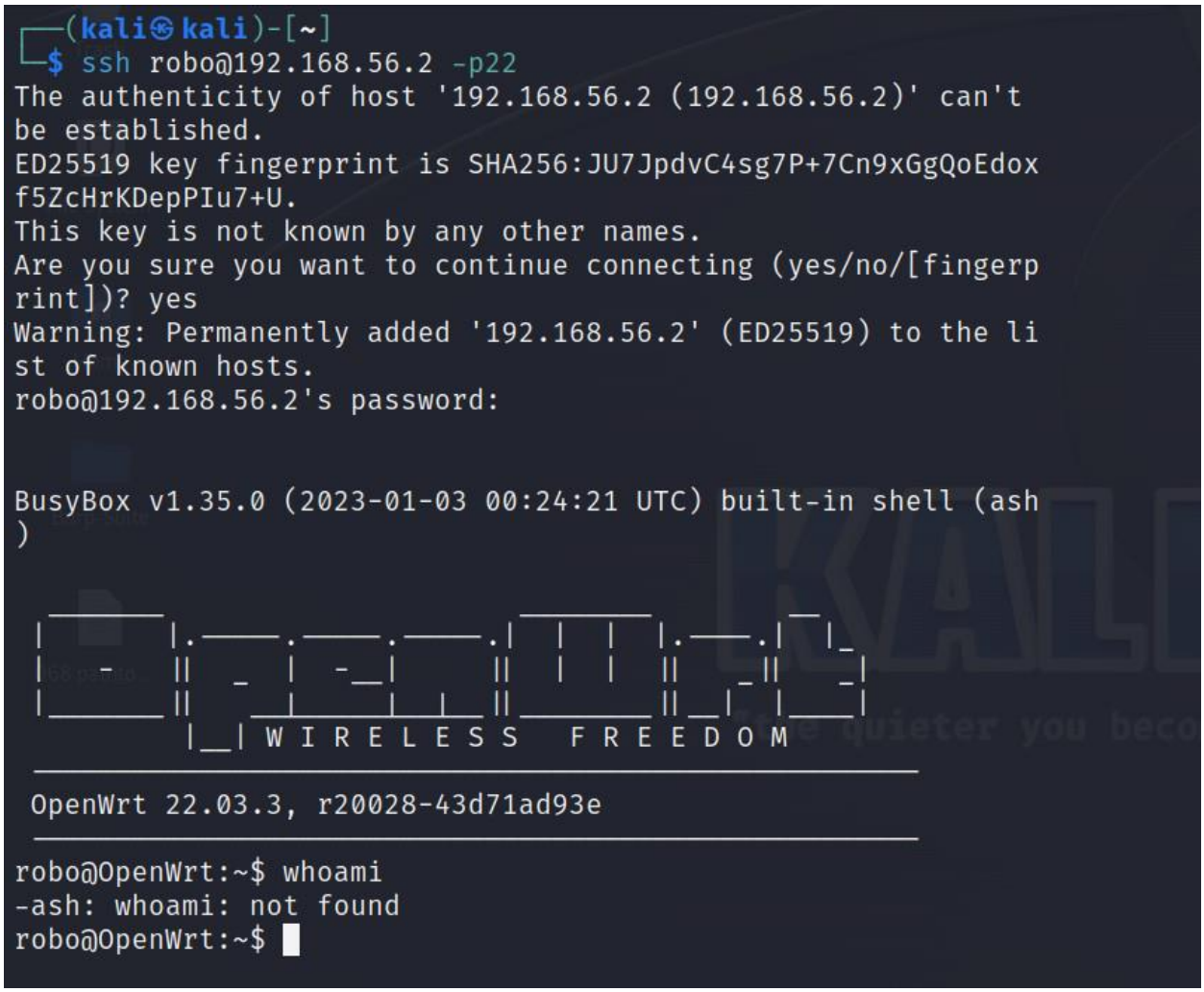
Choosing task (a) Key-based SSH login for OpenWRT Linux VM using

PuTTy Screenshots or copy-and-paste of the steps/commands you used.

After creating the newuser, I quickly wanted to test out the ssh login so I just tried simple ssh logging into the OpenWRT linux VM , on IP 192.168.56.2.

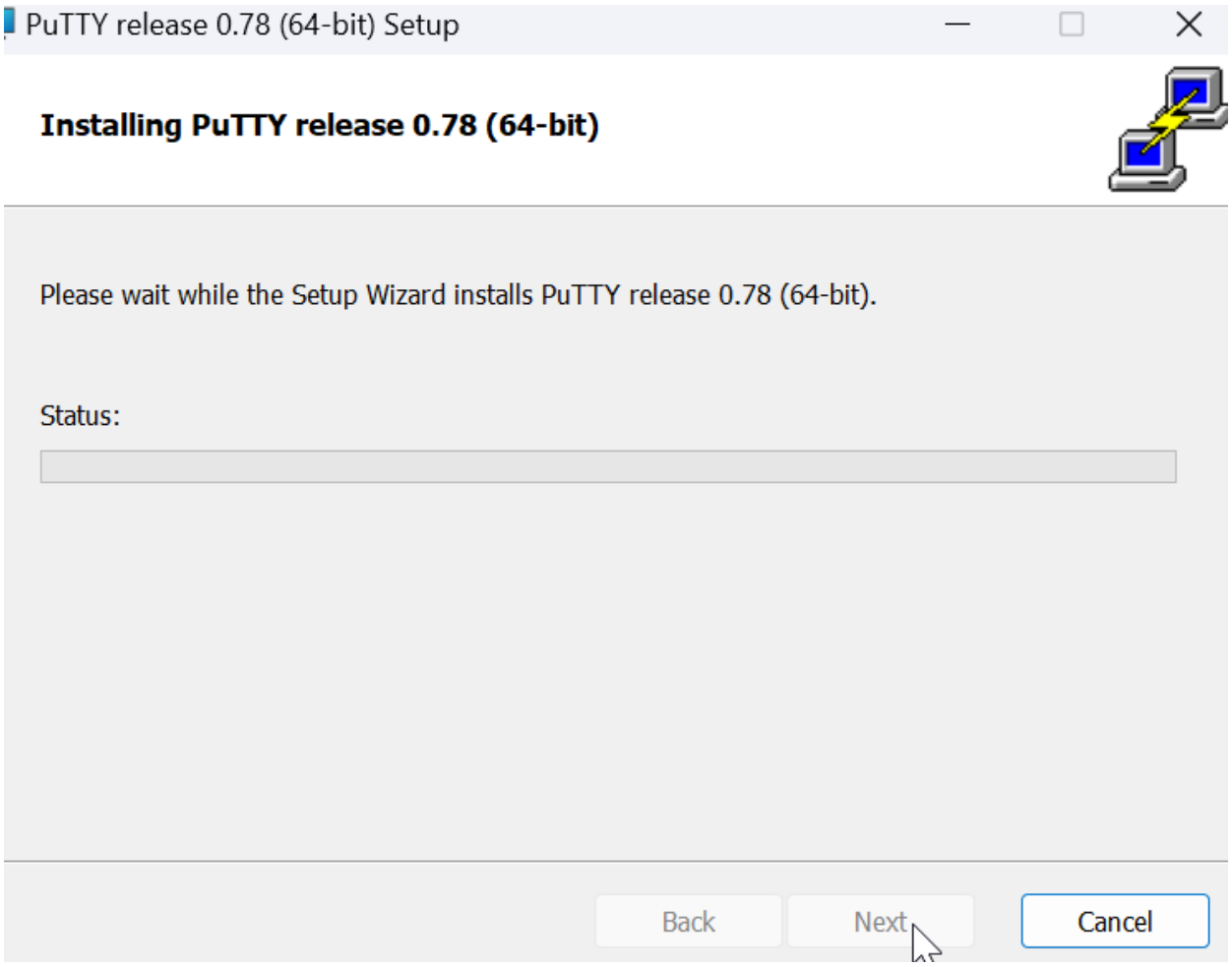
Command used ssh <username>@<ip_address> -p<port_number> [port number is 22 for ssh by

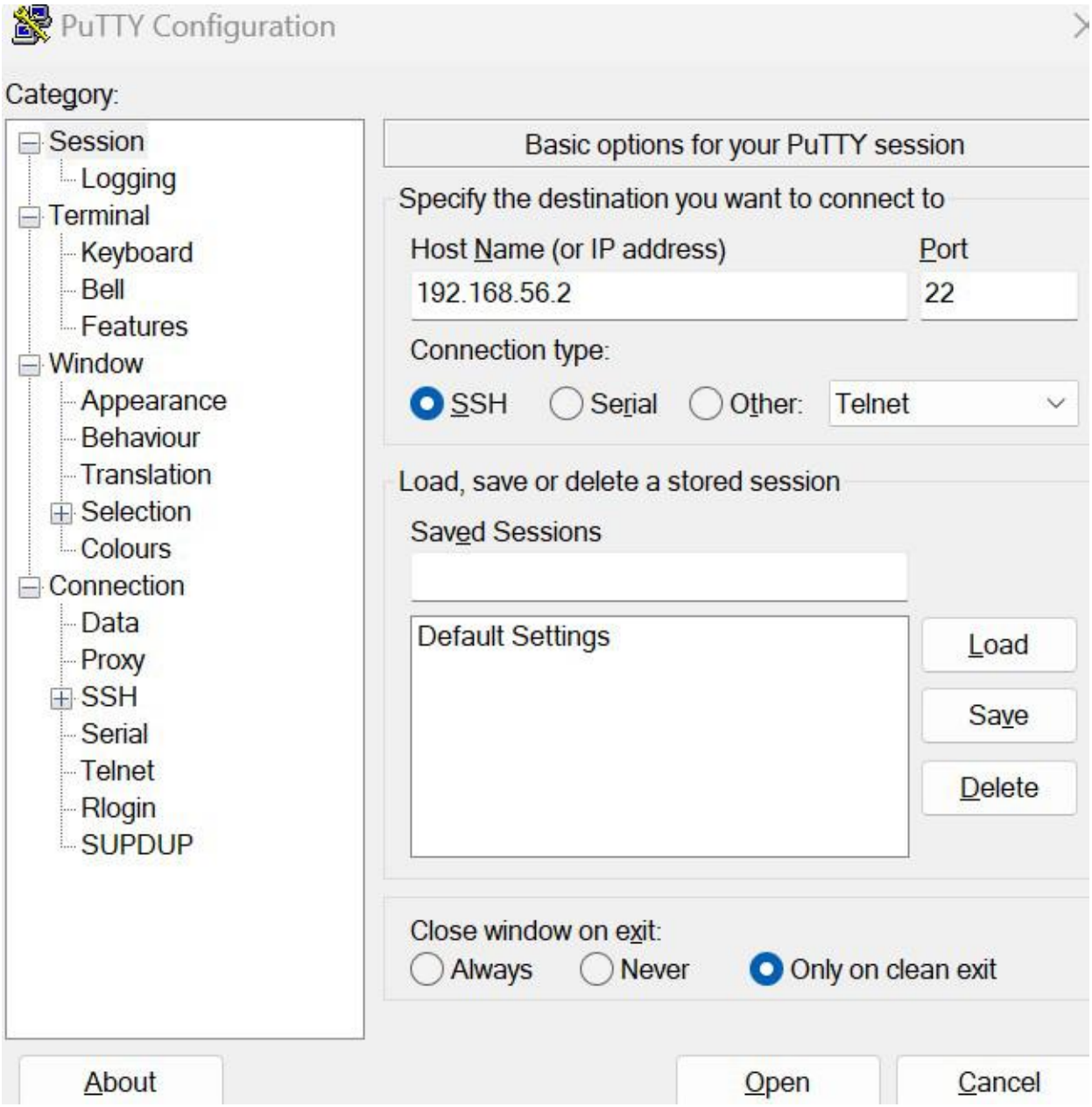
default].



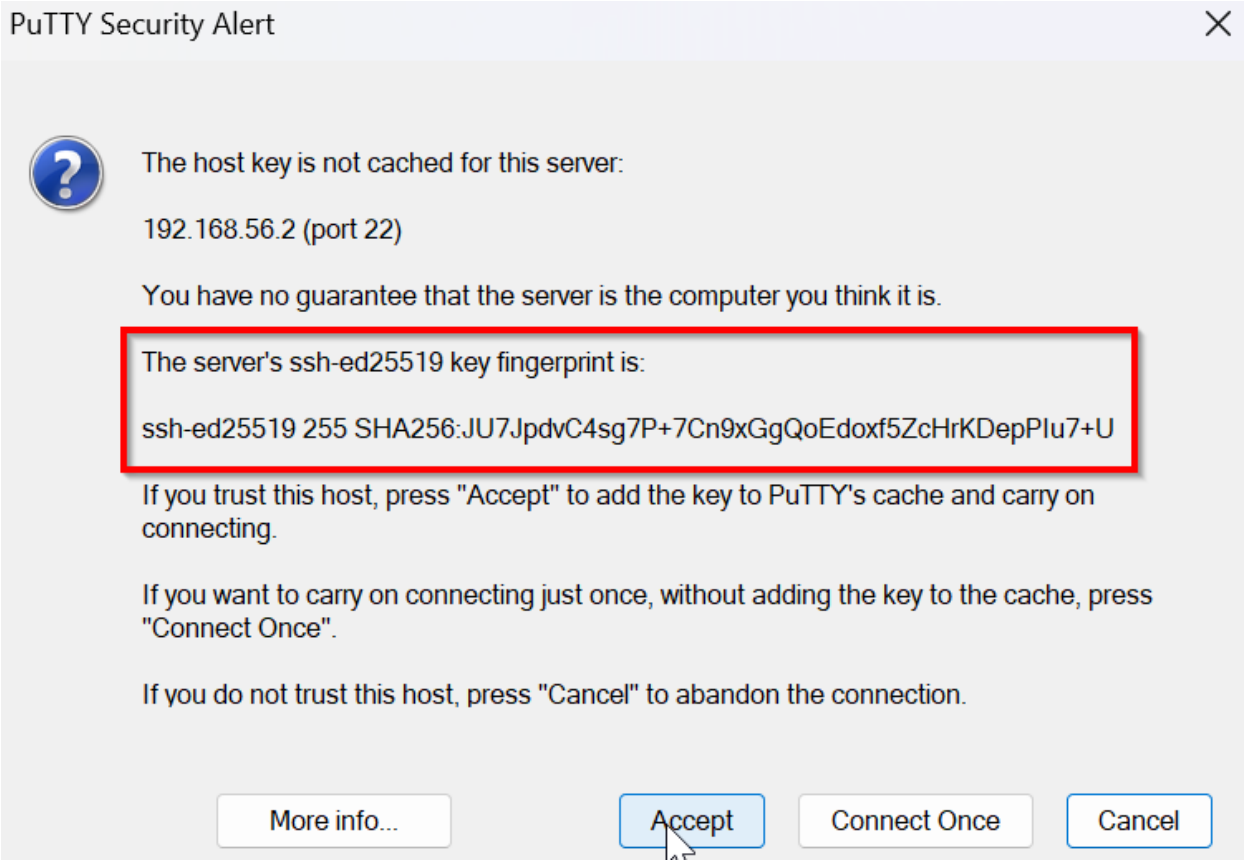
SSH login using

PuTTy: Installation :


PuTTY release 0.78 (64-bit) Setup
Installing PuTTY release 0.78 (64-bit)
Please wait while the Setup Wizard installs PuTTY release 0.78 (64-bit).
Status:
Back
Next
Cancel



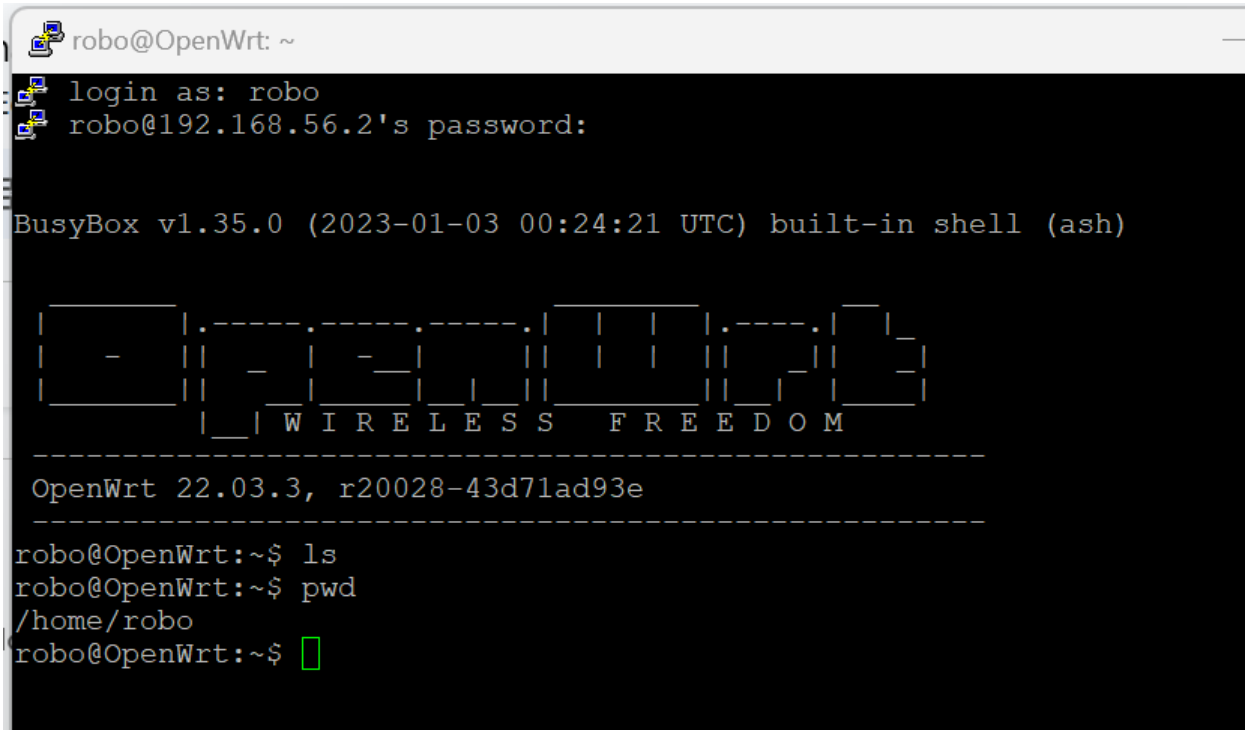
Let’s click on open the ssh connection, and read and accept the alert generated by the PuTTY client. Here OpenWRT is serving as the server.



After accepting the connection, we are prompted with a login screen.

Here enter the credentials for the user you want to login.

robo is the user in our case.



• Explain why key-based authentication can be more secure than password-based authentication when connecting to a SSH server (e.g. on OpenWRT, GitHub or Azure).

Key-based authentication method is more secure than password based authentication in situations of connecting to an SSH server because:

1. It has a stronger and even Complex password.
2. No concept of Password Sharing or reuse.
3. They are tough against brute force attacks.
4. Have Enhanced Security features like passphrase protection and key revocation.