Data Analysis Report

Course Details:

22603VIC Certificate IV in Cyber Security

VU23216 | Perform basic cyber security data analysis

VU23218 | Implement network security infrastructure for an organisation

Assessment Task 2: Project

Student Details:

Student Name: [Md Salam]

Student Number: [881829116]

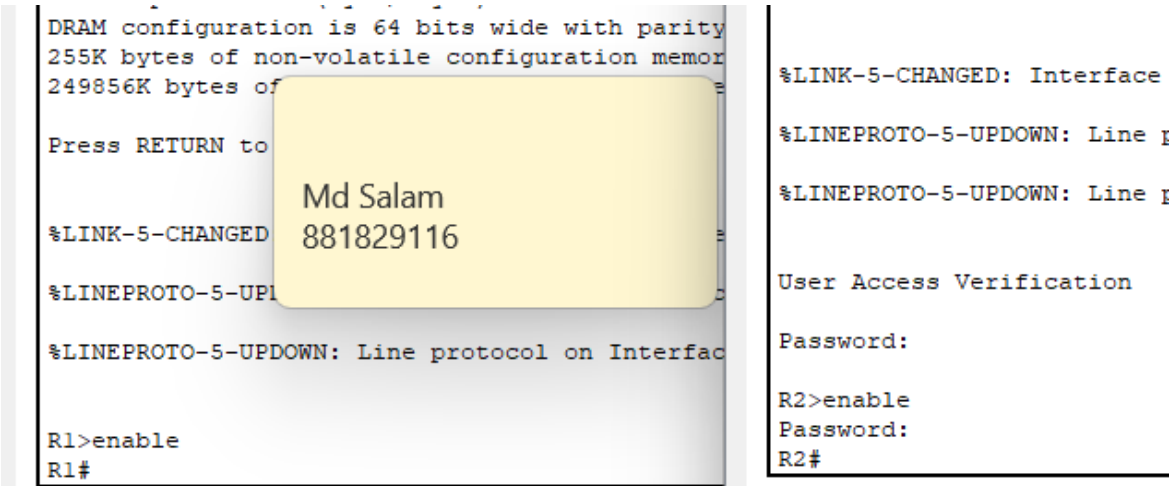
Part 1: Task 1 – Configure and secure network devices

Document the testing completed below. Where directed, TAFE digital students to provide screenshots of completed steps. On-campus students may demonstrate the corresponding step in class, with the assessor signing off the step.

Step 1: Configure the routers

1.1. Name the routers **R1** and **R2:**

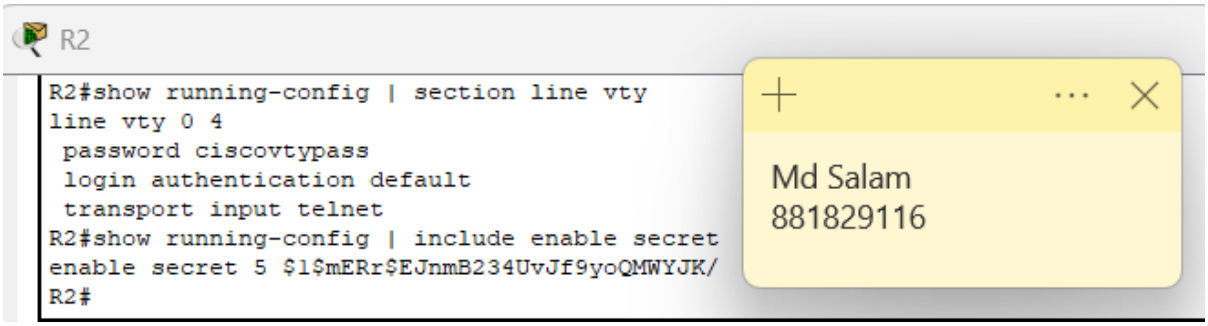
Refer to Md_Salam_881829116_Part1_Task1_PacketTracer.pka file

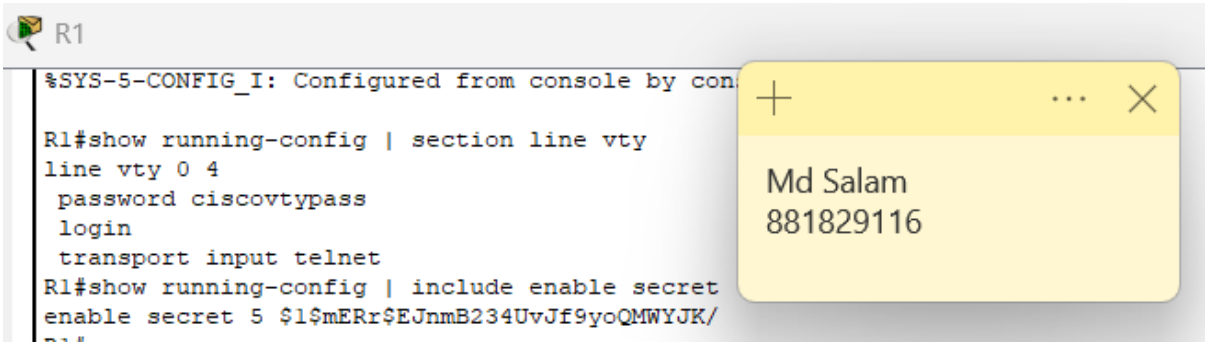


Assessor Sign-off (On-campus students):

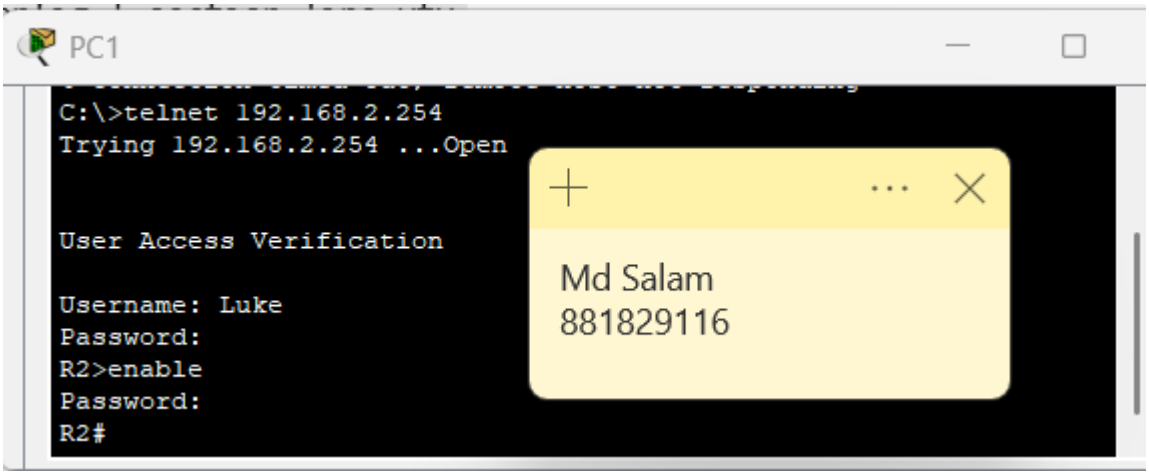
1.2. Secure the device connections such as **console**, **vty** and **aux** and provide evidence this has been completed:

Refer to Md_Salam_881829116_Part1_Task1_PacketTracer.pka file





Successfully connected from PC1 to R2 using Telnet:



Assessor Sign-off (On-campus students):

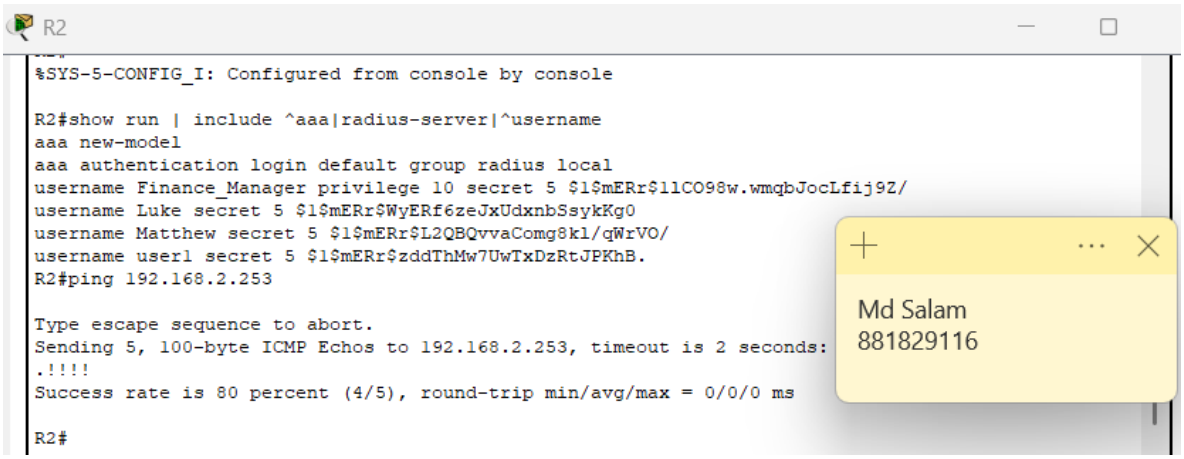
1.3. Enforce network access controls for employees to carry out their roles by:

a) assigning privileges based on their role

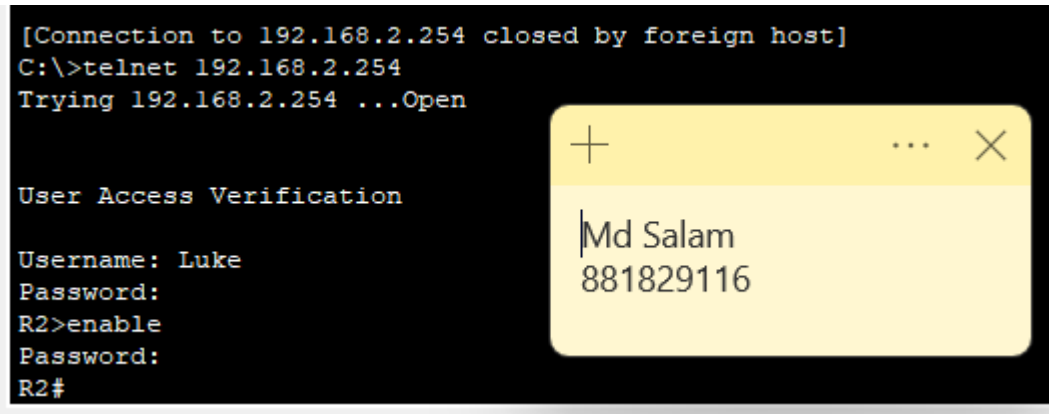
- configuring network access control by implementing AAA authentication using a Radius server to authenticate the following users:HR_Manager (Matthew)
- Finance_Manager (Luke).

Provide evidence of the above:

Refer to Md_Salam_881829116_Part1_Task1_PacketTracer.pka file



Ping from router to Radius server (successful)



Assessor Sign-off (On-campus students):

1.4. Provide config file or screenshot of running configuration for each router accompanying the config text as part of the report submission using procedures as outlined in the recommended lab guidelines manuals:

Refer to Md_Salam_881829116_Part1_Task1_PacketTracer.pka file

```
R1#
R1#show running-config | include hostname|enable secret|password
no service password-encryption
hostname R1
enable secret 5 $1$mERr$EJnmB234UvJf9yoQMWYJK/
 password ciscoconpass
 password ciscoconpass
 password ciscovtypass
R1#show running-config | section line
line con 0
 password ciscoconpass
 login
line aux 0
 password ciscoconpass
 login
line vty 0 4
 password ciscovtypass
 login
```

Md Salam
881829116

```
R2#show running-config | include ^aaa|radius-server|^username|line vty
aaa new-model
aaa authentication login default local
username Finance_Manager privilege 10 secret 5 $1$mERr$1lCO98w.wmqbJocLfij9Z/
username Luke secret 5 $1$mERr$WyERf6zeJxUdxnbSsykKg0
username Matthew secret 5 $1$mERr$L2QBQvvaComg8kl/qWrVO/
username user1 secret 5 $1$mERr$zddThMw7UwTxDzRtJPKhB.
line vty 0 4
R2#
```

Md Salam
881829116

```
!
radius server 192.168.2.253
 address ipv4 192.168.2.253 auth-port 1645
 key RADIUS
!
!
!
line con 0
 password ciscoconpass
!
line aux 0
!
line vty 0 4
 login authentication default
 transport input telnet
!
!
!
end


R2#
```

Md Salam
881829116

Assessor Sign-off (On-campus students):

Step 2: Configure the WLAN

2.1. Demonstrate authentication and association methods using security protocols (for example, WEP, WPA or WPA2).

A secure WLAN named **"Staff"** was configured on the **Wireless LAN Controller (WLC-1)** using **WPA2-PSK (AES)** encryption.
The pre-shared key **Cisco123** provides confidentiality and integrity for employee wireless communication.

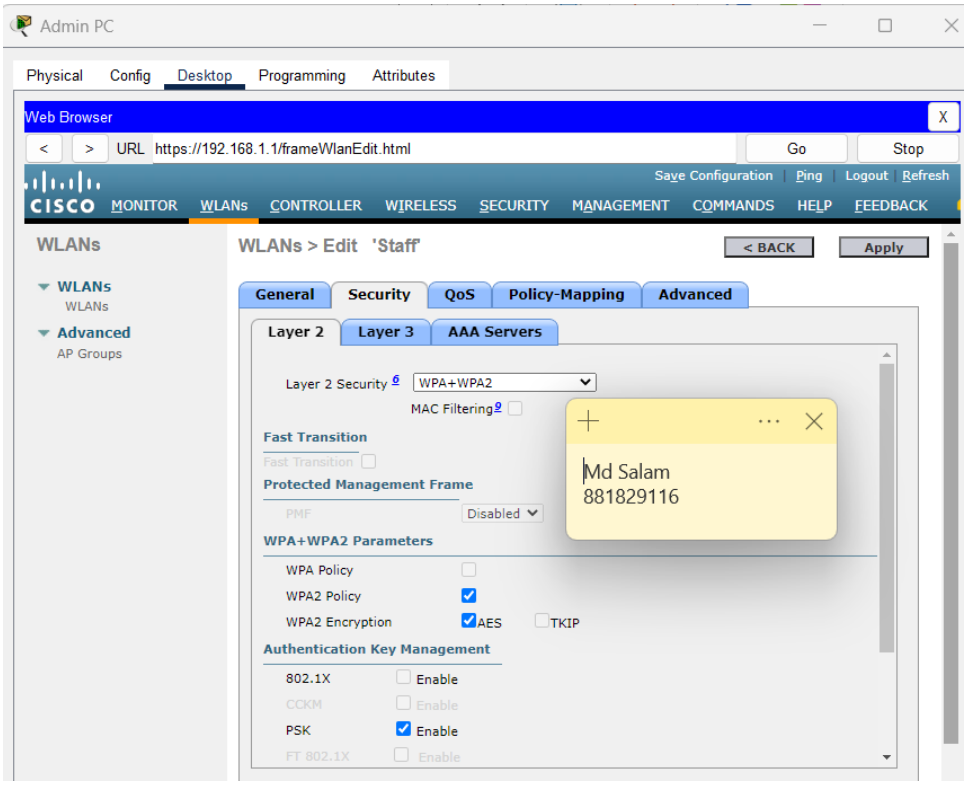
A second WLAN, **"Guest,"** was created with **open authentication** to demonstrate unsecured network association for visitors.
Both WLANs were broadcast by LAP-1 and LAP-2 and managed centrally by WLC-1.

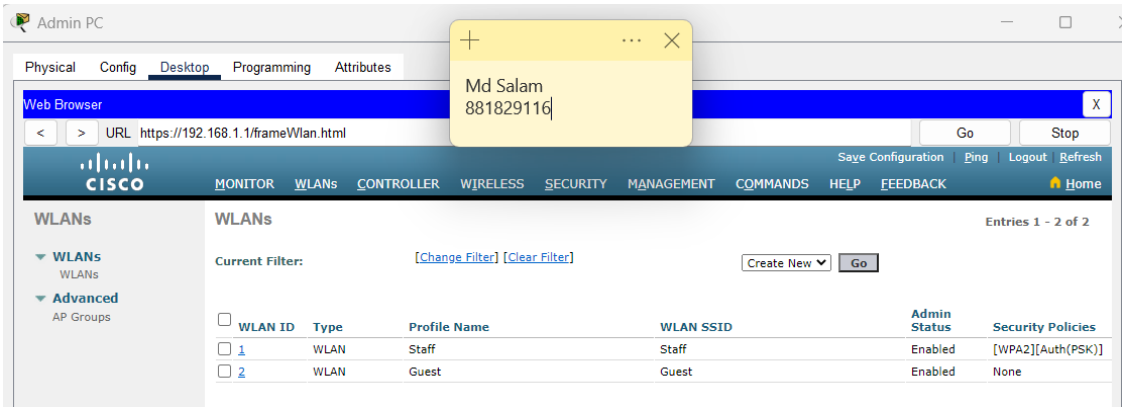
Verification

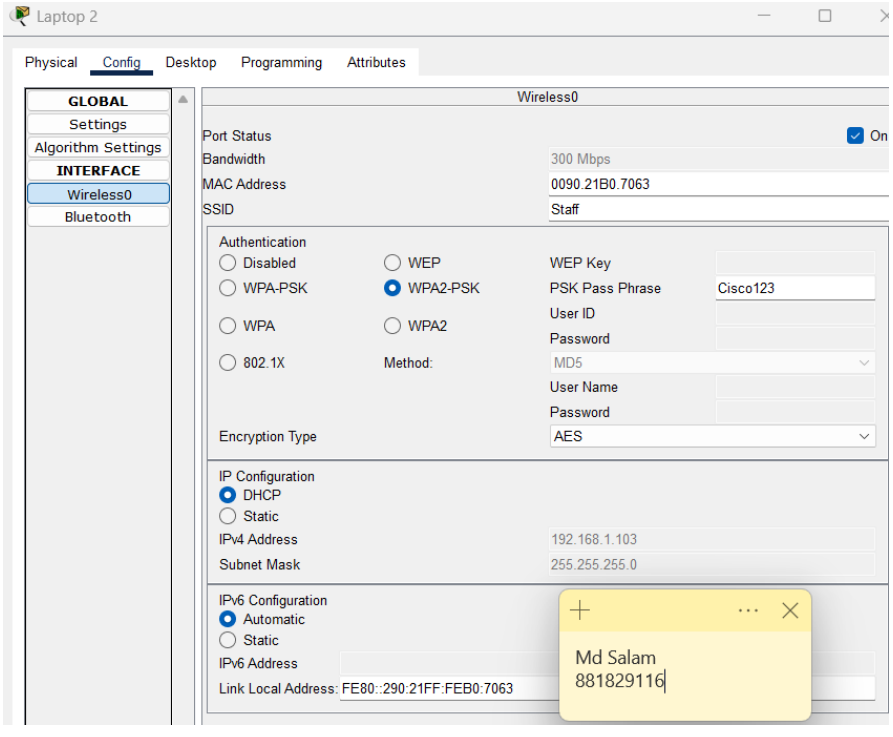
- **Laptop 2 (Staff):** connected successfully to *SSID = Staff* using WPA2-PSK (AES), receiving IP 192.168.1.101 from DHCP (192.168.1.253).
- **Laptop 1 (Guest):** connected to *SSID = Guest* (open), receiving IP 192.168.1.106 from the same DHCP server.
- **Ping tests:** confirmed connectivity to WLC (192.168.1.1) and DHCP/DNS server (192.168.1.253).

Provide evidence of the above.

Refer to Md_Salam_881829116_Part1_Task1_PacketTracer.pka file







Assessor Sign-off (On-campus students):

2.2. Use tools like packet tracer, NetStumbler, or Wireshark to discover details about available WLANs.

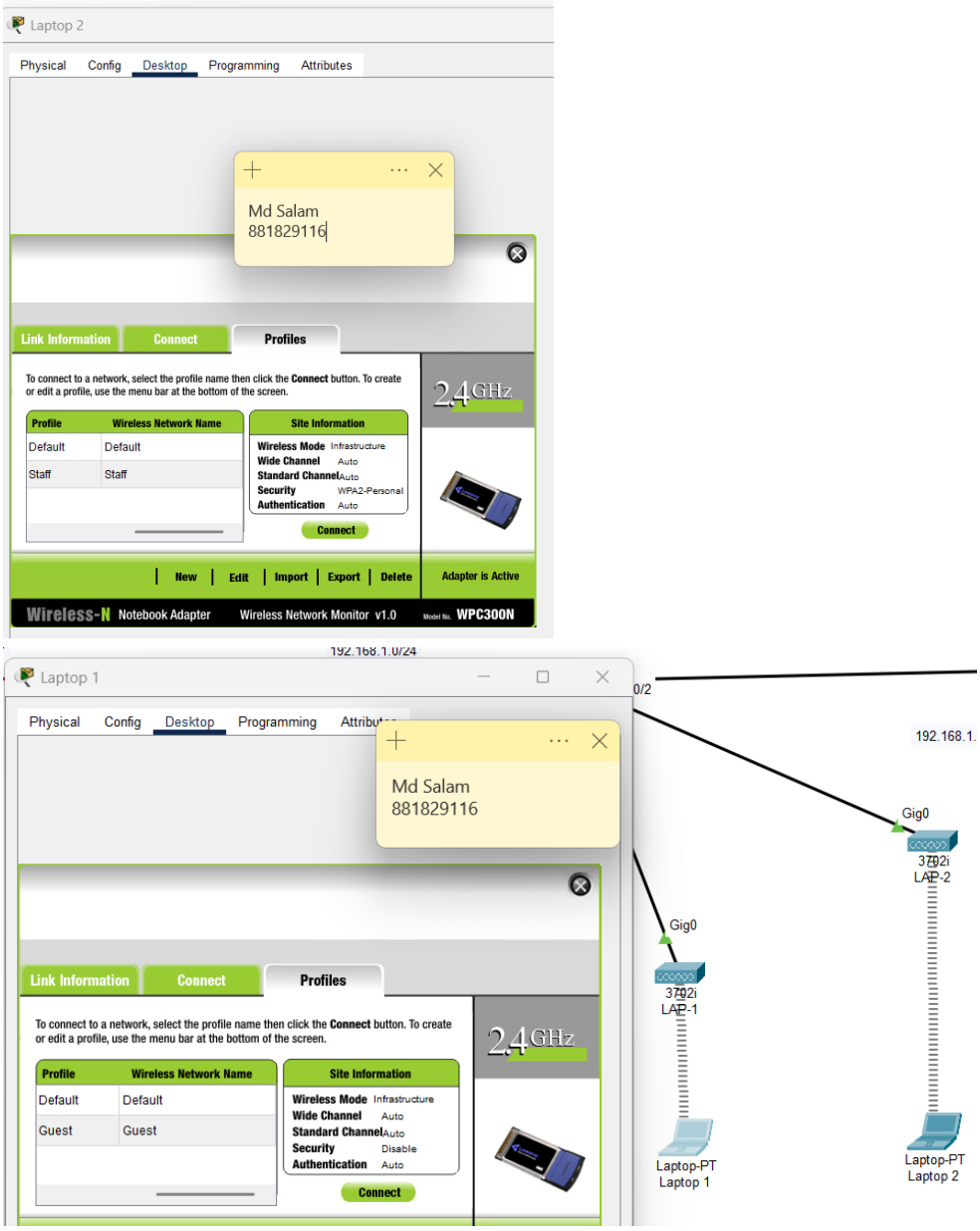
The **Wireless Network Monitor** tool in Packet Tracer was used to simulate WLAN discovery, similar to utilities such as **NetStumbler** or **Wireshark** in real environments. The scan detected the SSIDs **"Staff"** and **"Guest,"** including their channel, signal strength, and security types.

Findings

- *Staff SSID* – WPA2-PSK (AES) secured network
- *Guest SSID* – Open (unsecured) network
- Both SSIDs broadcast by LAP-1 and LAP-2 and managed by WLC-1.

Provide evidence of the above.

Refer to Md_Salam_881829116_Part1_Task1_PacketTracer.pka file



Assessor Sign-off (On-campus students):

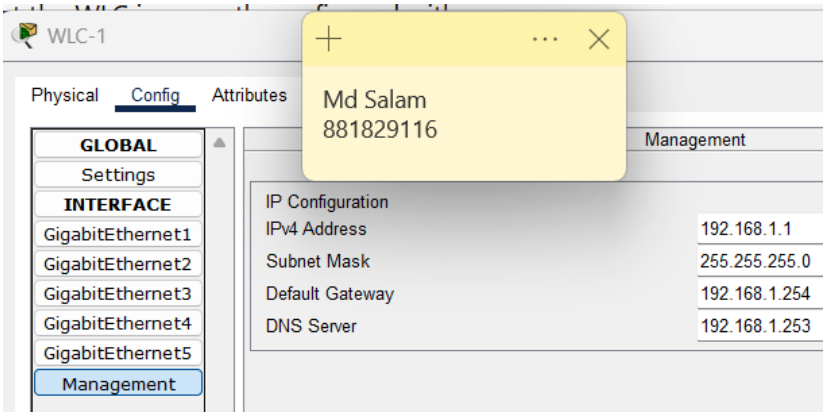
2.3. Develop a WLAN security checklist

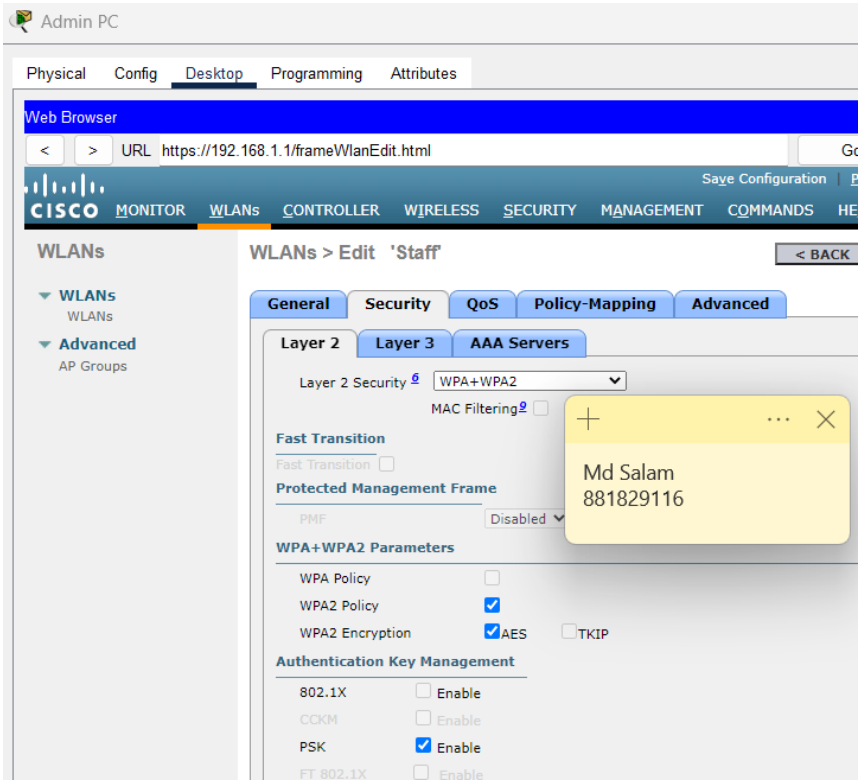
Security Element	Description / Purpose	Configured	Comments
SSID Broadcasting	SSIDs “Staff” and “Guest” visible for client access	✅	Required for device discovery
Authentication	WPA2-PSK (AES) for Staff	✅	Strong encryption for internal users
Guest Access	Open authentication	✅	Internet-only, no LAN access
Passphrase Strength	“Cisco123” (demo key)	⚠️	Use longer, complex key in production
Encryption Type	AES	✅	Industry standard for WPA2
DHCP Protection	Central DHCP (192.168.1.253)	✅	Prevents rogue servers
Access Point Control	Managed via WLC (192.168.1.1)	✅	Centralised configuration
Device Isolation	Separate SSIDs for Staff and Guest	✅	Limits broadcast domains
Firmware / Patch Updates	Keep WLC & AP firmware current	✅	Minimises vulnerabilities

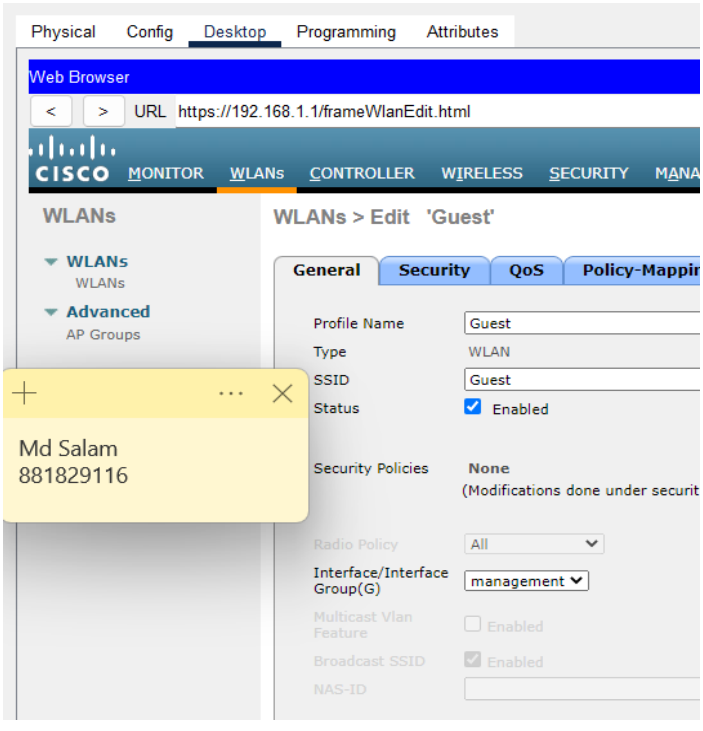
Assessor Sign-off (On-campus students):

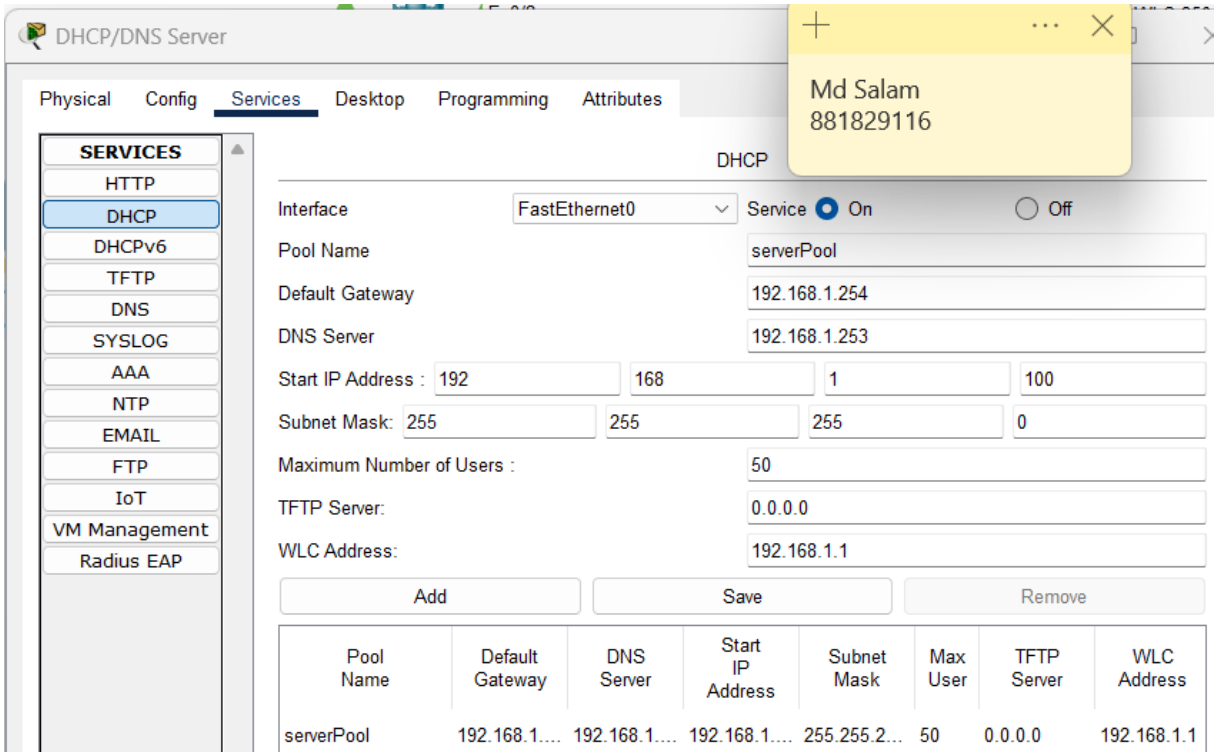
2.4. In the **Data Analysis Report**, provide either a config file or screenshot of the setup and configuration for the WLAN device.

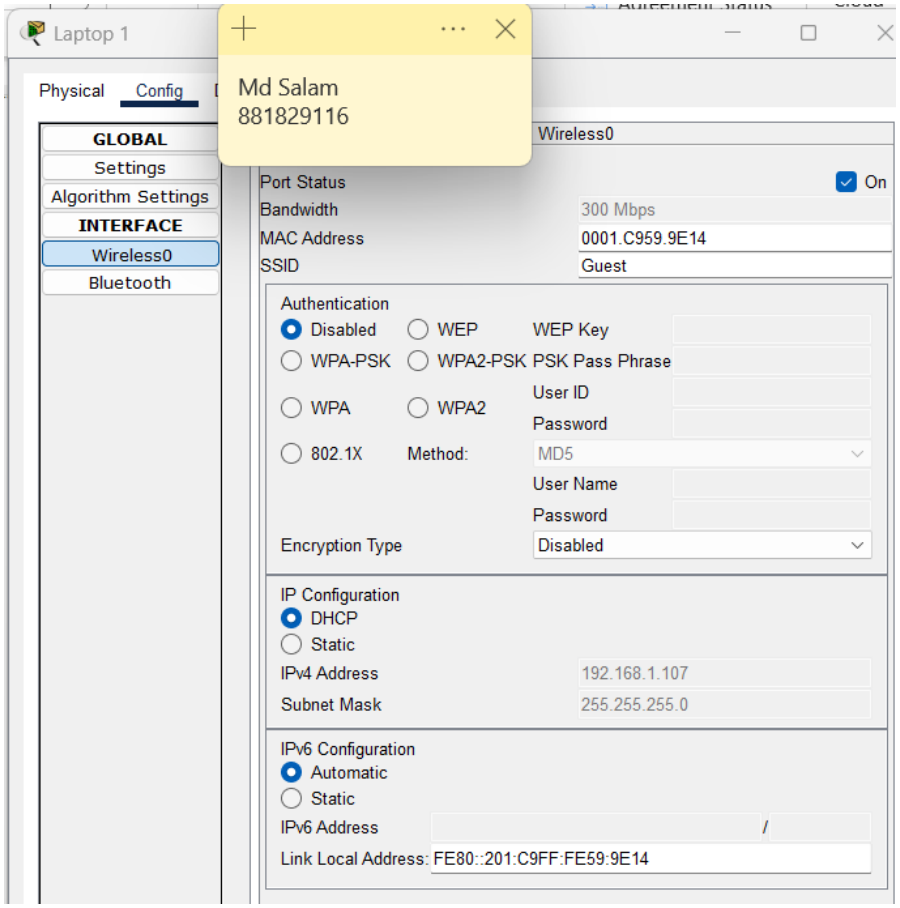
Refer to Md_Salam_881829116_Part1_Task1_PacketTracer.pka file

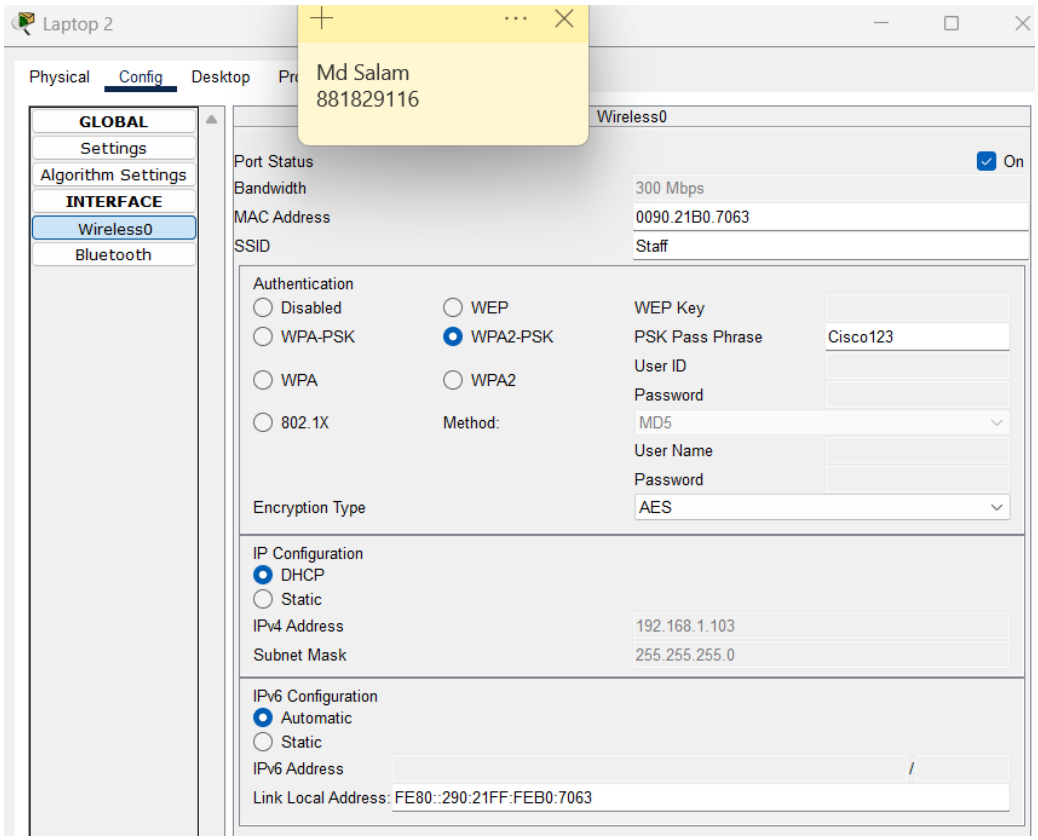


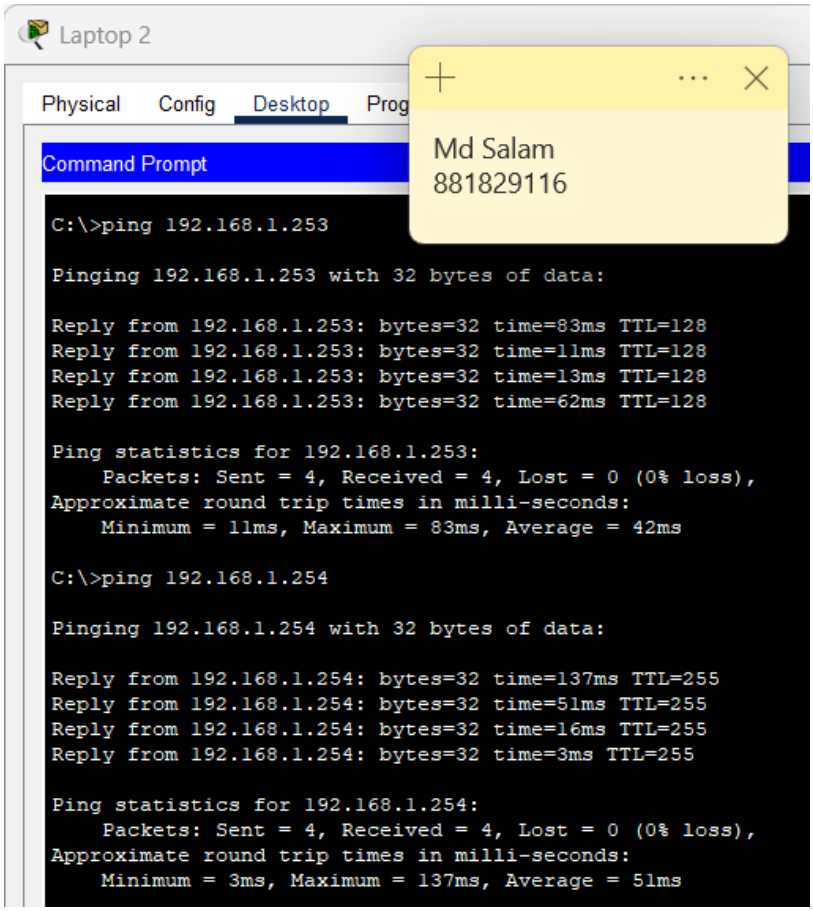





DHCP/DNS Server
Md Salam
881829116
Physical
Config
Services
Desktop
Programming
Attributes
SERVICES
HTTP
DHCP
DHCPv6
TFTP
DNS
SYSLOG
AAA
NTP
EMAIL
FTP
IoT
VM Management
Radius EAP
DHCP
Interface
FastEthernet0
Service
On
Off
Pool Name
serverPool
Default Gateway
192.168.1.254
DNS Server
192.168.1.253
Start IP Address :
192
168
1
100
Subnet Mask:
255
255
255
0
Maximum Number of Users :
50
TFTP Server:
0.0.0.0
WLC Address:
192.168.1.1
Add
Save
Remove
Pool Name
Default Gateway
DNS Server
Start IP Address
Subnet Mask
Max User
TFTP Server
WLC Address
serverPool
192.168.1....
192.168.1....
192.168.1....
255.255.2...
50
0.0.0.0
192.168.1.1


Laptop 1
Md Salam
881829116
Physical
Config
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
On
Bandwidth
300 Mbps
MAC Address
0001.C959.9E14
SSID
Guest
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
WPA
WPA2
User ID
Password
802.1X
Method:
MD5
User Name
Password
Encryption Type
Disabled
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.107
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::201:C9FF:FE59:9E14


Laptop 2
Physical
Config
Desktop
Md Salam
881829116
GLOBAL
Settings
Algorithm Settings
INTERFACE
Wireless0
Bluetooth
Wireless0
Port Status
On
Bandwidth
300 Mbps
MAC Address
0090.21B0.7063
SSID
Staff
Authentication
Disabled
WEP
WEP Key
WPA-PSK
WPA2-PSK
PSK Pass Phrase
Cisco123
User ID
WPA
WPA2
Password
802.1X
Method:
MD5
User Name
Password
Encryption Type
AES
IP Configuration
DHCP
Static
IPv4 Address
192.168.1.103
Subnet Mask
255.255.255.0
IPv6 Configuration
Automatic
Static
IPv6 Address
Link Local Address:
FE80::290:21FF:FEB0:7063


Laptop 2
Physical
Config
Desktop
Md Salam
881829116
Command Prompt
C:\>ping 192.168.1.253
Pinging 192.168.1.253 with 32 bytes of data:
Reply from 192.168.1.253: bytes=32 time=83ms TTL=128
Reply from 192.168.1.253: bytes=32 time=11ms TTL=128
Reply from 192.168.1.253: bytes=32 time=13ms TTL=128
Reply from 192.168.1.253: bytes=32 time=62ms TTL=128
Ping statistics for 192.168.1.253:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 11ms, Maximum = 83ms, Average = 42ms
C:\>ping 192.168.1.254
Pinging 192.168.1.254 with 32 bytes of data:
Reply from 192.168.1.254: bytes=32 time=137ms TTL=255
Reply from 192.168.1.254: bytes=32 time=51ms TTL=255
Reply from 192.168.1.254: bytes=32 time=16ms TTL=255
Reply from 192.168.1.254: bytes=32 time=3ms TTL=255
Ping statistics for 192.168.1.254:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 3ms, Maximum = 137ms, Average = 51ms

Assessor Sign-off (On-campus students):

Part 1: Task 2 – Structured and unstructured database setup

Complete the following steps:

2.1. Create two databases: One using **MySQL** and another using **MongoDB**
2.2. Install or connect to each database.
2.3. Create a table within each database.
2.4. Add or insert records or documents in each database.
2.5. Use SQL commands to access the table data to retrieve the records or documents in each database.
2.6. Insert records or documents into each database
2.7. Provide a screenshot of each of the steps completed above for each database.

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.00 sec)

mysql> CREATE DATABASE salam;
Query OK, 1 row affected (0.00 sec)

mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| salam              |
| sys                |
+--------------------+
5 rows in set (0.00 sec)
```

Md Salam
881829116

```
mysql> SHOW TABLES;
+---------------------+
| Tables_in_salam     |
+---------------------+
| vulnerabilities_tbl |
+---------------------+
1 row in set (0.00 sec)

mysql> DESCRIBE vulnerabilities_tbl;
+----------------+------------------+------+-----+---------+----------------+
| Field          | Type             | Null | Key | Default | Extra          |
+----------------+------------------+------+-----+---------+----------------+
| _id            | int(10) unsigned | NO   | PRI | NULL    | auto_increment |
| aNumber        | varchar(3)       | NO   |     | NULL    |                |
| type           | varchar(50)      | NO   |     | NULL    |                |
| threatAgent    | varchar(50)      | NO   |     | NULL    |                |
| exploitability | varchar(2)       | NO   |     | NULL    |                |
| prevalence     | varchar(2)       | NO   |     | NULL    |                |
| detectability  | varchar(2)       | NO   |     | NULL    |                |
| techImpact     | varchar(2)       | NO   |     | NULL    |                |
| busImpact      | varchar(50)      | NO   |     | NULL    |                |
+----------------+------------------+------+-----+---------+----------------+
9 rows in set (0.02 sec)
```

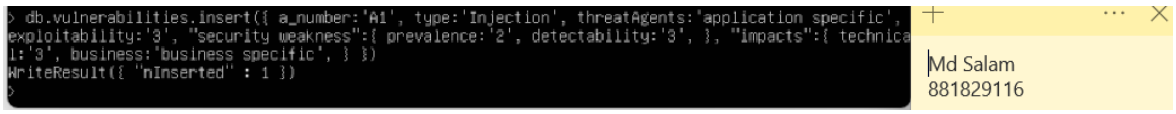
Md Salam
881829116

```
mysql> SELECT * FROM vulnerabilities_tbl;
+-----+---------+-----------------------+-------------------+--------------+------------+
| _id | aNumber | type                  | threatAgent       | exploitability | prevalence |
detectability | techImpact | busImpact        |
+-----+---------+-----------------------+-------------------+--------------+------------+
-------------+------------+------------------+
|   1 | A1      | Injection             | Application specific | 3            | 2          |
3             | 3          | Business specific |
|   2 | A7      | Cross-Site Scripting (XSS) | Application specific | 3            | 3          |
3             | 2          | Business specific |
|   3 | A8      | Insecure Deserialization | Application specific | 1            | 2          |
2             | 3          | Business specific |
+-----+---------+-----------------------+-------------------+--------------+------------+
-------------+------------+------------------+
3 rows in set (0.00 sec)

mysql> SELECT * FROM vulnerabilities_tbl WHERE exploitability = 3;
+-----+---------+-----------------------+-------------------+--------------+------------+
| _id | aNumber | type                  | threatAgent       | exploitability | prevalence |
detectability | techImpact | busImpact        |
+-----+---------+-----------------------+-------------------+--------------+------------+
-------------+------------+------------------+
|   1 | A1      | Injection             | Application specific | 3            | 2          |
3             | 3          | Business specific |
|   2 | A7      | Cross-Site Scripting (XSS) | Application specific | 3            | 3          |
3             | 2          | Business specific |
+-----+---------+-----------------------+-------------------+--------------+------------+
-------------+------------+------------------+
2 rows in set (0.00 sec)

mysql> _
```

Md Salam
881829116



Assessor Sign-off (On-campus students):

Part 1: Task 3 – Secure network and endpoints

Document the data analysis completed below. Where directed, TAFE digital students to provide screenshots of completed steps. On-campus students may demonstrate the corresponding step in class, with the assessor signing off the step.

3.1. Describe between 2-4 reasons why implementing firewall technology is important.

Provide your answer below (maximum 200 words). You may use bullet points:

- **Prevents unauthorised access:** A firewall acts as a protective barrier between trusted internal networks and untrusted external environments such as the internet. It blocks unauthorised or malicious traffic from entering the system, reducing the risk of data breaches and network compromise.
- **Controls and filters network traffic:** Firewalls manage how data moves between networks by filtering packets based on IP addresses, ports, and protocols. This ensures that only safe, approved communication is allowed, while suspicious or irrelevant connections are denied.
- **Protects against malware and exploitation:** By inspecting incoming and outgoing data, firewalls can detect and prevent malicious downloads, remote attacks, and exploitation attempts. They also restrict compromised systems from communicating externally, helping contain threats.
- **Provides monitoring, logging, and auditing:** Firewall logs record every allowed or denied connection, giving security teams valuable insight into attempted intrusions, configuration issues, and traffic patterns. This information supports proactive threat detection and network optimisation.

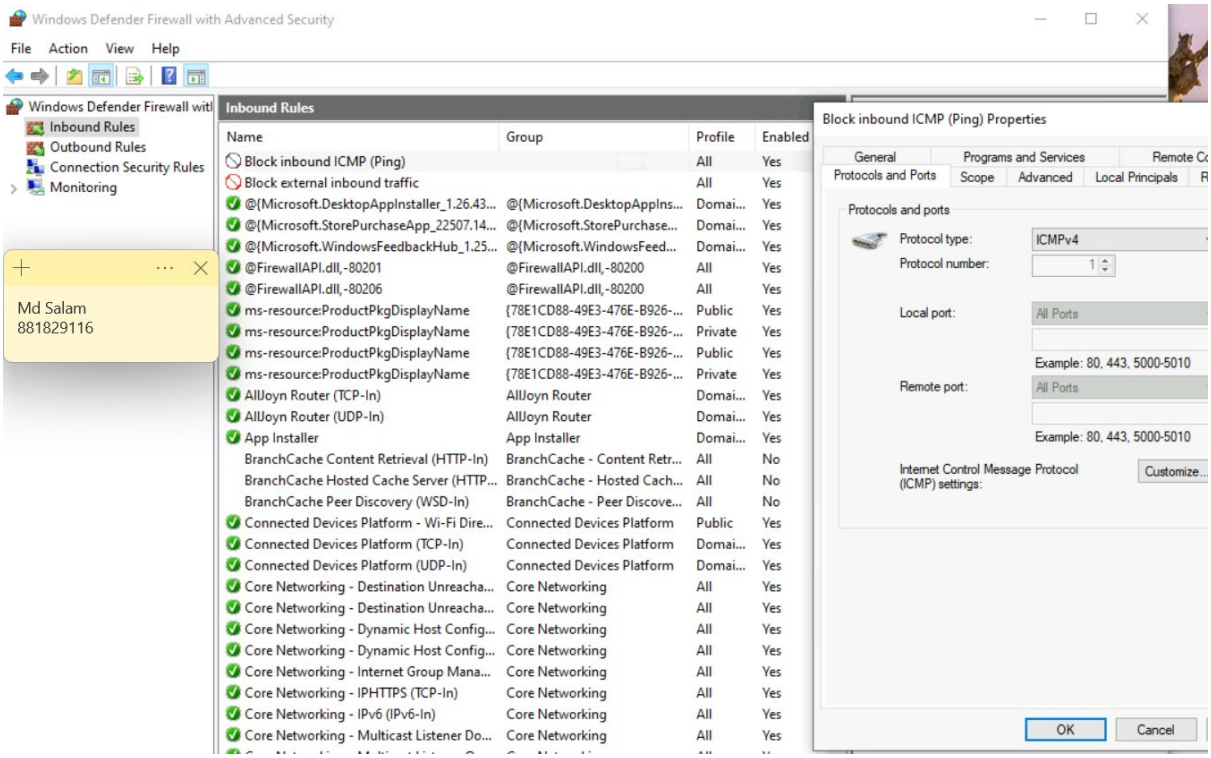
In summary, firewall technology is vital for maintaining network integrity, confidentiality, and availability by enforcing access control, preventing intrusions, and providing continuous visibility into network activity.

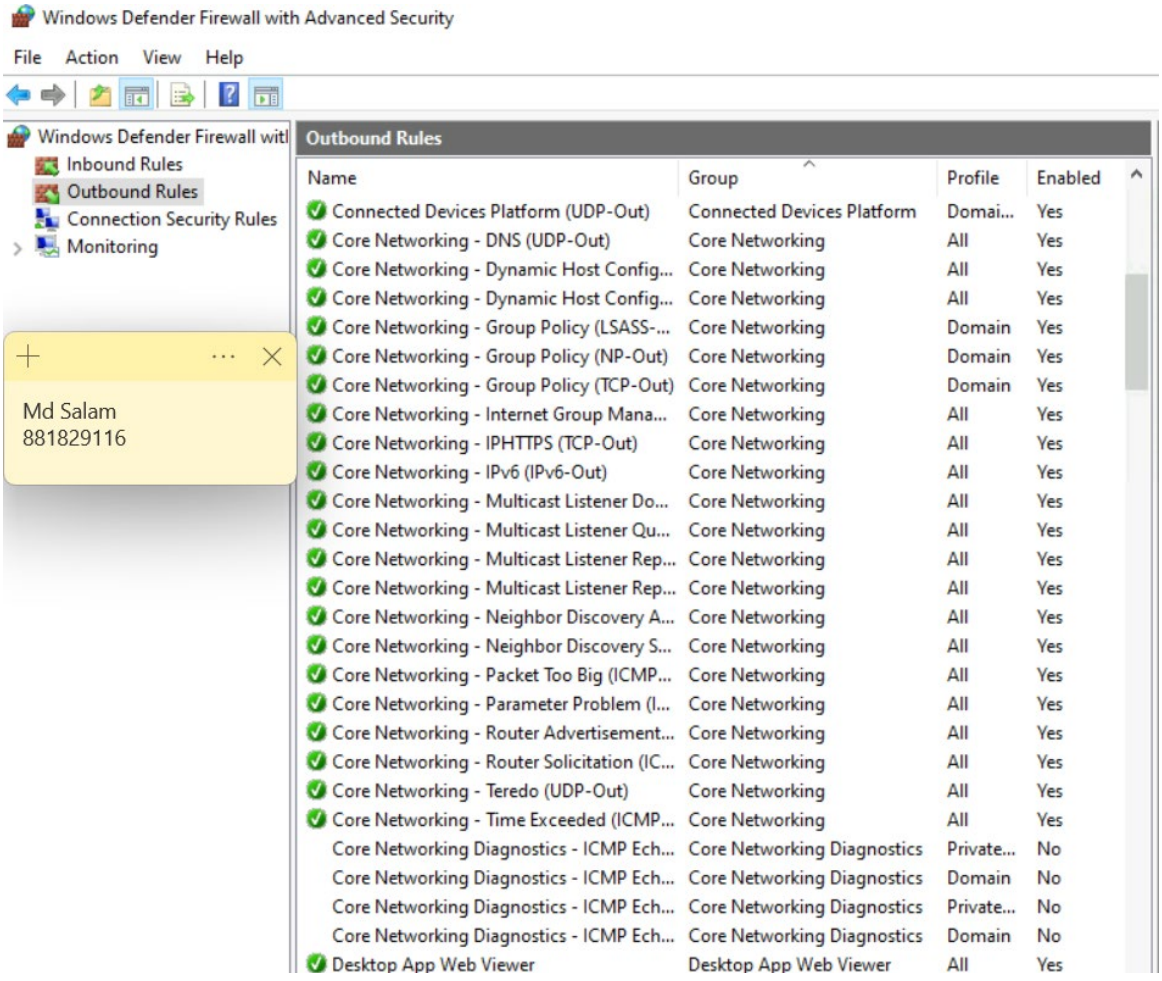
Assessor Sign-off (On-campus students):

3.2. Configure the firewall zones to implement basic packet filtering, allowing internal hosts access to external resources, and blocking external hosts from accessing internal resources (using the procedures outlined in the recommended lab)

Provide evidence this step is completed:

Created new Inbound rule Block inbound ICMP (Ping) to block ICMP (Ping) from external hosts. But outbound allowed.



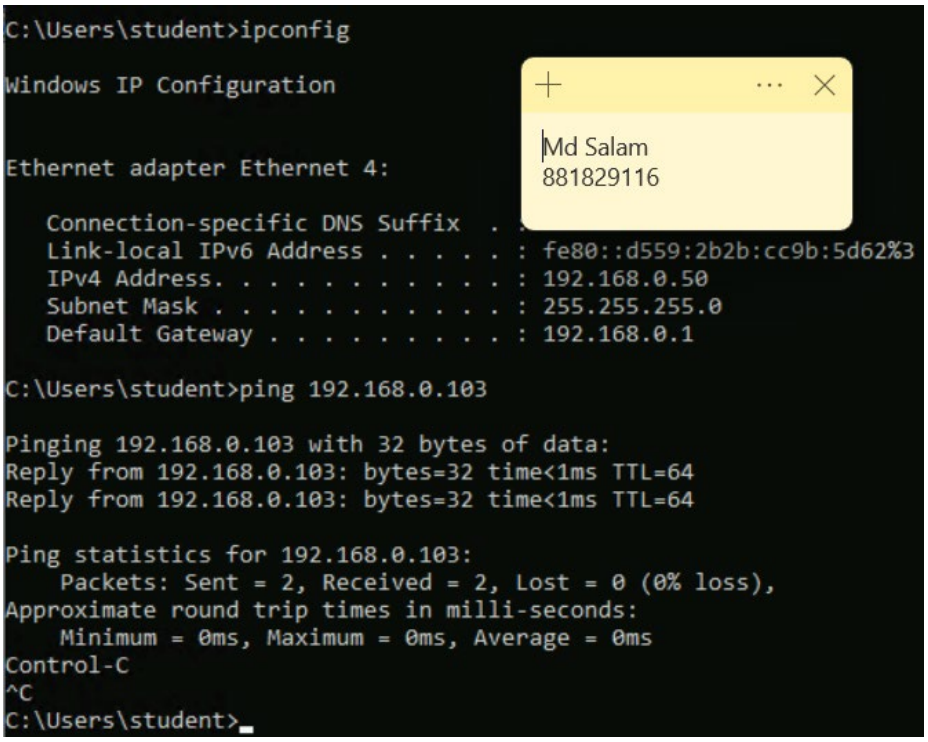


Assessor Sign-off (On-campus students):

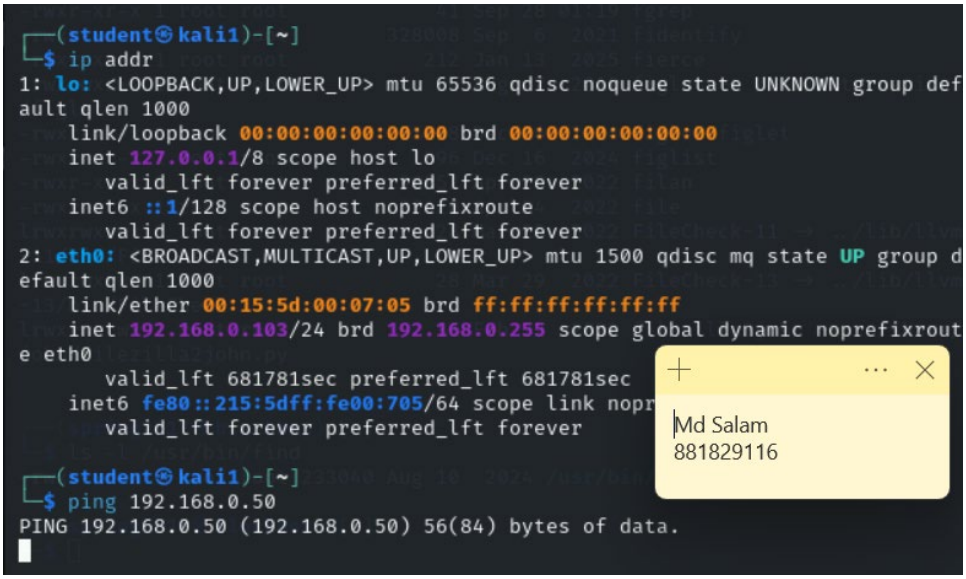
3.3. Verify firewall functionality from internal and external hosts (using the procedures outlined in the recommended lab).

Provide evidence this step is completed:

Ping from Windows10 to Kali succeeds → outbound traffic allowed



Ping from Kali to Windows10 fails → inbound traffic blocked



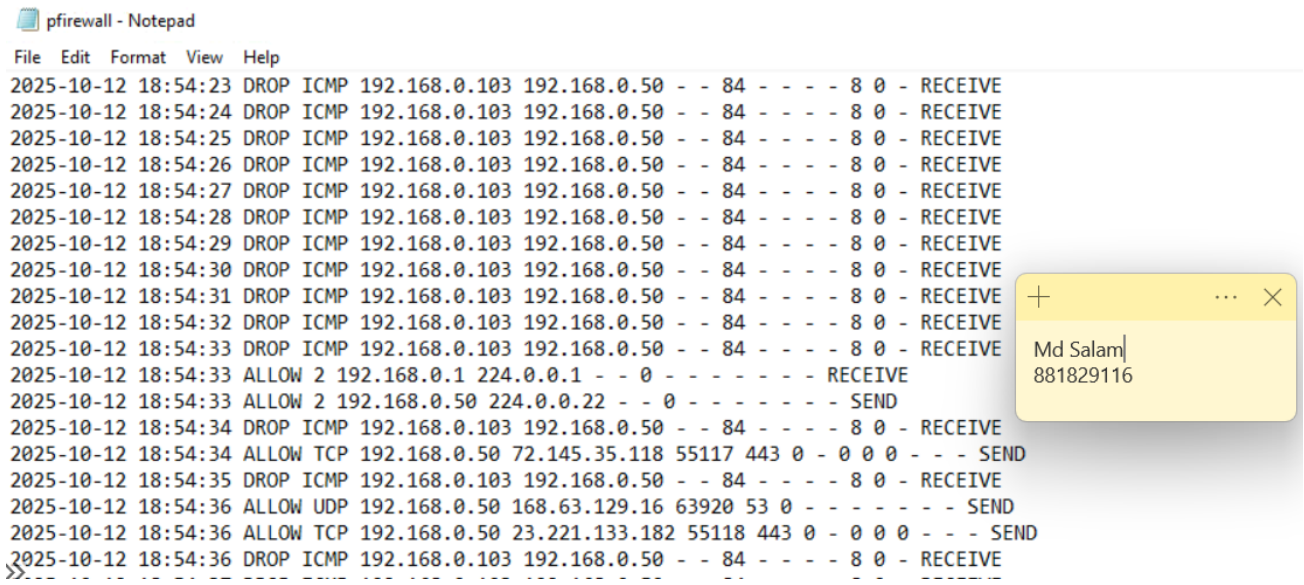
Assessor Sign-off (On-campus students):

3.4. Conduct a log analysis to establish if data coming through the firewall was permitted or denied (using the procedures outlined in the recommended lab).

Provide evidence this step is completed:

Screenshot shows the Windows Firewall log (pfirewall.log) entries with:

- Multiple lines marked **DROP ICMP** from Kali **192.168.0.103 → Windows10 192.168.0.50** → confirms inbound ping requests from the Kali host were blocked.
- Several **ALLOW TCP/UDP** lines (e.g., to ports 80, 443, 53) → confirms that outbound web and DNS traffic from Windows is still permitted.

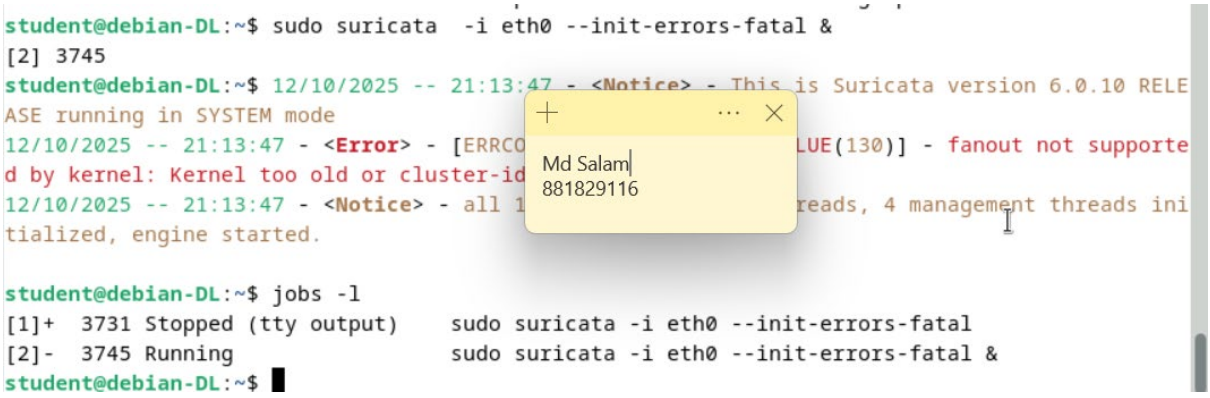


Assessor Sign-off (On-campus students):

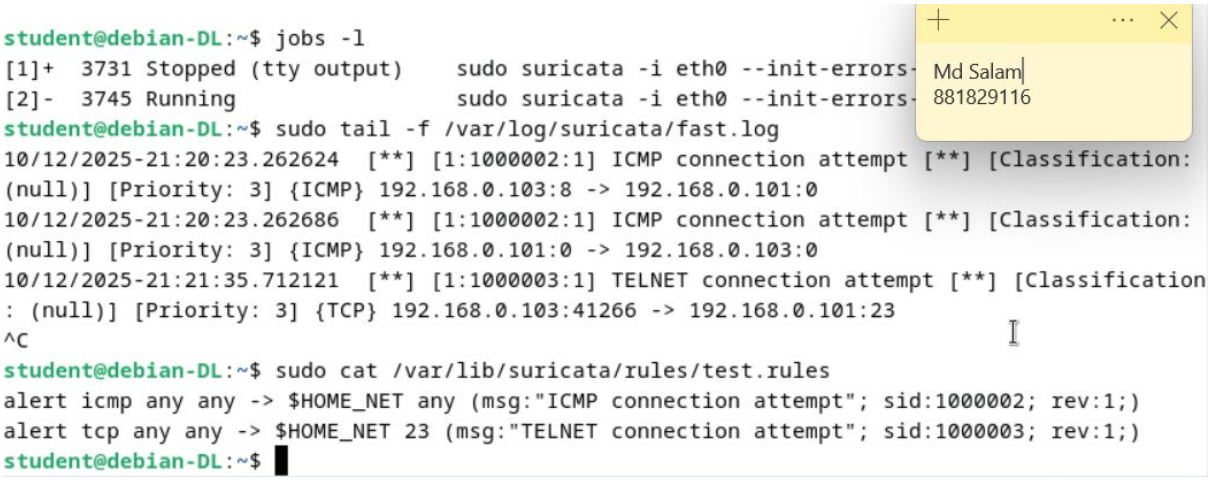
3.5. Install **Suricata** (a network monitoring tool) and its required packages (features) and define rules to either block or log any attempts to access malicious traffic across the entire company.

Provide evidence this step is completed:

Terminal showing sudo suricata -i eth0 … running:



Output of fast.log with alert lines and contents of test.rules file.



Assessor Sign-off (On-campus students):

Part 1: Task 4 – Install and configure proxy server

Document the data analysis completed below. Where directed, TAFE digital students to provide screenshots of completed steps. On-campus students may demonstrate the corresponding step in class, with the assessor signing off the step.

4.1. Install and configure a proxy server (for example, Squid) and block specific websites (for example google.com), using procedures as outlined in the recommended lab.

4.2. In the **Data Analysis Report**, provide a screenshot of the proxy configuration page blocking the website.

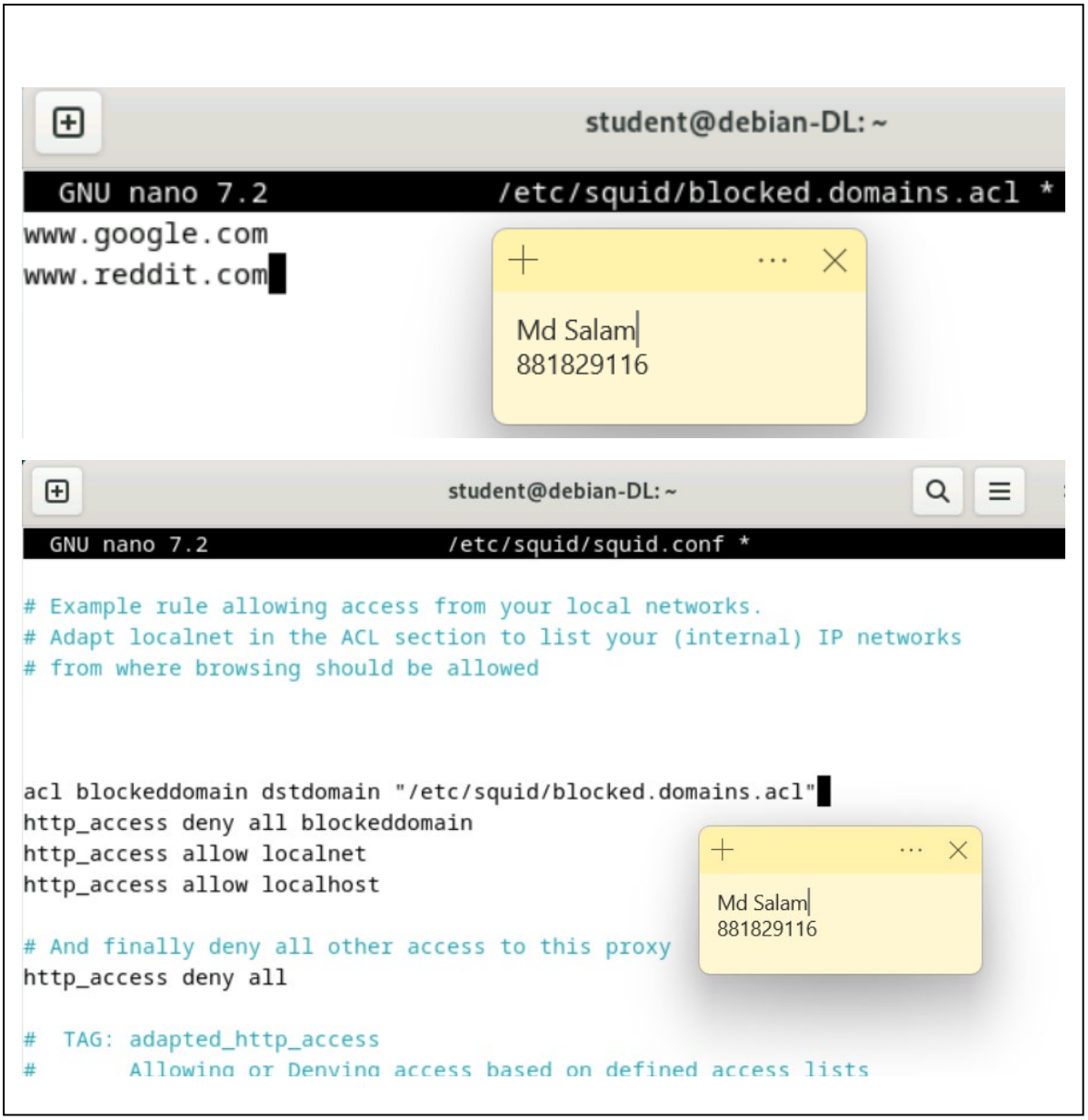
Provide evidence this step is completed:

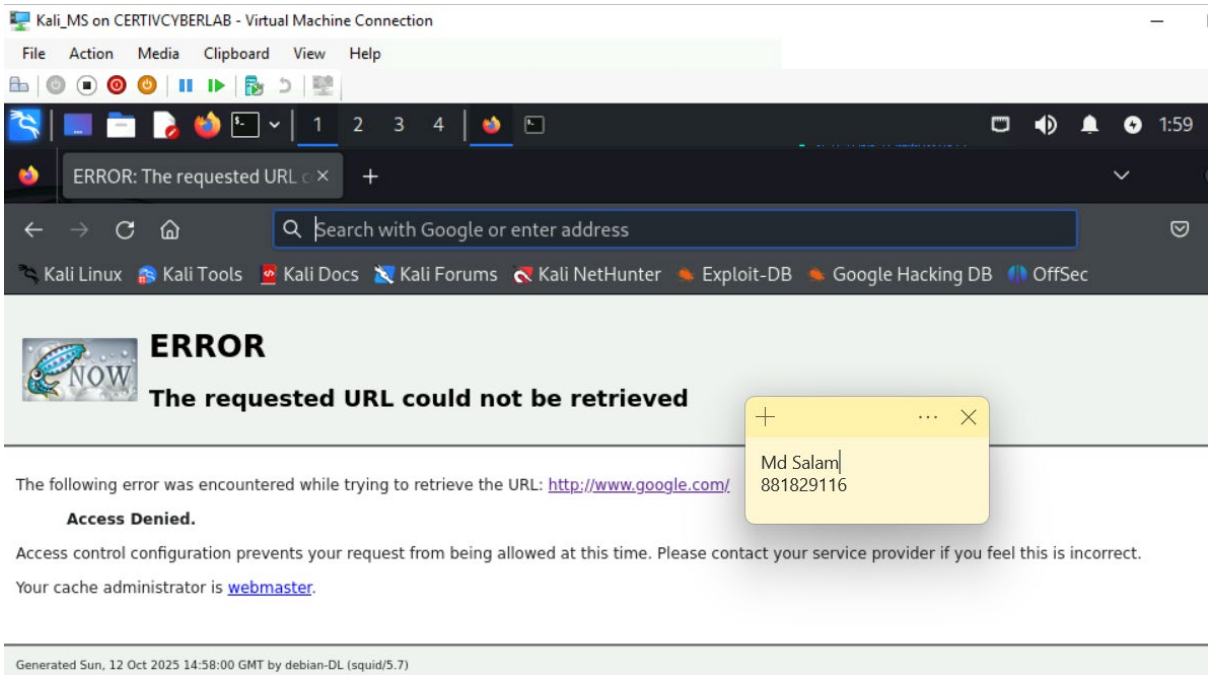
```
student@debian-DL:~$ sudo apt install squid -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libdbus-glib-1-2 libwpe-1.0-1 libwpebackend-fdo-1.0-1
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  libdbi-perl libecap3 squid-common squid-langpack
Suggested packages:
  libmldbm-perl libnet-daemon-perl libsql-statement-perl squidclient squid-cgi
  squid-purge resolvconf smbclient winbind
The following NEW packages will be installed:
  libdbi-perl libecap3 squid squid-common squid-langpack
0 upgraded, 5 newly installed, 0 to remove and 6 not upgraded.
Need to get 4,058 kB of archives.
After this operation, 16.3 MB of additional disk space will be used.
Get:1 http://deb.debian.org/debian bookworm/main amd64 libecap3 amd64 1.0.1-3.4
[17.3 kB]
Get:2 http://deb.debian.org/debian bookworm/main amd64 squid-langpack all 20220
30-1 [169 kB]
Get:3 http://deb.debian.org/debian bookworm/main amd64 squid-common all 5.7-2+d
b12u3 [315 kB]
```

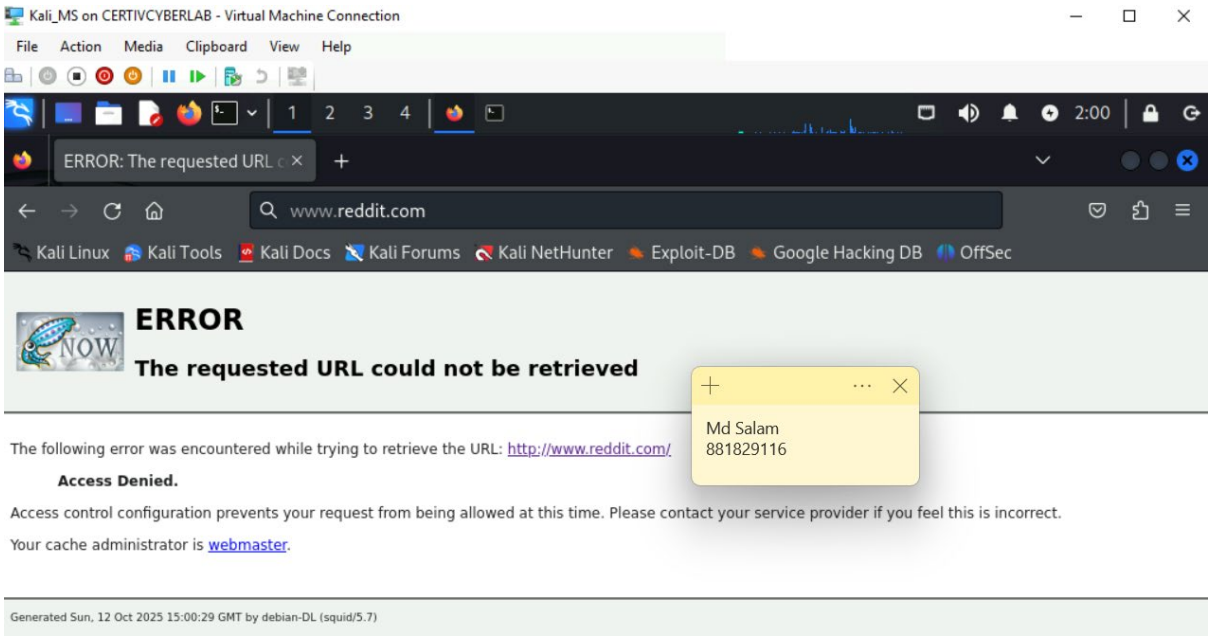
Md Salam
881829116

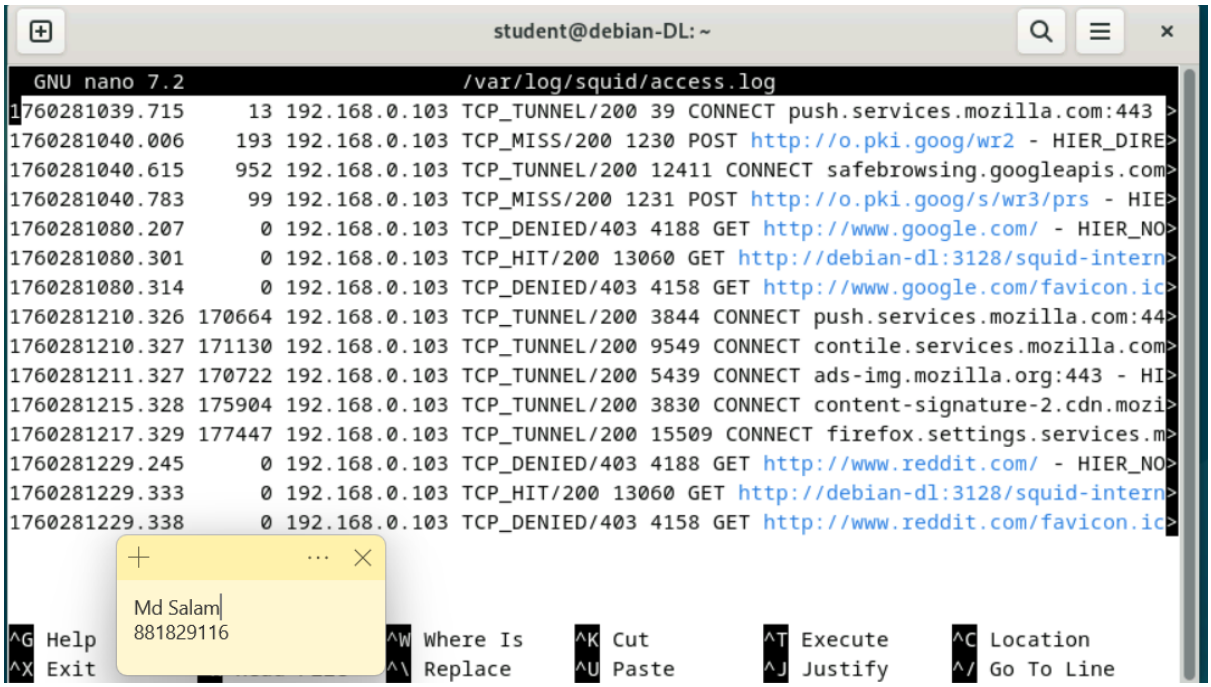
```
student@debian-DL:~$ sudo nano /etc/squid/squid.conf
student@debian-DL:~$ sudo systemctl restart squid.service
[sudo] password for student:
student@debian-DL:~$ sudo systemctl status squid
● squid.service - Squid Web Proxy Server
     Loaded: loaded (/lib/systemd/system/squid.service; enabled; preset: enable>
     Active: active (running) since Mon 2025-10-13 00:54:09 AEDT; 47s ago
       Docs: man:squid(8)
    Process: 3099 ExecStartPre=/usr/sbin/squid --foreground -z (code=exited, st>
   Main PID: 3103 (squid)
      Tasks: 4 (limit: 4536)
     Memory: 17.4M
        CPU: 183ms
     CGroup: /system.slice/squid.service
             ├─3103 /usr/sbin/squid --foreground -sYC
             ├─3105 "(squid-1)" --kid squid-1 --foreground -sYC
             ├─3106 "(logfile-daemon)" /var/log/squid/access.log
             └─3107 "(pinger)"
```

Md Salam
881829116


student@debian-DL: ~
GNU nano 7.2 /etc/squid/blocked.domains.acl *
www.google.com
www.reddit.com
Md Salam
881829116
student@debian-DL: ~
GNU nano 7.2 /etc/squid/squid.conf *
Example rule allowing access from your local networks.
Adapt localnet in the ACL section to list your (internal) IP networks
from where browsing should be allowed
acl blockeddomain dstdomain "/etc/squid/blocked.domains.acl"
http_access deny all blockeddomain
http_access allow localnet
http_access allow localhost
And finally deny all other access to this proxy
http_access deny all
TAG: adapted_http_access
Allowing or Denying access based on defined access lists
Md Salam
881829116


Kali_MS on CERTIVCYBERLAB - Virtual Machine Connection
File Action Media Clipboard View Help
1 2 3 4
1:59
ERROR: The requested URL c
Search with Google or enter address
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
ERROR
The requested URL could not be retrieved
Md Salam
881829116
The following error was encountered while trying to retrieve the URL: http://www.google.com/
Access Denied.
Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.
Your cache administrator is webmaster.
Generated Sun, 12 Oct 2025 14:58:00 GMT by debian-DL (squid/5.7)


Kali_MS on CERTIVCYBERLAB - Virtual Machine Connection
File Action Media Clipboard View Help
1 2 3 4
2:00
ERROR: The requested URL c
www.reddit.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
ERROR
The requested URL could not be retrieved
Md Salam
881829116
The following error was encountered while trying to retrieve the URL: http://www.reddit.com/
Access Denied.
Access control configuration prevents your request from being allowed at this time. Please contact your service provider if you feel this is incorrect.
Your cache administrator is webmaster.
Generated Sun, 12 Oct 2025 15:00:29 GMT by debian-DL (squid/5.7)



Assessor Sign-off (On-campus students):

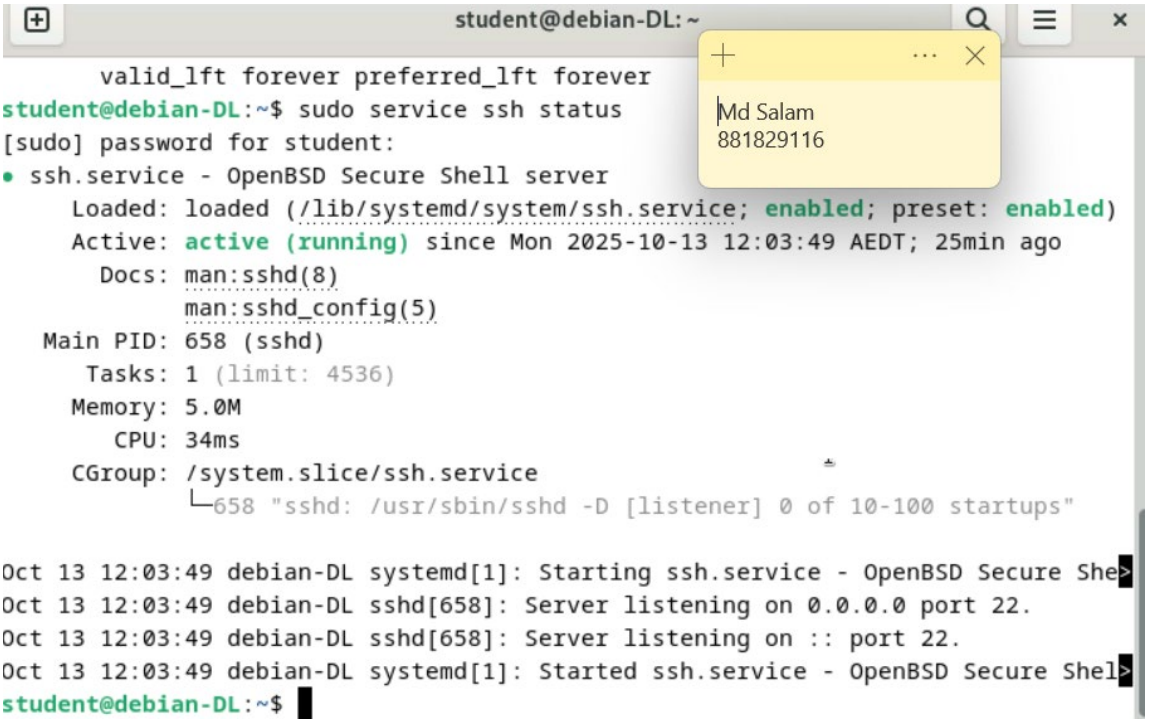
Part 2: Task 1 – Install and configure an SSH Server

Steps:

1.1. Install and configure an SSH server using procedures as outlined in the recommended lab guidelines manual.

Provide evidence this step is completed:

Installed OpenSSH server on Debian VM. Verified installation using sudo service ssh status. The service was active and running, confirming successful configuration.

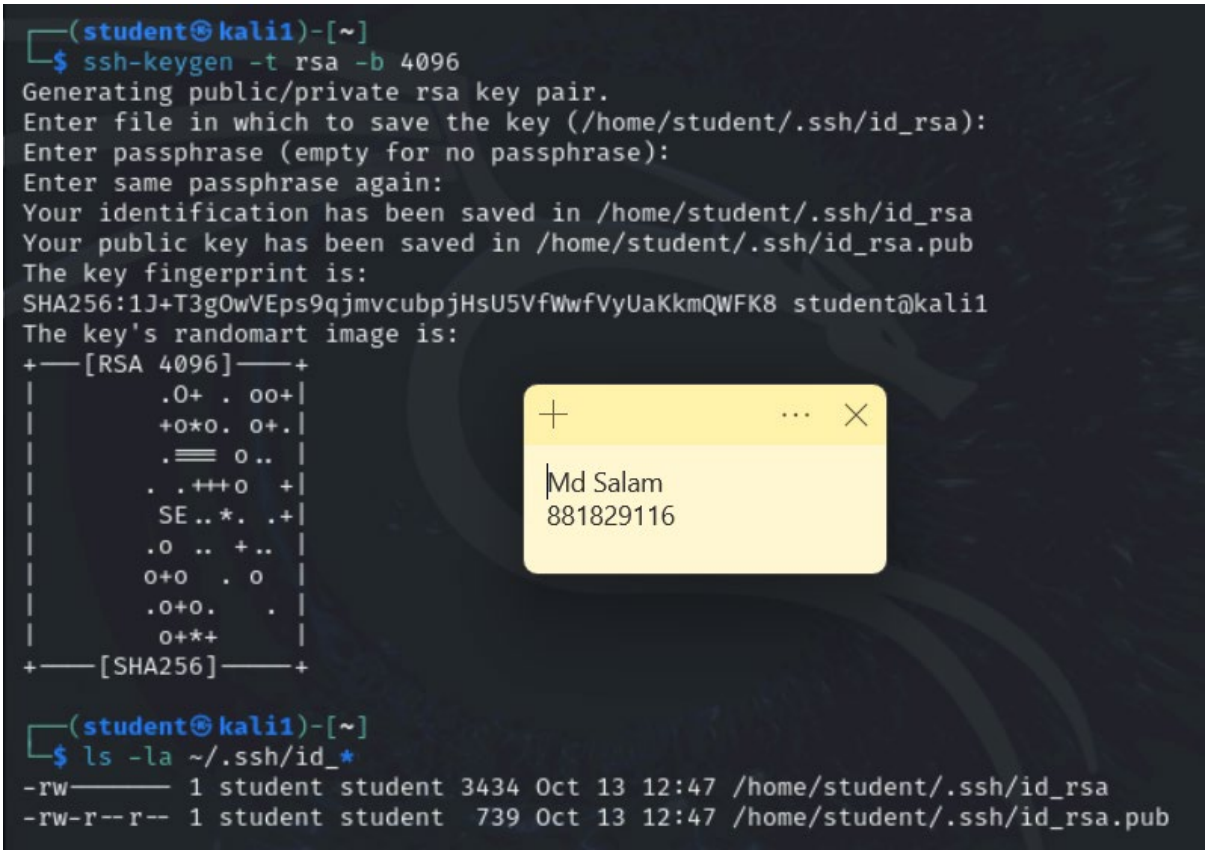


Assessor Sign-off (On-campus students):

1.2. Generate and verify public and private key-pair.

Provide evidence this step is completed:

Generated RSA 4096-bit key pair on Kali VM and verified creation.

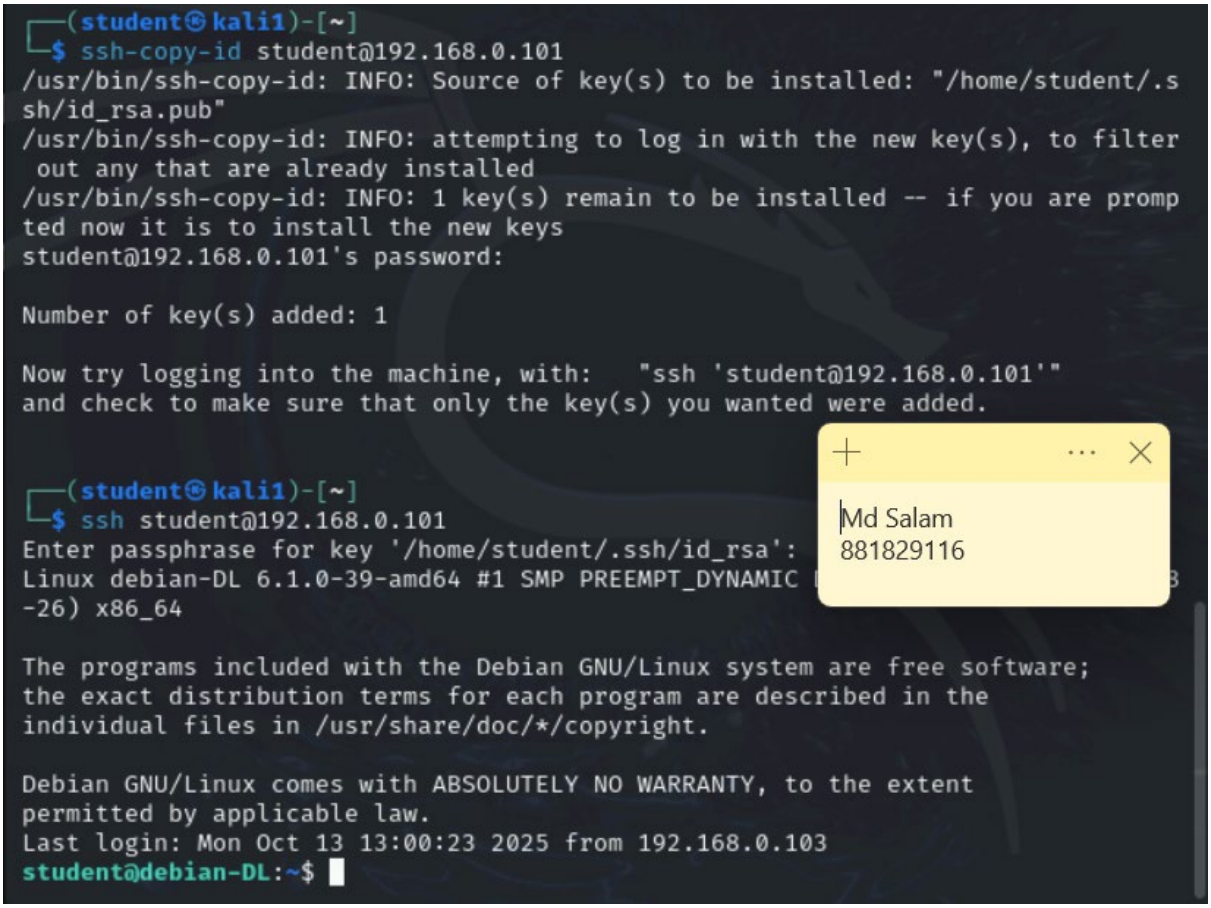


Assessor Sign-off (On-campus students):

1.3. Connect to an SSH server using a public key (which uses RSA authentication).

Provide evidence this step is completed:

Successfully connected to Debian via SSH using RSA key authentication.



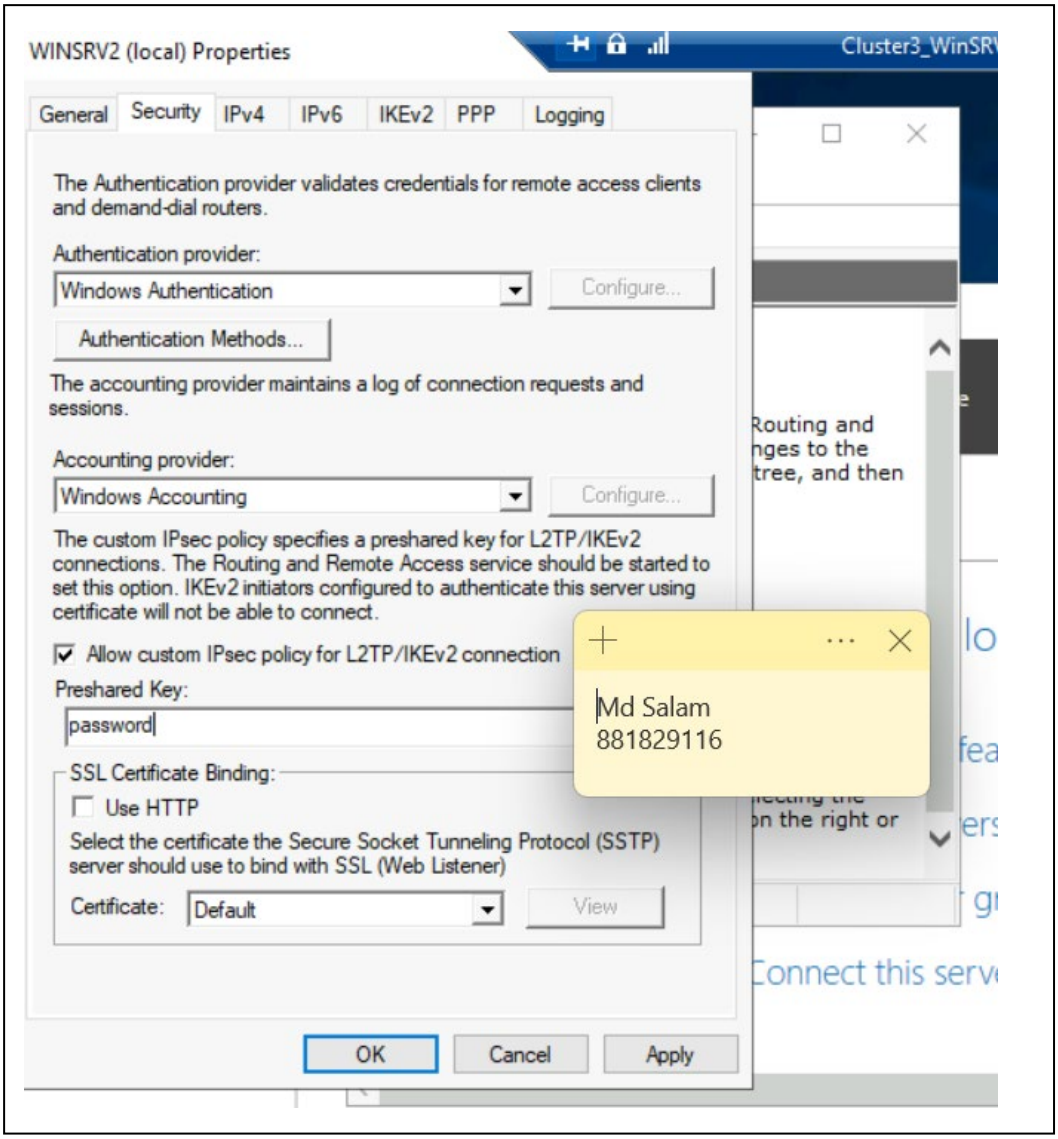
Assessor Sign-off (On-campus students):

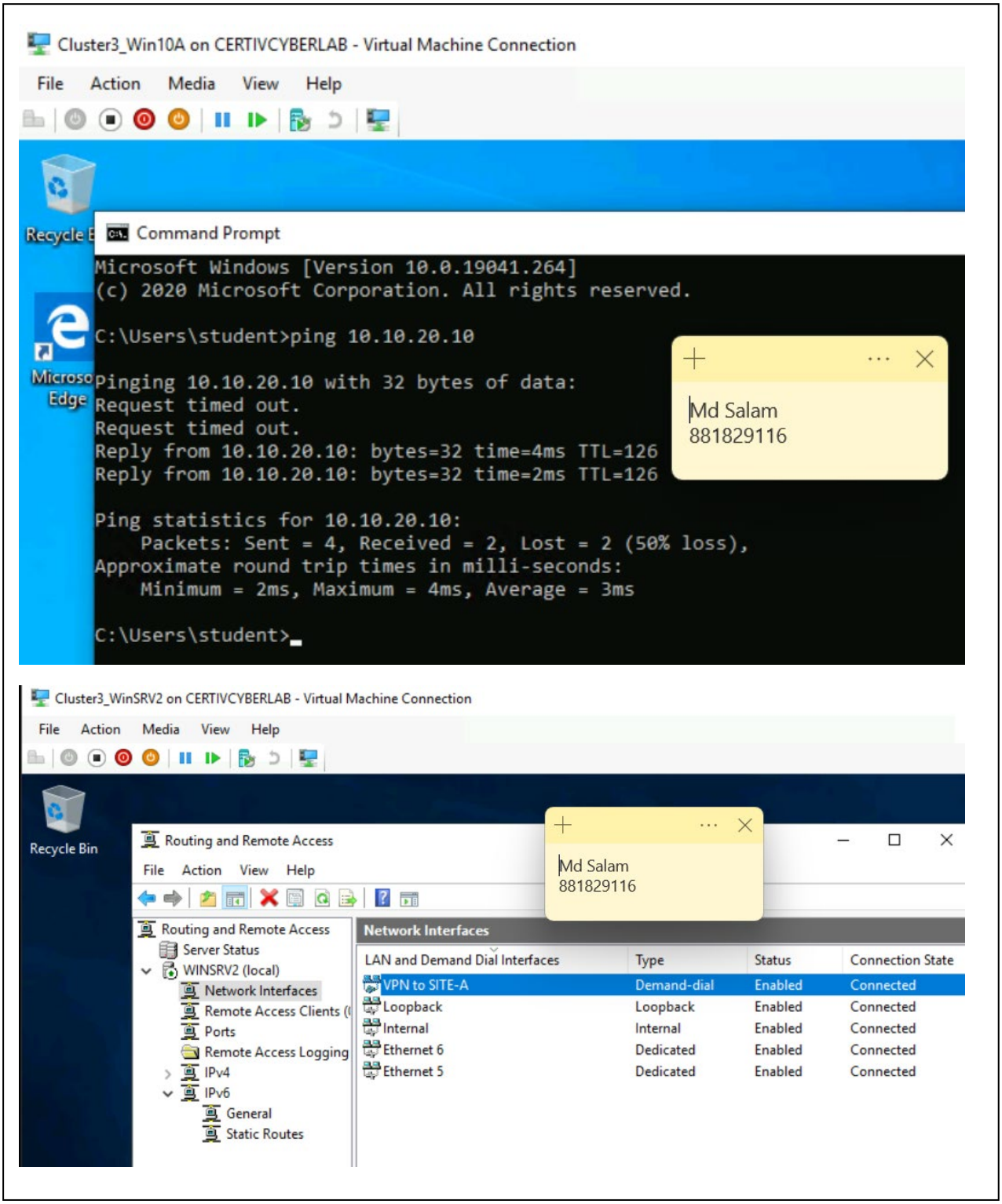
Part 2: Task 2 – Configure a VPN Server

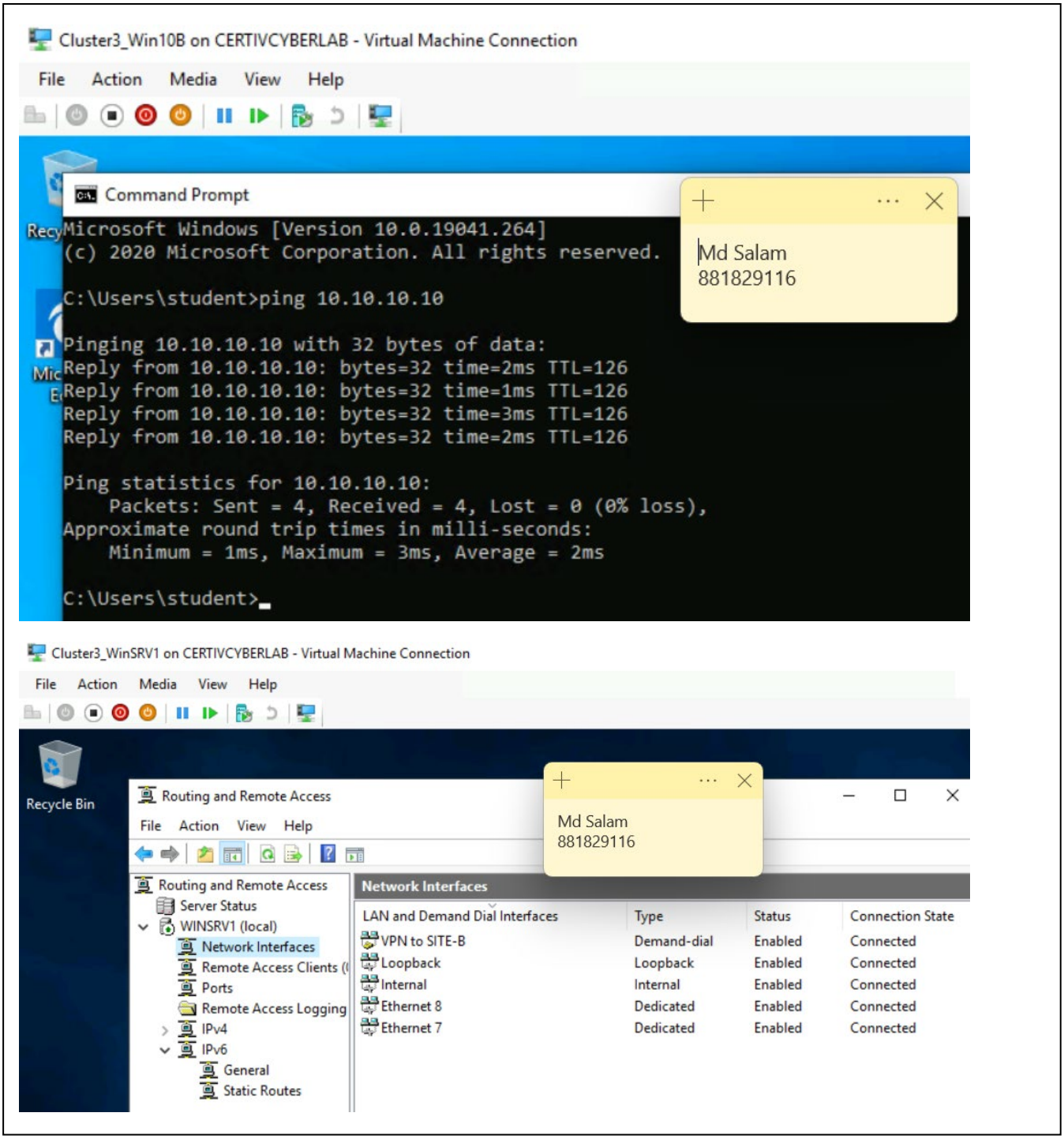
Steps:

2.1. **Configure and connect a** site-to-site VPN **tunnel** (using the procedures outlined in the recommended lab).

Provide evidence this step is completed:


WINSRV2 (local) Properties
General
Security
IPv4
IPv6
IKEv2
PPP
Logging
The Authentication provider validates credentials for remote access clients and demand-dial routers.
Authentication provider:
Windows Authentication
Configure...
Authentication Methods...
The accounting provider maintains a log of connection requests and sessions.
Accounting provider:
Windows Accounting
Configure...
The custom IPsec policy specifies a preshared key for L2TP/IKEv2 connections. The Routing and Remote Access service should be started to set this option. IKEv2 initiators configured to authenticate this server using certificate will not be able to connect.
Allow custom IPsec policy for L2TP/IKEv2 connection
Preshared Key:
password
SSL Certificate Binding:
Use HTTP
Select the certificate the Secure Socket Tunneling Protocol (SSTP) server should use to bind with SSL (Web Listener)
Certificate:
Default
View
OK
Cancel
Apply
Cluster3_WinSR
Md Salam
881829116

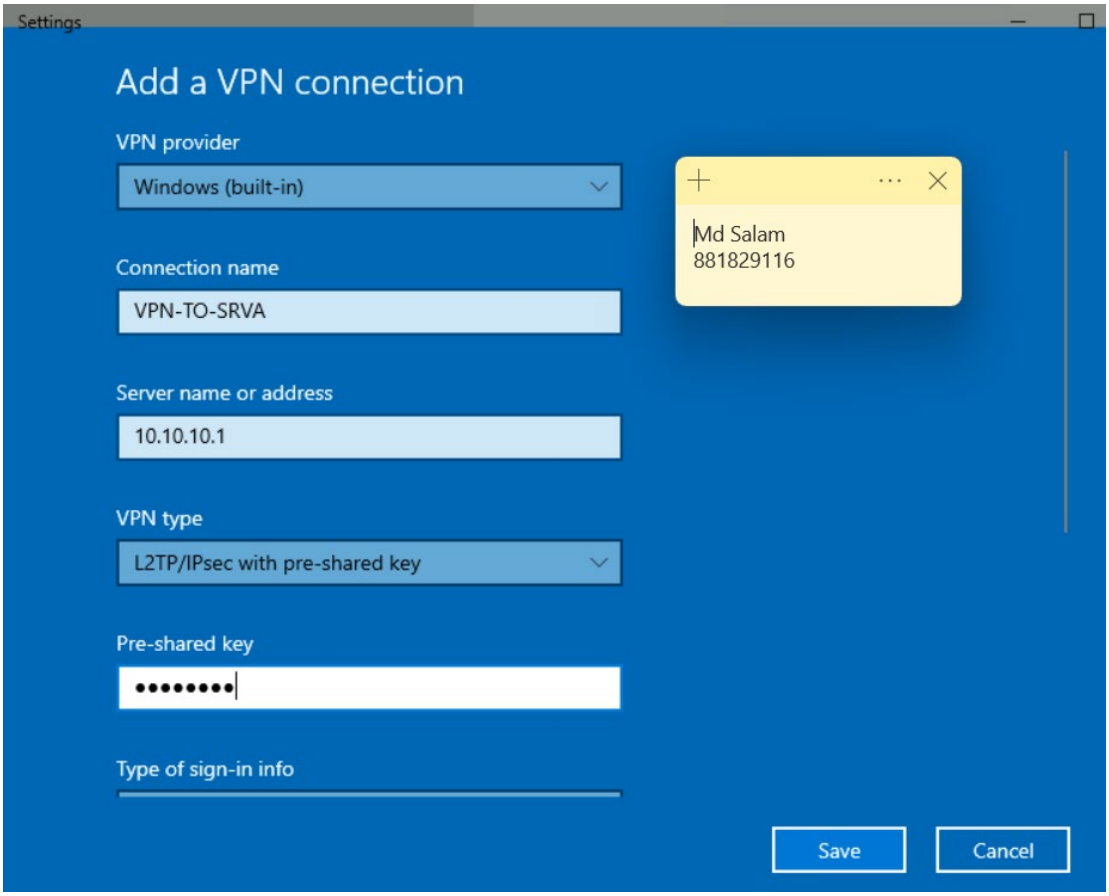

Cluster3_Win10A on CERTIVCYBERLAB - Virtual Machine Connection
File Action Media View Help
Recycle B
Microso Edge
Command Prompt
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.
C:\Users\student>ping 10.10.20.10
Pinging 10.10.20.10 with 32 bytes of data:
Request timed out.
Request timed out.
Reply from 10.10.20.10: bytes=32 time=4ms TTL=126
Reply from 10.10.20.10: bytes=32 time=2ms TTL=126
Ping statistics for 10.10.20.10:
Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 4ms, Average = 3ms
C:\Users\student>
Md Salam
881829116
Cluster3_WinSRV2 on CERTIVCYBERLAB - Virtual Machine Connection
File Action Media View Help
Recycle Bin
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
WINSRV2 (local)
Network Interfaces
Remote Access Clients
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Type
Status
Connection State
VPN to SITE-A
Demand-dial
Enabled
Connected
Loopback
Loopback
Enabled
Connected
Internal
Internal
Enabled
Connected
Ethernet 6
Dedicated
Enabled
Connected
Ethernet 5
Dedicated
Enabled
Connected
Md Salam
881829116

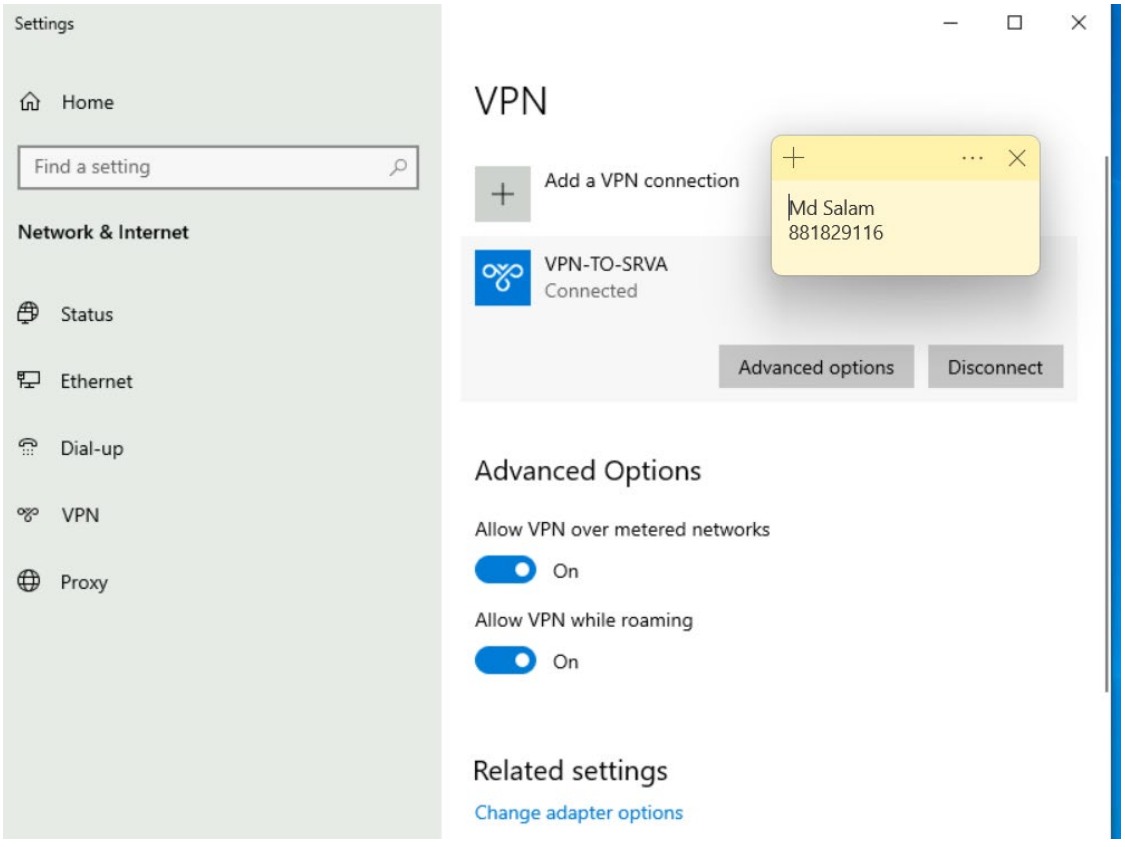


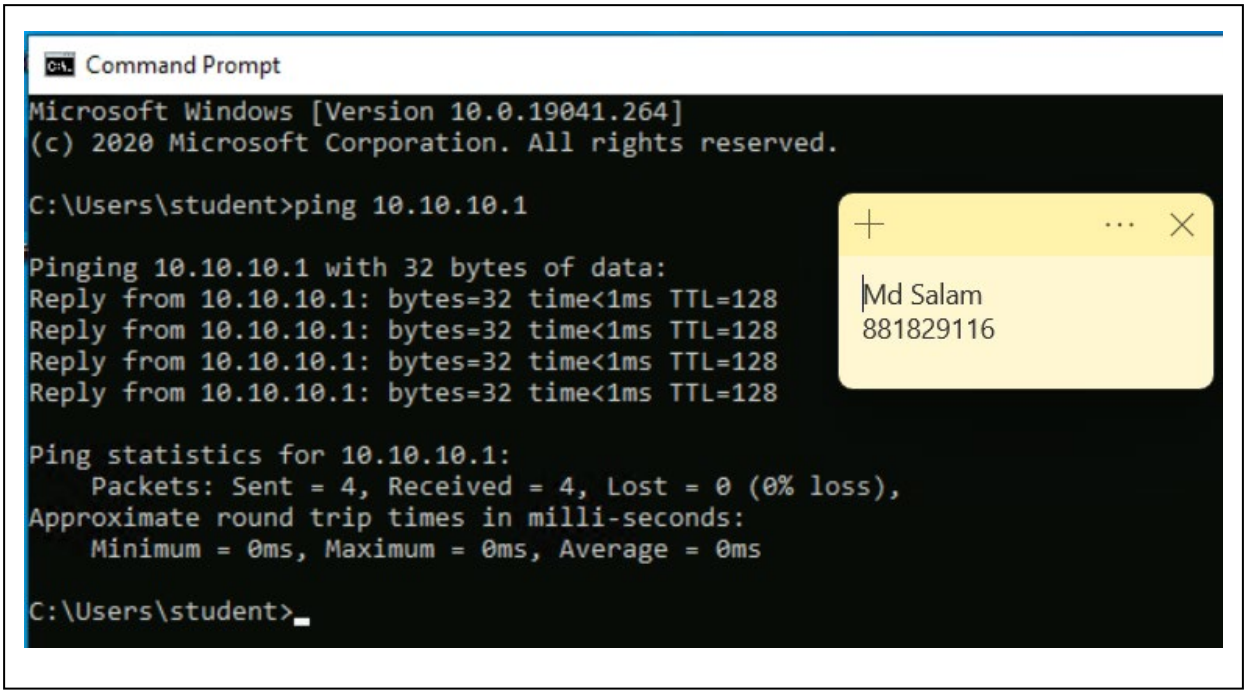
Assessor Sign-off (On-campus students):

2.2. Configure VPN Server as a Dial VPN server and connect from a remote PC (using the procedures outlined in the recommended lab).

Provide evidence this step is completed:


Settings
Add a VPN connection
VPN provider
Windows (built-in)
Connection name
VPN-TO-SRVA
Server name or address
10.10.10.1
VPN type
L2TP/IPsec with pre-shared key
Pre-shared key
Type of sign-in info
Save
Cancel
Md Salam
881829116


Settings
Home
Find a setting
Network & Internet
Status
Ethernet
Dial-up
VPN
Proxy
VPN
Add a VPN connection
VPN-TO-SRVA
Connected
Advanced options
Disconnect
Advanced Options
Allow VPN over metered networks
On
Allow VPN while roaming
On
Related settings
Change adapter options
Md Salam
881829116



Assessor Sign-off (On-campus students):

Part 3: Task 1 – Data analysis case study

Document the testing completed below. Where directed, TAFE digital students to provide screenshots of completed steps. On-campus students may demonstrate the corresponding step in class, with the assessor signing off the step.

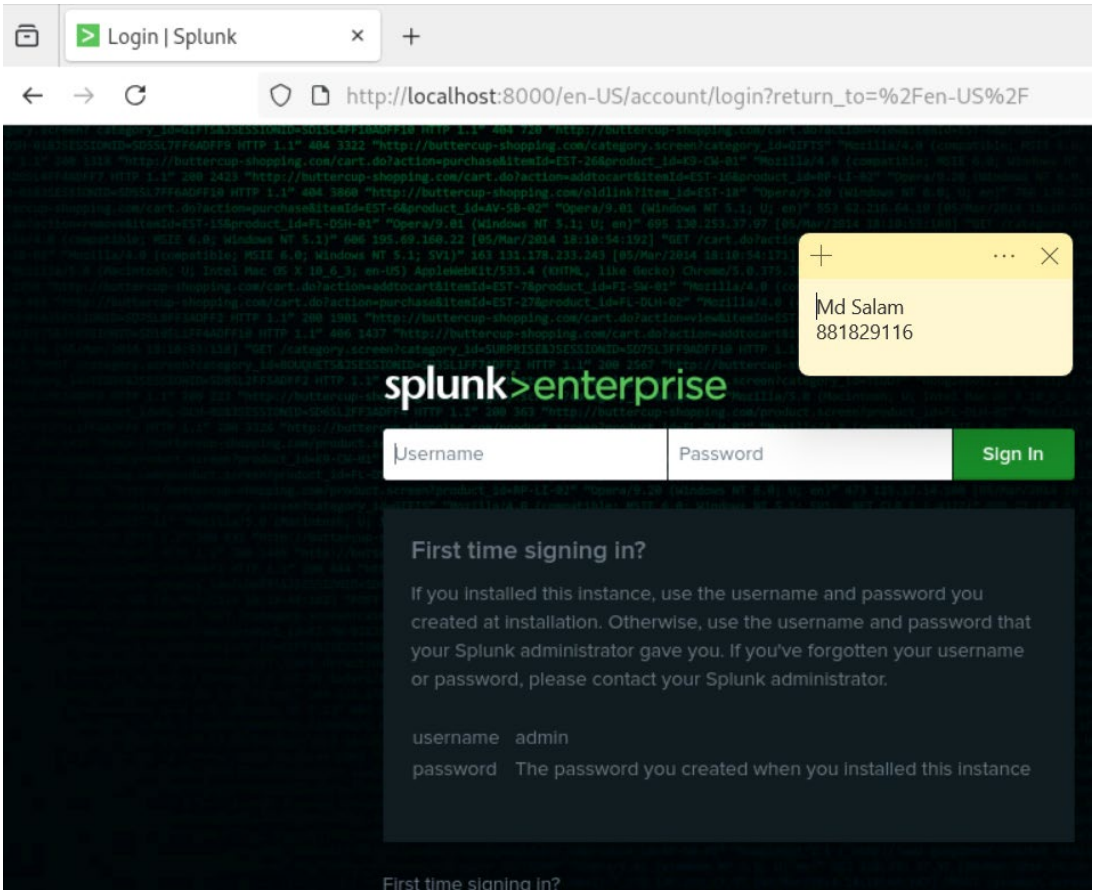
1.1. Successfully install Splunk.

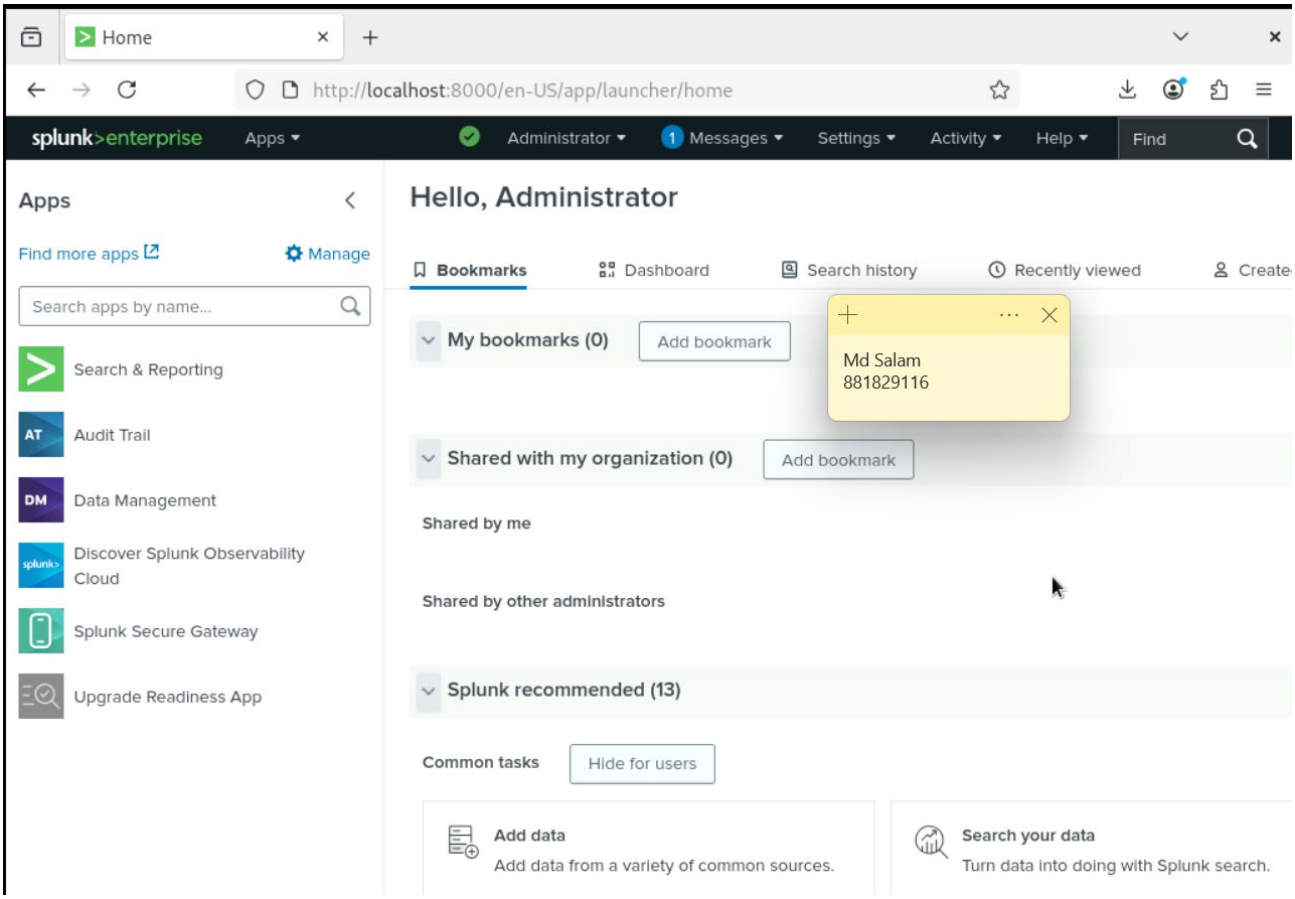
Provide evidence this step is completed:

Assessor Sign-off (On-campus students):

1.2. Log in to the Splunk homepage.

Provide evidence this step is completed:

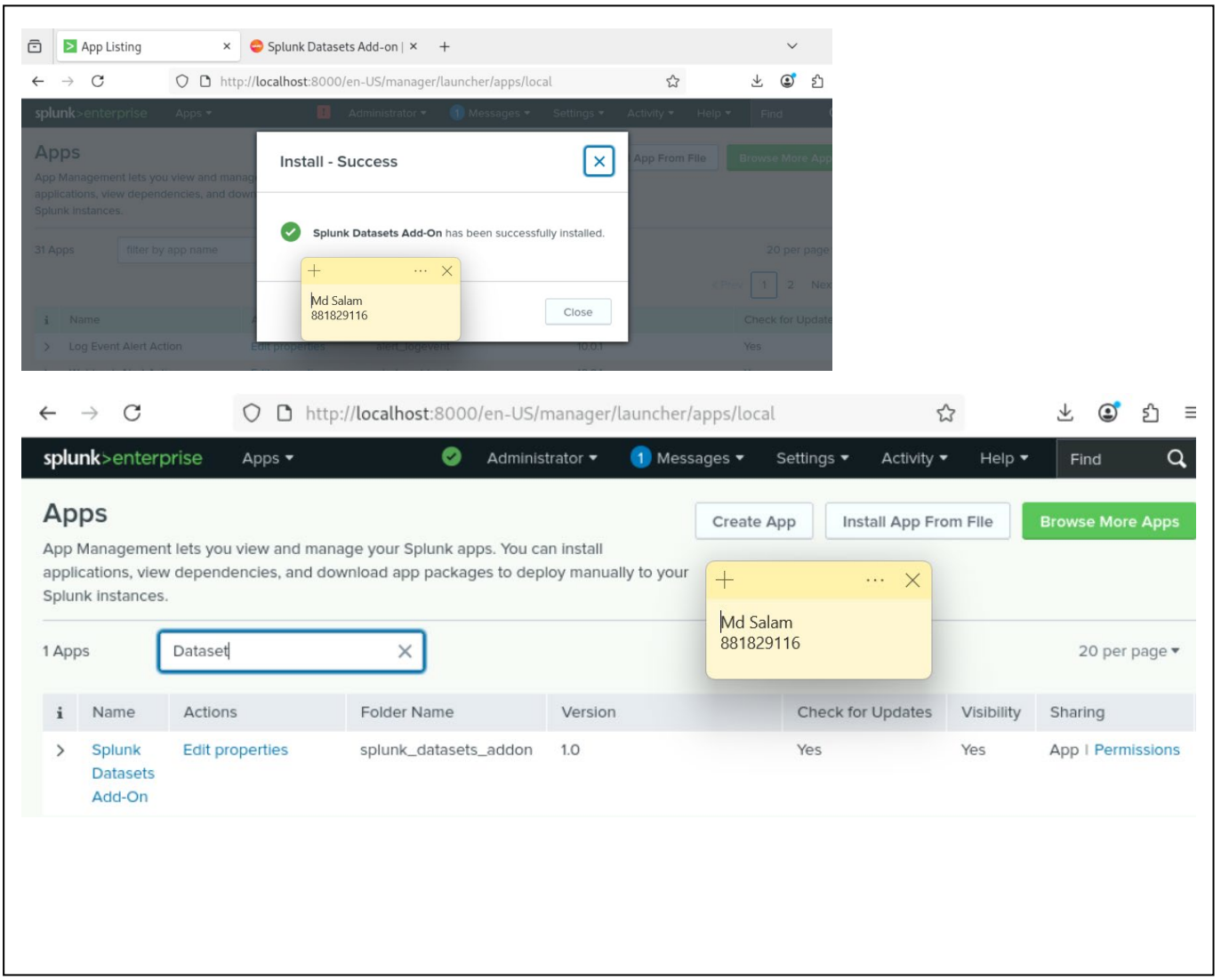

Login | Splunk
http://localhost:8000/en-US/account/login?return_to=%2Fen-US%2F
Md Salam
881829116
splunk>enterprise
Username
Password
Sign In
First time signing in?
If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.
username admin
password The password you created when you installed this instance


Home
http://localhost:8000/en-US/app/launcher/home
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Apps
Find more apps
Manage
Search apps by name...
Search & Reporting
Audit Trail
Data Management
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Hello, Administrator
Bookmarks
Dashboard
Search history
Recently viewed
Md Salam
881829116
My bookmarks (0)
Add bookmark
Shared with my organization (0)
Add bookmark
Shared by me
Shared by other administrators
Splunk recommended (13)
Common tasks
Hide for users
Add data
Add data from a variety of common sources.
Search your data
Turn data into doing with Splunk search.

Assessor Sign-off (On-campus students):

1.3. Install the Splunk datasets and add-on (using the procedures outlined in the recommended lab).

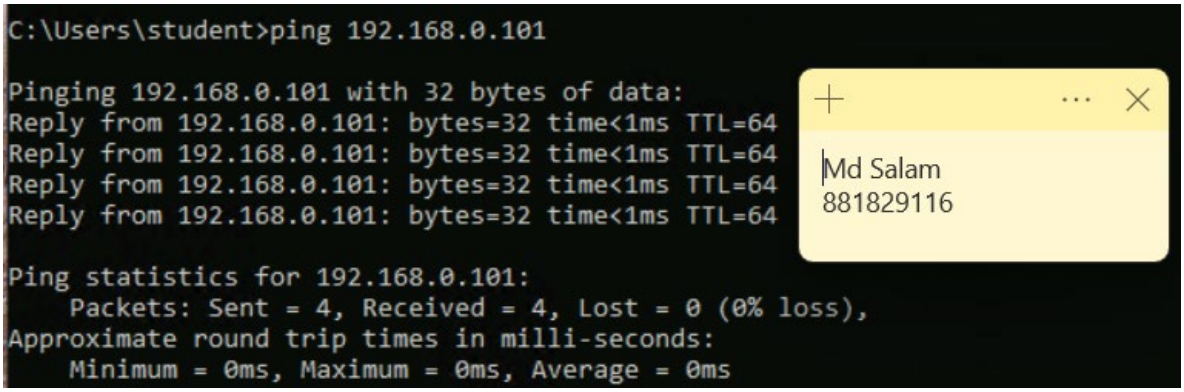
Provide evidence this step is completed:

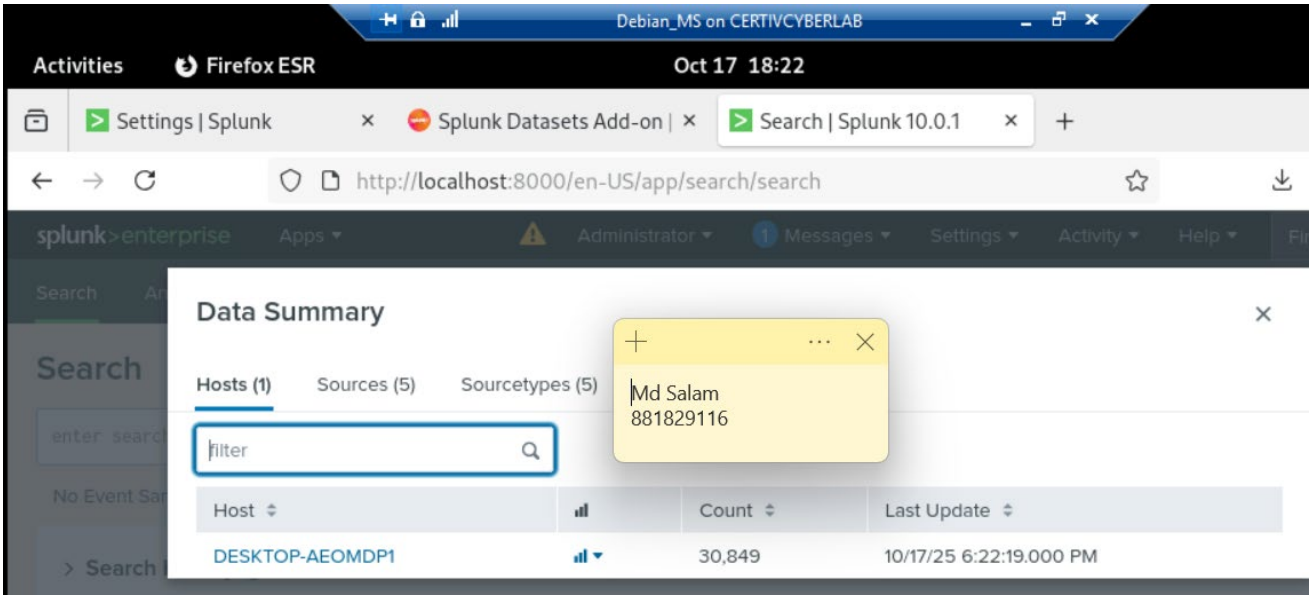


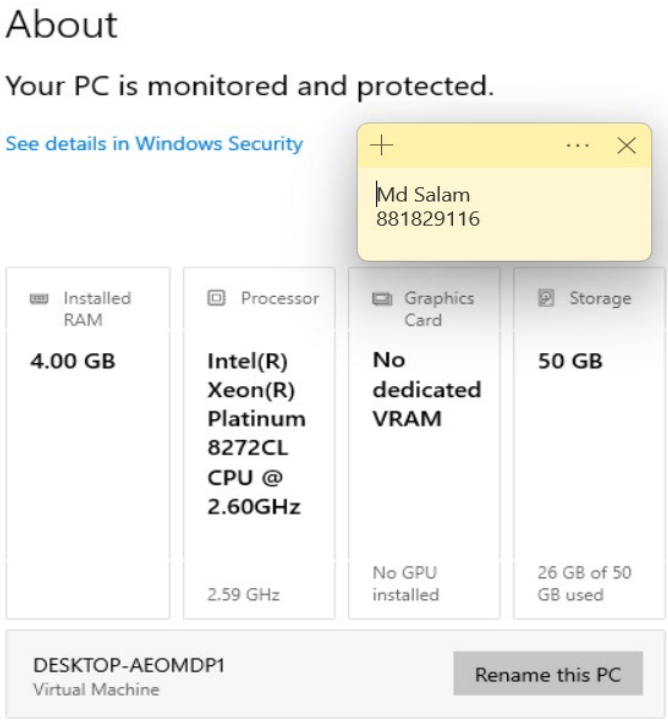
Assessor Sign-off (On-campus students):

1.4. Install universal forwarder on Windows machine and send data to Splunk server using procedures outlined in the recommended lab guidelines manual.

Provide evidence this step is completed:


C:\Users\student>ping 192.168.0.101
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=64
Reply from 192.168.0.101: bytes=32 time<1ms TTL=64
Reply from 192.168.0.101: bytes=32 time<1ms TTL=64
Reply from 192.168.0.101: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.101:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
Md Salam
881829116


Debian_MS on CERTIVCYBERLAB
Activities
Firefox ESR
Oct 17 18:22
Settings | Splunk
Splunk Datasets Add-on |
Search | Splunk 10.0.1
http://localhost:8000/en-US/app/search/search
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Search
Data Summary
Hosts (1)
Sources (5)
Sourcetypes (5)
filter
Host
Count
Last Update
DESKTOP-AEOMDP1
30,849
10/17/25 6:22:19.000 PM
Md Salam
881829116

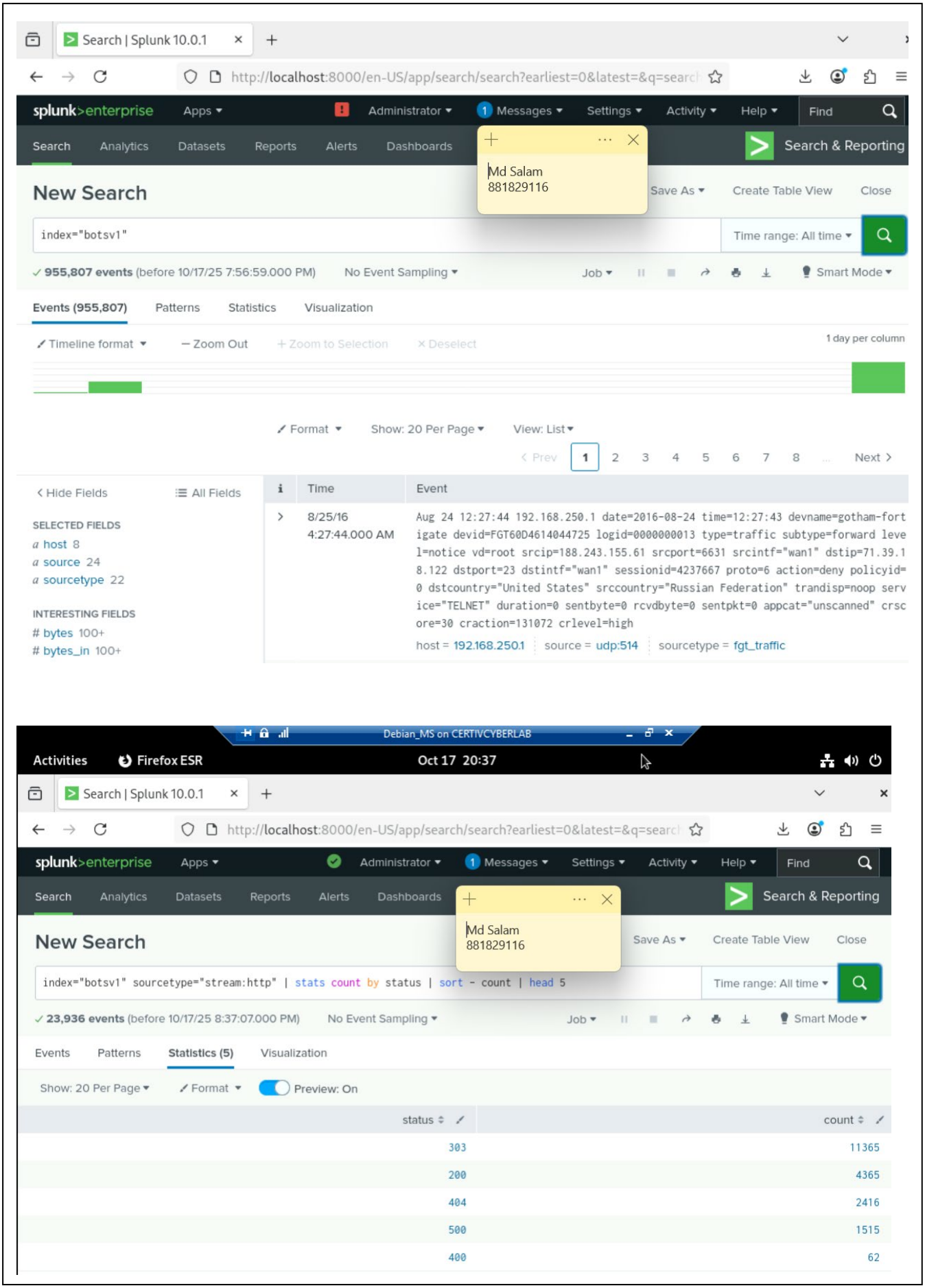

About
Your PC is monitored and protected.
See details in Windows Security
Installed RAM
4.00 GB
Processor
Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz
2.59 GHz
Graphics Card
No dedicated VRAM
No GPU installed
Storage
50 GB
26 GB of 50 GB used
DESKTOP-AEOMDP1
Virtual Machine
Rename this PC
Md Salam
881829116

Assessor Sign-off (On-campus students):

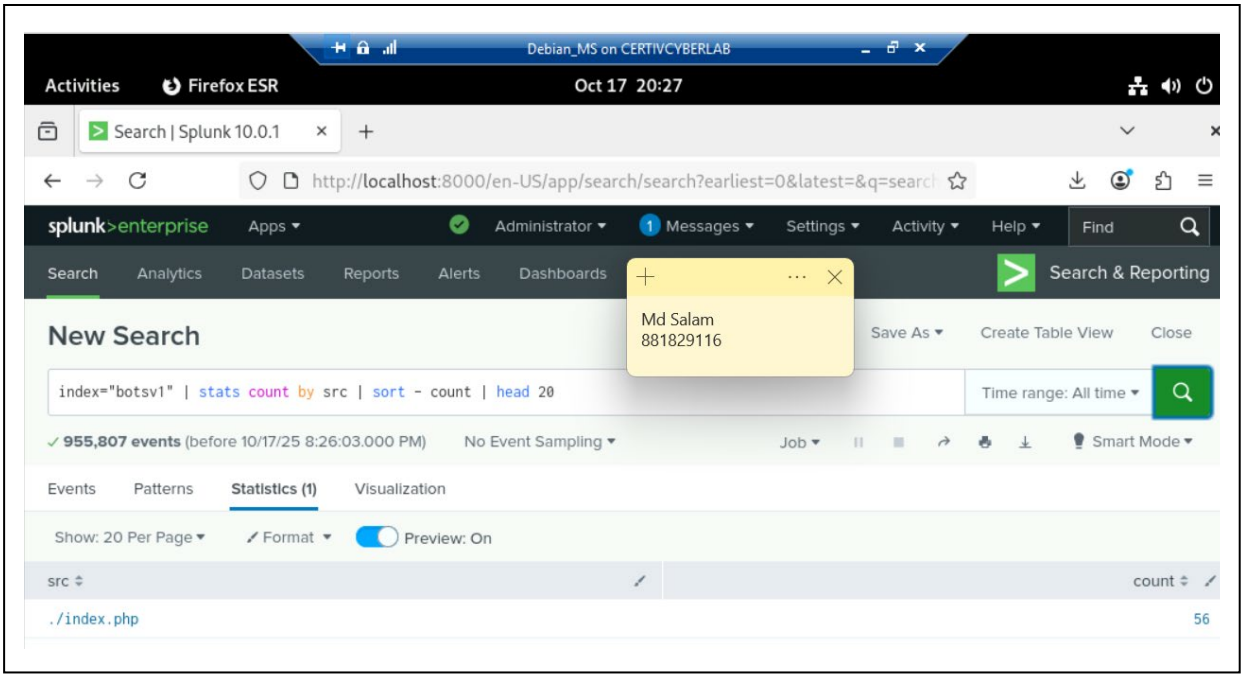
1.5. Develop and complete strategies to process this data, including:

- Perform relevant searches and pattern recognition SPL statements to detect anomalies and discrepancies in the data.
- Investigate and calculate the number of events.

Provide evidence this step is completed:


Search | Splunk 10.0.1
http://localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Md Salam
881829116
New Search
Save As
Create Table View
Close
index="botsv1"
Time range: All time
955,807 events (before 10/17/25 7:56:59.000 PM)
No Event Sampling
Job
Smart Mode
Events (955,807)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 day per column
Format
Show: 20 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 8
a source 24
a sourcetype 22
INTERESTING FIELDS
bytes 100+
bytes_in 100+
Time
Event
8/25/16
4:27:44.000 AM
Aug 24 12:27:44 192.168.250.1 date=2016-08-24 time=12:27:43 devname=gotham-fortigate devid=FGT60D4614044725 logid=0000000013 type=traffic subtype=forward level=notice vd=root srcip=188.243.155.61 srcport=6631 srcintf="wan1" dstip=71.39.18.122 dstport=23 dstintf="wan1" sessionid=4237667 proto=6 action=deny policyid=0 dstcountry="United States" srccountry="Russian Federation" trandisp=noop service="TELNET" duration=0 sentbyte=0 rcvdbyte=0 sentpkt=0 appcat="unscanned" crscore=30 craction=131072 crlevel=high
host = 192.168.250.1
source = udp:514
sourcetype = fgt_traffic

Debian_MS on CERTIVCYBERLAB
Activities
Firefox ESR
Oct 17 20:37
Search | Splunk 10.0.1
http://localhost:8000/en-US/app/search/search?earliest=0&latest=&q=search
splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
Md Salam
881829116
New Search
Save As
Create Table View
Close
index="botsv1" sourcetype="stream:http" | stats count by status | sort - count | head 5
Time range: All time
23,936 events (before 10/17/25 8:37:07.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (5)
Visualization
Show: 20 Per Page
Format
Preview: On
status
count
303
11365
200
4365
404
2416
500
1515
400
62



Assessor Sign-off (On-campus students):

1.6. Break down data into subtasks:

- implement the subtasks
- Analyse and evaluate the effectiveness of each subtask, and provide a comment in the Data Analysis Report, as to whether each was successful or not, and what modifications are required.

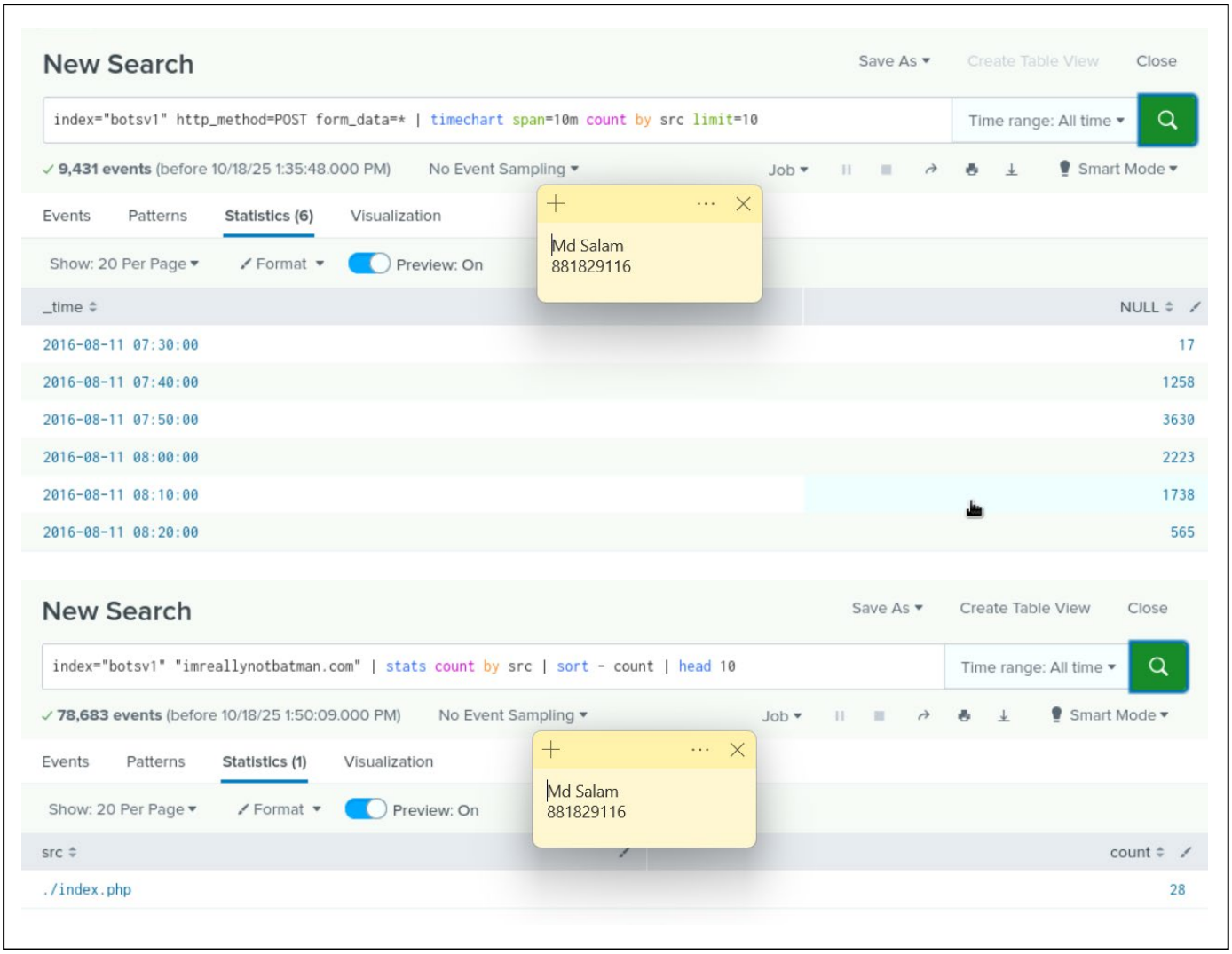
Provide evidence this step is completed:

Subtask	Implementation	Evaluation / Outcome
1. Ingest & Verify Data	Imported the BOTSv1 dataset using the Splunk GUI. Verified data by searching index="botsv1" and confirming total events count.	Successful — 955,807 events were ingested and searchable. Time range had to be changed to “All time” to display results.
2. Baseline Event Counts	Used SPL `index="botsv1"	stats count by sourcetype` to see which log types were present.
3. Web Scan Detection	Ran SPL `index="botsv1" "imreallynotbatman.com"	stats count by src
4. Anomaly / Pattern Recognition	Ran SPLs to check rare URIs and HTTP status codes: stats count by status and stats count by uri.	Successful — observed several unusual URIs and uncommon HTTP error codes suggesting probing behavior.
5. Brute Force Attack Analysis	Used regex extraction on POST form data: ` rex field=form_data "password=(?[^&]+)"	
6. Overall Data Analysis Workflow	Monitored results in real-time and compared with expected lab outcomes.	Successful — all major SPL searches ran correctly, anomalies identified, and suspicious source IP logged for reporting.

Assessor Sign-off (On-campus students):

1.7. Monitor for deviations and respond to suspicious behaviour.

Provide evidence this step is completed:



Assessor Sign-off (On-campus students):

1.8. Complete each of the following, according to the instructions provided in each section below:

a) Sourcetype table

b) SPL statement table

c) Index of botsv1 and IP address and destination, Top 10 URLs searches

d) Analysis of brute force password attacks

e) Identification of the first password used in a brute force attack.

i. Sourcetype table

Complete Table 3 with planned source types and an explanation of why those source types were chosen. Add or delete additional rows if required.

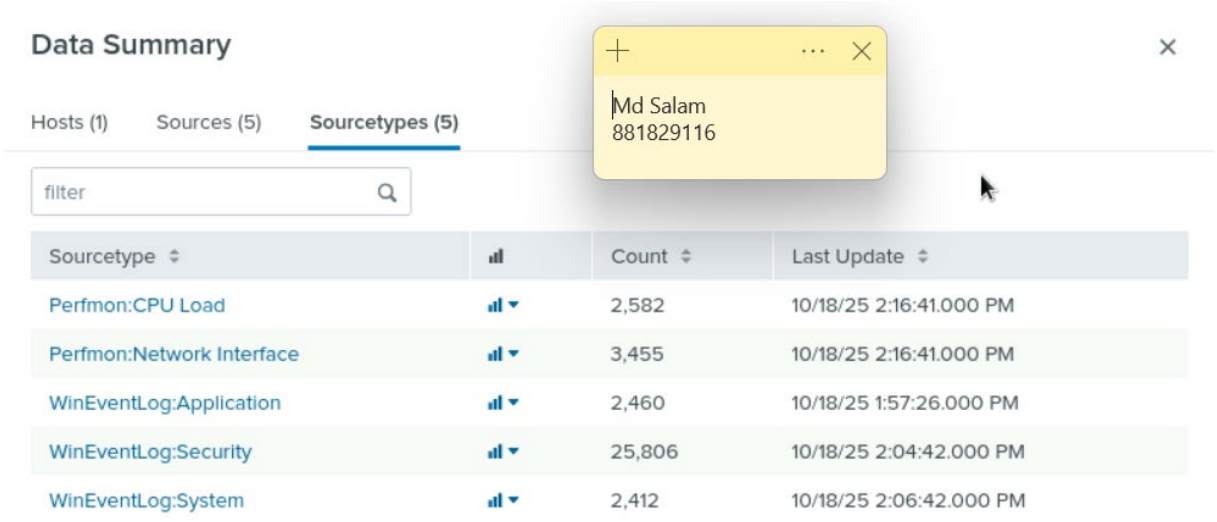


Table 1 – Source type

Source type	Why was source type chosen
Perfmon:CPU Load	Captures Windows system performance data related to CPU usage. Used to monitor system resource utilisation and detect performance anomalies that might indicate malware or heavy processing from suspicious activity.
Perfmon:Network Interface	Logs network performance metrics such as bandwidth and packets sent/received. Useful for identifying abnormal network usage or potential data exfiltration attempts.
WinEventLog:Application	Collects logs generated by Windows applications. Helps correlate application-level events with system or security incidents.
WinEventLog:Security	Contains Windows security-related events such as logons, logoffs, privilege use, and audit failures. Critical for monitoring authentication attempts and identifying possible intrusions or brute-force attacks.
WinEventLog:System	Records operating-system-level events like service start/stop, driver issues, or system reboots. Provides context for system stability and reliability during security incidents.

ii. SPL statement table

To determine the data required for the following table, review the steps within:

- C2T10L1 – Splunk installation
- C2T10L2 – Importing Splunk Botsv1 Dataset
- C2T10L3 – Splunk training.

This will include a list of the complete SPL statements for each query and an explanation of the logic behind the statements chosen. Add additional rows/columns if required.

Table 2 – SPL steps and statements

Step/sub-step	SPL statement	Logic behind choice
Count all events	index="botsv1"	stats count
Top scanning IPs	index="botsv1" "imreallynotbatman.com"	stats count by src
Top 10 URIs	index="botsv1" "imreallynotbatman.com"	stats count by uri
Extract passwords	index="botsv1" http_method=POST form_data=*	rex field=form_data "password=(?<password>[^&]+)"
First password used	index="botsv1" http_method=POST form_data=*	rex field=form_data "password=(?<password>[^&]+)"
Brute-force activity over time	index="botsv1" http_method=POST form_data=*	timechart span=10m count by src limit=10
Identify abnormal HTTP status codes	index="botsv1" sourcetype="stream:http"	stats count by status
Detect rare or suspicious URIs	index="botsv1" sourcetype=access	stats count by uri

iii. Index of botsv1

Perform a basic search of the **botsv1** index data

1. How many events did this return?

955,807 events

2. What was the SPL statement that you used?

index="botsv1"

iv. IP address source and destination

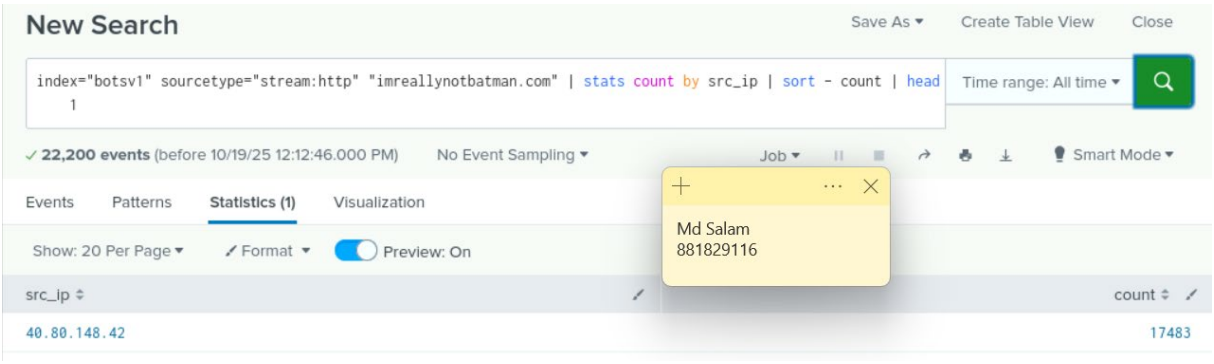
Answer the following questions regarding the IP address responsible for scanning the website.

1. What source type did you specify?

stream:http

2. What is the most likely source IP address scanning imreallynotbatman.com?

40.80.148.42



3. What was the SPL statement used, if different from the planning document?

index="botsv1" sourcetype="stream:http" "imreallynotbatman.com"

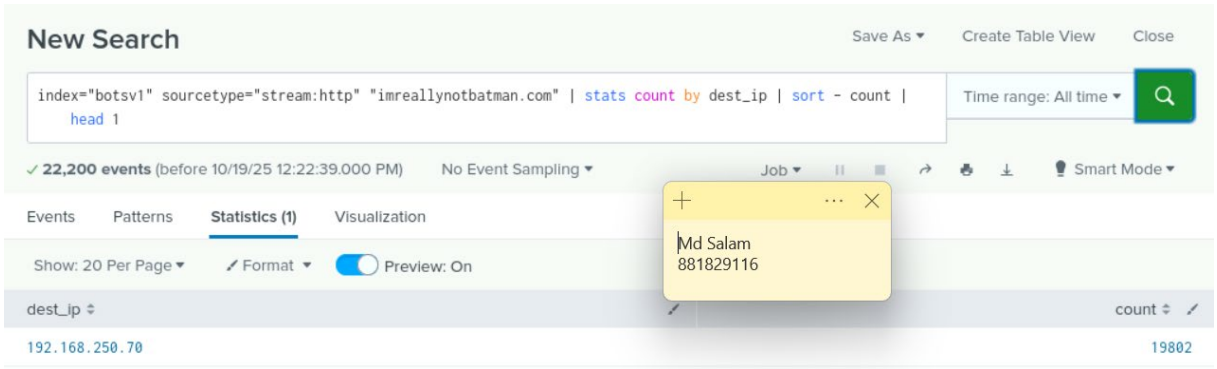
| stats count by src_ip

| sort - count

| head 1

4. What was the destination IP address that was being scanned?

192.168.250.70

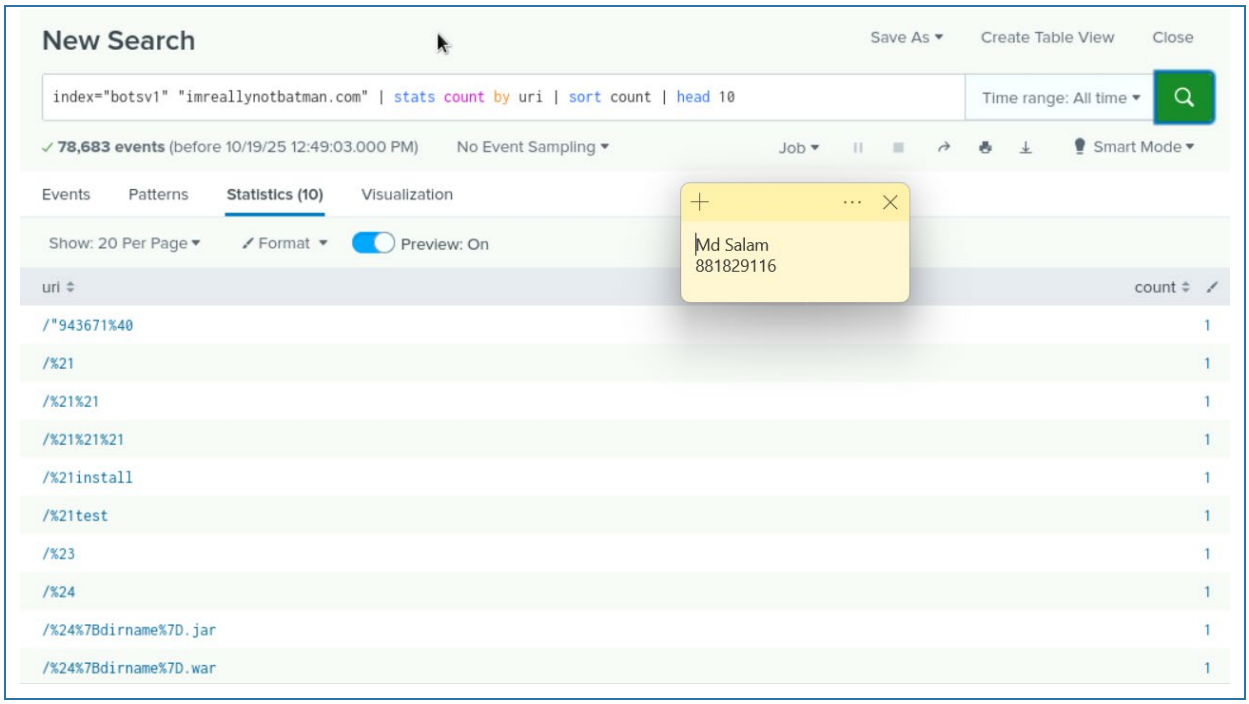


v. Top ten URI's

1. What are the top ten URI's (i not L) being returned during the scan of **imreallynotbatman.com**?

URI	Count
/"943671%40	1
/%21	1
/%21%21	1
/%21%21%21	1
/%21install	1
/%21test	1
/%23	1
/%24	1
/%24%7Bdirname%7D.jar	1
/%24%7Bdirname%7D.war	1

2. Use the stats, count, and sort search terms to display the top ten URI's in ascending order and paste a screenshot of the result.



3. What was the SPL statement used?

```
index="botsv1" "imreallynotbatman.com"
| stats count by uri
| sort count
| head 10
```

vi. Analysis of brute force password attacks

1. Use a "wild card" search to find all passwords used against the destination IP. As a hint, you will need to use a specific **http_method=** as the attack was against a web server. You will also need to pipe the result into a search that uses the form_data field to search for user passwords within the **form_data.** What is the SPL statement used?

```
index="botsv1" sourcetype="stream:http" http_method=POST form_data=*password*
```

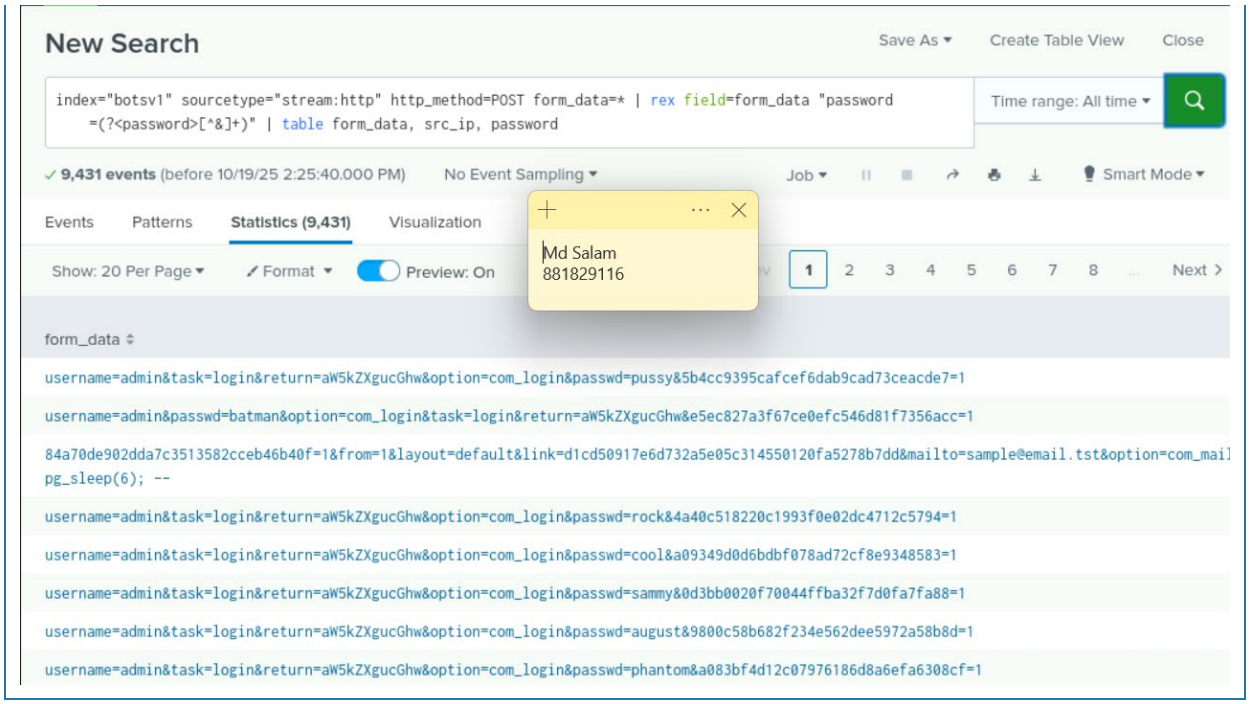
2. Use the **form_data** field with a regular expression (**rex**) to list all brute force password attempts. What was the SPL statement used?

```
index="botsv1" sourcetype="stream:http" http_method=POST form_data=* | rex field=form_data "password=(?<password>[^&]+)"
```

3. Format the result as a table with **form_data, src_ip,** and the **password** from the regular expression as headings. Provide a screenshot of the result including the SPL statement.

SPL used:

```
index="botsv1" sourcetype="stream:http" http_method=POST form_data=* | rex field=form_data "password=(?<password>[^&]+)" | table form_data, src_ip, password
```



4. Use a search command to find and sort the top attempts by source IP. What IP address was the most likely source of the brute force password attack?

SPL used:

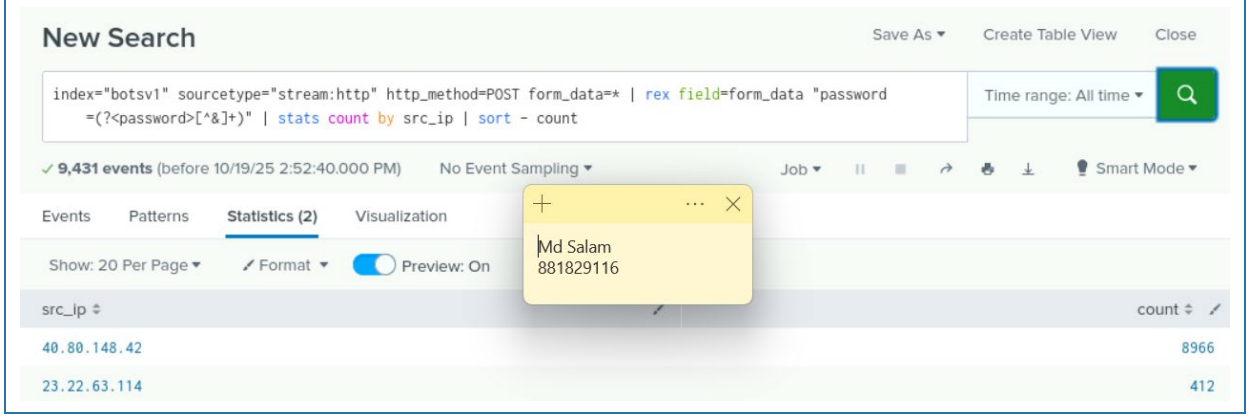
index="botsv1" sourcetype="stream:http" http_method=POST form_data=*

| rex field=form_data "password=(?<password>[^&]+)"

| stats count by src_ip

| sort – count

IP address was 40.80.148.42 having 8966 attempts.



vii. Identification of first password used in a brute force attack

1. Use the **_time** field and **form_data** fields to create a table that displays the times of the password attacks with the oldest attack at the top. Provide a screenshot of the results which includes the SPL statement.

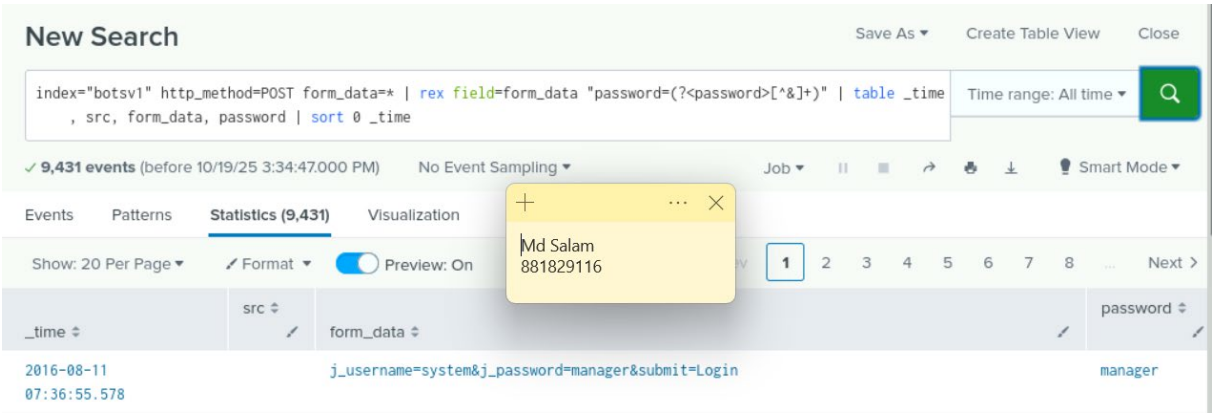
SPL used:

index="botsv1" http_method=POST form_data=*

| rex field=form_data "password=(?<password>[^&]+)"

| table _time, src, form_data, password

| sort 0 _time



2. What time was the first attack made, and what was the password used? (date and time)?

First attack occurred on **11 August 2016 at 07:36:55.578**

First password used: **manager**

3. What was the first password used in the brute force attack?

manager