

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]

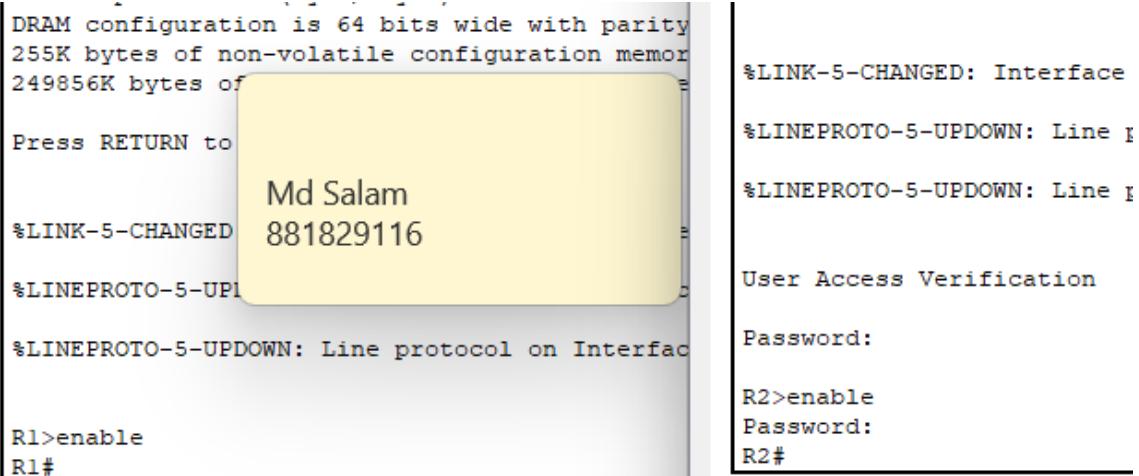
Part 1: Task 1 – Configure and secure network devices

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



The screenshot shows the configuration of two routers, R1 and R2, in Packet Tracer. Router R1's configuration includes setting its name to 'Md Salam' and its ID to '881829116'. Router R2's configuration includes enabling it and setting its password to 'R2#'. The configuration text is as follows:

```
DRAM configuration is 64 bits wide with parity  
255K bytes of non-volatile configuration memory  
249856K bytes of  
  
Press RETURN to  
  
Md Salam  
881829116  
  
%LINK-5-CHANGED  
%LINEPROTO-5-UPDOWN  
%LINEPROTO-5-UPDOWN: Line protocol on Interface  
  
R1>enable  
R1#
```

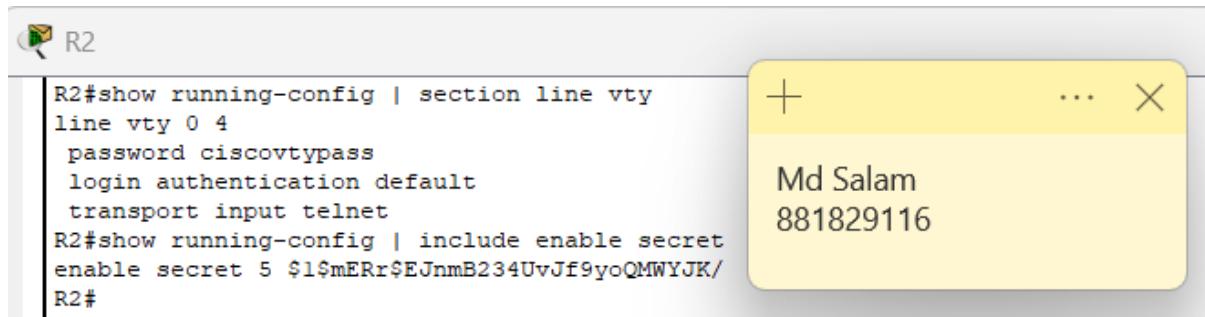
Router R2's configuration text is as follows:

```
%LINK-5-CHANGED: Interface  
%LINEPROTO-5-UPDOWN: Line 1  
%LINEPROTO-5-UPDOWN: Line 1  
  
User Access Verification  
Password:  
R2>enable  
Password:  
R2#
```

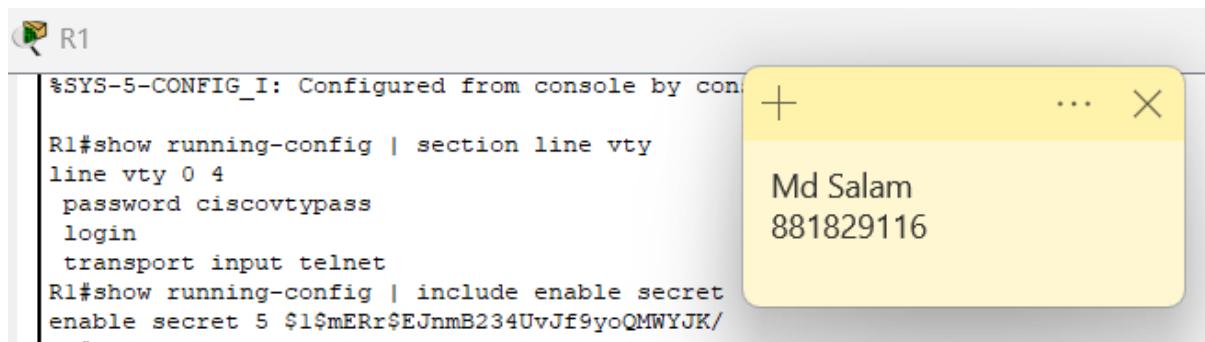
Assessor Sign-off (On-campus students):

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

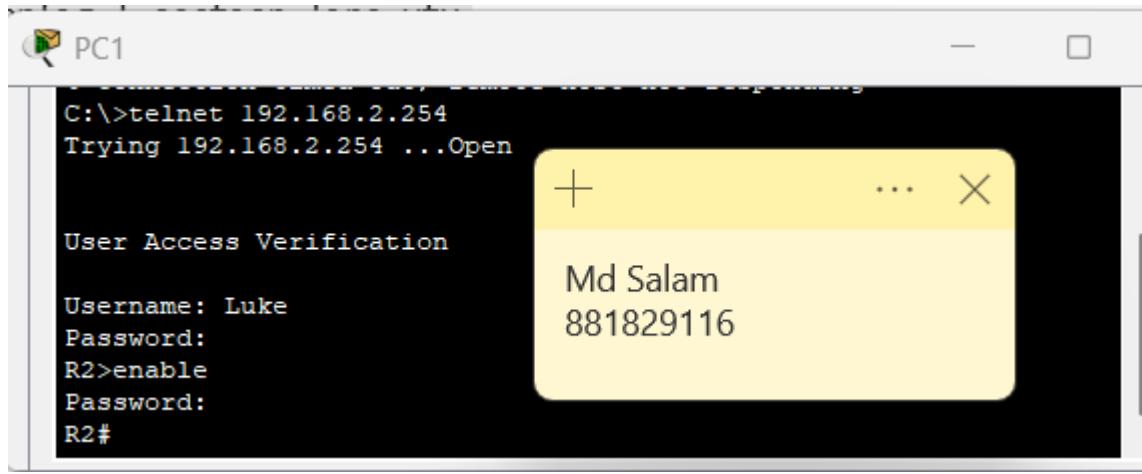


```
R2#show running-config | section line vty
line vty 0 4
password ciscovtypass
login authentication default
transport input telnet
R2#show running-config | include enable secret
enable secret 5 $1$mERr$EJnmB234UvJf9yoQMwYJK/
R2#
```



```
%SYS-5-CONFIG_I: Configured from console by con
R1#show running-config | section line vty
line vty 0 4
password ciscovtypass
login
transport input telnet
R1#show running-config | include enable secret
enable secret 5 $1$mERr$EJnmB234UvJf9yoQMwYJK/
R1#
```

Successfully connected from PC1 to R2 using Telnet:



```
C:\>telnet 192.168.2.254
Trying 192.168.2.254 ...Open

User Access Verification

Username: Luke
Password:
R2>enable
Password:
R2#
```

Assessor Sign-off (On-campus students):

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

- 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

```
%SYS-5-CONFIG_I: Configured from console by console
R2#show run | include ^aaa|radius-server|^username
aaa new-model
aaa authentication login default group radius local
username Finance_Manager privilege 10 secret 5 $1$mERr$11CO98w.wmqbJocLfij9Z/
username Luke secret 5 $1$mERr$WyERf6zeJxUdxnbSaykKg0
username Matthew secret 5 $1$mERr$L2QBQvvaComg8kl/qWrVO/
username user1 secret 5 $1$mERr$zddThMw7UwTxDzRtJKKhB.
R2#ping 192.168.2.253
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.253, timeout is 2 seconds:
.!!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
R2#
```

Ping from router to Radius server (successful)

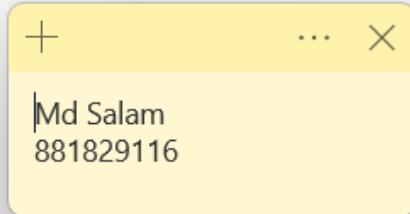
```
[Connection to 192.168.2.254 closed by foreign host]
C:\>telnet 192.168.2.254
Trying 192.168.2.254 ...Open
User Access Verification
Username: Luke
Password:
R2>enable
Password:
R2#
```

Assessor Sign-off (On-campus students):

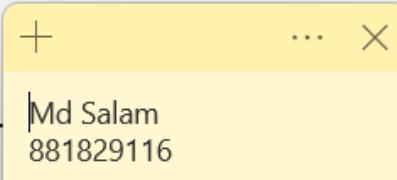
- 1.4. Provide config file or screenshot of running configuration for each router accompanying the config text as part of the report submission using procedures as outlined in the recommended lab guidelines manuals:

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
.
```

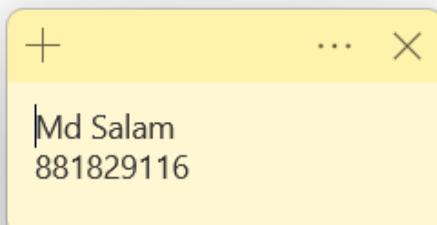


```
R2#show running-config | include ^aaa|radius-server|^username|line vty
aaa new-model
aaa authentication login default local
username Finance_Manager privilege 10 secret 5 $1$mERr$11C098w.wmgbJocLfij9Z/
username Luke secret 5 $1$mERr$WyERf6zeJxUdxnbSsykKg0
username Matthew secret 5 $1$mERr$L2QBQvvvaComg8kl/qWrVO/
username user1 secret 5 $1$mERr$zddThMw7UwTxDzRtJPKhB.
line vty 0 4
R2#
```



```
:
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#
```



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

Admin PC

Physical Config Desktop Programming Attributes

Web Browser < > URL: https://192.168.1.1/frameWlanEdit.html Go Stop

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

WLANS WLANS > Edit 'Staff'

General Security QoS Policy-Mapping Advanced

Layer 2 Layer 3 AAA Servers

Layer 2 Security: WPA+WPA2
MAC Filtering:

Fast Transition:
Protected Management Frame: PMP: Enabled

WPA+WPA2 Parameters: WPA Policy:
WPA2 Policy:
WPA2 Encryption: AES TKIP

Authentication Key Management: 802.1X: Enable
CCKM: Enable
PSK: Enable
FT 802.1X: Enable

Admin PC

Physical Config Desktop Programming Attributes

Web Browser < > URL: https://192.168.1.1/frameWlan.html Go Stop

CISCO MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home

WLANS WLANS

Current Filter: [Change Filter] [Clear Filter] Create New Go

WLAN ID	Type	Profile Name	WLan SSID	Admin Status	Security Policies
1	WLAN	Staff	Staff	Enabled	[WPA2][Auth(PSK)]
2	WLAN	Guest	Guest	Enabled	None

Laptop 2

Physical Config Desktop Programming Attributes

GLOBAL Settings Algorithm Settings INTERFACE Wireless0 Bluetooth

Wireless0

Port Status: On
Bandwidth: 300 Mbps
MAC Address: 0090.21E0.7063
SSID: Staff

Authentication: Disabled WEP WEP Key: Cisco123
 WPA-PSK PSK Pass Phrase: Cisco123
 WPA WPA2 Method: MD5
 802.1X Password: MD5
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: FE80::290:21FF:FE00:7063
Link Local Address: FE80::290:21FF:FE00:7063

Assessor Sign-off (On-campus students):

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

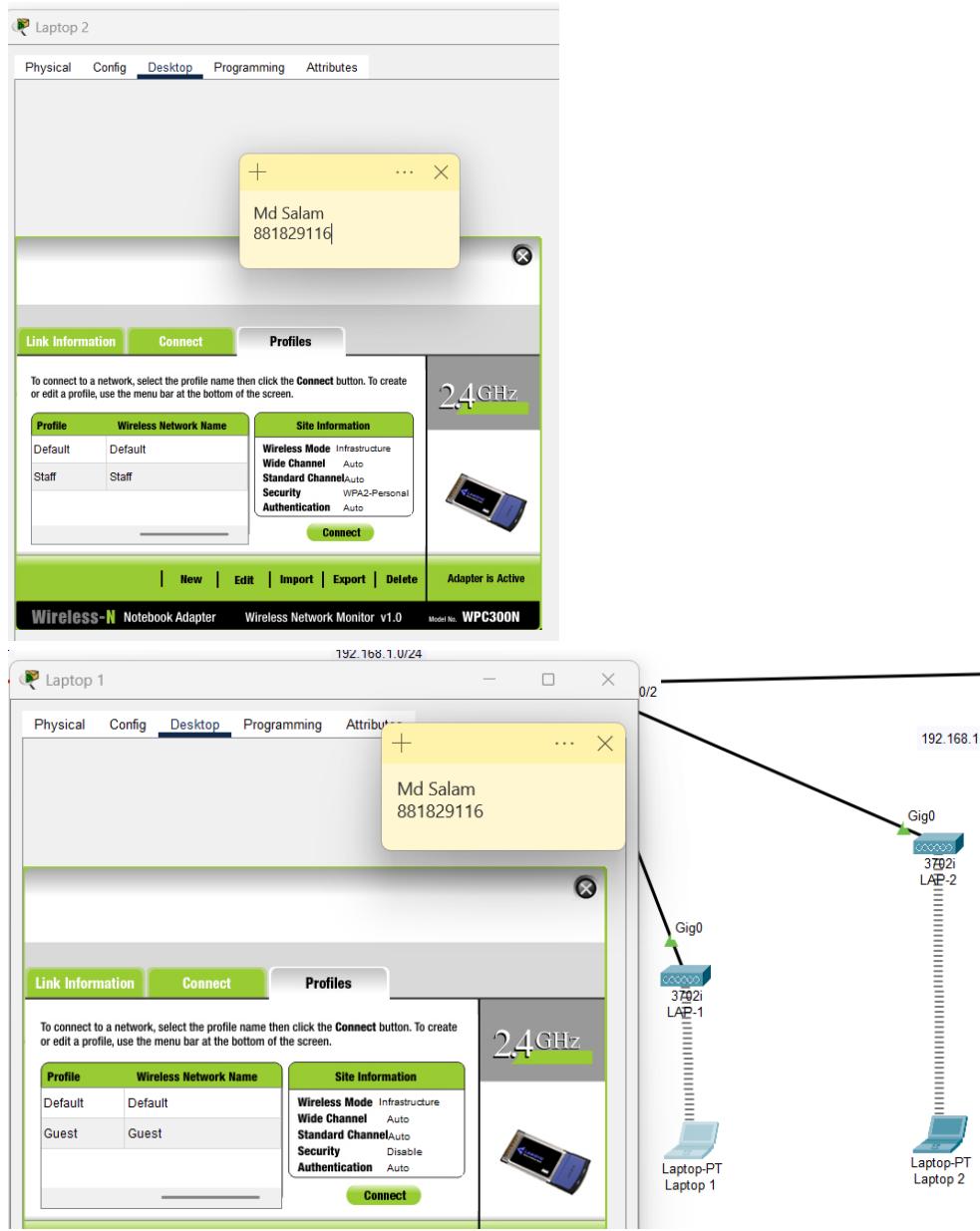
The **Wireless Network Monitor** tool in Packet Tracer was used to simulate WLAN discovery, similar to utilities such as **NetStumbler** or **Wireshark** in real environments. The scan detected the SSIDs “**Staff**” and “**Guest**,” including their channel, signal strength, and security types.

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):

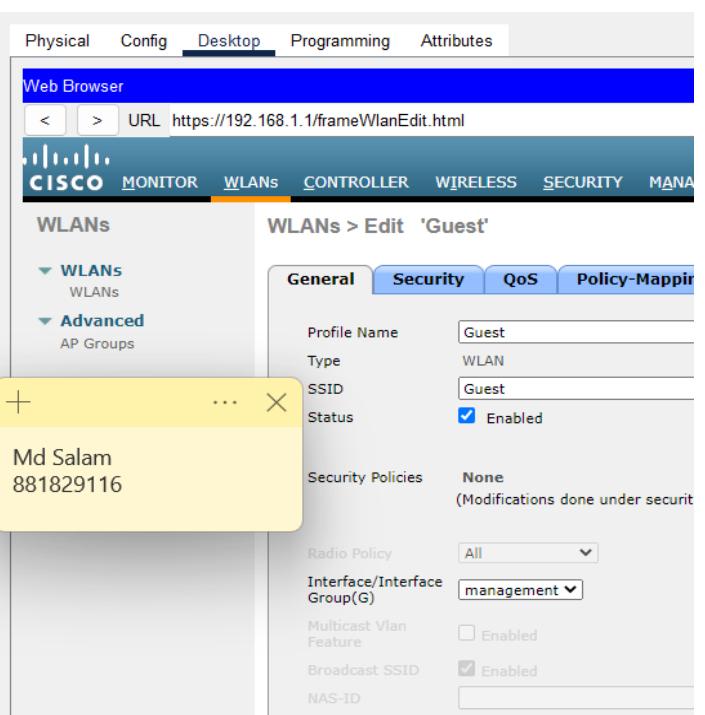
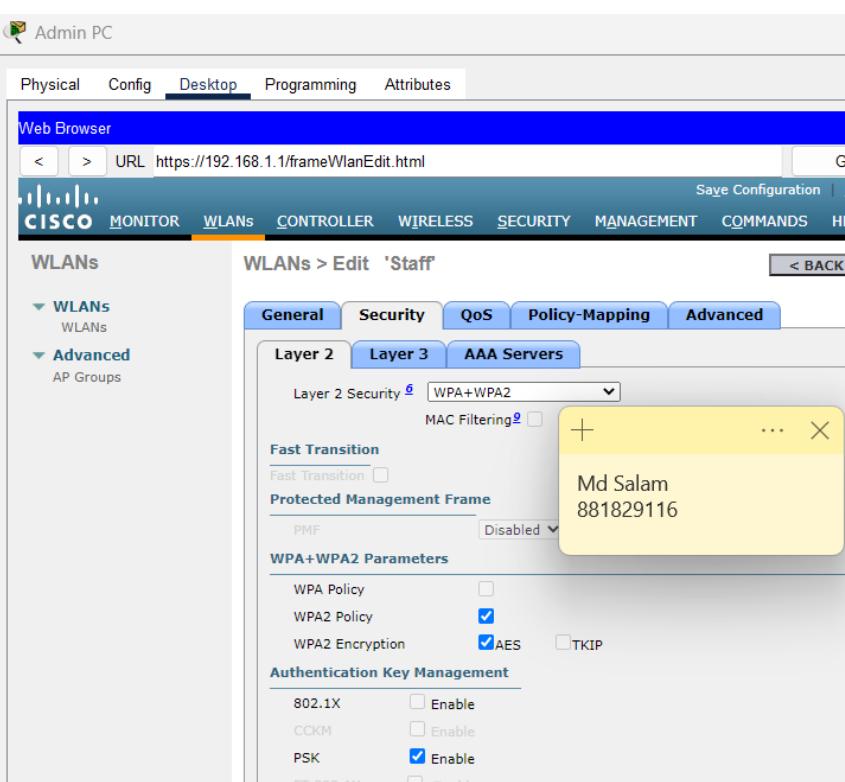
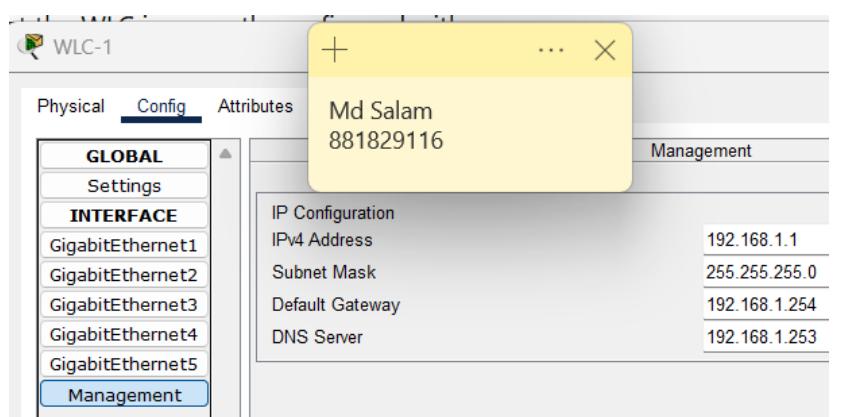
2.3. Develop a WLAN security checklist

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

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	<input checked="" type="radio"/> On	<input type="radio"/> 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

Physical Config

GLOBAL

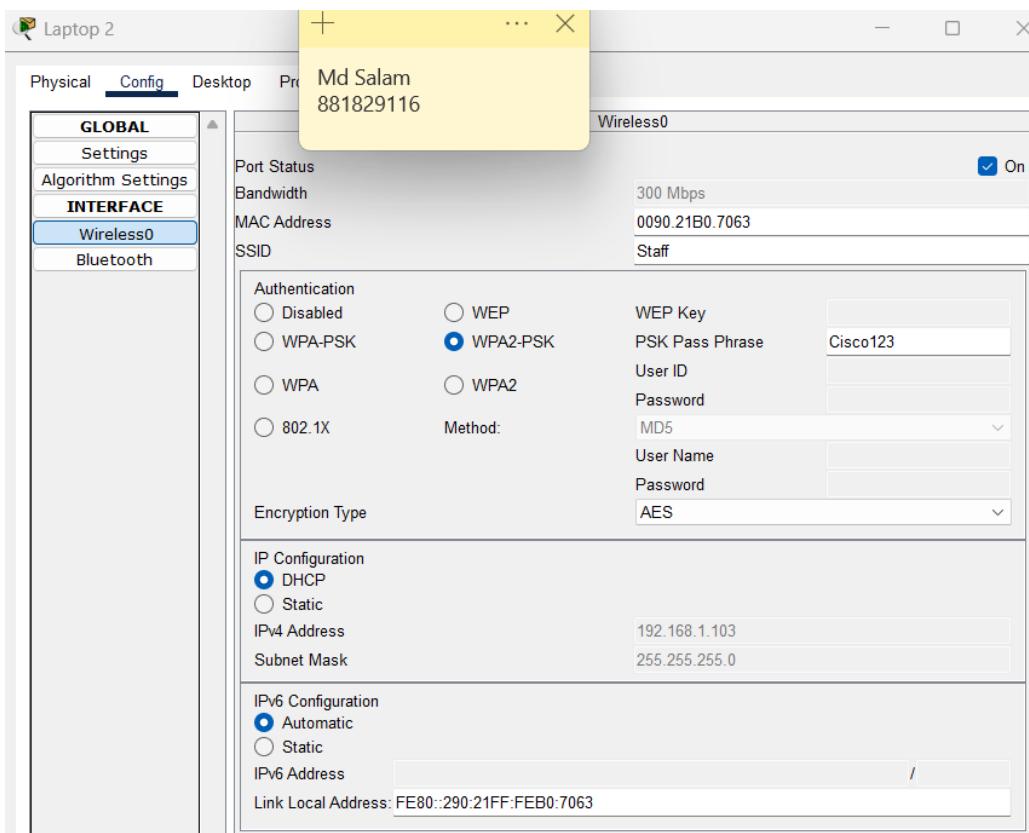
- Settings
- Algorithm Settings

INTERFACE

- Wireless0**
- Bluetooth

Md Salam
881829116

Port Status	Wireless0	On
Bandwidth	300 Mbps	
MAC Address	0001.C959.9E14	
SSID	Guest	
Authentication		
<input checked="" type="radio"/> Disabled	<input type="radio"/> WEP	WEP Key
<input type="radio"/> WPA-PSK	<input type="radio"/> WPA2-PSK	PSK Pass Phrase
<input type="radio"/> WPA	<input type="radio"/> WPA2	User ID
<input type="radio"/> 802.1X	Method:	Password
Encryption Type		
<input checked="" type="radio"/> DHCP	Disabled	
<input type="radio"/> Static		
IPv4 Address	192.168.1.107	
Subnet Mask	255.255.255.0	
IPv6 Configuration		
<input checked="" type="radio"/> Automatic		
<input type="radio"/> Static		
IPv6 Address	/	
Link Local Address: FE80::201:C9FF:FE59:9E14		



```

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

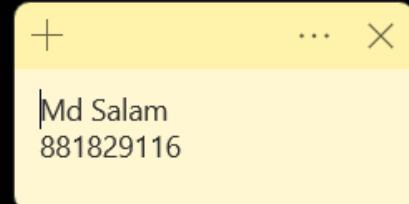
Complete the following steps:

- 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)

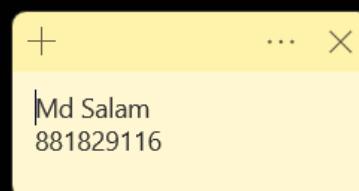
mysql> CREATE DATABASE salam;
Query OK, 1 row affected (0.00 sec)

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



```
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)
```



```
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)
```

```
To permanently disable
---
```

```
> show dbs
admin 0.000GB
config 0.000GB
local 0.000GB
> use salam
switched to db salam
> db.createCollection("vulnerabilities")
{ "ok" : 1 }
> show dbs
admin 0.000GB
config 0.000GB
local 0.000GB
salam 0.000GB
>
```

+ ... X

Md Salam
881829116

```
> db.vulnerabilities.insert({ a_number:'A1', type:'Injection', threatAgents:'application specific',
exploitability:'3', "security weakness":{ prevalence:'2', detectability:'3' }, "impacts":{ technical:'3', business:'business specific', } })
writeResult({ "nInserted" : 1 })
>
```

+ ... X

Md Salam
881829116

```
> db.vulnerabilities.find({ "impacts.technical": "3" }).pretty()
```

```
{
  "_id" : ObjectId("68ad92e092f27224c75ba815"),
  "a_number" : "A1",
  "type" : "Injection",
  "threatAgents" : "application specific",
  "exploitability" : "3",
  "security weakness" : {
    "prevalence" : "2",
    "detectability" : "3"
  },
  "impacts" : {
    "technical" : "3",
    "business" : "business specific"
  }
}

{
  "_id" : ObjectId("68ad963792f27224c75ba817"),
  "a_number" : "A6",
  "type" : "Insecure Deserialization",
  "threatAgents" : "application specific",
  "exploitability" : "1",
  "security weakness" : {
    "prevalence" : "2",
    "detectability" : "2"
  },
  "impacts" : {
    "technical" : "3",
    "business" : "business specific"
  }
}
```

+ ... X

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.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. On the left, the navigation pane includes 'Inbound Rules' (selected), 'Outbound Rules', 'Connection Security Rules', and 'Monitoring'. A yellow callout box highlights 'Md Salam' and '881829116'. The main pane displays the 'Inbound Rules' table:

Name	Group	Profile	Enabled
Block inbound ICMP (Ping)	All	Yes	
Block external inbound traffic	All	Yes	
@{Microsoft.DesktopAppInstaller_1.26.43...}	Domain	Yes	
@{Microsoft.StorePurchaseApp_22507.14...}	Domain	Yes	
@{Microsoft.WindowsFeedbackHub_1.25...}	Domain	Yes	
@FirewallAPI.dll,-80201	All	Yes	
@FirewallAPI.dll,-80206	All	Yes	
ms-resource:ProductPkgDisplayName (78E1CD88-49E3-476E-B926-...)	Public	Yes	
ms-resource:ProductPkgDisplayName (78E1CD88-49E3-476E-B926-...)	Private	Yes	
ms-resource:ProductPkgDisplayName (78E1CD88-49E3-476E-B926-...)	Public	Yes	
ms-resource:ProductPkgDisplayName (78E1CD88-49E3-476E-B926-...)	Private	Yes	
AllJoyn Router (TCP-In)	AllJoyn Router	Domain	Yes
AllJoyn Router (UDP-In)	AllJoyn Router	Domain	Yes
App Installer	App Installer	Domain	Yes
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No
BranchCache Hosted Cache Server (HTTP...	BranchCache - Hosted Cach...	All	No
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No
Connected Devices Platform - Wi-Fi Dire...	Connected Devices Platform	Public	Yes
Connected Devices Platform (TCP-In)	Connected Devices Platform	Domain	Yes
Connected Devices Platform (UDP-In)	Connected Devices Platform	Domain	Yes
Core Networking - Destination Unreacha...	Core Networking	All	Yes
Core Networking - Destination Unreacha...	Core Networking	All	Yes
Core Networking - Dynamic Host Config...	Core Networking	All	Yes
Core Networking - Dynamic Host Config...	Core Networking	All	Yes
Core Networking - Internet Group Mana...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Do...	Core Networking	All	Yes
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes
Core Networking - Parameter Problem (I...	Core Networking	All	Yes
Core Networking - Router Advertisement...	Core Networking	All	Yes
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes
Core Networking - Teredo (UDP-Out)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Private...	No
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Domain	No
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Private...	No
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Domain	No
Desktop App Web Viewer	Desktop App Web Viewer	All	Yes

A detailed properties window for the 'Block inbound ICMP (Ping)' rule is open, showing the 'Protocols and Ports' tab. It specifies 'Protocol type: ICMPv4', 'Protocol number: 1', and 'Local port: All Ports'. The 'Internet Control Message Protocol (ICMP) settings' section is also visible.

The screenshot shows the Windows Defender Firewall with Advanced Security interface. The navigation pane includes 'Inbound Rules' (selected), 'Outbound Rules' (highlighted with a yellow box), 'Connection Security Rules', and 'Monitoring'. A yellow callout box highlights 'Md Salam' and '881829116'. The main pane displays the 'Outbound Rules' table:

Name	Group	Profile	Enabled
Connected Devices Platform (UDP-Out)	Connected Devices Platform	Domain	Yes
Core Networking - DNS (UDP-Out)	Core Networking	All	Yes
Core Networking - Dynamic Host Config...	Core Networking	All	Yes
Core Networking - Dynamic Host Config...	Core Networking	All	Yes
Core Networking - Group Policy (LSASS-...)	Core Networking	Domain	Yes
Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes
Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes
Core Networking - Internet Group Mana...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes
Core Networking - Multicast Listener Do...	Core Networking	All	Yes
Core Networking - Multicast Listener Qu...	Core Networking	All	Yes
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes
Core Networking - Multicast Listener Rep...	Core Networking	All	Yes
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes
Core Networking - Neighbor Discovery S...	Core Networking	All	Yes
Core Networking - Packet Too Big (ICMP...	Core Networking	All	Yes
Core Networking - Parameter Problem (I...	Core Networking	All	Yes
Core Networking - Router Advertisement...	Core Networking	All	Yes
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes
Core Networking - Teredo (UDP-Out)	Core Networking	All	Yes
Core Networking - Time Exceeded (ICMP...	Core Networking	All	Yes
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Private...	No
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Domain	No
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Private...	No
Core Networking Diagnostics - ICMP Ech...	Core Networking Diagnostics	Domain	No
Desktop App Web Viewer	Desktop App Web Viewer	All	Yes

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

```
C:\Users\student>ipconfig
Windows IP Configuration

Ethernet adapter Ethernet 4:
  Connection-specific DNS Suffix . .
  Link-local IPv6 Address . . . . : fe80::d559:2b2b:cc9b:5d62%3
  IPv4 Address. . . . . : 192.168.0.50
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 192.168.0.1

C:\Users\student>ping 192.168.0.103

Pinging 192.168.0.103 with 32 bytes of data:
Reply from 192.168.0.103: bytes=32 time<1ms TTL=64
Reply from 192.168.0.103: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.103:
  Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
  Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
Control-C
^C
C:\Users\student>
```

Ping from Kali to Windows10 fails → inbound traffic blocked

```
[student@kali1:~] $ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host noprefixroute
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
  link/ether 00:15:5d:00:07:05 brd ff:ff:ff:ff:ff:ff
  inet 192.168.0.103/24 brd 192.168.0.255 scope global dynamic noprefixroute
    valid_lft 681781sec preferred_lft 681781sec
    inet6 fe80::215:5dff:fe00:705/64 scope link noprefixroute
      valid_lft forever preferred_lft forever
[student@kali1:~] $ ping 192.168.0.50
PING 192.168.0.50 (192.168.0.50) 56(84) bytes of data.
```

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.

```

pfirewall - Notepad
File Edit Format View Help
2025-10-12 18:54:23 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:24 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:25 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:26 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:27 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:28 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:29 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:30 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:31 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:32 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:33 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:33 ALLOW 2 192.168.0.1 224.0.0.1 - - 0 - - - - RECEIVE
2025-10-12 18:54:33 ALLOW 2 192.168.0.50 224.0.0.22 - - 0 - - - - SEND
2025-10-12 18:54:34 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:34 ALLOW TCP 192.168.0.50 72.145.35.118 55117 443 0 - 0 0 0 - - - SEND
2025-10-12 18:54:35 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
2025-10-12 18:54:36 ALLOW UDP 192.168.0.50 168.63.129.16 63920 53 0 - - - - - SEND
2025-10-12 18:54:36 ALLOW TCP 192.168.0.50 23.221.133.182 55118 443 0 - 0 0 0 - - - SEND
2025-10-12 18:54:36 DROP ICMP 192.168.0.103 192.168.0.50 - - 84 - - - 8 0 - RECEIVE
>>>

```

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:

```
student@debian-DL:~$ sudo suricata -i eth0 --init-errors-fatal &
[2] 3745
student@debian-DL:~$ 12/10/2025 -- 21:13:47 - <Notice> - This is Suricata version 6.0.10 RELEASE
ASE running in SYSTEM mode
12/10/2025 -- 21:13:47 - <Error> - [ERRCODE] - [ERRCODE] - fanout not supported by kernel: Kernel too old or cluster-id
12/10/2025 -- 21:13:47 - <Notice> - all 1 reads, 4 management threads initialized, engine started.

student@debian-DL:~$ jobs -l
[1]+ 3731 Stopped (tty output)      sudo suricata -i eth0 --init-errors-fatal
[2]- 3745 Running                 sudo suricata -i eth0 --init-errors-fatal &
student@debian-DL:~$
```

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

```
student@debian-DL:~$ jobs -l
[1]+ 3731 Stopped (tty output)      sudo suricata -i eth0 --init-errors-fatal
[2]- 3745 Running                 sudo suricata -i eth0 --init-errors-fatal &
student@debian-DL:~$ sudo tail -f /var/log/suricata/fast.log
10/12/2025-21:20:23.262624  [**] [1:1000002:1] ICMP connection attempt [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.103:8 -> 192.168.0.101:0
10/12/2025-21:20:23.262686  [**] [1:1000002:1] ICMP connection attempt [**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.101:0 -> 192.168.0.103:0
10/12/2025-21:21:35.712121  [**] [1:1000003:1] TELNET connection attempt [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.0.103:41266 -> 192.168.0.101:23
^C
student@debian-DL:~$ sudo cat /var/lib/suricata/rules/test.rules
alert icmp any any -> $HOME_NET any (msg:"ICMP connection attempt"; sid:1000002; rev:1;)
alert tcp any any -> $HOME_NET 23 (msg:"TELNET connection attempt"; sid:1000003; rev:1;)
student@debian-DL:~$
```

Assessor Sign-off (On-campus students):

Part 1: Task 4 – Install and configure proxy server

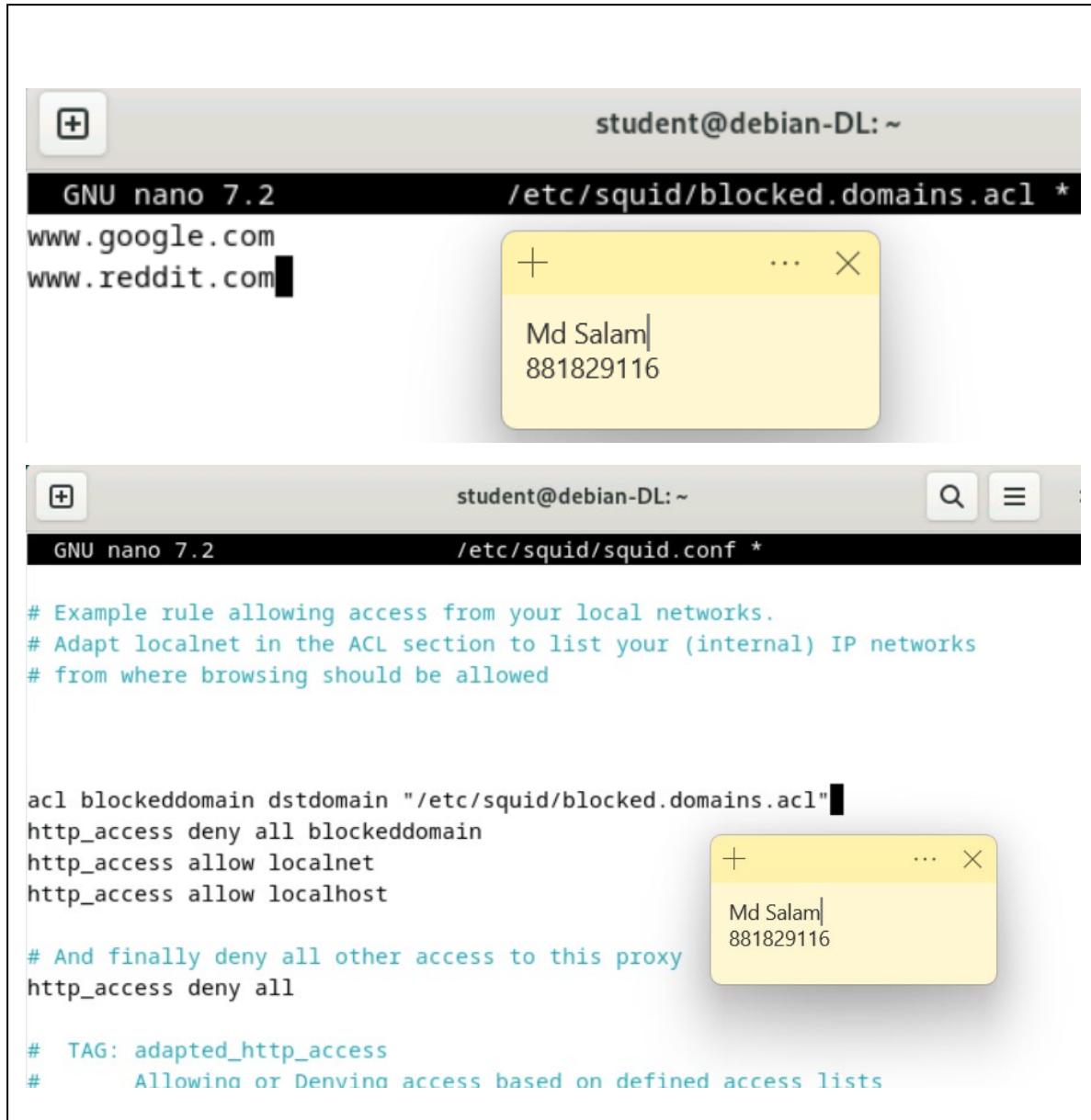
Document the data analysis completed below. Where directed, TAFE digital students to provide screenshots of completed steps. On-campus students may demonstrate the corresponding step in class, with the assessor signing off the step.

- 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:
  libmldb-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+de
b12u3 [315 kB]
get:4 http://deb.debian.org/debian bookworm/main amd64 squid 1.542+bu
[16.3 kB]
```

```
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)"
```



```
student@debian-DL:~
```

```
GNU nano 7.2          /etc/squid/blocked.domains.acl *
```

```
www.google.com
www.reddit.com
```

```
+ ... ×
```

```
Md Salam|
881829116
```

```
student@debian-DL:~
```

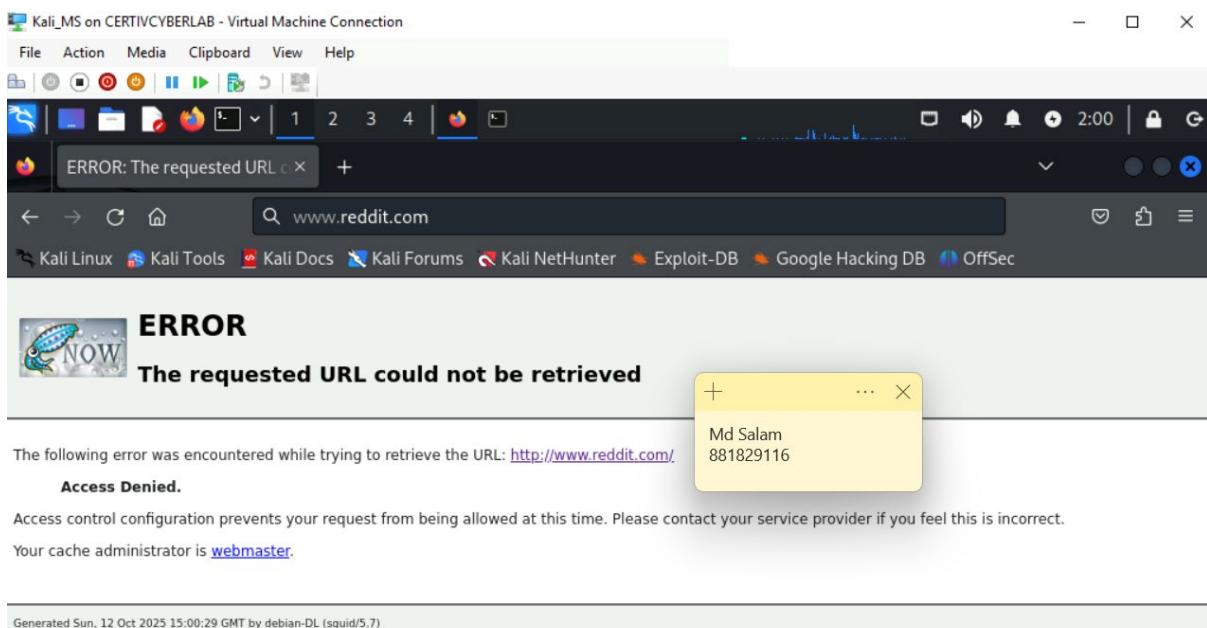
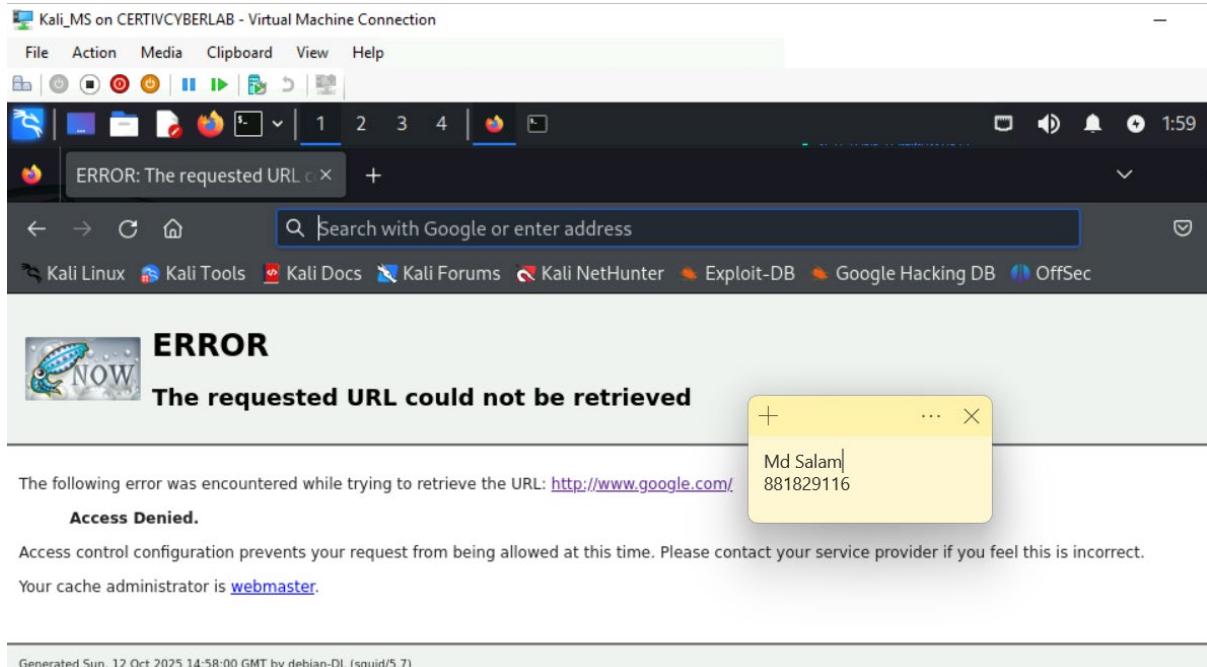
```
GNU nano 7.2          /etc/squid/squid.conf *
```

```
# 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
```



student@debian-DL: ~

```
GNU nano 7.2          /var/log/squid/access.log
1760281039.715      13 192.168.0.103 TCP_TUNNEL/200 39 CONNECT push.services.mozilla.com:443 >
1760281040.006      193 192.168.0.103 TCP_MISS/200 1230 POST http://o.pki.goog/wr2 - HIER_DIR>
1760281040.615      952 192.168.0.103 TCP_TUNNEL/200 12411 CONNECT safebrowsing.googleapis.com>
1760281040.783      99 192.168.0.103 TCP_MISS/200 1231 POST http://o.pki.goog/s/wr3/prs - HIE>
1760281080.207      0 192.168.0.103 TCP_DENIED/403 4188 GET http://www.google.com/ - HIER_NO>
1760281080.301      0 192.168.0.103 TCP_HIT/200 13060 GET http://debian-dl:3128/squid-intern>
1760281080.314      0 192.168.0.103 TCP_DENIED/403 4158 GET http://www.google.com/favicon.ic>
1760281210.326      170664 192.168.0.103 TCP_TUNNEL/200 3844 CONNECT push.services.mozilla.com:44>
1760281210.327      171130 192.168.0.103 TCP_TUNNEL/200 9549 CONNECT contile.services.mozilla.com>
1760281211.327      170722 192.168.0.103 TCP_TUNNEL/200 5439 CONNECT ads-img.mozilla.org:443 - HI>
1760281215.328      175904 192.168.0.103 TCP_TUNNEL/200 3830 CONNECT content-signature-2.cdn.mozi>
1760281217.329      177447 192.168.0.103 TCP_TUNNEL/200 15509 CONNECT firefox.settings.services.m>
1760281229.245      0 192.168.0.103 TCP_DENIED/403 4188 GET http://www.reddit.com/ - HIER_NO>
1760281229.333      0 192.168.0.103 TCP_HIT/200 13060 GET http://debian-dl:3128/squid-intern>
1760281229.338      0 192.168.0.103 TCP_DENIED/403 4158 GET http://www.reddit.com/favicon.ic>
```

+ ... ×

Md Salam
881829116

^G Help ^W Where Is ^K Cut ^T Execute ^C Location
^X Exit ^\ Replace ^U Paste ^J Justify ^/ Go To Line

Assessor Sign-off (On-campus students):

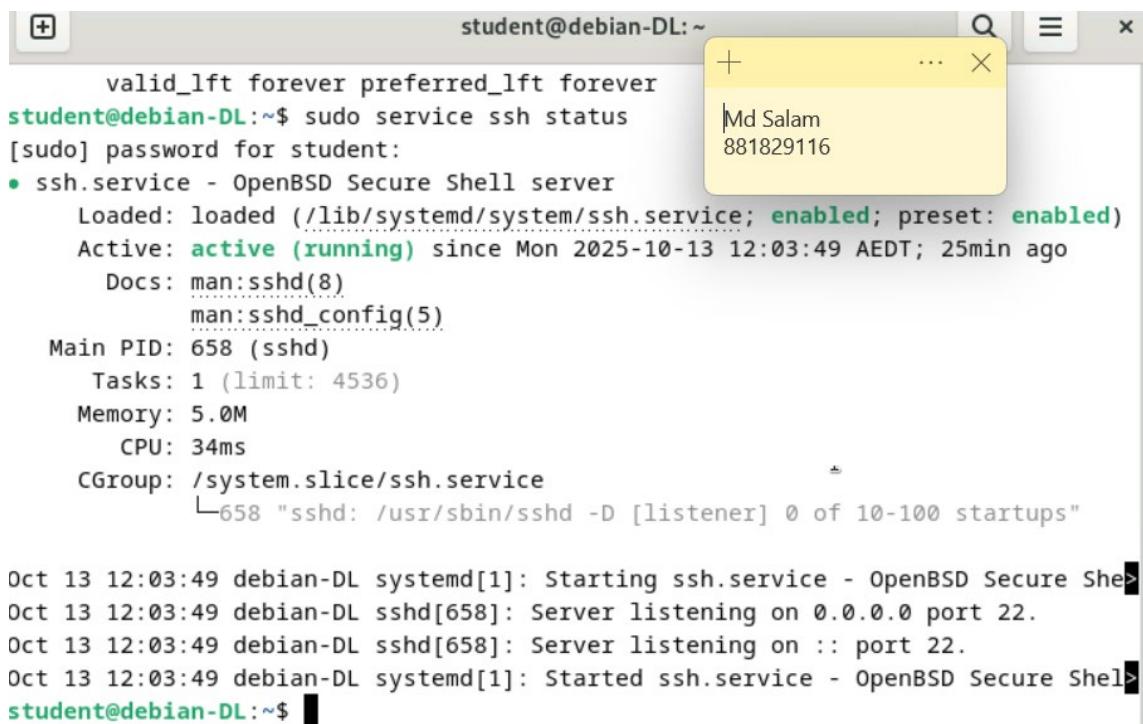
Part 2: Task 1 – Install and configure an SSH Server

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.



```
student@debian-DL:~ valid_lft forever preferred_lft forever
student@debian-DL:~$ sudo service ssh status
[sudo] password for student:
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-10-13 12:03:49 AEDT; 25min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
  Main PID: 658 (sshd)
     Tasks: 1 (limit: 4536)
   Memory: 5.0M
      CPU: 34ms
     CGroup: /system.slice/ssh.service
             └─658 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Oct 13 12:03:49 debian-DL systemd[1]: Starting ssh.service - OpenBSD Secure She>
Oct 13 12:03:49 debian-DL sshd[658]: Server listening on 0.0.0.0 port 22.
Oct 13 12:03:49 debian-DL sshd[658]: Server listening on :: port 22.
Oct 13 12:03:49 debian-DL systemd[1]: Started ssh.service - OpenBSD Secure Shel>
student@debian-DL:~$
```

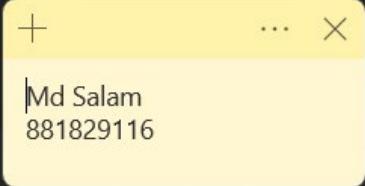
Assessor Sign-off (On-campus students):

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.

```
(student㉿kali1)~]$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/student/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/student/.ssh/id_rsa
Your public key has been saved in /home/student/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:1J+T3g0wVEps9qjmvcubpjHsU5VfWwfVyUaKkmQWFk8 student@kali1
The key's randomart image is:
+---[RSA 4096]---+
| .0+ . oo+|
| +o*o. o+.|
| . == o ..|
| . .+++o +|
| SE ..*. .+|
| .o .. + ..|
| o+o . o |
| .o+o. . |
| o+**+ |
+---[SHA256]---+
[student㉿kali1)~]$ ls -la ~/.ssh/id_*
-rw-r--r-- 1 student student 3434 Oct 13 12:47 /home/student/.ssh/id_rsa
-rw-r--r-- 1 student student 739 Oct 13 12:47 /home/student/.ssh/id_rsa.pub
```



Md Salam
881829116

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.

```
(student㉿kali1)~$ ssh-copy-id student@192.168.0.101
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/student/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
student@192.168.0.101's password:

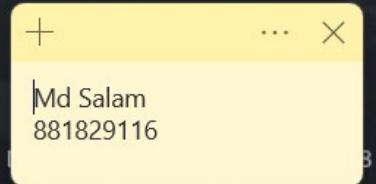
Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'student@192.168.0.101'"
and check to make sure that only the key(s) you wanted were added.

(student㉿kali1)~$ ssh student@192.168.0.101
Enter passphrase for key '/home/student/.ssh/id_rsa':
Linux debian-DL 6.1.0-39-amd64 #1 SMP PREEMPT_DYNAMIC 2025-10-13 13:00:23 UTC x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Oct 13 13:00:23 2025 from 192.168.0.103
student@debian-DL:~$
```



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

The accounting provider maintains a log of connection requests and sessions.

Accounting provider:

Windows Accounting

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

Preshard Key:

+ ... X
Md Salam
881829116

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

Routing and changes to the tree, and then

Meeting the on the right or
Connect this servi

OK

Cancel

Apply

Cluster3_Win10A on CERTIVCYBERLAB - Virtual Machine Connection

File Action Media View Help

Recycle Bin 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 (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 (l)
- 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

Cluster3_Win10B on CERTIVCYBERLAB - Virtual Machine Connection

File Action Media View Help

Command Prompt

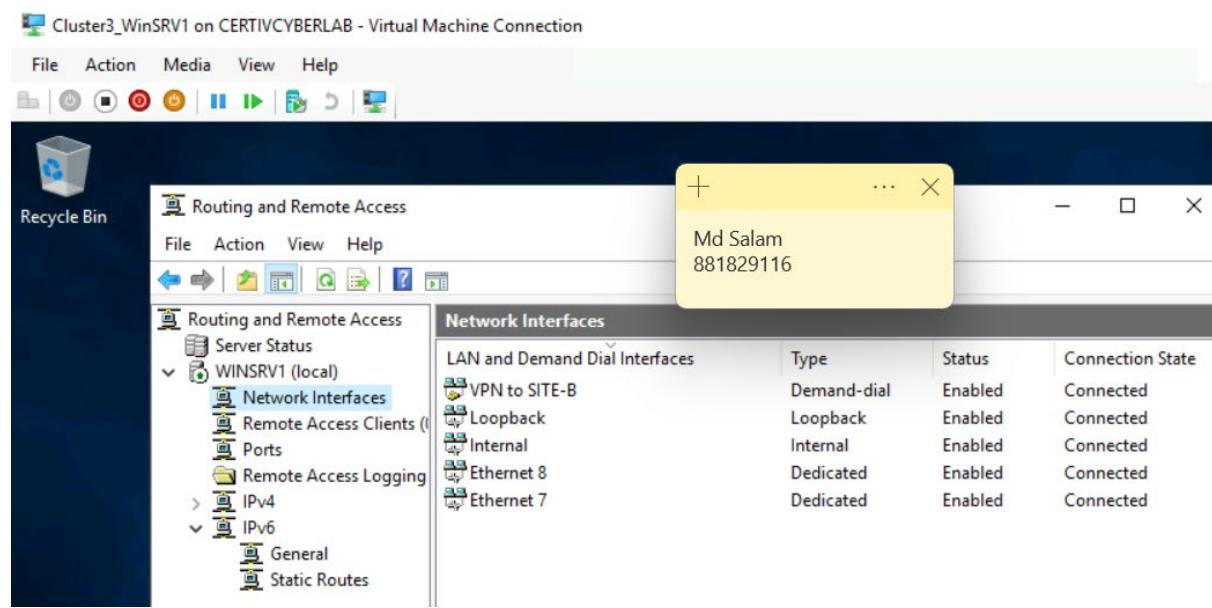
```
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\student>ping 10.10.10.10

Pinging 10.10.10.10 with 32 bytes of data:
Reply from 10.10.10.10: bytes=32 time=2ms TTL=126
Reply from 10.10.10.10: bytes=32 time=1ms TTL=126
Reply from 10.10.10.10: bytes=32 time=3ms TTL=126
Reply from 10.10.10.10: bytes=32 time=2ms TTL=126

Ping statistics for 10.10.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 3ms, Average = 2ms

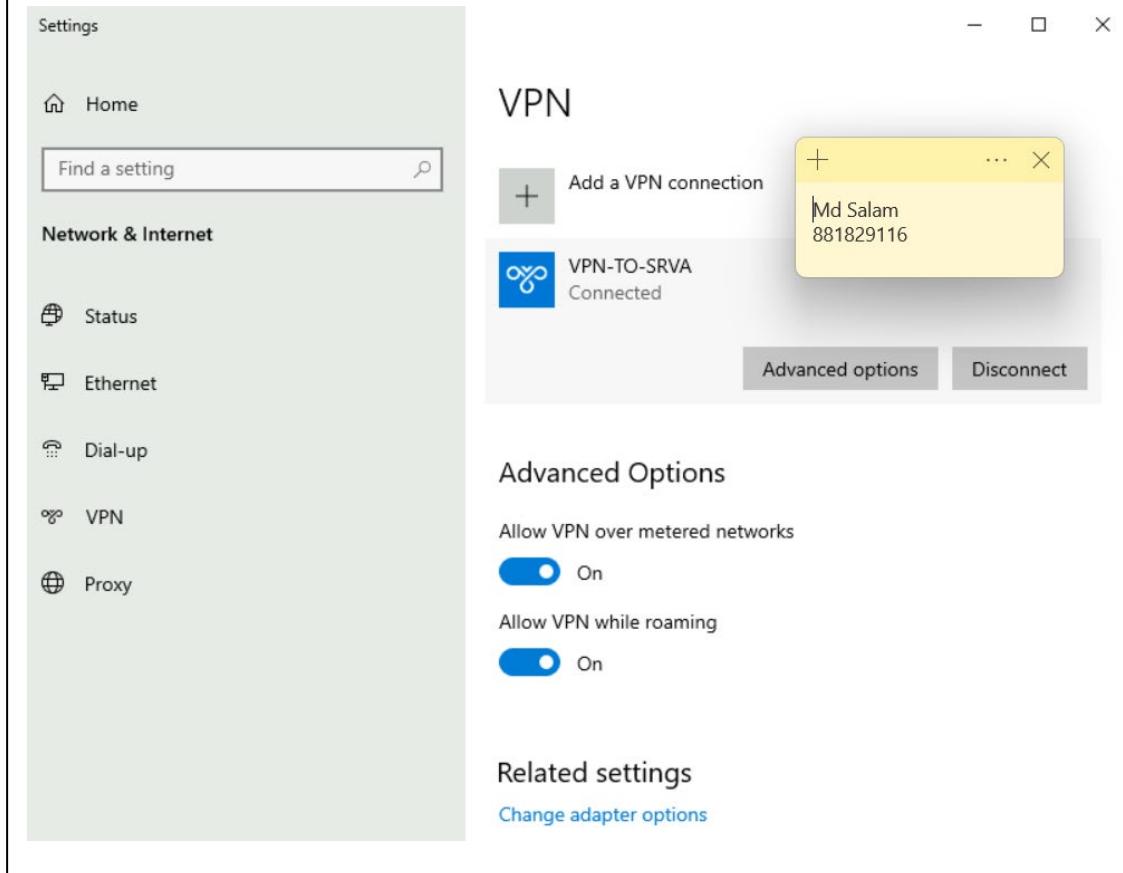
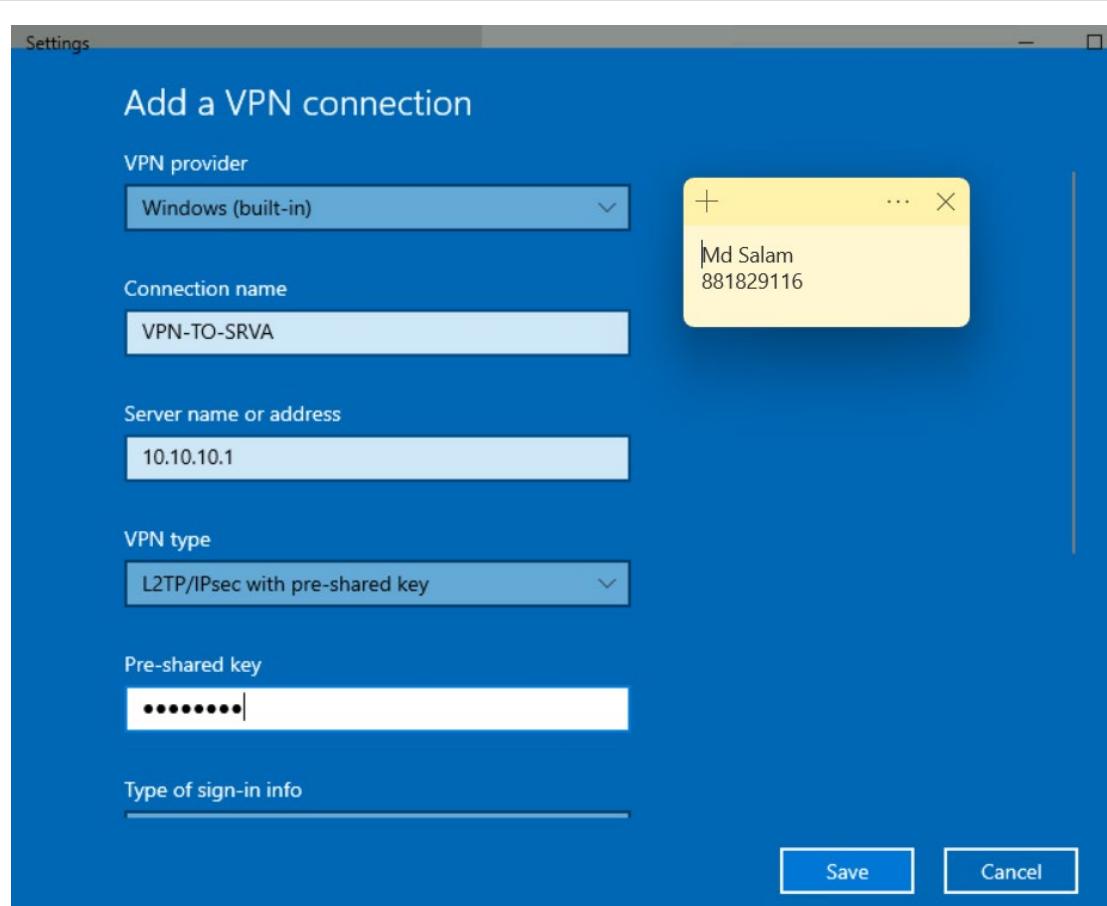
C:\Users\student>
```

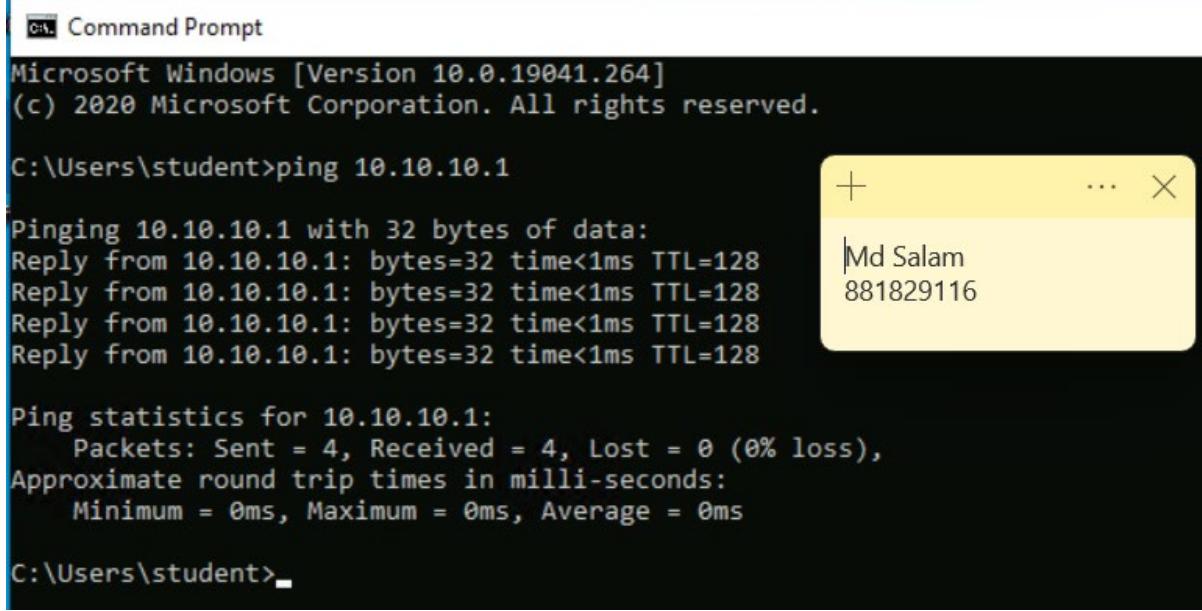


Assessor Sign-off (On-campus students):

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:





```
C:\> Command Prompt
Microsoft Windows [Version 10.0.19041.264]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\student>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
Reply from 10.10.10.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\student>
```

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.

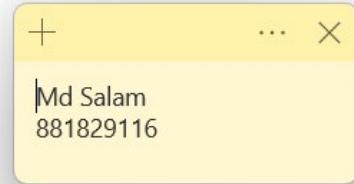
1.1. Successfully install Splunk.

Provide evidence this step is completed:

```
Certificate request self-signature ok
subject=CN = debian-DL, O = SplunkUser
Done
```

```
Waiting for web server at http://127.0.0.1:8000 to be available.....
..... Done
```

If you get stuck, we're here to help.
Look for answers here: <http://docs.splunk.com>



The Splunk web interface is at <http://debian-DL:8000>

```
student@debian-DL:~/Downloads$
```

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

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

Md Salam
881829116

Home

http://localhost:8000/en-US/app/launcher/home

splunk>enterprise Apps

Hello, Administrator

Administrator 1 Messages Settings Activity Help Find

Booksmarks Dashboard Search history Recently viewed Create

My bookmarks (0) Add bookmark

Md Salam
881829116

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:

The screenshot shows two screenshots of the Splunk App Management interface. The top screenshot shows a modal window titled 'Install - Success' with a green checkmark indicating that 'Splunk Datasets Add-On has been successfully installed.' The modal also contains a yellow callout box with the name 'Md Salam' and ID '881829116'. The bottom screenshot shows the main 'Apps' page with a search bar containing 'Dataset'. A yellow callout box highlights the same information ('Md Salam' and ID '881829116') from the modal above.

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

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
```

The screenshot shows a Firefox browser window titled "Debian_MS on CERTIVCYBERLAB". The address bar shows the URL <http://localhost:8000/en-US/app/search/search>. The main content area displays the "Data Summary" page from Splunk. The summary table shows one host entry:

Host	Count	Last Update
DESKTOP-AEOMDP1	30,849	10/17/25 6:22:19.000 PM

About

Your PC is monitored and protected.

The screenshot shows the Windows Security interface for a virtual machine named "DESKTOP-AEOMDP1". The interface displays the following hardware details:

Installed RAM	Processor	Graphics Card	Storage
4.00 GB	Intel(R) Xeon(R) Platinum 8272CL CPU @ 2.60GHz	No dedicated VRAM	50 GB
	2.59 GHz	No GPU installed	26 GB of 50 GB used

At the bottom, there is a "Rename this PC" button.

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:

Splunk > enterprise Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search & Reporting

New Search

index="botsv1"

955,807 events (before 10/17/25 7:56:59.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ ↻ ↺ ↻ ↺ 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 ▾

1 2 3 4 5 6 7 8 ... Next >

	Time	Event
< Hide Fields	All Fields	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 ssrcip=188.243.155.61 srport=6631 srcintf="wan1" dstip=71.39.1.8.122 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 rcvbyte=0 sentpkt=0 appcat="unscanned" crsccore=30 craction=131072 crlevel=high host = 192.168.250.1 source = udp:514 sourcetype = fgt_traffic

SELECTED FIELDS
 a host 8
 a source 24
 a sourcetype 22

INTERESTING FIELDS
 # bytes 100+
 # bytes_in 100+

Activities Firefox ESR Debian_MS on CERTIVCYBERLAB Oct 17 20:37

Splunk > enterprise Apps ▾ Administrator ▾ 1 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find Search & Reporting

New Search

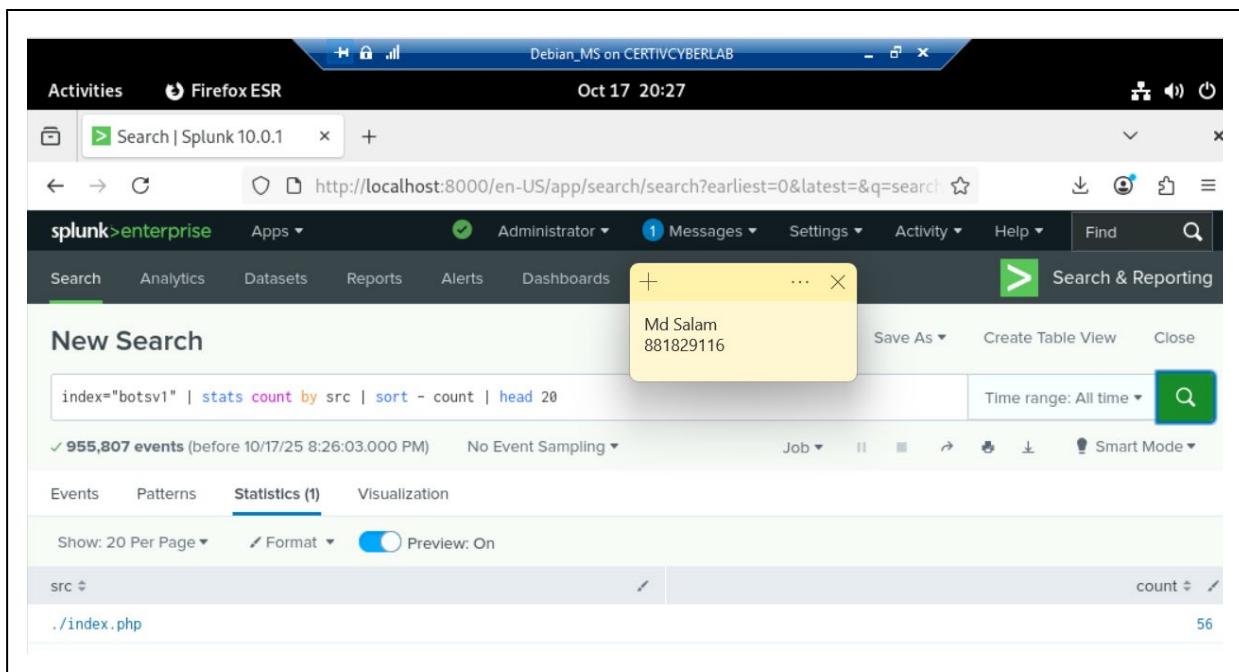
index="botsv1" sourcetype="stream:http" | stats count by status | sort - count | head 5

23,936 events (before 10/17/25 8:37:07.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ ↻ ↺ ↻ ↺ 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



The screenshot shows the Splunk Enterprise search interface. The search bar contains the query `index="botsv1" | stats count by src | sort - count | head 20`. The results table has two columns: `src` and `count`. One visible row shows `./index.php` with a count of 56.

src	count
./index.php	56

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:

New Search

Save As ▾ Create Table View Close

```
index="botsv1" http_method=POST form_data=* | timechart span=10m count by src limit=10
```

Time range: All time ▾



Events		Patterns	Statistics (6)	Visualization							
Show: 20 Per Page ▾	✓ Format ▾	Preview: On			Job ▾	II	III	IV	V	VI	Smart Mode ▾
_time ▾											NULL ▾
2016-08-11 07:30:00											17
2016-08-11 07:40:00											1258
2016-08-11 07:50:00											3630
2016-08-11 08:00:00											2223
2016-08-11 08:10:00											1738
2016-08-11 08:20:00											565

New Search

Save As ▾ Create Table View Close

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

Time range: All time ▾



Events		Patterns	Statistics (1)	Visualization			Job ▾	II	III	IV	V	Smart Mode ▾
Show: 20 Per Page ▾	✓ Format ▾	Preview: On										
src ▾												count ▾
./index.php												28

Assessor Sign-off (On-campus students):

- 1.8. Complete each of the following, according to the instructions provided in each section below:
- Sourcetype table
 - SPL statement table
 - Index of botsv1 and IP address and destination, Top 10 URLs searches
 - Analysis of brute force password attacks
 - 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.

Data Summary

Hosts (1) Sources (5) **Sourcetypes (5)**

filter

Sourcetype	Count	Last Update
Perfmon:CPU Load	2,582	10/18/25 2:16:41.000 PM
Perfmon:Network Interface	3,455	10/18/25 2:16:41.000 PM
WinEventLog:Application	2,460	10/18/25 1:57:26.000 PM
WinEventLog:Security	25,806	10/18/25 2:04:42.000 PM
WinEventLog:System	2,412	10/18/25 2:06:42.000 PM

Md Salam
881829116

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 URLs	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 URLs	index="botsv1" sourcetype=access	stats count by uri

iii. Index of botsv1

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

- How many events did this return?

955,807 events

- What was the SPL statement that you used?

index="botsv1"

iv. IP address source and destination

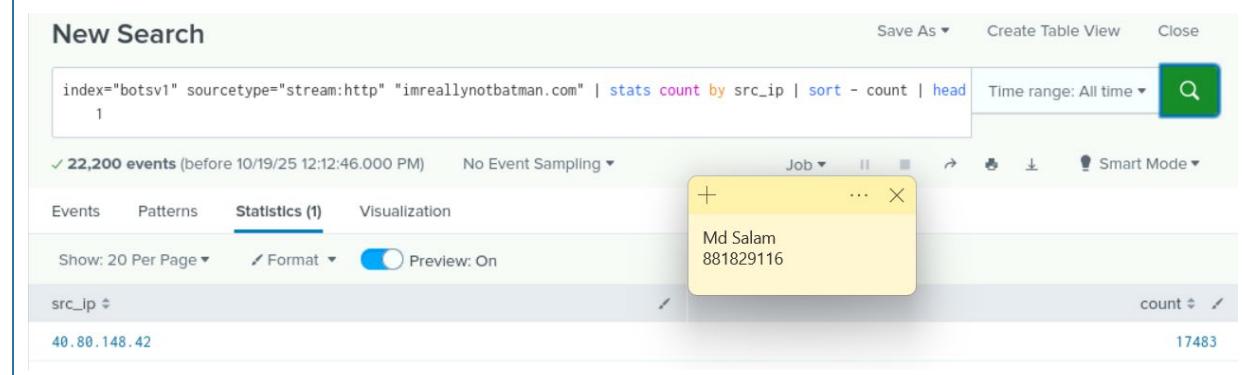
Answer the following questions regarding the IP address responsible for scanning the website.

- What source type did you specify?

stream:http

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

40.80.148.42



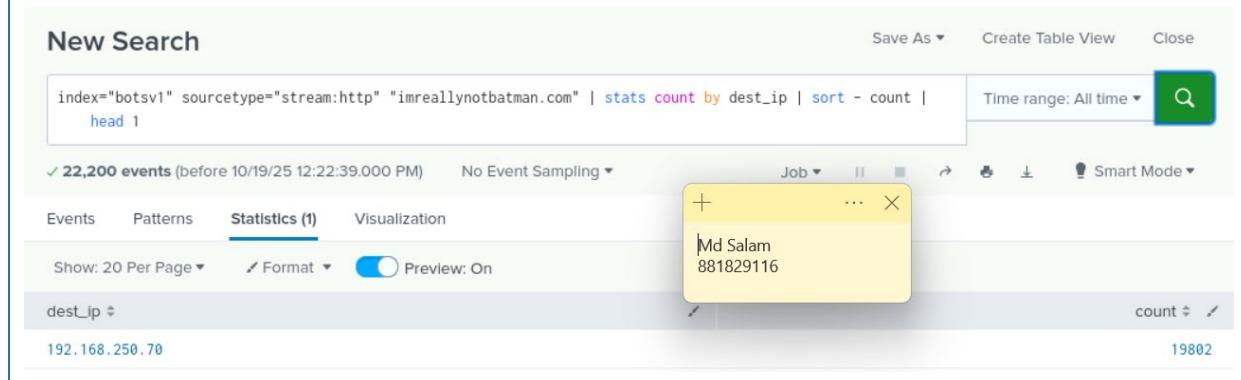
- What was the SPL statement used, if different from the planning document?

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

```
| stats count by src_ip
| sort - count
| head 1
```

- What was the destination IP address that was being scanned?

192.168.250.70

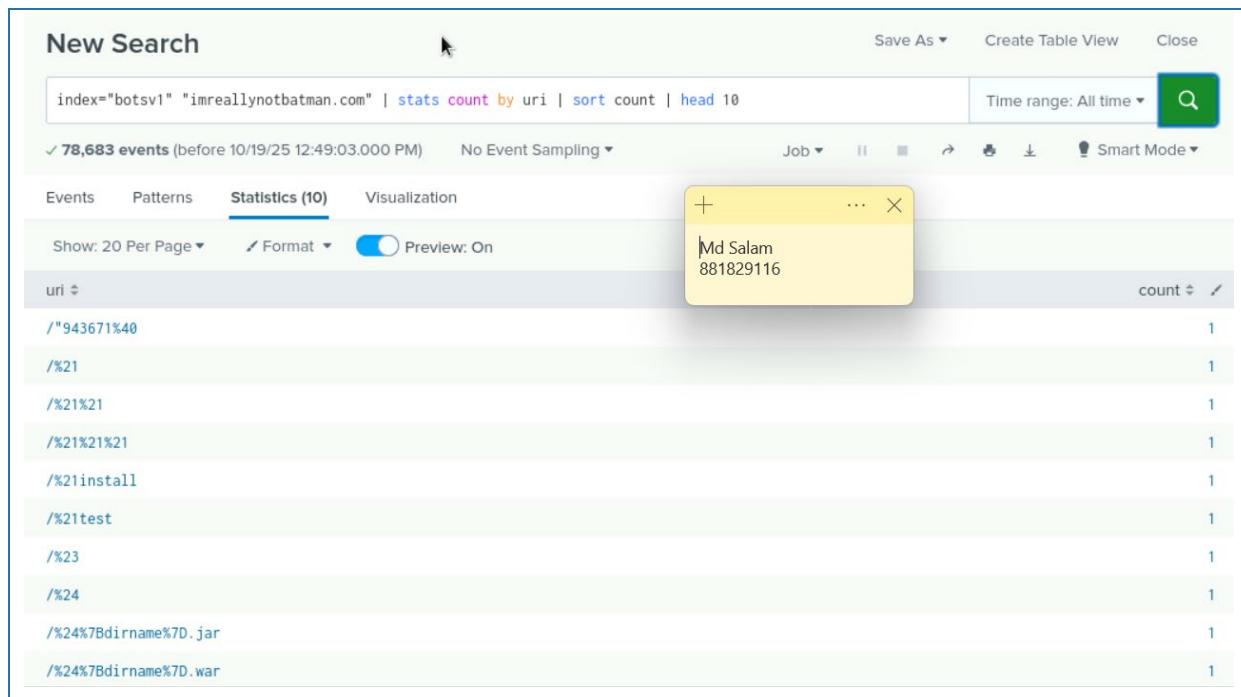


v. Top ten URI's

- 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

- 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
```

New Search

Save As ▾ Create Table View Close

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

Time range: All time ▾

✓ 9,431 events (before 10/19/25 2:25:40.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ Smart Mode ▾

Events Patterns Statistics (9,431) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

Md Salam
881829116

1 2 3 4 5 6 7 8 ... Next >

form_data ▾

```
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=pussy&5b4cc9395cafcef6dab9cad73ceacde7=1
username=admin&passwd=batman&option=com_login&task=login&return=aW5kZXgucGhw&e5ec827a3f67ce0fc546d81f7356acc=1
84a70de902da7c3513582cceba46b40f=1&from=1&layout=default&link=d1cd50917e6d732a5e05c314550120fa5278b7dd&mailto=sample@email.tst&option=com_mail
pg_sleep(6); --
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=rock&4a40c518220c1993f0e02dc4712c5794=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=cool&a09349d0d6bdbf078ad72cf8e9348583=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=sammy&0d3bb0020f70044ffba32f7d0fa7fa88=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=august&9800c58b68f234e562dee5972a58b8d=1
username=admin&task=login&return=aW5kZXgucGhw&option=com_login&passwd=phantom&a083bf4d12c07976186d8a6efa6308cf=1
```

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.

New Search

Save As ▾ Create Table View Close

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

Time range: All time ▾

✓ 9,431 events (before 10/19/25 2:52:40.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ Smart Mode ▾

Events Patterns Statistics (2) Visualization

Show: 20 Per Page ▾ Format ▾ Preview: On

Md Salam
881829116

src_ip ▾ count ▾

40.80.148.42	8966
23.22.63.114	412

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
```

The screenshot shows a Splunk search interface titled "New Search". The search bar contains the following command:

```
index="botsv1" http_method=POST form_data=* | rex field=form_data "password=(?<password>[^&]+)" | table _time  
, src, form_data, password | sort 0 _time
```

The search results indicate 9,431 events found before 10/19/25 3:34:47.000 PM. A tooltip over one event row shows the details: "Md Salam" and "881829116". The results table includes columns for _time, src, and form_data. One visible row from the table is:

_time	src	form_data
2016-08-11 07:36:55.578		j_username=system&j_password=manager&submit=Login

On the right side of the interface, there are buttons for "Save As", "Create Table View", and "Close". Below the search bar, there's a "Time range: All time" dropdown and a green search button. The bottom navigation bar includes "Events", "Patterns", "Statistics (9,431)", "Visualization", "Job", "Smart Mode", and pagination controls (1-8, Next >).

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