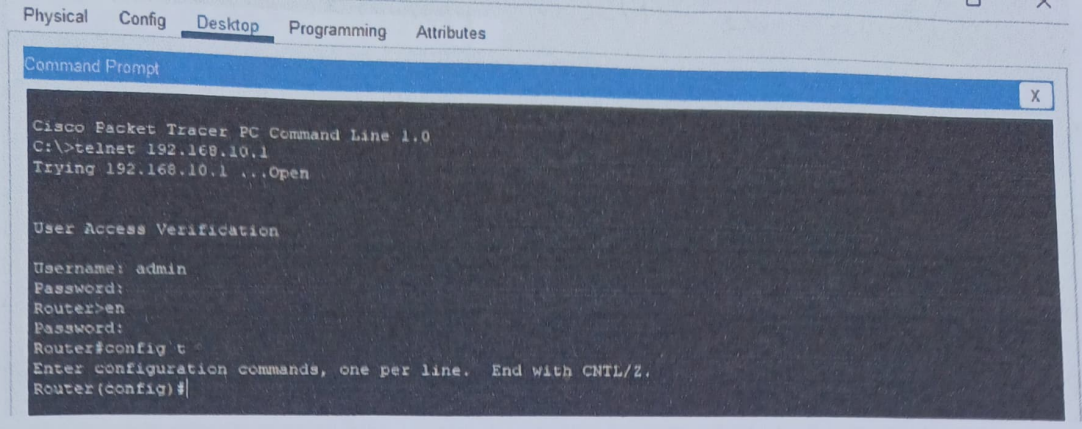


Conclusion:

In this experiment, we implemented and verified user authentication techniques for remote access to network devices using Cisco packet tracer. We successfully configured local username-password authentication, SSH-basked authentication & AAA based authentication, which provided encrypted communication.

xercises:

1. State the importance of user authentication in a secured system.
2. What will be the command for the following tasks?
   a) to create a local user account with the username "CNSLab" and the password "cisco".
   b) to set the privilege level for the local user account to 15.
   c) to create an encrypted password.
3. Explain the features of SSH protocol.
4. Compare and contrast SSH and Telnet.

olution:

1) user authentication is important in a secured system to ensure only authorised users can access network resources. It reduces risks of cyber threats, protects data integrity, enables accountability & improves reliability of the network.

Name: E. Jagadeeswar Patro

Regd. Number: 2241016309

2) a) Router(config)# username CNSLab password cisco

b) Router(config)# username CNSLab privilege 15 password cisco

c) Router(config)# service password-encryption
Router(config)# username CNSLab privilege 15 secret cisco

3) Features of SSH:

-> Encryption - Data exchanged between server & client is encrypted.

-> Authentication - SSH uses public & private key pairs which provide security.

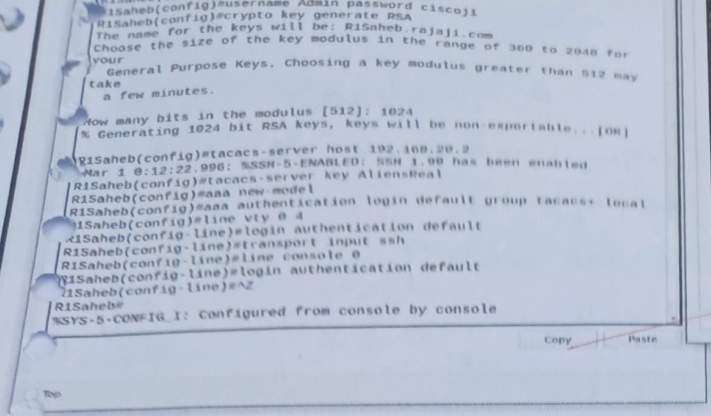
-> Data Integrity - SSH provides Data Integrity of message exchanged.

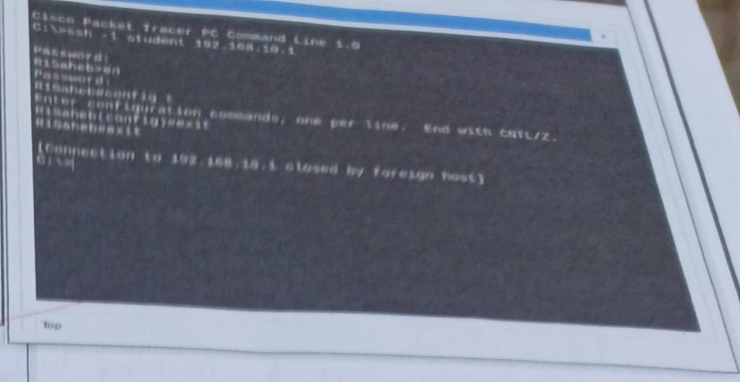
-> Tunneling - secure tunnels are created forwarding network connections over encrypted channels.

4)

SSH (Secure Shell)	Telnet (Telecommunication Network)
-> Data transmitted is encrypted	-> Transmits data in plain text
-> password / key based authentication is used	-> basic authentication without encryption
-> Default Port : 22	-> Default Port : 23
-> Commonly used for secure remote administration of network systems.	-> used for remote management but is obsolete due to lack of security
-> Supports file transfer using SCP (secure copy) or SFTP (Secure File Transfer Protocol).	-> Does not have native support for file transfer.

Jan 11/25





Conclusion:

→ AAA server based authentication secures n/w access by verifying users before allowing them to log in.

→ Using SSH with AAA enhance security by encrypting login credentials and preventing unauthorised access.

→ AAA ensures centralized access control, security & activity tracking making n/w reliable.

Exercises:

1. An AAA configuration given as following. Which login credentials are required when connecting to the console port in this configuration?

```
aaa authentication login NO_AUTH none

line console 0
login authentication NO_AUTH
```

2. State the advantages and disadvantages of AAA server based user authentication process.
3. Compare and contrast **RADIUS** (Remote Authentication Dial In User Service) and **TACACS+** (Terminal Access Controller Access-Control System) protocol.
4. State the significance of the following command in AAA server configuration:

   "AAA authentication login default group TACACS+ local"
5. How does SSH works here to protect the message?

Name: E. Jagadeeswar Patro Regd. Number: 2241016309

1) No authentication required as "no-auth". Since the console line uses 'login' authentication NO-auth the user can access the console without only username or password.

2)

Advantages

-> Centralised authentication and authorisation for multiple n/w device.

-> Enhance security with user role-based access control.

-> Provides accounting logs for tracking user activities

Disadvantages

-> Requires additional setup and configuration.

-> If AAA server fails, user may not be able to log in (unless a backup method is set).

-> Increased n/w overhead due to authentication request.

3)

RADIUS

-> Remote authentication Dial In user service protocol.

-> Encrypts only the password.

-> Combines authentication & authorisation

-> Uses UDP

TACACS+

-> Terminal access controller access control system protocol.

-> Encrypts the entire communication.

-> Separates authentication & authorisation for better control.

-> Uses TCP

4) Command 1st tries TACACS+ authentication from AAA server. If unavailable it falls back to local authentication using locally stored username & password.

5) SSH encrypts all login credentials and command communication. It prevents hackers from intercepting usernames, password or authentication request. Ensures remote access when logging into routers using AAA authentication.

Conclusion:

Successfully implemented & verified the use of ACL to permit & deny remote hosts in a network. Both standard & extended access list were successfully setup to controll access like HTTP & FTP services. Proper ACL implementation ensured secure & efficient network operations.

Exercises:

1. State the importance of Access Control List (ACL) in computer networking.
2. Differentiate the use of standard and extended ACL.
3. How does an ACL process traffic in a router? How would you apply an ACL to filter OSPF traffic?
4. What is the purpose of a "wildcard mask" in ACLs, and how does it differ from a subnet mask?

Solution:

1) ACL enhances network security by controlling the flow of traffic. They define rules that either permit or deny traffic based on specific conditions such as IP address, protocols, or port numbers. This helps protect networks from unauthorized access & manage traffic efficiently.

2)

Standard ACL	Extended ACL
-> Source IP address only.	-> Source IP, Destination IP & port numbers.
-> Simpler configuration	-> More complex configuration.
-> Basic traffic control.	-> Manual & detailed traffic control.

3) ACLs process traffic sequentially, evaluating each packet against the defined rules from top to bottom. Once a match is found, the corresponding action (permit / deny) is applied. To filter OSPF traffic, an extended ACL can be used to permit or deny traffic based on protocol type (e.g. allowing only OSPF protocol packets).

4) A wild card mask is used in ACLs to specify which bits of an IP address should be matched and which can be ignored. It helps define ranges of IP addres efficiently when permitting or denying traffic.

For example;

Subnet mask (255.255.255.0): This means the 1st 3 octets define the network & last one defines host.

wildcard mask (0.0.0.255): Used in ACLs to match any IP in the last octet while keeping the first three octets fixed.

```
                                                    ip_inverse_table)
In [13]: if __name__ == "__main__":
             plaintext = 0x0123456789ABCDEF
             key = 0x133457799BBCDFF1

             ciphertext = des_encrypt(plaintext, key)
             print(f"Ciphertext: {ciphertext:016X}")

             decrypted = des_decrypt(ciphertext, key)
             print(f"Decrypted : {decrypted:016X}")

         Ciphertext: 18A59627B69A80CD
         Decrypted : 0123456789ABCDEF

In [ ]:
```

Conclusion:

DES Algorithm was successfully implemented using understanding of theory in Jupyter Notebook with python. Experiment demonstrates secured transmission of digital information.

Excercise:

Using DES find the following for the given 8-bit plaintext 10010111 and 10-bit key 1010000010

1. Find the permuted key using the P10 table given as 3 5 2 7 4 10 1 9 8 6 and the round 1 key (K1) using the P8 table 6 3 7 4 8 5 10 9
2. Find the output of initial permutation as L0 and R0 using the given IP table 2 6 3 1 4 8 5 7
3. Find the output of expansion permutation on R0
4. Find the output of XOR (EP(R0),K1)
5. Find the output of the given S-boxes

$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array} \qquad S1 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 0 & 1 & 3 \\ 3 & 0 & 1 & 0 \\ 2 & 1 & 0 & 3 \end{bmatrix} \end{array}$$

6. Find the output of the permutation table using the P4 table 2 4 3 1

Solution:

1) P10:

1 (3)	0 (5)	0 (2)	0 (7)	0 (4)
0 (10)	1 (1)	1 (9)	0 (8)	0 (6)

after splitting & left shift : 00001 11000 (Required permuted key)

P8: 6 3 7 4 8 5 10 9

∴ R1 key: 1 0 1 0 0 1 0 0

∴ R1-Key is 10100100

Name: E Jagadeeswar Patro

Regd. No: 2241016309

2) 8-bit PT: 10010111

IP Table: 2 6 3 1 4 8 5 7 ∴ L0 = 0101 R0 = 1101

After IP: 0 1 0 1 1 1 0 1

3) R0 = 1101

EP Table: 4 1 2 3 2 3 4 1 ∴ Expanded R0: 11101011

4)
```
  1 1 1 0 1 0 1 1
⊕ 1 0 1 0 0 1 0 0
---------------
  0 1 0 0 1 1 1 1
```

5) Left half: 0100 ⇒ Row = 0 ⇒ $S_0[0][2] = 3 = (11)_2$

Column = 2

Right half: 1111 ⇒ Row = 3 ⇒ $S_1[3][3] = 3 = (11)_2$

Col = 3

∴ S-box o/p = 1111

6) P4 table: 2 4 3 1

⇒ 1 1 1 1

∴ o/p = 1111

AES is faster & efficient & is suitable for large data whereas RSA offers secure key exchange but is computationally slower.

Excercise:

1. Transform the plaintext "AES USES A MATRIX" into a state matrix form.
2. Compute the output of S-box with given input state matrix as $\begin{bmatrix} 4 & 5 \\ E & 2 \end{bmatrix}$ and S-box as

	00	01	10	11
00	1001	0100	1010	1011
01	1101	0001	1000	0101
10	0110	0010	0000	0011
11	1100	1110	1111	0111

3. Perform ShiftRow transformation on the given current matrix

$$\begin{pmatrix} 63 & EB & 9F & A0 \\ C0 & 2F & 93 & 92 \\ AB & 30 & AF & C7 \\ 20 & CB & 2B & A2 \end{pmatrix}$$

4. Find the output of Mix Column if the input state matrix is $\begin{bmatrix} D & 1 \\ A & F \end{bmatrix}$ with the predefined matrix as $\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix}$ an d the irreducible polynomial for GF(16) is x^4+x+1.
5. Given the following values for the RSA algorithm:
   - Two prime numbers: p=61, q=53
   - Public key: e=17

   Calculate the private key d, where d is the modular inverse of e modulo φ(n).

Solution:

1) AES USES A MATRIX

⇒ 41 45 53 20 20 41 20

55 53 45 53 20 40 41 59 53 49 58

↳ I/P state Array:

41	55	20	41
45	53	41	54
53	45	20	52
20	43	40	49

2) o/p of s-box: $\begin{bmatrix} 1101 & 0001 \\ 1111 & 1010 \end{bmatrix} = \begin{bmatrix} 13 & 1 \\ 15 & 10 \end{bmatrix}$

3) Shift Row o/p:

$$\begin{bmatrix} 63 & EB & 9F & A0 \\ 2F & 93 & 92 & C0 \\ AE & C7 & AB & 30 \\ A2 & 20 & CB & 2B \end{bmatrix}$$

4)

=> $(1 \times D) \oplus (4 \times A)$

=> $D \oplus E$

=> 3

$(1 \times 1) \oplus (F \times 4)$

=> $1 \oplus 9$

-> 8

$(4 \times D) \oplus (1 \times A)$

=> $1 \oplus A$

-> B

$(4 \times 1) \oplus (1 \times F)$

=> $4 \oplus F$

=> B

o/p: $\begin{bmatrix} 3 & 8 \\ B & B \end{bmatrix}$

$4 \times A = 0100 \times 1010$

$= x^2 + (x^3 + x)$

$= (x^5 + x^3) \bmod (x^4 + x + 1)$

$= x^3 + x^2 + x = E$

$F \times 9 = 1111 \times 0106$

$= (x^3 + x^2 + x + 1) \times x^2$

$= x^3 + 1 = 9$

$4 \times D = (0100) \times (1101)$

$= x^2 * (x^3 + x^2 + 1)$

$= (x^5 + x^4 + x^2) \bmod (x^4 + x + 1)$

$= 1$

5) $n = p \times q = 3233$

$\phi(n) = (p-1)(q-1) = 3120$

$d \cdot e = 1 \bmod 3120$

$d \cdot 17 = 1 \bmod 3120$

$d = \frac{k \cdot \phi(n) + 1}{e}$

$= 2753$