SIKSHA 'O' ANUSANDHAN
DEEMED TO BE UNIVERSITY

Admission Batch: 2022 Session: 2024-25

Laboratory Record

Computer Networking Security (CSE 3752)

Submitted by

Name: Sibasis Mahapatra

Registration No.: 2241013019

Branch: CSE

Semester: 6th Section: 2241001

Department of Computer Science & Engineering

Faculty of Engineering & Technology (ITER)

Jagamohan Nagar, Jagamara, Bhubaneswar, Odisha - 751030

Expt.-1:

Aim: Implementation of users authentication techniques for remote access of the network device in computer Networking using cpt.

OBJECTIVES:

1. An overview on users authentication technique used in secured system.

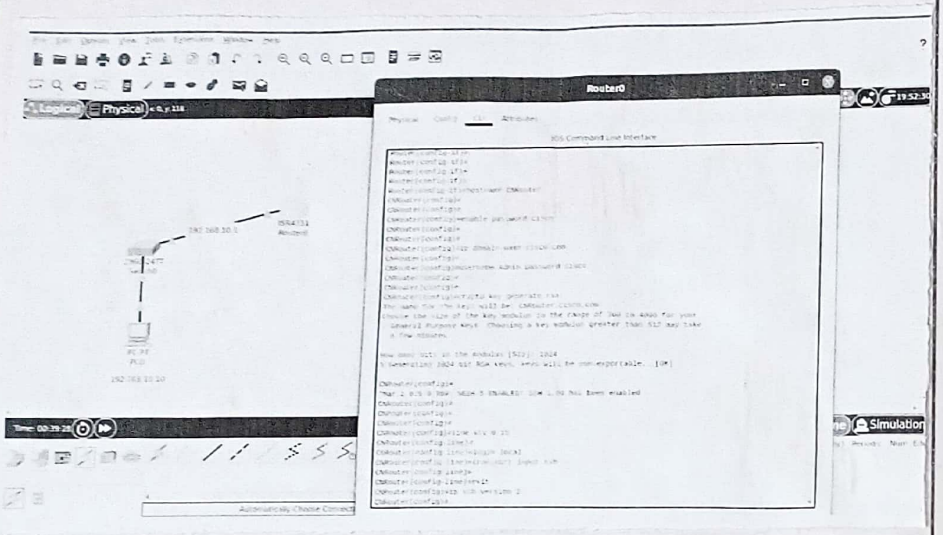
Users authentication in secured systems verifies the identity of users accessing the system. Common techniques include:

1. Password-Based Authentication: users enters a unique password, often combined with a username. It's simple but vulnerable to brute force or phishing attacks unless strengthened with complexity rules.

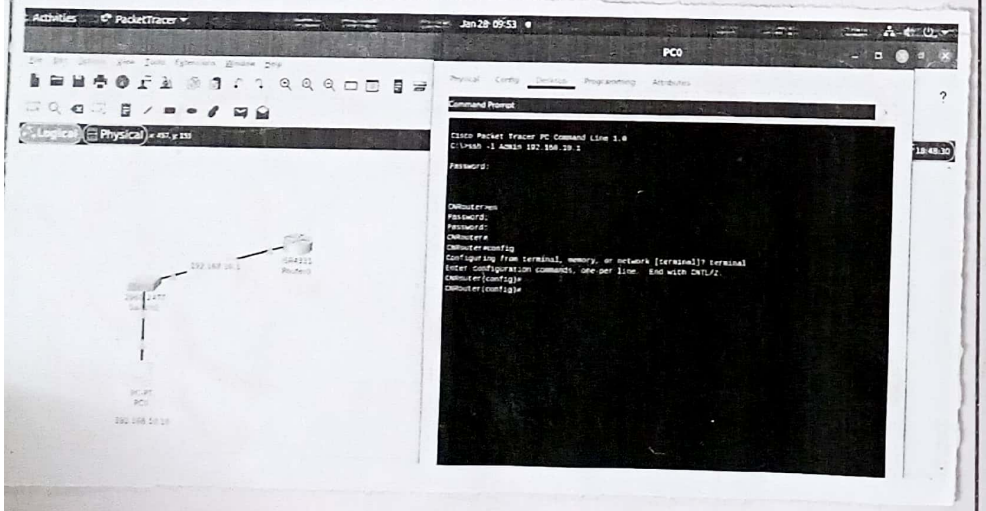
2. Multi Factor Authentication: Combines 2 or more factors like something you know (password), something you have (smartphone), or something you are (biometric) - enhancing security significantly.

3. Biometric Authentication: Uses unique physical traits (Fingerprint, facial recognition) for high accuracy, though it requires specialized hardware and raises privacy concerns.

2. configure and verification of remote users authentication on a cisco packet routers and switch using local username password authentication.



3. configure and verification of remote user authentication on a cisco router and switch using local username and password authentication using SSH.



Name:———————— Regd. Number:————————

Conclusion:

Secure user authentication for remote access in CPT ensures only authorization users can manage network devices. Implementing SSH, AAA and encryption enhances security, preventing unauthorized access and strengthening network protection.

Exercise:

1. State the importance of user authentication in a secured system.

a) prevents unauthorized Access

b) enhances user Accountability.

c) enhances user Data security.

d) Improves System Integrity.

2. What will be the command for the following tasks?

a) to create a local user account with the username "CNSLAB and password cisco".

→ Router(config)# username CNSLAB password cisco.

b) to set the privilege level for the local user account to 15.

→ Router(config)# username CNSLAB privilege 15 password cisco.

c) to create an encrypted password

→ Router(config)# enable secret cisco.

3. Explain the feature of SSH protocol.

→ SSH Authentication
→ Encryption
→ Data integrity
→ Port Forwarding (Tunneling)

Name:———————— Regd. Number:————————

4. Compare and contrast SSH and Telnet.

SSH	Telnet
• Highly secure.	• Insecure
• uses encryption to protect data.	• Transmits data in plain text.
• uses TCP port 22.	• uses TCP port 23
• used for secure remote access	• used for simple remote access.

Department of Computer Science & Engineering
Faculty of Engineering & Technology (ITER)

Expt-2:

Aim Of the expt.: Implementation of AAA server as user authentication and authorization technique for remote access to the network device in computer network using cisco packet tracer.

OBJECTIVES:

1. An overview of AAA used in secured system.

AAA stands for authentication, authorization and accounting, a framework used in secured systems to manage access and monitor usage.

1. Authentication verifies the identities of a user or device (e.g. using a password or token) to ensure only legitimate entities gain access.

2. Authorization determines what an authenticated user can do (e.g: read files or modify setting) based on predefined permission.

3. Accounting: tracks the user's actions (e.g. login time, resource accessed.) for auditing or troubleshooting.

Together, AAA enhances security by controlling access, enforcing policies and maintaining accountability in systems like networks, enterprises or cloud services.

2. configuration and verification to remote user authentication on a cisco router using AAA server based user-name password authentication.

3. Configuration and verification of remote user authentication on a cisco routing using AAA server based on username password authentication with SSH

Department of Computer Science & Engineering
Faculty of Engineering & Technology (ITER)

Conclusion:

In this expt., we successfully implemented and verified the AAA (authentication, Authorization and Accounting) mechanism for securing remote access to a network device using cisco packet tracer.

Exercise:

1. Login credentials for Console port, in the given AAA configuration.

aaa authentication login NO_AUTH none
line console 0
login authentication NO_AUTH

No authentication is required for console login because the none option allows access without credentials.

2. i) Advantages of AAA Authentication:

→ centralized control and enhanced security.
→ supports encryption and user accountability.
→ scalable for large networks.

ii) Disadvantages:

→ Requires setup and maintenance
→ AAA server failure can block access.
→ slight latency due to authentication process.

3.

TACACS+	RADIUS
1. cisco proprietary protocol	1. open standard protocol.
2. Uses TCP as a transmission protocol.	2. Uses UDP as a transmission protocol.

TACACS+	RADIUS
3. uses TCP port no. 49	3. uses UDP port no. 1812 for authentication and authorization
4. offers multiprotocol support.	4. No multicontrol protocol support.

4. Significance of AAA authentication login default group TACACS+ local.

→ This command configures login authentication method. If the TACACS+ server is unreachable, it falls back to local authentication, ensuring back up access.

5. SSH encrypts login credentials and session data, preventing eavesdropping and man-in-the-middle attacks. It ensures secure communication bet^n the client and router, unlike Telnet which transmits data in plain text.

———— o ————

Expt-3

Aim: Creating a user access list for permit and deny to a remote server.

OBJECTIVES:

1. An overview on standard and extended access list.

Access Control Lists (ACLs) in networking filter traffics based on specified rules. They are categorized into Standard ACLs and Extended ACLs.

1. Standard ACL:

→ Filters traffic based only on source IP address.

→ uses access list number 1-99 (IPV4) and 1300-1999 (expanded range).

e.g: accesslist 10 permit 192.168.1.0 0.0.0.255 interface GigabitEthernet0/0 ip access-group 10 in

2. Extended ACL:

→ Filters traffic based on source/destination IP, protocol and port numbers.

→ uses access list numbers 100-199 (IPV4) and 2000-2699 (expand range).

2. configuration and verification of a standard access-list for permit and deny to a remote server.

Department of Computer Science & Engineering
Faculty of Engineering & Technology (ITER)

3. Configuration and verification of an extended access list for permit and deny to a remote server (HTTP/FTP).

conclusion:
This expt. demonstrated how standard and Extended ACLs control remote access. Standard ACLs filter by source IP, while Extended ACLs provide detailed control using IP protocol and port (HTTP/FTP), enhancing network security.

Exercise:
1. Importance of ACL in computer Networking:
→ ACLs control network traffic by permitting or denying spelfic packets

- They enhance security by restricting unauthorized access.
- Help optimize network performance by filtering unnecessary traffic.

2. i) Standard ACL: Filters traffic based only on the source IP address.

ii) Extended ACL: Filters traffic based on source/destn IP, protocols and ports.

3. i) ACLs check incoming packets against rules sequentially. If a match is found, the action (permit/deny) is applied. Otw packets are implicitly denied.

ii) to filter OSPF traffic, use an extended ACL to block protocol 89 (OSPF) and apply it to an interface:

```
access-list 110 deny ospf any any
interface GigabitEthernet0/0
ip access-group 110 in
```

4. Purpose of Wildcard mask & difference from Subnet Mask:

→ Wildcard Mask: Defines which bits to check (0) and which to ignore (1) in an IP address for ACL matching.

→ Difference: Unlike a subnet mask (which identifies network and host portions), a wildcard mask is used in ACLs to specify flexible IP ranges. Eg: Subnet mask: 255.255.255.0 (Defines n/w).
Wildcard mask: 0.0.0.255 (matches any host in the subnet).