Sweta Gupta
Roll No: 61
SUBJECT:- ADVANCE SECURITY LAB

PRACTICAL NO – 1

Aim: Study of various Authentication and access control services such as Radius, Tacacs and Tacacs+

Theory:

NEED OF THE PROTOCOLS:

If a single administrator wants to access 100 routers and local database of the device is used for username and password (authentication) then the administrator have to make the same user account different times. Also, if he wants to keep different username and password for the devices then he have to manually change the authentication for the devices. Ofcourse, it's a hectic task.

To ease this task to some extent, ACS (Access Control Server) is used. ACS provides a centralised management system in which the database of username and password are kept. Also, authorization (means what the user is authorised to do) can be configured. But for this we have to tell the router to refer to ACS for its decision on authentication and authorization.

Two protocols are used between the ACS server and the client to serve this purpose:'

1. TACACS+
2. RADIUS

RADIUS –
RADIUS, stands for Remote Authentication Dial In User Service, is a security protocol used in AAA framework to provide centralised authentication for users who want to gain access to the network.

Features – Some of the features of RADIUS are:

1. Open standard protocol for AAA framework i.e it can used between any vendor device and Cisco ACS server.
2. It uses UDP as transmission protocol.
3. It uses UDP port number 1812 for authentication and authorisation and 1813 for accounting.
4. If the device and ACS server is using RADIUS then only the passwords of AAA packets are encrypted.
5. No explicit command authorization can be implemented.
6. In RADIUS, authentication and authorization are coupled together.

Working –

When other device want to access Network Access Server (NAS-client of RADIUS), it will send access-request message to ACS server for the matching the credentials. In response to the access-request of the client, the ACS server will provide an accessaccept message to the client if the credentials are valid and access-reject if the credentials do not match.

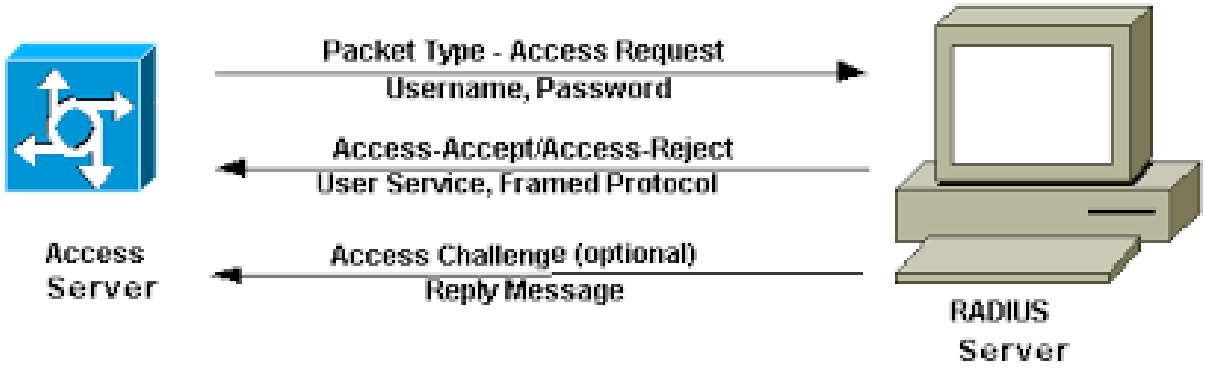

Fig Mo:1 RADIUS

Advantage –

1. As it is open standard, therefore it can be used between the other devices also.

Disadvantage –

1 As RADIUS uses UDP .
2 No explicit command authorization can be implemented.
3 RADIUS encrypt only the passwords. It doesn't protect other data such as username.

Tacas:

TACACS (Terminal Access Controller Access Control System) is an older authentication protocol common to UNIX networks that allows a remote access server to forward a user's login password to an authentication server to determine whether access can be allowed to a given system. TACACS is an encryption protocol and therefore less secure than the later TACACS+ and Remote Authentication Dial-In User Service protocols.

Tacacs+:

Remote Access Dial In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+) are two common security protocols used to provide centralized access into networks. RADIUS was designed to authenticate and log remote network users, while TACACS+ is most commonly used for administrator access to network devices like routers and switches. Both protocols provide centralized Authentication, Authorization, and Accounting (AAA) management for computers that connect and use a network service.

Authentication - Who is allowed to gain access to the network? Traditionally authorized users provide a username and password to verify their identity for both RADIUS and TACACS+

Authorization - What services can a user access once they are authenticated? It is unlikely that you want your finance people to have access to the developer database. Visitors may have access only to the Internet, while only IT staff can access the entire passwords database.

- Accounting - What services did each user access and for how long? Accounting records record the user's identification, network address, point of attachment and a unique session identifier—these statistics are tracked and added to the user's record. This is useful when time on the system is billed to individuals or departments.

Features – Some of the features of TACACS+ are:

1. Cisco proprietary protocol for AAA framework i.e it can used between the Cisco device and Cisco ACS server.
2. It uses TCP as transmission protocol.
3. It uses TCP port number 49.
4. If the device and ACS server is using TACACS+ then all the AAA packets exchanged between them are encrypted.
5. It separates AAA into distinct elements i.e authentication, authorisation and accounting are separated.
6. It provides greater granular control (than RADIUS) as the commands that are authorised to be used by the user can be specified.
7. It provides accounting support but less extensive than RADIUS.

Working –

The client of the TACACS+ is called Network Access Device (Nad) or Network Access Server (NAS).Network Access Device will contact the TACACS+ server to obtain a username prompt through **CONTINUE** message . The user then enters a username and the Network Access Device again contact the TACACS+ server to obtain a password prompt (Continue message) displaying the password prompt to the user, the user enters a password, and the password is then sent to the TACACS+ server.

The server can respond with one of the following reply messages:

- If the credentials entered are valid then the TACACS+ server will response with an ACCEPT message.
- If the credentials entered are not valid then the TACACS+ server will response with an REJECT message.
- If the link between the TACACS+ server and NAS or TACACS+ server is not working properly then it will respond with an ERROR message.
- If TACACS+ authorization is required, the TACACS+ server is again contacted and it returns an ACCEPT or REJECT authorization response. If the ACCEPT message is returned, it contains attributes which are used to determine services that a user is allowed to do.

For accounting, the client will send a REQUEST message to the TACACS+ server for which the Server responds with RESPONSE message stating that record is received.

Advantage –

1. Provides greater granular control than RADIUS.TACACS+ allows a network administrator to define what commands a user may run.
2. All the AAA packets are encrypted rather just passwords (in case of Radius).
3. TACACS+ uses TCP instead of UDP. TCP guarantees communication between the client and server.

Disadvantage –

1. As it is Cisco proprietary, therefore it can be used between the Cisco devices only.
2. Less extensive support for accounting than RADIUS.