Segurança de Sistemas e Informação

(SEGSI)
PL02

*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**)*
{@isep.ipp.pt}

Exercise 1: RADIUS

RADIUS is one of the most known protocol to provide AAA services. It is often seen in Wireless Infrastrucutre were 802.1X enabled networks allow users to connect to their corporate credentials to the network providing easy account management of the Wireless infrastructure itself.

1. Install FreeRadius on your virtual machine;
2. Create users on your machine: Bob, Alice, John, Madeleine, and Jake;
3. Bob and Alice are standard users, Madeleine is an accountant, and Jake is the the ”IT Guy” (Administrator). Create the necessary groups;
4. Configure FreeRadius such that it accepts authentications from Users and the Administrator only;
5. Test the connection with **radtest** (don’t forget to set a secret for the connection)
6. What is hostapd-WPE and what does it abuse regarding the authentication protocol? Describe a evil twin attack and how does it affect this protocol?
7. Make a TCPDUMP of the connection, can you break that password?

Exercise 2: TACACS+

TACACS is a similar protocol but often used to authenticate administrator to routers and switches. It’s based on a secret key to authenticate and is consider no longer secure. From time to time we see this deployed in old corporate networks.

1. Install TACACS+ package in a Linux Virtual Machine;
2. Configure the package with a secret key and serve it;
3. Create the same schema of users as in Exercise 1;
4. Capture the traffic and try to extract and crack your own key (suggestion: use the **hcxcaptool**)
5. What are your security considerations for this protocol?

Exercise 3: Diameter

Diameter is a protocol that brings new security features to the AAA scheme. It shares some similarities with RADIUS but offers several improvements. For instance, Radius Authentication is client-server oriented, however, Diameter can invert this logic if it needs to.

- Install the FreeDiameter package on your server;
- Configure it to server authentication to clients using a secure connection;
- Diameter is often tied with new generation networks such as 5G. What extra capabilities do you see fit in alignment with the concept of ”Secure Networks”?