Segurança de Sistemas e Informação
(SEGSI)
PL01
*Jorge Pinto Leite (**JPL**)*
*Pedro Sousa Rodrigues (**DCR**)*
{@isep.ipp.pt}

Exercise 1: Point-to-Point Protocol (PPP)

PPP is a legacy protocol that can still be found in several implementations. It was used to authenticate before a system. It can use Challange Authentication or Password Authentication. Take the PPPoE Packet Capture from Moodle and answer the following questions:

1. What kind of authentication is used in the PPP protocol?
2. What are the steps for authenticating the user?
3. Identify the ”secret” password.
4. Imagine you are a telecom provider and you provide this authentication method to your clients, what are your security considerations?

Exercise 2: Challenge Authentication

The Challenge authentication protocol, albeit having several implementations, proposes a set of steps to avoid sharing the password in clear text. However, it is not secure in its default form. Take the Radius Simple Protocol file example from Moodle and answer the following questions:

1. Describe the Radius protocol that you see (What it does, what purpose it serves and its security considerations).
2. Describe the Challange Authentication Principle?
3. Crack the credential using any password cracker such as JohnTheRipper or Hashcat.
4. While it is cracking comment on the resilience of the cipher.

Exercise 3: LightWeigt Directory Access Protocol (LDAP)

LDAP is a simplistic protocol that is still widely used in corporate Networks. Its simplicity and integration with additional values provide enterprises with scalability and malleability to achieve company goals.
It is often forgotten to secure it. Take the LDAP capture file and answer the following questions.

1. What is LDAP Simple Bind? And Anonymous Bind?

2. Name several types of authentication within LDAP.

3. What is LDAP Sign and Seal?

4. What is the advantage of using LDAP with Kerberos authentication?

Exercise 4: NTLM LDAP

As you noticed LDAP can support additional authentication methods. The following is a challenge for you to test your understanding of the protocol.
Load NTLM_LDAP and answer the following questions:

- What is the user logging in?
- Explain the different interactions of the protocol.
- Extract all pertinent data and crack the password.