Co-funded by the Erasmus+ Programme of the European Union

ISSES

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

Packet and communication session analysis

- Laboratory exercise -

Assignment: Using the *Wireshark* tool open the appropriate *.pcapng* file and analyze the package.

1. In the *SNMP.pcapng* file, find the version of the protocol that is used and the value of the *community* parameter.

2. In the *Telnet.pcapng* file find the username and password that are used.

3. In the *HTTP.pcapng* file, find the username and password that are used to access the system and the contents of the displayed page. Which port is this *HTTP* communication on?

4. In the *TLS.pcapng* file, find out which encryption algorithms are used in all *TLS* sessions.

5. In the *SSH.pcapng* file, find out with which device the *SSH* session was established and which cryptographic algorithms are used to protect that session. How long was the session?

6. In the *POP3.pcapng* file, find the *IP* addresses of the client and the e-mail server to which the client is communicating via *POP3* and *IMAP* protocols. Determine which cryptographic algorithms are used to protect these protocols.

7. In the *Malware.pcapng* file, the communication of one bot with its command and control center was recorded, as well as the beginning of the DoS attack.

- Describe how the bot communicates with the command and control center located at *IP* address 45.80.37.176. Which protocol is used for communication? What is the frequency of messages? What is the content of the messages? What is the bot's address?
- Determine the moment when the attack begins and describe the attack. Determine the intensity of the attack. What is the victim's IP address? On which port is the attack carried out?
- Determine the message by which the command and control center issues the attack command. Which package is that (number in order) and what is the content of the command?

NOTICE FOR STUDENTS

Topics of this laboratory exercise may involve the study of various mechanisms that violate information security and make intrusions into computer systems and networks.

The application of these mechanisms when executed towards the systems of individuals and legal entities, which are not familiar with them and are not consentient with the activities on checking vulnerability and testing intrusions into their systems, is punishable under the Criminal Law of the Republic of Serbia (Articles 298 to 304a).

Students performing this laboratory exercise may use these methods for study purposes only within the closed laboratory environment provided for teaching the Advanced Network and System Security course and described in Network Security Laboratory (NS Lab) Design and Hybrid NS and Crypto Lab Implementation documents available at: https://isses.etf.bg.ac.rs/labs/

Students may not imply that they are in any way encouraged or that they are recommended to use these methods toward systems of any third party entity or individual.

Any eventual activity that a student would undertake using these methods and mechanisms according to systems that are not within the laboratory on the course is the sole responsibility of the student.