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

Computer system and network reconnaissance

- Laboratory exercise -

1. Configure interfaces on virtual machines (during the first command containing sudo enter root password - **std2020**):

- VM1:
  - `sudo ip link set eth1 up`
  - `sudo ip link set eth2 up`
  - `sudo ip link set eth3 up`
  - `sudo ip addr add 10.12. x .1/24 dev eth1`
  - `sudo ip addr add 10.13. x .1/24 dev eth2`
  - `sudo ip addr add x.x.1.2/24 dev eth3`
- VM2:
  - `sudo ip link set eth1 up`
  - `sudo ip addr add 10.12.x.2/24 dev eth1`
- VM3:
  - `sudo ip link set eth1 up`
  - `sudo ip addr add 10.13.x.3/24 dev eth1`

2. Check that the network is working properly. After installing all interfaces on VM1 run the following `ping` commands (you should get a response):

- `ping 10.12.x.2`
- `ping 10.13.x.3`
- `ping x.x.1.1`

3. Install scanning tools on VM1:

- `sudo apt install nmap`
- `sudo apt install hping3`
- `sudo apt install p0f`

  (during installations, click Y when needed)

4. Install FTP server on VM3:

- `sudo apt install vsftpd`

5. From the VM1 virtual machine, scan the following networks and detect active devices on them (The nmap command needs to be run with root privileges, ie with the `sudo` prefix):

- `10.12.x.0/24`
- `10.13.x.0/24`
- `x.x.1.0/24`

6. For devices in these networks that are detected as active:
   - Use `nmap` to detect open TCP and UDP ports (apply different types of TCP scanning).
   - Use `nmap` to detect the operating system.

7. From the VM1 virtual machine:
   - Use `hping3` to test the ACK scan to ports 21, 22, 80, and 443 for devices that are detected as active
   - Try passive operating system detection. Open two terminals. In one terminal run the command: `sudo p0f -i eth1`, and in the other terminal connect to VM2 via ssh with the command: `ssh student@10.12.x.2` (answer yes and enter password). Observe what happens in the first terminal.

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.