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

Network attacks (ARP spoofing)

- Laboratory exercise -

For the ARP spoofing exercise, only the connections between the three virtual machines via the *eth0* interface on which the virtual machines are in the same network segment (network x.x.x.0/24) will be used.

The roles of virtual machines will be:

- VM1 - an attacked device that will receive fake *ARP* responses when it wants to communicate with VM3
- VM2 - an attacker who will use an *arpspoofing* attack to force VM1 to pass its communication with VM3 through VM2
- VM3 - web server to which VM1 connects

Use the *Putty* to connect via SSH protocol to three virtual machines: one connection to VM1, three connections to VM2 and one connection to VM3. On all devices, use the *ifconfig* command to find and record the *MAC* addresses on the *eth0* interfaces of all three virtual machines.

PHASE 1 - No *ARP spoofing* attack.

1. Using *WinSCP* connect to VM3 (same address and credentials as for *SSH* connection) and place the *SimpleAuthServer.py* file in a folder on the home/student/Documents/web/ path.

2. On VM3, boot a simple web server with the following commands:

- `cd Documents/web`
- `sudo python SimpleAuthServer.py 80 username:password` (username and password are the username and password used on the web server and can be changed as desired).

3. On VM2 in window 1 install the required tool with the command

- `sudo apt install wireshark`

and then start saving the package with the command:

- `sudo dumpcap –i eth0 –w /tmp/cap2.pcapng`

4. Connect to VM1 using *VNC*. After connecting, start the *Firefox* web browser and go to the address x.x.x.3. Enter credentials in the window.

5. After successful communication with the web server, stop recording packets on VM2 in window 1 (*CTRL + C*) and transfer the file with recorded packets to VM2 and give privileges to read the file with the following commands:

- `sudo mv /tmp/cap2.pcapng /home/student/Documents/`
- `sudo chmod +rw cap2.pcapng`

6. Use *WinSCP* to connect to VM2 (same address and credentials as for *SSH* connection) and download the file *cap2.pcapng*.

7. In the *Wireshark* tool, analyze the downloaded file. Does communication between VM1 and VM3 appears in it? Why?

8. Shut down the *WinSCP* session so that in later stages of operation this communication would not unnecessarily increase the amount of packets recorded.

PHASE 2 - *ARP spoofing*.

1. On VM2 in window 1 check if VM2 is routing the packet with the command:

- `sysctl net.ipv4.ip_forward`

If the answer is 0, then start routing with the command:

- `sudo sysctl -w net.ipv4.ip_forward=1`

2. On VM2 in window 2 install the required tool with the command:

- `sudo apt install dsniff`

and then start *ARP* spoofing with the following command:

- `sudo arpspoof -i eth0 -t x.x.x.1 x.x.x.3`
  (the command is run on the interface *eth0*, the target of the attack is VM1, and a fake address for VM3 is provided)

3. On VM2 in window 3 start *ARP* spoofing in the other direction with the following command:

- `sudo arpspoof -i eth0 -t x.x.x.3 x.x.x.1`

4. On VM2 in window 1 start packet recording with the command:

- `sudo dumpcap -i eth0 -w /tmp/cap2.pcapng`

5. On VM1 clear the *ARP* input for VM3 with the following command:

- `sudo arp -d x.x.x.3`

6. On VM1 start packet recording with the command:

- `sudo dumpcap -i eth0 -w /tmp/cap1.pcapng`

7. Connect to VM1 using *VNC*. After connecting, start the *Firefox* web browser and go to the address x.x.x.3. Enter credentials in the window.

8. After successful communication with the web server, stop recording packets on VM1 and VM2 in window 1 (*CTRL + C*) and transfer the file with recorded packets to VM1 and VM2 and

give privileges to read the file with the following commands (first two commands in window 1 of the machine VM2, other two commands on machine VM1):

- `sudo mv /tmp/cap2.pcapng /home/student/Documents/`
- `sudo chmod +rw cap2.pcapng`
- `sudo mv /tmp/cap1.pcapng /home/student/Documents/`
- `sudo chmod +rw cap1.pcapng`

9. Use *WinSCP* to connect to VM1 and VM2 (same address and credentials as for *SSH* connection) and download the files *cap1.pcapng* and *cap2.pcapng*.

10. In the *Wireshark* tool, analyze the downloaded files.

- Does communication between VM1 and VM3 appears in the *cap2.pcapng* file?
- What are the *MAC* addresses in the packets intended for VM3? Why are there two identical packages between VM1 and VM3? What are the *MAC* addresses on them?
- Can you see *ARP* packets on VM2 by which VM1 is being cheated with fake MAC address?
- Can you see the credentials that were used to log on to the web server in the packets that go through VM2? (If necessary, use a tool to convert base64 to text, e.g. web tool *base64decode.com*)
- Are these the same packets as those recorded on VM1?

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.