

TCP/IP Attack Writeup

Ethical Hacking 2021/22, University of Padua

Alessandro Brighente, Denis Donadel, Eleonora Losiouk, Gabriele Orazi

You can find attached the code for each task.

1 Task 1: SYN Flooding Attack

Task 1.1: Python is a good language to fastly write scripts. Anyway, its performances are poor and so many instances of the attack are needed to get a small success rate. Another options (not so realistic) is to keep a small queue length value on the victim machine.

Task 1.2: The C code is more effective thanks to the high performances of the C code. One instance of the attack is able to slow down the setup of a telnet connection.

Task 1.3: With the countermeasure turned on, the startup time of a `telnet` connection is still slow but acceptable.

2 Task 2: TCP RST Attacks on telnet Connections

You have to use as “seq” parameter of the TCP packet the “Sequence Number (raw)” in Wireshark (not the relative one). All the other params (i.e., addresses and ports) must match the last TCP packet analyzed.

3 Task 3: TCP Session Hijacking

Manually this task is not so different from Task 2. If you want to automate it, this might be a little bit more difficult since you have to correctly find all the parameters and detect the right moment to inject your packet. Notice that this attack may feeze the victim terminal.

4 (Optional) Task 4: Creating Reverse Shell using TCP Session Hijacking

You can checkout the proposed code for this task, which is mainly a copy of Task 3 code with a different payload.