Networks and Systems Security II - Winter 2022

Sambuddho Chakravarty

February 23, 2022

Exercise 3 (total points: 55)

Due date: March 6. Time: 23:59 Hrs.

Buffer overflow on target program using `msfvenom` (total points: 55)

You are being given a program – `simple_echo_server`. It runs as a server on port 22000. It is a simple echo server which echoes back whatever string you pass to it. You task is to create a shell code that you could pass to the program. The shell code should be a reverse TCP shell that may connect back to the attacker machine on any chosen port. You may use tools like `msfvenom` to generate the shell code payload. It must be noted that the program does have an executable stack. Thus, your shell code should be executable from the stack itself.

On your own machine, you may listen on any TCP port using the generic TCP Client/Server program – `netcat`. **[Go through the man page of `netcat` to understand exactly how that works.]**

What you need to submit:

1. Screenshots showing the commands you used to generate the shellcode, along with their descriptions and expected outcomes (15 points).
2. Shellcode binary (15 points).
3. Script/program (in any language) that you may use to deliver the shellcode to the server. One way is to establish a connection to TCP port 22000 on the server and send the payload bearing the shell code (10 points).
4. Screenshot showing the attacker receiving connection from the victim and thereafter the attacker executing shell commands on the victim, via the reverse TCP shell (10 points).
5. Write-up elaborating what you did inject the payload to the victim program (5 points).