

AEH LAB 1: Enumeration (10% of total marks)

This is a group work. All members of the same group should submit the same document in D2L. Submission is a must. If you don't submit and your group mates submit, then they will get marks and you won't.

- 1) Demonstrate Netcat TCP connection as mentioned in Lecture 1. You can use same computer or a different computer within the same network. Use port 9999. Test by sending two messages a) "This is a test from TCP Server" 2) "This is a test from TCP Client". Take screenshots of the whole process. **(1 mark)**
- 2) Demonstrate Netcat UCP connection as mentioned in Lecture 1. You can use same computer or a different computer within the same network. Use port 6666. Test by sending two messages a) "This is a test from UDP Server" 2) "This is a test from UDP Client". Take screenshots of the whole process. **(1 mark)**
- 3) Demonstrate Netcat Data transfer as mentioned in Lecture 1. Run the listener on port 5555. a) Use echo to send this message "This is a message via Echo" b) Save message to a file called "your_group_name_received.txt" (change your_group_name with your actual group name). Take screenshots of the whole process. **(1 mark)**
- 4) Chose a company from an active bounty hunt program. Demonstrate Dirbuster on that company. Please use all the options showed in the lecture. **(1 mark)**
- 5) Perform passive enumeration on the company you chose earlier. Use crt.ch, Virus Total, DNSdumpster to get information about the company. Take screenshots of the whole process. **(2 marks)**
- 6) Perform Active enumeration on the company you chose earlier. Use all the tools that were demonstrate so far to get information about the company. Take screenshots of the whole process. **(2 marks)**
- 7) Compare between the two set of results. What did you miss in passive enumeration versus in active? Or vice-versa. Comment on the missing data, why do you think the tool(s) missed it? **(2 marks)**

Submission file must be PDF. Submission deadline in Blackboard: **October 10th 2024 11 PM EST.**