Assignment 2

Date Assigned: Nov 16, 2021

Submission Date: Nov 24, 2021

Objective:

The objective of this assignment is to get hands-on expertise on Operating system exploitation and network penetration testing

Task1:

You are required to exploit a machine "Blue" available in "tryhackme". You need to search the vulnerability and find the suitable existing exploit. Once done you need to show Meterpreter session in your report with proper screenshots.

To complete this task, you first need to sign up tryhackme at https://tryhackme.com/.

Then you need deploy the blue machine available in the following link.

https://tryhackme.com/room/blue

The machine **should be** attacked by using your own attacking machine using VPN that can be given by the "tryhackme".

Task2:

You are required to perform MITM on your network. You need to sniff the network traffic using ARP poisoning and you need to capture the username and password of your slate and flex.

To perform this task, you need to login your slate and flex using wrong password or hide the password in case of correct one. Before login, you need to enable sniffing and ARP poisoning using Bettercap.

You are also required to show the credentials available in captured data in **wireshark and network miner.** This requirement is applicable on both slate and flex

Instructions:

1. You need to submit the report of the tasks. The report should be in your own words and plagiarism free. You are also required to add screenshots in your report and those screenshots should be properly referred.
2. Total Marks=40

   Task 1 = 20 Marks

   ➢ Tryhackme setups including VPN and attacking with your own kali/parrot machine=10 Marks
   ➢ Completing all the flags with meterpreter session= 10 Marks

   Task 2 = 20 Marks

   ➢ Tool setup, capturing and sniffing traffic = 10 Marks
   ➢ Showing credentials of both slate and flex in wireshark and network miner = 10 Marks
3. Submit your assignment in PDF format.
4. Submit your assignment before deadline. **Late assignments will not be accepted.**
5. All other discussed policies will be applied.