

Computer Forensics & Security Fundamentals

Week 5 Lab – User Enumeration and Password Cracking

Overview

In pairs start up the virtual machine from the previous lab session and undertake each of the following tasks, you have 1 hour after which there will be a class Q & A session on the tasks (I'll be providing the Q, you'll be providing the A 😊). Document the approach you made to tackling each of the tasks.

Tips:

Use Google to search for resources to help you carry out each task. Make a note of which websites, forums etc. that you used. Read around the forums and see what other useful information they provide.

Make notes on the solutions provided in Q & A session.

Task 1 - User Enumeration

Generate a list of users of the VM.

Task 2 - Password ageing policy

Identify the password ageing policy for the msfadmin user.

Task 3 - Password cracking

The virtual machine system image has John the Ripper installed in `/opt/john/` use this application to crack the passwords on the system.

Use the following commands to crack the passwords;

1. `sudo su`
 - a. This switches into super user mode, ideally you should not run at this privilege level ordinarily.
2. `cd /opt/john/run`
 - a. This changes into the directory containing the tool
3. `./unshadow /etc/passwd /etc/shadow -> passfile.txt`
 - a. This combines the list of user names and hashes
4. `cat passfile.txt`
 - a. This displays the list of combined usernames and hashes
5. `./john --show passfile.txt`
 - a. This cracks the passwords

This task may take some time for the computer to complete, be patient.

Task 4 – Coursework

Working individually, apply the knowledge and processes you have developed during this lab session to the part 1 of the coursework. **You are expected to have attempted part 1, tasks 1 & 2 before attending next week's formative feedback session.**