06-System Hacking

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online that have the services running and vulnerable

Advanced: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.
Advanced: capture encrypted packets, using decryption process from capture discussion

Attacker Data: Kali/ Parrot

Objective

Monitor a target system remotely and perform other tasks:

- Bypassing access controls to gain access to the system
- Acquiring the rights of another user or an admin
- Creating and maintaining remote access to the system
- Hiding malicious activities and data theft
- Hiding the evidence of compromise

Overview of System Hacking

There are four steps in the system hacking:Gaining Access: Escalating Privileges: Maintaining Access: Clearing Logs:

Lab Tasks

1. Gain access to the system
    1.1. Perform active online attack to crack the system's password using Responder
    1.2. Audit system passwords using L0phtCrack
    1.3. Find vulnerabilities on exploit sites
    1.4. Exploit client-side vulnerabilities and establish a VNC session
    1.5. Gain access to a remote system using Armitage

1.6. ~~Hack a Windows machines with a malicious Office document using TheFatRat~~

1.7. Perform buffer overflow attack to gain access to a remote system

2. Perform privilege escalation to gain higher privileges
   - 2.1. Escalate privileges using privilege escalation tools and exploit client-side vulnerabilities
   - 2.2. Hack a Windows machine using Metasploit and perform post-exploitation using Meterpreter
3. Maintain remote access and hide malicious activities
   - ~~3.1. User system monitoring and surveillance using Power Spy~~
   - ~~3.2. User system monitoring and surveillance using Spytech SpyAgent~~
   - ~~3.3. Hide files using NTFS streams~~
   - 3.4. Hide data using white space steganography
   - 3.5. Image steganography using OpenStego
   - 3.6. Covert channels using Covert_TCP
4. Clear logs to hide the evidence of compromise
   - 4.1. View, enable, and clear audit policies using Auditpol
   - 4.2. Clear Windows machine logs using various utilities
   - 4.3. Clear Linux machine logs using the BASH shell
   - ~~4.4. Clear Windows machine logs using CCleaner~~

*Indicates capture