Assigment #2

Graded

1. Uploaded complete
2. Submitted complete
3. Graded complete

Details

**Objective:**Perform various exploitation and post-exploitation techniques on the target system (Metasploitable) and make a summary report from this PenTest

**Due**: 03/25/2021 (Thr) 11:59 pm (submit your file in pdf format)

**Point: 40pt**

**Exploitation #1 [25]**

1. Based on the (Nessus) report you created from the Scanning phase, use the Metasploit Framework to **exploit** the system.  
   Perform two exploits using the lecture note. Prove that you got into the target system.
   * 1. Use "unreal\_ircd\_3281\_backdoor" with "CVE 2010‐2075" (from the lecture note)
     2. Use "Bind Shell Backdoor Detection" (from the lecture note)
     3. Summarize the exploitation **process & results**
     4. Please **add images for every step you performed**
2. Try to explain the vulnerability you exploited and what to do to protect the system

**Exploitation #2 [7]**

1. Use Armitage to exploit Metasploitable and provide snapshots for every stage you’ve done
2. Try to explain the vulnerabilities you’ve exploited

**Post-exploitation [8]**

1. Use NetCat to upload Nmap executable file to Metasploitable
   1. In Kali, executable files (Nmap) go into /usr/bin, resources into /usr/share, config files into /etc, and logs into /var/logs
   2. Find the Nmap executable file from your Kali, and upload the file to Metasploitable using the Netcat.  
      \*The uploaded Nmap executable file can be used for further scanning of the local network (which is not a part of the task)  
      \*Executable file in Linux doesn't have \*.exe like Windows. If you can see -rwxr-xr-x file permission from ls -l, that is an executable file.
   3. Show the process you’ve done by the screenshots