Computer Science Department
University of Crete

CS-455: Internet Attacks
Spring 2022 - 2023

Assignment 6
Live Pentesting

Live: 03/05/2023, 14:00 – 16:00

Introduction

In this assignment, in a live environment, you will try to exploit a vulnerable machine by gaining access to a low lever user, escalate privileges and eventually root it. Your answers must include screenshots and brief explanations.

Questions

1. **[5%] Step 1: Setup**
    - Load the vulnerable VM (VVM) in VirtualBox
    - Start Kali and the VVM
    - VVM: login with root:csd
    - VVM: **run dhclient** to get an IP (as an old VM it won't get an IP automatically)
    - Make sure these two VMs can communicate (ping)
    - **Record Kali's and VVM's IP address**

2. **[5%] Step 2: Scanning**
    - Kali: **run nmap** -A -p- -T4 VVM_IP
    - **Record a screenshot (briefly discuss the findings)**

3. **[10%] Step 3: Exploit FTP**
    - **Exploit the fact anonymous FTP is allowed**
    - Ignore vsftpd version and all other open port related exploits (ssh, etc.)
    - Login to the FTP server and download (on Kali) the only file shown
    - **Record the FTP credentials used, the command to download the file and the contents of the file (briefly discuss the findings)**

4. **[5%] Step 4: Crack the hash**
    - Use **hashcat** with appropriate arguments
    - **Record the command used and the password retrieved (briefly discuss the findings)**

5. **[5%] Step 5: Scan the VVM website looking for a page to use the password retrieved**
    - Use **dirbuster** (disable recursion, otherwise it will take hours to finish)
    - **Record dirbuster's initial settings and the results (briefly discuss the findings)**

6. **[10%] Step 6: Exploit the student management portal**
    - The portal allows for the uploading of a photo
    - As the web server runs PHP, instead of a photo, upload a **PHP reverse shell**
    - Download a PHP reverse shell from a trusted/reputable site!
    - Edit the PHP reverse shell to make necessary changes
    - Setup a listener on Kali
    - After you upload the shell, you will notice that it will immediately execute
    - **Record details about the PHP reverse shell used, the changes you made and a screenshot of the listener after you run the whoami command (briefly discuss the findings)**

7. **[20%] Step 7: Privilege escalation**
    - Use **linpeas**
        - https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS
        - https://github.com/Cerbersec/scripts/blob/master/linux/linpeas.sh
        - Download linpeas from a trusted/reputable site!
    - **Transfer linpeas.sh** from Kali to the VVM
        - Use a python web server on Kali to serve this file
        - Retrieve this file on the VVM
    - **Run linpeas.sh** on the VVM
        - Scan the output for passwords
        - Pay attention to a mySQL **password** and the **file** it is stored in
    - **Record the site you downloaded linpeas from, the commands for running the python web server and transferring the file to the VVM, the passwords identified in linpeas' output and the filename the mySQL password is stored in (briefly discuss the findings)**

8. **[20%] Step 8: Access the VVM with a username**
    - Retrieve the **username** shown in the file storing the mySQL password
    - Run cat /etc/passwd to identify the **role** of that user
    - Use **ssh** to access the VVM using the username and the MySQL password
    - Look for **interesting files** stored in the user's home directory
    - You will find one **script** that runs periodically (every minute)
    - Scheduled tasks usually run with **elevated privilege** (root)
    - **Record the username retrieved, the role of that user, the ssh command used to connect to the VVM and the contents of the script found (briefly discuss the findings)**

9. **[20%] Step 9: Gain root access**
    - Replace the contents of the script with something else
    - The **appropriate content** will return a reverse shell running as root
    - **Record the snippet of code that you used and Kali's listener output after running the whoami command (briefly discuss the findings)**

Submission

- Submit a pdf document including all the information requested above.
- Submissions will be done through eLearn.
- This assignment is a group of max 2 students creative process and students must submit their own work. You are not allowed, under any circumstances, to copy another person's work. You must also ensure that your work won't be accessible to others.
- You are encouraged to post any questions you may have in the eLearn forum. If, however you believe that your question contains part of the solution or spoilers for the other students you can communicate directly with the course staff at hy455@csd.uoc.gr.

Disclaimer

It is **ILLEGAL** to attempt any type of attack against a target (individual, network, public/private entity, etc.) without authorization / explicit permission. Such actions are **prohibited and punished by law and university policies**.