Lab 2 - Gaining Access to OS and Application

SUMMARY

In this lab you will explore all five phases of hacking:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

This lab is a complete hands-on and is based on exploiting real world applications and system vulnerabilities. You will get to experience different tools in Kali Linux, which will be your attacker machine. You will have to find the root cause of vulnerabilities and use methods to exploit them. Read the documentation section before proceeding with the lab to make sure you have all the necessary screenshots at each step.

Even though the bonus part of lab is optional, we highly motivate you to attempt it and give your 100% effort as it will be a good learning experience.

Please submit a single PDF file containing the required deliverables from each of the sections below.

LAB SCENARIO

CY Corp. has fired the IT and security teams after a data breach and hired you to clean up the mess. Your job is to conduct a penetration test to find vulnerabilities that are known to exist, also find any proof of existing compromise. All the people that knew about IT are no longer with the company. No one can explain the services or network architecture and you have no prior knowledge of the environment.

There is one rule: You are only allowed to test one system i.e. the VM that you have downloaded. You will be fired if you do anything malicious against any other system that does not belong to you or have written permission to attack on. You should use the attacker methodology taught in class along with any additional online searching.

To complete this lab you need to gain access to **3 different users** on the system. For the first bonus you need to gain access to the **fourth user** and for second bonus you need to gain access to the **root** user.

PREPARATION

- Download the target VM from the link provided on blackboard.
- Unzip, open and start the target VM in VMWare.
- Verify the VMWare’s network configuration is in NAT mode.
- Start Kali Linux in VMWare also in NAT mode.

TOOLS OVERVIEW

Kali Linux: Netdiscover, Nmap/Zenmap, Nikto, Dirb, Metasploit, WPScan

RECONNAISSANCE

1. The most important part of an assessment is enumeration of services. You need to understand the target before you can assess its security.
2. You do not have login information to the target VM. Remember the IT team was fired and is not interested in helping you.
3. You do not know the IP address assigned to the VM by VMWare. Use the knowledge gained during previous tasks to find the IP address of the target system. You can use Kali Linux and various tools to help you find all IP addresses on the LAN.

Hint: Netdiscover can be useful here

Deliverables

1. Submit a screenshot showing the IP address of the VM.

SCANNING

1. Once you have the IP, use Nmap / Zenmap (Google if you have not used these tools) to enumerate services on the machine. Use various options within the tool against the target VM. Make sure you can enumerate services on each port.
2. Try different type of scans. Example:
   - Ping Scan
   - Regular Scan
   - Intense Scan on all ports.
3. Once you have identified the vulnerable services, manually try to access them. For example, if you find wordpress running on the machine, connect to that machine from your Kali VM and see if you can browse the system to find any interesting files that might help you get access to the vulnerable machine. You should do the same to other ports that were enumerated above.

Hint: You might need to perform other Nmap/ Zenmap scans.

Deliverables

Answer the following questions and attach appropriate screenshots:

1. What is the lowest TCP port open on the VM and what service (including the version no.) is running on that port?
2. What is the second lowest TCP port open on the VM and what service (including the version no.) is running on that port?
3. What is the highest TCP port open on the VM and what service (including the version no.) is running on that port?
4. What is the operating system name and version number running on the target VM? (Hint: You can verify it once you have the shell access)

GAINING ACCESS USING APPLICATIONS AND OS ATTACKS

There are more than one ways to skin a cat, and there are more than one ways to compromise a system. The C.Y. Corp. IT team was not very good at application configuration and did not change the default configuration after application installation. This is the reason they were fired.

For this lab, you do not need to download additional tools to Kali Linux or use tools like Nessus and OpenVas. Everything you need to complete this lab is available on the default installation of Kali Linux and will require no extra setup.

Note: There are total **5 tracks or 5 ways to exploit the system** (that are known to us) that would give you access to 5 different users (web1, web2, web3, web4 and root). Start with the following steps and you would understand how are those tracks separated.

1. Manually try to explore the applications and services running on open ports on the system. For instance, explore the web application running.

    - Explore each application and look out for hint on these services.
    - Try to access different files on server.
    - Examine the web page and different links. Try common username and password if prompted.

    The developers have left clues in the plain sight and the purpose of the server can also help in gaining access. Do not use automated tools yet, try various passwords and glean hints from the content of the applications you are exploring.

    - Information is not always in plain English. There are online tools that can do the conversions for you. For example, *01101000 01101001* (binary) to *hi* or *aGVsbG8=* (base64) to *hello* or *NBSWY3DP* (base32) to *hello*.
    - Try to decode any suspicious looking information on the services you explored above.

2. After you have gathered information from plain sight, run Nikto and Dirb/Dirbuster on the open ports to discover hidden content.

    - **Nikto:** Run "nikto" and look for vulnerable applications and services

      Hint: Use the specific URI when performing Nikto Scan. For example: `nikto -h 192.168.209.142:9000 -root=/html`. Also try different switches to get concise output like “Tuning”.

    - **Dirb:** Use it to find information about hidden directories.

3. Use the information you have gathered and google it. For example, if the machine is running Apache tomcat/coyote version X. You can use Google to search “Apache tomcat/coyote version X exploit” and explore results you get.

4. You can perform this exploit search using Metasploit as well.

    - Start Metasploit.
    - For example: If the server is using Drupal --> Type `search drupal` --> Metasploit search module will display a list of all the exploit modules.

5. The next step is to exploit the vulnerabilities you found. You can exploit any vulnerability for any service running on the target VM.

6. The end goal of the exploit is to get shell access to the server. Metasploit should (by default) give you a meterpreter shell. In case you are downloading an exploit, make sure you understand what it does. You might have to change the shell-code or something similar to get a shell. You can refer to https://www.offensive-security.com/metasploit-unleashed/ in case you are not sure how to use Metasploit.
    - Search for commands to execute during meterpreter session.
    - Drop into system command shell.
    - Check your privileges and identify the username (Hint: Use `id`).
    - After you get a shell, locate the file containing the **flag** present inside the home directory of the current user.
    - Read the contents of the flag file to get the hint for the next track.

## Deliverables

Before moving forward - verify you can access all cert DNS names in a browser as each hostname has a different vulnerability.

1. Exploit **any 3** vulnerabilities in the target VM. Each vulnerability should lead you to a different user on the system. Following is the hint for first vulnerability:

    *"If they think first place is the winner, then they don't know a **ninja**"*

    For each vulnerability, write detailed steps that you took to exploit the vulnerability. Right from recon to exploitation including the commands you ran that helped you in successful exploitation.
2. Include the value of both the **flags** along with screenshots of the following commands (for each flag):
    - `stat <flag_file_name>`
    - `cat <flag_file_name>`

    Note: In case you do not get the shell directly, try the next part (maintaining access) to get a stable shell and then you can easily execute the above commands.
3. For the second track, mention the credentials that you found to access the website. Also, explain how did you find them.

MAINTAINING ACCESS & COVERING TRACKS

The shell that we get from the exploit is a temporary shell which is not reliable as vulnerable services can be patched in future. Therefore we need a way to maintain our access to the system once we have exploited a vulnerability and gained access to a user. One way to achieve this is by installing SSH key on the server.

Also, make sure to hide your tracks i.e. delete any temporary files or user accounts created on the system.

###Deliverables

1. Include a screenshot showing successful login to the VM using SSH command. Make sure the screenshot includes the following:
    - `ssh` command to login.
    - Output of `id` command after ssh-ing into the VM.

BONUS 1 (+10%)

RG8geW91IHJlYWxseSB0aGluaywgd2Ugd2lsbCBnaXZlIHlvdSBhIGhpbnQgZm9yIHRoZSBleHRyYSBib251cy EhISEgUk9GTA==

Exploit another vulnerability in the VM and gain access to the system shell. Run `id` command to make sure the exploited user is different from previous 3 users. You should get access as `web4` user to complete this bonus.

Deliverables

1. Write detailed steps that you took to exploit the vulnerability. Add screenshots to make it easier for us to understand.
2. Include the value of the **flag** along with screenshots of the following commands:
   - `stat <flag_file_name>`
   - `cat <flag_file_name>`

BONUS 2 (+10%)

You have successfully exploited the machine and found access to the OS. But, do you know what would prove you as a h4x0r? **Getting root access!**

Root access is only possible after you have completed the Bonus 1. So, please make sure you have completed the track and have a shell with `web4` user to perform this part. This is different from previous tracks as this involves **privilege escalation**.

Kernel exploit is not allowed.

Deliverables

1. Write detailed steps that you took to exploit the vulnerability. Add screenshots to make it easier for us to understand.
2. Include the value of the **flag** along with screenshots of the following commands:
   - `stat <flag_file_name>`
   - `cat <flag_file_name>`