EITP20 Secure Systems Engineering
Pentest Assignment
Blow the Weapons!

1 Introduction

This project will introduce you to the basic of network and application penetration testing.

2 Objectives

1. Gain exposure to the network and application penetration testing.
2. Applying the 4-step-model of penetration testing to a real-life use case.
3. Learn to use the tools in penetration testing.
4. Ability to write a thorough and detailed report on vulnerability.

3 Behind The Scene

You work as an offensive hacker at one of the leading security consultancy firm in the country. For the sake of this course, let's call the company you work for as ”E-Corp”. Recently, E-Corp signed an agreement with a foreign government. Unfortunately, the government who offers you this exciting project has a lot of enemies. They suspect that one of their enemies secretly develops a massive biological weapon that endangers the existence of human lives. They try to stop it by all means necessary!

They have done their homework by deploying agents on the ground, trying to capture as much as possible pieces of information for you. Here is what they know so far:

- The weapon is connected to a backend server which can be accessed only by an authorized system administrator.
- The backend server is assumed to be the single point where most logic of the weapon is being developed and deployed.
- The initial scan from the team on the ground shows that the backend server is running Linux, probably the latest kernel, but they are not sure.

- There is a high probability that the backend server is also running an in-memory database. The purpose of this DB is yet to be determined by the team on the ground.
- There exist a website where the system administrator can manage the backend server with a very nice and beautiful GUI. However, the initial probing shows that the web might not run on a standard port, i.e. 80 and 443. But, this might be wrong.
- The team on the ground found several ciphertexts[1]. They believe that the ciphertext contains key information about other nodes of the backend server, i.e. identity of other backend servers such as IP address and possibly open-ports, etc. However, since they cannot decrypt the text, they cannot decide on what to do.

Hence, they ask you for help to do the following tasks:

1. The team on the ground will send you several ciphertexts, possibly containing information about the existence of one of the backend servers.
2. Your task is to decrypt such ciphertexts, and if you find any information, the follow-up tasks would be:
    - To try to get into the system, where the IP address is written in the ciphertext you received.
    - To try to get access as a "root" in the system.

However, it is very important to leave as minimum as possible "footprint" when you infiltrate the system. The government will not help you in court if you accidentally reveal your identity, i.e. your IP, your name, etc, and get caught by the enemy. You're all on yourself. However, they will pay you a considerable amount of money (in BTC[2] or ethereum[3]) if you successfully gained access to the backend server. The amount of money will however depend on the gained level of access, i.e :

1. **Level 1**: Successfully decrypt the ciphertext and infiltrate to the system would give you 100 BTC.
2. **Level 2**: Successfully infiltrate the system (but not gaining root access) and extracting some information from them, would give you 1000 BTC.
3. **Level 3**: Successfully gain the "root" level of access to the system would give you 10000 BTC. Please note that you're not allowed to do anything once you gain root access. Everything should happen under the radar. The leader of the foreign government might ask you to shut down the system though, but always remember that it is **NOT** your call!. Overstepping the rules would lead to a contract termination of your company.

[1] https://en.wikipedia.org/wiki/Ciphertext
[2] https://bitcoin.org/en/
[3] https://ethereum.org/en/

4 Actual Task

You will be given a target virtual machine containing all the applications above, acting as your victim. There will be multiple versions of VM (which has the same level of difficulty). Which VM you will get is assigned randomly. For each VM, there will be **at least** 2 vulnerabilities. For each vulnerability, you should associate that with the respective CVE[4] code in the report. To some extent, the way we do this task would be similar to Capture The Flag [1] competition. To pass this assignment, you need to **at least** find **one** flag.

The first vulnerability is related to the application running in the VM, which is also exposed to the outside world. As a hint, the VM will give you many ”exposed services” which means two things, i) The vulnerable application(s) is/are always one (or maybe more) of them, ii) do not waste your time by assessing an open port too long. If you can't find a vulnerability in one of the exposed services, move on to the other one, and so on. If you found the first vulnerability, you will directly able to see the first flag, namely ”flag1.txt”. The first vulnerability would lead you to get access to a non-root user in the victim server. You will be able to read the first flag as it is merely plaintext.

To be able to read the second flag, you need to have a ”root” level access in your victim server. We do not provide any hint about the second flag in this document. Instead, you need to enumerate again. Together with an acceptable report (see Deliveries), here is the points you get for each flag you discover:

- 1^{st} flag : 3 points
- 1^{st} and 2^{nd} flags : 4 points
- 1^{st}, 2^{nd}, and presenting the vulnerabilities mitigation : 5 points

In any part of this assignment, you are allowed to use any :

- Information, and/or
- Tools, and/or
- Publicly accessible code

However, please include the source of the information on where you get that in the reference section. Also, to simplify your journey, we provide you with a list of recommended software to be used in section 6. Combined with basic linux commands, it should be enough to use these software to achieve all the tasks in this assignment.

5 Rules

- This is a group work with maximum 2 members per group. You are only allowed to discuss with your teammate. Overstepping this rule would lead you to grade F in this course.

[4] https://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures

6 Software

Here is a list of softwares you might need to use during this assignment:

- **Metasploit** [2]. It is possible to run metasploit on your own computer. But, for simplicity, Kali also provides built-in metasploit inside their OS.
- **Flan** [3] [4]. A wrapper for nmap for network vulnerability scanner. It is a fairly new tool just released on November 2019 by CloudFlare. You will be able to map specific vulnerability with the respective CVE code with this tool.
- **nmap** [5]. Network exploration tool and security / port scanner.
- **tcpdump** [6]. A tool to dump traffic on the network. The options ”-w” might be useful for this assignment.
- **wireshark** [7] Packet analyzer. The captured packet of tcpdump can be viewed with this tool.
- **netcat** [8]. A swiss army knife related to TCP and UDP.

7 Deliveries

Here is a list of questions you need to answer in your report, depends on the points you are aiming for.

1. 1^{st} flag:
    - Write the decrypted ciphertext as part of your written solution!
    - Give a brief description of how you proceeded in your attacks!. **Note:**
        - A sloppy explanation is not accepted.
        - You might be able to get the plaintext directly by using the online tool available. But, answering this question with something like *”tool X give me answer Y”* is not accepted. Please explain what is happening under the hood! (Conceptually, how did you perform the attack?)
    - Which cipher is used to encrypt the plaintext? And, what is the key? What happens if the keylength is changed?
    - What is the IP address of your target?
    - Which port(s) is/are vulnerable?
    - What is the name of the application(s) is/are running in the vulnerable port(s)?
    - What is the vulnerability? If it exists, please include the CVE number as well.
    - What makes the application vulnerable? Is it bug or misconfiguration? Describe in detail.

- Describe what you did in detail to get the 1^{st} vulnerability. Make sure that your explanation is clear. It is better to include the step-by-step command line you use, along with a brief explanation and the purpose of each command. If you need to write code, please attach your code to the report and write a brief explanation of what the code is doing.
- What did you do in the reconnaissance phase?
- What did you do in the scanning phase?
- What did you do in the exploitation phase?
- What needs to be done to secure the vulnerability?
- Who is the name of the computer scientist in the first flag?

2. 2^{nd} flag:
   - What is the vulnerability? If it exists, please include the CVE number as well.
   - Why are you able to switch user from a non-root to the root user? Describe in detail.
   - Describe what you did in detail to get the 3^{rd} vulnerability. Make sure that your explanation is clear. You also need to write your code to solve this part. Attach it to the report and give a brief explanation on what the code is doing.
   - What did you do in the reconnaissance phase?
   - What did you do in the scanning phase?
   - What did you do in the exploitation phase?
   - What needs to be done to secure the vulnerability?
   - Who is the name of the computer scientist in the third flag?

Depends on your target of the point(s), you have to answer the questions above correctly. The deadline is shown in the canvas page. If you are uncomfortable with a weekend deadline, just submit it in advance.

Report **must** be written in latex and you **have to** use the provided template to do that. The template is available in the course webpage. Submission is done through canvas.

Have fun!

References

References

[1] https://en.wikipedia.org/wiki/Capture_the_flag#Computer_security

[2] https://www.metasploit.com/

[3] https://github.com/cloudflare/flan

[4] https://blog.cloudflare.com/introducing-flan-scan/

[5] https://nmap.org/

[6] https://www.tcpdump.org/

[7] https://www.wireshark.org/

[8] https://linux.die.net/man/1/nc