ACIT 4630 – Lab 3 – Exploitable

Notes:

If you worked with a partner in Lab 1, you will be working with the same partner for this lab.

Instructions:

We are going to use Metasploit on Kali to exploit the vulnerable Metasploitable machine.

Perform a port scanning from Kali to remember what services are running on what ports on Metasploitable2 VM.

Take screenshots of your code snippets and important results and explain what you observe as you go through the lab.

Exploiting vulnerability in MYSQL server

Assume you are hired as a penetration tester to test security controls on Metasploitable2. As a first step, you're going to try to get access to the MySQL service using MetaSploit modules.

- Type msfconsole on the command line on the Kali machine to open the Metasploit console.
- Once the console is ready (msf6> prompt is shown), type search mysql to search for modules related to MySQL.
- From the results, choose an Auxiliary Module (read more about the modules you find on this link, look under both Admin and Scanner modules) to attempt to **find the credentials** of the MySQL server running on the target machine.
    - **Note:** We don't know the credentials yet, so don't choose a module that assumes you can provide a given set of credentials
    - Type use <module name> to select a module
        - Hint: you can also type use <the # from the search result>
- When the module is selected, type show options to see what options (parameters) are available for the selected module. What are the **required** options with no current setting?
    - Use set <name of the option> <value> command to assign values to them.
- Create a file with some generic usernames like root, guest, etc, and use it as an option for this module.
- When all the required options are set, type run
- (Q0) Were you able to find any username and password?

From our vulnerability scanning results in the previous lab, you could see that the same weak username and passwords have also been detected through vulnerability scanning under "MySQL/ MariaDb weak password".

The next step is to attempt and exploit this vulnerability. Once you've gained access to the server (find a username and password), use another auxiliary module to perform **a SQL query** on the target machine and find what databases exist.

- (Q1) What is the auxiliary module you used in this step, how did it help you in this lab? (provide a screenshot of your commands and their results)
- Now assume that there's a table called user in the mysql database. Change an option in the second auxiliary model you used to print out user and password columns from this table.
    - You need to use your SQL knowledge here!
- (Q2) Which part of the CIA triad was compromised in this attack?
- (Q3) Did we use any malware in this part? Explain your answer.

Exploiting vulnerability in IRC service

From the vulnerability scanning report provided in the previous lab find a vulnerability named "Check for backdoor in UnrealIRCd".

- Find the CVE reference number in the report and search Metasploit console for any module related to this vulnerability.
- Type use <module name/path> to select a module
- When the module is selected, type show options to see what options (parameters) are available for the selected module.
- Set any required option
- Run show payloads to see compatible payloads that can be used to take advantage of this vulnerability.
- Select one of the options by set payload <name of the payload> This will set up a backdoor (remote access shell) on the target that we could access from Kali.
    - If you select one of the reverse shells you also need to also run set LHOST <Kali VM's IP>
    - Watch this video to understand different kinds of remote shells
- Run the exploit by typing run
- (Q4) How can you prove you have access as the root account to the Metasploitable2 VM?
- (Q5) What Linux command can you run to you find the root's hashed password while you are running a shell on the Metasploitable2 VM?
    - Hint: hashed passwords are saved in /etc/shadow file
- (Q6) Users of this version of UnrealIRCd were infected with this backdoor when they downloaded the latest version. Explain what kind of malware was used to distribute this payload.

For more info about this vulnerability
read https://www.unrealircd.org/txt/unrealsecadvisory.20100612.txt

Submission For Lab 3:

- Create a report answering the questions in the lab above.
- Walk through your report with your instructor.
- Submit your report to the Learning Hub in PDF format.

This lab is due at the beginning of the Week 4 class and is worth a maximum of 10 marks.