

Metasploit

Chaitanya Vooradi

Abstract: This paper covers the basics of widely used penetration testing tool by security researchers Metasploit. It covers why the metasploit framework is more powerful than the other testing tools present. Some basic program terminologies are discussed. At the end of the papers we will discuss about the drawbacks of the metasploit.

1 Introduction:

Due to the rampant success of Internet, many sites are launching daily. There are very limited resources available to monitor and secure these sites. Then there is requirement of software to exploit the vulnerabilities in a system. Metasploit came into picture to make the life of security researchers easy with built in 1647 exploits, 1037 auxiliary modules, 472 payloads and 40 encoders.

Metasploit was designed to use it as a penetration testing tool that could be easily utilized by even novice users to perform penetration testing, regression testing, patch verification, and development of new exploits.

Metasploit is a script based web attack framework written in languages like Ruby, C, C++ or even Python. Such framework is able to carry numerous attack scripts, many of which are able to exploit vulnerabilities of a specific application across many versions.

Network Security professionals use metasploit for penetration testing, Security Administrators for patch installation verification, Product vendors for Regression testing and Security researchers for Development of exploits.

Some Basic terminologies need to know before understanding about Metasploit :

Vulnerability: A weakness which allows an attacker to break into or compromise a system's security.

Exploit: Code which allows an attacker to take advantage of a vulnerability system.

Payload: Actual code which runs on the system after exploitation

Auxiliary Modules: Used for Scanning, fuzzing, sniffing, etc..

Payloads are of three types:

Singles: A single payload contains the exploit and full shell code for the selected task.

Singles are payloads that are self-contained and completely standalone

Stagers:Stager establishes a communication channel between the attacker and the victim and reads in a stage payload to execute on the remote host.

Stages: Stages provide the components for the stager to deploy. Stages are payload components that are downloaded by Stagers modules

Metasploit Opcode Database: Web based interface has comprehensive list of opcode.It has rich collection of codes over 14 million opcodes covering 320 different opcode types and 14 operating systems. One of the best feature of Metasploit and reason behind it is used widely was its great feature of saving data in its internal database.

Simple commands used to help novice users are: 1) show exploits/payloads 2) info 3) show options and 4) help.

Five basic Steps used to exploit in many situations:

1. Choose and configure the exploit.
2. Check if target is vulnerable to exploit
3. Configuring payload
4. Encode the payload to un-detect the virus.
5. Execute exploit

2 Literature Search:

Security Auditors Research Assistant is the network analysis tool which was in third generation. It became benchmark for security analysis.It supports nix, Linux, MAC OS/X or Windows (through coLinux).

Nessus is also a very good vulnerability testing tool still integrated with metasploit to scan for the loop holes in the network.

HD Moore release the first version of framework in October 2003 with 12 exploits developed in perl.With the help from SPoonm, he release version 2.0 in April 2004 with 19 exploits over 27 payloads. As received backing from Information Security community

and its wide popularity they come up with version 3.0 in 2007. Migration from perl to ruby happened with lots of changes in the code.

Later it came with different interfaces. Msfconsole, msfcii and Armitage. Msfconsole is the most widely used with command line interface. Msfcii puts priority on scripting and interpretability with other consoled tools. Armitage is GUI version of Metasploit. Instead of executing commands, GUI provides pretty easy way of working with metasploit.

3 Body of the Report:

Main features of Metasploit:

Framework Base: It has a rich framework base which provides functionality required in Penetration testing. Some functionalities are logging, configuring, database storage, meterpreter scripting etc..

Auxiliary modules: These are functional modules work both pre and post exploitation like scanning, information gathering, launching specific attacks, OS detection, service detection.

Packaged tools: Comes with very handy tools helps during penetration testing. These add-on packages can create standalone payloads and encrypt the payloads using different algorithms

Third-party plugins: It can integrate with third party plugins.

3.1 Classification of previous Work:

Metasploit has many features, each feature was designed for a specific vulnerability detection. Will discuss the two major attacks possible with Metasploit.

3.1.1 Attacking Oracle DB:

One of the challenge for exploits is attacking db. Large important data resides in db. Oracle is most secure organization in maintaining db. Majority of database use oracle. Chris Gates and Mario Ceballos came with the solution to attack oracle db. Attacking it contains 7 steps: 1) Locate system running Oracle 2) Determine the version 3) Determine oracle SID 4) Brute force user name and password 5) Privilege escalation via SQL injection 6) Post exploitation 7) Cover tracks

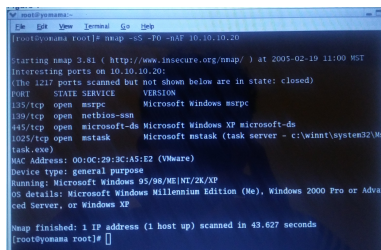
Each step requires the use of auxiliary modules. NMAP was used to search port number. TNS mix-in was added to determine the version. SID enumerator was used to determine SID. Now oracle no longer gives this information. Brute forcing using dictionary list by Pete Finnigan for user name and password. SQL injection in DBMS EXPORT EXTENSION package can help to get privileged escalation. Win32exe was used to create user name on system for future use.

3.1.2 Attacking Windows Operating System:

This attack is based on the only knowledge of Network segment where the boxes resides. The network segment where both Linux boxes configured are 10.10.10.0/24 subnet. Linux machine or VPT box is at 10.10.10.10.

→ ICMP scan to locate the address 10.10.10.20

→ NMAP scan on this address to know the services and OS details and the port details.



```
root@kali:~# nmap -sS -p 135,139,445,593 -iL 10.10.10.20
Starting Nmap 7.81 ( http://www.insecure.org/nmap/ ) at 2017-02-19 11:00 WOT
Interesting ports on 10.10.10.20:
(The 1217 ports scanned but not shown below are in state: closed)
port      state         service
135/tcp    open          msrpc         Microsoft Windows msrpc
139/tcp    open          netbios-ssn   Microsoft Windows XP microsoft-ss
445/tcp    open          microsoft-ds   Microsoft Windows XP microsoft-ds
593/tcp    open          wscntask       Microsoft wscntask (task server - c:\winnt\system32\W
(task.exe)
MAC Address: 00:0C:29:8C:A5:E2 (VMware)
Device type: general purpose
Running: Microsoft Windows 95/98/NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Pro or Advan
ced Server, or Windows XP
Nmap finished: 1 IP address (1 host up) scanned in 43.627 seconds
root@kali:~#
```

Source: Introduction to Metasploit project for Penetration Tester.

Here we can see loop hole at port 445.

→ Nessus scan to know the more about loop holes in the network.

→ Choose the exploit lsass_ms04_011. Using command: use sass_ms04_011

→ Select payload. ex: set PAYLOAD win32_reverse

→ set port and ip address

set RPORT 445, set RHOST 10.10.10.20, set LHOST 10.10.10.10 Give command "show options" to know details are updated.

→ Type command "exploit" to exploit the target. On successful exploit it opens 'C:\WINNT\system32 >'. Type ipconfig to know the details and confirm that target system.

3.2 Comparison:

Well in-order to work with Metasploit, one should know the way to find the loop holes in the system. Each exploit was designed based on the loop holes present in the network. Ex-

exploits are developed for different platforms including Android, Windows, Linux...etc. Here in the above two explained attacks, first one was very complicated where different modules were used for each loop hole to find the desired information. In the second one too nmap, nessus were used to find the open ports to attack.

3.3 Short-Comings and Weakness:

Msfcli and msfweb do not provide for any authentication of the remote user. No exploits for web based vulnerabilities. There are no reporting capabilities, which would help the tester produce a comprehensive report of the exploits run and the vulnerabilities discovered.

As metasploit is an open source framework, the exploits developed are known to everyone and can defend their systems against the newly developed exploit. Metasploit was developed mainly for security researchers but it was used as a hacking tool by many people.

3.4 Lessons Learned:

Learned about the testing tool metasploit and its implementation. Came to know about some of the major issues in the security field. Learned how the security researchers are trying to develop new methodologies in generating payload to obfuscate from the Anti virus using different encoding techniques. Learned about METASM in the process of exploring encoding techniques and how it can be used to obfuscate the payload. Worked on Kali Linux operating system to effectively use the metasploit features.

4 Conclusion and Future Work:

Like many security tools, the Metasploit has great potential with all of the features that have been presented. But again like many security tools there is the possibility of misuse. It is up to the individual end user to decide how it will be used.

The future may include payloads that are dynamically written at the time of attack to be as stable and stealthy as possible depending on the target. Need to work on development to support all functionalities in all the platforms. Windows doesn't have all the

functionalities that are present in linux operating system. Need to have a varied encoding techniques in-order to obfuscate from anti virus.

5 Bibliography:

- [1] Protection against penetration attacks using Metasploit Himanshu Gupta; Rohit Kumar 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions)
- [2]An Analysis of the IDS Penetration Tool: Metasploit Carlos Joshua Marquez Department of Technology Systems East Carolina University Greenville, NC, U.S.A. cmarquez09@students.ecu.ed
- [3]An Introduction to Metasploit Project for the Penetration Tester
- [4] <https://www.pentestgeek.com/penetration-testing/using-metasm-to-avoid-antivirus-detection-ghost-writing-asm>
- [5] http://www.nothink.org/metasploit/documentation/metasploit_payloads.pdf
- [6] <http://nessus.org/>
- [7]<https://repo.zenk-security.com/Metasploit/Metasploit>