

Forum:[Hack Forums](#)

Thread: [\[Samaritans\] Metasploit: An Introduction](#)

Meterpreter - September 4, 2019, 4:54 am

Metasploit: An Introduction (And Other Things)

Metasploit is a penetration testing framework which was first developed in 2003 by HD Moore. Originally being programmed in Perl, it was later rewritten in Ruby. Then in 2007 Metasploit was adopted by Rapid7 who to this day maintain all services. Metasploit can be used for information gathering(port scanning), non-intrusive vulnerability checks, initial and post exploitation.

Information Gathering & Reconnaissance Port Scanning

What is port scanning? It is exactly what it sounds like essentially. It is the process of scanning ports in the search for open ports. Open ports are ports that can be accessed because they are used by a particular service (i.e. FTP server, SMB). You also have filtered which limits port access, and closed which are ports that are not accessible.

How to undergo port scanning with Metasploit: In Metasploit if you give the command "search portscan" you will find an array of auxiliary modules for a range of port scanning including NAT-PMP, ACK (Firewall), FTP Bounce, etc. The main port scanner is the plain TCP Port Scanner and will simply output all open ports. Finding the open ports allows you to gain intelligence on the points of attack.

Discovering Versions

Once you have a full list of open ports you will now need to discover what is running on those ports. The most common ports and services are:File Transfer Protocol (FTP) - 20/21

Secure Shell (SSH) - 22

Telnet - 23

Simple Mail Transfer Protocol (SMTP) - 25

Domain Name System (DNS) - 53

Dynamic Host Configuration Protocol - 67/68

HTTP - 80

HTTPS - 443

NetBIOS (SMB) - 137/138/139

Internet Message Access Protocol (IMAP) - 143

Of course, ports can be modified, but if you see any of these ports that is a stage of service finding, you have most likely identified the service already. You need to have a rough idea of what services are running on each port, because now you need to run a specific auxiliary module to discover specific version information.

For example, if you scanned a host and found port 137 is open, using the list above you can see that it is most likely SMB. If SMB is open you can use the SMB version module to scan for the Windows Operating version. Let's say you use the SMB module and it returns with version: Windows Server 2008 SP2. You now have a specified target, port, and version. You can use a module by typing: use /path/to/module - then give command: show options and input any required information.

Finding Exploitation's

So you have the target, you have an open port, and you have the version of the service on said port. What now? Well, say hello to exploits. Exploits

are that which make use of vulnerabilities. When you have a potential vulnerability which works, it then becomes an exploit. Enter <https://www.cvedetails.com>. Top right insert your version information (Windows Server 2008 SP2). Click the top link and it will bring you to a page of potential vulnerabilities with their score (security risk). Here you will see 2 remote exploits for this version. The first is a DoS code execution exploit, clicking it brings you to an information page explaining where the vulnerability exists and why it occurs. Scrolling down you will find links to external articles talking about the exploit, and sometimes their will be a pre-made exploit, such as: <https://www.exploit-db.com/exploits/9594>. We'll get to this later on.

Now you can take the MS identifier for this vulnerability and put it into Metasploit, using: search MS07-063 will give you potential exploits for this specific vulnerability.

Password Sniffing

Password sniffing in Metasploit is accomplished with the module psnuffle. This is a local attack and requires access to the internal network. Psnuffle can be used to sniff out passwords sent over POP3, IMAP, FTP, and HTTP. This can be a quick way to obtain credentials.

Initial Exploitation

Exploit Setup

So you have found a target machine, scanned the ports, found an open SMB port, scanned the version, and found potential exploits in Metasploit for that version. What now? Now you exploit. By giving the use command you can tell Metasploit what exploit you want to use. So: use /path/to/smb/exploit

Then you give: show options - which tells you what information you can give the exploit. It tells you what is required and what is not. RHOST/S = Remote Host/s, RPORT = Remote Port, LHOST = Local Host, LPORT = Local Port. To set this information give commands: set rhosts enter.target.ip - then give: set rport yourport (i.e. 137) and so on and so forth for any "required" options.

To run this exploit type: run - or if you want to be a super l33t haxor type: exploit

If the exploit is successful you will be given a meterpreter shell. Hey! That's me!

Meterpreter Shells

What is a meterpreter shell? A meterpreter shell is a Metasploit payload (post-exploitation) that is executed on the target machine as a DLL. It communicates back to the attackers machine via Transport Layer Security (TLS). Essentially, it talks to your computer, and allows your computer to talk to the victims PC. The DLL execution occurs because the exploit you use has a method of "code execution" as mentioned previously with the DoS SMB exploit.

One of the most common methods of code execution is via buffer overflow vulnerabilities. I will explain what this is with a very basic example. Say the victims PC is your kitchen and the SMB service is a glass in said kitchen. Now imagine you pour water into the cup, it fills up, you drink some, and so on and so forth (service running normally). But what happens when you fill the cup too fast? Well if your cup doesn't have anti-spill (invulnerable code), it will "overflow" into the kitchen. The water which is now in the kitchen, has leaked into other areas. The other area in this example being the kitchen, and the kitchen being neighboring memory regions. It begins in a source, and leaks into different memory regions, giving you code execution. If it overflows at this length:

#####<-You could put arbitrary code here. Cool.

Post Exploitation

Pivoting

What is pivoting? Pivoting is using a compromised system to access or "pivot" to new networks and machines that weren't previously accessible. The most basic example of this requires basic topology. Say you have a Windows server and its running your HTTP server, FTP server, and this and that. Connected to this server might be an internal network such as an organisations internal systems or a someones internal home PC, laptops, and phones.

External Facing (World Wide Web) <- Web Server <-> 2 PCs <-> 1 Laptop <-> 2 Android Smartphones. With (Web Server <-> 2 PCs <-> 1 Laptop <-> 2 Android Smartphones) being the internal network.

You exploit the server, using Metasploit functions such as autoroute you can route scans from your attacker PC to the exploited server to be run as the exploited server. This turns an external/remote scan into a local scan. You can then do the above steps: Port scan, version scan, vulnerability analysis, and then exploitation. Exploitation can be routed through the compromised server, or you can set up an individual link from the newly compromised system directly to your machine.

Post Exploitation

To wrap it up, I wish I could have written more. It's nearly 12am and I am not a late to bed kinda guy. I really hope you enjoy this read, I know to the knowing eye I seemed to miss quite a lot, but if I didn't limit myself, this wouldn't be an "introduction" thread and I would write forever. Much love <3

My First Samaritan Thread

Written by Meterpreter

pms - September 4, 2019, 5:07 am

Looking forward to see what this post will contain, good luck :)

Meterpreter - September 4, 2019, 6:53 am

(Sep 4, 2019 05:07 AM)pms Wrote: [\[CITE\]](#) Looking forward to see what this post will contain, good luck :)

All done, hope you enjoy!