Metasploit Post-Exploitation Command List

If for any reason you cannot access/edit these files in the future, please contact mubix@hak5.org

You can download these files in any format using Google Doc's File->Download As method

If you are viewing this on anything other than Google Docs then you can get access to the latest links to the Linux/Unix/BSD, OSX, Obscure, Metasploit, and Windows docs here: http://bit.ly/nuc0N0

DISCLAIMER: Anyone can edit these docs, and all that entails and implies

Table of Contents

Presence, Persistence, and Pivoting

Everyone does things differently, and explaining what goes through an attackers head when they get a shell is virtually impossible and even more so to generalize into a methodology, but I've tried to do that with the "3 'P's of Post Exploitation" and they are in a certain order for a reason but certainly up to circumstance to what order is best.

The first P is Presence. It is first because the attacker needs to get a sense of what he/she has got before they move on. It plays a crucial part in the other two 'P's, making them much stealthier or easier. Many times I've seen people jump from box to box and totally miss that what they were looking for was on the first one. So "Presence" is all about discovering what you (the attacker) has already. This has many levels and the order of which the attacker checks them and how is arbitrary as well, but they should have at the very least a check list of categories to check on. Here are some to think about:

File System:

> Knowing "where" to look is tough but in each section below we'll go into known good places to check and ways to search for files and folders with interesting names and extensions

OS

> Proxy settings, Group Policy settings, login scripts, MOTD, User lists (net user and /etc/passwd). Knowing how the system and attacker has compromised is a crucial piece to understanding how it communicates and works as a piece to the network.

RAM

> Mostly known for pulling hashes and credentials out of it, there are a lot of other interesting things that reside solely in memory

Media

> CDs, DVDs, NFS mounts, SMB mounts, USB sticks. These are often bypassed and forgotten during an attack but can hold the keys to the kingdom

Network

> Routes, ARP entries, netstat are pretty common to check, but broadcast messages, listeners, and IPv6 are less so.

Permissions and Credentials

> This is the obvious one but there is usually a mountain of data as even TinyCore linux has hundreds of files, each with their own permissions. This category extends past the borders of the others but important to single out as a separate step.

Persistence is achieved at varying levels depending on what the attacker is trying to survive and what the attacker is willing to give up on the stealth side. Staying in memory pretty much kills the attackers chance of surviving a reboot for instance. Tactics to survive a rebuild or revert are also very different. Persistence can also come in the form of simple authentication, if the attacker has a password and it nets him/her code execution or access to the data they are after then that's all they need. Special focus should be applied to the information gathering section of penetration tests or red team engagements in regards to places that require authentication.

Pivoting simple means extending the attackers current access, and can mean anything from connecting to a remote NFS mount to the attacker PSEXEC-ing their Meterpreter payload onto another box that they have administrative access to. This is the last stage because concentration on the previous two is hard to do in the adrenaline high of initial access.

Honorable Mention (the mysterious 4th "P") Privilege Escalation is not part of the Trio (because then there would be 4 and I wouldn't know what to call it) while it's a regular step performed by attackers, it's something that usually gets too much emphasis. _You do not always need Domain Admin access to access the "crown jewels"_ .These highly privileged accounts should be assumed to be extremely monitored and coveted. (adding a new user to the Domain Admins group is like lighting your hair on fire and running in the front door of the targets office building screaming "h4x!!")

Windows Native Meterpreter

Payloads available:
windows/meterpreter/bind_ipv6_tcp
windows/meterpreter/bind_nonx_tcp
windows/meterpreter/bind_tcp
windows/meterpreter/find_tag
windows/meterpreter/reverse_http
windows/meterpreter/reverse_https
windows/meterpreter/reverse_ipv6_http
windows/meterpreter/reverse_ipv6_https
windows/meterpreter/reverse_ipv6_tcp
windows/meterpreter/reverse_nonx_tcp
windows/meterpreter/reverse_ord_tcp
windows/meterpreter/reverse_tcp
windows/meterpreter/reverse_tcp_allports
windows/meterpreter/reverse_tcp_dns
windows/patchupmeterpreter/bind_ipv6_tcp
windows/patchupmeterpreter/bind_nonx_tcp

windows/patchupmeterpreter/bind_tcp
windows/patchupmeterpreter/find_tag
windows/patchupmeterpreter/reverse_ipv6_tcp
windows/patchupmeterpreter/reverse_nonx_tcp
windows/patchupmeterpreter/reverse_ord_tcp
windows/patchupmeterpreter/reverse_tcp
windows/patchupmeterpreter/reverse_tcp_allports
windows/patchupmeterpreter/reverse_tcp_dns
windows/x64/meterpreter/bind_tcp
windows/x64/meterpreter/reverse_tcp

Windows Meterpreter is the most developed and well known payload set inside of Metasploit, while the other sections will try to push the limits of the functionality of the different Meterpreter types, this section will focus more on the “best” way of using it. Since this is a publicly editable page that will mean that “best” will develop over time, but expect a fight if you put in something I feel is stupid, will get an attacker caught, or hard/impossible to clean up. [--mubix]

Presence

Persistence

Pivoting

Java Meterpreter

Payloads available:
java/meterpreter/bind_tcp
java/meterpreter/reverse_http
java/meterpreter/reverse_https
java/meterpreter/reverse_tcp

Presence

Persistence

Pivoting

PHP Meterpreter on Linux

Payloads available:
php/meterpreter/bind_tcp
php/meterpreter/reverse_tcp
php/meterpreter_reverse_tcp

Presence

Persistence

Pivoting

PHP Meterpreter on Windows

Payloads available:
php/meterpreter/bind_tcp
php/meterpreter/reverse_tcp
php/meterpreter_reverse_tcp

Presence

Persistence

Pivoting

Linux Meterpreter

Payloads available:
linux/x86/meterpreter/bind_ipv6_tcp
linux/x86/meterpreter/bind_tcp
linux/x86/meterpreter/find_tag
linux/x86/meterpreter/reverse_ipv6_tcp
linux/x86/meterpreter/reverse_tcp

Presence

Persistence

Pivoting

Compatibility is listed for each command, here is the key for the abbreviations:

Windows Meterpreter	win
Java Meterpreter	java

PHP Meterpreter	php
Linux Meterpreter	linux
Command Shell	shell

Metasploit 4.2 documentation:
https://community.rapid7.com/docs/DOC-1751

Information Gathering

Command	Compatibility	Description and Reason
getuid	win,java,php	Lists current user

Meterpreter Scripts

(deprecated but still useful)

Post Modules

TAKEN FROM WINDOWS LISTS, NEEDS TO BE FORMATTED

Meterpreter Commands

ps	(show running processes and their associated users/id numbers)
getuid	Get user ID
getpid	Gets the process ID
getprivs	(shows current privileges)
getsystem	Attempts to get SYSTEM using 4 methods, the last being a local exploit called Kitrap0d. This can sometimes be caught by host based IDS systems and even in rare occasions blue screen the machine.
getsystem - (place holder for targetd getsys)	If anyone wants to fill this in before I can please do
sysinfo	Get system information
timestomp	Remove/screw up timestamps if you are good enough this messes up audit tools
clearev	Clears event logs
hashdump	dump SAM file hashes for pass the hash or cracking
migrate [pid]	Move from exploited process into another process

Useful Meterpreter Scripts

killav.rb (Meterpreter script that kills all Antivirus processes.)
winenum.rb (Retrieves all kinds of information about the system including environment variables, interfanetworkces, print_line "routing, user accounts, and much more.)

- scraper.rb (harvest system info including network shares, registry hives and password hashes.)
- persistence.rb (Meterpreter Script for creating a persistent backdoor on a target host.)

- keylogrecorder.rb (This script will start the Meterpreter Keylogger and save all keys.)
- getgui.rb (Windows Remote Desktop Enabler Meterpreter Script.)
- For a complete list please see: http://metasploit.com/svn/framework3/trunk/scripts/meterpreter/

Useful Meterpreter Post Modules

- post/windows/gather/smart_hashdump
- post/windows/gather/credentials/vnc
- post/windows/escalate/bypassuac (mixed results)

Useful Multi-Step Techniques

- “Pass The Hash” attack (Gain access to other computers with stolen hashes, no cracking involved)
- Token impersonation via incognito

  use incognito
  list_tokens -u
  impersonate_token

  ->http://www.offensive-security.com/metasploit-unleashed/Fun_With_Incognito

Convert Metasploit’s MSCACHE output to Hashcat version (performed in ~/.msf4/loot/):
cat *mscache* | awk -F "" '{print $4":"$2}'