**Covering tracks: The finishing touch of a hacker**

***By Abir Atarthy***

Dear my budding hackers! Hackingheart is back again. Sorry as I couldn’t post for long time!

I have written many articles on how to compromise the remote system. Thanks for all your comments! It’s your encouraging words that motivates me to write the blog. Thank you once again and love u all….!

In this guide, I'll show you a few ways that we can cover our tracks, making it VERY difficult for a system admin, forensic investigator, or law enforcement agent to track our malicious activities.

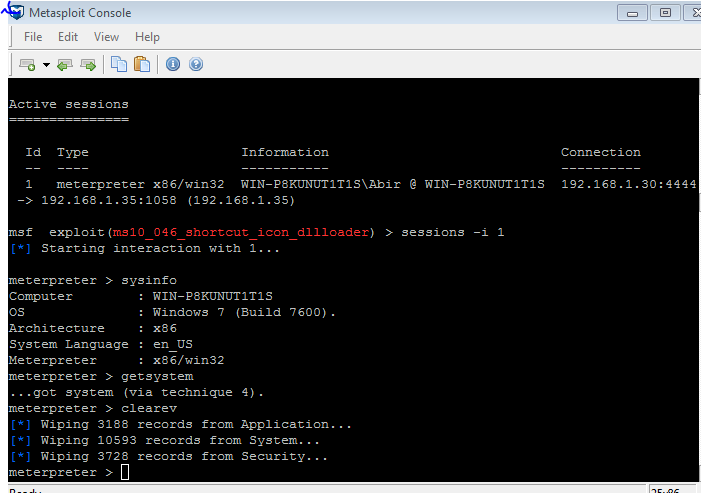
Every unsuccessful login, successful login, and security event is logged into the log files. System admin can check this log file to see who has entered into system and what actually has happened. So, the first thing we need to do is to make certain there is no trace of our malicious activities in those log files.

**Clearing Event Logs with the Meterpreter**

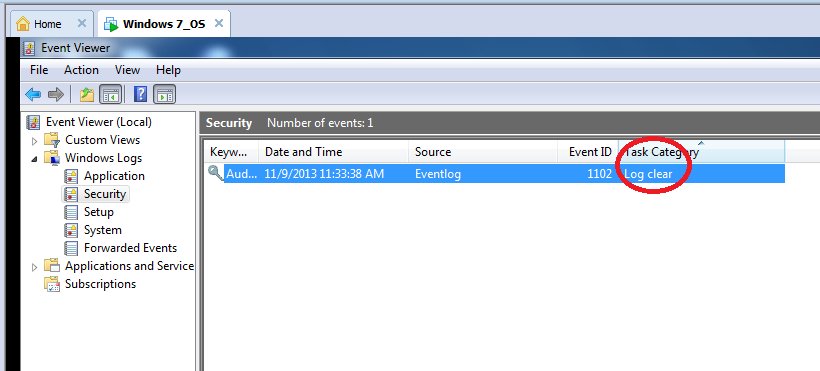
In Metasploit's  meterpreter , there's a script called **clearev** to clear all event logs. This program will go into the event logs on a Windows system and clear out ALL of the logs. This might look a little suspicious to the vigilant system admin, but most system admins are NOT vigilant.

At the very least, it will remove our connection and/or attempted connection from the log files. Of course, there may be other evidence left behind such as router logs and IDS logs, but we'll deal with those in a future tutorial.

First, use Metasploit to compromise the system and get a meterpreter command prompt. Then use clearav command.



The clearav command can clear three three types of logs., namely Application,system and Security. Go to windows eventviewer to check these all logs had been cleared.



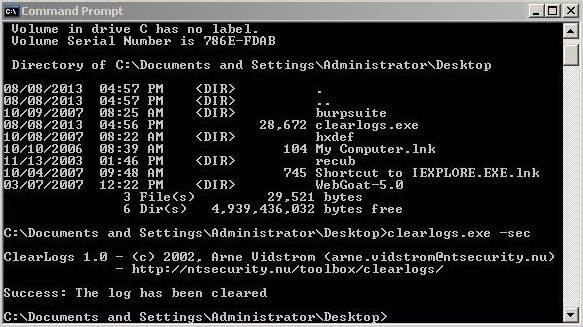
As we can see in this screenshot above, all of the event logs from Application, System, and Security have been cleared from the log files on the victim system.

**Clearing Event Logs on Windows Machines**

You can also clear the log files on Windows systems is to use the**clearlogs.exe** file.

If we have physical access to the system, we can simply install it and then run clearlogs. We can choose to clear the Security, Application, or Security logs. To clear the security logs, type:

* **clearlogs.exe -sec**

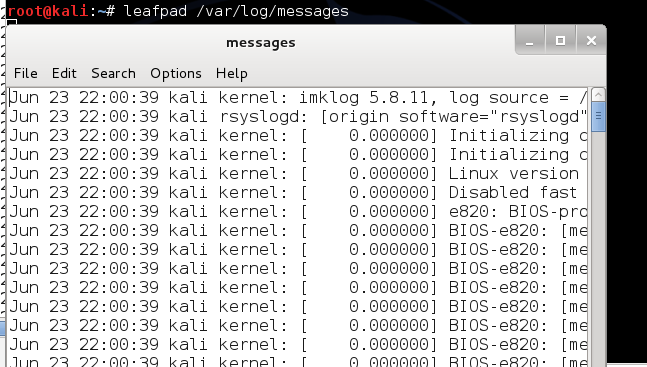


We can then go to the Event Viewer and click on Security events, where we can see that all the security events have been cleared! There is no trace we had been there!

**Clearing Event Logs on Linux Computers**

In Linux systems, log files are stored in the **/var/log** directory. We can open and view that plain text file containing log messages by opening with any text editor (I'm using leafpad in Kali Linux)

**leafpad /var/log/messages**



**Erasing the Command History**

Finally, before we leave the compromised Linux system, we want to make certain that our command history is erased. Remember, the bash shell we're typing in will save our last 500 commands. A system admin could track all of our commands and detect and decipher our activities on the system and potentially use them as evidence.

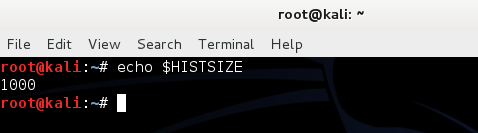
To see our history, we can use the **more** command:

* **more ~/.bash\_history**



The size of our history file is determined by the environment variable**HISTSIZE**. We can check the size of the HISTSIZE variable by typing:

* **echo $HISTSIZE**



We could then set it to zero by typing:

* **export HISTSIZE=0**

Now, our shell will not store any of our history! If you remember, change it to zero before beginning the hack and none of your commands will be stored, but if you've already written some commands, remember to log out and log back in to clear your history after setting the HISTSIZE to zero.

**Shredding the History File**

Sometimes we won't have enough time to erase the history file or change the HISTSIZE variable. In a hurry, we can simply shred our history file by typing:

* **shred -zu root/.bash\_history**

The **shred** command with the **-zu** switches will overwrite the history with zeros and delete the file.

[](http://img.wonderhowto.com/img/original/87/46/63511652667283/0/635116526672838746.jpg)

To check to see if our history has been shredded, we can view the history file by typing:

* **more /root/.bashhistory**