

Forum:[Hack Forums](#)

Thread: [How to clear logs and covering track after hacking a system?](#)

h1tman - August 12, 2017, 9:29 pm

Hi,

How to clear logs and covering track after hacking a system?

Do you know any good book or tutorial about this topic??

Baud - August 14, 2017, 4:44 am

I doubt you will find entire books on the subject, since all you need to know is how the operating system of the system you are using works. So, first of all, detect the operating system, then if you don't already know where that specific OS stores its logs, you can always look for it on Google. About Linux, which is the operating system you will run into most of the times, logs are usually kept under `/var/log/` so all you need to do is delete the files contained in that folder, they will be recreated automatically by the system itself so no need to worry about it, although it can be suspicious if a sysadmin finds semi empty logs, so the most efficient and safest way would be writing a script that opens every log file, and deletes the records of your own IP, leaving everything else intact.

Also keep in mind that some third party softwares (an FTP server or an IDS for example) can keep their own logs inside their directories, so always look for installed programs that might have detected your activities, and delete their logs as well. Here are a few links that may be useful to you:

[LINUX]

<http://www.thegeekstuff.com/2011/08/linux-var-log-files>

<https://www.lifewire.com/introduction-to-linux-log-files-2192233>

<https://www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/>

[WINDOWS]

<https://serverfault.com/questions/70328/where-how-does-windows-store-the-data-in-the-event-logs>

h1tman - August 16, 2017, 5:29 am

(Aug 14, 2017 04:44 AM)Baud Wrote: [\[CITE\]](#) I doubt you will find entire books on the subject, since all you need to know is how the operating system of the system you are using works. So, first of all, detect the operating system, then if you don't already know where that specific OS stores its logs, you can always look for it on Google. About Linux, which is the operating system you will run into most of the times, logs are usually kept under `/var/log/` so all you need to do is delete the files contained in that folder, they will be recreated automatically by the system itself so no need to worry about it, although it can be suspicious if a sysadmin finds semi empty logs, so the most efficient and safest way would be writing a script that opens every log file, and deletes the records of your own IP, leaving everything else intact.

Also keep in mind that some third party softwares (an FTP server or an IDS for example) can keep their own logs inside their directories, so always look for installed programs that might have detected your activities, and delete their logs as well. Here are a few links that may be useful to you:

[LINUX]

<http://www.thegeekstuff.com/2011/08/linux-var-log-files>

<https://www.lifewire.com/introduction-to-linux-log-files-2192233>

<https://www.cyberciti.biz/faq/linux-log-files-location-and-how-do-i-view-logs-files/>

[WINDOWS]

<https://serverfault.com/questions/70328/where-how-does-windows-store-the-data-in-the-event-logs>

Thanks 'Baud', I see the links. but I want to find a complete book or checklist for covering tracks for example in Linux clean web server logs and bash history and

Nomad.Null - August 16, 2017, 6:06 am

I prefer null-byte's tutorials on wonderbyte.

<https://null-byte.wonderhowto.com/how-to/hack-like-pro-cover-your-tracks-leave-no-trace-behind-target-system-0148123/>

As Baud mentioned, this will only affect logs on systems you own. You will have no luck clearing logs on IPS/IDS, firewalls, SIEM, or WAPs with this. If you pop shell on a website after bypassing the WAF, you would also need to find the WAF logs and clean house there as well. If you encounter a network protected by a SIEM...well...there's no way to get the logs out of there, honestly. Logs get propagated to a separate system entirely, so when it comes to SIEM, there's really no feasible way to clean up afterwards.

If you're gonna bust a nut in the network, better wear a condom.

mutybyte - August 17, 2017, 12:14 am

Also try to look for python scripts/bash scripts/perl scripts which delete logs automatically. Why i am telling this? because you will get idea after reading those scripts the locations of all files and folders where all these logs are located. Many CTFs writeups might have such script

Also check cron jobs to know about operating system more.

In last the two above users know much very much compare to me

Enjoy

Vana - August 17, 2017, 12:16 am

Code `rm -rf /var/log/` Gets rid of a good amount, dependent on your privilege level.

h1tman - August 21, 2017, 12:11 am

(Aug 17, 2017 12:14 AM)mutybyte Wrote: [\[CITE\]](#) Also try to look for python scripts/bash scripts/perl scripts which delete logs automatically. Why i am telling this? because you will get idea after reading those scripts the locations of all files and folders where all these logs are located. Many CTFs writeups might have such script

Also check cron jobs to know about operating system more.

In last the two above users know much very much compare to me

Enjoy! search some CTF writeups on github but can't find any useful script, Can you tell me one of them for log cleaning?

Thanks?

xotictastez - August 26, 2017, 2:33 pm

This thread has been EXTREMELY helpful, thank you all!