

Forum:[Hack Forums](#)

Thread: [Clearing Apache access.log](#)

WOLGA - November 25, 2015, 10:55 pm

Hey Hackforums,

I have shelled an apache webserver. How would I clear the logs from /apache/logs/access.log after I use the shell, or does this not matter?

Gee4rce - November 26, 2015, 2:06 am

Well depends on the type of access you have with that shell,

if you'd only can send comands and get back the final output only, then you'd be better of deleting the access.log and creating a new, empty one.

That's kinda suspicious tough and admin may figure that something is going on (implying he checks logs) but on the other hand better than having the entries in the logs on how the hack was performed.

Or, if you have for example direct connect to the server with live output in shell/putty, then you could use vim/vi/nano to edit out the entries your actions have caused.

If you go for deleting logs, make sure to stop apache Server before deleting the access.log, like this "/etc/init.d/apache2 stop", then delete logs and create new access.log file, then start apache again.

In some cases it might be "/etc/init.d/httpd stop" or "systemctl httpd stop" (for redhat based nix distro).

Cheers, Gee.

WOLGA - November 26, 2015, 3:02 am

(Nov 26, 2015 03:06 AM)Gee4rce Wrote: [\[CITE\]](#) Well depends on the type of access you have with that shell,

if you'd only can send comands and get back the final output only, then you'd be better of deleting the access.log and creating a new, empty one.

That's kinda suspicious tough and admin may figure that something is going on (implying he checks logs) but on the other hand better than having the entries in the logs on how the hack was performed.

Or, if you have for example direct connect to the server with live output in shell/putty, then you could use vim/vi/nano to edit out the entries your actions have caused.

If you go for deleting logs, make sure to stop apache Server before deleting the access.log, like this "/etc/init.d/apache2 stop", then delete logs and create new access.log file, then start apache again.

In some cases it might be "/etc/init.d/httpd stop" or "systemctl httpd stop" (for redhat based nix distro).

Cheers, Gee.

It is a PHP shell on a windows server, I do not think I can edit the log with the apache webserver disabled.

Essentially, the problem is that the http request to the php shell to edit the log, leaves a log.

Gee4rce - November 26, 2015, 3:35 am

(Nov 26, 2015 04:02 AM)Qwertyuiopasdfghjklzxc Wrote: [\[CITE\]](#) It is a PHP shell on a windows server, I do not think I can edit the log with the apache webserver disabled.

Essentially, the problem is that the http request to the php shell to edit the log, leaves a log.

Ahh, i didnt think of the situation that if you stop apache, then you have no access via shell anymore : >

Well how about backconnecting with netcat or so and then use cli?
Then you are not dependand anymore from the webservice running.

Cheers, Gee.

HaxOr? - November 26, 2015, 6:14 am

You could just spam it with other information? Just a tough..

Vellichor - November 26, 2015, 8:00 am

(Nov 26, 2015 03:06 AM)Gee4rce Wrote: [\[CITE\]](#) Well depends on the type of access you have with that shell,

if you'd only can send comands and get back the final output only, then you'd be better of deleting the access.log and creating a new, empty one.

That's kinda suspicious tough and admin may figure that something is going on (implying he checks logs) but on the other hand better than having the entries in the logs on how the hack was performed.

Or, if you have for example direct connect to the server with live output in shell/putty, then you could use vim/vi/nano to edit out the entries your actions have caused.

If you go for deleting logs, make sure to stop apache Server before deleting the access.log, like this "/etc/init.d/apache2 stop", then delete logs and create new access.log file, then start apache again.

In some cases it might be "/etc/init.d/httpd stop" or "systemctl httpd stop" (for redhat based nix distro).

Cheers, Gee.Re-read the OP. He's accessing the site through a web shell.

ProblemSolva - November 26, 2015, 12:42 pm

you need to root the server to have access to the logs mate.

Gee4rce - November 27, 2015, 2:15 am

(Nov 26, 2015 09:00 AM)Vellichor Wrote: [\[CITE\]](#) Re-read the OP. He's accessing the site through a web shell.

Correct, thats why i later suggested back connecting to the server.