

Forum:[Hack Forums](#)

Thread: [LINUX : Server rooted, how to keep a hidden root access/shell](#)

X-HAT - August 12, 2017, 3:05 am

Hello folks,

For example i have rooted a linux server and i want to stay root on this server without adding a new root user to /etc/shadow because the owner will find that,

I've tried a rootkit kalled "MAFIX" and it seem that it get detected & deleted.
anyone have a better idea.

Thanks to all.

Phizo - August 12, 2017, 6:00 am

Write your own rootkit. Hook `__*stat{,64}, __*statat{,64}, access, *open{,64}, *dir{,64} *statvfs{,64}, unlink{,at}, etc.`, to hide your rootkit and other files. Hook `*execve{,64}, execv, execl`, and the rest of the exec family, system, ptrace, etc., to monitor debuggers and similar "watchdog" processes. Unload the shared library from memory, and map it back into shared memory when the "watchdog" process dies. Hook `dlsym, dlvsym, dlopen, etc.`, to hide the addresses of the symbols which represent your interposed functions by returning the addresses of the real symbols in `/lib/libc.so, /lib/libdl.so, etc.` Write a little LKM (Linux Kernel Module) that hides the memory mappings from `/proc/pid/maps` also. Change the default preload path (`/etc/ld.so.preload`) by patching the dynamic linker. Preserve a false version. This beats rkhunter and chkrootkit easily. There are many things you can do in order to evade detection. These are some simple things you can do to get started. People think userland rootkits are weak, but they just don't know how to properly evade detection. They have the advantage of being mostly kernel-independent also. You can always write a kernel-land rootkit using LKMs, though.

X-HAT - August 12, 2017, 8:41 am

Thank u, Phizo. I agree with you idea, but i need something ready & undetectable. did u hear about the (Horse Pill Rootkit)

<https://www.youtube.com/watch?v=wyRRbow4-bc>

Source Code : <https://github.com/r00tkillah/HORSEPILL>

Beurk Rootkit : <https://github.com/unix-thrust/beurk>

lwrist - August 16, 2017, 5:20 pm

(Aug 12, 2017 08:41 AM)X-HAT Wrote: [\[CITE\]](#) Thank u, Phizo. I agree with you idea, but i need something ready & undetectable. did u hear about the (Horse Pill Rootkit)

<https://www.youtube.com/watch?v=wyRRbow4-bc>

Source Code : <https://github.com/r00tkillah/HORSEPILL>

Beurk Rootkit : <https://github.com/unix-thrust/beurk>

His solution is 10/10 though.

s1xp4th - August 18, 2017, 4:25 am

get your hands on defiler's rekit and youre done