

Forum:[Hack Forums](#)

Thread: [Kali Linux - How to Persistent payload?](#)

cocoricco1 - November 12, 2015, 4:46 pm

Hello guys,

I was searching for weeks how to hack a computer on local network, I know how to do it now. But, I want my payload (generated by Setoolkit : powershell injection) stays on the victim's computer and can be launched automatically at boot. I have some problems and I don't know how can I launch the payload with system's privileges. It's for hack Windows 7 and "getsytem" didn't work for me, Thank for any help!

Key Punch - November 12, 2015, 5:52 pm

MetSvc should solve the persistence issue.. if you are unable to get system.. you can always attempt to pivot ex:pass the hash.. to another machine on the local network

cocoricco1 - November 13, 2015, 1:02 am

My remote control works with a backdoor wich was open manually, pivot will works without any backdoor?

dusername - November 13, 2015, 3:52 am

In my opinion you shouldnt use the payloads that come with kali as they are quiet detectable. I'd rather use a fud rat to infect him. That way i would have control even on an external network. In my opinion kali payloads are not to be taken serious but just for testing purposes.. If you're doing something for real i suggest using a fud rat you may have

mattzap - November 13, 2015, 6:44 am

Yes.... you'd have to encrypt the kali exes and transfer Malware like a rat or, depending on the exploit, just use the fud rat instead of intermediary

cocoricco1 - November 13, 2015, 9:45 am

Can I found rats for free or are they codable in C++?

dusername - November 13, 2015, 10:29 am

(Nov 13, 2015 10:45 AM)cocoricco1 Wrote: [\[CITE\]](#) Can I found rats for free or are they codable in C++?

you can possibly setup darkcomet and ask a member to crypt it for you. but my suggestion is to learn to code your own so that you will not be depending on the others, in the future.

Rats can be coded in almost every language.

cocoricco1 - November 13, 2015, 2:14 pm

Thanks a lot man! I'll search for WinSock!