

Forum:[Hack Forums](#)

Thread: [Opinions on White Hat Hacking to protect Insecure hosts](#)

ry4wnn - March 25, 2016, 10:24 am

I am curious for peoples opinions on white hat hackers hacking vulnerable hosts and patching and backdooring them. I did some research and found this group who had compromised 1000's of hosts just to secure them. Looking for some feedback - I did a write up on this at one of my sites and opened it up for comments but comments here are just as good. If you want to read and comment there it is [computersecurity.org](#)

f1re_w1re - March 25, 2016, 11:48 am

You have a lot of typos you need to fix on that write up. My opinion is that there is a fine line on what "intentions" are that people can't really put a finger on. Either way you look at it, it's not legal. Ever heard of the CFAA? I suppose is a good gesture, but it's not legal. You can't skip asking for consent to test something you don't own. You're just asking for trouble.

People don't think the same and have different morals, someone may interpret your actions differently. Every head is its own world.

?Criminal - March 26, 2016, 11:45 am

Compromising most hosts is childs play most small to medium ones run WHMCS which theres multiple shelling methods once you get admin credentials via various means and the larger ones either run coldfusion or some large web framework such as apache struts(need a java based shell php shells are useless here) which is somewhat easy to shell as well although most coldfusion hosts the coldfusion admin panel the directory is either ip whitelisted or password protected so cold fusion hacking is pretty much dead in 2016.I think the worst security fail hostwise was volumedrive due to cross data leakage the main billing info was stored in the DBMS on volumedrive.com which ran a relatively old version of wordpress despite the login server being on a different box(manage.volumedrive.com or something like that) starfall if you know who he was was able to get the hiddenwiki private key by I assume cracking random volumedrive hashes and looking around, while f1re_w1re seems to be white hat im gray hat I don't really pwn big stuff just small stuff you can get fucked if the sites big enough for small sites that teen sysadmins run they usually don't give a shit, consolecrunch was one example where the sysadmin recruited people to harden their xenforo install.Although when exploiting any web application its always good to have great opsec going in.

0x7FFDF000 - March 26, 2016, 1:55 pm

I am curious for peoples opinions on white hat hackers hacking vulnerable hos-

Stop there. They're not white-hats. They're grey-hats. White-hats do not break the law. They only hack with complete consent.