

Forum:[Hack Forums](#)

Thread: [**--Intranet Oday exploit remotely! --**](#)

CyberM@X - May 22, 2011, 6:42 am

Oday exploit - remotely

Here is a little story of what I experienced in my spare time at school .. Enjoy?

This story is based on: File execution & Oday exploitation remotely from intranet!

Code Well it all started up at my school, and I wanted to getting access for the teacher computer, and I was like ... what can I mess with here.

So I was thinking, if I could crack that md5 hash of that computer to gain administrator access then I would be able to execute commands remotely from the intranet. ?

So I began with using ophcrack at a local machine, and found the password for the local administrator network.. right. I exploited the password of the administator, what now.

Well what I did next was to go at the teacher computer and start login as administrator. It succeed when I logged in, and I was like ... umm let me try this password and username on other computers... WOW! I was chocked... the security was = 0 .. The passwords all above the whole school were the same. This password was also used for BIOS editing!!?

Well I messed around creating a backdoor from the teacher's computers (I have to say in each classroom we do have an admin computer which only the teachers "should" be allowed to access... But I was able to access them as well and create my self a super user to execute these commands.

I was curious and did thinking of .. hmmm if the teacher was on the computer & the studens were working at same local intranet, well then I should be able to have access for the computer as well... So I had!! - I just went to the CMD and prompted in "Net view" (this was to exploit the vulnerabililities of what I could access at!)

So I was typing in a few net commands to gain access for \$IPC / \$ADMIN and as well files at the computer the teacher was working on...

when I looked into one of the files, then I did go to probities and viewed the permissions at the teachers computer (so I'm running from an XP box to and XP box, and viewing the permissions) - By here I could go at advanced and add my self to the domain for having my user to access the teachers computer I did like added EFIF\user and hit ok.. afterwards I did go at the teachers computer for curiosity while he was afway, I sneaked over and logged into my account and was supricing how this was easy done! - since usually the normal users cannot access the teacher computer without having an super-user account.

Hope you like my story, throw a comment, and tell me what you think..?

lol 50 views no comments ... dissapointing ! :(..

[/hr]

Did anyone found this interesting ?

Frostbite™ - July 14, 2011, 6:46 am

Very interesting, going to try some of these methods on my school. Dont know why noone commented. Thankyou

CyberM@X - July 14, 2011, 2:03 pm

Well thank you for showing some kind of interest in my thread :)! - nice to see some activity finally !..

BUMP!

Toaster - July 14, 2011, 7:53 pm

Nice thread man, I found this interesting.

Big Baller Shot Caller - July 14, 2011, 7:59 pm

It was pretty interesting. What up with the title, I don't get the "0 day"

Jarien - July 14, 2011, 8:33 pm

Nice story, maybe not so similar to mine:

My school has a website, where other students can see it's grade by login in, so I found an exploit that I was able to upload a shell from some place, and I did upload a password-protected one, so I had access to the whole website, I even managed the database of the website, but couldn't download the database file which has everything, because it's being used by other process, but I still was able to control everything, but I didn't do anything bad, I closed the exploit, and protected the website by myself, but I still had access to everything, I wanted to tell my teacher about this, but I was scared that he could think, that I hacked the school website grade system, without even thinking of I'am doing something good but I didn't tell him to the moment yet. It would be cool if someone can help me to download that file :P

Thanks,

PS: Nice story bro :)

Hentai? - July 14, 2011, 8:34 pm

very nice lol should install rat from backdoor and mess with everyones computers ?

?Ñâzg?! - July 14, 2011, 10:12 pm

Yea I tried this also ?

And now its summer and my Rat is still on the computers?

Thats what the school gets for using mcafee..?

CyberM@X - July 15, 2011, 9:45 am

Yeah well school security is = Zero ! ...

Security ... What security ?? ... Security is an illusion!

Thanks for all the comments on my own exploit :)!

I'm working on how to crack a harddrive password ATM, since I got a new IBM + DELL computer for free, and thoese are both password protected.. and I can't boot up on backtrack for cracking the password or even Ophcrack... nothing can boot without the password :(!.. if you got any ideas of how to bypass this then please answer me through PM!.

Kindly regards,

