

Forum:[Hack Forums](#)

Thread: [\[TUT\] How To Hack Your School Network \[WORKS\]](#)

Jacques Chirac - January 8, 2011, 1:24 pm

Hello world ?

So, a lot of people here should want to hack his school's network.

It can be really easy, and it can be quite difficult if your school have active network administrators.

Anyway, you can do it following my tutorial, there are a lot of possibilities but I will explain the most efficient methods here...

So, Let's started !

Gain local admin privileges

It's very easy to gain admin privileges.

1st method :

(cmd not blocked)

How to open CMD?

-Press Windows+R ==> type "cmd.exe" in the box
or

-create a new text file, just write it inside :

Code @echo off

command

pause and save it as "something.bat"

just click on it.

In cmd, type :

Code net user *nameyouwantfortheaccountthere* /add

(don't write the stars)

and now type :

Code net localgroup Administrators *nameoftheaccount* /add

note :

For non-english computers, the group "Administrators" could not be the same, on french computers, it's called "Administrateurs", so for check what is the name of the group, just type "net localgroup" for see the list of groups on the computer

Now you can connect yourself on the local machine with an admin account

2nd method :

Just burn ophcrack on a dvd

ophcrack can be found here :

<http://ophcrack.sourceforge.net/download.php?type=livedcd>

If the BIOS of the computer is password-protected, go [here](#) and look for the software solution

Now boot the computer, and when you got the motherboard message, press a key for enter in the BIOS or in the boot-order menu (the key you have to press is different on a lot of motherboards, but it's generally DEL or F2, it's will be displayed on the screen)

Change the boot order and move the DVD to the first position.

Now normally boot the computer and ophcrack will started, in 95% of case, it will find the admin password of the computer.

If not, go to the 3rd method

3rd method :

Ophcrack didn't find the admin password? It's not a problem ?

Just boot on a linux live CD (i highly suggest Backtrack 4 for the following of the tutorial) the live CD can be found [HERE](#)

Just start on the CD, and wait for the command prompt appears

now type in :

Code fdisk -l and search for the windows partition, basicaly the biggest

We will say that the partition is called "dev/sda2" (It can be different on your computer!!!)

now type :

Code mkdir /mnt/xp

mount /dev/sda2 /mnt/xp

cd /mnt/xp

Now you are in the root of your windows partition, without any restrictions

just type :

Code cd WINDOWS/system32 and remove sethc.exe

Code rm sethc.exe and copy cmd.exe with the name "sethc.exe"

Code cp cmd.exe sethc.exe

and you're done.

Just reboot the computer and on the winlogon screen, just hit SHIFT key five times and the cmd prompt will appears.

Now just follow the 1st method and you can access to an admin account.

Gain Network Admin Privileges

Ok this must be the hardest part, but you can do it ?

So you need to know how is built your school network, it's not a problem, just go, with local admin account, to start>network or go to the control pannel and look at all the computers in the network. You'll certainly find a lot of computers, search for a computer called "server" or with a name different to others

In my school, the server is called "server1"

try to click on it, it will certainly ask you for username and pass, you can give the pass of your limited account, and you'll certainly access only to the "normal" files that you can acces in normal time when you connect to the network.

So, you need admin passwords, you can succesfully do it easily ?

1st method :

If you can access to a computer that is used by admins or teachers, just unistall the AV on the computer (easily done in control panel) and install this great tool, fakegina ?
downloadable [here](#)

Just move fakegina.dll into C:\WINDOWS\system32
and now press windows + R
type in : "regedit"

go to : "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
and create "GinaDLL" in "REG_SZ" with value "fakegina.dll"

OK you're done, just wait for someone connect to the computer, and the usernames and passwords of the users will be stored in "C:\WINDOWS\system32\passlist.txt"
wait for an admin connect to the machine, and voila, you got his pass.

passlist exemple :

Spoiler ([Click to View](#))

[img]http://s2.noelshack.com/uploads/images/20533773997242_fakegina.jpg[/img]
in the format domainname\username password

2nd method :

No privileged users are connecting on the computer, it's not a problem, just intercept the packets send by the users to connect to the server.

Just download and install [Cain & Abel](#)

Now just google for ARP Poisonning and sniff SMB packets, it contains the login informations of the user connecting, just decrypt it with cain and you're done.

You just have to wait an admin to connect on the network

3rd method :

Ok it's not really a skilled method, but it works well.

Just try to watch an admin or a teacher connecting to the network, try to see what is the password typed.

If it's only numbers, it can be a birthday date or something else

Social Engineering is also a good way to go.

Gain Full Access To The Main Server

Okay, once you've got an admin password, you'll want to have a fully access to the main server.

1st method :

Normally, the administrators are using remote desktop for having access to the main server.

Just try to connect to it : Start > accesories > remote desktop connection

And then,type in the box the name of the main server, in my school, it's "server1"

If you got access to an windows login screen, it's good!

Just try type the admin username and pass.

If it works, you're done, welcome to the main server of your school, you can do what you want ?

2nd method :

If it doesn't work, the server only got one account that can access to the server interactively, generally called "administrator"

So just try to find the password, maybe the same as the admin user.

If you don't find the password, use Cain & Abel and sniff for RDP packets.

These packets are used when someone uses the remote desktop to connect to the server, and they contain the username and the password of the admin user that can access to the main server with remote desktop.

If you successfully find packets, great, just open it and search for the password

And when you got it, just connect to the main server, and you're done ?

3rd method :

If you don't find any packet while sniffing, you can pentest the server.

Just use a backtrack live CD, use metasploit and autopwn the server (there are a lot of tutorials on hackforums and all over the internet), there are a lot of chances that the server isn't updated, so enjoy and try to find any vulns to the server

If metasploit successfully finds a vuln, you're done, and you'll have access to a shell, ENJOY

What To Do With The Main Server

A lot of things...

But the first thing to do is to dump the hashes of the server, google for fgdump and use it to dump the hashes of the server.

Now crack them with Ophcrack and you'll gain the password of all the accounts of your school, enjoy

Now you got all the powers, I recommend you to not do "funny" things and don't leave any tracks, don't touch all the accounts, just access to the teacher's files (some of them store their tests in their account folder) just enjoy and increase your grades ?

Do it silently and all will be fine
tested and approved by me..

Thanks for reading ?
(sorry for my bad english, I'm French)

Recitile - January 8, 2011, 1:31 pm

Nice tutorial but I am happy that there's like NO Security at our school Hah.

Jacques Chirac - January 8, 2011, 1:39 pm

thx ? , in my school I have a paranoid (but inefficient) network admin and the computers are very secured.

It's for help peoples having problems to gain full access of their school's network that I wrote this tutorial ?

Sonic Boom - January 8, 2011, 1:41 pm

If this is your first tut, it's awesome and useful.

Keeter - January 8, 2011, 1:43 pm

I found this useful, the whole cmd replacement thing in particular I haven't seen before. Will definitely use this!

wisd0m - January 8, 2011, 1:44 pm

Quite detailed tutorial, hopefully it's legitly written by you.

If it is, Props.

Mr. 9 - January 8, 2011, 1:44 pm

Wow very detailed great contribution :)

Jacques Chirac - January 8, 2011, 1:46 pm

(Jan 8, 2011 02:41 PM)aggouras Wrote: [\[CITE\]](#) If this is your first tut, it's awesome and useful.

Yeah it's my first tut

I've gained a full access to my school's network 2 month ago, and I waste a month trying to get the full access, I've only found few tutorials only working when the school security is very low, so I decided to make a tut working for all schools (or maybe 99%) based on my personal experience ?

pushl %ebp - January 8, 2011, 1:48 pm

Wow, I opened this and was prepared to flame and tell you not to post shit that's been posted 1million times. This was a really good tutorial. Thank you. I warn people though, if you get caught, you will end up suspended and possible police action. ?

Jacques Chirac - January 8, 2011, 1:49 pm

(Jan 8, 2011 02:44 PM)wisd0m Wrote: [\[CITE\]](#) Quite detailed tutorial, hopefully it's legitly written by you.

If it is, Props.

Yeah I just wrote it now, i've just wrote how i gain full access to my school network, I hope I will help some people here ?

(Jan 8, 2011 02:48 PM)C!RCU!T tr0jAn Wrote: [\[CITE\]](#) Wow, I opened this and was prepared to flame and tell you not to post shit that's been posted 1million times. This was a really good tutorial. Thank you. I warn people though, if you get caught, you will end up suspended and possible police action. ?

I agree, don't do that if you're sure to not get caught, you must be silent when you do this, try to never let some personnels ID when you're doing this.

Personnaly, on the computer's room, i've nerver log in my account and i've never written my name on the paper you must fill for enter in the room

(I used to use "Charles Baudelaire" or "Serge Gainsbourg" as nickname ?)

Tate's Daughter - January 8, 2011, 1:54 pm

i already have access to my school network. Our it department are dumbshits so i told them i could help them. I did but i also helped myself

Fuzzyhacker - January 8, 2011, 3:01 pm

I was skeptical at first when I saw the title and then saw that the first method was adding an account to the admin usesgroup... Because that's what you get 1/10 times you click on a thread titled something like "Hack your schools network". I have to give it to you though. After i read the entire tutorial I was impressed and am now going to be attempting this. I could definitely use a good look at my midterms. But what the hell is a MAJ key bro. Can't find anything that remotely looks like MAJ

key. Where is this rumored MAJ key located on a keyboard?

Rainbow Dash - January 8, 2011, 3:07 pm

I looked at the title and thought it was going to be the same stuff which I've tried dozens of times before, but I found a whole new range of methods to aid my way to admin on my school network. Well done! Very good Tut. :)

Jacques Chirac - January 8, 2011, 3:12 pm

(Jan 8, 2011 04:01 PM)Fuzzyhacker Wrote: [\[CITE\]](#) I was skeptical at first when I saw the title and then saw that the first method was adding an account to the admin usesgroup... Because that's what you get 1/10 times you click on a thread titled something like "Hack your schools network". I have to give it to you though. After i read the entire tutorial I was impressed and am now going to be attempting this. I could definitely use a good look at my midterms. But what the hell is a MAJ key bro. Can't find anything that remotely looks like MAJ key. Where is this rumored MAJ key located on a keyboard?

Thanks ?

Really sorry, the "MAJ" key is shift key ? in France, we usually say "MAJ" instead of "shift" I'll correct it ?

Do0ks - January 8, 2011, 6:10 pm

Great tutorial man, I wish i knew this shit when i was in school. I know nothing was blocked. I just didn't know my thumb from my ass when it came to computers back then.

chrome24 - January 8, 2011, 6:13 pm

I wish I knew hackforums before I left high school.

?4???4?™ - January 8, 2011, 7:02 pm

wow... nica tutor..

btw, i dont see my school has a server.. hehe..

em,how can i hack the pc if it on a room that student cant go inside?

bernardbear - January 8, 2011, 7:12 pm

my school network admin using redhat . .idk about linux

KaptaiN - January 8, 2011, 7:14 pm

There are some methods I had never thought of doing, well done ?

envenomed - January 8, 2011, 9:17 pm

Nice, definitely going to try a few of these out when I get back to school Monday.

iDuL - January 8, 2011, 9:54 pm

Good tutorial man, keep it up.

Jacques Chirac - January 9, 2011, 1:44 am

(Jan 8, 2011 08:02 PM)d4rk_m4n Wrote: [\[CITE\]](#) wow... nica tutor..

btw, i dont see my school has a server.. hehe..

em,how can i hack the pc if it on a room that student cant go inside?

You can use ARP poisoning for do a man-in-the-middle attack and infect the computer, after that you can have a shell access and grab passwords using fakegina, or you can keylog the computer...

You also can try metasploit the computer, because there are chances that it is not updated ?

(Jan 8, 2011 08:12 PM)bernardbear Wrote: [\[CITE\]](#) my school network admin using redhat . .idk about linux

For a linux server, you don't have remote desktop, but you can metasploit it, and there are chances you can get a shell on it...

But in my school, the server is a Windows 2000 server, so I haven't tested this with linux...

be smart, test everything you can, and you'll certainly find a way to gain admin access to the server ?

NeoXx™ - January 9, 2011, 2:53 am

The best school hacking TuT on HF! Thanks! :D

Developer - January 9, 2011, 3:01 am

I got to say man, this is the best tutorial I have seen for hacking school networks. Very detailed and explained quite well.

5 stars +3rep

TheWord - January 9, 2011, 3:13 am

haha, ill be trying some of these

?4???4?™ - January 9, 2011, 3:14 am

(Jan 9, 2011 02:44 AM)clmnt47 Wrote: [\[CITE\]](#) You can use ARP poisoning for do a man-in-the-middle attack and infect the computer, after that you can have a shell access and grab passwords using fakegina, or you can keylog the computer...

You also can try metasploit the computer, because there are chances that it is not updated ?wow.. thx man for reply...

any tutor about that..

btw,what do u mean with man-in-the-middle attack?

i need someone that can access that pc?

?

Jacques Chirac - January 9, 2011, 3:29 am

(Jan 9, 2011 04:14 AM)d4rk_m4n Wrote: [\[CITE\]](#) wow.. thx man for reply...

any tutor about that..

btw,what do u mean with man-in-the-middle attack?

i need someone that can access that pc?

?

With a man-in-the-middle attack, you'll be able to sniff all the traffic from the computer to the school server.

If you want to get into the computer, and if you don't have any access to it, just use this and use dns spoofing for infect the computer, look at this tutorial for DNS spoofing, it can help you :

<https://hackforums.net/showthread.php?tid=152687>

and a tutorial for man-in-the-middle attack : <https://hackforums.net/showthread.php?tid=695677>

All you need is the IP adress of the computer in the network and the IP adress of the server, it's not a problem, just find their names in start>network and ping them for find their IP

These tuts are for Linux but you can use cain & abel for do it on windows ?

lala123 - January 9, 2011, 3:30 am

lol thats great. thanks dude!

?4???4?™ - January 9, 2011, 7:59 am

(Jan 9, 2011 04:29 AM)clmnt47 Wrote: [\[CITE\]](#) With a man-in-the-middle attack, you'll be able to sniff all the traffic from the computer to the school server.

If you want to get into the computer, and if you don't have any access to it, just use this and use dns spoofing for infect the computer, look at this tutorial for DNS spoofing, it can help you :

<https://hackforums.net/showthread.php?tid=152687>

and a tutorial for man-in-the-middle attack : <https://hackforums.net/showthread.php?tid=695677>

All you need is the IP adress of the computer in the network and the IP adress of the server, it's not a problem, just find their names in start>network and ping them for find their IP

These tuts are for Linux but you can use cain & abel for do it on windows ?thx man!!?
i will try this,but i have some question that make me confuse...

1. the Server school mean wireless/internet that the school's pc use?
2. may i do this if i just boot bt4 from my pendrive but dont install it?
3. may i have ur msn? =)

sorry for noob question,
im really want to learn..?

Jacques Chirac - January 9, 2011, 8:09 am

(Jan 9, 2011 08:59 AM)d4rk_m4n Wrote: [\[CITE\]](#) thx man!!?

i will try this,but i have some question that make me confuse...

1. the Server school mean wireless/internet that the school's pc use?
2. may i do this if i just boot bt4 from my pendrive but dont install it?
3. may i have ur msn? =)

sorry for noob question,
im really want to learn..?

1- The server is the machine where all the computers are connecting when they want to connect to the network, not necessary wireless, in my school, all the computers have ethernet cables for connect.

2- Sure, don't install backtrack on your school's computer, or you will spotted ? just boot on the live cd

3- Sorry but i don't MSN supports for some reasons i'll not explain here... Anyway you can PM me if you want ?

jurre1990 - January 9, 2011, 8:16 am

Nice tut,

1 Qetion, is there a way to use a USB instead of a CD, Becouse the bios is protected @ our school. but i know the boot order: First USB and then HDD.

So can i use a USB?

?4???4?™ - January 9, 2011, 8:25 am

(Jan 9, 2011 09:09 AM)clmnt47 Wrote: [\[CITE\]](#) 1- The server is the machine where all the computers are connecting when they want to connect to the network, not necessary wireless, in my school, all the computers have ethernet cables for connect.

2- Sure, don't install backtrack on your school's computer, or you will spotted ? just boot on the live cd

3- Sorry but i don't MSN supports for some reasons i'll not explain here... Anyway you can PM me if you want ?ow..

1. so if my school pc is using wireless to connect to network, i should get the modem/router ip?

2. ok.. =)

3. ok.. =)

(.)(.) Pï@T€ (.)(.) - January 9, 2011, 8:31 am

good tut only issue is igf a admin looks in the user accounts they will see your newly added account so you might wanna not make it your name mybe something like "New user"

also this dont have to be done at school here is some american places this can be done

School

Library

Mcdonalds most have a pc bolted to a table somewhere

Mybe even Starbucks

Your Local University or trade school

Jacques Chirac - January 9, 2011, 8:41 am

(Jan 9, 2011 09:16 AM)jurre1990 Wrote: [\[CITE\]](#) Nice tut,

1 Qetion, is there a way to use a USB instead of a CD, Becouse the bios is protected @ our school. but i know the boot order: First USB and then HDD.

So can i use a USB?

Sure you can boot on a USB drive, just go [here](#)

(Jan 9, 2011 09:25 AM)d4rk_m4n Wrote: [\[CITE\]](#) ow..

1. so if my school pc is using wireless to connect to network, i should get the modem/router ip?

2. ok.. =)

3. ok.. =)

Probably, but there are multiples ways to make a school network, so you have to search how the network is built, and after that you'll know where the computers are connecting and what you can do with ?

D(A)(R)K R??\$O?™ - January 9, 2011, 11:50 am

I found this useful good tutorial. ;)

Nort - January 9, 2011, 12:45 pm

Great Tutorial
thanks for the share

Vires - January 9, 2011, 1:20 pm

i am new to all this "hacking" thing, and i want to know if i can do anything (bad) to their network..
infiltrate it:P
if i have their IP adress?
(Revenge on my teachers :P)

andreinescastro - January 9, 2011, 1:27 pm

Thanks a lot my friend!
I had problems in booting ophcrack, because the boot option was blocked!

Fredr1k™ - January 9, 2011, 1:30 pm

merci beaucoup ?

Nice tut ?

?4???4?™ - January 10, 2011, 2:19 am

thx man..
i will try this soon after i get my server FUD.. =)

Trickz4U - January 10, 2011, 2:22 am

good way to get in a world of hurt

Nadleeh - January 10, 2011, 2:31 am

thanks for the info hope this work

new hacker - January 10, 2011, 4:32 am

WOW GREAT I WILL BE TEST IT TOMOROW

SIM-570417 - January 10, 2011, 9:11 am

Nice tut
didn't read all but is great
there are and some other tools for finding or bypassing admin pass but etc...

Noobsweeper - January 10, 2011, 10:12 am

Is the password part possible with cmd? :D

From the PC you created the acc too...

Noobsweeper - January 10, 2011, 11:34 am

Nice, shame is that our school sucks. i wonder if you get the admin priviledged account, can you get onto the account and shut down PCs cuz our teacher has a program for even controlling the mouse xD. Password part i dislike :[

AFRO - January 10, 2011, 12:32 pm

Thanks man! To bad my school has really good security and monitoring. I wonder if you can disable all monitoring without the computer notifying the network dudes.

asad1912 - March 23, 2011, 1:12 pm

kudos to you brother..

clap clap

watch out system admin....cuz here i come...with Gainsbourg's instructions :P :P

?Sean - March 23, 2011, 1:14 pm

Looks good but I can't access CMD from my school?

jtjoe33 - March 23, 2011, 7:21 pm

I love this tutorial! i bookmarked it and will post back with my results the second I try it!

Jacques Chirac - March 24, 2011, 9:37 am

(Mar 23, 2011 01:14 PM)deadlysh0tz Wrote: [\[CITE\]](#) Looks good but I can't access CMD from my school?

Gain local admin access, and you'll have access to the CMD, just look at my tutorial

aliengamers - April 16, 2011, 9:38 am

awesome dude keep those "hacks" upppo D:D:D::D

Vexna - April 16, 2011, 3:53 pm

Great tutorial, thank's for sharing!

Cyber-Security - April 16, 2011, 5:11 pm

This has been posted a million times but this is the most detailed one so far.

Great job :D

Fetus - April 16, 2011, 5:20 pm

My school is way too secure for this.

I have access to the local machine admin but the server we use goes by computer names and if any changes happen it drops you haha

creed0113 - April 16, 2011, 7:28 pm

yes i was wondering if you can help me, if you could help me i would greatly be thankful. im trying to make this USB invisible to a school computer and the USB can also, when you plug it in it'll auto run a program. what i meant about making the USB invisible is it wont be seen when checking on the computer except when you press a certain code EX. ctrl+shift+f

Acidious - April 16, 2011, 7:45 pm

(Jan 8, 2011 02:24 PM)Gainsbourg Wrote: [\[CITE\]](#) Hello world ?

So, a lot of people here should want to hack his school's network.

It can be really easy, and it can be quite difficult if your scholl have actives network administrators.

Anyway, you can do it following my tutorial, there are a lot of possibilities but I will explain the most efficients methods here...

So, Let's started !

Gain local admin privileges

It's very easy to gain admin privileges.

1st method :

(cmd not blocked)

How to open CMD?

-Press Windows+R ==> type "cmd.exe" in the box
or

-create a new text file, just write it inside :

Code @echo off

command

pause and save it as "something.bat"

just click on it.

In cmd, type :

Code net user *nameyouwantfortheaccountthere* /add

(dont write the stars)

and now type :

Code net localgroup Administrators *nameoftheaccount* /add

note :

For non-english computers, the group "Administrators" could not be the same, on french computers, it's called "Administrateurs", so for check what is the name of the group, just type "net localgroup" for see the list of groups on the computer

Now you can connect yourself on the local machine with an admin account

2nd method :

Just burn ophcrack on a dvd

ophcrack can be found here :

<http://ophcrack.sourceforge.net/download.php?type=livecd>

If the BIOS of the computer is password-protected, go [here](#) and look for the software solution

Now boot the computer, and when you got the motherboard message, press a key for enter in the BIOS or in the boot-order menu (the key you have to press is different on a lot of motherboards, but it's generally DEL or F2, it's will be displayed on the screen)

Change the boot order and move the DVD to the first position.

Now normally boot the computer and ophcrack will started, in 95% of case, it will find the admin password of the computer.

If not, go to the 3rd method

3rd method :

Ophcrack didn't find the admin password? It's not a problem ?

Just boot on a linux live CD (i highly suggest Backtrack 4 for the following of the tutorial)
the live CD can be found [HERE](#)

Just start on the CD, and wait for the command prompt appears
now type in :

Code fdisk -l and search for the windows partition, basically the biggest
We will say that the partition is called "dev/sda2" (It can be different on your computer!!!)
now type :

```
Code mkdir /mnt/xp  
mount /dev/sda2 /mnt/xp  
cd /mnt/xp
```

Now you are in the root of your windows partition, without any restrictions
just type :

```
Code cd WINDOWS\system32 and remove sethc.exe  
Code rm sethc.exe and copy cmd.exe with the name "sethc.exe"  
Code cp cmd.exe sethc.exe  
and you're done.
```

Just reboot the computer and on the winlogon screen, just hit SHIFT key five times and the cmd prompt will appear.

Now just follow the 1st method and you can access to an admin account.

Gain Network Admin Privileges

Ok this must be the hardest part, but you can do it ?

So you need to know how is built your school network, it's not a problem, just go, with local admin account, to start > network or go to the control panel and look at all the computers in the network. You'll certainly find a lot of computers, search for a computer called "server" or with a name different to others

In my school, the server is called "server1"

try to click on it, it will certainly ask you for username and pass, you can give the pass of your limited account, and you'll certainly access only to the "normal" files that you can access in normal time when you connect to the network.

So, you need admin passwords, you can successfully do it easily ?

1st method :

If you can access to a computer that is used by admins or teachers, just uninstall the AV on the computer (easily done in control panel) and install this great tool, fakegina ?
downloadable [here](#)

Just move fakegina.dll into C:\WINDOWS\system32
and now press windows + R
type in : "regedit"

go to : "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"
and create "GinaDLL" in "REG_SZ" with value "fakegina.dll"

OK you're done, just wait for someone connect to the computer, and the usernames and passwords of the users will be stored in "C:\WINDOWS\system32\passlist.txt"
wait for an admin connect to the machine, and voila, you got his pass.

passlist exemple :

Spoiler ([Click to View](#))

[img]http://s2.noelshack.com/uploads/images/20533773997242_fakegina.jpg[/img]

in the format domainname\username password

2nd method :

No privileged users are connecting on the computer, it's not a problem, just intercept the packets send by the users to connect to the server.

Just download and install [Cain & Abel](#)

Now just google for ARP Poisonning and sniff SMB packets, it contains the login informations of the user connecting, just decrypt it with cain and you're done.

You just have to wait an admin to connect on the network

3rd method :

Ok it's not really a skilled method, but it works well.

Just try to watch an admin or a teacher connecting to the network, try to see what is the password typed.

If it's only numbers, it can be a birthday date or something else

Social Engineering is also a good way to go.

Gain Full Access To The Main Server

Okay, once you've got an admin password, you'll want to have a fully access to the main server.

1st method :

Normally, the administrators are using remote desktop for having access to the main server.

Just try to connect to it : Start > accesories > remote desktop connection

And then,type in the box the name of the main server, in my school, it's "server1"

If you got access to an windows login screen, it's good!

Just try type the admin username and pass.

If it works, you're done, welcome to the main server of your school, you can do what you want ?

2nd method :

If it doesn't work, the server only got one account that can access to the server interactively, generally called "administrator"

So just try to find the password, maybe the same as the admin user.

if you don't find the password, use Cain & Abel and sniff for RDP packets.

This packets are used when someone use the remote desktop for connect to the server, and they contains the username and the pass of the admin user that can access to the main server with remote desktop.

If you successfully find packets, great, just open it and search for the password

And when you got it, just connect to the main server, and you're done ?

3rd method :

If you don't find any packet while sniffing, you can pentest the server.

Just use a backtrack live CD, use metasploit and autopwn the server (there are a lot of tutorials on hackforums and all over the internet), there are a lot of chances that the server isn't updated, so enjoy and try to find any vulns to the server

If metasploit successfully find a vuln, you're done, and you'll access to a shell, ENJOY

What To Do With The Main Server

A lot of things...

But the first thing to do is to dump the hash of the server, google for fgdump and use it to dump the hashes of the server.

Now crack them with Ophcrack and you'll gain the password of all the accounts of your school, enjoy

Now you got all the powers, I recommend you to not do "funny" things and don't let any tracks, don't touch at the accounts, just access to the teacher's files (some of them store their test in their account folder) just enjoy and increase your grades ?

Do it silently and all will be fine
tested and approved by me..

Thanks for reading ?

(sorry for my bad english, I'm French)

lol seems like an amazing tutorial, tried it at my school but since they are Department of Defense school i totally got caught and they were like who taught you to do this, i was like no one i was goofin around lol i got kicked out lol

n3ms1. - April 17, 2011, 3:19 am

Very, very nice tutorial bro... ?

And I have one question. If school server security is not on so high level, and if i breach it successfully. Can someone see from which computer on network I was working?

Sorry for bad English if there were mistakes. ?

Jacques Chirac - April 17, 2011, 3:30 am

(Apr 17, 2011 03:19 AM)n3ms1. Wrote: [\[CITE\]](#) Very, very nice tutorial bro... ?

And I have one question. If school server security is not on so high level, and if i breach it successfully. Can someone see from which computer on network I was working?

Sorry for bad English if there were mistakes. ?

The better way is to use a computer that can be used by a lot of people, and you must using a local admin account. With this, if they find what computer is used, they will not find you.

Personnaly, i used a computer in the school library. I used Ophcrack to find the local admin password. I get into this account and I uninstalled the AV. Then I installed fakegina and a keylogger. I stole nearly 200 facebook accounts and 500 session passwords. I looked around the network and I found the server. I made a metasploit autopwn, but it was inconclusive. So I performed an Acunetix scan and I found some vuln. I had the possibility of send command with SYSTEM privileges.

So I used a fgdump program and I dumped all the passwords stored on the server (2000 accounts)
So I get full admin access on RDP to the server

Hope that helped someone ?

x-iPleasure - April 17, 2011, 4:58 am

LOL! Imma do this and delete accounts XD!!

(Apr 16, 2011 07:45 PM)1UP Mushroom Wrote: [\[CITE\]](#) lol seems like an amazing tutorial, tried it at my school but since they are Department of Defense school i totally got caught and they were like

who taught you to do this, i was like no one i was goofin around lol i got kicked out lol
That sucks bro.. I feel bad for you, now I'm scared to do it at my school lol..

Asa Butterfield - April 27, 2011, 3:28 pm

for the replacing sticky keys with cmd bit you should use a recovery disk on a usb with the code saved to it then opne it up in cmd then restart pc then done then u dont have to mess about loading backtrack which can be evidently seen because its differnt to windows load up so u are most likely to get caught but, Very good tutorial i have been looking for something like this for a week thanks

polarbear - April 28, 2011, 6:38 am

message me. i have a few funny stories about my school and their network.

'Snorlax - April 28, 2011, 6:46 am

I've seen these kind of threads 100 of times.
But cool, I guess..?

shadowline.ifr - April 28, 2011, 8:49 pm

This may come in handy. Cool stuff man!

tekniko - April 29, 2011, 12:36 am

I did this 9 years ago in Grade 12 and let me tell one bit of advice. Dont tell anyone!! Dont brag to your friends, your dog, no one! Word gets around! I was busted and banned from the computers for 6 months. Luckily it wasn't for changing my grades. Punishment might of been a lot worse.

One last thing when changing grades. Don't go crazy and give your self straight A's. Especially if you are an idiot/slacker. Instead add 2-3% on each project and your over all mark will increase 2-3%. Again dont tell anyone! I got offers from several people to change their grades for 20 to 100 dollars. That's attention you don't want.

MahmoodHB - April 29, 2011, 1:18 am

Damn! Bookmarked This ?
Thanks alot ?

theleperchaun76 - April 30, 2011, 10:39 pm

very nice tut easy to understand i believe i just read your tut on hacking a teachers pc. Good info simple but very good. I think you deserve a plus on your rep.

N3me\$!s - April 30, 2011, 11:41 pm

Wow very detailed great contribution :)

The Dane - May 4, 2011, 2:26 am

Epic tut homie, thanks alot :D

KongenT - May 4, 2011, 1:25 pm

nice!
Spoiler ([Click to View](#))too Short Message!!

Miyata - May 4, 2011, 3:30 pm

Omg thats awesome. Going to try it out tomorrow. Just wanted to ask, if im going to download ophcrack for vista is it going to work for windows 7? Because there is no version for w7. Most of computers in our school are using w7. Thanks.

Derky - May 4, 2011, 8:08 pm

I will definitely be trying this someday :)

Thanks for the great tutorial, I read it all the way through without any hiccups.

Cat Daddy - May 4, 2011, 9:13 pm

Access is denied when I used the CMD command):

Peelsaven - May 4, 2011, 9:19 pm

yeah your not even allowed to go to command prompt at my school so I am guessing that this probably will not work

iReFLeXeZz - May 5, 2011, 12:44 am

Nice tut, ill try it out soon

noober1001 - May 5, 2011, 1:39 am

Hey, this is the best tut I have ever seen.

Thank you so much for that.

BTW I used metasploit to gain access to my school server. And I did so many funny things, but they don't know still, what's happening in their computer. LOL.

lamaninja3012 - May 5, 2011, 6:25 am

wow i just knew that we can use ophcrack for that:D

-coded32 - May 5, 2011, 7:00 am

This is a superb tut i have evr seen !!

lee74saurusr3x - May 5, 2011, 3:35 pm

A few weeks ago, a couple kids from my school actually hacked the network and the computer teacher like sprinted into the room, pointed at the kids and yelled "HANDS UP!!!!" and everyone like stood still and the kids put their hands up. They only got one week computer suspensions lol. Something tells me my school's network is pretty secure... :/

RussianFederation - May 5, 2011, 3:36 pm

Good tut. Deep Thanks. Thankyou.

sped55 - May 5, 2011, 5:10 pm

very nice, i may try this some time

AC130 - May 5, 2011, 5:57 pm

holy leechers XD 3,991 views and 80 post nice tut dude ima try it

holy leechers XD 3,991 views and 80 post nice tut dude ima try it

Nullusia - May 5, 2011, 6:14 pm

Detailed guide, nice tutorial, a lot of effort spent. ^^

Mr Royal - May 5, 2011, 6:59 pm

You could also open CMD by opening "NotePad" and typing "Command >Enter< Command.com" and saving as a batch file, if I remember. Use to do this all the time, until I moved schools >.< Nice guide though keep it up.(:

pwnedbycancer - May 5, 2011, 7:22 pm

Nice tutorial, I can't wait to see if this works.

Developer - May 21, 2011, 3:59 am

I'll bring this thread back alive as it deserves to be read by many others and it will slow down the same questions asked everyday about hacking their schools.

Shad0w_St3p - May 21, 2011, 4:03 am

Love the tut mate, +rep :D

Turtle - May 21, 2011, 4:09 am

Thanks im gunna use this the tutorial at school

toto422 - May 21, 2011, 2:20 pm

Merci beaucoup, je pense m'en servir aussi :p

PrO1337HaCKeR - May 21, 2011, 3:11 pm

the third method i found out about a year ago when hacking my schools comps. Never got to the point where I made a tut.. Meh, ima go make one soon..

i hav ubuntu on my usb at all times

oh ya, btw tht method will only work for that specific comp u hacked into and it's not tht hard to net user /all and see what acc is there lol

oh ya, btw if run is blocked, make a shortcut to cmd. if cmd is blocked, use command.com

Darktheif - May 21, 2011, 11:25 pm

question is this trackable?...

Like if i do it on a certain computer will they know which 1?
(for the local admin)

joe5181 - January 28, 2012, 12:24 pm

Thank you for this Tut- It really finalized my ideas on what i was going to do to my school's network
^_^

It's also very well written, and I cant thank you enough for that.

cookiedan - January 29, 2012, 7:20 pm

Great post!

Goes into great detail!!

Thanks for sharing!

Nepal Cyber Army - January 29, 2012, 9:09 pm

wow great tutorial..

and very usefull

AcerMac - March 31, 2012, 5:49 am

Okey.. question.. can't make new user or use localgroup command, what should I do now? I can get into C:/ and C:/Windows on cmd but can't get anywhere else cus cmd at my school disables path command.. Well.. It says something about this mark : / . Is there anyother ways to get into system32 directory? Can't open cmd from there and can't copy anything to there. Please help. Ty

Oh and.. nice tutorial :p

WolfbladeM - March 31, 2012, 8:09 am

Good tutorial, and quite useful as well. thanks

GeneralStarshade - March 31, 2012, 10:55 am

One of the best tutorials here on HF. Absolutely genius. Wonderful. Amazing. Keep up the good work!!!!

ii_SNiPEzZ_xX - March 31, 2012, 11:59 am

CMD is blocked at my school... but i can open it with a notepad file saved as a .bat, But be cause its blocked i cant use most stuff like adding accounts and giving admin permissions. Also i cant open the CD drive at my school. Is there any other ways to get admin rights?

Sensibility - March 31, 2012, 12:23 pm

Wow very detailed great contribution :)

I zodiac - March 31, 2012, 12:24 pm

haha surely going to try this one out, thanks mate

HoundPup - March 31, 2012, 12:41 pm

This tutorial is... amazing...

You, my good friend, deserve a reward.

French, you say? Thats cool, im learning that as a second language

mike2320 - March 31, 2012, 5:27 pm

Very nice tutorial. I wish I had read this when I was still in high school.

Germans - March 31, 2012, 6:13 pm

CMD, notepad, etc. are unlocked but when I try things like making batch files to make admin accounts I get error five access denied messages... ?

Callisto89 - March 31, 2012, 6:20 pm

for the first method of gething Admin power
when i write: net user TheNameIWant /add
it said Access denied on my own PC !

vywus - March 31, 2012, 6:50 pm

Hmm really nice tut indeed.

Okay so when I'm on a school computer I have to enter my id and pass (teacher have too)
And there are people everywhere watching you.

Do you think RAtIng a school computer, then lock it, and use all your methods to get password..
would be a good idea ?

Also, what can they log ? Can they see you used a USB and launched something that was on it and know what account did it ?

Huskar - March 31, 2012, 11:00 pm

Nice TUT Bro

i really appreciate it! :D

Bill Nye - April 12, 2012, 12:40 am

thank you OP, I have been studying this thread for about 3 hours. I'll talk it into consideration tomorrow when I attempt to gain access and change the balance on my lunch account, and move my classes around.

corvenik - April 12, 2012, 4:32 am

Woow, a tut to hack school network. Seems interesting :)

Fefo111 - April 12, 2012, 6:51 am

Great tut I find the first method really useful for me

sashob - April 14, 2012, 4:53 am

Some nice tutorials in there. Some of them seem really easy to be caught with though, but still good job!

Superior1 - April 14, 2012, 6:25 am

that made my start menu broken.. whenever i open start menu it says "The remote procedure call failed and did not execute." so ima do my restore point. im sure ur method was correct just idk lmao

halo4196 - April 14, 2012, 6:56 am

I want to try this but what if we are caught while doing this?

broski98423 - April 14, 2012, 7:32 am

Great Tutorial
thanks for the share.

Kaskade - April 15, 2012, 6:45 am

Yup, tested on my school's network and it works great =]

h4kr! - April 15, 2012, 7:16 pm

I know the Tech person at my school, but I really don't want to have him be suspicious because i'm staring at his laptop while logging in. :(

teacher once accidentally mentioned the pw was one of her bro/sisters, didn't think to ask which(after time, of course. that would be awkward to do it right after, because then there would be some problems,LOL).

unfortunantly everyone changes their pw regularly and there wasn't another slip. yet :D

sin0c - April 15, 2012, 7:39 pm

good tut

i have access to cmd in my school pc i managed to create new account and put administrator but each time we restart pc it erases everything. and it was like if i did nothing

Ivo Mercy - April 15, 2012, 7:41 pm

more than probably im going to use this, btw thanks for the info?

roxxzor - April 15, 2012, 8:14 pm

Heh, the guy that hacked our school network last became one of the admins :)

cdaddy - April 16, 2012, 3:22 am

Cool guide man really helpful thanks

M31ST3R - May 6, 2012, 5:29 am

Ophcrack only works with Windows XP. I've used it successfully and became even more powerful

then the actual administrator! Just remember not to do too obvious stuff, like changing the admin password!

If you want to use Ophcrack with Vista, 7 or 8 you need to download Rainbow tables which are at least 100GB!

Xray'in - May 6, 2012, 5:47 am

I have to try this one out!

Even tough my dad is like chief of the computer shizzle in the commune or how you should say lol.

?mnipotent - May 6, 2012, 10:58 am

Nice guide although at my school the admin computer can watch everything you doing and is very careful about what people can and can't do.

CodexzZ - July 21, 2012, 5:20 am

Nice post! A friend and I hacked our schools network before, and they invited us over to try again after they applied new security. This will make the haters go mad :)

WR213374u :)

Fossil - July 21, 2012, 6:08 am

Nice tutorial, any efficient method's to gain admin privileges without CMD?

My school has blocked CMD from being used.

Aggie - July 21, 2012, 11:52 am

Thank you so much, this might come in handy next year.

??? - July 21, 2012, 12:39 pm

Is it possible to hack the server through the wireless networks? My school has wireless networks that are unprotected and you can connect to them whenever you want, and it's usable.

Haseo™ - July 21, 2012, 12:55 pm

this is a very nice tut, thank you for taking the time to do this.

H4 The Penguin - July 21, 2012, 1:14 pm

This is a great tutorial except all the computers in my school are macs ?

Mastery - July 21, 2012, 1:16 pm

This is great tut man! Thanks so much for posting!

Ardi22 - October 5, 2012, 11:47 am

looks awesome bro, thanks for the tut :D

Ku?s?h? - October 5, 2012, 11:48 am

Annd what if your school uses Macs instead of PC's?...

Venus23 - October 5, 2012, 12:13 pm

On all schools' computers i've seen there is always a hidden administrator account in the LSA secret.

h4nnibal__67 - October 6, 2012, 4:02 am

Thanks for this nice tutorial :)

I will test it in my school xD

5h1t_warrior - October 6, 2012, 4:54 am

I want to Shut down my schools internet connection any tips how i can do that?

403 - October 6, 2012, 7:47 am

Nice detailed tutorial, but i am already admin on our school computers. ;)

Swixtor32 - October 6, 2012, 8:08 am

Yes, I have been wanting to hack these stupid "Protected" Computers at my school. :)

Sane™ - October 8, 2012, 7:03 am

Great tut, I gained the local admin password be becoming an assistant to the system administrator and he told me it :P i just have to get network admin now xD

BigBang - October 8, 2012, 7:40 am

will the police arrest you for doing these things ?

Raz Riverblade - October 8, 2012, 8:20 am

aand... i'm going to get good grades eyes closed, thanks bud!

(Oct 8, 2012 07:40 AM)BigBang Wrote: [\[CITE\]](#) will the police arrest you for doing these things ?
no but chances are that you'll be kicked out of the school

ntoskrnl.exe - October 8, 2012, 10:44 am

OMG: So nice tutorial...

This user deserves more reputation.

ComplexMist - October 8, 2012, 12:03 pm

Nice im going to have to try this out !

Desktop - October 8, 2012, 12:07 pm

If this is your first tut,it's awesome and useful.

Jacques Chirac - October 8, 2012, 12:46 pm

This tutorial is quite old now... I'm gonna update it soon with more ways to get into your school server.

Some of the techniques here only work on windows XP, so I'll add other ones working on windows server 2008/windows 7.

Euphorical - October 8, 2012, 1:14 pm

Thanks for the tutorial, however when your spending time with ophcrack, it becomes quite suspicious if your at a computer lab (my school is very nazi on computer usage)

un4gettable - October 9, 2012, 10:35 am

thx for the tutorial!

i think i'm gonna try this ;p

?Ñāzg?! - October 9, 2012, 5:08 pm

Wow nice tutorial.

you have a lot of options there, some I never even heard of

Owl City - October 9, 2012, 6:28 pm

This is a great guide; but remind people of the consequences of being caught.

Wú Yifán - October 9, 2012, 7:21 pm

Great tutorial. Back at school soon so going to try this :D

tigerz09 - October 12, 2012, 2:17 am

Nice tutorial! You may wanna edit on how to get admin password. You can get it if you program your USB into resetting passwords at bootup. I'll PM you with the link.

It's been tested and approved by me.

glu3d - October 12, 2012, 2:31 am

Yeah nice tut, deadset worked ! Cheers man

v12dock - October 12, 2012, 2:36 am

As a network administation thanks for posting so I can find ways to block :)

Dark Emperor - October 12, 2012, 6:14 am

hmm thanx man i thought about this a few times ago, but all the tutorials here lacked some info while yours on the other hand are perfect! :D

i found the only pc i can access that is the closest one to the server: the library's pc! :D
i already disabled deep freeze from it so on monday ill go and try your methods :D

The Raccoon - October 13, 2012, 5:25 pm

Very nice ,perhaps its a bit dangerous , Imagine if somebody catch you . lol

Probably. - October 13, 2012, 6:10 pm

This is really, good, just read the whole thing! might try this at my school if I get the chance! Very useful, HQ tut!

Meow Cat - October 14, 2012, 8:44 am

awesome tutorial, i'll be trying this on monday! haha

Haynes - October 14, 2012, 11:58 am

I've tried this almost got caught never trying again

qurfy - October 15, 2012, 6:46 am

Thanks for the sick tut, really appreciate it. I might try it but of course taking the all of the nec. precautions to stay annonymous.

ZeZCo - October 15, 2012, 7:10 am

Nice tutorial, keep up the good work!

winner876 - October 15, 2012, 9:56 am

ahaha will try this when i go back nice tut

Jobi Won - October 15, 2012, 10:50 am

sick! if I wouldn't be too nerdy I would do this..

Sought - October 15, 2012, 11:25 am

Its a good tut, Thanks it could be beneficial for people trying to be annoying =)

xRoyalFlushx - October 15, 2012, 9:01 pm

Thanks for the contribution. I will try this at my school tomorrow.

Bulbasir - October 15, 2012, 10:18 pm

Great tutorial!

Maybe make a less advanced one for low-security school networks?

Hacksalot - October 15, 2012, 10:27 pm

It worked man this rules :/ thnx fot info

The old warrior fan - October 16, 2012, 2:05 am

Damn, i always wanted to do this. Thanks.

Salman Khan - October 16, 2012, 2:26 am

there is a wifi server in our collage as well there is multimedia and other sites are locked.
via this may i unlock it?

Rajat - October 16, 2012, 3:08 am

I found this useful, the whole cmd replacement thing in particular I haven't seen before. Will definity use this!

TheWhiteHattedMan - October 16, 2012, 4:27 am

Any tutorial for a mac? If so please reply as soon as you can.

Darkrai - October 16, 2012, 6:59 am

This will come in handy someday, thanks for the tut OP!

UhMayZinG - October 17, 2012, 5:01 pm

sweet that is cool ill try it out later

-BRUTAL- - October 18, 2012, 1:09 am

Great tutorial :) Only if i could hack SonicWall, then i'd be happy.

Bballdude94 - October 18, 2012, 11:14 am

When I do the cmd net user, it says "System error 5 has occurred, access is denied". What can I do about this?

AuT0 b0T - October 18, 2012, 11:29 am

nice and detailed tutorial thanks. helpful

Illicit - October 18, 2012, 11:57 am

Very nice TUT ;) !

But a few things:

- 1.The backdoor cmd thing with seth.exe does NOT work.
- 2.You can NOT add a user in cmd without admin privilege's.
- 3.How can your school be secure if Regedit is allowed???

wasdylan - October 18, 2012, 12:41 pm

is it possible to RAT on a school computer after gaining admin?

Badside416 - October 18, 2012, 2:40 pm

this is an awesome tut, thanks for the share :)

uz3 - October 20, 2012, 10:44 am

(Oct 18, 2012 11:57 AM)here2hack Wrote: [CITE](#) Very nice TUT ;) !

But a few things:

1.The backdoor cmd thing with seth.exe does NOT work.

2.You can NOT add a user in cmd without admin privilege's.

1. How does seth.exe method not work? Tell us a little more because it worked for me. You just have to know a little bit about navigating folders in Linux.

2. Obviously, but with the seth.exe thing working you would be the computer's SYSTEM user.

Unless they removed all privileges from the account, SYSTEM, then it should work.

-Tip for people doing the seth.exe method-

Navigate to the antivirus program's folder and delete it. Use `rm -rf` (Be careful to select the right folder or you could fuck something up!) This deletes the folder you select (antivirus) on that computer for all users who log on. This makes it very easy to run unFUD servers.

-Optional tip for those who want to rat every account that logs in on the computer-

If it is windows 7 then navigate to `C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup` (ProgramData is a hidden folder)

and place your rat there. It will start up on every account that logs in.

Illicit - October 20, 2012, 11:05 am

Really does seth.exe work?I have tried it many time's on XP's (not through Linux) and It failed. ?

It only worked when I had logged in.

Johnny Cage - October 20, 2012, 11:35 am

Like the method bro keep up the good work this is great

uz3 - October 20, 2012, 12:32 pm

(Oct 20, 2012 11:05 AM)here2hack Wrote: [CITE](#) Really does seth.exe work?I have tried it many time's on XP's (not through Linux) and It failed. ?

It only worked when I had logged in.

It is done through BackTrack which is built on linux. Did you do all of the steps for it?

Quote:Just boot on a linux live CD (i highly suggest Backtrack 4 for the following of the tutorial) the live CD can be found [HERE](#)

Just start on the CD, and wait for the command prompt appears

now type in :

Code:

`fdisk -l`

and search for the windows partition, basicly the biggest

We will say that the partition is called "dev/sda2" (It can be different on your computer!!!)

now type :

Code:

`mkdir /mnt/xp`

`mount /dev/sda2 /mnt/xp`

`cd /mnt/xp`

Now you are in the root of your windows partition, without any restrictions

just type :

Code:

`cd WINDOWS/system32`

and remove sethc.exe

Code:

rm sethc.exe
and copy cmd.exe with the name "sethc.exe"
Code:
cp cmd.exe sethc.exe

and you're done.

Just reboot the computer and on the winlogon screen, just hit SHIFT key five times and the cmd prompt will appear.

Now just follow the 1st method and you can access to an admin account.

Maybe it doesn't work on XP? I'll go try right now and report back.

Edit: 100% works for xp, I'll upload a video soon.

Watch it here

[Video: <http://www.youtube.com/watch?v=CTw4yCUmQgU>]

Illicit - October 21, 2012, 4:44 am

Thanks really appreciate it Ive only ever done through through the XP OS not Backtrack :3
Thanks again ?

S k O r M - October 21, 2012, 7:52 am

SOunds good, I'll try it soon.
Merci mec ;)

Jabberjay - November 30, 2012, 8:20 am

Thanks for the tutorial, hopefully i'll give this a go soon.

BladeZ201 - November 30, 2012, 9:37 pm

Change your grades? (Evil Laugh)! Awesome!

SIM-1648682 - February 4, 2013, 8:46 am

I have tried this today at my school, but i could not get admin acces. When i type in Net user nameofaccountiwant /add

I get user name does not exist ? Any tips on the use of Net user ? I got acces to cmd.exe with backtrack btw by renaming the other .exe in system32 which is awesome!

offsecstudent - February 4, 2013, 12:53 pm

is anybody still interested in helping a brother out? local community college student with admin access to all local computers on our network but still unable to fulfill dreams of controlling the network and finding what servers I can attack. thanks much please pm me if interested in stuff. also interested in mining bitcoin on the computers here

Chris_Racer_24 - February 4, 2013, 4:26 pm

This was a really good tutorial thanks for this I am going to be gaining admin on my school network very soon :P I also like how you covered most eventualities

p.m - February 5, 2013, 5:26 am

nopes, this doesn't work with parental controls enabled

Camaro.ice - February 5, 2013, 9:56 am

thank you dude,great tutorial
tres bon tuto.

I_Cx_I - February 5, 2013, 10:42 am

i dont think this will work on a it school

4RG0S - February 5, 2013, 12:48 pm

Great Tutorial, bookmarked it and keep this Work up !

BugginBrendan - February 5, 2013, 12:57 pm

I tried this method. It allowed me to type in the commands, but once I tried to set up an account to become an admin, it said access denied. Any help?

-Slick- - February 5, 2013, 1:12 pm

My schools computers / networks have little to no security on them. I might try this, but I think it's a bit risky.

anonymous7473 - February 5, 2013, 2:28 pm

This is so old, I've done this a million times and the F.B.I. brought me to jail and I ended up getting raped.

Haseo™ - February 5, 2013, 2:44 pm

This is very useful and helpful thank you for the share! nicely done

MinecraftUser - February 28, 2013, 1:32 pm

This man deserves a medal for making this HQ tutorial.

LuckyLocky - February 28, 2013, 1:48 pm

Wouwaw very detailed great tutorial ! :D

TheRealSlimShady - February 28, 2013, 2:13 pm

This is legit thanks man im going to try this as soon as i go back to school.

MBD_f0rest - March 1, 2013, 6:58 pm

Well im lucky that i don't have any security at my school,i do have the Administrators password and i use it to do all kind of stuff,but i have only one problem i can't get rid of the Lan School Teacher,i tried to delete the file called student.exe but i couldn't do it because it says that i can't delete it (File in use cannot delete the file) i tried to kill it in the Task Mngr and as i kill that process it comes back up again in a matter of seconds (If someone can help me i would be greathfull) ... But im pretty happy that i in the whole school know the Administrator password and also the PW for the WiFi network,so i can connect to it during class and search stuff i need. Awesome thread very helpfull! ? I vouch for you! ?

PatchKillOver - March 1, 2013, 8:37 pm

Wow. Amaizing guide.

Thanks guys

your awesome :3

Cesar Morales - March 1, 2013, 8:41 pm

good tutorial =)... i might end up using this during senior year XD

Lev (???) - March 2, 2013, 10:06 am

I wd just check it out
and post

thank you for the thread

Ch1m4zz - March 10, 2013, 7:06 am

I will try it when i get to school :)

Cavs - March 10, 2013, 7:16 am

Nice tutorial, found our principals tax return and more of our teachers personal files.

Thanks.

rfpd - March 10, 2013, 7:29 am

You will get caught don't do this, stil is nice to know!

flight05 - March 10, 2013, 7:37 am

^^Very nice to know. No reason to be messing with schools though.... stick to gov't

Im gone brah - March 10, 2013, 7:41 am

Nice work, keep it up bro..:)

,regards

-limpa124

https - March 10, 2013, 7:50 am

I couldn't get time to read this but very detailed tut , gj!

bckc - March 10, 2013, 8:04 am

Your methods for getting domain administrator access won't work on most professionally owned networks, fakegina only intercepts passwords physically logging in or UNCing onto the computer, most networks have individual localadmin accounts for UNCing so you'll just get the username and password of the localadmin, cain and abel won't sniff passwords in most business networks because they'll use wired connections and as for looking at a domain administrators password that simply won't work. No place of employment would let a teacher/ordinary worker be a domain administrator and if a domain admin was going to physically log onto a computer other than his own he'd use the localadmin password for that computer.

Bckc

Nmanpure Pkr - March 10, 2013, 12:45 pm

This is a really great tutorial! Bookmarked! I love that if something fails you have a solution for it! Keep up the good work.

Tando - March 10, 2013, 1:47 pm

Nice tutorial, bookmarked it and will look into it.

sLeaks - March 10, 2013, 2:22 pm

nice tutorial add to my favs and going to try it soon.

Qandi - March 10, 2013, 3:18 pm

Ok, about getting network admin priv. ... What if all users are authenticated by a server run by the governement?

peggy23 - March 10, 2013, 7:14 pm

hahah nice tutorial ..i will definitely try this sooner after i graduate so i cant be expelled or something :)

Synraw - March 10, 2013, 8:52 pm

Nice tutorial. At our school they have completely locked up the command line to our accounts, so we've resorted to the old DOS COMMAND.COM . Sad, but it works for us

Rymax99 - March 10, 2013, 9:33 pm

That wouldn't quite work at my school :P

Java only runs on certain sites, BIOS password, pretty much the only things you can run are explorer, and internet explorer, with the exception of a few school installed programs.

Frankly, making a botnet (or even just victims to troll, or other stuff) can be a terrible idea if you don't know what you're doing. First off, a normal student account being administrator? That'd look a bit odd.

Anyway, nice ideas OP.

FakeName69 - March 10, 2013, 10:17 pm

Nice job! Thanks! Very thorough and clear tutorial!

saskemailbox - March 10, 2013, 10:23 pm

Great article. By the way, in some PCs with Oracle SQL server installed, it is difficult to gain Admin status for your account, as it doesn't allow it. Try it out yourself. Otherwise, rest goes smoothly.

Flaming Hot - March 11, 2013, 8:02 am

Nice tutorial thanx for sharing :) :-) ?

Fact - March 11, 2013, 10:21 am

Thanks so much for this! Bookmarked

Nnathan - March 11, 2013, 2:25 pm

Thanks man for the share , i appreciate !

Null Routed - March 29, 2013, 11:20 am

Really great tutorial and it has different solutions to many different scenarios.
Good job :)

counterboy9039 - March 29, 2013, 11:51 am

(Jan 8, 2011 02:24 PM)Jacques Chirac Wrote: [\[CITE\]](#) Hello world ?

So, a lot of people here should want to hack his school's network.

It can be really easy, and it can be quite difficult if your scholl have actives network administrators.

Anyway, you can do it following my tutorial, there are a lot of possibilities but I will explain the most efficients methods here...

So, Let's started !

Gain local admin privileges

It's very easy to gain admin privileges.

1st method :
(cmd not blocked)

How to open CMD?

-Press Windows+R ==> type "cmd.exe" in the box
or
-create a new text file, just write it inside :
Code @echo off
command
pause and save it as "something.bat"
just click on it.

In cmd, type :

Code net user *nameyouwantfortheaccountthere* /add
(dont write the stars)
and now type :

Code net localgroup Administrators *nameoftheaccount* /add
note :

For non-english computers, the group "Administrators" could not be the same, on french computers, it's called "Administrateurs", so for check what is the name of the group, just type "net localgroup" for see the list of groups on the computer

Now you can connect yourself on the local machine with an admin account

2nd method :

Just burn ophcrack on a dvd
ophcrack can be found here :
<http://ophcrack.sourceforge.net/download.php?type=livecd>

If the BIOS of the computer is password-protected, go [here](#) and look for the software solution

Now boot the computer, and when you got the motherboard message, press a key for enter in the BIOS or in the boot-order menu (the key you have to press is different on a lot of motherboards, but it's generally DEL or F2, it's will be displayed on the screen)

Change the boot order and move the DVD to the first position.

Now normally boot the computer and ophcrack will started, in 95% of case, it will find the admin password of the computer.
If not, go to the 3rd method

3rd method :

Ophcrack didn't find the admin password? It's not a problem ?

Just boot on a linux live CD (i highly suggest Backtrack 4 for the following of the tutorial)
the live CD can be found [HERE](#)

Just start on the CD, and wait for the command prompt appears

now type in :

Code fdisk -l and search for the windows partition, basically the biggest

We will say that the partition is called "dev/sda2" (It can be different on your computer!!!)

now type :

Code mkdir /mnt/xp

mount /dev/sda2 /mnt/xp

cd /mnt/xp

Now you are in the root of your windows partition, without any restrictions

just type :

Code cd WINDOWS/system32 and remove sethc.exe

Code rm sethc.exe and copy cmd.exe with the name "sethc.exe"

Code cp cmd.exe sethc.exe

and you're done.

Just reboot the computer and on the winlogon screen, just hit SHIFT key five times and the cmd prompt will appear.

Now just follow the 1st method and you can access to an admin account.

Gain Network Admin Privileges

Ok this must be the hardest part, but you can do it ?

So you need to know how is built your school network, it's not a problem, just go, with local admin account, to start > network or go to the control panel and look at all the computers in the network.

You'll certainly find a lot of computers, search for a computer called "server" or with a name different to others

In my school, the server is called "server1"

try to click on it, it will certainly ask you for username and pass, you can give the pass of your limited account, and you'll certainly access only to the "normal" files that you can access in normal time when you connect to the network.

So, you need admin passwords, you can successfully do it easily ?

1st method :

If you can access to a computer that is used by admins or teachers, just uninstall the AV on the computer (easily done in control panel) and install this great tool, fakegina ?

downloadable [here](#)

Just move fakegina.dll into C:\WINDOWS\system32

and now press windows + R

type in : "regedit"

go to : "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon"

and create "GinaDLL" in "REG_SZ" with value "fakegina.dll"

OK you're done, just wait for someone connect to the computer, and the usernames and passwords of the users will be stored in "C:\WINDOWS\system32\passlist.txt"

wait for an admin connect to the machine, and voila, you got his pass.

passlist exemple :

Spoiler ([Click to View](#))

[img]http://s2.noelshack.com/uploads/images/20533773997242_fakegina.jpg[/img]

in the format domainname\username password

2nd method :

No privileged users are connecting on the computer, it's not a problem, just intercept the packets send by the users to connect to the server.

Just download and install [Cain & Abel](#)

Now just google for ARP Poisonning and sniff SMB packets, it contains the login informations of the user connecting, just decrypt it with cain and you're done.

You just have to wait an admin to connect on the network

3rd method :

Ok it's not really a skilled method, but it works well.

Just try to watch an admin or a teacher connecting to the network, try to see what is the password typed.

If it's only numbers, it can be a birthday date or something else

Social Engineering is also a good way to go.

Gain Full Access To The Main Server

Okay, once you've got an admin password, you'll want to have a fully access to the main server.

1st method :

Normally, the administrators are using remote desktop for having access to the main server.

Just try to connect to it : Start > accesories > remote desktop connection

And then,type in the box the name of the main server, in my school, it's "server1"

If you got access to an windows login screen, it's good!

Just try type the admin username and pass.

If it works, you're done, welcome to the main server of your school, you can do what you want ?

2nd method :

If it doesn't work, the server only got one account that can access to the server interactivly, generally called "administrator"

So just try to find the password, maybe the same as the admin user.

if you don't find the password, use Cain & Abel and sniff for RDP packets.

This packets are used when someone use the remote desktop for connect to the server, and they contains the username and the pass of the admin user that can access to the main server with remote desktop.

If you successfuly find packets, great, just open it and search for the password

And when you got it, just connect to the main server, and you're done ?

3rd method :

If you don't find any packet while sniffing, you can pentest the server.

Just use a backtrack live CD, use metasploit and autopwn the server (there are a lot of tutorials on hackforums and all over the internet), there are a lot of chances that the server isn't updated, so enjoy and try to find any vulns to the server

If metasploit succesfully find a vuln, you're done, and you'll access to a shell, ENJOY

What To Do With The Main Server

A lot of things...

But the first thing to do is to dump the hash of the server, google for fgdump and use it to dump the hashes of the server.

Now crack them with Ophcrack and you'll gain the password of all the accounts of your school, enjoy

Now you got all the powers, I recommend you to not do "funny" things and don't let any tracks, don't touch at the accounts, just access to the teacher's files (some of them store theirs test in their account folder) just enjoy and increase your grades ?

Do it silently and all will be fine
tested and approved by me..

Thanks for reading ?
(sorry for my bad english, I'm French)
worked for me vouch from you :D

Regards..

urzi - March 29, 2013, 2:04 pm

Thanks for the tut, might try it at my school :P

liam1 - March 29, 2013, 2:06 pm

Thanks man, shame i finished school.

mike_nunes - March 29, 2013, 2:43 pm

ahah I wish I knew this back in school. Very detailed, thank you

Niloc - April 2, 2013, 11:34 am

Thanks man! Gonna try it when i'm back at school :3

m0resleep - April 2, 2013, 12:53 pm

Very nice tutorial! Thanks for sharing :)

sakuro - April 16, 2013, 9:48 am

What should the boot disk be like if theres a locked cmd prompt??

Auxil - April 29, 2013, 8:47 pm

Extremely nice tutorial! Love it! I have never seen the CMD method before...Nice job!

ZoC. - April 29, 2013, 9:24 pm

wow nice tutorial.. thanks for sharing.. i will try this ;)

AuJack - April 29, 2013, 11:19 pm

Nice tutorial mate ;)

Helped me out alot :P

iDuL - April 30, 2013, 2:56 am

Great tuts, hope nobody gets caught doing anything!

Remember that there are consequences!!!

Olli - April 30, 2013, 3:44 am

C:\Dokumente und Einstellungen\schueler>net user test12345 /add
Systemfehler 5 aufgetreten.

Zugriff verweigert

fasipai - April 30, 2013, 4:15 am

(Jan 8, 2011 02:39 PM)Jacques Chirac Wrote: [\[CITE\]](#) thx ? , in my school I have a paranoid (but inefficient) network admin and the computers are very secured.

It's for help peoples having problems to gain full access of their school's network that I wrote this tutorial ?

The command doesn't work at my school it says that i don't have permission....

(Apr 30, 2013 03:44 AM)Olli Wrote: [\[CITE\]](#) C:\Dokumente und Einstellungen\schueler>net user test12345 /add
Systemfehler 5 aufgetreten.

Zugriff verweigert
i have the same olli:(
hope there is another way

simox147 - April 30, 2013, 4:40 am

ow, I opened this and was prepared to flame and tell you not to post shit that's been posted 1million times. This was a really good tutorial. Thank you. I warn people though, if you get caught, you will end

vopi181 - April 30, 2013, 6:10 am

My school macs :(but I have the admin password anyway,

Tomtim99 - April 30, 2013, 6:53 am

Lol this is smart and interesting, thanks for sharing :P

Darkjosh - April 30, 2013, 8:16 am

good one for a first tutorial did a good job :)

Heufd - April 30, 2013, 8:22 am

Great tutorial mate, but don't you have to be admin to add a user?
I mean through CMD, did it a lot.

Thanks and kind regards.

- **R1z.** - April 30, 2013, 8:57 am

Thank's Man i just hope this works =D

yessine1 - April 30, 2013, 9:43 am

I'm gonna try it.

But i know now,that the 1. Method never gonna work,all school have blocked this with a error 5 code i think

Makabra666 - April 30, 2013, 10:36 am

Nice Tutorial thanks alot <33

~Ashba

Deathy - April 30, 2013, 3:24 pm

Really good method, not that I'll probably ever try it...

Jafooly - April 30, 2013, 5:22 pm

Looks awesome, will test it out next time im in school.

TheGh0s7 - April 30, 2013, 7:48 pm

Some Old methods but still Very Good :))

postis

rasvi24 - April 30, 2013, 7:55 pm

nice tutorial, have to try at my school

cwscowboy1998 - May 1, 2013, 2:07 pm

This looks great I wanna try this so bad

JoeHandy - May 1, 2013, 2:57 pm

Shcool networks can be very easy, just need common sence and the right things.

doodlederm - May 4, 2013, 4:44 pm

Lol i will try it on monday :D that's a funny thing

Neophytez - October 29, 2013, 2:53 pm

do you have any ideas how to log into school network without using your own username/pass?
otherwise, thanks for tutorial, gonna try it :)

?Homie g dawg - October 29, 2013, 3:13 pm

Wow, this is nice I must try this out sometime. :)

grady - October 29, 2013, 3:58 pm

Very, very nice TUT, I'm actually very glad that you mentioned the way to change out the cmd with sethc, which automatically is root if not logged in to the computer.

My advice to anyone using this is to not alter your grades, someone will notice and shit will hit the fan, best way to do it would be to jack with someone else's and their attendance.

At my school though, the grades are done via the internet, so all I have to do is get on the teacher network and sniff for packets there.

outhacked - October 29, 2013, 7:25 pm

Very cool. Thanks for Tut, I am definitely going to check this out.

kgb1953 - October 29, 2013, 11:27 pm

My last day of school in my final year is tomorrow, time to have fun :) EDIT: Does anyone have a mirror for FakeGina as the dl link is not working for me.

T1M3 2 R4T - October 29, 2013, 11:31 pm

nice tut baby My last day of school in my final year is tomorrow, time to have fun haha nice

Trimerus - October 30, 2013, 2:26 am

Wow awesome, I easily bypassed password of the BIOS following your tutorial! It's too bad I can't do anything major on our school computers.... except for installing games for everybody to play!

Thanksa again, OP!

U63R - October 30, 2013, 3:25 am

great tut man! bookmarked :)

-U63R

Shaggy - October 30, 2013, 10:28 am

Too bad for me , Already finished Schooling :(

arabgunner06 - October 30, 2013, 6:20 pm

Looks amazing! I now have something to do at Saturday school. ;)

Zyped - October 30, 2013, 6:46 pm

Okay, What if my school computers are mac? Also my school has VPN and decent security... ive attempted to ddos the network.

DarkMove - October 30, 2013, 11:10 pm

yeah it would work in old days

now schools and universities have a customized system so basically you have no rights, only viewing and editing documents surfing the web printing etc

the only way to get around that is using browser exploits to execute your backdoor :) let it slip through a trustworthy port and you will be fine

CaptainDynamic - October 30, 2013, 11:20 pm

solid tutorial, wish i had have done this whilst at school

jashin0 - November 6, 2013, 7:50 am

thanks for sharing :D.. hahahahahaha very nice

luckysunny - November 6, 2013, 8:01 am

nice share . i will share ur method with my friends .

Samira - December 10, 2013, 9:19 am

Posting to view it at school.

Thanks

WrathTheAbaddon - December 21, 2013, 9:59 pm

hey man this for the great tut, will try later :)

SIM-2090815 - December 22, 2013, 10:43 am

Looks interesting i might give this ago !!

Accid4nt - December 22, 2013, 1:12 pm

Great tutorial man, I wish i knew this shit when i was in school. I know nothing was blocked. I just didn't know my thumb from my ass when it came to computers back then.

shadowcracker - December 23, 2013, 3:41 pm

It is so very usefull sir,keep on sharing sir

Migael - January 5, 2014, 9:24 am

Too bad my school's got a good security system :(

Tipigle - January 5, 2014, 11:40 pm

Wow, great tut. Your english was pretty good only like 2 or 3 errors but still easily readable. I will definitely try this at my school. Cant wait to try.

hamza984u - January 6, 2014, 4:32 am

Le jour de Gloire est arrivé Jaques Chirac, Le meilleur président est dans le hack :)

osidrusher - January 11, 2014, 8:03 pm

very cool, people might do this haha

NuclearCharged - January 11, 2014, 9:46 pm

Very detailed, but also dangerous. Kid at my school tried doing something like this and was suspended since they have people watching if someone has got into the CMD or have made them self and admin on the network. Very dangerous if you don't know what your doing. Great tut though.

Mung - January 11, 2014, 9:59 pm

Lel, so hard compared to what I did.

I walked into my network administrators office with a USB, asked him to give me all of the passwords. He copied. I pasted. Done.

It's good to be friends with people.

spnwe - January 15, 2014, 6:42 am

My school has done something, everytime i try to write an"/" when its changing it into an "&", really annoying. :(

parkerbrahhh - January 15, 2014, 6:45 am

Wish I had this when I was at school

Viagra - January 15, 2014, 6:49 am

I think I'm going to try this soon. Thanks for sharing!

MAZZIMO - January 15, 2014, 6:57 am

This is beautiful, going to try this ASAP. Bookmarked.

InfinityRex - January 16, 2014, 2:47 am

I found this useful good tutorial. ;)

warlock994007 - January 16, 2014, 7:06 am

I had tried all this tricks in my school days better be useful to others, Nice tutorial.

SIM-341126 - January 16, 2014, 7:12 am

Very nice tutorial , might try this next time in the library when i am bored to death. Thanks.

whyso - January 16, 2014, 7:13 am

This Tutorial Is Awesome!! Im gonna try this on my collage Network!! lol Keep up the good work man.

Death - January 16, 2014, 7:14 am

I'm gonna have to print off a few pages and take the copies into College - It's so annoying not being able to get onto certain websites, plus my favourite computing website, HackForums.

abadguy87 - March 12, 2014, 8:24 am

Great tutorial mate THX a lot for sharing

Tajmonekus - March 12, 2014, 9:54 am

Great tut man, thanks :) But unfortunately the net user command doesn't work on the school computers, it just says "access denied"

Sexy Devil - March 12, 2014, 10:03 am

Thank you for this detailed tutorial...
nice work! :)

yollo - March 12, 2014, 6:02 pm

thanks for the info hope this work :)

oldy2511 - March 12, 2014, 7:10 pm

thanks alot cant wait to try some of this :D

BojoHKs - March 15, 2014, 4:51 pm

Great set of methods man I will be sure to try

BlazeBruh - March 15, 2014, 6:06 pm

Nice tut bro cant wait to test this in my school

jasoncher - March 15, 2014, 7:17 pm

Wouldnt this need to be done on a computer on the school network, causing you to get caught?..

Voxinat - March 16, 2014, 1:57 am

Vu que je suis tout nouveau dans le hackinget que tu as l'air français je vais te poser une question en francais pour mieux comprendre: où faut-il saisir les parties où il y a écrit code STP?
Merci d'avance!

Grimzyy - March 16, 2014, 12:53 pm

the fakegina.dll thing doesn't work for meh.. tried it on myself and it doesnt work.. think I'm doing the regedit thing wrong

Jony Blaze - March 16, 2014, 12:57 pm

I haven't tried it. But Idea looks awesome.

-Red Dragon

Mr.ViewTi - March 16, 2014, 2:21 pm

haha awesome man. I already got admin in mine school, but i would've used this if i haven't done it yet. great tut

Mutiny - March 16, 2014, 10:56 pm

where can I find backtrack 5 download? its not continued anymore.

When I try to run cain and abel it says I need a admin password and username but I cant get it because acces 5 or something error denied

kev1nop - March 17, 2014, 1:57 am

I am pretty sure the admin's knowledge on IT is far superior than mine. But glad to know there is a way to do it.

im a lama - March 17, 2014, 8:21 am

this looks awesome, will try it when i get the chance

Lucarios11 - March 17, 2014, 9:38 am

At our school CMD is blocked by the Admin.

In that case just open 'Powershell'. It's the se as CMD but it's scriptable.
(And you can open Cmd from Powershell by just typing: 'start' or 'start cmd' twice.)

--

Lucarios

Stack Overflow - March 17, 2014, 11:12 am

Never. Fucking. Mind. Nope. Nope. Nope.

GoatOfWar - March 17, 2014, 12:55 pm

Hmmm im gonna try it, I hope it works:P

But, is it safe to do?

Lucarios11 - March 17, 2014, 1:30 pm

(Mar 17, 2014 12:55 PM)GoatOfWar Wrote: [\[CITE\]](#) Hmmm im gonna try it, I hope it works:P

But, is it safe to do?

No it's not.

When using a school computer logged in at your school, you will leave to much evidence of you ti say its safe.

The can see which account was logged in and kick you from school. (Pretty much)

Bin4ry - March 17, 2014, 2:36 pm

Isnt OPHCrack kind of outdated?

But nice tutorial :)

Regards,

Bin4ry

Ignitions - March 17, 2014, 7:46 pm

Thanks man it really helped me out so much

D44n - March 18, 2014, 8:50 am

Very good tutorial...

But really watch out when using this.

I used to block teacher accounts on magister (System for marks and homework) by entering a wrong password several times. But some girls in my class discovered it was me and decided to tell the teacher.

Well, to keep a long story short. It ended up in several weeks of going to school early and going home late. Also i had to talk with some psychologist a few times.

Oh, and if it happens again, they will contact the police :).

What i want to say is, Watch out with doing this, and leave no traces.

