

Forum:[Hack Forums](#)

Thread: [Hacking someone \(with permission\)](#)

JeremyGuzzler69 - January 8, 2024, 10:47 pm

They say hacking someone without permission can have negative consequences. What about if your own close friend gave you the "all clear" to try and hack them? What are the steps you would take to pwn your friend with their permission. Obviously, you don't want to negatively harm your friend in the long run, so no DoS attacks or anything else that could harm them. You can do anything as long as you can make it like nothing happened later, or as long as it could benefit them in the future to improve their security. Think of this as a mini pen test, against your friend. However, social engineering in this case can be allowed, just don't get caught until you are done ;)

DramaKing - January 9, 2024, 5:49 am

(Jan 8, 2024 11:47 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) They say hacking someone without permission can have negative consequences. What about if your own close friend gave you the "all clear" to try and hack them? What are the steps you would take to pwn your friend with their permission. Obviously, you don't want to negatively harm your friend in the long run, so no DoS attacks or anything else that could harm them. You can do anything as long as you can make it like nothing happened later, or as long as it could benefit them in the future to improve their security. Think of this as a mini pen test, against your friend. However, social engineering in this case can be allowed, just don't get caught until you are done ;)

The primary rule of ethical hacking is not to hack anyone without permission. This is fine.

JeremyGuzzler69 - January 9, 2024, 1:59 pm

(Jan 9, 2024 06:49 AM)DramaKing Wrote: [\[CITE\]](#) The primary rule of ethical hacking is not to hack anyone without permission. This is fine.

Yes, I see how it is fine, but my question is how you would go about hacking your friend? What methodology would you employ?

TestingHH - January 9, 2024, 2:19 pm

(Jan 9, 2024 02:59 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) Yes, I see how it is fine, but my question is how you would go about hacking your friend? What methodology would you employ?

I'd assume anything you would do with a normal hack against someone, if they don't have 2FA or much security on something like their email you could try breaking into that, or doxxing.

JeremyGuzzler69 - January 9, 2024, 2:38 pm

(Jan 9, 2024 03:19 PM)TestingHH Wrote: [\[CITE\]](#) I'd assume anything you would do with a normal hack against someone, if they don't have 2FA or much security on something like their email you could try breaking into that, or doxxing.

How would you break into the email without 2FA? Would you try social engineering? Would you try to brute force it? Use that to gain access to other stuff? What would your priorities be?

TestingHH - January 9, 2024, 3:29 pm

(Jan 9, 2024 03:38 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) How would you break into the email without 2FA? Would you try social engineering? Would you try to brute force it? Use that to gain access to other stuff? What would your priorities be?

I'm not exactly sure since I'm not very into hacking for now, I'm just here to chill on the forum but others can probably help you with that. You can try searching on the forum or other websites since I know the internet has very good resources.

DramaKing - January 9, 2024, 4:21 pm

(Jan 9, 2024 02:59 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) Yes, I see how it is fine, but my question is how you would go about hacking your friend? What methodology would you employ?

I'd start with step 1 of the hacking methodology: Reconnaissance. You need to examine your target, gather information, and only then move on to enumeration and exploitation. Only once you know in detail what you're attacking, details on who you're attacking, and what you want to achieve, should you launch actual attacks.

Spore - January 9, 2024, 5:07 pm

This seems like a weird reddit post in a kink sub and you just replaced "fucking" with "hacking"

JeremyGuzzler69 - January 9, 2024, 6:23 pm

(Jan 9, 2024 05:21 PM)DramaKing Wrote: [\[CITE\]](#) I'd start with step 1 of the hacking methodology: Reconnaissance. You need to examine your target, gather information, and only then move on to enumeration and exploitation. Only once you know in detail what you're attacking, details on who you're attacking, and what you want to achieve, should you launch actual attacks.

Kink sub? Which kind of sub are we talking about here ;)

(Jan 9, 2024 05:21 PM)DramaKing Wrote: [\[CITE\]](#) I'd start with step 1 of the hacking methodology: Reconnaissance. You need to examine your target, gather information, and only then move on to enumeration and exploitation. Only once you know in detail what you're attacking, details on who you're attacking, and what you want to achieve, should you launch actual attacks.

I love it, as someone newer to the field it is always fascinating to hear someone more experienced talk about their methodology. Let's say during the recon phase, you found various email addresses, social media profiles, family and friends names/phone numbers, as well as the target's home IP address. What would you do to move forward towards further enumeration or exploitation? I would assume running an NMAP scan, but with my experience I am not sure if I would be able to exploit whatever ports I find open at the moment tbh haha.

DramaKing - January 9, 2024, 7:27 pm

(Jan 9, 2024 03:19 PM)TestingHH Wrote: [\[CITE\]](#) I'd assume anything you would do with a normal hack against someone, if they don't have 2FA or much security on something like their email you could try breaking into that, or doxxing.

Dox his own friend? What?

(Jan 9, 2024 07:23 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) Kink sub? Which kind of sub are we talking about here ;)

I love it, as someone newer to the field it is always fascinating to hear someone more experienced talk about their methodology. Let's say during the recon phase, you found various email addresses, social media profiles, family and friends names/phone numbers, as well as the target's home IP address. What would you do to move forward towards further enumeration or exploitation? I would assume running an NMAP scan, but with my experience I am not sure if I would be able to exploit whatever ports I find open at the moment tbh haha.

You'll definitely want to run Nmap. You could do a lot with those things. Searching the forums will probably help with the specifics.

JeremyGuzzler69 - January 9, 2024, 8:12 pm

(Jan 9, 2024 07:23 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) Kink sub? Which kind of sub are we talking about here ;)

I love it, as someone newer to the field it is always fascinating to hear someone more experienced talk about their methodology. Let's say during the recon phase, you found various email addresses, social media profiles, family and friends names/phone numbers, as well as the target's home IP address. What would you do to move forward towards further enumeration or exploitation? I would

assume running an NMAP scan, but with my experience I am not sure if I would be able to exploit whatever ports I find open at the moment tbh haha.

Thank you, I appreciate your insight!

DramaKing - January 9, 2024, 8:24 pm

Have you heard of CTFs in the context of hacking? Vulnhub.com and Metasploitable are good for playing around with hacking on your own. You'll need some virtualization knowledge, which you'll need anyway if you get serious about hacking.

linkinpork - January 9, 2024, 10:07 pm

(Jan 8, 2024 11:47 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) Think of this as a mini pen test, against your friend. However, social engineering in this case can be allowed, just don't get caught until you are done ;)

1. Good opportunity to teach your friend about phishing. Try an email address from a website like [this one](#). Then send a believable email with a link towards [a website that teaches how to tell a phishing attack](#). They click, lesson learned.
2. If you know one of their old passwords (whether through a public database leak or otherwise) you can test it out on, say, Facebook. Then post something like "I should never use the same password everywhere."
3. You're friends, so you should know the favorite websites you visit. Consider a [watering hole attack](#).
4. Are you in the same network? Do you know their PC profile's credentials? If they left RDP turned on without using it, you could teach them to shut it off by connecting there yourself.
5. I used to toy around with [MITME](#) back in the day. Fun way to teach about Rogue Hotspots. Easy way to get kicked out of Starbucks too.
6. Do they keep Bluetooth enabled on their phone? Change your phone's name to "HACKED XOXO". Then try to pair. [.com/blog/bluejacking/What is Bluejacking?](#)
7. BT headset worn while unpaired? Pair, open Youtube Music, then Rickroll.

Have fun!

SIM-5186353 - January 10, 2024, 10:37 am

(Jan 8, 2024 11:47 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) They say hacking someone without permission can have negative consequences. What about if your own close friend gave you the "all clear" to try and hack them? What are the steps you would take to pwn your friend with their permission. Obviously, you don't want to negatively harm your friend in the long run, so no DoS attacks or anything else that could harm them. You can do anything as long as you can make it like nothing happened later, or as long as it could benefit them in the future to improve their security. Think of this as a mini pen test, against your friend. However, social engineering in this case can be allowed, just don't get caught until you are done ;)

If they allow you, why not?

JeremyGuzzler69 - January 10, 2024, 10:43 am

(Jan 9, 2024 09:12 PM)JeremyGuzzler69 Wrote: [\[CITE\]](#) Thank you, I appreciate your insight! Yes, I have done couple of CTFs and I am actually taking a pen testing course at the moment. Feel free to PM for more details if interested. I just feel like CTFs are different than when it comes to

hacking someone you already know, as ctf's tend to be focused on finding a flag rather than exploitation, post exploitation & trolling lol. I'm thinking something more on the line of installing ransomware with the ransom being \$1 or a pizza or something xD

(Jan 9, 2024 09:24 PM)DramaKing Wrote: [\[CITE\]](#) Have you heard of CTFs in the context of hacking? Vulnhub.com and Metasploitable are good for playing around with hacking on your own. You'll need some virtualization knowledge, which you'll need anyway if you get serious about hacking.

The facebook one is funny, I might try this as I do have access to some passwords. My main concern is 2FA. Phishing, he is very weary of links and double checks them. He is pretty tech savvy.

Regarding a watering hole attack, I need to do more research. I just don't want to put myself at risk if it involves doing something risky on a website that hasn't given me permission. However if that isn't a risk, I'm super intrigued by the concept.

RDP might be a good play too and I did a similar HTB challenge. Probably should practice more first but it's an incredible idea. Would be funny if I got into a SM acc using breached data and then posted as I connected via rdp and installed ransomware with a \$1 key or something lmfao

idk how I keep quoting the wrong reply smh

(Jan 9, 2024 11:07 PM)linkinpork Wrote: [\[CITE\]](#) 1. Good opportunity to teach your friend about phishing. Try an email address from a website like [this one](#). Then send a believable email with a link towards [a website that teaches how to tell a phishing attack](#).. They click, lesson learned.

2. If you know one of their old passwords (whether through a public database leak or otherwise) you can test it out on, say, Facebook. Then post something like "I should never use the same password everywhere."

3. You're friends, so you should know the favorite websites you visit. Consider a [watering hole attack](#).

4. Are you in the same network? Do you know their PC profile's credentials? If they left RDP turned on without using it, you could teach them to shut it off by connecting there yourself.

5. I used to toy around with [MITME](#) back in the day. Fun way to teach about Rogue Hotspots. Easy way to get kicked out of Starbucks too.

6. Do they keep Bluetooth enabled on their phone? Change your phone's name to "HACKED XOXO". Then try to pair. [.com/blog/bluejacking/What is Bluejacking?](#)

7. BT headset worn while unpaired? Pair, open Youtube Music, then Rickroll.

Have fun!

Can you PM me?

TestingHH - January 10, 2024, 9:42 pm

(Jan 9, 2024 08:27 PM)DramaKing Wrote: [\[CITE\]](#) Dox his own friend? What?

I don't think I was thinking straight sorry lol.