

Forum:[Hack Forums](#)

Thread: [Ask any question. Beginner friendly.](#)

Omega_X - April 27, 2019, 10:42 am

I'm sure when people are posting threads here, they're either new/not sure of where to start or what they're doing.

I want to help out the community and offer: Any questions you have regarding exploits, hacking, programming, etc. please feel free to PM me or reply to this thread.
I'll get back to you ASAP.

Everyone has to start somewhere so I don't want you to be afraid to ask your questions :).

If you don't know where to start or need a guide feel free to let me also !

Lavincii - April 27, 2019, 12:25 pm

(Apr 27, 2019 10:42 AM)Omega_X Wrote: [\[CITE\]](#) I'm sure when people are posting threads here, they're either new/not sure of where to start or what they're doing.

I want to help out the community and offer: Any questions you have regarding exploits, hacking, programming, etc. please feel free to PM me or reply to this thread.
I'll get back to you ASAP.

Everyone has to start somewhere so I don't want you to be afraid to ask your questions :).

If you don't know where to start or need a guide feel free to let me also !

How does spyware work and can it be used on iPhones???

Bastille - April 27, 2019, 1:40 pm

Interested about the answer, following this thread

Omega_X - April 28, 2019, 11:08 am

(Apr 27, 2019 12:25 PM)Lavincii Wrote: [\[CITE\]](#) How does spyware work and can it be used on iPhones???

Yes, spyware can work with iPhones. It's especially easy if their iPhone is jailbroken and keeps the default root passwords.

This can work if your using exploits in Metasploit; Once you learn how to use it, it can be really useful :)

By this, it will allow you too access any file on the phone and be able to take screenshots, etc.

Spyware is a bit different than using it on a computer. iPhone's are much more complicated and complex.

Bastille - April 28, 2019, 11:55 am

And how does it work ?

It sends information from the target, but through a specific port ? Can we determine which

information we want to know ?

9Oppip0 - April 28, 2019, 3:17 pm

where can I study exploits?

Omega_X - April 28, 2019, 8:24 pm

(Apr 28, 2019 03:17 PM)9Oppip0 Wrote: [\[CITE\]](#) where can I study exploits?
exploit-db is a good place to learn exploits. Simply googling is also a good idea.
When learning exploits it'll also be useful to learn a programming language also.
(Apr 28, 2019 11:55 AM)Yseurk Wrote: [\[CITE\]](#) And how does it work ?

It sends information from the target, but through a specific port ? Can we determine which information we want to know ?

You can determine which information you want to know, yes. A spyware can be used for keylogging, track websites, etc. You can use the keylogging to find email passwords, account passwords ect. It will look something like "gmail.commyemail@gmail.compassword123"

You'll have to break it down though, since it tracks every key that's typed. Using context clues you can see that it goes to "Gmail.com" then it shows an email "Myemail@gmail.com" then anything after will be a password. Just a basic example.

Some ports can be affected by an exploit, some cannot. Sometimes you don't need a port for an exploit. It all depends on the OS, versions, etc.

DolceRancore70 - April 29, 2019, 11:46 am

Hi Omega_X, I'm here because I would like to ask you more information about where I can find working Amazon giftcard generators. I still don't know what to do in these forums. I have browsed various forums to find various programs, but I don't know how to use them effectively. Could you help me ? Could I find somewhere a detailed guide to generating Amazon giftcards? Thank you in advance for your help.

Omega_X - April 29, 2019, 5:25 pm

(Apr 29, 2019 11:46 AM)DolceRancore70 Wrote: [\[CITE\]](#) Hi Omega_X, I'm here because I would like to ask you more information about where I can find working Amazon giftcard generators. I still don't know what to do in these forums. I have browsed various forums to find various programs, but I don't know how to use them effectively. Could you help me ? Could I find somewhere a detailed guide to generating Amazon giftcards? Thank you in advance for your help.

It's nearly impossible to generate gift cards.

Imagine generating thousands of gift cards that you can use or sell.

Technically it's not impossible, but it would be beyond my knowledge to know exactly how this works. Only thing I can tell you is: It is really really really hard - almost impossible - to do this.

HolyLucifer - April 29, 2019, 5:31 pm

How do I hack instagram accounts from people?

(Apr 27, 2019 10:42 AM)Omega_X Wrote: [\[CITE\]](#) I'm sure when people are posting threads here, they're either new/not sure of where to start or what they're doing.

I want to help out the community and offer: Any questions you have regarding exploits, hacking, programming, etc. please feel free to PM me or reply to this thread.

I'll get back to you ASAP.

Everyone has to start somewhere so I don't want you to be afraid to ask your questions :).

If you don't know where to start or need a guide feel free to let me also !

Omega_X - April 29, 2019, 5:34 pm

(Apr 29, 2019 05:31 PM)HolyLucifer Wrote: [\[CITE\]](#) How do I hack instagram accounts from people? Social Engineering, Brute force it, guessing, wordlists.

It can be fairly simple.

My first attempt and approach would be social engineering.

Make a fake instagram login page, host it locally, and try to get them to click the link and login. If you need guidance on it or help, let me know.

That's just the bare basics of approaching this

HolyLucifer - April 29, 2019, 5:36 pm

Yes please help me with this

(Apr 29, 2019 05:34 PM)Omega_X Wrote: [\[CITE\]](#) Social Engineering, Brute force it, guessing, wordlists.

It can be fairly simple.

My first attempt and approach would be social engineering.

Make a fake instagram login page, host it locally, and try to get them to click the link and login. If you need guidance on it or help, let me know.

That's just the bare basics of approaching this

Omega_X - April 29, 2019, 5:39 pm

(Apr 29, 2019 05:36 PM)HolyLucifer Wrote: [\[CITE\]](#) Yes please help me with this

Step one. Go to Instagram login page.

Step two. Copy the HTML of the site and post in in your own hosting.

Step three. edit the login page to direct any input to your email.

Step four. Get him to click it.

Xpokemon45 - April 29, 2019, 5:46 pm

As a high-schooler, what's the most beneficial hack I could learn/do?

Omega_X - April 29, 2019, 5:49 pm

(Apr 29, 2019 05:46 PM)Xpokemon45 Wrote: [\[CITE\]](#) As a high-schooler, what's the most beneficial hack I could learn/do?

Learn a programming language/scripting language.

C++
PHP
Python

These three are very beneficial
Then also learn HTML, CSS, Javascript.

They will help you out a lot in life if you use it correctly.

I know they are not necessarily "Hacks" or "Techniques" but they will be much more beneficial.

That's the best advice I can give :)

Xpokemon45 - April 29, 2019, 5:53 pm

(Apr 29, 2019 05:49 PM)Omega_X Wrote: [\[CITE\]](#) Learn a programming language/scripting language.

C++
PHP
Python

These three are very beneficial
Then also learn HTML, CSS, Javascript.

They will help you out a lot in life if you use it correctly.

I know they are not necessarily "Hacks" or "Techniques" but they will be much more beneficial.

That's the best advice I can give :)

So I'm pretty proficient at C++, JVSC, and am extremely proficient in HTML and Python. I'm trying to do something fun and crazy like hack/bug the wifi, or get the school loop password from a teacher, or access the security cameras. Ideas on how I could get started on all of those?

Omega_X - April 29, 2019, 5:57 pm

(Apr 29, 2019 05:53 PM)Xpokemon45 Wrote: [\[CITE\]](#) So I'm pretty proficient at C++, JVSC, and am extremely proficient in HTML and Python. I'm trying to do something fun and crazy like hack/bug the wifi, or get the school loop password from a teacher, or access the security cameras. Ideas on how I could get started on all of those?

Okay, perfect. So you know some programming language/scripting.

School's will be on your A** about hacking into their stuff and it is highly not suggested. Don't want to get kicked out of school or something worse.

Anyways, lets continue :)

If you're on the same network as the cameras, typing the IP in the browser should work. I think it works with CCTV cameras.

You can make a fake login page for the school, host it locally, get all the login information.
Find an exploit/vulnerability in the schools website.
etc. etc.

To get started, why not try something simple. Make a fake login page and social engineer some ;)

HolyLucifer - April 29, 2019, 6:07 pm

How do you change the coding and stuff to do that?

(Apr 29, 2019 05:39 PM)Omega_X Wrote: [\[CITE\]](#) Step one. Go to Instagram login page.
Step two. Copy the HTML of the site and post in in your own hosting.
Step three. edit the login page to direct any input to your email.
Step four. Get him to click it. How do I get it to host locally and make it so when they log in it shows me theyre username and password?

(Apr 29, 2019 05:39 PM)Omega_X Wrote: [\[CITE\]](#) Step one. Go to Instagram login page.
Step two. Copy the HTML of the site and post in in your own hosting.
Step three. edit the login page to direct any input to your email.
Step four. Get him to click it.

Omega_X - April 29, 2019, 6:29 pm

(Apr 29, 2019 06:07 PM)HolyLucifer Wrote: [\[CITE\]](#) How do you change the coding and stuff to do that?

How do I get it to host locally and make it so when they log in it shows me theyre username and password?

Google it. Google is your friend ;)

by learning yourself it will be much more productive, but i can give you general knowledge and advice.

Try starting it yourself, then any questions you have contact me.

aJy6IYyDOQ - April 30, 2019, 3:38 pm

I want to start hacking stuff but I have no idea where to start, suggestions please?

Omega_X - April 30, 2019, 5:01 pm

(Apr 30, 2019 03:38 PM)aJy6IYyDOQ Wrote: [\[CITE\]](#) I want to start hacking stuff but I have no idea where to start, suggestions please?

Learning a scripting/programming language. This way, you'll understand better some of the things you're doing/learning. I also suggest starting with reading a ebook too, they can be useful; Search for them on the forum.

Travikator - April 30, 2019, 5:56 pm

Good to see people like you on this forum. Need more folk willing to teach and help others learn. Cheers keep up the work!

Omega_X - April 30, 2019, 6:36 pm

(Apr 30, 2019 05:56 PM)Travikator Wrote: [\[CITE\]](#) Good to see people like you on this forum. Need more folk willing to teach and help others learn. Cheers keep up the work!

Thanks!

Travikator - April 30, 2019, 6:42 pm

(Apr 30, 2019 06:36 PM)Omega_X Wrote: [\[CITE\]](#) Thanks!

ofc op ? any way you could shoot me a pm, i need a little help with this issue that's been kicking my ass. So close to hacking this account. But yet so far ?

Omega_X - April 30, 2019, 6:47 pm

(Apr 30, 2019 06:42 PM)Travikator Wrote: [\[CITE\]](#) ofc op ? any way you could shoot me a pm, i need a little help with this issue that's been kicking my ass. So close to hacking this account. But yet so far ?

Sounds good. Send me a PM and i'll see what I can do for you

Travikator - April 30, 2019, 6:54 pm

(Apr 30, 2019 06:47 PM)Omega_X Wrote: [\[CITE\]](#) Sounds good. Send me a PM and i'll see what I can do for you
sent ?

Ace Whole - April 30, 2019, 7:09 pm

Hi, this thread is exactly what I was looking for!

I cracked my wifi password using brute force (wifite). If I had a stronger password that didn't fall into an average wordlist, what would be the next method someone would try to get in?

Thanks in advance!

Omega_X - April 30, 2019, 7:14 pm

(Apr 30, 2019 07:09 PM)Ace Whole Wrote: [\[CITE\]](#) Hi, this thread is exactly what I was looking for!

I cracked my wifi password using brute force (wifite). If I had a stronger password that didn't fall into an average wordlist, what would be the next method someone would try to get in?

Thanks in advance!

I love these kind of questions. You're not asking me to do something, and it's a legitimate question.

I value social engineering highly, so i would attempt this.

edit: Well obviously you cannot SE yourself since you already know the password, but assuming it's a victim.

There's many tools that you can use such as: [https://github\(dot\)com/ZerBea/hcxdumptool](https://github(dot)com/ZerBea/hcxdumptool).

I mean you can just look around. Regardless, most of the tools are going to be using wordlists etc.

I tried my best to answer the question, but i'm not really the most experienced in WiFi hacking, it's not what I focus on :P

equi_gonzales13 - May 1, 2019, 11:37 am

Hello there,

How could someone possibly take advantage of large txt. files with data stolen from breaches/leaks?

Most of them are not of the form username/email:password, but rather random words without their corresponding "credential".

Omega_X - May 1, 2019, 11:52 am

(May 1, 2019 11:37 AM)equi_gonzales13 Wrote: [\[CITE\]](#) Hello there,

How could someone possibly take advantage of large txt. files with data stolen from breaches/leaks?

Most of them are not of the form username/email:password, but rather random words without their corresponding "credential".

Using context clues and logic

butwal99 - May 1, 2019, 12:22 pm

There was a video posted long time back about a small software which can hack any mobile in 5 minutes on YouTube.

I am still searching for that bot and cant find it anywhere as its really private tool.

elespion - May 1, 2019, 12:32 pm

Bonjour je suis tout nouveaux dans ce site et debutant en hacking, qui peut me dire comment rentrer dans un serveur non securisé s'il vous plait . merci a vous

Symplistic - May 1, 2019, 2:16 pm

Probably the most noobiest question I could ever ask, but IP Sniffers. Even when I start pulling for IP's , no IP's show up and then my internet disconnects. What is a quick fix or a better program than LANC? I've watched a tut on Commview but no IP's pull what so ever. Do I need to Bridge?

Omega_X - May 1, 2019, 6:47 pm

(May 1, 2019 12:22 PM)butwal99 Wrote: [\[CITE\]](#) There was a video posted long time back about a small software which can hack any mobile in 5 minutes on YouTube.

I am still searching for that bot and cant find it anywhere as its really private tool.

Keep looking :). Not exactly sure what the question is here. Use google

(May 1, 2019 12:32 PM)elespion Wrote: [\[CITE\]](#) Bonjour je suis tout nouveaux dans ce site et debutant en hacking, qui peut me dire comment rentrer dans un serveur non securisé s'il vous plait . merci a vous

pouvez-vous définir "serveur non sécurisé" plus. À quoi voulez-vous également accéder?

(May 1, 2019 02:16 PM)Symplistic Wrote: [\[CITE\]](#) Probably the most noobiest question I could ever ask, but IP Sniffers. Even when I start pulling for IP's , no IP's show up and then my internet disconnects. What is a quick fix or a better program than LANC? I've watched a tut on Commview but no IP's pull what so ever. Do I need to Bridge?

Not exactly sure with this one. Probably an issue to do with not having a WiFi adapter card (Or whatever they're called).

This may be it because I know certain tools such as aircrack-ng also require one

Ace Whole - May 2, 2019, 5:33 am

(Apr 30, 2019 07:14 PM)Omega_X Wrote: [\[CITE\]](#) I love these kind of questions. You're not asking me to do something, and it's a legitimate question.

I value social engineering highly, so i would attempt this.

edit: Well obviously you cannot SE yourself since you already know the password, but assuming it's a victim.

There's many tools that you can use such as:

I mean you can just look around. Regardless, most of the tools are going to be using wordlists etc.

I tried my best to answer the question, but i'm not really the most experienced in WiFi hacking, it's not what I focus on :P

Thanks for the reply! I wanted to PM you but I have to get a couple dozen more "quality post" to be able to do-so.

I am pretty green still, I figured starting on my own wifi was a safe way to try out some tools. Do you have any recommendations for servers set up to practice different tools against? Im running Kali but I don't know how to use most of them and I am trying to stay out of trouble! ;) I've been doing some challenges on the common sites but I am really looking to try these tools out to get a better understanding of what can be done.

vanilla_unicorn - May 2, 2019, 5:58 am

Hi all. I'm brand spankin' new here.

I have a sufficient amount of web software development experience (mostly doing full/lamp stack dev work) and have been itching to get into security.

I've been covering a lot of information:

- covered the new frameworks on the frontend (react, vue, etc)
- picked up node in the process and now have an intimate understanding with how the js on the frontend and backend is working
- am pretty proficient in using different high level languages as well as working with automating with bash, python, etc.
- already read through Web app hacker handbook, web browser hacker handbook, and a plethora of other software dev design pattern guides and such (about 45 books)
- I've been following some pentester and reverser blogs to get an understanding of their processes.
- I've gone through DVWA and a few web-based CTFs already with a pretty decent success rate for a little more than half of my attempts
- understand the concepts of XSS, RFI/LFI, and some other attack types

I recently started learning assembly (x86) and want to get into reversing in the near future so I'm teaching myself using books as resources. I have a mentor but don't want to bother him much with seemingly stupid questions so, here I am.

Anyways, my question is, am I on the right track if I want to become more efficient with breaking applications (mostly web but also native)? I still have a lot to learn with crypt/decrypt and steganography and such. It's just difficult to know if what I'm learning is going to be useful in the future or if I'm getting side-tracked.

I'd ultimately like to be on here selling my own wares (following the guidelines of course ?) and phase my career into security.

Hope that wasn't an overload of info, just wanna give enough to help give good advice.

Spacealien - May 2, 2019, 6:21 am

(Apr 27, 2019 10:42 AM)Omega_X Wrote: [\[CITE\]](#) I'm sure when people are posting threads here, they're either new/not sure of where to start or what they're doing.

I want to help out the community and offer: Any questions you have regarding exploits, hacking, programming, etc. please feel free to PM me or reply to this thread.
I'll get back to you ASAP.

Everyone has to start somewhere so I don't want you to be afraid to ask your questions :).

If you don't know where to start or need a guide feel free to let me also !
how do I take advantage of data breaches?/Take info from websites (Gmail pswds, etc.)

Ace Whole - May 2, 2019, 3:20 pm

(May 1, 2019 11:37 AM)equi_gonzales13 Wrote: [\[CITE\]](#) Hello there,

How could someone possibly take advantage of large txt. files with data stolen from breaches/leaks?

Most of them are not of the form username/email:password, but rather random words without their corresponding "credential".

I enjoy data. If you sent me a sample I will give you my thoughts.

Psychedelic. - May 3, 2019, 3:29 am

(Apr 27, 2019 12:25 PM)Lavincii Wrote: [\[CITE\]](#) How does spyware work and can it be used on iPhones???

Probably already answered, but no malware works on Idevices.

Omega_X - May 3, 2019, 3:38 am

(May 3, 2019 03:29 AM)Jasonfaps Wrote: [\[CITE\]](#) Probably already answered, but no malware works on Idevices.

It's possible and it's been done before :)

A jailbroken iPhone can be exploited if the root password is set at default.

EDIT: Reason being, with a jailbroken phone, you can exploit and run remote commands using the command prompt from the jailbroken phone.

Psychedelic. - May 3, 2019, 3:53 am

(May 3, 2019 03:38 AM)Omega_X Wrote: [\[CITE\]](#) It's possible and it's been done before :)

A jailbroken iPhone can be exploited if the root password is set at default.

EDIT: Reason being, with a jailbroken phone, you can exploit and run remote commands using the command prompt from the jailbroken phone.

I guess i learned something new today. Leaving you a green apple.

Asdethprime - May 3, 2019, 4:10 am

(May 3, 2019 03:29 AM)Jasonfaps Wrote: [\[CITE\]](#) Probably already answered, but no malware works on Idevices.

Hehe u are relying on the Apple signature to protect u. Works wonderfully if a person is targeting u with an unsigned app but what if the app is signed.

Devices that have not been jail broken (iPhone) u can control it entirely using a mobile device management app (Apple MDM protocol - google that). That has been misused as malwares I t the past.

Other than that , without without a signature from Apple (or a provisioning profile) native API does not work ; web api works just fine.

Hacking iOS though Trojan or an intentionally vulnerable app. The idea that iPhone is unhackable is not actually correct.

Also low level vulnerabilities like blueborn, spectre , meltdown etc etc will affect whatever device is running the vulnerable hardware / firmware (Apple can't prevent u hacking their Nic for example or exploiting meltdown through an arm processor)

jennyphisher - May 4, 2019, 4:11 pm

Just wondering, what are some good places to practice actual hacking skills (except from maybe brute-forcing your own accounts)?

Omega_X - May 5, 2019, 8:45 am

(May 4, 2019 04:11 PM)jennyphisher Wrote: [\[CITE\]](#) Just wondering, what are some good places to practice actual hacking skills (except from maybe brute-forcing your own accounts)? Virtual Machines probably, or an extra computer you have laying around.

Make your own website, etc.

many things you can do

man7uunn - May 5, 2019, 9:36 am

I want to learn hacking email especially gmail
But i don't know from where i start with this

Faith Connors - May 5, 2019, 9:56 am

Would writing a wrapper for some sort of standard lib affect detection rates?

I know lots of that stuff is determined compile-time statically, but if I make a library that basically just calls some standard libraries in its stead, would compilers be smart enough to ignore the wrapping and go straight to those functions or potentially try to work with it and end up linking everything together as verbosely as I write it?

Or rather, are there any compiler options/optimizations that could add this functionality that you know of? I'm about 90% sure that MSVCP/VS C++ compiler debug mode does something like this, but again, I don't like having a resulting binary that's 10x bigger than the release mode.

As far as detection rates are concerned, I'm more focused on the usual signature detection, so it's pretty easy to get around with other means (LD_PRELOAD, adding shit, changing shit, throwing around the order of shit, etc.)

.C1PH3R. - May 5, 2019, 9:59 am

(May 5, 2019 09:36 AM)man7uunn Wrote: [\[CITE\]](#) I want to learn hacking email especially gmail
But i don't know from where i start with this
You need to know about brute-force and social engineering.
Use a browser and type those 2 words. That's your start.
From there out you can start asking yourself question like is brute-force better then social engineering. What do I need to know about the target for social engineering how do I get that information.

Good luck ? if you have any question feel free to pm me

Omega_X - May 5, 2019, 10:51 am

(May 5, 2019 09:36 AM)man7uunn Wrote: [\[CITE\]](#) I want to learn hacking email especially gmail
But i don't know from where i start with this
Start simple and easy.

Your goal: Hack email's (Gmail)

what do you know, and what do you NOT know?

Your goal is to obtain a password, now what strategies will you use?

- Social Engineering
- wordlists
- brute force
- If you're a god, why not just hack google.