I am a convicted hacker. AMA. ~ 1094795585

First, let me just clarify the title - I do not label myself a "cracker". In my world, crackers crack copy-protection in software. Hackers write tools such as exploits and rootkits. Hackers also break into computer networks.

A brief history about me: I've grown up with computers and started programming when I was about 11. This programming interest gradually become more low-level oriented, focusing on how to break software. Eventually I started using this knowledge to break into computers that didn't belong to me. The targets became more and more high-profile, and in my late teens I found myself in the middle of an early-morning raid. I took great care in hiding my real identity online, but in the end it was one teenager against several well-funded agencies - and I lost. This was before the age of tor.

I was given a suspended prison sentence and ridiculous amounts of fines that I will never be able to pay off. I am in my 20s now and will likely leave for a different country when I am done with my studies, to start a new life.

Ask me anything that isn't too specific - I won't answer questions like "Are you X? Did you hack XYZ.com in 2004?". Some people will say that because I got caught, I must not have been a very good hacker. I don't want to turn this into an ego battle, so I will disregard those posts.

I never hacked anything for financial gain and I don't consider myself a criminal. I'm actually a pretty nice guy. Ask away (:

edit: I'll be back in about 2-3 hours. Great questions so far.

edit2: Back..lots and lots of new posts, I'll get some coffee and start answering.

edit3: Will be back to answer more questions in a while. Thanks for all the good questions, I hope my answers have helped. And thanks to the people who disagree with my views but still keep it civil.

PleaseForgiveMe 143 Points

> edit: I'm given the usual "you are trying to submit to fast"-treatment when replying..bear with me.

Shouldn't you be able to, I don't know, find a way around this somehow?

1094795585 116 Points

It appears to have stopped ;)

reseph 77 Points

hax.

PhilxBefore 19 Points

Eh, Game Genie.

someguyz 2 Points

Or it could be ↑ ↑ ↓ ↓ ← → ← → A B Select Start

orezpraw 52 Points

How do you secure your own system?

helekopters 49 Points

Don't download "MySpace Cool Editor 3.0.bat" from KaZaa.

1094795585 28 Points

I keep my services to a minimum, and I keep them updated. On my Linux box I use custom kernel hardening patches to make memory corruption bugs pretty hard to exploit. OpenSSH is firewalled and only accepts a connection from your ip if you visit a custom port-knocking

page on my webserver. Basically the only service listening is apache, without PHP.

On my desktop and laptop I don't have any services listening at all.

orezpraw 5 Points

Do you think OpenSSH is a security risk if not firewalled?

pra 6 Points

it's a plausible attack vector. It is always better to have less open to the world.

plagueyear 7 Points

I have always wondered this myself, how do hackers protect themselves from being hacked?

akmark 12 Points

From what I've seen/read/heard it's mostly a case of reinstall frequently and just pay attention. Even on Windows it's not especially hard to not be an idiot.. 'Good' hackers usually limit what their traffic is normally anyway, and 'proper' hacking doesn't mean you are doing stuff frequently/at all from your home computer. You usually have some sort of rooted host/proxy on proxy obfuscating the path.

From what I have read it usually means: Free shell somewhere to hack somewhere else and now that is 'home base.' You could do this from an out-of-town coffee shop from your personal comp with the basic ident masking skills. Once you have that 'secure' home base you use it for a few days and then you start over again. Unless you are building a botnet you really just go through new places and things, and even if you reuse existing nodes in the net you always make a new one after things. Once you have this 'home base' computer if you clean up after yourself it's pretty hard to find the route back to the originating host. You just have to keep coming in from different angles and continually creating new 'networks' to stay 'safe.'

Basically unless someone can really drive-by attack your personal computer you are pretty well off. Again the moral of hacking is that 'nothing is safe.' So the more you know the more suspicious you are of things coming and going. The average savvy computer user can dodge most the bullets, but it's the 50%~ that can't that are really the meat and potatoes. Hackers nowadays from what I've read are more 'shoot 100 times, kill one bird' than targeted strikes.

buzz93 43 Points

Did you listen to techno music all the time like the hackers in the movies?

1094795585 23 Points

I listened to oldschool techno and a lot of italo. I still do, but have widened my tastes somewhat. It's still exclusively electronical music though ;)

TellEmSoulja 5 Points

awesome. I love old school 90s techno (acid, gabber, hard). Italo is cool too but it's kind of gay sometimes.

1094795585 8 Points

Yeah.. sometimes it can definitely get pretty gay. But it will always cheer you up.

Jalisciense 3 Points

redundant comment.

Skyguard 6 Points

I think this is a question more than one person wants to know :-)

abenton 58 Points

Were you Acid Burn? Also, how many total Gibson's did you hack?

1094795585 71 Points

No. But I hacked thousands of gibsons.

veritaba 17 Points

Can you crack 128-bit RSA at gunpoint in a minute while getting a blowjob?

samagon 3 Points

A blow job from the guy waving the gun in your face?

Booster21 34 Points

HACK THE PLANET!

TheMightyDane 8 Points

They're trashing our rights, man. TRASHING.!

thornae 15 Points

Related: What did you, as a genuine hacker, think of Hackers? Or Sneakers?

1094795585 13 Points

Entertaining movies. But my reaction was similar to the reaction a doctor has when confronted with some medical drama series, it's very far from reality ;)

realmadrid2727 8 Points

Holy shit man, it's Zero Cool!

mattindustries 12 Points

I thought he was black.

cup 43 Points

I have no computer background and 'hacking' always piqued my interest especially as I had no clue as to how the hell it worked. I read magazines like 2600 to try and glean information but no luck. So the question is:

How does one begin to get to a level where you were, hacking into computers. I'll leave a disclaimer saying I have no intention to hack into anything, computers are not my forte. It's just a curiosity.

Regards.

1094795585 49 Points

The way I got started was that I saw a documentary about hackers at defcon, they were interviewing one of the top teams in the CTF and I thought they were completely awesome. So I looked them up and mailed the leader, asking how to become a hacker. He told me to buy "Hacking Exposed" and read it from cover to cover 5 times, then I would begin to understand how it is possible to hack into computers. It's a pretty basic book, it mostly covers specific hacking techniques but also introduces some concepts like buffer overflows. Then you just need to experiment and read, hacking is a lot about experience, you can't learn everything from a book.

Signal 31 Points

What would you recommend for someone interested in starting out today? Is "Hacking Exposed" still relevant, or are there more up to date books / guides?

1094795585 19 Points

It is still relevant. The basic layout of a "hack" hasn't changed.

eco_was_taken 6 Points

You went to DefCon before you had read anything about hacking?

1094795585 21 Points

Nope, tv.

Notmyrealname 20 Points

Do you pay for cable?

Isvara 25 Points

Learning to write software would be a good start. The more you know about how software works, the better chance you have of exploiting it.

For example, if you learn, say, how to write a dynamic web site with PHP, then SQL injection, cross-site scripting and cross-site request forgery will make sense to you. Go a bit deeper, and actually understand HTTP, and you will better understand things like HTTP header

splitting.

If you then learned C, and how programs and data are laid out in memory, you'd be able to understand buffer overflow attacks and heap exploits. Once you get really into how your source is compiled and executed, you'll understand things like integer overflows.

Of course, there are other avenues, but I'm more of a software guy than anything else.

> **im_a_mac** 13 Points
>
> Here is a great site for much of those concepts.
>
> *edit: Why am I getting downvoted? Is milw0rm not a good site? I used it almost exclusively for a security class in college.
>
> > **Pacolaco** 20 Points
> >
> > It's considered to be for 'script kiddies'

johntheripper 15 Points

I consider myself a security professional. I have broken sites, manipulated web applications and rooted personal boxes. How did I start? www.hellboundhackers.com Give it a try, honestly. From there, head over to packetstormsecurity.com and just start reading. While you're there, look for any articles by TeamQuarantine (thats us). Good luck, and feel free to PM me if you feel like chatting/asking questions.

> **Fiend** 9 Points
>
> > www.hellboundhackers.org
>
> FTFY.

iameric 16 Points

Did you do any social engineering?

> **1094795585** 9 Points
>
> No.

lcaldas 9 Points

Have you ever created a GUI interface in Visual Basic to see if you can track an IP address?

> **1094795585** 20 Points
>
> How else would you track an IP address?
>
> **just_quit_smoking** 2 Points
>
> A Graphic User Interface interface?

TheRiff 8 Points

What would you do for a Klondike bar?

> **ReiToei** 4 Points
>
> W-w-would you kill a man?
>
> **antardis** 2 Points
>
> It's something more than one person wants to know.

mikm 24 Points

Without naming specifics, how big was your highest-profile target?

> **1094795585** 55 Points
>
> Fortune-500-big. NIPRnet-big.
>
> > **Signal** 5 Points
> >
> > You hacked government networks? What was your motivation? Didn't you consider what kind of shit you could get into?
> >
> > Was it before Guantanamo and water-boarding and all that stuff happened?
> >
> > > **mossblaser** 22 Points

> You hacked government networks? What was your motivation?

The fact that you are surprised about the target answers the question. Why visit the moon? "Because it is hard".

1094795585 22 Points

Exactly, because it is hard and "dangerous". I did not consider the amount of shit I could get into.

avnerd 5 Points

if you had known then what you know now - would you have been more careful or would you have not hacked at all? or better said - *is it better to have hacked and lost than to never have hacked at all?*
also, what are you studying now?

1094795585 9 Points

> if you had known then what you know now - would you have been more careful or would you have not hacked at all?

I would have been a lot more careful.

> is it better to have hacked and lost than to never have hacked at all?

It is better to have hacked and lost than to never have hacked at all, even though it slightly fucked my life.

> also, what are you studying now?

Computer science.

avnerd 2 Points

In studying computer science what is it that you most want to learn?

LightShadow 2 Points

Are you studying CS just for the degree, or are you actually learning something?

foobar83 2 Points

CS is a lot more than just knowing how to exploit a buffer overflow. There will always be something new and interesting to learn as long as the subject interests you.

qgyh2 22 Points

Typically, how secure are modern web sites?

1094795585 57 Points

Not very secure. SQL-injections are *everywhere*.

movzx 56 Points

Oh my god! There's one over there, run!!

reseph 67 Points

pulls pants up My bad.

PhilxBefore 14 Points

Sequel Injection != Semen Ejection

epiph 21 Points

just wait till web 3.0

CockBlocker 2 Points

What about sausage?

PhilxBefore 2 Points

Not this time, Mr. Blocker.

CockBlocker 2 Points

And I would have gotten away with it if it wasn't for that pesky PhilxBefore!

timeshifter_ 5 Points

That's kinda depressing, actually.. I'm a web dev, and SQL injection is pretty easy to protect against...

1094795585 6 Points

Yep. Which is why it's so surprising that it's as common as it is.

qgyh2 21 Points

Have you considered getting a job with a security company? you definitely have the skill needed and you would probably easily make good money

1094795585 23 Points

I have considered it but it's not something for me. I strongly dislike the security industry.

Isvara 25 Points

I worked in the security industry. What do you dislike about it?

1094795585 27 Points

I think has become less about knowledge and innovation and more about hype. Extreme hype. Everyone wants to make money off their name. Bugs become a commodity that is sold to companies that charge subscription fees for advance notice, etc..

laberge 7 Points

No doubt, so why don't you become that security dude without the hype and just deliver on the promise... at a high cost? ;)

1094795585 26 Points

I think there is more to life than money. I could compromise some of my beliefs to make post-conviction life easier, but I won't.

yoscar 11 Points

A tear dropped off my eye just by reading your response. You, sir, have just become my hero.

qgyh2 14 Points

which country are you considering moving to? would you work in computing there?

1094795585 16 Points

I am not sure. New Zealand seems like a nice place. I'll most likely work with computers.

kitsuneudon 11 Points

As an American ex-pat programmer in New Zealand, I can highly recommend it. Given that you still want to work with computers, perhaps have a look over http://seek.co.nz to get a feel for the job market here.

Wellington is largely considered to be the heart of the IT industry in New Zealand. Fortunately it's also a nice place to live! Auckland however I would avoid! :)

1094795585 4 Points

Thanks.. bookmarked that site!

redrobot5050 12 Points

You do realize its going to be 10x harder to emigrate to this country as a convicted felon, right? Even Canada probably wouldn't let you in.

Abe_Frohman 10 Points

Pffft, he's a hacker! He'll be travelling on a government jet with diplomatic immunity with a few keystrokes.

samagon 2 Points

It's just been revoked.

Narwhales 9 Points

That's not true - Canada has an application process for us 'buddies' that are a bit tainted, victimless/non-violent crimes that are 5+ years in your past with no 2nd offenses of any kind usually get approved. Same goes for most other countries

tiktaalink 14 Points

How does the famous qgyh2 know about 1094795585's skill level? Unless... it couldn't be....

They've never posted at the exact same time. By gosh qgyh2 is 1094795585.

and to think they would have gotten away with it if it weren't for those pesky kids.

wuzzup 2 Points

FINKLE IS EINHORN!!!!

Signal 6 Points

I predict tiktaalink's comment will disappear mysteriously.

1252941367 18 Points

what's significant about 2004-09-10 01:53?

1094795585 7 Points

See my reply above..it's not a timestamp ;)

infinite 12 Points

Back in my day, there was no caller ID so life was pretty good for hackers like myself.

How in the hell do you avoid getting caught? Do you go to a public library and use the internet there? But then they can trace your IP and you're a target. Seems kinda risky.

Also, have you written any stack overflow exploits or any such exploits? Have you discovered any holes?

I have a server with only 2 ports open. One of them being tomcat port 80 which requires a login to do anything, the other ssh with only 1 user allowed to login, assume all passwords are randomly generated. It blocks your IP after 3 failed login attempts. How are you getting in?

Also, what do people use to scan for php scripts, etc?

1094795585 14 Points

> Back in my day, there was no caller ID so life was pretty good for hackers like myself. How in the hell do you avoid getting caught? Do you go to a public library and use the internet there? But then they can trace your IP and you're a target. Seems kinda risky.

Nowadays wireless networks are everywhere. Combine that with something like tor and I'd say you are pretty anonymous.

> Also, have you written any stack overflow exploits or any such exploits? Have you discovered any holes?

Yes, I've written exploits for most types of bugs. Buffer overflows, format strings, int overflows. I have discovered some holes myself. Nowadays the most popular thing to audit is webapps. The age of remote root holes in popular ftpds is gone.

> I have a server with only 2 ports open. One of them being tomcat port 80 which requires a login to do anything, the other ssh with only 1 user allowed to login, assume all passwords are randomly generated. It blocks your IP after 3 failed login attempts. How are you getting in?

I hack the computer you are logging in from.

> Also, what do people use to scan for php scripts, etc?

Google. "inurl" + "site"

doomstork 15 Points

What tools do you use?

MagikalGoat 25 Points

Password Cracker v4 + Trace tracker v4

SidewaysFish 17 Points

If that's the Uplink reference I think it is, you win an orangered envelope.

1094795585 11 Points

And a voice recorder. They are essential when hacking banks.

benplaut 2 Points

That sounds interesting... explain?

1094795585 6 Points

It was just a reference to Uplink ;)

1094795585 32 Points

Exploits, network scanners, rootkits, google (perhaps the best network scanner).

avnerd 2 Points

how do you use google as a network scanner?

celticninja 2 Points

I note that the question was present tense, was the response supposed to be?

accidentallywut 3 Points

a GUI interface made in VB. custom stuff. made for tracking IP addresses on blogs and whatnot.

riggariggarigga 14 Points

I work in the IT industry. I am curious if there is anything that we can do to protect our computers\networks from guys like you. Is there anything we can do? If you some how WANT to get into our network is there anything that CAN stop you?

1094795585 22 Points

In short, if you have a network that is connected to the internet and someone wants to get in, they will eventually get in. If you are running the latest versions of all possible software you might think you are safe. But what if someone comes along with a 0day, or someone hacks the home computer of one of your administrators?

KingOfSwords 14 Points

What is a 0day?

wastedfish 25 Points

It's a term for an exploit that has just been created. Hence the '0' day. Meaning it hasn't even been around for 1 day yet.

xbrand 10 Points

Not exactly. 0day means that there have been zero does for the whitehat security industry to respond to the threat after being notified of it. It basically means an exploit that exists that the maintainers and "good guys" don't know about yet to fix.

ColinSmiley 9 Points

http://en.wikipedia.org/wiki/Zero_day_attack

mossblaser 7 Points

How many of your break-ins relied on social engineering or were they all purely technical. (i.e. do organisations need to take more care of keeping their staff aware?)

If some were social engineering, to what level and to which staff? Do you break in at the top or go in near the unsuspecting minions at the bottom?

1094795585 7 Points

I never did social engineering.

riggariggarigga 6 Points

I have always figured that. So basically put our head between our legs and kiss our ass goodbye.

apage43 10 Points

Still, you -should- keep everything up to date and follow good security practices. This will keep out people who aren't specifically targeting you.

As for targeted attacks, avoid keeping sensitive data on internet-facing systems, and thoroughly monitor the border between your internet facing systems and your sensitive systems. Use remote logging so even if a system is compromised, logs can't be deleted without compromising the log collection system. You can never be 100% certain a targeted attacker will not get in, but you can make it VERY difficult to do it quietly.

anon7002 11 Points

Security is a game and you have to play. You need to make it difficult, make your target less attractive than somebody elses and protect your real assets. Good backup protects against loss but I think the only real way of protecting corporate assets are by classifying your data and basing your security policies on it. We're still focussed on securing infrastructure rather than securing data and all the tools in the world struggle to understand the real value of data. We protect the eBusiness server but we forget about the back-end Database server, we don't encrypt data, we don't audit database access at the row or column level because it's difficult. We deploy firewalls, IDS, packet-sniffing gizmos but do nothing to stop people copying and pasting screenshots from their ultra-secret databases and sending them to a Hotmail account. And then we say we're doing a fantastic job because we stopped 96% of spam (with an off-the-shelf tool) and we didn't appear in the press this week.

In my experience, IS Security just needs to grow up. You will get hacked if your data is valuable and somebody can be bothered to outwit you. Sadly, most security systems can be easily bypassed through user stuipidity and social engineering and many simply achieve security through obscurity which is a poor defense to a seasoned professional.

riggariggarigga 4 Points

I agree. You can only add layers to your security ideology. Make it hard, make it take time. Perhaps then they will pass you by. I personally think that there is too much emphasis placed on buying the right security product. Security is all about adjusting internal processes and adjusting existing product to make it difficult. (IMHO)

Doing security right and making your system easily accessable for users are not mutually inclusive. By securing your network and computer systems IT WILL make using them a bigger pain in the ass for your end users. All it takes is one bad security decision and you are owned.

Hey 1094795585 thank you for the interesting discussion it made me remember why I like Reddit.

kitsuneudon 4 Points

I'm a web developer, so my knowledge is somewhat limited to that area, but in terms of securing web applications and web severs http://www.owasp.org has pretty much everything you need to know.

Leprecoon 17 Points

Are you forbidden from using computers or anything like that?

1094795585 26 Points

No, you can't forbid someone from using computers where I live.

DamienWind 9 Points

What country are you from? Can you say?

jwilke 5 Points

> Why would he risk violating parole to post an AMA?

michaelwsherman 6 Points

Can you give more details about what happened when you were raided? How scared were you? Did they just walk into your house and start taking your stuff? What time was it? Did they arrest you when you were raided? What was your family doing? What did they take that wasn't yours. How long (if ever) until you got stuff back.

Also, I'm curious what OSes you consider the most and least hackable. I saw some comments about this in the thread, but I'd be curious if you could say some more.

1094795585 10 Points

> Can you give more details about what happened when you were raided? How scared were you? Did they just walk into your house and start taking your stuff? What time was it? Did they arrest you when you were raided? What was your family doing? What did they take that wasn't yours. How long (if ever) until you got stuff back.

My parents weren't home. I opened the door and there were about 6 men with briefcases. I knew I was screwed. I can't say I was especially scared, I didn't start crying or so and was very calm. They sat down at my computer and copied data (I had forgotten to lock it the night before..). Then I was taken to the police station for questioning, when I came back they had loaded most of my stuff into their vans. They took everything that had ever been in touch with an integrated circuit. Even my mother's Celine Dion CDs. Most of the stuff was returned, but I never got my computers back.

> Also, I'm curious what OSes you consider the most and least hackable. I saw some comments about this in the thread, but I'd be curious if you could say some more.

Personally I use Linux. I don't consider Linux especially secure, just look at the number of local kernel root vulns found in the last year. I do however know that this is because there are so many people auditing Linux every day. I'd rather use an OS that has a few serious public vulns each year than one where the vulns are still there but aren't found.

lowbot 13 Points

How would you advise someone like you to avoid this fate? For instance there's probably a young hacker reading this, what would you tell them? What better and more rewarding ways are there to use their skills and curiosity?

1094795585 28 Points

> How would you advise someone like you to avoid this fate?

I would advise them to use tor and not brag about their feats. Also, never get sloppy.

> What better and more rewarding ways are there to use their skills and curiosity?

Personally I am a blackhat. I loathe the cesspool of inflated egos that is the computer security industry. Therefore, I would never ever advise them to become "whitehats". As for a more rewarding way to use their skill and curiosity, I can't think of a good answer. Hacking into computers is simply the most rewarding experience I have ever had. I don't see it as a problem if you are hacking big companies or governments for the sake of adventure, you are not out to hurt people.

Just make sure not to make money from your hacking, be it selling out to the security industry or selling botnet-stuff to russians. Both will destroy your passion.

stutheidiot 10 Points

> Hacking into computers is simply the most rewarding experience I have ever had.

Assuming you have a penis, have you ever tried putting it in a woman's vagina?

mrwynd 27 Points

> In my experience people who make this joke usually haven't.

1094795585 16 Points

> Yeah, it was pretty cool!

> stutheidiot 21 Points

> Not quite so rewarding as penetrating a tight network, probing and easing past that initial resistance until finally it embraces your presence and succumbs to your will, though?

> **1094795585** 15 Points

> I couldn't have put it better myself.

yoscar 4 Points

After reading your responses, it seems as if you have hatred towards big companies, as well as just the curiosity of simply hacking into whatever is available, just for the thrill. You also seem to have the idea of doing it for fun, mentioning that "Money isn't everything in life".

What is, then, your "political" affiliation? It always interested me how the best programmers were always prone to giving away their source code, to help the community, and just to improve the software industry overall. I have always assumed that most (if not all) hackers are anarchists; can you confirm/deny this? Or are hackers just too disconnected or upset with the world that they focus solely on programming, or on the internet?

cookiecaper 11 Points

Did you do anything malicious when you entered these computer systems? i.e., deface, replace or remove websites or other important data? Was it just for the thrill of reading someone else's confidential information?

Were you hacking into government systems? Did you learn anything cool or worthwhile while doing so?

How did you find exploits, or did you just use already known exploits?

Were you involved and nailed for any activity besides illicit access to computer systems? Piracy, etc.?

Were you charged with anything you're not guilty of? If so, were you convicted or acquitted?

How was your family affected by the raid?

Were you treated leniently because you were a juvenille? Is your record sealed or expunged such that it doesn't appear to employers?

How long ago did this happen?

> **1094795585** 60 Points

> > Did you do anything malicious when you entered these computer systems? i.e., deface, replace or remove websites or other important data? Was it just for the thrill of reading someone else's confidential information?

> I only defaced a website once, simply because it was too high-profile not to deface.

> > Were you hacking into government systems? Did you learn anything cool or worthwhile while doing so?

> Yes. I found some cool stuff. No ufos though.

> > How did you find exploits, or did you just use already known exploits?

> I'd lie if I said I didn't use exploits written by others. You can't have a personal toolkit for every possible software. Sometimes I had real 0day months before the vulnerability was made public (mostly due to sloppy hackers leaving exploit binaries...gluck.debian.org comes to mind). I find bugs by reading code and fuzzing.

> > Were you involved and nailed for any activity besides illicit access to computer systems? Piracy, etc.?

> No. I had a lot of warez on my computer but that wasn't what they were looking for.

> > Were you charged with anything you're not guilty of? If so, were you convicted or acquitted?

One intrusion charge was completely false, and was dropped, because no intrusion had taken place.

> How was your family affected by the raid?

I was living at home and they took every electronic device in the residence. I wasn't very popular. After the initial shock had worn off they supported me, it wasn't as if I had raped and murdered a girl in 1990.

> Were you treated leniently because you were a juvenille? Is your record sealed or expunged such that it doesn't appear to employers?

If I was older I probably would have gotten a year in jail. This is on my record and will be for a long time.

> How long ago did this happen?

In this decade.

itsnotlupus 36 Points

> No ufos though.

Thank you for respecting your plea agreement.

mikm 10 Points

> > Were you hacking into government systems? Did you learn anything cool or worthwhile while doing so?
>
> Yes. I found some cool stuff. No ufos though.

So who really killed Kennedy? ;)

mrtepi 15 Points

It wasn't a conspiracy, it was just brain cancer.

c000gi 11 Points

exploding brain cancer

watwat 7 Points

Explosive brain cancer.

hatter 4 Points

> it wasn't as if I had raped and murdered a girl in 1990.

thank you for this.

tugteen 6 Points

erm, like, what KIND of cool stuff?

billwoo 5 Points

> Yes. I found some cool stuff.

Aren't you tempted to become a 'leaker' (that the right term), and expose governmental corruption, cover-ups etc.?

eco_was_taken 8 Points

Can you describe your most proud hack? What kind of exploit was used? What was the whole process like from start to finish?

1094795585 28 Points

1) Find a custom admin interface.

2) Get read access to a db from an SQL-injection.

3) Find tables corresponding to the custom admin interface.

4) Crack the admin password.

5) Log in and upload a new picture, containing PHP.

6) Exploit buggy custom cron-scripts that delete directories in /tmp once a day.

7) Wait for exploit to trigger..

8) Infect a binary on an NFS-share.

9) Wait for someone to use the binary..

10) Enjoy access to the main servers.

Something like that ;)

orbifold 9 Points

Have you learned afterwards how you were caught, considering you did enough measures to hide your identity? I was thinking it was your IP that give you out, but I may be too naive.

1094795585 15 Points

Yes, they undertook an extensive trace.

crocowhile 11 Points

how extensive? how many connections between you and the victim? People say #1 rule is never hack from home, right?

1094795585 10 Points

It's a pretty good rule, and I broke it. I had about 7 steps between me and targets.

enkiam 7 Points

You never hack a bank across state lines from your house, man, that'll get the secret service on your ass.

diversionmary 7 Points

Unix timestamp 1094795585 Fri, 10 Sep 2004 05:53:05 GMT

5 yr statutory limit?

im_a_mac 16 Points

PDF explanation

It is what the EIP register contains when overflowing a buffer with A's (x41) using strcpy(). If you can insert a valid memory location into the EIP register, you can jump to your code and start executing it.

Forgive my terrible explanation, but I have not visited the low level world since taking my job as a .Net developer.

*edit - spelling

Signal 7 Points

41414141

1094795585 10 Points

It has a special place in the heart of every exploit writer. It's clearer in a different base..

dave_L 9 Points

> ...will likely leave for a different country when I am done with my studies, to start a new life.

When that time arrive, would you be interested in seeking opportunities in the Far East? And if so, will an academic/research environment pique your interest?

EDIT : Typo

1094795585 12 Points

It's possible, I'm not sure. All I know is that I want to work with computers but I don't want to work for a computer security company. Network/system administration, programming.. I'll probably end up doing something like that in the future.

conorp 13 Points

I think he was offering you a job.

billwoo 8 Points

You mentioned above that you do not feel bad about causing extra work for admins due to hacking into their systems. If you go to the other side of the fence do you think your attitudes will change when you are cleaning up after other peoples hacking attempts, or do you not think it will be an issue?

1094795585 17 Points

If someone would cleverly defeat my setup, I would respect that. On my private server I actually have a text file in /root that is specifically to be read by anyone that manages to root me.

moderndogs 4 Points

There's no way that I would ever read that text file as a non-hacker, but would you mind sharing what it says? I'm mad curious

dem358 4 Points

I got so very curious...Will you please keep it there for the next few decades,till I learn how to hack into computers? I think I've finally found the aim of my life, something I have been searching for since years: to read 1094795585's text file! I'll do whatever it takes.

gatsby137 9 Points

Don't bother. All it says is "The princess is in another castle."

kraemahz 4 Points

It sounds like he'll probably see it like a game of chess.

accidentshappen 2 Points

Have you ever considered contributing to the Wikileaks site document wish lists?

A lot of documents out there that could be interesting, ranging from Operation Gladio to whether Osama is still alive or not.

Also, was 911 an inside job? :)

impendingdoom 11 Points

If you didn't do it for financial gain, that what was the incentive? Did you work alone or were you hired by someone?

1094795585 27 Points

The incentive was the thrill of breaking into something that could sometimes have taken over a month of preparation. Looking at information that you weren't supposed to be looking at. I suppose it's the same feeling you get when solving any complex problem. It's better than sex. I mostly worked alone, and I was not hired for anything.

tugteen 6 Points

sort of like safe crackers and lock pickers, they just do it because it a complex barrier or puzzle

mbtbh 9 Points

Maybe a silly question: Did you know you got caught before you got contacted by the Police(Assumingly)? As in 'Uh oh, maybe i shouldnt of done that, bad feeling about this one'

1094795585 22 Points

Yes. My hacking was getting a bit out of control, the last months I was basically hacking into stuff every waking moment that I wasn't in school. About 3 months before the police came I was tipped off about a possible raid. This freaked me out and I hid my encrypted harddrives at my grandmother's place. Sadly, after a few weeks I got comfortable again and retrieved them..

cookiecaper 8 Points

Did they retrieve the data off of those hard drives? If so, did they find your keys somewhere? Did they compel you to provide the passphrase?

1094795585 12 Points

The night before they came I had dozed off without locking my computer. One of my encrypted drives was open. They tried to get me to divulge the key for the other drive but I didn't comply.

cookiecaper 10 Points

So ... did they ever get the data off of that?

Was your non-compliance wholly independent or on the advice of a lawyer? Don't they have methods to compel the divulgence of that information? Weren't you scared?

What kind of encryption did you use?

1094795585 13 Points

No, they never got the data from the locked drive. My lawyer advised me to ignore their requests, but I realized that was the best approach even before his advice. I used AES with a ridiculously long password.

eatadonut 6 Points

Do you have a favorite password-choosing technique?

1094795585 27 Points

Think of some good passwords that you can remember. Then combine them.

Pacolaco 5 Points

That's what I do, wooooooooo! My encryption password is actually 8 separate passwords. It makes it very easy to memorize 80+ character passwords.

onshouldersofgiants 3 Points

Is it passwordpasswordpasswordpasswordpasswordpasswordpass

downvote_seeker 2 Points

Very true. My passwords only ever get longer. Even if one has been compromised, it's still a perfectly valid salt for the next password.

n8r0n 6 Points

How often did you encounter honeypots? How easy was it for you to detect them?

sahila 4 Points

If you wish to, would you be able to hack into online gambling software? More specifically, is it possible to hack poker, like fulltiltpoker.com, and gain an advantage over the ordinary user? I wonder because millions of users put hundreds of dollars on them with the expectation that they are completely fair.

1094795585 6 Points

Yes, since they have computers running in the background it is completely hackable. Even your bank statement is stored on a computer somewhere. If someone switches a few bits in a database, you can go withdraw thousands of dollars, just like that. People put far too much trust in computers, and now they are everywhere.

Nacht 7 Points

What do you think about this guy?

1094795585 12 Points

I think it would be a shame if he was extradited.

thebassethound 8 Points

Mega-understatement.

pinchyfingers 2 Points

Which targets are generally more difficult, corporate or government systems?

jeremybub 5 Points

Did you ever hack a computer twice by accident? Did you ever hack a computer someone else already had control of? What about vice versa?

> **1094795585** 7 Points
>
> Yes. On a few occasions I would hack a server only to discover that a friend had already installed a rootkit on it.
>
> A much more common thing would be to find eggdrops (irc bots) belonging to scriptkiddies. I would then carry out some forensics (they don't hide their presence very well) and proceed to steal their "roots" for my own use.
>
> > hokkos 3 Points
> >
> > Did you ever hack YOUR computer ?

quick_witted_ 1 Point

Did you use existing hacking tools (back orifice, scripts, etc) or did you write programs (in C, etc) doing your own research into the OSes and systems you were hacking and invent new exploits?

chillagevillage 2 Points

Can I have my credit card info back?

asdasd777 4 Points

I have a Linux server with apache/nginx/mysql/php and postfix. Which basic advice can you give to protect it? Which kind of security software would you use? What would be your perfect setup for a webserver?

Was you ever approached by some criminal organizations?

Could you hack reddit?

> **1094795585** 8 Points
>
> > I have a Linux server with apache/nginx/mysql/php and postfix. Which basic advice can you give to protect it? Which kind of security software would you use? What would be your perfect setup for a webserver?
>
> Make sure whatever PHP software you are using is always up to date. PHP stuff has a tendency to be written very poorly. Install some custom hardening patches like Grsec.
>
> > Was you ever approached by some criminal organizations?
>
> I was approached by criminal people, they were probably affiliated with an organization.
>
> > Could you hack reddit?
>
> I didn't try. I'm sure the website code itself is pretty good, I'm a big fan of Python. It's much easier to write insecure software in PHP than in Python.

binary 2 Points

Would you discourage similar practices from youth? I've been dabbling in hacking--as you define it--for a while now, mainly as a way to learn more about the intricacies of computers and servers. As of yet I still consider myself an extreme novice, and I think the more I try the better I get.

Additionally, how dedicated were you to learning and how long did it take you to reach that level of skill?

iamah 4 Points

What are the best measures to clean your own traces today?

rhoffer21 2 Points

Im in my second year of an IT degree and I have learned quite a few programming languages, but I can't seem to get over that 'hump' of knowing the basic syntax well to creating useful apps. Any advice? As an example, I know PHP pretty well but I haven't really created anything worth showing anybody. Thanks,

1094795585 5 Points

Try to think of some application that you'd like to make, and then just start programming. If you can think of something, you can make it, but experience will dictate how long it takes to finish and how good the result will be. If you code enough, eventually you will just "get it", and language specifics like syntax won't matter.

searchon 2 Points

How will they let you leave the country if you owe them fines from the conviction?

1094795585 2 Points

I live in a free country, so that won't be a problem.

buzzard_nuts 5 Points

If teenagers can figure out how to hack into systems what chance do we have against well funded sources that want to do real harm?

1094795585 22 Points

Not a very big chance. Personally I think that there are government agencies in the US, China, Russia etc. that have already backdoored each other to hell and back.

benediktkr 6 Points

Is it true that there are groups of organized crime interested in people like you? And that they are willing to pay a hefty fee for root on e.g. sourceforge.net?

1094795585 8 Points

Yes, I've had people offer to pay me for shady services. I never accepted though.

rumbleminz 5 Points

My neighbor was one of the first ones to be convicted under the federal hacker laws in the 80s. Got into the DoD among other things.

Served time too.

Herbert Zinn, the 'shadowhawk.'

Great fucking guy.

1094795585 6 Points

I sometimes curse the fact that I was just a toddler in the 80s.. it seems like it was a fun time to be a hacker.

fortytl 2 Points

Your username is much more awesome when converted to hex....