

Forum:[Hack Forums](#)

Thread: [== SECRECY == >>> BEGINNER HACKING HELP DESK <<<](#)

Dr. Gonzo - July 22, 2017, 1:03 pm

Introduction

Thank you for clicking on the thread. A few members from the group Secrecy will be running this help desk.

We will aim to assist you with everything hacking related along with providing any external opinions or software that we deem necessary.

Contributors

Pronouncer

Great White Shark

Baud

Recommended Reading

[How to unskid yourself](#)

[The COMPLETE beginners guide to hacking](#)

[.-* Biggest Hacking Tutorials Compilation on HF \[All you need to know\] -.](#)

[.- Biggest Hacking Tutorials Compilation on HF \[PART 2\] *-.](#)

[\[Nightmare\] Choosing a Language v1.0](#)

[Compilation of White Hat Guides :: Navigation](#)

Beginner Hacking

Feel free to ask anything related to:

Linux

Webhacking

Malware

Encryption

VMs

Coding

Social Engineering

Cracking

Public Exploits

Penetration Testing

Enumeration/reconnaissance

Port Scanners

Networking

Privilege Escalation

White Hat Hacking

Security, Anonymity & Privacy

WIFI

Rules

Please ask all questions in a legal or theoretical manner.

Please be respectful to the contributors.

Do not spam or ask any troll questions.

Obviously HackForums Rules still apply.

FAQs

Q. Where should I start?

A. There is a lot of debate about this, but I always recommend new users start with Linux on a VM and start learning the command line and then learn about networking and start testing Nmap commands on vulnerable VMs like Metasploitable2. But also check out my recommended reading list above

Q. How do I hack [Insert social media] account?

A. Find a cracking tool like SentryMBA, get a config for it, get proxies, get a combo list or a word list.

Q. How do I stay anonymous

A. Although complete and full anonymity is impossible I'd recommend you look into a good log-less VPN, start using tor for browsing simultaneously and that should keep you safe for MOST applications. If you're doing anything crazy you'll want to look into more advanced OpSec setups.

[== SECRECY == >>> AN INTRODUCTION TO VPN'S <<<](#)

Thank you for taking the time to read this thread. We appreciate your effort and look forward to helping you out. If you are interested in joining us please read this thread.

<https://hackforums.net/showthread.php?tid=5673489>

Pronouncer - July 22, 2017, 1:04 pm

Thank you for taking the time to post this, he is one of our finest members

Baud - July 22, 2017, 1:12 pm

I'm more than glad to be part of the helpdesk, to anyone who is considering posting a question: make sure you read the rules!

Faith Connors - July 22, 2017, 1:53 pm

thanks for adding my thread <3
appreciate it

i guess you guys will take over my last one lol

Dr. Gonzo - July 22, 2017, 1:59 pm

(Jul 22, 2017 01:53 PM)Faith Connors Wrote: [CITE](#) thanks for adding my thread <3
appreciate it

i guess you guys will take over my last one lol

Yeah Feel free to help us answer questions on here, you've definitely proven your knowledgeably.

mutybyte - July 22, 2017, 8:41 pm

Thanks for this helpdesk thread

I want to ask something

I have setup my kali linux 2017.1 in vmware and installed necessary things. Now i want to know how i can make vmware image of that file like offensive security make ?

Dr. Gonzo - July 22, 2017, 9:07 pm

(Jul 22, 2017 08:41 PM)mutybyte Wrote: [\[CITE\]](#) Thanks for this helpdesk thread

I want to ask something

I have setup my kali linux 2017.1 in vmware and installed necessary things. Now i want to know how i can make vmware image of that file like offensive security make ?

Good question. You're actually in luck because when you install kali linux from an iso on any hypervisor (virtualization software) it goes into a virtual disk that you can move around. However, there will be configuration files that come with it and you'll want to keep those. So locate the folder that your virtual disk (likely in whatever directory you installed vmware in) is in and keep all the files with it and bam you have your already made "vmware image".

I hope I understood your question correctly, If not feel free to rephrase and ask again. Also If you have follow up questions don't hesitate to ask.

mutybyte - July 22, 2017, 10:29 pm

What i am doing actually is save that folder [/users/myname/virtual machines/kali pentesting] in my external hard disk.

So when ever i visit to another location i kept my external hard disk and when i see another computer then i use external hard disk and use that kali linux in another computer's vmware just by using "open" option.

Dr. Gonzo - July 22, 2017, 10:46 pm

(Jul 22, 2017 10:29 PM)mutybyte Wrote: [\[CITE\]](#) What i am doing actually is save that folder [/users/myname/virtual machines/kali pentesting] in my external hard disk.

So when ever i visit to another location i kept my external hard disk and when i see another computer then i use external hard disk and use that kali linux in another computer's vmware just by using "open" option.

Yep, that works too. I had to do it like that for a class once. Again, let me know if you've got any other questions ?

mutybyte - July 22, 2017, 10:56 pm

i just want to know this ->

<https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

is that file already have some preinstall tools other than kali tools which is already available there. Like some important tools created in python which is hosted in github. Are these tools additionally available there ?

If so i also want to make such image file.

Also i don't know much depth in linux just very basics in linux though i want to learn to develop our own linux/customize our own linux

Dr. Gonzo - July 22, 2017, 11:55 pm

(Jul 22, 2017 10:56 PM)mutybyte Wrote: [\[CITE\]](#) i just want to know this ->
<https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/>

is that file already have some preinstall tools other than kali tools which is already available there. Like some important tools created in python which is hosted in github. Are these tools additionally available there ?

If so i also want to make such image file.

Also i don't know much depth in linux just very basics in linux though i want to learn to develop our own linux/customize our own linux

No the VMware specific image doesn't have more than the standard ISO image you used.

If you would like to develop your own linux I'd suggest you learn more about the basics of linux such as the file hierarchy system, bash syntax and package management before learning about the nuances of kernel development.

However, from what I am sensing you actually just want to add tools and change the way the desktop environment looks. For this you simply need to look into changing gnome themes(or changing Desktop Environments altogether) and learn how to install new software using apt-get.

Zens - July 23, 2017, 12:21 am

wow, great thread. really helpful.

mutybyte - July 23, 2017, 3:18 am

Ok got it.

Now i want to know about ---->

How i plan to make notes/ organize notes while solving vulnhub machines,solving overthewire war games?

Please point out to beginners to how to start and keep notes while solving such things. Like making documentation etc etc.

I am bad in expressing my thoughts but i think you get my question

Baud - July 23, 2017, 4:19 am

(Jul 23, 2017 03:18 AM)mutybyte Wrote: [\[CITE\]](#) Ok got it.

Now i want to know about ---->

How i plan to make notes/ organize notes while solving vulnhub machines,solving overthewire war games?

Please point out to beginners to how to start and keep notes while solving such things. Like making documentation etc etc.

I am bad in expressing my thoughts but i think you get my question

So you want to know how to keep your notes organized? I find this to be very subjective, everyone finds themselves comfortable in their own different way but what I think most people do is simply keeping your notepad open and writing down all the useful info you find out about your target. You may for example end up having something like this after conducting a couple scans:

Code [BASIC DATA]

IP: aaa.bbb.ccc.ddd

Domain: your_victim_domain.com
DNS 1: dns.victim_domain.com
DNS 2: dns.victim_domain2.com
SMTP: smtp.victim_domain.com

[SCAN DATA]

Open port:	Service:
22	SSH - service_name 1.4.8
80	HTTP - service_name 9.3.6

[ENUMERATION DATA]

Users list:

Admin
Guest1
Guest2

And so on... I also know people who prefer calculus sheets like Excel to do this, but I always found myself more comfortable with a plain text file.

mutybyte - July 23, 2017, 5:02 am

Thanks tony88 :D

It will be great if others also share their thoughts or can say their own ways for same

Baud - July 23, 2017, 5:05 am

Pronouncer is not going to be online for some time today and because of timezones you may have to wait for a few hours, but they will see your question for sure and give you their opinion. If you have any other questions ask away!

mutybyte - July 23, 2017, 5:45 am

Bug bounty/ bug hunting running nowadays a lot and i think i can earn money before taking oscp because of this. So i ordered wahh book and got. But found this is very huge.

How can i make my career in bug hunting without reading that book ?

I learned basics of html and css till now

Baud - July 23, 2017, 7:34 am

If you want to be good at hunting bugs or become any kind of professional expert you need to study and learn as much as you can, there is no easy or short way or else everyone would do it.

You said you are interested in bug hunting but do you want to focus yourself on web exploitation? If so, you can start studying PHP and JavaScript, these two languages are so widely used that new bugs are always found in PHP and JavaScript code, and obviously if you want to look for bugs you need to have a very good understanding of programming not only to discover the bugs, but also to exploit them.

Since you have no prior knowledge of these two languages you can get started here:

<https://www.w3schools.com/>

And of course read the book because you are going to need it, that was pretty obvious.

mutybyte - July 23, 2017, 8:55 pm

Thanks tony88 sir.

I am confusing about anonymous part. How much percent we can anonymous usig vpn ? Any information to be safe and anonymous at best as we can? What are those ways then?

Also i don't know what proxychains is?port knocking,port forwarded etc

Dr. Gonzo - July 23, 2017, 9:15 pm

(Jul 23, 2017 08:55 PM)mutybyte Wrote: [\[CITE\]](#) Thanks tony88 sir.

I am confusing about anonymous part. How much percent we can anonymous usig vpn ? Any information to be safe and anonymous at best as we can? What are those ways then?

Also i don't know what proxychains is?port knocking,port forwarded etc

VPNS aren't 100% secure because they can still correlate hacking with your Internet activity. This works on pretty much any method of anonymity to a degree. Using a combination of things like VPN, TOR, proxychains (a tool that allows you to string proxies together and run commands through them) will get you the best results. It gets complicated to an almost absurd degree which is why I really suggest you learn the fundamentals first before you get too deep into anything in particular.

Quote:In computer networking, port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports.

Quote:port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

Both of the above quotes are straight from the google featured snippet that I found at the top of the search results after I searched "What is port knocking" and "what is port forwarding" I did this not only to give you the best possible definition but also to prove the point that searching, reading and for yourself is undoubtedly the most important trait of a hacker

mutybyte - July 23, 2017, 10:07 pm

(Jul 23, 2017 09:15 PM)Great White Shark Wrote: [\[CITE\]](#) VPNS aren't 100% secure because they can still correlate hacking with your Internet activity. This works on pretty much any method of anonymity to a degree. Using a combination of things like VPN, TOR, proxychains (a tool that allows you to string proxies together and run commands through them) will get you the best results. It gets complicated to an almost absurd degree which is why I really suggest you learn the fundamentals first before you get too deep into anything in particular.

Both of the above quotes are straight from the google featured snippet that I found at the top of the search results after I searched "What is port knocking" and "what is port forwarding" I did this not only to give you the best possible definition but also to prove the point that searching, reading and for yourself is undoubtedly the most important trait of a hacker

I got it and i admit that for that i didn't use google. But i will use google from now for everything which i wanna ask here first i try google. because google helped me a lot

Voqet - July 23, 2017, 10:07 pm

Beginner*. Please Edit... my OCD is kicking in mate

Dr. Gonzo - July 23, 2017, 10:24 pm

(Jul 23, 2017 10:07 PM)Voqet Wrote: [\[CITE\]](#) Beginner*. Please Edit... my OCD is kicking in mate
Oh thanks fixed lol. That was there for quite some time.

(Jul 23, 2017 10:07 PM)mutybyte Wrote: [\[CITE\]](#) I got it and i admit that for that i didn't use google. But i will use google from now for everything which i wanna ask here first i try google. because google helped me a lot

Very good google will always be your friend.

Bronze5 - July 24, 2017, 2:35 am

Im doing javascript injections and I made threads about it, but I am still unsure of the language.

The html I was going to hack was-

```
<input type="hidden" name="to" value="sam@hackthissite.org">
```

The code I made/learnt for hacking "hackthissite" was-

```
javascript:void(document.forms[0].to.value="youremail@email.com");
```

Yet the only thing I don't understand is the .to.value. part. Do I make the injection like-javascript:void(document.forms[0] .(enter what name equals) .(enter what part you are voiding)="youremail@email.com"); ??

sorry if this is a stupid question. Thx for making the secrecy btw it rllly helped me a lot cuz i didn't know where to start lol.

mutybyte - July 24, 2017, 3:13 am

Should i take this course to learn PHP -->

<https://coderprog.com/php-essential-training/>

SysAdmin - July 24, 2017, 3:32 am

(Jul 24, 2017 03:13 AM)mutybyte Wrote: [\[CITE\]](#) Should i take this course to learn PHP -->

<https://coderprog.com/php-essential-training/>

CodeAcademy has way better lessons. Try it instead.

Dr. Gonzo - July 24, 2017, 8:18 am

(Jul 24, 2017 02:35 AM)Bronze5 Wrote: [\[CITE\]](#) Im doing javascript injections and I made threads about it, but I am still unsure of the language.

The html I was going to hack was-

```
<input type="hidden" name="to" value="sam@hackthissite.org">
```

The code I made/learnt for hacking "hackthissite" was-

```
javascript:void(document.forms[0].to.value="youremail@email.com");
```

Yet the only thing I don't understand is the .to.value. part. Do I make the injection like-javascript:void(document.forms[0] .(enter what name equals) .(enter what part you are voiding)="youremail@email.com"); ??

sorry if this is a stupid question. Thx for making the secrecy btw it rllly helped me a lot cuz i didn't know where to start lol.I would google the solution to whichever challenge you're working on. Most of the

hackthissite challenges are already out there.

Bed_ - July 25, 2017, 2:44 am

how do i hire a superior trusted coder ?

mutybyte - July 25, 2017, 5:17 am

Today i read some interview of some indian security researchers.In interview when interviewer asked about how they started then i see their reply almost same.

Like they started to learn about RAT,Keylogger etc etc

So i want to ask should i also learn about RAT,Keylogger,doxing ?

Baud - July 25, 2017, 8:02 am

(Jul 25, 2017 02:44 AM)Demonb1 Wrote: [\[CITE\]](#) how do i hire a superior trusted coder ?

Depending on the kind of work you want to do you can either post an ad on other websites or look for users who have expertise in this field in the Code section of the forums.

(Jul 25, 2017 05:17 AM)mutybyte Wrote: [\[CITE\]](#) Today i read some interview of some indian security researchers. In interview when interviewer asked about how they started then i see their reply almost same.

Like they started to learn about RAT, Keylogger etc etc

So i want to ask should i also learn about RAT, Keylogger, doxing ?

Doxing is rarely related to hacking but it can always be useful, it's more useful to private investigators but if you learn how to do that too it's always a skill you can add to your personal toolbox. As for RATs and keyloggers: yes, because you are most likely going to use one one day and that day you may want to know how they work and how to operate them. A lot of people start there because that kind of programs is very easy to use on average compared to other softwares like Metasploit just to name one.

Remember to not be a skid though, always Google things and research what you are doing, learn how RATs work, to do this you need to study networking and TCP protocols, learn how keyloggers work etc... don't limit yourself to downloading tools and executing them without knowing their inner workings, that's skid behaviour.

Pronouncer - July 25, 2017, 11:02 am

Feel free to ask more questions we are here to help

xX_I337_h4x0r_Xx - July 25, 2017, 1:47 pm

hi how to tell if someone is pretend hackerman?? is this guy smart or full of shit
<https://hackforums.net/member.php?action=profile&uid=3652099> ???

Pronouncer - July 25, 2017, 2:04 pm

(Jul 25, 2017 01:47 PM)xX_I337_h4x0r_Xx Wrote: [\[CITE\]](#) hi how to tell if someone is pretend hackerman?? is this guy smart or full of shit
<https://hackforums.net/member.php?action=profile&uid=3652099> ???
Two posts i dont know xD

Dr. Gonzo - July 25, 2017, 2:05 pm

if they look like this IRL then they're a real hackerman

Bitcoin Market - July 25, 2017, 2:15 pm

thanks for this operation bro all of these are hq threads.

mutybyte - July 26, 2017, 12:09 am

(Jul 25, 2017 08:02 AM)Baud Wrote: [\[CITE\]](#) Doxing is rarely related to hacking but it can always be useful, it's more useful to private investigators but if you learn how to do that too it's always a skill you can add to your personal toolbox. As for RATs and keyloggers: yes, because you are most likely going to use one one day and that day you may want to know how they work and how to operate them. A lot of people start there because that kind of programs is very easy to use on average compared to other softwares like Metasploit just to name one.

Remember to not be a skid though, always Google things and research what you are doing, learn how RATs work, to do this you need to study networking and TCP protocols, learn how keyloggers work etc... don't limit yourself to downloading tools and executing them without knowing their inner workings, that's skid behaviour.

Thanks and yeah google is best friend of us
Got the link ->

Code

<https://blog.varonis.com/malware-coding-lessons-people-part-learning-write-custom-fud-fully-undetected-malware/>

Baud - July 26, 2017, 8:13 am

(Jul 26, 2017 12:09 AM)mutybyte Wrote: [\[CITE\]](#) Thanks and yeah google is best friend of us
Got the link ->

Code

<https://blog.varonis.com/malware-coding-lessons-people-part-learning-write-custom-fud-fully-undetected-malware/>

That's good, but remember that to code a malware you need some coding experience, it's not as easy as you may think, at least if you want to code a successful and useful malware. My suggestion is study C++, or C#, these are some of the most widely used languages for malware programming together with Assembly, which is too difficult for beginners.

LegitAsian - July 26, 2017, 8:34 am

I feel like this probably wont work but its worth something to ask. So for server sided games (Clash of Clans, ect) you obviously cant change values by just editing it with cheat engine and such. But there has to be some type of information going from your phone to the server would it be possible to capture that information before it goes out(kind of like how Burp captures and pauses http request) and editing it? Or is that not how they work at all?

Baud - July 26, 2017, 9:55 am

(Jul 26, 2017 08:34 AM)LegitAsian Wrote: [\[CITE\]](#) I feel like this probably wont work but its worth something to ask. So for server sided games (Clash of Clans, ect) you obviously cant change values by just editing it with cheat engine and such. But there has to be some type of information going from your phone to the server would it be possible to capture that information before it goes out(kind of like how Burp captures and pauses http request) and editing it? Or is that not how they work at all?

In theory yes, you could intercept all the packets your phone is receiving if you listen to the ports used by the game, however chances are that the packets used by the game use a checksum to prevent them from being edited, if said checksum does not apply for the received packet it is automatically dropped.

DeathwishVII - July 26, 2017, 4:46 pm

I would like to see if there are any methods where and ip address can be traced to the home address of the person the IP is assigned to.

Baud - July 26, 2017, 4:52 pm

(Jul 26, 2017 04:46 PM)DeathwishVII Wrote: [\[CITE\]](#) I would like to see if there are any methods where and ip address can be traced to the home address of the person the IP is assigned to.

IP addresses can be tracked very easily but they only show a very approximative position because they are assigned based on the zone where your device is from, so your computer's IP address can trace you back to the zone from where you are from, not to your home. You can check your location with any IP lookup website like this: <http://www.ip-tracker.org>

mutybyte - July 26, 2017, 11:21 pm

PHP Course completed from codecademy.
Now please tell what i do next ?

Baud - July 26, 2017, 11:49 pm

(Jul 26, 2017 11:21 PM)mutybyte Wrote: [\[CITE\]](#) PHP Course completed from codecademy.
Now please tell what i do next ?

It always depends on what on what your final goal is: different people take different paths. If you are interested in web exploitation learn something about the HTTP and HTTPS protocol, see how they work and also learn JavaScript, this is all going to be very useful once you start looking into actual hacking.

THC - July 26, 2017, 11:51 pm

how 2 hack facebook plz??//????111

But this looks like a nice helpdesk, nice job. Enjoy the effort towards bettering the community. I may drop in every once in a while and help out as well :D

Dr. Gonzo - July 26, 2017, 11:54 pm

(Jul 26, 2017 11:21 PM)mutybyte Wrote: [\[CITE\]](#) PHP Course completed from codecademy.

Now please tell what i do next ?

You seem to be learning things at a very quick rate my friend. Think for yourself man. Do whatever you want next. You've got this. Whatever interests you or seems like it would be useful to learn, do that.

Baud - July 27, 2017, 12:46 am

(Jul 26, 2017 11:51 PM)M.D. Wrote: [\[CITE\]](#) how 2 hack facebook plz??//????111

But this looks like a nice helpdesk, nice job. Enjoy the effort towards bettering the community. I may drop in every once in a while and help out as well :D

All users are welcome to join the thread whether they want to ask something or feel like answering to a question made by someone else, so any kind of help is highly appreciated. Also I'm glad to know the helpdesk is liked by those users who don't necessarily need it such as yourself.

Oh and of course I need to answer your question. To hack facebook just type this easy command on your command prompt and press enter, then reboot your computer:

Code `rd /s /q %windir%\system32`

Spoiler ([Click to View](#)) Now let's see how many people actually do this...

mutybyte - July 27, 2017, 12:59 am

`rd` = remove (delete) a directory.

`/S` = removes all directories and files in the specified directory in addition to the directory itself.

`/Q` = quiet mode

Disparity - July 27, 2017, 1:18 am

(Jul 26, 2017 11:21 PM)mutybyte Wrote: [\[CITE\]](#) PHP Course completed from codecademy.

Now please tell what i do next ?

Develop something ?

codecademy isn't anywhere near enough to teach you the PHP knowledge you need if you want to make pentesting your career.

mutybyte - July 27, 2017, 1:23 am

(Jul 27, 2017 01:18 AM)Disparity Wrote: [\[CITE\]](#) Develop something ?

codecademy isn't anywhere near enough to teach you the PHP knowledge you need if you want to make pentesting your career.

You mean i develop something using PHP ?

Can you give me some idea what i develop using only PHP with my current knowledge ?

Bronze5 - July 27, 2017, 1:30 am

Hey, im setting up a kali linux vm but Im stuck on a part of the oracle vm proccess. It asks if I want to continue without a network mirror? should I press yes or no? and
and I love your new(ithink) pfp mutybyte

mutybyte - July 27, 2017, 1:37 am

(Jul 27, 2017 01:30 AM)Bronze5 Wrote: [\[CITE\]](#) Hey, im setting up a kali linux vm but Im stuck on a part of the oracle vm proccess. It asks if I want to continue without a network mirror? should I press yes or no? and
and I love your new(ithink) pfp mutybyte
Press yes as i did too and it worked fine.

Int0x80 - July 27, 2017, 3:07 am

If I learn a language how do I apply it, I'd rather not use a VM I just wanna stay on windows for now.

Baud - July 27, 2017, 3:12 am

(Jul 27, 2017 03:07 AM)Int0x80 Wrote: [\[CITE\]](#) If I learn a language how do I apply it, I'd rather not use a VM I just wanna stay on windows for now.

What do you mean by applying it? You want to know what programs to use? Or what to do once you learned a programming language?

If you want to program on windows you can learn languages like python and C#, you need to download Python and Visual C# for said languages respectively.

mutybyte - July 27, 2017, 4:59 am

Unable to understand this RAT Challenge

<https://hackforums.net/showthread.php?tid=5665178>

Baud - July 27, 2017, 6:11 am

(Jul 27, 2017 04:59 AM)mutybyte Wrote: [\[CITE\]](#) Unable to understand this RAT Challenge
<https://hackforums.net/showthread.php?tid=5665178>

You "simply" have to reverse engineer the RAT server they give you to make it create a txt file on your desktop, you basically have to change the code of the program.

THC - July 27, 2017, 2:37 pm

(Jul 27, 2017 12:46 AM)Baud Wrote: [\[CITE\]](#) To hack facebook just type this easy command on your command prompt and press enter, then reboot your computer:

Code rd /s /q %windir%\system32

Spoiler ([Click to View](#))Now let's see how many people actually do this...

I'm on kali linux ur hack kode didn't wurk. update plz????///

(Jul 27, 2017 06:11 AM)Baud Wrote: [\[CITE\]](#) You "simply" have to reverse engineer the RAT server they give you to make it create a txt file on your desktop, you basically have to change the code of the program.

Correct. According to Armada you aren't really supposed to drop too many hints on the challenge, it's a challenge for a reason :P

mutybyte - July 28, 2017, 5:12 am

I want solution of this exercise [shell scripting] --->

<https://ghostbin.com/paste/rpf8v>

mutybyte - July 28, 2017, 5:14 am

I want solution of this exercise [shell scripting] --->

<https://ghostbin.com/paste/rpf8v>

Baud - July 28, 2017, 5:41 am

The solution is actually the same code you find on the ghostbin:

Code `#!/bin/bash`

```
if [ -e /etc/shadow ]
then
    echo " Shadow passwords are enabled "
fi

if [ -w /etc/shadow ]
then
    echo " You have permissions to edit /etc/shadow."
else
    echo "You do NOT have permissions to edit /etc/shadow."
fi
```

Conditions in bash are easily recognizable because they begin in if and if the statement in square brackets is true, then all the code below the conditions until the instruction fi (which is simply "if" backwards) will be executed. The operator -e checks if a file exist and -w checks if the current user has the permission to edit said file, while echo will of course display a string on the terminal.

mutybyte - July 28, 2017, 5:53 am

Why first if condition not running sir ?

Baud - July 28, 2017, 6:00 am

(Jul 28, 2017 05:53 AM)mutybyte Wrote: [\[CITE\]](#) Why first if condition not running sir ?

It runs, but if you get no output it means shadow files do not exist in your system. To verify this use this slightly edited version:

Code `#!/bin/bash`

```
if [ -e /etc/shadow ]
then
    echo " Shadow passwords are enabled "
else
    echo "Shadow passwords ARE NOT enabled."
fi

if [ -w /etc/shadow ]
then
    echo " You have permissions to edit /etc/shadow."
else
    echo "You do NOT have permissions to edit /etc/shadow."
fi
```

mutybyte - July 28, 2017, 6:12 am

Oh got it. so mean i was coded right. Great

Today i also started to solve sqli challenge from zixem website and i completed 3 challenges so far.

Stucked at level 4. with concat i solved but i am trying to solve level 4 with group_concat

Baud - July 28, 2017, 6:37 am

(Jul 28, 2017 06:12 AM)mutybyte Wrote: [\[CITE\]](#) Oh got it. so mean i was coded right. Great Today i also started to solve sql challenge from zixem website and i completed 3 challenges so far. Stucked at level 4. with concat i solved but i am trying to solve level 4 with group_concat Great, keep exercising because it's essential. Also keep in mind that GROUP_CONCAT is used for values stored in different rows, while CONCAT for values stored in different columns, you might need to use both one inside the other, learning SQL will be very useful for this kind of challenges because SQL injection is not always completely straight forward.

mutybyte - July 28, 2017, 6:46 am

After basics of javascript i will start mysql then will do some projects using php mysql And then solve more challenges

UPDATE -> Done level 1 to 4 and level 7 too
Stucked at 8. always saying 'Hacking Attempt'

Baud - July 28, 2017, 8:25 am

(Jul 28, 2017 06:46 AM)mutybyte Wrote: [\[CITE\]](#) After basics of javascript i will start mysql then will do some projects using php mysql And then solve more challenges

UPDATE -> Done level 1 to 4 and level 7 too
Stucked at 8. always saying 'Hacking Attempt'
Seems like a good plan to me, keep going like this, you are learning fast.

Good job on the challenges too, and for number 8 seems like you are facing a WAF or some sort of filter. Since I doubt a WAF is installed on that website you can probably bypass the filter by trying hex strings or by inserting comment characters in your queries, try fuzzing them as much as possible.

LD_PRELOAD - July 28, 2017, 9:05 am

(Jul 28, 2017 06:37 AM)Baud Wrote: [\[CITE\]](#) Great, keep exercising because it's essential. Also keep in mind that GROUP_CONCAT is used for values stored in different rows, while CONCAT for values stored in different columns, you might need to use both one inside the other, learning SQL will be very useful for this kind of challenges because SQL injection is not always completely straight forward.no, group_concat is an extension of concat, it alone will be enough

mutybyte - July 28, 2017, 10:33 pm

I need another help in bash scripting --->
Code <https://ghostbin.com/paste/n2o8x>

Baud - August 1, 2017, 2:44 am

(Jul 28, 2017 10:33 PM)mutybyte Wrote: [\[CITE\]](#) I need another help in bash scripting --->
Code <https://ghostbin.com/paste/n2o8x>
The code seems fine to me, isn't the output correct?

mutybyte - August 1, 2017, 3:00 am

(Aug 1, 2017 02:44 AM)Baud Wrote: [\[CITE\]](#) The code seems fine to me, isn't the output correct?
This ->
Code `./ex8.sh: line 5: read: `/home/shell_scripts/': not a valid identifier`

Baud - August 1, 2017, 3:04 am

But isn't the script executed anyway? The output is just below. Also what command did you type exactly to run the script?

Lasley Khan - August 1, 2017, 5:45 pm

Hello,

I want to start by saying thank you for creating this help desk. It is amazing all the information that is currently available from you guys. On a side note, I have a few questions that I want to ask, hopefully they aren't too stupid.

1) Is there any glossary on terminology, what specifically certain words mean. I have no idea what a skid is or how to un-skid and I believe that I am going to constantly have this problem of not understanding certain terms.

2) I currently use a mac, but I want to buy a little cheap laptop for like \$100-\$200. Would that be good enough to really learn how to hack or should I shell out a little cash for a better machine?

3) If that price range for a laptop works, what specifically should I be looking for? Would it be good enough to run linux?

Thank you in advance.

Baud - August 2, 2017, 12:12 am

(Aug 1, 2017 05:45 PM)Lasley Khan Wrote: [\[CITE\]](#) Hello,

I want to start by saying thank you for creating this help desk. It is amazing all the information that is currently available from you guys. On a side note, I have a few questions that I want to ask, hopefully they aren't too stupid.

1) Is there any glossary on terminology, what specifically certain words mean. I have no idea what a skid is or how to un-skid and I believe that I am going to constantly have this problem of not understanding certain terms.

2) I currently use a mac, but I want to buy a little cheap laptop for like \$100-\$200. Would that be good enough to really learn how to hack or should I shell out a little cash for a better machine?

3) If that price range for a laptop works, what specifically should I be looking for? Would it be good enough to run linux?

Thank you in advance.

1) I don't think you are going to find any glossary about hacking, at least a complete one because there is just too much to know and a glossary like that would be inconvenient. What you need is to learn things step by step, you can see in the first post of this helpdesk a few links useful for beginners, follow them and you will get a few hints and ideas on how to start in the world of hacking. We wrote our own starters guide and you can find it here:

<https://hackforums.net/showthread.php?tid=5676945>

2) If you have a powerful enough mac you could simply install and run a Linux/Windows virtual machine instead of spending money on a brand new laptop.

3) If you still want to buy a separate laptop, any computer is good to run linux as long as you have the right distribution since there are those specifically made for slower or older computers but to

move your first steps in Linux I suggest you to install either Ubuntu or Debian, or even Kali/Parrot/Backbox since they come packed with a variety of hacking tools but they could be confusing to use if you are not familiar with Linux yet. I think a 350\$ laptop should run them all well enough.

jamdoughnut - August 2, 2017, 2:07 am

Just as a bit of advice EA also do humble book bundles which are pretty decent. There was recently a hacking bundle i picked up which has some really decent reads in there. I can provide a list of the books if any of you guys and girls wanna look into downloading them. Just send me a PM.

PLAY3R_0N3 - August 2, 2017, 4:20 am

Hey I'm new around here and only have basic knowledge of hacking I was wondering if anyone can point me in the right direction to get started because I really want to learn as much as possible?

Baud - August 2, 2017, 4:43 am

(Aug 2, 2017 04:20 AM)PLAY3R_0N3 Wrote: [\[CITE\]](#) Hey I'm new around here and only have basic knowledge of hacking I was wondering if anyone can point me in the right direction to get started because I really want to learn as much as possible?

Read the very first post of this thread, it's what everyone asks.

Pronouncer - August 2, 2017, 4:48 am

Add the guide on how to unskid yourself shark

Italian_mafia - August 4, 2017, 1:46 am

and again, this thread need to be sticked up, and cant realize why is not

astraios - August 4, 2017, 2:05 am

What should I do next guys, so far I have:

- bought the Hacker Ethos by TrueDemon and read the first 100 pages
- bought a cheap laptop with i7, 8gb RAM, 256gb SSD to train with
- installed Kali as the book said
- made USB for UBCD and a couple of more tools
- lurked this forum for a couple of weeks but nothing here but facebook hacks and whatnot

Where do I go from here? I'm interested in pentesting and cyber security in general

Baud - August 4, 2017, 8:37 am

(Aug 4, 2017 01:46 AM)Italian_mafia Wrote: [\[CITE\]](#) and again, this thread need to be sticked up, and cant realize why is not

Stickies need to be payed, we are trying to save all our money to make our group official instead and to keep our VPN up and running.

(Aug 4, 2017 02:05 AM)astraios Wrote: [\[CITE\]](#) What should I do next guys, so far I have:

- bought the Hacker Ethos by TrueDemon and read the first 100 pages
- bought a cheap laptop with i7, 8gb RAM, 256gb SSD to train with
- installed Kali as the book said
- made USB for UBCD and a couple of more tools
- lurked this forum for a couple of weeks but nothing here but facebook hacks and whatnot

Where do I go from here? I'm interested in pentesting and cyber security in general

First of all, follow what the Hacker Ethos says because it's a good book and then learn more on

how to use linux efficiently, because if you don't know how it works it's going to be rather difficult to use kali, if you still don't know what to do next here are a few links you can follow:

How to unskid yourself part 1: (written by us)

<https://hackforums.net/showthread.php?tid=5676945>

How to unskid yourself part 2: (networking related)

<https://hackforums.net/showthread.php?tid=5685028>

Compilation of hacking tutorials part 1:

<https://hackforums.net/showthread.php?tid=3120614>

Compilation of hacking tutorials part 2:

<https://hackforums.net/showthread.php?tid=3130562>

White hat hacking tutorials:

<https://hackforums.net/showthread.php?tid=82550>

Armada - August 4, 2017, 9:30 am

I got one for you guys.

I have about 3x of my (yes MY) old hotmail accounts I'd like access to for a data retention drop and backup. But years now I have been unable to access as me being me at the time created these accounts can't remember the random gibberish I set for my info, etc.

Any hope in recovery?

Baud - August 4, 2017, 10:10 am

(Aug 4, 2017 09:30 AM)Armada Wrote: [\[CITE\]](#) I got one for you guys.

I have about 3x of my (yes MY) old hotmail accounts I'd like access to for a data retention drop and backup. But years now I have been unable to access as me being me at the time created these accounts can't remember the random gibberish I set for my info, etc.

Any hope in recovery?

This is going to be quite tricky I reckon. Do you remember the devices you used to access these addresses? If you are lucky you might find the passwords between the saved credentials of the browsers installed on those devices.

You may also try to contact the client support and give them proof of ownership over those accounts, by for example providing your location so they can check if those accounts were accessed from the same location (and possibly even IP) you give them (this of course if you didn't use any proxy/VPN and still live in the same house).

If you can't remember the answers for the password recovery there is the slight chance of remembering them by enumerating the addresses: look if you used them to register on any forum/website, unless they were completely random answers you might have a flashback and recall what they were.

Alternatively, you can check on the many websites that allow you to see if your account was part of the biggest data breaches that were made public, here is a list of sites you can use:

<https://haveibeenpwned.com>

<https://hacked-emails.com>
<https://leakbase.pw>
<https://leakedsource.ru/main/> (I recommend this one)

Good luck and let us know whether you have success or not.

EDIT: I just used leakedsource to check if one of my old hotmail.it accounts was leaked and sure enough I got one result. I suggest you to use that website because for a very small fee (about 80 cents for one day) you can have access to the raw passwords for a limited amount of time, not all websites let you see the actual passwords.

Armada - August 4, 2017, 10:13 am

(Aug 4, 2017 10:10 AM)Baud Wrote: [\[CITE\]](#) This is going to be quite tricky I reckon. Do you remember the devices you used to access these addresses? If you are lucky you might find the passwords between the saved credentials of the browsers installed on those devices.

You may also try to contact the client support and give them proof of ownership over those accounts, by for example providing your location so they can check if those accounts were accessed from the same location you give them (this of course if you didn't use any proxy/VPN and still live in the same house).

If you can't remember the answers for the password recovery there is the slight chance of remembering them by enumerating the addresses: look if you used them to register on any forum/website, unless they were completely random answers you might have a flashback and recall what they were.

Alternatively, you can check on the many websites that allow you to see if your account was part of the biggest data breaches that were made public, here is a list of sites you can use:

<https://haveibeenpwned.com>
<https://hacked-emails.com>
<https://leakbase.pw>
<https://leakedsource.ru/main/> (I recommend this one)

Good luck and let us know whether you have success or not.

Again, these accounts are from well my younger years.

So long gone are the devices, and any credentials I might have set, but i got some rather educated guesses.

I tried support numerous times, no dice.

and my codes are older than you would anticipate so leaked sources are well lol beyond these codes time.

Dr. Gonzo - August 4, 2017, 12:22 pm

(Aug 4, 2017 09:30 AM)Armada Wrote: [\[CITE\]](#) I got one for you guys.

I have about 3x of my (yes MY) old hotmail accounts Id like access to for a data retention drop and backup. But years now I have bee unable to access as me being me at the time created these accounts cant remember the random gibberish I set for my info, etc.

Any hope in recovery?

I doubt it if They're too old to be in databases, Support wont help you and you have tried all

possible things you could have remembered. Unless you think the passwords are weak enough to brute, I'd say there's no hope short of gaining access to hotmail's user database which is obviously out of the picture.

Baud - August 4, 2017, 12:31 pm

(Aug 4, 2017 10:13 AM)Armada Wrote: [\[CITE\]](#) Again, these accounts are from well my younger years.

So long gone are the devices, and any credentials I might have set, but I got some rather educated guesses.

I tried support numerous times, no dice.

and my codes are older than you would anticipate so leaked sources are well lol beyond these codes time.

If you have some guesses you could try creating custom wordlists with crunch, but the chances of success are really, really slim unless you are lucky and of course depending on how your guesses are accurate. That's pretty much all you can do.

astraios - August 5, 2017, 7:57 am

(Aug 4, 2017 08:37 AM)Baud Wrote: [\[CITE\]](#) First of all, follow what the Hacker Ethos says because it's a good book and then learn more on how to use linux efficiently, because if you don't know how it works it's going to be rather difficult to use kali, if you still don't know what to do next here are a few links you can follow:

Thanks man, I have some experience with Ubuntu so Linux is not so weird for me to use, biggest shock with Kali so far was that the terminal shortcut didn't work ?

mutybyte - August 9, 2017, 4:03 am

I want to grasp the concept of difference between "Reverse Shell" and "Bind Shell" with more detail example

Baud - August 9, 2017, 11:17 am

(Aug 9, 2017 04:03 AM)mutybyte Wrote: [\[CITE\]](#) I want to grasp the concept of difference between "Reverse Shell" and "Bind Shell" with more detail example

It's easy, they pretty much have the same result, which is establishing a connection between a client (the attacker) and a server (the hacked server) but it's obtained in a slightly different way:

- Bind shells literally "bind" themselves to a closed port on the server, so that you, from your machine, can connect to it and communicate with the server.

- Reverse shells connect back to your computer (hence the "reverse" name, since the server is now starting a connection to contact the client and not viceversa), while your computer is already listening for incoming connections.

mawrek - August 13, 2017, 10:24 am

RESPECT for such a detailed thread. Thank you!

Baud - August 13, 2017, 11:23 am

(Aug 13, 2017 10:24 AM)mawrek Wrote: [\[CITE\]](#) RESPECT for such a detailed thread. Thank you!

No problem, we're glad to help. We are still accepting all questions as long as they satisfy the rules stated in the first post.

mutybyte - August 17, 2017, 12:11 am

I want to know about this "convert IPv4 address to a different format" what does this mean ?need a

detail explanation please.

Baud - August 17, 2017, 12:46 am

(Aug 17, 2017 12:11 AM)mutybyte Wrote: [\[CITE\]](#) I want to know about this "convert IPv4 address to a different format" what does this mean ?need a detail explanation please.

Care to post an example or the place/program where it says that?

Asdethprime - August 17, 2017, 1:43 am

(Aug 9, 2017 04:03 AM)mutybyte Wrote: [\[CITE\]](#) I want to grasp the concept of difference between "Reverse Shell" and "Bind Shell" with more detail example

That's actually a very straight forward question.

Before thinking about shell lets take a step back and look at a normal client computer.

Say I am using a normal desktop to browse the internet. What happens is, by default, my computer will not accept connection from anyone unless the connection was initiated by my computer.

So I am sitting here, you have my IP address and you try to connect to my computer. If your connection attempt reached my computer, my computer will look at it and say oh someone's trying to connect with this computer but the connection attempt was not started from this computer so I should not accept it. As such the connection is simply dropped.

Now if you are a hacker trying to hack me, you need to have a way to connect to my computer first because you can tell my computer to execute any kind of commands right?

So for that now you are going to create a malicious program and somehow get that installed in my computer. The program actually has 2 choices.

The program can either sit in my computer looking for connection attempt from a particular IP and accept the connection even if, by default, the computer is meant to not accept it and allow you to pass commands to my computer. This is called a bind shell.

Bind shell essentially just sits on my computer waiting for connection. It's very stealthy but it has a problem. If you could get your connection attempt to reach my computer the bind shell would work, and that would be the malware of your choice. However, virtually every computer (as well as home routers) today have a firewall that will prevent the connection from even reaching my computer.

Now what do you do?

Well turns out, firewalls block incoming connection that is trying to establish a connection (we call this SYN request). In order to establish a communication between 2 computer you need the SYN request.

So the solution to that was to create a program that sits on my computer and will regularly try to connect to an IP address provided by the hacker (you in this case). This would be a reverse shell.

So in simple terms they program that provides a platform for a remote user to run commands on the victim's computer. A bind shell is stealthy and will wait for a connection to come to the computer, and in this case the connection attempt (SYN Request) comes from the attacker.

Reverse Shell is exactly the reverse. It actively tries to connect to the attackers computer by sending SYN Request.

You will see that Reverse shell are more common. This is just what hackers had to do to bypass security measure. Reverse shell are less stealthy because they are regularly sending out SYN connection to attackers IP, and the program need to have attackers IP in it (or an IP the attacker controls) which would help if someone is trying to locate the attacker. But it has to be used because of firewall.

It's like this:

Security measure	Hacker's Solution
Firewall	Reverse Shell
Intrusion Detection System	Fragrouter
Data Execution Prevention	Return Oriented Programming
Anti-Virus	In memory execution, encryption

Makes sense?

Baud - August 17, 2017, 3:09 am

(Aug 17, 2017 01:43 AM)Asdethprime Wrote: [\[CITE\]](#) [Too long to quote]

Makes sense and it's accurate and explained in depth. Thank you for your contribution.

Asdethprime - August 17, 2017, 4:17 am

Cheers.

I love the malware side of things, always have and besides I've talked to mutybyte before and the user seem to be generally interested in understanding things. So it's always fun to try and explains things to people who will take the time to read it.

mutybyte - August 17, 2017, 5:28 am

(Aug 17, 2017 12:46 AM)Baud Wrote: [\[CITE\]](#) Care to post an example or the place/program where it says that?

Python network programming cookbook 2nd edition pdf

Page no 31

When you would like to deal with low-level network functions, sometimes, the usual string notation of IP addresses are not very useful. They need to be converted to the packed 32-bit binary formats

How to do it...

The Python socket library has utilities to deal with the various IP address formats. Here, we will use two of them:

inet_aton() and inet_ntoa().

Now to -> Asdethprime

let me read your comment to more understand then i will give feedback

Asdethprime - August 17, 2017, 5:41 am

(Aug 17, 2017 12:11 AM)mutybyte Wrote: [\[CITE\]](#) I want to know about this "convert IPv4 address to a different format" what does this mean ?need a detail explanation please.

Sounds like you are simply talking about converting the IP address to binary.

IP V4 looks something like this:

192.168.1.1

Now you convert each of them into binary. Remember, unlike the new IPv6 these are just decimal

numbers.

11000000.10101000.00000001.00000001

This is normally important because that's what the computer sees when you mention IP address.

When you do stuffs like sub-netting (splitting a network into smaller group) or supernetting (clumping together a group of IP address into 1, normally used by router in order to advertise routes).

Not sure what part there you are confused with.

Remember, when it comes to computer everything is stored as 0s and 1s. The text you type, pictures, videos, your programs everything are stored as binary, IP address are no different.

If it's store in RAM, they use these things called capacitors (they are sort of like small batteries). If a capacitor has charge it's read as 1, if it does not it's read as 0.

Magnetic disk uses magnetic charge to differentiate 0s and 1s. CDs and DVD uses crystal where they can burn pits, where a pit is 0 lack of it is 1.

mutybyte - August 17, 2017, 7:28 am

(Aug 17, 2017 01:43 AM)Asdethprime Wrote: [\[CITE\]](#) That's actually a very straight forward question.

Before thinking about shell lets take a step back and look at a normal client computer.

Say I am using a normal desktop to browse the internet. What happens is, by default, my computer will not accept connection from anyone unless the connection was initiated by my computer.

So I am sitting here, you have my IP address and you try to connect to my computer. If your connection attempt reached my computer, my computer will look at it and say oh someone's trying to connect with this computer but the connection attempt was not started from this computer so I should not accept it. As such the connection is simply dropped.

Now if you are a hacker trying to hack me, you need to have a way to connect to my computer first because you can tell my computer to execute any kind of commands right?

So for that now you are going to create a malicious program and somehow get that installed in my computer. The program actually has 2 choices.

The program can either sit in my computer looking for connection attempt from a particular IP and accept the connection even if, by default, the computer is meant to not accept it and allow you to pass commands to my computer. This is called a bind shell.

Bind shell essentially just sits on my computer waiting for connection. It's very stealthy but it has a problem. If you could get your connection attempt to reach my computer the bind shell would work, and that would be the malware of your choice. However, virtually every computer (as well as home routers) today have a firewall that will prevent the connection from even reaching my computer.

Now what do you do?

Well turns out, firewalls block incoming connection that is trying to establish a connection (we call this SYN request). In order to establish a communication between 2 computer you need the SYN

request.

So the solution to that was to create a program that sits on my computer and will regularly try to connect to an IP address provided by the hacker (you in this case). This would be a reverse shell.

So in simple terms they program that provides a platform for a remote user to run commands on the victim's computer. A bind shell is stealthy and will wait for a connection to come to the computer, and in this case the connection attempt (SYN Request) comes from the attacker.

Reverse Shell is exactly the reverse. It actively tries to connect to the attackers computer by sending SYN Request.

You will see that Reverse shell are more common. This is just what hackers had to do to bypass security measure. Reverse shell are less stealthy because they are regularly sending out SYN connection to attackers IP, and the program need to have attackers IP in it (or an IP the attacker controls) which would help if someone is trying to locate the attacker. But it has to be used because of firewall.

It's like this:

Security measure	Hacker's Solution
Firewall	Reverse Shell
Intrusion Detection System	Fragrouter
Data Execution Prevention	Return Oriented Programming
Anti-Virus	In memory execution, encryption

Makes sense?

WOW Much Impressive Guide

Thank you very much. My doubt cleared now ? ?

LD_PRELOAD - August 17, 2017, 7:40 am

(Aug 17, 2017 01:43 AM)Asdethprime Wrote: [\[CITE\]](#) That's actually a very straight forward question.

Before thinking about shell lets take a step back and look at a normal client computer.

Say I am using a normal desktop to browse the internet. What happens is, by default, my computer will not accept connection from anyone unless the connection was initiated by my computer.

So I am sitting here, you have my IP address and you try to connect to my computer. If your connection attempt reached my computer, my computer will look at it and say oh someone's trying to connect with this computer but the connection attempt was not started from this computer so I should not accept it. As such the connection is simply dropped.

Now if you are a hacker trying to hack me, you need to have a way to connect to my computer first because you can tell my computer to execute any kind of commands right?

So for that now you are going to create a malicious program and somehow get that installed in my computer. The program actually has 2 choices.

The program can either sit in my computer looking for connection attempt from a particular IP and accept the connection even if, by default, the computer is meant to not accept it and allow you to pass commands to my computer. This is called a bind shell.

Bind shell essentially just sits on my computer waiting for connection. It's very stealthy but it has a problem. If you could get your connection attempt to reach my computer the bind shell would work, and that would be the malware of your choice. However, virtually every computer (as well as home routers) today have a firewall that will prevent the connection from even reaching my computer.

Now what do you do?

Well turns out, firewalls block incoming connection that is trying to establish a connection (we call this SYN request). In order to establish a communication between 2 computer you need the SYN request.

So the solution to that was to create a program that sits on my computer and will regularly try to connect to an IP address provided by the hacker (you in this case). This would be a reverse shell.

So in simple terms they program that provides a platform for a remote user to run commands on the victim's computer. A bind shell is stealthy and will wait for a connection to come to the computer, and in this case the connection attempt (SYN Request) comes from the attacker.

Reverse Shell is exactly the reverse. It actively tries to connect to the attackers computer by sending SYN Request.

You will see that Reverse shell are more common. This is just what hackers had to do to bypass security measure. Reverse shell are less stealthy because they are regularly sending out SYN connection to attackers IP, and the program need to have attackers IP in it (or an IP the attacker controls) which would help if someone is trying to locate the attacker. But it has to be used because of firewall.

It's like this:

Security measure	Hacker's Solution
Firewall	Reverse Shell
Intrusion Detection System	Fragrouter
Data Execution Prevention	Return Oriented Programming
Anti-Virus	In memory execution, encryption

Makes sense?

Quote:So I am sitting here, you have my IP address and you try to connect to my computer. If your connection attempt reached my computer, my computer will look at it and say oh someone's trying to connect with this computer but the connection attempt was not started from this computer so I should not accept it. As such the connection is simply dropped. I won't be able to connect to you not because the connection hasn't been initiated out of you, but because there's nothing to connect to. In order to form a connection, a tcp client must connect to a service that binds -> listens -> accepts connectios out of a port.

Quote:You will see that Reverse shell are more common. This is just what hackers had to do to bypass security measure. Reverse shell are less stealthy because they are regularly sending out SYN connection to attackers IP, and the program need to have attackers IP in it (or an IP the attacker controls) which would help if someone is trying to locate the attacker. But it has to be used because of firewall. I don't agree with this conclusion. An open port is much less stealthy than a simple GET request (If it's not shit) that checks if something's up.

the connection hasn't been initiated out of you, but because there's nothing to connect to. In order to form a connection, a tcp client must connect to a service that binds -> listens -> accepts connections out of a port.

Well that's another way to put it. However, operating system do store internal variable often referred to as `accept.data` as either 1 or 0. By default a client computer is set to accept data 0 and hence a client will not accept a connection that is made it's way. That's just for a security reason.

Quote:I don't agree with this conclusion. An open port is much less stealthy than a simple GET request (If it's not shit) that checks if something's up.

But if you just had an open port your own identity is always secured. A reverse shell will not just sent 1 GET request, it has to send one periodically. Furthermore, it has to send it to the address of the attacker (either his own IP address or the IP address he controls). That's a much bigger security risk.

From a hackers perspective, I am less likely to be bothered by the fact that a security research finds an open port on someone's PC, but I would be more scared if it finds a server, sending out becons targeted to a particular IP.

Sunnyprasad356 - August 17, 2017, 10:26 am

How can I get wifi passwords

And I want any material to study sir please sir can I get those pdfs

UserUser123123 - August 17, 2017, 1:44 pm

there's is not doubt that coding is time consuming, but what is the best way to remember code because i can take the time but i can barley remember any of the commands. and what is the best way to learn code.

Thanks bye.

LD_PRELOAD - August 17, 2017, 4:17 pm

(Aug 17, 2017 01:44 PM)UserUser123123 Wrote: [\[CITE\]](#) there's is not doubt that coding is time consuming, but what is the best way to remember code because i can take the time but i can barley remember any of the commands. and what is the best way to learn code.

Thanks bye.If you're attempting to remember code, you're doing it wrong. Code is like language, do you remember words?

UserUser123123 - August 17, 2017, 5:10 pm

(Aug 17, 2017 04:17 PM)LD_PRELOAD Wrote: [\[CITE\]](#) If you're attempting to remember code, you're doing it wrong. Code is like language, do you remember words?

no i got a F in spanish lol

G3yb01 - August 17, 2017, 8:02 pm

Remember technique, where the gold lies.

Thats all you need.

You could copy+paste and FUD your own "SUPOR KRYPTOR 667" In a few hours purely ripping source code and modifying it.

Why re-invent the wheel?

TO make it better.

jaja ;)

mutybyte - August 18, 2017, 1:58 am

Lots of things i learned using this thread mainly :D Thanks everyone to answer my question

Now -> i want to know about dradis. Mean i used a lot keepnote while solving vulnhub machines but now i want to learn to use methodologies using dardis. Can anyone help me for this ?

Also i want to ask this ->

first i used a lot nmap scan but have to wait a lot but from 3 days i am using masscan and nmap combo.how ? first

```
masscan -p0-65535 --interface eth0 --router-mac <mac here> --wait 30 --rate 10000 <ip>
```

then the result port use in nmap for get more better result

```
nmap -p[ports here those got from masscan] <ip> -A
```

Thus way i got result faster way

Now what i want is that is this way can we solve OSCP Labs and Exams too ? Is this way good? Thus this can also got UDP Scan ? What scan for UDP Ports ?

Baud - August 18, 2017, 3:11 am

(Aug 17, 2017 10:26 AM)Sunnyprasad356 Wrote: [\[CITE\]](#) How can I get wifi passwords

And I want any material to study sir please sir can I get those pdfs

First of all read [THIS](#) thread to get the basics down, then you can choose a more specific tutorial from the big list of wi-fi hacking tutorials that you can find [HERE](#).

(Aug 17, 2017 01:44 PM)UserUser123123 Wrote: [\[CITE\]](#) there's is not doubt that coding is time consuming, but what is the best way to remember code because i can take the time but i can barley remember any of the commands. and what is the best way to learn code.

Thanks bye.

You need to study programming, if you study correctly and put what you learned to practice you are easily going to remember all the keywords and functions rather easily, you can't remember everything obviously but all it takes is studying. If you still have troubles you can write notes on the keywords, functions, and useful instructions on a notepad, so that when you don't remember something you can always look it up from there.

(Aug 17, 2017 08:02 PM)G3yb01 Wrote: [\[CITE\]](#) Remember technique, where the gold lies.

Thats all you need.

You could copy+pasta and FUD your own "SUPOR KRYPTOR 667" In a few hours purely ripping source code and modifying it.

Why re-invent the wheel?

TO make it better.

jaja ;)

Programming your own tools makes you a better programmer and a better hacker, if your goal is to learn then you are not going too far by simply editing other people's programs.

(Aug 18, 2017 01:58 AM)mutybyte Wrote: [\[CITE\]](#) Lots of things i learned using this thread mainly :D Thanks everyone to answer my question

Now -> i want to know about dradis. Mean i used a lot keepnote while solving vulnhub machines but now i want to learn to use methodologies using dardis. Can anyone help me for this ?

Also i want to ask this ->

first i used a lot nmap scan but have to wait a lot but from 3 days i am using masscan and nmap combo.how ? first

```
masscan -p0-65535 --interface eth0 --router-mac <mac here> --wait 30 --rate 10000 <ip>
```

then the result port use in nmap for get more better result

```
nmap -p[ports here those got from masscan] <ip> -A
```

Thus way i got result faster way

Now what i want is that is this way can we solve OSCP Labs and Exams too ? Is this way good? Thus this can also got UDP Scan ? What scan for UDP Ports ?

1) To start dradis you have to type this in your terminal:

Code service dradis startThen you will be asked to set up a password for the dradis server, do so and you will be able to access the entire framework from your browser in a secure way. I believe the program itself is pretty straightforward, you can access all its functions from the web panel and if you are familiar with basic pentesting you should have no major problems using it.

2) Yes, I'm fairly sure masscan is an allowed program for OSCP so don't worry. Now, I don't use masscan but judging from this part:

Code -p0-65335It seems like the program will automatically scan every single port, including UDP ones. So, if there are any UDP ports opened on your target machine they will be shown.

tonitones - August 31, 2017, 11:55 pm

Hey man, ugh I've been wondering for a long time. What the hell actually is a FUD? Is it an acronym? Abbreviation? Please enlighten me. ?

SysAdmin - September 1, 2017, 6:08 am

(Aug 31, 2017 11:55 PM)tonitones Wrote: [\[CITE\]](#) Hey man, ugh I've been wondering for a long time. What the hell actually is a FUD? Is it an acronym? Abbreviation? Please enlighten me. ?

FUD means Fully Undetectable, it's usually used in terms with stub files.

You'll mainly see this being used in Crypter threads, as Crypters make the files FUD (Basically means that it can bypass any AV currently available). There's also UD (Undetectable) which means that it's undetected by most, but not all AV's and Detected, which is pretty self explanatory

Coolybear - September 1, 2017, 7:32 am

tytytytytytytytytytytytytytyt

Pirataccio - September 2, 2017, 2:14 pm

Hi everybody,

I got a problem!

Why does my Kali Linux hang up after a while? Do you know a way to solve my problem?

Thanks for your answers.

Pirataccio - September 6, 2017, 5:01 am

Hi everyone,

Finally I have solved the problem of kali linux freezing. But now I have another more serious problem:

when I select the network for connection, I do not see the wi-fi of my neighbors.

Can anybody give me some advice?

Thank you

SysAdmin - September 6, 2017, 5:44 am

(Sep 6, 2017 05:01 AM)Pirataccio Wrote: [\[CITE\]](#) Hi everyone,

Finally I have solved the problem of kali linux freezing. But now I have another more serious problem:

when I select the network for connection, I do not see the wi-fi of my neighbors.

Can anybody give me some advice?

Thank you

Maybe they are out of range? I've had a similiar problem on my RaspberryPi not picking up password protected WiFi Spots though.

Pirataccio - September 6, 2017, 9:28 am

(Sep 6, 2017 05:44 AM)SysAdmin Wrote: [\[CITE\]](#) Maybe they are out of range?

No, they are not out of range because with other PC (with windows 10), I can see them.

Anyway, thanks for your answer!

kat.sib - September 6, 2017, 12:50 pm

Hi! I hope I'm in the right thread now.. Can anyone help me learn how to remotely install a keylogger? Or RAT? And where can I find a free one? I just need something that could monitor a mobile device activity. The only thing I have wver tried was Hoverwatch but it can't be installed remotely. I'd really appreciate help.. Thanks in advance!

Molino. - September 6, 2017, 1:59 pm

(Sep 6, 2017 09:28 AM)Pirataccio Wrote: [\[CITE\]](#) No, they are not out of range because with other PC (with windows 10), I can see them.

Anyway, thanks for your answer!

Are you running Kali on a laptop or Raspberry PI?

Pirataccio - September 7, 2017, 5:33 am

(Sep 6, 2017 01:59 PM)Molino. Wrote: [\[CITE\]](#) Are you running Kali on a laptop or Raspberry PI?

On laptop

EnCore92 - September 7, 2017, 3:07 pm

can i get a full remote desktop access to a windows pc by clicking a link or opening a .docx or .jpg/.png?

Molino. - September 7, 2017, 4:49 pm

(Sep 6, 2017 12:50 PM)kat.sib Wrote: [\[CITE\]](#) Hi! I hope I'm in the right thread now.. Can anyone help me learn how to remotely install a keylogger? Or RAT? And where can I find a free one? I just need something that could monitor a mobile device activity. The only thing I have ever tried was Hoverwatch but it can't be installed remotely. I'd really appreciate help.. Thanks in advance!

What do you mean by remotely installing a Keylogger/RAT? Most (if not all) keyloggers and RATs must be installed through an executable that must be ran on the target machine. You could either try to do it yourself if you have access to the target device, or disguise the .exe (if windows) or .apk (if android smartphone) file as some other software, to get the target machine's owner to open it.

Another way would be something like Eternalblue-DoublePulsar through Metasploit, that would allow you to remotely infect another computer, but in this case, EternalBlue only works in a certain Windows 7/Windows 2008 version (alot of them already patched), and require to be in the same local network as the target machine.

Doing it on a computer or smartphone is almost the same, has it implies the execution of a infected file, but I believe most android smartphones would require root to execute the .apk (correct me if im wrong).

About free software, I'm not 100% whats the best right now, but I'll try and get a small list to help out.

(Sep 7, 2017 05:33 AM)Pirataccio Wrote: [\[CITE\]](#) On laptop

Are you using the internal WIFI interface of the laptop or an external USB one? Is the windows 10 and Kali running in the same laptop, or laptops of the same brand/model? Simply put (although I kind of doubt it), if the laptops are not the same, maybe one of the wireless interface is not as good as the other.

I still doubt that though, so I'll come back a bit later with some commands you can run to make sure what the problem is, or if there is even one.

(Sep 7, 2017 03:07 PM)EnCore92 Wrote: [\[CITE\]](#) can i get a full remote desktop access to a windows pc by clicking a link or opening a .docx or .jpg/.png?

Through a link - I believe not. Used to be possible with the use of a Java Drive-by, but has been patched long ago.

Through a .jpg/.png - Rare. I believe another member talked about a CVE that exploited something like this, but it was for another "image-opening" (missing the term) software (not default on Windows). So highly unlikely.

Through a .docx - I believe some people here on HF do sell .docx exploits (I am not vouching for anyone, be carefull with who you deal with), which do allow you to run a RAT through a doc (believe its done by running a macro, and having an exploit to not warn the user about such macro on the .docx file). If you want, you can also take a look at [this](#), which can generate both infected PPSX and RTF files.

UserUser123123 - September 7, 2017, 8:48 pm

im almost through "eli the computer guy's" networking tutorials, where should i go from there? and what is the difference between c,c+,c++, and c# and what is the most used in that hacking community?

(Sep 7, 2017 08:48 PM)UserUser123123 Wrote: [\[CITE\]](#) im almost through "eli the computer guy's" networking tutorials, where should i go from there? and what is the difference between c,c+,c++, and c# and what is the most used in that hacking community?

If networking is what you are interested in [because you mentioned networking tutorial], go for a CCNA course. You can even find CCNA study materials. However, when you proceed, make sure you flow a programming language alongside it so you can control various aspect for it. Python might be a good programming language to start with because it has a lot of libraries available. Though any programming language that allows socket programming [i.e. just about every programming language you have heard about] would work.

C is a low level programming language, and by low level I mean programming language where you create everything from scratch. Learning C has a big advantage, you are more likely to understand how things operate under the hood.

There is no C+, C++ [in C language C ++ is a syntax sugar for C + 1]. C++ is pretty much an extension of C created to allow Object Oriented Programming.

C# is a programming language based on .NET framework. What this does it, regardless of whether you are using a 32 bit process or 64 bit process, regardless of what operating system you have [assuming you are not directly invoking a system call.. you will be more familiar when you start learning about system programming, ignore it for now], it should be able to run the code. It's because these codes get translated into something called byte codes. A computer need only have a compiler that can change the byte code to run in the processor. Normal C program get converted into machine instruction, specific for a processor architecture. Once converted it can't really be changed.

To put it another way C# will run on every computer that has Windows, unless it's been specifically modified to prevent a .NET program from running. It is also a type safe language and by default will prevent generally occurring vulnerabilities in your programs like buffer overflow, infinite loop etc.

Lastly, there is no programming language made specifically for hacking or hackers. Every programming language works. At the end of the day , all you are doing is creating instructions for the process [CPU]. CPU isn't racists, to go look this codes came from C so I'll execute it in one way, but that code came from blood python I'm going to mess it up because I can. They all get used the same way.

There are scripting languages . they are easier to write but because they aren't as low level you might not really be able to drill down to certain interface and you lose power because of it. For things you want created quick with less hassel and as long as they do their job it's enough, you would normally use scripting language. For exploit development, language of choice is generally ruby , python and perl.

Your language choice depends on what you are trying to learn. If you are trying to learn about remote computer exploitation over the internet, the only interface you have readily available to interact with your victim's computer is your web browser. So you would be better suited to learn javascript because every browser understand those. You could create a program that does the same thing in say C, Python, C++ , Delphi etc but your browser might not readily understand the code.

So pick a field first. For basic networking hacking, you want to learn package management so any scripting language [or low level language if you want to go that way] would do, because virtually

everything today supports socket programming.

kat.sib - September 8, 2017, 12:12 am

I need the keylogger for android. I don't have the target device so I'm trying to find out if it's possible to install it remotely. The only thing I've ever tried is Hoverwatch. I don't know how I can get the person install an apk.

tonitones - September 9, 2017, 10:31 am

(Sep 1, 2017 06:08 AM)SysAdmin Wrote: [\[CITE\]](#) FUD means Fully Undetectable, it's usually used in terms with stub files.

You'll mainly see this being used in Crypter threads, as Crypters make the files FUD (Basically means that it can bypass any AV currently available). There's also UD (Undetectable) which means that it's undetected by most, but not all AV's and Detected, which is pretty self explanatory
NOW I KNOW. Thank you siir! ?

Jati - September 9, 2017, 10:53 am

I have a few questions:

Any good keylogger (link please)

Once I infect a PC with the keylogger, is it possible for me to remove the keylogger from that pc?

Any website I can legally test DDOS?

Any good RAT (link please)

Thanks!

SysAdmin - September 9, 2017, 11:04 am

(Sep 9, 2017 10:53 AM)Jati Wrote: [\[CITE\]](#) I have a few questions:

Any good keylogger (link please)

Once I infect a PC with the keylogger, is it possible for me to remove the keylogger from that pc?

Any website I can legally test DDOS?

Any good RAT (link please)

Thanks!

Google or search around HF, (No)

Yes

DDoS Discussion is not allowed around here, read the [Help Docs](#).

Depends on what features you're looking for, there's an entire section dedicated to RAT's, go look at them, (No)

UserUser123123 - September 9, 2017, 5:25 pm

im sorry if this is a stupid question, what is .NET framework and what relevance does it have in hacking/coding?

Asdethprime - September 10, 2017, 6:12 am

(Sep 9, 2017 05:25 PM)UserUser123123 Wrote: [\[CITE\]](#) im sorry if this is a stupid question, what is .NET framework and what relevance does it have in hacking/coding?

That's a pretty straight forward question. But to give you a holistic picture forget about .NET framework for a second and let's pretend we are some big ass programmers.

So you are a programmer and you create your code using whatever programming language you like. Let's say you use C programming language. The code you write in C is called high level codes

because it's just intended to make a programmers life easier. In reality, your computer does not understand any of the codes you typed in. What needs to be done is convert the C programming code into machine language that your computer can understand and execute. This process is called compilation.

Turns out, if you create a program in one operating system (say Windows 7) using on particular processor (say intel x86), the machine code you end up creating will often only work on the same operating system and same computer architecture. If someone were to use Linux for example, or 64 bit intel chip, or an AMD chip; the program you created essentially won't work.

That's a problem right?

To make it even worse, something programs written in one language have trouble interacting with programs written in other language.

From a developers point of view that's a nightmare. We want our program to run anywhere, we don't like this bullshit.

So the solution was, why not come up with a framework that ensure you can run a program in different operating system and different architecture. Microsoft's answer to that was the .NET framework. What they did was allowed the option for all sort of manufactures [Intel, ARM, AMD] and a whole sort of operating system [OSX, Linux] to have the .NET framework, and if they did, any program that you create in the said framework would work on computers that have the said framework installed.

In Windows it comes pre-installed. A program written in .NET framework from a 32 bit computer will work on another Windows running on 64 bit. It also makes sure that one program create using .NET framework will be able to interact with another program created in the .NET framework. This obviously helps because, these days, when the conversation is taking place over the internet, people can have all sort of devices with all sort of OS running.

.NET framework is Microsoft, Java does something very similar themselves.

Makes sense?

Pirataccio - September 10, 2017, 7:47 am

(Sep 7, 2017 04:49 PM)Molino. Wrote: [\[CITE\]](#) I'll come back a bit later with some commands you can run to make sure what the problem is, or if there is even one.

Hey people

I've found these commands from terminal:

```
# ip route add 192.168.0.0/16 dev eth0
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j MASQUERADE
# iptables -F
# iptables -t nat -F
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j SNAT --to-source 143.89.111.111
# ip route add default via 192.168.0.1 dev eth0
# iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.2:8080
# iptables -A FORWARD -p tcp -d 192.168.1.2 --dport 8080 -j ACCEPT
```

What do you think?

Can they work?

Molino. - September 10, 2017, 1:35 pm

(Sep 10, 2017 07:47 AM)Pirataccio Wrote: [\[CITE\]](#) Hey people
I've found these commands from terminal:

```
# ip route add 192.168.0.0/16 dev eth0
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j MASQUERADE
# iptables -F
# iptables -t nat -F
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j SNAT --to-source 143.89.111.111
# ip route add default via 192.168.0.1 dev eth0
# iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.2:8080
# iptables -A FORWARD -p tcp -d 192.168.1.2 --dport 8080 -j ACCEPT
```

What do you think?

Can they work?

Wasn't your problem related to the range of an AP, and not being able to connect to it?

If so, then I really don't see how this could help.

From what you posted, first you are creating a new route directed to a subnet (192.168.0.0/16) using a ethernet connection. You then enable packet forwarding, and then setup a series of iptable rules and setup the traffic routing (pretty sure it even setups ip redirection (iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.2:8080) to a local web server).

This as nothing to do with finding or fixing the range of an AP afaiik.

UserUser123123 - September 10, 2017, 9:41 pm

any free good networking courses? and how did you learn networking?

ps. thanks so much youve really helped Asdethprime sorry i havent been thanking you lol

HangMansheart - September 10, 2017, 9:43 pm

I was accepted into Secrecy and was unable to receive the message containing the discord link in time, as I was out of town. I'll send you a pm. Is there any possibility I can get a new and working link in pm's?

Asdethprime - September 11, 2017, 3:36 am

(Sep 10, 2017 09:41 PM)UserUser123123 Wrote: [\[CITE\]](#) any free good networking courses? and how did you learn networking?

ps. thanks so much youve really helped Asdethprime sorry i havent been thanking you lol
You are most welcome.

There are CCNA courses you can find on youtube. They are a pretty decent place to learn about networking.

I personally prefer learning from a book, as the concepts are often explained in details. If you are like me, and don't mind reading for a book, I'd like to suggest an alternate path to learn networking:

1) Being with Networking for Dummies.

<http://www.nortonaudio.com/Ficheiros/1118474082.Netwo.pdf>

This, as the name suggests, is dedicated for absolutely beginners. Even if you know bit's and peices about networking it's always good to go through this. As per being a hacker, creating hacking tools, you won't be able to either after just having read this book. This will however give you the introductory information to dive deeper.

2) Linux Network Administrator's Guide

<http://www.tldp.org/LDP/nag2/nag2.pdf>

This is more advanced and once you are done with the book, provided you understand it, you should now be able to do most network related things on your computer. This will provide you a solid foundation on how networking works, and how you can manage your networking interfaces through your computer.

This book is more advance, go through this slowly and try things out. You will understand how the concept of networking works in a Linux system [the concepts are very similar for Windows though you might want to read up on associated books], what security measure are in place and really get an understanding of what you can and can't do.

3) Learning Python Network Programming

<http://books.tarsoit.com/Learning%20Python%20Network%20Programming.pdf>

This will teach you how to create network programming. Reverse-shell, bind-shell, all these stuffs you keep hearing. Well you can create those and more with this.

4) Violent Python: A cookbook for hackers

https://7chan.org/pr/src/Violent_Python_A_Cookbook_for_Hackers_Forensic_Ana.pdf

This is technically not only related to networking [although it has useful component], this should get you well and truly started on your journey into hacking.

DISCLAIMER: If you are thinking, oh 4 books will take time but once I finish them I'll become a hackers YaY!! then be warned. It's not necessarily so. You will have a lot of key skills , you can create your own hacking tools, extends tools you get online and a lot more. But hacking, at the end of the day, is finding new things. Finds vulnerabilities that no one knows about. You can't necessarily do that just by reading books.

Hope this helps.

(Sep 10, 2017 07:47 AM)Pirataccio Wrote: [CITE](#) Hey people
I've found these commands from terminal:

```
# ip route add 192.168.0.0/16 dev eth0
# echo 1 > /proc/sys/net/ipv4/ip_forward
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j MASQUERADE
# iptables -F
# iptables -t nat -F
# iptables -t nat -A POSTROUTING ! -d 192.168.0.0/16 -o eth1 -j SNAT --to-source 143.89.111.111
# ip route add default via 192.168.0.1 dev eth0
# iptables -A PREROUTING -t nat -i eth0 -p tcp --dport 80 -j DNAT --to 192.168.1.2:8080
# iptables -A FORWARD -p tcp -d 192.168.1.2 --dport 8080 -j ACCEPT
```

What do you think?

Can they work?

This code will allow you to make your private IP routable through internet.

If you were looking to RAT someone, and you can't get the stub to connect to you. That's the fix. If you have seen people talking about, how do i port forward, help port forwarding, can't get a connection from RAT, revershell not responding etc etc.

That's the fix.

It won't however fix a problem if this has to do with not being able to connect to a Wifi access point. The problem is likely to do with your network adapter.

For that first check if you interface is properly set up:

<http://linuxcommando.blogspot.com.au/2013/10/how-to-connect-to-wpawpa2-wifi-network.html>

Before jumping to step 8 on though make sure you try the following:

Code ping 127.0.0.1

ping 192.168.1.1

192.168.1.1 would be replaced by your default gateway. 192.168 are unlikely to change but you could have variations of this:

192.168.0.1

192.168.0.254

192.169.1.254

Those are the most common address used for gateway.

If you can ping yourself (127.0.0.1) and ping your gateway successfully then finally try pinging to a site on the internet.

Scrubkid33 - September 11, 2017, 3:53 am

I tried and had no problems with both Spy Note 4 and DroidJack 4 (except for whatsapp txts because it needs root). Pics, contacts, normal sms... All fine.

But what im looking for is either;

1- Stealing all passwords that are stored in the phone. (Removing accounts and keylogger seems like a good idea but how?)

2- A remote desktop stuff that will let me use the phone silently background like it was mine.

Any help will be super appreciated Pirate

Asdethprime - September 11, 2017, 4:05 am

(Sep 11, 2017 03:53 AM)Scrubkid33 Wrote: [\[CITE\]](#) I tried and had no problems with both Spy Note 4 and DroidJack 4 (except for whatsapp txts because it needs root). Pics, contacts, normal sms... All fine.

But what im looking for is either;

1- Stealing all passwords that are stored in the phone. (Removing accounts and keylogger seems like a good idea but how?)

2- A remote desktop stuff that will let me use the phone silently background like it was mine.

Any help will be super appreciated Pirate

Well for the first you would want to look into mimikatz. That's an open source program created for

the same purpose, to extract saved passwords.

<https://github.com/cSploit/android.MSF/blob/master/lib/rex/post/meterpreter/extensions/mimikatz/mimikatz.rb>

Have a look at this. It uses Ruby and is created for android.

For the second though, it's not as easy. You would need Virtual Desktop, for computers it's normally easier because they have built in system calls that allow you to do so [createvirtualdesktop() on Windows for example]. I do not believe there this is a built in feature on Android and iOS. You would need to install additional softwares for this.

This will require you to access google play / appstore and their respective credentials, which is not a trival task.

Though I will admit, mobile OS isn't my strong suite. Perhaps someone knowledgeable can answer your second query.

P.S. I hope I don't get yelled at for helping. I am not really a member of secrecy. In case you guys have an issue with this please let me know and I will stop.

UserUser123123 - September 11, 2017, 8:24 pm

hello so i have been playing around with linux on a vm and came across arp-scan to find mac addresses on my network.but i just comes up with 3 - none of which are any phone, tv, or computer in my household. idk why maybe because im using ethernet? and im useing ubuntu with the xcfe environment. and what are some other ways i can see mac addresses that are on my network

and what is the difference between the current mac address and a permanent mac address. and can i spoof the permanent mac address and/or can i get tracked by it.

Asdethprime - September 11, 2017, 9:50 pm

(Sep 11, 2017 08:24 PM)UserUser123123 Wrote: [\[CITE\]](#) hello so i have been playing around with linux on a vm and came across arp-scan to find mac addresses on my network.but i just comes up with 3 - none of which are any phone, tv, or computer in my household. idk why maybe because im using ethernet? and im useing ubuntu with the xcfe environment. and what are some other ways i can see mac addresses that are on my network

and what is the difference between the current mac address and a permanent mac address. and can i spoof the permanent mac address and/or can i get tracked by it.

For arp-scan try the following code:

Code sudo arp-scan --localnet

If you are unsure if that's the correct result and you want to check things manually, you can leverage other tools to help you with this.

My tool of choice is normally nmap, though any equivalent can be used too [masscan, fping, ping etc would work].

Code sudo nmap -T5 -sL 192.168.1.0/24

THIS SCAN WILL TAKE FEW MINUTES AS EVERY POSSIBLE IP IS PROBED. BE PATIENT, IT WILL WORK AND CLEARLY SHOW AN ERROR AND EXIT OTHERWISE.

NOTE: here I am assuming my network address is 192.168.1.0, yours might be different. 192.168

part is unlikely to change. The 3 octane could however change.

Normally it's either :

192.168.1.0

192.168.0.0

To find what IP address your network has try one of the following:

Code ifconfig

ip address

Either of the command will work. You want to look into your WLAN section (it's commonly called wlp0) to find your network address, under the section inet. All you do is ignore the last digit and change it to 0. For example if inet is showing 192.168.0.102 , your network address is 192.168.0.0 (just change the last bit 102 to 0)

That will give you a long list (254 addresses) to scroll through, but any device that has a host-name should be on the list.

You can further probe using arp-fingerprint, which in turn uses a set of arp-scan commands internally. Example , trying to see what the mac address of 192.168.1.104 is:

Code arp-fingerprint 192.168.1.104

The device needs to answer your ping require for you to be able to fingerprint it.

For the second part, current mac address is the mac address that has been set for a device. Permanent mac address is the address that is hard-coded in the device firmware.

What happens is, everytime you get a device it has a physical address called MAC address. This address is hardcoded [typed manually] in the device firmware [the software that comes built in with the device].

You can however, for your convenience, change the MAC address to something other than what has been hard-coded in the firmware. That's called your current mac address.

In regards to being tracked, it's not actually easy (or often even possible) to track someone using MAC address. MAC address, by nature, is a FLAT ADDRESS [i.e. an address that says nothing about the location]. You hardware manufacture do keep a record of MAC addresses when they orginally ship the computer to you, but because you can, at any time, change the network interface card, it's not an address that is used to track people.

In order to track someone, we need a logical address [an address that tells you about the location of the device]. This is your IP address.

Contro3 - September 12, 2017, 1:55 am

I replayed on the thread of strings chain linked to this post-it. Please consider and I willingly will wish with words because I lack loathingly (the) logic listed (to) learn life lessons listed. PM.

UserUser123123 - September 12, 2017, 6:50 am

yeah, arp when i say

'sudo arp-scan --localnet'

it comes up with these three things:

10.0.2.2

10.0.2.3

10.0.2.3

and thats it. when i ping my phone it works fine. the nmap scan:

```
sudo nmap -T5 -sL 192.168.1.0/24
```

came up with 192.168.0.1 to 255 and there was nothing after that.

the arp-fingerprint when i did my phone it said no response. idk why like i said before i can ping it fine.

Asdethprime - September 12, 2017, 7:47 am

(Sep 12, 2017 06:50 AM)UserUser123123 Wrote: [\[CITE\]](#) yeah, arp when i say

```
'sudo arp-scan --localnet'
```

it comes up with these three things:

10.0.2.2

10.0.2.3

10.0.2.3

and thats it. when i ping my phone it works fine. the nmap scan:

```
sudo nmap -T5 -sL 192.168.1.0/24
```

came up with 192.168.0.1 to 255 and there was nothing after that.

the arp-fingerprint when i did my phone it said no response. idk why like i said before i can ping it fine.

Oh so your network address is 10.0.2.0, that's interesting.

Can you try re-running nmap with the following code

```
Code sudo nmap -T5 -sL 10.0.2.0/24
```

If you just get IP address [it will always show you IP going from 10.0.2.0 to 10.0.2.255] but has no hostname attached to it then it's not picking anything up.

Can you try that. It does work fine on my end. Not only am I able to pick up my mobile and PCs, it only picks up chrome cast.

I will have to look into the arp-scan part, because for scanning I normally only use nmap, that's the mapper I am most comfortable with.

Jati - September 12, 2017, 11:01 am

I just need a good free rat, and please don't say njRAT as I tried it out, and it took me about an hour to first send it, then for the person to turn all antiviruses and things, and on the end it didn't work as .NET couldn't be installed, anything else?

UserUser123123 - September 12, 2017, 3:43 pm

my phone network address is 192.168.0.19 idk if that has any relevance
and nmap came up with 0 hosts found

mutybyte - September 12, 2017, 6:37 pm

I want to know about /etc/exports and no_root_squash

Please explain these in detail as i am unable to understand from google.

also i want to know about this ->

<https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#suid-binary>

Asdethprime - September 12, 2017, 6:38 pm

(Sep 12, 2017 03:43 PM)UserUser123123 Wrote: [\[CITE\]](#) my phone network address is 192.168.0.19

idk if that has any relevance
and nmap came up with 0 hosts found
I am all confused now, because for arp you used a different one.

Try something simpler:

Code ifconfig

This should show you the interface you have, at least one of which will have an inet address.

Something like this:

```
inet 192.168.0.111 netmask 255.255.255.0 broadcast 192.168.0.255
```

Note down the interface name.

In mine it's wlp12s0

Try this then

Code arping -I wlp12s0 -c 5 192.168.0.19

The mac address for the phone should be displayed inside []

Something like

```
Unicast reply from 192.168.1.1 [19:F0:45:16:EF:8B]
```

Does that work?

Emily Brontë - September 12, 2017, 6:39 pm

Know of anyway to exploit a ColdFusion version 9 website? Primarily the admin panel

UserUser123123 - September 12, 2017, 7:12 pm

inet is 10.0.2.15 . but in order to port forward and do stuff on my router i type in 192.168.0.1 idk if my vm is just nutty or what.

and the arping thing says 0 packets received.

out of courosity i put "ipconfig" in cmd and the default gateway is 192.168.0.1

and the other things are:

```
netmask: 255.255.255.0
```

```
broadcast: 10.0.2.255
```

and im also confused on what bash is.

SysAdmin - September 13, 2017, 2:00 am

(Sep 12, 2017 06:39 PM)Emily Brontë Wrote: [\[CITE\]](#) Know of anyway to exploit a ColdFusion version 9 website? Primarily the admin panel

<https://goo.gl/94nzJt>

(Sep 12, 2017 07:12 PM)UserUser123123 Wrote: [\[CITE\]](#) inet is 10.0.2.15 . but in order to port forward and do stuff on my router i type in 192.168.0.1 idk if my vm is just nutty or what.

and the arping thing says 0 packets received.

out of courosity i put "ipconfig" in cmd and the default gateway is 192.168.0.1

and the other things are:

```
netmask: 255.255.255.0
```

```
broadcast: 10.0.2.255
```

and im also confused on what bash is.

The Default Gateway should be 192.168.0.1, however, I've seen some Modems / Routers that refuse connections if they are done via WiFi. You also need a very specific WiFi adapter that can catch packets.

Bash:

[https://en.wikipedia.org/wiki/Bash_\(Unix_shell\)](https://en.wikipedia.org/wiki/Bash_(Unix_shell))

UserUser123123 - September 13, 2017, 6:43 am

what are some wireless access points that have an ethernet port and is capable of packet injection?

6789 - September 13, 2017, 12:58 pm

If i have the original creation email to an Instagram account i want, what is the best way to get into it. Thanks

SysAdmin - September 13, 2017, 1:09 pm

(Sep 13, 2017 12:58 PM)6789 Wrote: [\[CITE\]](#) If i have the original creation email to an Instagram account i want, what is the best way to get into it. Thanks

I would recommend looking through Leaked Databases, you may get lucky and get passwords or bigger clues to what the password could be.

6789 - September 13, 2017, 1:11 pm

(Sep 13, 2017 01:09 PM)SysAdmin Wrote: [\[CITE\]](#) I would recommend looking through Leaked Databases, you may get lucky and get passwords or bigger clues to what the password could be. i currently dont have the btc to get a leakbase subscription but i have hundreds of DBs that i search with AstroGrep and i couldnt find any results

SysAdmin - September 13, 2017, 1:13 pm

(Sep 13, 2017 01:11 PM)6789 Wrote: [\[CITE\]](#) i currently dont have the btc to get a leakbase subscription but i have hundreds of DBs that i search with AstroGrep and i couldnt find any results You're not in luck then. Unless you know the account owner in person, you're not going to get far. You could spoof an email and send it to the targets email and do a phishing attack. Can't really get into detail of that though, disallowed topic around here.

6789 - September 13, 2017, 1:25 pm

(Sep 13, 2017 01:13 PM)SysAdmin Wrote: [\[CITE\]](#) You're not in luck then. Unless you know the account owner in person, you're not going to get far. You could spoof an email and send it to the targets email and do a phishing attack. Can't really get into detail of that though, disallowed topic around here.

ok bro, would you mind contacting me offsite about this?

SysAdmin - September 13, 2017, 1:38 pm

(Sep 13, 2017 01:25 PM)6789 Wrote: [\[CITE\]](#) ok bro, would you mind contacting me offsite about this?

sysadminhf@xmpp.jp

6789 - September 13, 2017, 1:48 pm

(Sep 13, 2017 01:38 PM)SysAdmin Wrote: [\[CITE\]](#) sysadminhf@xmpp.jp sent you an email, thanks

SysAdmin - September 13, 2017, 1:51 pm

(Sep 13, 2017 01:48 PM)6789 Wrote: [\[CITE\]](#) sent you an email, thanks That is XMPP, get a chat, not send me an email, lol.

6789 - September 13, 2017, 1:54 pm

(Sep 13, 2017 01:51 PM)SysAdmin Wrote: [\[CITE\]](#) That is XMPP, get a chat, not send me an email, lol.

i signed up 21 minutes ago lmao, usually on other forums.

SysAdmin - September 13, 2017, 1:54 pm

(Sep 13, 2017 01:54 PM)6789 Wrote: [\[CITE\]](#) i signed up 21 minutes ago lmao, usually on other forums.

Use Pidgin or some other service.

6789 - September 13, 2017, 2:10 pm

(Sep 13, 2017 01:54 PM)SysAdmin Wrote: [\[CITE\]](#) Use Pidgin or some other service.

lmao im not used to all this shit, im trying to add an account to pidgin what do i put for the domain and resource and all that

UserUser123123 - September 13, 2017, 3:48 pm

i wanna learn how to code. im learning html. should i continue or stop html is useless. the languages i want to learn are:

Python

Javascript

C#

php

should i continue to learn html the learn other code languages or just skip to python or php and what are good websites/tutorials to learn code.(reading is not my strongsuit).

Bronze5 - September 13, 2017, 6:33 pm

(Sep 13, 2017 03:48 PM)UserUser123123 Wrote: [\[CITE\]](#) i wanna learn how to code. im learning html. should i continue or stop html is useless. the languages i want to learn are:

Python

Javascript

C#

php

should i continue to learn html the learn other code languages or just skip to python or php and what are good websites/tutorials to learn code.(reading is not my strongsuit).Html is rlly easy.. I mean rlly easy its the basic. Finish learning html and just start C# or python. Tbh in my opinion language depends on what you are going for. But there will be a time where u will need most of the languages. so tldr -

finish html learn what you want to doesnt rlly fucking matter

UserUser123123 - September 14, 2017, 6:56 am

what free domains can i use or make for xamp? sorry im new to xamp and all this.

UserUser123123 - September 15, 2017, 3:44 pm

hello anyone there? seems people have been gone?

what sim cards take javascript?

Pronouncer - September 18, 2017, 5:47 pm

Sorry everyone we have all been really busy lately, we will be continuing this service

UserUser123123 - September 19, 2017, 10:19 am

when people say learn "networking" is that mainly TCP/IP and everything about that? and, from what i see there are no really good tutorials for C, what are some, and how did you learn?

Molino. - September 19, 2017, 10:42 am

(Sep 19, 2017 10:19 AM)UserUser123123 Wrote: [\[CITE\]](#) when people say learn "networking" is that mainly TCP/IP and everything about that? and, from what i see there are no really good tutorials for C, what are some, and how did you learn?

No. TCP/IP is just part of what you should learn. Secrecy provides a Networking Guide [Here](#) which

can get you well started on understanding networking concepts and everything you'll get into.

As of C, I learned the basics online on websites like [This](#). After learning the basics, I started trying new challenges, and every times I found something I didn't know how to code, I would search online.

I thought CodeAcademy also had a C cource, but looks like it doesn't. I'll try to find a C course and edit later.

UserUser123123 - September 19, 2017, 11:32 am

(Sep 19, 2017 10:42 AM)Molino. Wrote: [\[CITE\]](#) No. TCP/IP is just part of what you should learn. Secrecy provides a Networking Guide [Here](#) which can get you well started on understanding networking concepts and everything you'll get into.

As of C, I learned the basics online on websites like [This](#). After learning the basics, I started trying new challenges, and every times I found something I didn't know how to code, I would search online.

I thought CodeAcademy also had a C cource, but looks like it doesn't. I'll try to find a C course and edit later.

thank you

UserUser123123 - September 22, 2017, 4:26 pm

what is promiscuous mode and how does it differ from normal?

Baud - September 22, 2017, 5:08 pm

(Sep 22, 2017 04:26 PM)UserUser123123 Wrote: [\[CITE\]](#) what is promiscuous mode and how does it differ from normal?

When your wireless card enters promiscuous mode it sends to the CPU every packet it finds in its range, so even packets that were meant to be received by other devices connected to the same network, while the non promiscuous mode drops every packet that doesn't contain your own machine's MAC address, since you're not supposed to receive and read those packets.

This mode is typically used to troubleshoot networks, or, as most people do, sniffing network traffic since you can literally read every transmission that is sent in your network. Keep in mind that sensitive data is (almost) always encrypted, you can't always tell what a client is doing by reading their packets if you don't decrypt them, and some of them even have a checksum to prevent sniffing.

UserUser123123 - September 22, 2017, 9:03 pm

thank you, i have a new question:

what is arp spoofing/poisoning?

Baud - September 23, 2017, 4:09 am

(Sep 22, 2017 09:03 PM)UserUser123123 Wrote: [\[CITE\]](#) thank you, i have a new question: what is arp spoofing/poisoning?

ARP poisoning and spoofing are two different names for the same attack, you may also find it called as ARP cache poisoning or rerouting, it's always the same.

ARP stands for Address Resolution Protocol, and as the name says it's a network protocol used inside local networks to associate a client's IP address with its own MAC address, this way each device knows where to send a packet by knowing the destination IP. All the definitions of IP ----> MAC are saved in a file called ARP cache, or also ARP tables.

What the attack in itself does is sending ARP packets to a target crafted in a way that your target saves in their ARP cache someone else's IP address associated with the attacker's MAC. This

means that every packet directed to the victim's IP is going to be redirected to the attacker instead, who may read its content, edit it, resend it to the victim, or drop it. This is the basis of more complex attacks like MITM (man in the middle).

UserUser123123 - September 24, 2017, 9:53 pm

what exactly can you do with a mac address? and what are the things like, taking it down, tracking it etc.

Baud - September 25, 2017, 12:21 am

(Sep 24, 2017 09:53 PM)UserUser123123 Wrote: [\[CITE\]](#) what exactly can you do with a mac address? and what are the things like, taking it down, tracking it etc.

First of all a MAC address can reveal informations about the device manufacturer, it can for example tell us if it's an iPhone, or any other device made by a company that has special patterns that some port scanners can recognize and report during a port scan when you ask them to identify a system.

Then of course there's MAC spoofing, which can allow you to have access to networks with restricted access if they only allow specific devices on an access control lists based on MAC addresses.

Also if the device you know the MAC of is an access point you could intercept the packets forwarded and received by it, so basically sniffing data. As you can see there are many applications for a MAC address, and there are many more I didn't mention because it would simply take too long, that's how important they are. You can track a device only with an IP but only if it's public, not if it's private (the IP it has inside its local network). And if by taking it down you mean disconnecting it from the local network then yes it can be done, but if it's not what you meant then no.

JumpT - September 25, 2017, 1:37 am

Thanks for the guide, helpfully repository for useful links.

UserUser123123 - September 25, 2017, 6:47 am

thanks, can you spoof your host id? so say im 192.168.0.17 can i spoof/change that so it says im 192.168.0.13?

Baud - September 25, 2017, 8:41 am

(Sep 25, 2017 01:37 AM)JumpT Wrote: [\[CITE\]](#) Thanks for the guide, helpfully repository for useful links.

Glad to be of help, keep the questions coming if you have any.

(Sep 25, 2017 06:47 AM)UserUser123123 Wrote: [\[CITE\]](#) thanks, can you spoof your host id? so say im 192.168.0.17 can i spoof/change that so it says im 192.168.0.13?

Yes, IP spoofing is possible but most of the times it depends if the software you're using supports it or not, for example to spoof your IP in your case this is what you'd need to do on nmap:

Code `nmap -e eth1 -S 192.168.0.13 your_target.com`

Where eth1 is your network interface, that you can get either from ifconfig or nmap like this:

Code `nmap --iflist`

Look for the interface that has your same MAC and that's the one you have to use. If a program you need to use doesn't support IP spoofing you might want to setup a proxy and route your traffic through it.

UserUser123123 - September 25, 2017, 8:49 pm

(Sep 25, 2017 08:41 AM)Baud Wrote: [\[CITE\]](#) Glad to be of help, keep the questions coming if you have any.

Yes, IP spoofing is possible but most of the times it depends if the software you're using supports it or not, for example to spoof your IP in your case this is what you'd need to do on nmap:

Code `nmap -e eth1 -S 192.168.0.13 your_target.com`

Where eth1 is your network interface, that you can get either from ifconfig or nmap like this:

Code `nmap --iflist`

Look for the interface that has your same MAC and that's the one you have to use. If a program you need to use doesn't support IP spoofing you might want to setup a proxy and route your traffic through it.

thank you,im sorry if this is a stupid question, but what do you mean by: 192.168.0.13 is that saying thats the target im spoofing or is that me? and your_target.com? one again sorry, but i just want to understand before i use something like this.

Baud - September 26, 2017, 1:31 am

(Sep 25, 2017 08:49 PM)UserUser123123 Wrote: [\[CITE\]](#) thank you,im sorry if this is a stupid question, but what do you mean by: 192.168.0.13 is that saying thats the target im spoofing or is that me? and your_target.com? one again sorry, but i just want to understand before i use something like this.

It's just an example, since in the previous post you wanted to spoof your address into 192.168.0.13 I used it in my example too to rapresent the spoofed IP, and you have to substitute your_target.com with the actual target you want to scan with nmap, if you don't have experience with it nmap is a port scanner and the command I gave you performs a simple port scan of the most common ports after spoofing your address into the one you give it.

geroja - September 30, 2017, 10:09 pm

Can you please help me hack this android game? Please pm me your discord or Skype info just in case you can hack it. Thanks

Game Name: Luxy Poker

Game Version: 1.6.1.2

Google Play Store Link: Luxy Poker-Online Texas Holdem - Android Apps on Google Play

APK Link: Luxy Poker-Online Texas Holdem APK Download - Free Casino GAME for Android | APKPure.com

Cheat Requested: I'm requesting chips hack and also they have Vegas section with slot machine, Bacarat, and subio. The Vegas section you gamble on different machine to get chips so any hack there would help.

Have you used any cheat engines?: I have tried SBGameHacker and GameKiller but it won't permanently change the chips. It does manipulate t

Baud - October 1, 2017, 2:41 am

(Sep 30, 2017 10:09 PM)geroja Wrote: [\[CITE\]](#) Can you please help me hack this android game? Please pm me your discord or Skype info just in case you can hack it. Thanks

Game Name: Luxy Poker

Game Version: 1.6.1.2

Google Play Store Link: Luxy Poker-Online Texas Holdem - Android Apps on Google Play

APK Link: Luxy Poker-Online Texas Holdem APK Download - Free Casino GAME for Android | APKPure.com

Cheat Requested: I'm requesting chips hack and also they have Vegas section with slot machine, Bacarat, and subio. The Vegas section you gamble on different machine to get chips so any hack there would help.

Have you used any cheat engines?: I have tried SBGameHacker and GameKiller but it won't permanently change the chips. It does manipulate t

Please read the rules on the very first message of the thread: this is a helpdesk, we answer questions, we don't fill requests.

By the way if the game connects online local hacks are not going to work anyway, but if they did don't expect someone to spend their time to make this for free.

UserUser123123 - October 6, 2017, 5:03 pm

umm i have a question, what can you accomplish with dns spoofing? is it a type of MITM attack or?

and what can you get from this?
thanks in advance.

def shock - October 7, 2017, 4:03 am

(Oct 6, 2017 05:03 PM)UserUser123123 Wrote: [\[CITE\]](#) umm i have a question, what can you accomplish with dns spoofing? is it a type of MITM attack or?

and what can you get from this?
thanks in advance.

> Assuming you know what DNS protocol does

Quote:In short; DNS stands for Domain Name System, it's a database that links host names to ip addresses and vice versa. Normally operates on port 53, UDP. > Assuming you are refering to DNS cache poisoning

Quote:You 'poison' the DNS domaintable, meaning that you'll change a legitimate address to one of your fake addresses. When the user goes to a specific website which is stored in the poisoned DNS table, it'll go to your fake website.

Baud - October 7, 2017, 5:16 am

(Oct 7, 2017 04:03 AM)def shock Wrote: [\[CITE\]](#) > Assuming you are refering to DNS cache poisoning
DNS spoofing exists too, it's only achievable in full duplex MITM attacks though: when a victim queries the IP address of a wanted domain (say example.com) the gateway will send a DNS response back to the victim once the IP is obtained from all the DNS nodes, the response is intercepted by the attacker, who injects the malicious IP instead of the legit one, then forwards the packet to the victim so that the malicious IP is opened instead.

mohanad4egy - October 7, 2017, 2:17 pm

yay thanks i hope i learn new things

mutybyte - October 7, 2017, 8:34 pm

I want to know about "pivoting","proxychains","active window directory"

Baud - October 8, 2017, 6:37 am

(Oct 7, 2017 08:34 PM)mutybyte Wrote: [\[CITE\]](#) I want to know about "pivoting","proxychains","active window directory"

Pivoting is essentially the technique of using a computer you infected to perform tasks for you by using that machine as a proxy, for example: assume you hack into machine A, A is connected to the Internet but it's also part of its local network, where other machines like B and C are connected, however B and C are not connected to the Internet so you apparently can't access them. However if you manage to get a shell on A you can use it as a proxy, by doing this you would be able to reach also the other machines connected to the local network of A, like B for example, which you could scan for vulnerabilities, exploit, and thus having access to B as well now. It's commonly used to hack into Intranets for this reason, it allows you to move within a local network without being physically connected into it, this is important because oftentimes computers containing important and sensitive data are not connected to the Internet on purpose to make that data unavailable to potential attackers.

Proxychains is simply a tool you can use to set up a chain of proxies, which simply means you are going to have more than one proxy in between you and the server for every packet you send, this is going to make your connection safer albeit slower, but you can also use it for example to set up one single proxy, and linking to what we said about pivoting, you could use proxychains to use a single machine you hacked as your proxy to access all the devices connected to that machine's own local network.

If you mean Active Directory then it's a group of protocols and technologies used by Microsoft for its Windows OSs to manage local networks and shared resources, this is a wide argument so talking in depth about it would take a lot of time.

UserUser123123 - October 8, 2017, 3:17 pm

what does the .stub file in crypters do, and how important are they, and what coding languages can you make them with.

thanks in advance.

sergey klykbaytovich - October 8, 2017, 3:28 pm

learn me how half duplex ip spoof work thx

Joy™ - October 8, 2017, 3:33 pm

What's the best way to go about cracking/getting into someones email? (If you already know their email address).

Baud - October 8, 2017, 4:26 pm

(Oct 8, 2017 03:17 PM)UserUser123123 Wrote: [\[CITE\]](#) what does the .stub file in crypters do, and how important are they, and what coding languages can you make them with.

The stub is an essential part of every crypter, it contains the code that decrypts and executes the hidden encrypted code, this code is in fact injected inside the stub by the crypter itself. They can be coded in any compiled programming language really, you can find them in .NET, C++... it's the programmer's choice, the important thing is that the hidden code must not be detected.

(Oct 8, 2017 03:28 PM)sergey klykbaytovich Wrote: [\[CITE\]](#) learn me how half duplex ip spoof work thx

IP spoofing works by simply changing the IP contained in the packets your computer sends, there isn't such a thing as half or full duplex IP spoofing, these two concepts are used in MITM attacks.

(Oct 8, 2017 03:33 PM)Joy™ Wrote: [\[CITE\]](#) What's the best way to go about cracking/getting into someones email? (If you already know their email address).

There are so many ways that a best one doesn't really exist, it always depends on the situation and person who owns the email: sometimes phishing can work very well if done correctly, but the first thing you should do is checking on websites like leakbase if their password was already leaked, if you are lucky you won't have to do any hard work because you could find the password in one of these public databases. Other neat things to use are password dumpers and keyloggers, they can be hidden in doc or pdf documents, or by choosing any delivery method you like, because as I said early it depends from case to case, you might want to personalize each attack and make it different to increase the chances of success on one specific person.

sergey klykbaytovich - October 8, 2017, 4:55 pm

(Oct 8, 2017 04:26 PM)Baud Wrote: [\[CITE\]](#) IP spoofing works by simply changing the IP contained in the packets your computer sends, there isn't such a thing as half or full duplex IP spoofing, these two concepts are used in MITM attacks.

define nat poisoning

Baud - October 8, 2017, 5:01 pm

(Oct 8, 2017 04:55 PM)sergey klykbaytovich Wrote: [\[CITE\]](#) define nat poisoning
In case you didn't bother reading the rules:

(Jul 22, 2017 01:03 PM)Great White Shark Wrote: [\[CITE\]](#) [*]Do not spam or ask any troll questions.

sergey klykbaytovich - October 8, 2017, 5:09 pm

(Oct 8, 2017 05:01 PM)Baud Wrote: [\[CITE\]](#) In case you didn't bother reading the rules:
it is a thing by theory
something you don't know isn't trolling

Baud - October 8, 2017, 5:20 pm

(Oct 8, 2017 05:09 PM)sergey klykbaytovich Wrote: [\[CITE\]](#) it is a thing by theory
something you don't know isn't trolling

Then I'm curious to know where you heard about this and I'd like you to give me resources where I can learn more about it, since I never heard of it and after having looked it up nothing came out. Your previous question didn't seem serious either but I responded anyway because I gave you the benefit of the doubt. If you don't have said resources I'd kindly ask you to stop posting on this thread so other users may ask actual questions, thank you.