

Forum:[Hack Forums](#)

Thread: [\[Official\] Empire Hacking Help Desk](#)

Th3PonyWizard - March 17, 2014, 4:04 am

The Empire - Beginner Hacking Help Desk

Credits goes to Komodo for his writing and dedicated help as well.

Re-Opening:

Old thread. <https://hackforums.net/showthread.php?tid=4071115>

Help-desks should always be there. Not being a mandatory assignment for the sake of doing "my" part, it's for the sake of the community as a whole because they're more than "just" need it.

About Us:

We strive to provide top-notch Beginner Hacking support. Our team consists of members of The Empire who are experienced within all fields Beginner Hacking related, and more.

We will answer all of your Beginner Hacking related questions, solve all of your problems, and remotely assist you when needed.

No matter what your post count or reputation count is, we will help you to the best of our ability. We will assist and support you with any and all situations

Each member is specialized within different skills, but our members should be able to answer any question thrown at them. If not, we will state so without wasting your time.

Please remember to search for your question or problem within the Forum/Thread/Google, prior to asking it here. Thank You!

skill-set -

We have guys in most if not all known fields, consisting with the best and most knowledgeable people to their profession.

Form:

Quote:What is your question/problem:

Explain your problem the best you can: You don't really have to use it, just a way to sort things out

Supported subjects:Rating NO.

Doxing NO.

Ewhoring NO.

Beginner guidance

Web-based Hacking

Low-level exploitation

Pentesting, server auditing and exploitation

Networking

Malware analysis and removal

Programming in most languages

Whatever you can possibly think of.*

*Answer not guaranteed. We'll try our best though.

Rules:

You can answer even without being an empire member.

We have the right to not attempt answering at any time, assuming the question is misleading, poorly

written, or just is there to piss us off.

Zapu - March 17, 2014, 4:26 am

Will be lurking his help desk helping out

vaggie_talez - March 17, 2014, 4:41 am

sub'd as I'm sure this will be very educational. Thx for this.

0x03a8 - March 17, 2014, 6:24 am

Not part of empire but I just enjoy helping people :)

Posting so I'll be notified of questions & new replies :)

cyberducky - March 17, 2014, 6:26 am

I will be here answering hacking related questions as well.

RRRoooRRR - March 17, 2014, 6:44 am

Vouch vouch vouch :)

Hopefully this gets rid a lot of the junk that burdens this subforum.

-Chosen-

Cathal - March 17, 2014, 6:59 am

Holy shit, a hacking help desk not run by e-whores. Op actually knows his shit, although you never did get back to me on that challenge hehe

TR4CE - March 17, 2014, 7:07 am

I was just thinking out how does users create private proxies?

How much work does it need? Any money is required? Can anyone provide me any method for that? I will really appreciate it :)

Thanks in advance for helping me :)

0x03a8 - March 17, 2014, 7:37 am

(Mar 17, 2014 07:07 AM)TR4CE Wrote: [\[CITE\]](#) I was just thinking out how does users create private proxies?

How much work does it need? Any money is required? Can anyone provide me any method for that? I will really appreciate it :)

Thanks in advance for helping me :)

You can use infected computers for that if you want. For example, imminent monitor has a reverse proxy tool that allows you to use your victims computer as a proxy.

You can also use vps's as vpn's

TR4CE - March 17, 2014, 9:12 am

(Mar 17, 2014 07:37 AM)Semizias Wrote: [\[CITE\]](#) You can use infected computers for that if you want. For example, imminent monitor has a reverse proxy tool that allows you to use your victims computer as a proxy.

You can also use vps's as vpn's

Thats good...

But i have seen millions of proxy at HMA.... How do they get it?

I will really appreciate it :)

Th3PonyWizard - March 20, 2014, 6:20 am

(Mar 17, 2014 09:12 AM)TR4CE Wrote: [\[CITE\]](#) Thats good...

But i have seen millions of proxy at HMA.... How do they get it?

I will really appreciate it :)Lots of methods. Proxy harvesting might be done just by scanning bulk IP lists to see if they're active by checking common ports (8080 etc), crawling them from other sites, etc.

Jai999 - March 20, 2014, 7:27 am

Can you tell me how can I hide my hosting details from WHOIS and change IP for a domain? I'm buying domain using Godaddy private domain registration. Please help :)

0x03a8 - March 20, 2014, 9:14 am

(Mar 20, 2014 07:27 AM)Jai999 Wrote: [\[CITE\]](#) Can you tell me how can I hide my hosting details from WHOIS and change IP for a domain? I'm buying domain using Godaddy private domain registration. Please help :)

When you have a domain you should be able to manage everything Including contact information. The contact information is what is displayed, To be completely safe when hiding your details you need to give up some false info when registering.

#BORNE - March 20, 2014, 9:16 am

What is your question/problem: I am currently learning Python and would like a few project ideas. (just basic ones)

Thanks alot for doing this Help Desk.

0x03a8 - March 20, 2014, 9:32 am

(Mar 20, 2014 09:16 AM)UnpredictedKnight Wrote: [\[CITE\]](#) What is your question/problem: I am currently learning Python and would like a few project ideas. (just basic ones)

Thanks alot for doing this Help Desk.

Try a calculator or an rpg game they can be a good challenge

Lemonadeisprettydamngood - March 20, 2014, 9:35 am

how can I find an cloudflare IP? it wont work when I use CloudFlare Resolver.

#BORNE - March 20, 2014, 9:38 am

(Mar 20, 2014 09:32 AM)Semizias Wrote: [\[CITE\]](#) Try a calculator or an rpg game they can be a good challenge

Appreciate you getting back to me so quickly, will keep these projects in mind.

Th3PonyWizard - March 21, 2014, 5:18 am

(Mar 20, 2014 09:35 AM)Lemonadeisprettydamngood Wrote: [\[CITE\]](#) how can I find an cloudflare IP? it wont work when I use CloudFlare Resolver.Use your mind. Whether it's pinging out common subdomains or abuse the activation SMTP method, it's about getting the system puke out the IP for you by using one of it's services.

Komodo - March 31, 2014, 8:24 am

Quote:Not being a mandatory assignment for the sake of doing "my" part, it's for the sake of the community as a whole because they're more than "just" need it. This was not the reason I closed the old thread.

Even after it stopped being a Mandatory Assignment, I kept it alive.

Members stopped posting in it.

Brule - March 31, 2014, 11:01 am

I'm neither a member of The Empire, but I'll be more than happy to serve some help & knowledge.?

King Cin - April 1, 2014, 10:13 am

This is the hacking helpdesk of The Empire, not to be rude but outsiders shouldn't post answers here. If you really want to help people that post here and you're not a member of The Empire, please PM them.

Th3PonyWizard - April 1, 2014, 10:25 am

(Apr 1, 2014 10:13 AM)Unknown• Wrote: [\[CITE\]](#) This is the hacking helpdesk of The Empire, not to be rude but outsiders shouldn't post answers here. If you really want to help people that post here and you're not a member of The Empire, please PM them. I don't care who helps here as long as he knows his shit

King Cin - April 1, 2014, 10:51 am

(Apr 1, 2014 10:25 AM)Th3PonyWizard Wrote: [\[CITE\]](#) I don't care who helps here as long as he knows his shit

Oh well, if it's okay with you--disregard what I said.

?????? - April 2, 2014, 12:32 pm

Hi. I'm currently trying to "learn" networking.

I understand what an IP is, but it seems that there is more to it than I understand. There seem to be a few different types. For example, what is the difference between a 192.168.x.x and your normal 74.x.x.x? Is the first reserved for use in LANs? Meh - haven't found a definitive answer that I understand. For example: the result of the 'route' command in Linux.

Code Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	192.168.8.1	0.0.0.0	UG	0	0	0	wlan0
link-local	*	255.255.0.0	U	1000	0	0	wlan0
192.168.8.0	*	255.255.255.0	U	9	0	0	wlan0

What do the 192.168.8.1 and the 192.168.8.0 mean? Why is one under Destination and the other under Gateway? If I'm not mistaken, the gateway address is the router IP - it connects me to the internet and is what I would use if I were to access the router control panel.

Sorry if I'm spewing shit - I haven't wrapped my head around this yet, and you seem quite knowledgeable with this.

cyberducky - April 2, 2014, 1:54 pm

(Apr 2, 2014 12:32 PM)?????? Wrote: [\[CITE\]](#) Hi. I'm currently trying to "learn" networking.

I understand what an IP is, but it seems that there is more to it than I understand. There seem to be a few different types. For example, what is the difference between a 192.168.x.x and your normal 74.x.x.x? Is the first reserved for use in LANs? Meh - haven't found a definitive answer that I understand. For example: the result of the 'route' command in Linux.

Code Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	192.168.8.1	0.0.0.0	UG	0	0	0	wlan0
link-local	*	255.255.0.0	U	1000	0	0	wlan0
192.168.8.0	*	255.255.255.0	U	9	0	0	wlan0

What do the 192.168.8.1 and the 192.168.8.0 mean? Why is one under Destination and the other

under Gateway? If I'm not mistaken, the gateway address is the router IP - it connects me to the internet and is what I would use if I were to access the router control panel.

Sorry if I'm spewing shit - I haven't wrapped my head around this yet, and you seem quite knowledgeable with this. If I am not mistaken those are your subnets. Research subnetting to learn more about it.

?????? - April 2, 2014, 1:59 pm

(Apr 2, 2014 01:54 PM)Abide Wrote: [\[CITE\]](#) If I am not mistaken those are your subnets. Research subnetting to learn more about it.

Thanks for the reply, I'll look into subnets.

Goodies - April 2, 2014, 2:18 pm

(Apr 2, 2014 12:32 PM)?????? Wrote: [\[CITE\]](#) Hi. I'm currently trying to "learn" networking.

I understand what an IP is, but it seems that there is more to it than I understand. There seem to be a few different types. For example, what is the difference between a 192.168.x.x and your normal 74.x.x.x? Is the first reserved for use in LANs? Meh - haven't found a definitive answer that I understand. For example: the result of the 'route' command in Linux.

Code Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
default	192.168.8.1	0.0.0.0	UG	0	0	0	wlan0
link-local	*	255.255.0.0	U	1000	0	0	wlan0
192.168.8.0	*	255.255.255.0	U	9	0	0	wlan0

What do the 192.168.8.1 and the 192.168.8.0 mean? Why is one under Destination and the other under Gateway? If I'm not mistaken, the gateway address is the router IP - it connects me to the internet and is what I would use if I were to access the router control panel.

Sorry if I'm spewing shit - I haven't wrapped my head around this yet, and you seem quite knowledgeable with this.

Hello!

I'll explain this fairly simply (even though I'm no longer in Empire, but I was when the original thread was posted).

Where it says "default", that is your default route. Anything that is not in the routing table will be sent out your wlan0 interface to IP 192.168.8.1. This is called your "default gateway". 192.168.8.1 is a host (in this case, most likely a router) to which all data will be sent if the destination IP is NOT inside your subnet.

How does it know if it's in your subnet? That's a good question, thanks for asking.

The 192.168.8.0 and subnet mask of 255.255.255.0. This is where we get into subnetting.

255.255.255.0 in binary goes to:

11111111.11111111.11111111.00000000

in binary. A mask is what dictates the IP range. With the mask, every bit that is a 1 is deemed to be a "network bit". This just means it defines the network and they are constant, even though they are not actually all "1"s in the real IP.

The "0"s are called the "host bits". Each combination represents a host on that network. This is a /24 CIDR (24 1's in the subnet mask). Since IPv4 is a 32 bit address, we know there are 8 0's (or you can just observe that each octet is 8 bits lol).

Each combination of those 8 bits represents a new host. There are 2^8 combinations (256) which means there are 256 possible IPs.

However, the very first combination and the very last combination are reserved for "network address" and "broadcast address" respectively. For example:

192.168.8.X in binary:
11000000.10101000.00001000.XXXXXX

We know those 24 bits are permanent because the subnet mask says that the first 24 bits cannot change. So, making a range, we can see the network and broadcast address.

11000000.10101000.00001000.00000000 = 192.168.8.0

11000000.10101000.00001000.11111111 = 192.168.8.255

Note that .0 and .255 are NOT AUTOMATICALLY NETWORK AND BROADCAST! You can have a normal host as a .0 and a normal host as a .255. However, /24's are very common (especially for home networks) so many people just assume.

?????? - April 2, 2014, 2:24 pm

(Apr 2, 2014 02:18 PM)Goodies Wrote: [\[CITE\]](#) Hello!

I'll explain this fairly simply (even though I'm no longer in Empire, but I was when the original thread was posted).

Where it says "default", that is your default route. Anything that is not in the routing table will be sent out your wlan0 interface to IP 192.168.8.1. This is called your "default gateway". 192.168.8.1 is a host (in this case, most likely a router) to which all data will be sent if the destination IP is NOT inside your subnet.

How does it know if it's in your subnet? That's a good question, thanks for asking.

The 192.168.8.0 and subnet mask of 255.255.255.0. This is where we get into subnetting.

255.255.255.0 in binary goes to:

11111111.11111111.11111111.00000000

in binary. A mask is what dictates the IP range. With the mask, every bit that is a 1 is deemed to be a "network bit". This just means it defines the network and they are constant, even though they are not actually all "1"s in the real IP.

The "0"s are called the "host bits". Each combination represents a host on that network. This is a /24 CIDR (24 1's in the subnet mask). Since IPv4 is a 32 bit address, we know there are 8 0's (or you can just observe that each octet is 8 bits lol).

Each combination of those 8 bits represents a new host. There are 2^8 combinations (256) which means there are 256 possible IPs.

However, the very first combination and the very last combination are reserved for "network address" and "broadcast address" respectively. For example:

192.168.8.X in binary:
11000000.10101000.00001000.XXXXXX

We know those 24 bits are permanent because the subnet mask says that the first 24 bits cannot change. So, making a range, we can see the network and broadcast address.

11000000.10101000.00001000.00000000 = 192.168.8.0

11000000.10101000.00001000.11111111 = 192.168.8.255

Note that .0 and .255 are NOT AUTOMATICALLY NETWORK AND BROADCAST! You can have a normal host as a .0 and a normal host as a .255. However, /24's are very common (especially for home networks) so many people just assume.

And Goodies to the rescue.

THANK YOU! Finally something that I understand. So basically, when I'm sending something to a place that's NOT in my subnet it uses the default gateway to send it, right? It is indeed my router. The subnet is itself defined by the subnet mask, which identifies which octets can change, right?

What if I want to send something to somewhere that IS in my subnet? Would I use the actual IP of the machine?

Thanks a lot!

Goodies - April 2, 2014, 2:31 pm

(Apr 2, 2014 02:24 PM)?????? Wrote: [\[CITE\]](#) And Goodies to the rescue.

THANK YOU! Finally something that I understand. So basically, when I'm sending something to a place that's NOT in my subnet it uses the default gateway to send it, right? It is indeed my router. The subnet is itself defined by the subnet mask, which identifies which octets can change, right?

What if I want to send something to somewhere that IS in my subnet? Would I use the actual IP of the machine?

Thanks a lot!

Actually, yes and no ;) Data is not actually sent to IP addresses but to MAC addresses. Weird, I know, but that's how it works. If you, say, ping 192.168.8.5 (assuming it's an alive host)

First it will calculate the range:

192.168.8.0/24 = 192.168.8.1 - 192.168.8.254

If it is in that range, it will look up the MAC address in the ARP table. ARP (address resolution protocol) is used just to find the MAC address of a known IP address.

It will then send the data to the MAC address, not necessarily the IP address. This is where ARP spoofing comes into play.

For example,. Even though 192.168.8.5 is at 11:22:33:11:22:33, an attacker can update your ARP table by sending ARP responses with a source IP of 192.168.8.5 but a source MAC of 77:77:77:77:77:77 and data will be sent to the destination IP of 192.168.8.5, but to the attacker's machine.

If it sends data to something that is NOT in your subnet, it looks up the MAC of the default gateway either by looking in the ARP table or, if it's not in there, by doing an ARP request. Again, an attacker can spoof ARP responses to become MITM.

Also, it doesn't necessarily need to be an entire octet changing. If we were given an IP of:

192.168.8.0/20 we would have to do a little math.

20 1's:

11111111.11111111.11110000.00000000 = 255.255.240.0

So with an IP of:

192.168.8.0, we match this up with the mask so:

These bits don't change (network bits)

These bits do change (host bits)

11000000.10101000.00001000.00000000 = 192.168.8.0

We can see that the value in the 3rd octet is cut, right? If we do the entire range, it goes from:

11000000.10101000.00000000.00000000 = 192.168.0.0

to

11000000.10101000.00001111.11111111 = 192.168.15.255

So, since you use the network address to identify a network, it would be 192.168.0.0/20, however, 192.168.8.0/20 is just as valid.

In this network, 192.168.8.0 and 192.168.8.255 are just host addresses.

An easy way of doing this (in case you're interested) is by seeing how many host bits are in the first octet with host bits... sorry if that is confusing.

Look at them octet by octet.

255 = 1111 1111

255 = 1111 1111

240 = 1111 0000 <-- everything from the first 0 in the subnet mask is hosts... there will never be a 1 after a 0.

000 = 0000 0000

There are 4 host bits in the 3rd octet. Take those 4 bits, and raise 2 to that number.

$2^4 = 16$. This means that 16 in the 3rd octet will be the next network, and it is.

192.168.0.0/20 +16 in the third octet

192.168.16.0/20 +16 in the third octet

192.168.32.0/20

etc.. etc.. etc...

So now, just by looking at that, you can see that the next subnet has a range of 192.168.16.0 - 192.168.31.255 :)

vulpixbrinley - April 2, 2014, 2:50 pm

I'm looking into ratting someone with Mac. I was wondering if jrat really works bc I've heard that it doesn't. And I was also trying to find out if dc works on macs.

Goodies - April 2, 2014, 3:00 pm

(Apr 2, 2014 02:50 PM)vulpixbrinley Wrote: [\[CITE\]](#) I'm looking into ratting someone with Mac. I was

wondering if jrat really works bc I've heard that it doesn't. And I was also trying to find out if dc works on macs.

Dark comet does not work on Macs because the compilation process, instructions opcode, and dependencies/libraries are very different.

Jrat will work as long as they have Java installed (who doesn't?)

vulpixbrinley - April 2, 2014, 3:07 pm

Ah, that explains so much! Thank you! (:

hav0x - April 2, 2014, 4:07 pm

Hm, I guess this is a good place to start :3. So, I'm currently in the process of learning C# and I was wondering if there was a simple way to port it to Mac? Thanks!

Goodies - April 2, 2014, 5:31 pm

(Apr 2, 2014 04:07 PM)hav0x Wrote: [\[CITE\]](#) Hm, I guess this is a good place to start :3. So, I'm currently in the process of learning C# and I was wondering if there was a simple way to port it to Mac? Thanks!

Well, you can install a pseudo-.net implementation with Mono:

<http://www.go-mono.com/mono-downloads/download.html>

I think that's dumb. I'd say start learning C/C++. Unless this is your first language, Then I recommend something like Python.

C# is a Microsoft proprietary language (though I believe it's becoming an international standard, but that won't change anything). C# is for Microsoft.

?????? - April 2, 2014, 6:58 pm

(Apr 2, 2014 02:31 PM)Goodies Wrote: [\[CITE\]](#) Actually, yes and no ;) Data is not actually sent to IP addresses but to MAC addresses. Weird, I know, but that's how it works. if you, say, ping 192.168.8.5 (assuming it's an alive host)

First it will calculate the range:

$192.168.8.0/24 = 192.168.8.1 - 192.168.8.254$

If it is in that range, it will look up the MAC address in the ARP table. ARP (address resolution protocol) is used just to find the MAC address of a known IP address.

It will then send the data to the MAC address, not necessarily th IP address. This is where ARP spoofing comes into play.

For example,. Even though 192.168.8.5 is at 11:22:33:11:22:33, at attacker can update your ARP table by sending ARP responses with a source IP of 192.168.8.5 but a source MAC of 77:77:77:77:77:77 and data will be sent to the destination IP of 192.168.8.5, but to the attacker's machine.

If it sends data to something that is NOT in your subnet, it looks up the MAC of the default gateway either by looking in the ARP table or, if it's not in there, by doing an ARP request. Again, an attacker can spoof ARP responses to become MITM.

Also, it doesn't necessarily need to be an entire octet changing. If we were given an IP of:

192.168.8.0/20 we would have to do a little math.

20 1's:

11111111.11111111.11110000.00000000 = 255.255.240.0

So with an IP of:

192.168.8.0, we match this up with the mask so:

These bits don't change (network bits)

These bits do change (host bits)

11000000.10101000.00001000.00000000 = 192.168.8.0

We can see that the value in the 3rd octet is cut, right? If we do the entire range, it goes from:

11000000.10101000.00000000.00000000 = 192.168.0.0

to

11000000.10101000.00001111.11111111 = 192.168.15.255

So, since you use the network address to identify a network, it would be 192.168.0.0/20, however, 192.168.8.0/20 is just as valid.

In this network, 192.168.8.0 and 192.168.8.255 are just host addresses.

An easy way of doing this (in case you're interested) is by seeing how many host bits are in the first octet with host bits... sorry if that is confusing.

Look at them octet by octet.

255 = 1111 1111

255 = 1111 1111

240 = 1111 0000 <-- everything from the first 0 in the subnet mask is hosts... there will never be a 1 after a 0.

000 = 0000 0000

There are 4 host bits in the 3rd octet. Take those 4 bits, and raise 2 to that number.

$2^4 = 16$. This means that 16 in the 3rd octet will be the next network, and it is.

192.168.0.0/20 +16 in the third octet

192.168.16.0/20 +16 in the third octet

192.168.32.0/20

etc.. etc.. etc...

So now, just by looking at that, you can see that the next subnet has a range of 192.168.16.0 - 192.168.31.255 :)

Wow. Thank you. Such a nice and detailed explanation. Thanks a lot, this is exactly what I needed.

Im gone brah - April 4, 2014, 3:00 pm

How would you go 'bout launching a microp local stack based buffer overflow? And does it only work on Windows XP sp2?!?!?

Zapu - April 5, 2014, 11:02 am

(Apr 4, 2014 03:00 PM)zayne_temp Wrote: [\[CITE\]](#) How would you go 'bout launching a microp local stack based buffer overflow? And does it only work on Windows XP sp2?!?!?

hey zayne nice to see you m8y ?

Im gone brah - April 5, 2014, 11:16 am

(Apr 5, 2014 11:02 AM)Extrnl Wrote: [\[CITE\]](#) hey zayne nice to see you m8y ?
Sup, login to skype sometime??

Zapu - April 5, 2014, 11:23 am

(Apr 5, 2014 11:16 AM)zayne_temp Wrote: [\[CITE\]](#) Sup, login to skype sometime??
I'll be back on in about a month. ?

geomck - April 5, 2014, 12:50 pm

So I'm fairly new at this and I've been trying to sniff over L2L/ IPSec VPN (old routers only supported protocol) with wireshark. (I have the preshared encryption keys), but I and i can't sniff any packages they send over the network... Both routers are properly connected and configured. (local ips respond to pings from both sides).

Thanks in advance!

GM