

Forum:[Hack Forums](#)

Thread: [TELNET TUTORIAL](#)

harsh - April 18, 2009, 6:53 am

well this is'nt mine but i just forund it so i thought i might share it is for some guy...
any way here it is;

TABLE OF CONTENTS:

Chapter One: Intro

1. Introduction
2. Warnings
3. Copyright Information
4. Disclaimer
5. Who Am I?
6. Shout Outs

Chapter Two: Before We Start

1. What The Hell Is Telnet?
2. What Was The Original Purpose?
3. What Can I Do With It?
4. Is It Illegal?
5. Will I Go To Jail?
6. Is It Fun?

Chapter Three: Getting Started

1. Possible Targets
2. Is The Target Alive?
3. Scanning For Ports
4. Getting An IP
 - 4.A. Messenger
 - 4.B. Social Engineering It
 - 4.C. Your Firewall

Chapter Four: Connecting

1. Connecting To An IP

Chapter Five: What To Do After Your Connected

1. Doing Something!
2. FTP

Chapter Six: Cracking A Pass

1. Brutus
2. Password Lists
3. Default Passwords

Chapter Seven: FAQ's

1. 'I Get A Blank Screen After Connecting!'
2. 'It Says It Can't Connect! WTF!'
3. 'My Computer Flips Off After Connecting!'
4. 'Where Do I Type My Commands?'
5. 'I Got Arrested!!! Can I Sue You?'

Chapter Eight: Wrapping Up

1. Contact Me
2. TGS

~`CHAPTER ONE: INTRODUCTION`~

~`Introduction`~

Hey. I decided that my old telnet tutorial was not sufficient, so I decided to redo it, among all the other work I have to do. This will provide a step by step method to: Connect to an IP, Connect to a certain port, Decide if the port is responsive, Find commands that you can use on this 'Box', Use the commands, Crack a password using 'Brutus', Find Targets, and many other things. It will also include many pictures that you can use as a reference. Remember, all command prompts are different, don't be discouraged.

~`Warnings`~

This is a form of hacking. Whether you do or do not damage a computer, you are committing a felony. Connecting to a computer or something of the kind without permission is punishable by law and will get you corn holed in a state prison by a 365 pound, one eared black man by the name of bubba. You can be held to Criminal, as well as Civil suites for your actions.

Doing this is a good way to get enemies' also. Remember, there are hundreds of hacking groups out there, and hundreds of hackers, there's a chance that you can be fucking with a hacker of a group, and that is not a fun thing to do.

~`Copyright Information`~

This or any portion of this paper is allowed to be duplicated. You may host it on your site, as long as it stays intact. Failure to comply with this will result in swift legal action.

~`Disclaimer`~

I cannot be held responsible for your actions because of this. I will not take responsibility. If you don't agree with this, DO NOT READ FURTHER. I do not condone hacking, as well as any other form of illegal behavior. Also, you will encounter a number of IP's in this forum, DO NOT USE ANY OF THEM. The ones I used for demonstration I did not hurt, and I take no responsibility if you do use them. You have been warned.

NOTE: I used www.sjms.org (the website of a fine military academy) in some of my examples. I mean no harm to come to www.sjms.org. I did not hack www.sjms.org, and I don't recommend you doing it either. I take no responsibility if you do though.

~`Who Am I?`~

I am Errorised of the www.waushare.com forums. If you'd like to get a hold of me, do so at koft@habbocommunity.co.uk

~`Shout Outs`~

Hey I'd like to say hello to my good buddies: Wau / Placi / Maki / Unstable / Phantom / BOOSTER / Chaos Zero / T1M3 / M4K3 / RedFox / Mr.Wolves / h3r3t1c and whoever else I forgot (due to the pot) These are all buddies, as well as PSP-Hacks members.

~`CHAPTER TWO: BEFORE WE START`~

~`What Was The Original Purpose Of Telnet?`~

Telnet was originally made for someone to do all sorts of things. From checking your mail to connecting to your company's server while on a business trip, telnet does it all. The makers of

it had a dream in mind that the average person could deal with command/text based programs. But of course when the masses got into it

and every brother and sister bought a computer,

Windows was made, which totally destroyed most text based programs. Now fucking idiots run computers and company's with computers, and can't even deal with a damn telnet program!

~`What Can I Do With It?`~

Although Telnet has died for the business men, it is still growing quickly with the not-so-trustful person. For the hacker, Telnet is the hammer in the tool box. Telnet is one of the most

world wide programs among hackers, as well as other fun loving people. When you finally hit that golden hack after your first long hours of struggling with telnet (not!), you are god!

You can change other people's passwords, snoop on e-mails, forge dirty e-mails to ones lover,

~`Is It Illegal?`~

Two words: HELL YES. Hacking is the most illegal thing one can do on the internet. Do not be mistaken, it's quite illegal.

~`Will I Go To Jail?`~

Only if you're caught. This is why it's good to encrypt your entire hard drive, if they can't get anywhere in your hard drive, how the hell are they going to charge you with anything? It is very good to be paranoid. My computer is a vault. The military runs 1800 bit encryption tops. The average bit encryption for any given file in my computer is around 7000, Triple Blowfish encrypted. There's also a shredder that hides in the startup registry that I made in a batch file, it hides there and if you don't turn it off within 15 seconds of starting up, bye bye computer and bye bye evidence. It's always good to be paranoid.

~`Is It Fun?`~

Despite my comments about jail, it is quite fun. Most hackers do what they do for the simple thrill of knowing secrets that no ones supposed to know. Having inside information on people

who they barely know or care about. Knowing top secret information that only god and the president are supposed to know, now that's fun!

~`CHAPTER THREE: GETTING STARTED`~

~`Possible Targets`~

A target is a person, place, or thing (kind of like a noun, eh?) in which you are planning on attacking. A target can be anyone! Common targets include: Family, Friends, Government, Phone

Company's, and Former Attackers. Normally the first target is a friend or family member, someone who's not so smart and someone you know for a fact has no security. Security just gets in the way. '7337' hackers learn to deal with security, newbie's fall into the trap. So for now stick with someone easy.

~`Is The Target Alive?`~

Go to command prompt (or Ms-DOS) and type ping 0.0.0.0. (replacing the zeros for the real IP). If it returns, then the computer is connected to the internet. If it says that its lost, then the computer offline (duh!).

~`Scanning For Ports`~

We will be using Blues Port Scanner to scan for ports. You can get blues port scanner at download.com or www.library.2ya.com. It is about 400 KB, not too big.

You scan an IP for ports by pasting (CTRL V) the IP in both boxes in the top. This makes it scan only that ip. You then put the selected range of ports in which you wish to scan.

The more you scan, the more of a chance they will notice your movements, but do as you please.

~`Getting An IP`~

IP is short for Internet Protocol. Each computer has an IP. Getting someones IP can be as easy as asking for it. Here's a few ways:

Messenger:

Ok, so you have MSN messenger. Your a 'bad mofo', a 'rough rider', now its time to get what you need from your victim. The first thing to do is build trust. It would be wise to do this on someone you know will trust you enough to buy into your shit. Here's how you get their IP:

1. Send them a file through MSN (or whatever they have). It can be anything, a game, a dead hamster, a naked picture of yourself, whatever.
2. Once they accept, go into Command Prompt and type "netstat".
3. With a bit of hunting and picking you should be able to find their IP in the box.

Social Engineering:

Social Engineering is a fancy term that people use to describe smooth talkers. Social Engineers are slick, smooth, smart, and know what they're talking about. They get into the part before

attacking, they have great social skills and are easy people to trust. Social Engineers build up a nice level of trust, the more the better, until they get the information they want.

Once, on a SC 'field trip' with a friend of mine, we actually got dressed up to walk to a payphone and make the attack that we've been building trust for months. It was worth it.

But anyway, back to the subject.

Usually, all you need to do is ask the person. If they know better than to give you the IP if you flat out ask them, then they will know better than if you try to scare it out of them. Get em to go to ipchicken.com and give you the numbers in the blue letters.

Your Firewall:

If you have a firewall, then chances are you've seen someone trying to scan you for open ports. If you use Black ICE, all the better. I suggest you download it at www.library.2ya.com.

What Black ICE does is gather up all the attempts to port probe you, connect to your computer, or anything else, and stick it in a database for further use. You can easily pick out targets from the list and use them for your will.

Double click on the person you wish to get the IP with, and on the right it gives you the IP AND the DNS! How nice eh? ~`CHAPTER FOUR: CONNECTING`~

~`Connecting To An IP`~

Ok, so you've got your list of open ports on the computer. For this demonstration I'll be using someone who attempted to hack me a while

back. After scanning a few thousand ports, we come up with this list. Now not all of these allow connections. The ones labeled with a red box next to them are 'dead' ports for the telnet program. This is usually because they only communicate using a certain 'language' that Telnet doesn't support. When you try to connect to these you get a blank screen with dashes where you try to type (see below). The listings labeled with a green next to them allow connections and will talk to you without having to give it a user or pass. The ones labeled with a blue box next to them means that they are responsive, are not dead, but they require authentication before your allowed to connect. If you really need into this computer and they've got password protected ports, there's a section later in the paper that tells you how to get in. So anyway, lets focus on the responsive port. This is unfortunately the SMTP port (Simple Mail Transfer Protocol). Although it does not allow a significant amount of access to this persons computer without knowing advanced things, it does give us a good basis for a demonstration in Telneting. Below will show you step by step on how to connect and other things with this port.

1. Connect to the computer by typing "Telnet 0.0.0.0 25" in Command Prompt/Ms DOS. You should replace the "0.0.0.0" for the IP address you wish to connect to, and the 25 for the specific port you plan on connecting to. For this demonstration, I will be using the IP 161.58.163.4 and the port 25. So the command should read "telnet 161.58.163.4 25". There's no special place to type (as I've received many e-mails questioning this), when you type, it should show up at the bottom.

2. Press enter.

Congratulations! You just made your first connection! Although it's not a quantum leap in the exploration of computer security, it's a start.

~`Doing Something After You Connect

~`CHAPTER FIVE: WHAT TO DO AFTER YOUR CONNECTED`~

~`Doing Something!`~

Alright, so you've got your open connection on an open port. It's best to keep the connection time down to a minimum to reduce them knowing.

I'll now demonstrate on what to do after you're connected.

1. Generically speaking, typing help will give you a list of all the commands supported for that Box. However, some require you to log on before doing so, what a drag!

Alright, after typing help this is how it responded.

You see that there's a nice listing of commands you can use. Since this port is not password protected, you have no worries about restrictions. Typing "help" and then the command in which you want help on will make it elaborate, which is a great feature for a newbie! This is a pic of me asking it to elaborate on a few things.

2. You can never forget to say "hello". It's quite rude to run through someone's home (computer) without even introducing yourself. This young lady was much nicer after I said "hello" to it.

[NOTE: I lost the pics and I'm too fucking lazy to make a hello pic, I'm sure you're smart enough to figure it out]

3. Use the commands in the box to figure out what you want to do. Since every computer and port is different, it is impossible for me to show you every single thing you can do. Learn to get off your bum and ask it what some of the commands mean, it's a good learning tool.

~`FTP`~

You can also connect to port 21 (FTP, or File Transfer Protocol) using telnet. Typing help will give you a listing that you need

~`CHAPTER SIX: CRACKING A PASSWORD`~

~`Brutus`~

Brutus is a great Brute Force password cracker. It is easy to use for the newbie, fast, and reliable. You can find it by doing a search at www.google.com for "Brutus".

~`Password Lists`~

I'm proud to announce that two of our TGS members, The_IRS and Computer Geek, have combined many lists and have come out with a password list with a total of 2.1 passwords. You can download it here: <http://www.aftdesign.com/hacking/passwords.html>

~`Default Passwords`~

You can find many lists of default passwords for any operating systems on the web. Doing a search at google.com for "Default Password Lists" will come in handy. Here is a very good site with many default passwords that you can access in the meantime: <http://www.phenoelit.de/dpl/dpl.html>

~`CHAPTER SEVEN: FAQ`~

1. "I Get A Blank Screen After Connecting!"

The port that your connecting to is 'dead', or unusable. This could be due to a number of different things. For instance, lets say that your trying to connect to someones computer through telnet, on the kazza port (which I beleive is 1214). This port is not designed to take packets (data) from the telnet program, and is specifically designed to give and receive packets (data) from the kazza program. This could be one of your problems. Trying to connect to a backdoor for a Sub7 program will also do the same.

2. "It Says I Can't Connect! WTF!"

This is because the port is either closed, or the computer is firewall protected. As a newbie I wouldn't suggest messing with it.

3. "My Computer Flips Off After Connecting!"

I'll bet money your using Windows. You are aren't ya? I knew it! This is a Windows Dump File. Either update Windows, get Linux, or forget hacking.

4. "Where Can I Type My Commands?"

Type a few letters to see where they commands will show up. Most likely it will be at the bottom of the Command Prompt/MS DOS screen.

5. "I Got Arrested!!! Can I Sue You?"

NO! You read my disclaimer at the top. I don't care who you are, I'm not taking responsibility.

~`CHAPTER EIGHT: WRAPPING UP`~

~`Contact Me`~

You can get a hold of me at koft@habbocommunity, or the www.waushare.com or www.crazy-coderz.net forums, I usually hang around there. Any questions are welcome, however, I will not do illegal things for you, don't ask.

Hope This Helps!

Errorised / Error.

fretan - April 18, 2009, 7:02 am

Thanks mate gona read trough this now =)

harsh - April 18, 2009, 7:16 am

youre welcome

and me too coz i havent read it yet myself

rgayan - April 18, 2009, 7:42 am

thanks for this tutorial

harsh - April 18, 2009, 7:43 am

your welcome

any time...

Zoncko - April 23, 2009, 12:20 am

jo thx help me alot

good job keep going

INFACT - April 25, 2009, 3:39 am

bluescan only gives me the ftp port 21

[IMG]<http://www.pic-upload.de/25.04.09/nwtvo.jpg>[IMG]

And Nmap only gives me useless ports.

Which alternative can i take? and it gives me always port 23 and when i want to connect it doesnt work, even if i know the PC is on the internet

out2getu - May 13, 2009, 9:08 pm

Hey nice paste tut. Helped alot!!

harsh - May 13, 2009, 11:52 pm

your welcome

any time

Crys1sw0w - May 14, 2009, 4:09 am

Wtf m8 i always get "Connect failed" to XX port.

Tried with blue scan and nmap but doesnt give me ports for scan on its ip :S

ty w8 for reply

hoLe[R]a - November 4, 2009, 12:20 pm

Even if I tryed this many times, it doesnt work. I think the problem is somewhere in TelNet becouse every time it gave me " press any key to continue" and after pressing it just exit. :/

But even this good tut. ?

ariffin246 - November 4, 2009, 8:43 pm

very detailed n well explained... thx :D

silver_hawk - January 22, 2010, 5:55 am

can anyone tell me how not to got caught by doing hacking and how did he set encryption key on his harddrive

please mail me @ super_taran2@yahoo.co.in

please mail that answer only

I'll be thankful to you

overklok - January 22, 2010, 6:01 am

Great TUT man, Very informing. Thank you for posting. (Jan 22, 2010 06:55 AM)silver_hawk

Wrote: [\[CITE\]](#) can anyone tell me how not to got caught by doing hacking and how did he set encryption key on his harddrive

please mail me @ super_taran2@yahoo.co.in

please mail that answer only

I'll be thankful to you

Wrong place to post... Read rules and guidelines..

Relentless™ - January 22, 2010, 3:18 pm

sick tutorial but you should include how to enable telnet for vista users - I had to enable my telnet T_T

I would explain how in this post but I can't remember... a quick google search should do the trick for anyone who needs to know though.

ramesharvind - March 7, 2010, 8:42 pm

Nice tut on telnet but in the passwords list i think you meant 2.1 million passwords

BlackJem - March 8, 2010, 1:09 am

lame when you can;t get help and noone explianed wha thte bloody commands mean :P

Ultimate Hacker - May 1, 2010, 4:52 pm

this is probably the best telnet Tut....xD

-mothered- - May 1, 2010, 5:51 pm

Good on you mate. I must say that this Is a well detailed and Informative tutorial. It's certainly captured my Interest, hence I've bookmarked for future reference.

Cheers mate :)

SUNNY BABA! - June 2, 2010, 5:34 am

dude your password link has been fuck off so re post it <<

skrew - June 2, 2010, 8:18 am

nice tut . one thing i want to know how to use that shredder you mentioned in "will i go to jail"

Tinzmahn - June 9, 2010, 9:01 pm

Nice.. no... Awesome tut.. Helped a lot.

FakeOrder - November 24, 2010, 5:46 am

i am arrested , can i sue you ...

what the fuckin lol sentence that i ever heard ...

?

btw nice thread pal

FakeOrder - November 29, 2010, 6:49 am

when i connect to a web via their 25 port ...

then where i put the user login and password ..

please answer me .

mahktm - December 8, 2010, 6:32 am

is internet surfing possible via telnet tunnel

AcidZero - December 8, 2010, 6:40 am

Looks great.Thanks for sharing.

roma4ka - July 28, 2012, 1:23 am

Oh dam so long tutorial for a telnet,

I will not read it all but thanks for the share!