

Forum:[Hack Forums](#)

Thread: [\[TUT\]Introduction to Hacking an Ip Address\[TUT\]](#)

The 7th Sage - November 18, 2009, 6:39 am

Introduction to Hacking an Ip Address

Now i have seen people ask this question over and over and over. So i thought of making a detailed tutorial on this, which might help "some" people.

Intro:

This tut does require certain basics, so i suggest beginners should read about ports and other things

(although i have explained it here it might be intermediate level).

Now basically you cannot just do anything you want with the ip address. You can but you need right things some mind and also luck.

Anyways lets begin shall we.

Getting an Ipaddress:

Ok there are lots of ways of getting an ip address. For example you can use ipget plugin of msnplus and send him a picture or a smiley that he doesn't have. Or you can do this the easy and effective way:

<http://www.reza24.com/ip/>

[img]http://i48.[censored].com/27zkk2g.jpg[/img]

Now this site basically has some scripts installed, and when you register to them they give you a referral link like reza24.com/id=1180 something. All you have to do is give it to your victim and say "Hey can you check if this site is opening? Its not opening for me."

He clicks and you get his ip EMAILED to you, instantly.

Also keep in mind that not all ipaddresses are static. Some isp provide dynamic addresses, so its matter of time the user will turn off his net and the ip will be changed. So try to hack him as soon as you get his ip.

That sums up that part of getting victim's ip. Lets move on to hax0ring.

Port Scanning:

First thing you do is try to ping the ip. So if the victim is online you will get reply else request timed out.

[img]http://i48.[censored].com/1fg5km.jpg[/img]

In my case yep he is online. Lets scan for open ports now.

1) I use Blues port Scanner you can download from:

Download:

Code <http://depositfiles.com/files/i1psjerg3>

The result now:

Interesting ports on ipaddress*:

(The 65522 ports scanned but not shown below are in state: closed)

Port State Service

21/tcp open ftp

25/tcp open smtp

80/tcp open http

111/tcp open sunrpc

135/tcp open loc-srv

443/tcp open https 1027/tcp open IIS

1030/tcp open iad1

2306/tcp open unknown

5631/tcp open pcanywheredata

7937/tcp open unknown

7938/tcp open unknown

36890/tcp open unknown

Take note of all the ports that you see listed before you. Most of them will be paired up with the type of protocol that uses that port (IE. 80-HTTP 25-SMTP Etc Etc...) Simply take all that information and paste it into notepad or the editor of your choice. But there is one problem, we all know its not that easy, we dont even know what type of software or what operating system that this system is running.

2) NMAP - Port Scanner Has unique OS fingerprinting methods so when the program sees a certain series of ports open it uses its best judgement to guess what operating system its

running. Generally correct.

So we have to figure out what type of software this box is running. Many of you have used TELNET for those who haven't TELNET is used to open a remote connection to an IP Address through a Port.

Download:

Code www.nmap.org

Translations:

we are accessing their computer from across the internet, all we need is their IP Address and a port number. With that record you are starting to compile, open a TELNET connection to the IP Address and enter one of the OPEN ports that you found on the target.

So say we typed 'TELNET -o xxx.xxx.xxx.xxx 25' This command will open up a connection through port 25 to the IP xxx.xxx.xxx.xxx. Now you may see some text at the very top of the screen. you may think, well what the hell, how is that little string of text going to help me. Well get that list you are starting to write, and copy the banners into your compilation of the information you've gathered on your target. Banners/Headers are what you get when you TELNET to the open ports. Heres an example of a banner from port 25.

```
220 7thsage.gha.chartermi.net ESMTP Sendmail 8.12.8/8.12.8; Fri, 7 Oct 2005 01:22:29 -0400
```

Now this is a very important part in the enumeration process. You notice it says 'Sendmail 8.12.8/8.12.8' Well what do ya know, we now have discovered a version number. This is where we can start identifying the programs running on the machine. There are some instances in which companies will try and falsify their headers/banners so hackers are unable to find out what programs are truly installed. Some ports may not have banners.

Other points of interest may be the DNS server, that contains lots of information and if you are able to manipulate it than you can pretend to hotmail, and steal a bunch of peoples email. Well now back to the task at hand. Apart from actual company secrets and secret configurations of the network hardware, you got some good info.

<http://www.securityfocus.com> is a very good resource for looking up software

vulnerabilities. If you cant find any vulnerabilities there, search on google. There are

many, many, many other sites that post vulnerabilities that their groups find and their affiliates. www.milw0rm.com is also very popular, but its generally down for me, fools ddosing it.

At SecurityFocus you can search through vendor and whatnot to try and find your peice of software, or you can use the search box. I looked up and i found a paper on how Sendmail 8.12.8 had a buffer overflow. There was proof of concept code where they wrote the shellcode and everything, so if you ran the code with the right syntax, a command prompt would just spawn. You should notice a (#) on the line where your code is being typed. That pound symbol means that the command prompt window thats currently open was opened as root. The highest privilage on a UNIX/Linux Box. You have just successfully hacked a box. So now you have cmd shell infront of you, start doing whatever you want.

HOWEVER its not recommended just leave a text file saying how you did it so they can patch it. For Blackhats such as mine you can just keep it a secret. This will avoid visits from unwanted authorities :P

There are many types of exploits out there, some are Denial of Service exploits, where you shut down a box, or render an application/process unusable. Called denial of service simply because you are denying a service on someones box to everyone trying to access it. Buffer Overflow exploits are involved when a variable inside some code doesnt have any input validation. Each letter you enter in for the string variable will be 1 byte long. Now where the variables are located at when they are in use by a program is called the buffer. Now what do you think overflowing the buffer means. We overflow the buffer so we can get to a totally different memory address. Then people write whats called shellcode in hex. This shellcode is what returns that command prompt when you run the exploit. That wasnt the best description of a buffer overflow, however all you need to remember is that garbage data fills up the data registers so then the buffer overflows and allows for remote execution of almost every command available. There are many, many other types of attacks that cannot all

be described here, like man-in-the-middle attacks where you spoof who you are. Performed correctly, the victim will enter <http://www.bank.com> and his connection will be redirected to your site where you can make a username and password box, make the site look legit. And your poor mark will enter their credentials into your site, when they think its really <http://www.bank.com>. You need to have a small script set up so it will automatiically display like an error or something once they try and log in with their credentials. This makes it seem like the site is down and the victim doenst give it a second thought and will simply try again later.

Summary:

So as a summary of how to OWn a box when you only have an IP Address Method Works On BOTH UNix and Windows. You can do the same with domain names (IE google.com) than what you can with IP Addresses. Run a WHOIS Lookup or something along those lines. Or check up on InterNIC you should be able to resolve the domain name to an IP address.

- Port Scan The Address And Record Open Ports.
- Telnet To Open Ports To Identify Software Running On Ports.

3) NetCat:

Like TELNET only better and with a lot more functionality. Both can be used when you are trying to fingerprint software on open ports.

- Record Banners And Take Note Of The Application Running and The Version Number
- Take A Gander Online At SecurityFocus.com or Eeye.com. If you cant find any

vulnerabilities then search google.

- Make a copy of some Proof-Of-Concept code for the vulnerability.

*Read the documentation if there is any, for the proof-of-concept code you will be using for your exploit

- Run The Exploit Against The Victim.
 - Reap The Cheap-Shot Ownage.
-

WARNING:

This tutorial does not cover up clearing the tracks. If you dare try any of this stuff on a box you dont have consent to hack on, They will simply look at the logs and see your IP Address and then go straight to your ISP. So i suggest you learn how to anonymize yourself, there are lotta tuts here on HF.

Always remember the more info on the system you have the more are your chances to exploit it.

Credits:

Credits also goes to Hitman from whom i found a tut regarding some of the topics mentioned here. I took lot of pro tips from his tut.

That does it for our "Introduction to Ip-Hacking". Thank you and Pls Comment if you liked it. More tuts coming soon ^_^

Have a great 1337 day.

JointMaster - November 18, 2009, 7:25 am
Very nice tutorial, m8 ;)

Even some info I've been looking for :D

Verdande - November 18, 2009, 7:28 am
wow this is really really TLDR

Reaping - November 18, 2009, 7:33 am
Good job, very good to understand.
However I think you disappointed lots of nubs who think it's possible to get passwords over an IP address:P

Anubis - November 18, 2009, 10:03 am
gr8 tut man...bookmarked...thanX i would rep but i cant...:S

The 7th Sage - November 18, 2009, 10:13 pm
(Nov 18, 2009 08:33 AM)Reaping Wrote: [\[CITE\]](#) Good job, very good to understand.
However I think you disappointed lots of nubs who think it's possible to get passwords over an IP address:P
lol, would be great if that was ever possible. It is still possible though, provided they're on your network.

NinjaGeek - November 18, 2009, 10:18 pm

Man I'm trying to give you +REP for about 3 days now and now I can give you one, didn't gave any for today.....

Nice tutorial it helped me.... got into my First PC with telnet....

Thanks

pushl %ebp - November 18, 2009, 11:02 pm

Nice tut dude.

heroin - November 19, 2009, 1:48 am

very good thread, thanks

Moscow - November 20, 2009, 6:09 am

thanx bro...<3 ur tut..

:D :D :D

u rock!!!!

;))

The 7th Sage - November 23, 2009, 9:47 pm

i hear that all the time, but it never gets old xD

ston3dmonk3yxx - November 24, 2009, 12:35 pm

SWEET TUTORIAL ;D IT HELPED ME AND SHOWED ME HOW TO START :D

Loka~ - November 24, 2009, 12:45 pm

Great Tut as always :)

to shoort i think

illus1onz - November 24, 2009, 1:20 pm

I understand everything until the part where you have the run the script and then suddenly have access to them.

pelle - November 24, 2009, 1:25 pm

Great tut. Made my life abit easier. Thanks :))

solaree - November 24, 2009, 5:58 pm

pls am stuck my laptop not openin this site www.reza24.com/ip/ it tells me 'The Domain is temporarily not available.'

pls help

The 7th Sage - November 24, 2009, 9:17 pm

hmm i think they are down oO wait for sometime or try other ip link sites.

ds ds - November 24, 2009, 11:07 pm

mmm.....i tasted this tut and it is delicious. Thank you for sharing, I enjoyed it immensely!

The 7th Sage - November 24, 2009, 11:56 pm

my tuts ain't for eating :P

animexfan09 - December 2, 2009, 11:51 pm

Nice TuT! it was very sexy

bullzye xxx - December 3, 2009, 12:06 am

bookmarked and il read it later
thanks :D

Resident - December 3, 2009, 6:04 am
nice tutorial there m8

h4x0rinsid3 - December 3, 2009, 6:16 am
nice tut cough stickie *cough* so I'm get a few IP addresses and try to ping them but it says
"Request time out" WTF ? They are online and chatting with me they can't be offline...Solution ?

masterfan - December 5, 2009, 3:49 am
good tut...But when i wanna launch nmap it just closes instantly

flAmingw0rm - December 5, 2009, 4:34 am
You should update your tutorial, since reza24's website is closed. Good job though.

sunmaungoo - December 5, 2009, 7:58 am
Very nice tutorial,i love the tutorial and it will help a lot of n00b.

The 7th Sage - December 5, 2009, 8:18 am
(Dec 5, 2009 05:34 AM)flAmingw0rm Wrote: [\[CITE\]](#) You should update your tutorial, since reza24's website is closed. Good job though.
Sorry not a leet :/ Cannot edit it now.

knightskos - December 6, 2009, 12:12 am
A very good TUT. Simple to understand and easy to identify the left out areas.

thx.

hoLe[R]a - December 6, 2009, 12:25 am
Very very nice tutorial The 7th Sage! 5 stars from me. ?

eXeSoul™ - December 6, 2009, 11:44 pm
Good tut mate :) but i need more info after getting port and ip and after connecting telnet.!!

d4t4st34l - December 7, 2009, 12:13 am
Good tut :victoria:

Ill try it later ;)

imAcarrot - December 7, 2009, 12:17 am
great tutorial The 7th Sage! thanks

_3rr0r - December 7, 2009, 10:21 am
if their computer has vista, telnet is turned off by default.. other than that great tut!!

Graff1ti - December 7, 2009, 10:36 am
i learned this through ethical hacking lessons ... but still very good explained and bookmarked for later :) thanks for the share dude .. keep this unique work up

AsS?mbleR - December 7, 2009, 11:41 am
reza24 wont work for me?

Amazing in depth tutorial!

Lol good tut, gonna bookmark this for whenever I see that question ^^

very good tutorial

```

0000000000
10000000
100000
1000[
10[
10
1[
[

```

Wow this is excellent, thank you :)

Good tutorial, however VERY outdated atleast as far as hacking home PC's are concerned. Here's why:

At least 80-90% of people nowadays are behind routers to access the internet. Therefore the external IP of EVERY COMPUTER on the network behind the given router will be the same. So essentially, all you're doing is trying to hack the router, and even having a rooted router is fairly pointless. The most I've EVER been able to do with a rooted router (SSH enabled with custom firmware) was have it packetsniff and upload via ftpd, and even that was a bitch to set up.

Don't get me wrong, this tutorial could POTENTIALLY be useful for for websites and such, but the probability that they're running port-vuln software is fairly low. Correct me if I'm wrong of course.

How do you run the Exploit on the targeted server?

Like I know that he is using some program that is exploited(ex. I found a exploit for the program on milw0rm), so without using telnet I know this and I also know that he has his 27015port open (hosting CS server), can I do something with this? Or do I have to find this information out via telnet(or netcat)?

Nice tutorial; Full details ; noob friendly; good job.

this is a good tut and full up to u man, Today like every connects with a router and hides behind a router ip (that is the way i see it). You would just hack (get accesses) to what ever is on there network like shared files and what not . You want have permission to write files to the computer only read and take files from it. But if they have a printer on there Net work you can print funny things off. That is the best this method got me.

(Jan 12, 2010 10:02 PM)Big.Eye Wrote: [\[CITE\]](#) this is a good tut and full up to u man, Today like every connects with a router and hides behind a router ip (that is the way i see it). You would just

hack (get accesses) to what ever is on there network like shared files and what not . You want have permission to wright files to the computer only read and take files from it. But if they have a printer on there Net work you can print funny things off. That is the best this method got me.

You have no idea what you're talking about and you basically just ripped off my post.

The Sharable Prince - January 13, 2010, 8:21 am

.....this is hard to follow

The 7th Sage - January 16, 2010, 9:45 pm

Locking the thread. Thank you guys for all your support for the past two months.

mechanic33 - July 24, 2010, 9:08 am

A great TuT The 7th Sage Thanks

SIM-135152 - July 24, 2010, 3:08 pm

good work my friend this is great i arrived to the orange text and i'm scarred lol

don't worry i will read it like too soon

thank you

Frivolous - July 24, 2010, 5:57 pm

Nice tutorial dude! +Rep ;').

T.R/Dropper.Gen - July 29, 2010, 5:48 am

Thanks for taking the time to write this tutorial. I've spent a lot of time on it so far. I'm hacked into a wep network and have easy access to the clients router, there's no password settings on it. Through the router I can see a list of all clients on the network, their mac address, ip address etc.

I pinged one of the ip addresses and got 4 sent 4 received packets, so they're online. I then used Zenmap (thanks for sharing this particular program with us, I had never even knew of it's existence till now) to find out what OS the client is running as well as any open ports. I found out that the client is running Microsoft Windows Vista Business SP1, and has 13 open ports.

It's what to do with these 13 open ports which is now my challenge. This is still new to me so I'm at a learning curve here. Here's a list of the open ports Zenmap found :

Port State Service Reason Product Version Extra info

80 tcp open http syn-ack

139 tcp open netbios-ssn syn-ack

445 tcp open netbios-ssn syn-ack

554 tcp open rtsp syn-ack

2869 tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 SSDP/UPnP

5357 tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 SSDP/UPnP

10243 tcp open http syn-ack Microsoft HTTPAPI httpd 2.0 SSDP/UPnP

49152 tcp open msrpc syn-ack Microsoft Windows RPC

49153 tcp open msrpc syn-ack Microsoft Windows RPC

49154 tcp open msrpc syn-ack Microsoft Windows RPC

49155 tcp open msrpc syn-ack Microsoft Windows RPC

49156 tcp open msrpc syn-ack Microsoft Windows RPC

49157 tcp open msrpc syn-ack Microsoft Windows RPC

My goal now is find any exploits in any of these open ports. I'm currently using google to find out exactly what these ports are and if they can be exploited and how. I know that the windows netbios ports of 137-139 are exploitable, and my target has 139 open. Also she has port 445 open which I

know is exploitable. I just don't know how to exploit them !!

I would appreciate it if anyone in the hack forums could pm me (or post here for the benefit of others) any advice on how to go about exploiting these open ports.

i wouldn't have got this far and learned about an ace program like nmap where it not for this tut. so thanks for that :)

MagicMushroom™ - July 29, 2010, 6:13 am

Nice Tutorial...but Telnet is very unsecure!

Schizoid™ - July 29, 2010, 6:15 am

20% of computers in world have telnet opened.. 80% are closed... Man telnet is the thing used for chat now,,, kevin mitnick used this shit :D

I bet u spent lot of time and hard work to write this tutorial.. It might help someone

Cam G - July 29, 2010, 6:20 am

Good tutorial, I won't say anything about telnet but I think people can figure out the one problem it has.

Triple Z - August 1, 2010, 7:05 am

Very good tutorial. Very Descriptive!

Good Job.

azeer - September 9, 2010, 6:57 pm

thats a real good tutorial , many thanks man

Z?us - September 9, 2010, 9:37 pm

Hey this is accentually nice, Thanks for sharing.

jaymejo89 - March 27, 2014, 7:34 am

Good Tut... question about this... IP is very easy to obtain as is scanning ports and determining the versions to identify the OS.

my question is this...

with setting up a connection thru IP - is is possible and if so, how - can you go through to grab google cookies I.E. is there a way to establish the connection via IP and browse cookie or qbin files to obtain further information?

iori_mourad - March 27, 2014, 5:01 pm

Thank you for this TuT, I def learned alot

Endaron - November 28, 2015, 3:07 pm

(Nov 18, 2009 08:33 AM)Reaping Wrote: [\[CITE\]](#) Good job, very good to understand.

However I think you disappointed lots of nubs who think it's possible to get passwords over an IP address:P

Hey

I am pretty new, but shouldnt it be able to make the targets PC run a bruteforce-attack on its own password?

luor - *November 29, 2015, 3:33 am*

Nice tutorial but a little bit confusing, maybe try to change your text format next time

_Asad - *December 1, 2015, 10:38 am*

Nice tut, But ISPs prefer ssh over telnet.