

Forum:[Hack Forums](#)

Thread: [NMAP Tutorial \(WARNING: Heavy on images\)](#)

Austral Hacker - December 10, 2007, 6:32 am

Ok, people, I present to you the NMAP tutorial:

So... let's say that you downloaded NMAP in one of its latest versions, if you didn't then go get it immediately! And come back only when you have it.

When you start/launch/whatever you call it NMAP you should see a screen like this one here:

[img]http://img518.imageshack.us/img518/2295/nmap1fx3.jpg[/img]

You will quickly get used to this Interface, its really user friendly:

(1) IMPORTANT: This is the most important part of the interface, here you will type the IP of the target, or a Web Page Address, for you geeks out there it works both on IPv4 protocol and in IPv6 protocol.

(2) This is the type of scan you want to make, unless you are hacking something really hardcore like government or big company shit then leave it as intensive, no one will notice. This also defines the speed and the aggression it will use until it checks if a port is open or closed or if its using an specific OS

(3) This is where you'll set the commands to run in the process of scanning, leave it be, if you really want to change this use the wizard and create your own scan type so you can use later.

(4) Well, here you'll see displayed all the information you get. Well see that in just a second.

So lets go ahead and enter what we know, i'll be scanning a pretty crappy japanese page that i found 20 minutes ago when i wake up, i dont know what it is about because i dont read japanese, i only know it had its CGI-BIN wide open and without protection so i checked all their stuff... Its still default security, so its not really a challenge :)

[img]http://img502.imageshack.us/img502/1695/nmap2wl5.jpg[/img]

(5) As you see i've entered the URL for that jap site

(6&7) This will remain the same, though you must know that you can change them if you want to

(8) With all set lets go ahead and click on SCAN

(9) You'll see the "Scanning..." text under host

(10) You should see an introductory text like this and some seconds later the scan per se will begin.

Now the scan is running, so just sit back and smoke a cigarette (HEY ITS BAD FOR YOUR HEALTH DON'T DO IT) or listen to some music (BUT NOT TOO LOUD, THATS BAD FOR YOUR HEALTH TOO)

[img]http://img152.imageshack.us/img152/9456/nmap3ow6.jpg[/img]

Luckily for us this site has many ports wide open so you can see perfectly how the scan shows them AT FIRST. (11)

Now, since this could take a while specially if you are running it slowly to pass undetected every couple of minutes you'll see a percentage of the scan completed, just to let you know NMAP is still running. (12)

[img]http://img440.imageshack.us/img440/593/nmap4cd8.jpg[/img]

(13) VOILA! The ports that are open or filtered, their protocol (typically TCP) and their main function and even the version of the software it is running, so you can search for your exploiting pleasure!

(14) And THIS is what i love about NMAP, it tells you the OS of the host! Well see this just now in depth...

[img]http://img527.imageshack.us/img527/8878/nmap5dh1.jpg[/img]

Now, let see, oh yes, the OS! Look at this! its wonderful! The perfect tool for a hacker, to know your enemy! And knowledge is power!

(15) A nice image of the OS, in this case a relative of LINUX

(16) A graphic representing the average difficulty to hack into this, in this case a bomb, in safer systems you can see a Security Box, in the easiest of them a piece of cake (literally!)

(17) A brief report of the scan

(18) The EXACT version of the operative system (if found) an the accuracy (if found)

[img]http://img230.imageshack.us/img230/208/nmap6ke1.jpg[/img]

Now for you exploiter out there, click on the services (19) tab

(20) Look for the port you want to exploit (sendmail here)

(21)VOILA again! All the info on the software running on that port including the version its using (2010 here)

Austral Hacker - December 10, 2007, 6:34 am
Buena suerte en su hackeo ;)

Stamgren - December 10, 2007, 9:33 am
iMucho gracias!

nicoleman - December 10, 2007, 1:46 pm
exactly what i wanted? that is big help for every noob
i finally got it....phew.....

Kuroda_Shun - December 10, 2007, 1:49 pm
Brilliant post. Kudos

sup3r501d13r - December 10, 2007, 2:54 pm

Nice tutorial man! Very informatice! I use ZenNMAP

nicoleman - December 10, 2007, 3:47 pm

i cant do scans for anything...even tried the website you did and it said'failed to open device eth4 QUITTING!'..any ideas?

sup3r501d13r - December 10, 2007, 4:59 pm

Is your NIC on? Is a cable unplugged.

nicoleman - December 10, 2007, 5:30 pm

sup3r501d13r Wrote:Is your NIC on? Is a cable unplugged.think its vistas problem, tried it with xp and it worked~

sup3r501d13r - December 10, 2007, 5:42 pm

That's vista for you, problem after problem. There will be a patch in February that is expected to fix everything.

nicoleman - December 10, 2007, 6:30 pm

ha yea a big dissapointment not even stable. only thing good bout it is the graphics

Austral Hacker - December 10, 2007, 7:00 pm

Nah.. it burns RAM like hell... win XP is better at this moment... Wait until Vista gets SP2 (or maybe even 3)

sup3r501d13r - December 10, 2007, 7:07 pm

It should be a lot better after the update, from what I have heard. I'm getting a laptop in a few weeks. It will have Vista on it (not by my choice). But the salesman said it will get better. Plus the Geek Squad is going to partition my hard drive for me for free so I will have a dual boot with both Windows and Ubuntu. And with it partitioned, both Operating systems can share programs and files.

nicoleman - December 10, 2007, 7:12 pm

well my vista comp has 3 gigs of ram so its not a problem...

and 1 thing... why do my scan results always show 0 hosts up? ive tried a couple of sites already. only worked once for my school web with 1 host...which had a vault icon.

trx07 - April 30, 2008, 2:18 pm

dude its still not working :(

when ever i scan any thing its just says scan failed, i get some open ports, like a lot of them but near the end it goes bang! and its over... :(

V41kYRi3 - April 30, 2008, 5:39 pm

doesn't work on Win ME ?

kode-x - May 2, 2008, 12:57 pm

thanks anyway for the tutorials

Alpha_Hax - December 7, 2008, 8:04 pm

nice tut helped me a lot =D

MorbidSteve - December 7, 2008, 8:20 pm

Thanks for making this

fenixjn - December 7, 2008, 9:21 pm

Nice

BTW, works on WVU x64

dtmn2knw - December 9, 2008, 3:12 pm

this is great!

SytsemFailure - December 9, 2008, 3:28 pm

HELP FIND EXPLOITS PLOX!

blackcat - January 20, 2009, 9:04 am

thx mate nice tut!

Akshat - January 26, 2009, 8:18 am

Zenmap gives the following message : Initiating Ping Scan at 21:48

dnet: Failed to open device eth5

QUITTING!

Can anyone suggest a solution.Thanks

Excellent Posts though

maxamber - January 30, 2009, 5:21 am

really thank you ;)

Jrodd - February 7, 2009, 12:49 pm

I have a problem, i am new to this stuff and all of the scans i have tried to do result in a message saying

dnet: Failed to open device eth5

QUITTING!

how do i solve this and have it do what its supposed to do? please help, thankyou.

batfink - February 7, 2009, 1:08 pm

the CLI is much more beautifull

Haki - February 7, 2009, 1:46 pm

Nice TuT :)

blackcat - February 7, 2009, 3:54 pm

edit: shit, i didnt notice i have thanked you already :S soz@!

Pooky - February 7, 2009, 3:57 pm

Brilliant - especially for me a beginner.

Thank you.

JuStCaLLMeC10Wn - February 7, 2009, 4:22 pm

nice tut man

BigMac - February 7, 2009, 4:55 pm

you guys should learn the command line...

Tosh - February 7, 2009, 5:04 pm

amazing tutorial thanks :D

Pooky - February 8, 2009, 1:57 am

To Austral Hacker

Your second image, nmap2wl5.jpg, is missing

dipshit #1252 - February 8, 2009, 2:27 am

Dude thats zenmap dont use zenmap use nmap!

blackcat - February 8, 2009, 4:39 am

nmap is the command prog, zenmap has an interface... same thing...

hamza6us - February 8, 2009, 5:48 am

good tut i love it

oajhao - February 8, 2009, 9:28 am

very nice tut, when i searched site, i got find open ports, should i search for the service name or port number?

punkpure1994 - February 8, 2009, 10:13 am

great post!

kutmustakurt - February 21, 2009, 1:39 am

? great post dude..

Dark0ne1 - February 21, 2009, 1:50 am

The best, most explained Nmap tutorial around. Great job

n4pst3r - February 21, 2009, 1:55 am

Nice post man!! :D

GreetzZ :D

Akshat - February 21, 2009, 7:36 am

(Feb 7, 2009 01:49 PM)Jrodd Wrote: [CITE](#) I have a problem, i am new to this stuff and all of the scans i have tried to do result in a message saying

dnet: Failed to open device eth5
QUITTING!

how do i solve this and have it do what its supposed to do? please help, thankyou.

Hey Jrodd,I am also new here.I hope you are using Vista and therefore you are facing this problem.Just right click on the Nmap icon<Run as administrator<continue and the problem should be solved .If you are using XP you should probably log in as an administrator.

hk54 - February 21, 2009, 7:40 am

Thanx bro i really wanted to know how to use Zenmap.

Trebor - February 21, 2009, 2:31 pm

HAHA Nmap works fine with vista i have tried it. it must be your pc i have an quad core 4 gig ram

macano - February 28, 2009, 3:04 pm

I use nmap 4.76 and i follow your every single step and it's ok but last step i can't, i mean on that how to send mail i don't got that option on my nmap so the question is how to send mail or exploit ..tanx

ki11s0ap - March 2, 2009, 2:26 am

ook so i have two questions. For any site that I search, when I go to look at what type of OS under the 'host details' tab, they all say "Apple air port extreme" which is the type of router that I use. What am i doing wrong? Secondly what do i do with all this information?

Ben10 - March 2, 2009, 3:03 pm

This is an amazing tool.

Thanks

curtis12999 - March 2, 2009, 3:43 pm

good tut now just what to do with the info, ill figure it out other tut's explain ports

Borden - March 2, 2009, 3:54 pm

thank you for this.Keep up the good work m8!

â™¥_%Heart%_â™¥ - March 2, 2009, 6:33 pm

Sweet tutorial, lots of pics is always nice :D

chestercheng75 - March 2, 2009, 8:08 pm

Very nice format tut.. Very easy to understand for noobs too.

SimplyIgnored - March 2, 2009, 9:47 pm

Very good indeed. I hope this thread is a big success.

crazyboy4902 - March 22, 2009, 10:33 pm

Very nicely done. Thank you for sharing!

NightKid - March 23, 2009, 1:08 am

nice..get in the habit of using the terminal ;) you'll end up doing most of your reg. computing from it.

chomu - March 23, 2009, 4:54 am

what else can i say, your great, thanks for this

mi633t - April 4, 2009, 8:49 pm

that was awesome...exactly what i was looking for

â™¥_%Heart%_â™¥ - April 4, 2009, 11:02 pm

Intense guide, so many pictures :O :O Great reference, good post.

Tazoo0o - April 5, 2009, 3:38 am

You got a pic missing

Scottyboi92 - April 6, 2009, 2:42 am

Hey i found it pretty easy :) but... i don't exactly know what i need it for im a real noob

hack1st - April 7, 2009, 1:30 am

i tried it with kh1me.com it is an arabic forum >>i get this WARNING: Using raw sockets because ppp2 is not an ethernet device. This probably won't work on Windows. can you help me with that??

0m3ga - April 27, 2009, 9:10 pm

Nice Tut, very helpful! + REP for this one!

-0m3ga

L33ko - April 27, 2009, 9:54 pm

Thanks for this tutorial, very helpful and informative. +rep

I have a question about the different graphics for the vulnerability of the server, for example: the bomb, cake, security box, etc.. What is the scale it runs on, and/or what does each graphic mean?

f1ea - April 27, 2009, 11:43 pm

(Apr 27, 2009 09:54 PM)L33ko Wrote: [\[CITE\]](#) Thanks for this tutorial, very helpful and informative. +rep

I have a question about the different graphics for the vulnerability of the server, for example: the bomb, cake, security box, etc.. What is the scale it runs on, and/or what does each graphic mean?

Each host has an icon that provides a very rough "vulnerability" estimate, which is based solely on the number of open ports. The icons and the numbers of open ports they correspond to are

[vault] "2 open ports,
[chest]"3"4 open ports,
[box] "5"6 open ports,
[cake] "7"8 open ports, and
[bomb] "9 or more open ports.

credit: [h++p://nmap.org/book/zenmap-results.html#zenmap-tab-host-details](http://nmap.org/book/zenmap-results.html#zenmap-tab-host-details)

waka_choko - April 28, 2009, 5:48 am

Great Tut. Thank you.

I wish all tutorials are like yours since I'm a visual person.

So now I know the open ports and services.... what is the next tutorial i should learn?the next step? what do you recommend me.

L33ko - April 28, 2009, 10:04 am

Ahh, Thanks for that f1ea. I looked for it, but couldn't find it.

Hazelfox - April 28, 2009, 12:13 pm

Umm, hello im new here. I downloaded nmap and when i tried to scan websites it always gives error: "Failed to open device eth4"

Jettboi93 - April 28, 2009, 2:26 pm

GOt many ips with open ports...

How can I send them my rats....?!?!?!?!?

GNCM - April 28, 2009, 2:46 pm

Hey, nice tut. I have to ask, most every time I run a scan with nmap it gives me the message "dnet: Failed to open device eth5". Can anyone tell me what this means? Cheers.

Hazelfox - April 29, 2009, 10:48 am

To me it gives error eth4 ?

ioannis66 - May 1, 2009, 3:16 pm

It works for me in Vista x64.

camzq - May 1, 2009, 9:02 pm

waaaaaaaaawwwwww... hahahahhaa.. superb..... ill vote for your repu... haha.. very nice..

(Feb 7, 2009 01:49 PM)Jrodd Wrote: [\[CITE\]](#) I have a problem, i am new to this stuff and all of the scans i have tried to do result in a message saying

dnet: Failed to open device eth5
QUITTING!

how do i solve this and have it do what its supposed to do? please help, thankyou.
ethernet cross over,, when your a vista try.. run as an administrator.. i think that helps..

zeroclass - May 18, 2009, 6:47 pm

thanks for the nice and very informative tut. :)

one very noob question? whats next after this? :)

C1tron^ - May 19, 2009, 9:23 am

The weird thing is that you say that this tutorial is to how to use Nmap. But the images are only Zenmap, and when i open Nmap thats not what i get.

So?

sp4 - May 25, 2009, 1:06 am

nmap is not working for me, should i use NEWT Professional ?

eLTeaCHeL - May 28, 2009, 4:42 am

What If the service version says UNKNOWN ????? =\

IceOnFire - May 28, 2009, 11:59 am

I get an error when i scan. It will say,
Quote:dnet: Failed to open device eth20

QUITTING!

Caff - June 5, 2009, 4:45 am

what do i do with it once i'm in?

Decon - June 7, 2009, 3:01 pm

Very Nice tut. Looking forward to soaking up more information. Thanks for knowledge on the ever growing subject.

Glitchezz - June 9, 2009, 2:54 pm

Thanks a lot!

:):)

{TOO SHOORT}

John Craig - June 18, 2009, 8:53 am

RE: NMAP Tutorial (WARNING: Heavy on images)

The tutorial is very helpful. The 2nd graphic <http://img502.imageshack.us/img502/1695/nmap2wl5.jpg> is missing. Does it exist anywhere?

â~ â~ â~ JÑ²Â¢îª,¬Ñ? Ã? \$ Dâ,-â~\$d â~ â~ â~ - June 18, 2009, 10:06 am

Holy Shitttt !!

This is a very good tutorial ..

Thanks for this my friend... ?

Hellflash - June 21, 2009, 10:20 am

nice post man ^^?

DragonX - June 21, 2009, 11:16 am

so if i find an exploit on someones computer what do i do then? how do i exploit it

encrypt - June 21, 2009, 11:33 am

Good basic tutorial for beginners. I thought this sort of stuff is too easy for a tutorial to actually be made about. Not hard is it to figure out how it actually works.

sherekhan - June 24, 2009, 12:05 pm

Thanks for the tutorial, worked like a charm

Daziease - July 2, 2009, 6:14 am

(Dec 10, 2007 04:47 PM)nicoleman Wrote: [\[CITE\]](#) i cant do scans for anything...even tried the website you did and it said'failed to open device eth4 QUITTING!'..any ideas?
You must run as an administrator.

133720 - July 2, 2009, 6:32 am

where can downloaod zemap software
i not understand hacking
i am beinigner need your help

lukman_files - July 2, 2009, 6:45 am

goood tutorial
i like it

Marrow - July 2, 2009, 7:07 am

Just spectacular, love this tutorial

Daziease - July 2, 2009, 7:27 am

(Jul 2, 2009 06:32 AM)minkoko Wrote: [\[CITE\]](#) where can downloaod zemap software
i not understand hacking
i am beinigner need your help
Download it here: <http://nmap.org/download.html>

kngofdahnz - July 7, 2009, 2:07 am

i love it it looks so easy.. omg im going to do this today!

133720 - July 7, 2009, 3:41 am

thank of your help
very thank

MarkW7 - July 7, 2009, 4:39 am

Wow, 2 years old xD - Still reative, nice thread, Thanks!

legendabc123 - July 7, 2009, 5:34 am

great noob friendly
-thanks

wizfull - July 8, 2009, 7:31 pm

very nice! Thanks for this TuT man!

Jolty - July 9, 2009, 5:43 pm

Amazingly good tutorial thank you ?

kngofdahnz - July 10, 2009, 3:34 am

i followed it and i got the open ports but man i can't get threw.. it says Good Luck! yea ima need it!..
not intill they get my new virus!

g0tit - July 10, 2009, 5:21 am

Can I scan game servers with this tool?

? R Y ? ? H ? C K ? ? - July 13, 2009, 7:22 pm

I love your tutorial with picture.... ?
Nice job brother ?

jhonnyblaze - July 24, 2009, 9:04 pm

great tutorial thanks :) i got it :)

bye bye 256 - July 24, 2009, 9:35 pm

nice one is that the new nmap???

anthzer0 - July 25, 2009, 8:20 am

Entertaining and helpful thanks :P

Now, since this could take a while specially if you are running it slowly to pass undetected every couple of minutes you'll see a percentage of the scan completed, just to let you know NMAP is still running. his! its wonderful! The perfect tool for a hacker, to know your enemy! And knowledge is power!

I think i fucked the quoting up but i had a question on this part. How would i slow down the search in order for it to stay undetected? I read a different thread where someone was actually caught port scanning and was sent a email by their ISP acknowledging them that they know what he is doing.. Any and all info here would be greatly welcome!!

SyndicateforGOP - August 10, 2009, 11:07 am

Noob questions,

I got the cannonball.. what does that one mean? easy? also what do I do with the info I just got from the scan?

Thanks,

Syndi

Jokinha - August 12, 2009, 10:21 am

Picture 2 missing.

Now a noob question. How can I hack the web-site through the opne door?

catlover - August 12, 2009, 12:08 pm

Same question here what exactly we can do with the open port. I have been asking this question a lot but no response :(

ProspectDotNet - August 12, 2009, 5:10 pm

every time i try to scan i get:

dnet: Failed to open device eth12
QUITTING!

can anyone help me resolve this?

LeetrN - August 12, 2009, 6:26 pm

I haven't read it but i looks really good

InsaneG0d - August 19, 2009, 4:18 am

(Aug 12, 2009 10:21 AM)Jokinha Wrote: [\[CITE\]](#) Picture 2 missing.

Now a noob question. How can I hack the web-site through the opne door?

Same question here :X

ylexigun - August 19, 2009, 4:28 am

When i try to scan i have this massage ..

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

What i do wrong ?

Any one can help please ?

ylexigun - August 19, 2009, 7:23 am

(Aug 19, 2009 04:28 AM)ylexigun Wrote: [\[CITE\]](#) When i try to scan i have this massage ..

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

What i do wrong ?

Any one can help please ?

Hi I think i know the problem now, i understand Windows Servicepack 2 has removed raw sockets but how can i come around this problem ?

onyourrisk - September 8, 2009, 11:27 pm

Thanks a lot ! I mean you were right Knoladge is power , thanks a again !! Very help full post

bountyhunter0007 - September 14, 2009, 11:07 am

Waht if you only wanted to scan someones emails with this or get their isp adress, would it still work..Bounty

GnomiK - September 23, 2009, 12:36 pm

Great tool!!

love it!

since i'm a beginner, tell me ways to hide/change my IP? ?

I_Learning_I - September 23, 2009, 12:47 pm

(Sep 23, 2009 12:36 PM)GnomiK Wrote: [\[CITE\]](#) Great tool!!

love it!

since i'm a beginner, tell me ways to hide/change my IP? ?

<https://hackforums.net/showthread.php?tid=74534>

Here's a list of possible proxys and explaining why you should chose that proxy, it is also explaining what a proxy is.

Have fun ?

GnomiK - September 23, 2009, 1:27 pm

Thanx man!

"It's never too late to be what you might have been"- G.Eliot

Loka~ - September 23, 2009, 1:29 pm

God tut. Thanks :D

sh00rt...

ashes20 - September 23, 2009, 1:35 pm

your delivery is definiitely funny...I like that!?

rayven18 - September 29, 2009, 11:16 am

shit it doesnt open the images

Jon£zy - September 29, 2009, 11:35 am

like the tut just a shame a few pictures r missing

createch - September 29, 2009, 1:51 pm

helpful and nice basics,thx

immoteck - October 2, 2009, 12:26 am

very nice tut..please updatet the images

Moneybo - October 2, 2009, 6:08 am

verry detailed thank you

? **Slava Rossie** ? - October 2, 2009, 6:29 am

Tutoria - super ..

respect to the autor

aquabats - October 11, 2009, 1:05 am

Can anyone update these images or have the original tutorial?

133720 - *October 11, 2009, 2:03 am*

(Oct 11, 2009 01:05 AM)UnknownUser Wrote: [\[CITE\]](#) Can anyone update these images or have the original tutorial?
me too friend plesae

fraga - *October 19, 2009, 9:27 am*

I have this problem when using Nmap...
nexthost: Failed to determine dst MAC address for target 69.72.193.114

QUITTING!

solomon2 - *November 21, 2009, 4:38 pm*

this tool is just incredible, a nice masterpiece for all-around hackers

bugswillhack - *November 21, 2009, 5:46 pm*

well written tut loved it and clearly organized well done i wan more tuts from you

danExclusive - *November 21, 2009, 6:38 pm*

gracias. aesthetically appealing!

bugswillhack - *November 21, 2009, 7:16 pm*

Also image under step 4 missing but that's no big deal

Needlz - *November 22, 2009, 1:45 am*

Ah great tutorial, NMap is great when doing a targetted attack, use it for banner grabbing all that shit lol

dj0kugel - *November 23, 2009, 5:09 am*

dude good job
but are you going to continue with your tut explaining what to do and how to do it once you have all this info about this server?

..xX[ThunderStorm]Xx.. - *November 23, 2009, 8:48 am*

Nice tutorial man! Very informatice! I use ZenNMAP

illus1onz - *November 23, 2009, 11:37 am*

ty for tutorial using nmap now

Myblackboard - *November 23, 2009, 6:28 pm*

Nice tutorial there bud, cheers

Exceptions - *November 23, 2009, 8:57 pm*

So when you want to exploit that port, in this case, port 21, what options do you have?

?ss??? ???s - *December 21, 2009, 9:33 pm*

a noob thanks you for this. although i dont exactly know what it all means its sure a step in the right direction :]

hellstarter - *January 7, 2010, 11:17 pm*

Ty i have found this very helpful

bLiNk - January 7, 2010, 11:19 pm

Awesome tutorial! Thanks, it helped me alot.

Tetrahedra - January 8, 2010, 1:09 am

Nice tutorial. Great work mate.

lorens13 - January 8, 2010, 2:31 am

Great tutorial,thanks for sharing it on HF^^

CTRL PC - January 20, 2010, 12:22 pm

greattt tutorial! im going to have a lot of fun with this!

Enokay - January 25, 2010, 11:16 am

There is a newer version with more funtions.

it would be great if some one would renew this post?

ChrisMaster - January 31, 2010, 2:17 am

thank you very much for that great tut, but can you (or someone else) upload the second picture again, cause it don't works (for me O:)

Team Angeldust™ - January 31, 2010, 2:34 am

Thanks dude, nice tutorial

hxkd - January 31, 2010, 7:44 am

Muy bien :P

How about you show us how to exploit it?

hxkd

robotronc3 - February 20, 2010, 1:55 am

hey i did the scan, but can some1 tell me what can i do with these ports?

Discovered open port 21/tcp on 91.121.83.32
Discovered open port 995/tcp on 91.121.83.32
Discovered open port 143/tcp on 91.121.83.32
Discovered open port 443/tcp on 91.121.83.32
Discovered open port 53/tcp on 91.121.83.32
Discovered open port 587/tcp on 91.121.83.32
Discovered open port 80/tcp on 91.121.83.32
Discovered open port 110/tcp on 91.121.83.32
Discovered open port 8080/tcp on 91.121.83.32
Discovered open port 993/tcp on 91.121.83.32
Discovered open port 25/tcp on 91.121.83.32
Discovered open port 106/tcp on 91.121.83.32
Discovered open port 465/tcp on 91.121.83.32
Discovered open port 8443/tcp on 91.121.83.32

is any of these useful?

Neo-Dioxide - February 28, 2010, 10:40 am

Excellent I ran though it Step by Step ! The Exploiter part has me a little confused a bit but ill read

over it again

Foyalitus - March 1, 2010, 6:12 pm

very cool

I wonder if tis works with the nmap provided in linux

Hack_for_life - March 2, 2010, 10:00 am

this link to download zenmap... it dont work for me... it says the file has been deleted from mediafire... from where should i download it ?

r0ckstar - March 2, 2010, 9:21 pm

Nice TUT there, thanks :)

bigpapa80 - March 7, 2010, 4:16 am

how do i know wich port to exploit and what do you mean with "(sendmail here)"

Sprew - March 17, 2010, 2:27 pm

gr8 tutorial, now its really easy 2 understand

Sprew - March 20, 2010, 11:46 am

(Mar 7, 2010 05:16 AM)bigpapa80 Wrote: [\[CITE\]](#) how do i know wich port to exploit and what do you mean with "(sendmail here)"

Yeah, what do u mean with "sendmail here"? and what do i need to connect to that ip/port (hacking) ?

Thx! ?

Love Neg Reps - March 20, 2010, 12:24 pm

(Mar 20, 2010 11:46 AM)Sprew Wrote: [\[CITE\]](#) Yeah, what do u mean with "sendmail here"? and what do i need to connect to that ip/port (hacking) ?

Thx! ?

Metasploit

x1y1z1 - March 24, 2010, 5:08 am

nice share brother, this is brief one thanks :)

B0nph1re - March 24, 2010, 8:02 am

I like the GUI, hadn't seen it before. Nice tut, images are good!

hatim - March 25, 2010, 9:35 am

Thanks for sharing.....

This is very supporing but there is a lil problem while scaning victum so how can i discuus that kindly reply for this as soon as u can

funkyhax - March 28, 2010, 9:16 pm

Could someone add me on msn and help me learn to exploit open ports that i've found? - justin6977@live.com

-Hyperion - March 28, 2010, 9:21 pm

nice post man really explains how to use nmap

4rch1t3ct - April 6, 2010, 11:29 pm

nice good tut easily understood

mrkbuddy - April 24, 2010, 12:49 pm

can v try it on our own pc?

blksith0 - April 24, 2010, 4:30 pm

Your missing images, fix that.

Mario - April 24, 2010, 8:43 pm

Great tutorial. Not many people use this anymore thou

Nevison - April 30, 2010, 1:31 pm

What do people tend to use now? also could someone pm me with steps to go about exploiting open ports found please...or any good hacking tut's you know that could teach me, ive read a few but dont really know which ones are effective...theres just so many!.

High Definition - April 30, 2010, 8:37 pm

hmm...Everytime i try to scan something I get this

Code NSE: Loaded 35 scripts for scanning.

Initiating Ping Scan at 09:05

WARNING: Using raw sockets because ppp2 is not an ethernet device. This probably won't work on Windows.

socket troubles in UltraScanInfo::Init: An attempt was made to access a socket in a way forbidden by its access permissions.

Version : Zenmap 5.10BETA1

OS : Win 7

The same thing I get when I do the scanning with metasploit..Anyone have same problem?

Naww - May 1, 2010, 12:49 pm

Thanks man, I been lookin' for this!!?

?

eXeSoul™ - May 2, 2010, 10:03 am

second photo is missing plz reupload the image.!

(Apr 30, 2010 08:37 PM)High Definition Wrote: [\[CITE\]](#) hmm...Everytime i try to scan something I get this

Code NSE: Loaded 35 scripts for scanning.

Initiating Ping Scan at 09:05

WARNING: Using raw sockets because ppp2 is not an ethernet device. This probably won't work on Windows.

socket troubles in UltraScanInfo::Init: An attempt was made to access a socket in a way forbidden by its access permissions.

Version : Zenmap 5.10BETA1

OS : Win 7

The same thing I get when I do the scanning with metasploit..Anyone have same problem?
Same error.!!

sebsebar - May 8, 2010, 9:51 am

nice tut i thinks it is funny and helpful;D

JoK?R - May 8, 2010, 10:05 am

WHY did you BUMP this old ass thread?

!!!! - May 8, 2010, 10:15 am

<http://img502.imageshack.us/img502/1695/nmap2wl5.jpg> doesnt work.reupload it and nice tutorial

D3LuSiOn - May 15, 2010, 10:39 am

Awesome tutorial.

Thanks for helping me out of my noob shell of using the nmap.

DemonFiren - May 26, 2010, 2:23 am

I guess now these Japanese guys have their security updated, heh.

MORPH-182 - May 26, 2010, 2:36 am

Awesome tutorial, thanks heaps for the share!!

mrstupidface - May 31, 2010, 1:57 pm

im new to hacking and all... what is the difference between open ports, filtered, and closed... what can i do with open ports?

thetoad - June 4, 2010, 6:42 am

works great on mine... im using a copied version of windows 7 found on youtube, so cant figure out why all you people are having problems :s

h11mb0b - June 25, 2010, 6:59 am

Thank you so much for this TuT on NMAP.

One question... How can I search for exploits from nmap ??

In other words, what would you do after the scanning is complete and you've found open ports?
Please be detailed.

Thanks again. I've learned a lot from you. Respect, for teaching the beginners.

Montana" - June 25, 2010, 8:09 am

Great tutorial, thanks for sharing.

ShellBreakers - July 1, 2010, 7:47 pm

Second image still isn't showing up. You should re-upload.

Hydro420 - July 11, 2010, 6:23 am

Dude ok so i downloaded the program and everything and i followed your tutorial, but i wanna know how to hack the site. y si me puedes ayudar el site es www.xat.com por fas y gracias

h~o~s~s~a~m - July 21, 2010, 4:42 pm

?

good work thaanks

HACK3R9 - July 23, 2010, 3:35 am

Cheers :)

(grr too short)

andi123 - July 25, 2010, 2:00 am

thank u....i will start from here..i will think first for my next step..

he..he...he....i really want to be a hacker..cause i dont have money to start bussiness....

Mundial - July 25, 2010, 6:20 am

Awesome I'll have to give this a shot sometime. Thanks!

underarmhair - July 28, 2010, 11:26 am

Thanks great tutorial and easy to understand :D

CaptainNegatory - July 28, 2010, 7:42 pm

Vista has so many security issues it's ridiculous.

Hells Hitman - July 28, 2010, 9:57 pm

great tutorial but the bomb means that it has 9+ open ports and the piece of cake means it has 7-8 open ports

gangsta1 - August 2, 2010, 10:36 am

NOBODY has answered the what to do with the open port question - amazing!

MartialLaw - August 28, 2010, 5:14 pm

Thanks for including the screenshots with highlighted and numbered sections, this is a huge help to someone just learning, I'll definitely be saving this tut to my favorites! Thanks again!

Grudgeee - August 28, 2010, 5:15 pm

Dam this was in 2007. Nice tutorial tho.

Toxic Waste - October 4, 2010, 12:58 am

Just what I needed, thanks.

Broken Ampz - November 21, 2010, 1:52 pm

nice tut and funny part about the smokin.

axmetmcl - November 22, 2010, 1:30 pm

lol this was in 2007 and images still alive. i read them again like a noob :D

cosone - November 24, 2010, 8:11 am

Nice tut! but i can't get any IP's to give up the goods, i even tried my own address. im using nmap-5.21. i have also tried .co.blabla sites. if anyone has had the same hiccups and can help that would be cool

QuickTime115 - November 26, 2010, 9:53 pm

Great tutorial. I really like how you use screensnpr, or some other program that you can edit with. You were able to highlight everything, which made it very easy. Thanks

lord fox - November 26, 2010, 11:38 pm

nice tut thanks for share

Dire-wolf - November 29, 2010, 9:12 am

Im using zenmap, wich provided me with the whole info on some website, but what to do next? u know how its hard to dont know where to strart from, some guiding pliz...

Dire-wolf - December 3, 2010, 6:12 pm

Thanks a lot, basics are evrythin :)

godblast - December 6, 2010, 10:48 am

yet again I will ask...what do we do next once we have the ip/know what ports are open? Please help us n00bs!

iGoinify - December 6, 2010, 12:10 pm

Unable to find answer so I'll ask it once more:

What do I do when found many open ports? A little advice, please.

N3oNight - December 7, 2010, 10:30 am

its the best and the most useful tutorial i have ever seen on hf...

Thanks man and keep it up...

Zmind - December 7, 2010, 2:43 pm

Nmap could be cool and all, and i am always tryng to work with it...but all the tests that i made with the ip´s from my victims it says all the time that they are on Linux lol always! even on my ip (xp sp3) why the hell it gets always linux??

wannabe - December 9, 2010, 8:49 pm

looks great.. good for novice like me?tnnt

Asteriqz - December 9, 2010, 8:51 pm

great tutorial, sure it will help alot of noobs :)

mafiax - December 11, 2010, 12:01 am

got da exactly thing i wanted...! ;)

genup1234 - December 12, 2010, 12:49 am

thanks alot, ive just about managed to spoof my mac address (smac is the easy wasy) and hiding your IP via proxy server or 3rd party software is quite straight forward, and learning about port scanning seems the next logical step and this piece is great article, but if i am running out of VMware can certain viruses get through this into my main OS?

BlaVlaWla - December 12, 2010, 11:20 pm

and now what? what do I do with all of those open ports?

ayudD34dh4cK3R - December 17, 2010, 9:17 pm

really nic post man..

but cn u tell me hw to get such vernuable website more easily??

betmenthekill - December 18, 2010, 6:24 am

hmmm what can nmap do??^^

Polard - December 23, 2010, 9:07 am

thank you for this tutorial I'll try it all now but it would be nice to have a tutorial video as a kind and also what can be done with.

sorry for my English because I just translated with google view I do not speak English

The PreDaToR - December 23, 2010, 9:09 am

Nice Work!Great tutorial!

The Unknown - December 23, 2010, 9:10 am

that a great tut , rated 5 on 5 man , keep up the good work

coool_dave111 - December 23, 2010, 10:21 pm

nicee..

i will give it a try ..

Thanks man for sharing

eduard77 - December 30, 2010, 8:41 pm

It doesn't matter what I do I receive the same error

Starting Nmap 5.21 (<http://nmap.org>) at 2010-12-31 04:41 Morocco Standard Time

NSE: Loaded 36 scripts for scanning.

Initiating Ping Scan at 04:41

Scanning home.mahoroba.ne.jp (210.224.104.24) [8 ports]

WARNING: Using raw sockets because ppp3 is not an ethernet device. This probably won't work on Windows.

pcap_open_live(ppp3, 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(ppp3, 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(ppp3, 100, 0, 2) failed three times. Reported error: Error opening adapter: The system cannot find the device specified. (20)

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!

sid8012 - January 8, 2011, 9:42 am

Great thread. Thanks man.

rabbit333 - January 11, 2011, 6:24 am

Great tutorial :D but keep in mind that the noobs dont know the difference on Nmap and Zenmap ;)

Scriptect - January 11, 2011, 9:09 am

At number 19 of the tutorial a image is missing, & without that I couldn't understand the rest of the tutorial, may be just me because I'm a noob at this, but if you could please re-upload that photo or explain to me what to do next. please and thank you :D.

triplewide - January 11, 2011, 9:48 am

I'm getting the same problem with eduard77. Can anyone clear up on this?

easton x - January 11, 2011, 10:22 am

Nice tut..man very noon friendly.

Strudels - January 12, 2011, 4:07 pm

Was very easy to follow, but the second and last images did not show up. A good post none the less.

Sniper26 - January 12, 2011, 4:48 pm

Really easy. Thank you for all of the images!

Polleborre - January 13, 2011, 7:48 am

Does this only wotks with XP ?? cause im be trying alots of sutes even the site u did and it always says "Invalid host expression: <http://home.mahoroba.ne.jp/> -- colons only allowed in IPv6 addresses, and then you need the -6 switch

QUITTING! "

so what to do ??!!

Polleborre - January 16, 2011, 3:56 am

Hi, I have done averything on ur Tutorial NMAP but thing is that i dont know what i can do when its more then see the email sent and other things. So im asking u if i could whit the nmap read the other peoples mail or place keyloggers just to know theirs IP?

tklein42 - January 16, 2011, 5:24 am

Sick tut! Definately gonna give this a go!

Blainee - February 2, 2011, 7:46 am

Nevermind think Im sorted.

nick123456 - February 2, 2011, 5:57 pm

CRASH REPORTED:

SYS.PLATFORM: win32

OS.NAME: nt

Zenmap Version: 5.50

TRACEBACK:

Traceback (most recent call last):

File "zenmapGUI\ScanInterface.pyo", line 228, in filter_toggle_toggled

File "zenmapGUI\ScanInterface.pyo", line 248, in filter_hosts

File "zenmapGUI\ScanInterface.pyo", line 629, in update_ui

File "zenmapGUI\ScanHostsView.pyo", line 277, in mass_update

TypeError: an integer is required

iEnCrYpT - February 2, 2011, 6:29 pm

Great job, very detailed ... Helped me a lot =)

copywasted - February 9, 2011, 8:44 am

this is such a great tutorial!

uuuuuuyyyyyzzzzz - February 9, 2011, 9:56 am

very nice tut..

thank u for sharing :)

Sheldor - February 13, 2011, 10:21 am

Where is [Image: nmap2wl5.jpg]?

kneonKodo - February 15, 2011, 9:02 pm

Thanks man, Its helps for nubs like me :D

BlunkX - February 21, 2011, 6:21 am

Hey i've a stupid question im new to this forum and even didn't hacked anything...
what can i do with that information and open ports?

expl0rer - February 22, 2011, 4:25 pm

Hey i did try to scan this site on your example. My question is; is it safe to portscan these kind of sites? i mean easy sites, friends ips exe? What is the risk in getting caught? Is port scanning a crime anyways? And should we be behind somekind of proxy when we port scan? What can u tell us? Security comes always first right?

Bill776 - March 15, 2011, 11:59 am

hi i am totally knew hence reason im reading this topic, iv tried scanning a forums site and i get this:

colons only allowed in IPv6 addresses, and then you need the -6 switch

QUITTING!

can someone please explain how to make it scan ipv6 to.

panama1 - April 8, 2011, 8:17 pm

After i found out the ports that are open how do i hack it do i have to have a program to go in to the port

whopoopdinmycar - May 26, 2011, 9:21 am

Thanks really helpful. Like the lables

(Apr 8, 2011 08:17 PM)panama1 Wrote: [\[CITE\]](#) After i found out the ports that are open how do i hack it do i have to have a program to go in to the portUse a rat or a key logger

danzo15 - May 26, 2011, 9:28 am

nice very complex though..

ofrepose - May 30, 2011, 6:12 am

Great post, thanks. Nmap is easily one of the best tools

?r1PP|? - May 30, 2011, 6:54 am

Nice tutorial, keep up this work

sseagal - July 13, 2011, 11:25 am

thx for tut

(May 30, 2011 06:12 AM)ofrepose Wrote: [\[CITE\]](#) Great post, thanks. Nmap is easily one of the best tools

man, you just wait... (it will get a lot worse :)

-Revolution- - August 26, 2011, 10:26 am

Brilliant tutorial !

Very well laid out !

Thanks !

benzebuth198 - September 30, 2011, 2:14 am

Thx a lot for those explanations, I think it will be very usefull

PaperBag - December 9, 2011, 9:35 am

Nice post and very useful... Thank you!

bernardbear - December 10, 2011, 1:51 am

omg fuck owesome tutorial...BOOKMARKED NOW !

Mishoo - March 5, 2012, 2:41 pm

(Mar 15, 2011 11:59 AM)Bill776 Wrote: [\[CITE\]](#) hi i am totally knew hence reason im reading this topic, iv tried scanning a forums site and i get this:

colons only allowed in IPv6 addresses, and then you need the -6 switch

QUITTING!

can someone please explain how to make it scan ipv6 to.

i am getting same error...any help with that maybe?? whts wron how to fix it?? google it and didnt found notthing

DsntExist - June 28, 2012, 6:02 pm

Gracias, quick and simple tutorial.

Much props.

lawabidingcitizen666 - June 28, 2012, 7:32 pm

(Jun 28, 2012 06:02 PM)DsntExist Wrote: [\[CITE\]](#) Gracias, quick and simple tutorial.

Much props.

Thats got to be to biggest gravedig ever lol. Props.

d4rk41g0r1thm - August 6, 2012, 11:37 am

i think this is the best tut about nmap / zenmap thank you brother <3

power4gear - September 22, 2012, 12:08 pm

My victim is behind a firewall. All the ports are filtered, no other information. What are my options?
Thanks.

itsupport.dr - September 23, 2012, 2:36 am

very nice tutorial keep up the good work

NeverDown - June 16, 2019, 7:23 am

this looks interesting

I hope they work as you say

abc1231230zz - June 20, 2019, 2:08 pm

thats not really working now