

Forum:[Hack Forums](#)

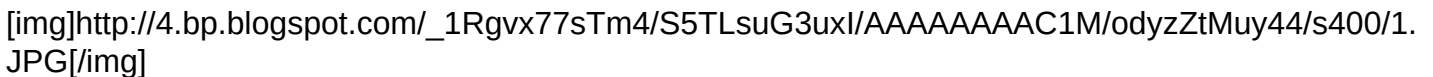
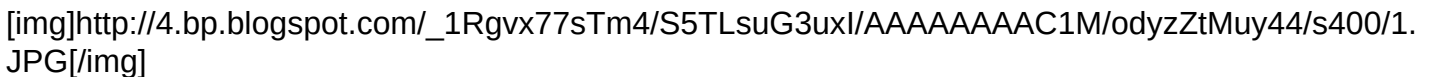
Thread: [\[TUT\]How to Spoofing IP Addresses: Learn how to create custom IP packets Using tool Rafale](#)[\[TUT\]](#)

Tooth Fairy - April 9, 2010, 6:54 am

How to Spoofing IP Addresses: Learn how to create custom IP packets Using tool RafaleX and Engage Packet Builder

The RafaleX application allows for the creation of custom IP packets. The packet is very customizable and allows for the spoofing of the IP, setting the flags, number of packets, and so forth. RafaleX is becoming hard to locate on the Internet as it appears it is now called Engage Packet Builder.

The RafaleX application is an excellent way to "spoof" custom packets. Attackers can place a valid IP address as the source of the packet and the target will have to attempt to respond to the spoofed address. By sending hundreds of thousands of packets in this manner, an attacker can create a Denial of Service attack against a target.

http://4.bp.blogspot.com/_1Rgvx77sTm4/S5TLsuG3uxI/AAAAAAAAAC1M/odyzZtMuy44/s400/1.JPG

In this example, the Source IP of the packets to be sent is set to 10.10.10.10 with the source address of port 123. According to Internet etiquette, this should never be able to route on the Internet as the 10.x.x.x range is reserved for Private addressing. Set the destination IP to the target address. In this example it is 172.16.1.40. Set the Destination port to port 21. The SYN and ACK flags were set for each packet.

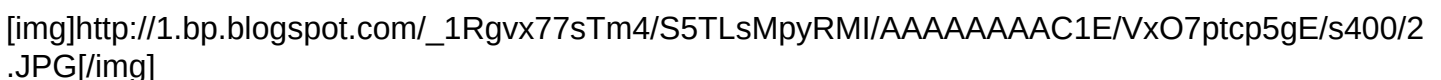
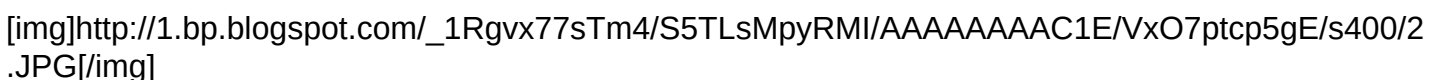
*Note: The Ethernet communications process requires a three-way handshake:

SYN: Synchronize

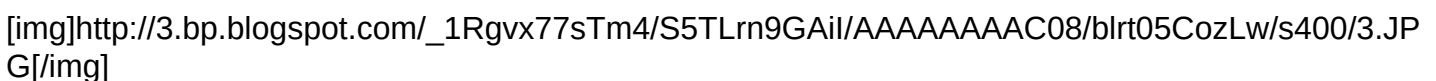
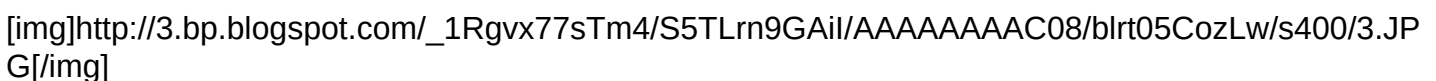
SYN-ACK: Synchronize-Acknowledge

ACK: Acknowledge

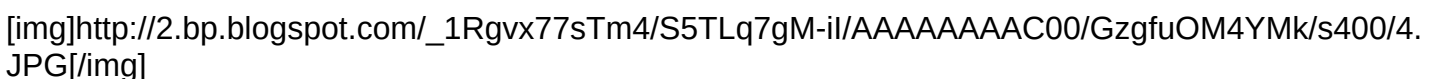
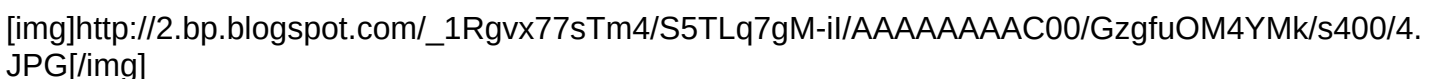
When a computer receives an uninitiated SYN-ACK packet its response is to send a RST (Reset) packet.

http://1.bp.blogspot.com/_1Rgvx77sTm4/S5TLsMpyRMI/AAAAAAAAAC1E/VxO7ptcp5gE/s400/2.JPG

The number of packets was set to 100. Click the Send button to send the packets to the target. The Status area at the bottom left of the application will tell you that the packets were sent.

http://3.bp.blogspot.com/_1Rgvx77sTm4/S5TLrn9GAil/AAAAAAAAAC08/blrt05CozLw/s400/3.JPG

The proof is below screen shot captured from packet capturing tool:

http://2.bp.blogspot.com/_1Rgvx77sTm4/S5TLq7gM-il/AAAAAAAAAC00/GzgfuOM4YMk/s400/4.JPG

[img]http://1.bp.blogspot.com/_1Rgvx77sTm4/S5TLqvQ414I/AAAAAAAAAC0s/PCg_2eVdprU/s400/5.JPG[/img]

Please reply ,to make it even better ? ?

Jack. - April 9, 2010, 7:00 am

Very intresting guide thanks!

Tooth Fairy - April 9, 2010, 7:02 am

Loved to help you :)

catlover - April 9, 2010, 12:13 pm

seems good. is it better than proxies??

Tooth Fairy - April 10, 2010, 4:54 am

Yes it is better than proxies :)

MindAway - April 10, 2010, 9:20 am

I have a question please

now suppose you have a ip address which is 12.34.56.78

and I have another ip address which is xx.xx.xx.xx

by this tut

can i make xx.xx.xx.xx=12.34.56.78 ?!

if not, please correct me :)

Leg4cy - April 10, 2010, 9:54 am

Cool Tut imma try this much thanks

vrysleepy - April 10, 2010, 9:59 am

noob question, but what exactly does this do? give a false ipaddress to sites,games,connections, etc?

Tooth Fairy - April 10, 2010, 10:55 am

Yes you are right .

D0ggyD0gg - April 10, 2010, 3:51 pm

This looks good ill try it out.

-mothered- - April 10, 2010, 6:16 pm

Great work with your tut there mate. Very well Introduced, documented, Illustrated and elaborated. I've bookmarked this and shall analytically delve Into It, within the next few days (time Is not on my side at the moment!).

Appreciate the effort you put Into this :)

DexHacker - April 10, 2010, 8:57 pm

Thanks for the tut, but one big problem your spoofing your IP, but the problem is the handshake will send the response to the spoof IP, so you will not get them and you need to return the rand number

+1.

But there is a use for such programs, for example i got banned from OS Dev forum, so i decided to ban the mods, first i got all the mods IPs, this was simple just sent them to a fake site, that i said was a OS Dev fake site i found, this just saved there ip's to a text file (simple php).

Once i had all the mods IP's, i test there forum and found that if you port scan the forum, it would block your IP.

Now it was a simple case of spoofing my IP with the mods IP's as if they were port scanning them and the mods IP'S where block, i did this in a loop, from a old 486 pc.

Tooth Fairy - April 10, 2010, 10:13 pm

(Apr 10, 2010 06:16 PM)mothered Wrote: [\[CITE\]](#) Great work with your tut there mate. Very well Introduced, documented, Illustrated and elaborated. I've bookmarked this and shall analytically delve Into It, within the next few days (time Is not on my side at the moment!).

Appreciate the effort you put Into this :)

Thanks man.

Hope you like it ?

-mothered- - April 10, 2010, 10:18 pm

(Apr 10, 2010 10:13 PM)???????x ?™ Wrote: [\[CITE\]](#) Thanks man.

Hope you like it ?

You're welcome mate. Looking forward to giving It a crack soon.

Cheers :)

R16H713 - April 11, 2010, 1:29 pm

This is epic! In theory, you can employ an amplification attack by flooding a company, that has large bandwidth, and spoofing the source as the person who's computer you want to take down. I can't wait to try this out. Thanks for the share!

(Link: <http://www.engagesecurity.com/downloads/#engagepacketbuilder>)

proisr - April 11, 2010, 1:52 pm

Thanks bro, but what about a DL for the prog'?

sh0bhit - April 11, 2010, 2:08 pm

thanks bro very useful :P

Charity - April 11, 2010, 3:39 pm

(Apr 11, 2010 01:29 PM)R16H713 Wrote: [\[CITE\]](#) This is epic! In theory, you can employ an amplification attack by flooding a company, that has large bandwidth, and spoofing the source as the person who's computer you want to take down. I can't wait to try this out. Thanks for the share!

(Link: <http://www.engagesecurity.com/downloads/#engagepacketbuilder>)

It's called a reflected DDoS. You send spoofed packets to a bunch of systems with the victim's IP and they all respond to that IP = no more whatever.

R16H713 - April 11, 2010, 3:44 pm

Oh, ok. Let's not get too technical. (It's pretty much the same thing ;)

MindAway - April 11, 2010, 4:55 pm

I have a question please

now suppose you have a ip address which is 12.34.56.78

and I have another ip address which is xx.xx.xx.xx

by this tut

can i make xx.xx.xx.xx=12.34.56.78 ?!

if not, please correct me :)

R16H713 - April 11, 2010, 5:33 pm

You cannot make your ip address (I assume) actually turn into that address, but you sure can fool other servers into thinking that it is!

3 olaH - April 11, 2010, 7:10 pm

seems really cool, but would this work for things other than computers...per say an xbox console? and if so that would be amazing. nice tutorial.?

collinetnick - April 11, 2010, 7:29 pm

(Apr 9, 2010 06:54 AM)???????x ?™ Wrote: [CITE](#) How to Spoofing IP Addresses: Learn how to create custom IP packets Using tool RafaleX and Engage Packet Builder

The RafaleX application allows for the creation of custom IP packets. The packet is very customizable and allows for the spoofing of the IP, setting the flags, number of packets, and so forth. RafaleX is becoming hard to locate on the Internet as it appears it is now called Engage Packet Builder.

The RafaleX application is an excellent way to "spoof" custom packets. Attackers can place a valid IP address as the source of the packet and the target will have to attempt to respond to the spoofed address. By sending hundreds of thousands of packets in this manner, an attacker can create a Denial of Service attack against a target.

[img]http://4.bp.blogspot.com/_1Rgvx77sTm4/S5TLsuG3uxI/AAAAAAAAAC1M/odyzZtMuy44/s400/1.JPG[/img]

Seems good im just to lazy to do it right now

In this example, the Source IP of the packets to be sent is set to 10.10.10.10 with the source address of port 123. According to Internet etiquette, this should never be able to route on the Internet as the 10.x.x.x range is reserved for Private addressing. Set the destination IP to the target address. In this example it is 172.16.1.40. Set the Destination port to port 21. The SYN and ACK flags were set for each packet.

*Note: The Ethernet communications process requires a three-way handshake:

SYN: Synchronize

SYN-ACK: Synchronize-Acknowledge

ACK: Acknowledge

When a computer receives an uninitiated SYN-ACK packet its response is to send a RST (Reset) packet.

[img]http://1.bp.blogspot.com/_1Rgvx77sTm4/S5TLsMpyRMI/AAAAAAAAAC1E/VxO7ptcp5gE/s400/2.JPG[/img]

The number of packets was set to 100. Click the Send button to send the packets to the target. The Status area at the bottom left of the application will tell you that the packets were sent.

[img]http://3.bp.blogspot.com/_1Rgvx77sTm4/S5TLrn9GAil/AAAAAAAAAC08/blrt05CozLw/s400/3.JPG[/img]

The proof is below screen shot captured from packet capturing tool:

[img]http://2.bp.blogspot.com/_1Rgvx77sTm4/S5TLq7gM-il/AAAAAAAAAC00/GzgfuOM4YMk/s400/4.JPG[/img]

[img]http://1.bp.blogspot.com/_1Rgvx77sTm4/S5TLqvQ414I/AAAAAAAAAC0s/PCg_2eVdprU/s400/5.JPG[/img]

Please reply ,to make it even better ? ?

DexHacker - April 11, 2010, 7:42 pm

You need to remember YOU CAN NOT get any return packets back, if you spoof.

Also remember your router writes YOUR IP into the packet header, so i would not try this BEHIND a ROUTER.

gatherer - April 11, 2010, 8:38 pm

Would there be a way to craft the packets so that they'll act as HTTP form POST Requests, or AJAX requests?

Tooth Fairy - April 12, 2010, 4:18 am

Thanks for all your comments.

Tooth Fairy - April 12, 2010, 6:19 am

I am delighted to help.

MindAway - April 12, 2010, 5:10 pm

I have a question please

now suppose you have a ip address which is 12.34.56.78

and I have another ip address which is xx.xx.xx.xx

by this tut

can i make xx.xx.xx.xx=12.34.56.78 ?!

if not, please correct me :)

COOL_zERO - April 14, 2010, 6:25 pm

very useful tutorial! tnx mate!...

Tooth Fairy - April 15, 2010, 4:18 am

I am delighted to help :)

DreamXx - April 29, 2010, 8:43 pm

this doesn't work... yes wireshark picks up the spoofed IP
but any website you visit while sending your spoofed IP will still see your real IP address

like google mail etc...

Ironsides - April 30, 2010, 1:17 am

Where can I download it?

?Yang? - April 30, 2010, 2:35 am

Where do i download this?

mastrmind - April 30, 2010, 3:27 am

very nice tut

pic's always help ? (Apr 30, 2010 02:35 AM)::Yang:: Wrote: [\[CITE\]](#) Where do i download this?
here you go

<http://www.engagesecurity.com/downloads/#eaglex>

Ironsides - April 30, 2010, 4:06 am

Thank you :D

/too short

ZGEGEG123 - April 30, 2010, 11:08 am

Any chance you can get this to work with Windows 7?

N!tzi.00x0 - April 30, 2010, 3:02 pm

Where the fuck you can download that app?

shneikid - April 30, 2010, 6:44 pm

(Apr 30, 2010 11:08 AM)ZGEGEG123 Wrote: [\[CITE\]](#) Any chance you can get this to work with Windows 7?

MEE TOOO im also using Windows 7 [ANY ADVICE] I DONT KNOW... try maybe ? (Apr 30, 2010 03:02 PM)N!tzi.00x0 Wrote: [\[CITE\]](#) Where the fuck you can download that app?
Ups... Ups... [WHERE IS THE ANSWER?]

:S

?

DreamXx - May 3, 2010, 9:57 am

does this actually 100% work for anyone?

like have you spammed a fake Ip and logged onto the internet and visited a website
to see if your fake ip is being recorded or not?

and also this doesn't work for windows 7??

random87 - May 3, 2010, 11:06 am

Nice tutorial, but you could mention the creators of it, infact not u wrote this:

<http://learnethicalhacking.wordpress.com/2010/03/08/how-to-spoofing-ip-addresses-learn-how-to-create-custom-ip-packets-using-tool-rafalex-and-engage-packet-builder/>

I just used google dork for the tool that the tutorial told me, didn't searched exactly for this tut...really no offense... inurl:RafaleX download and the only result is that tutorial that I posted the link above.

You can find teh downloadlink there guys, but I didnt tested if its infected or not, please scan it before you run. ?

If you are too lazy to click on link above I uploaded to a mirror...:

<http://www.mediafire.com/?yjmmzywg53l>

- herm1t

DreamXx - May 7, 2010, 9:57 am

this doesn't work lol idk what people are talking about

Tooth Fairy - May 7, 2010, 10:22 am

It do works man .

DreamXx - May 14, 2010, 9:16 am

(May 7, 2010 10:22 AM)BloO_v™ Wrote: [\[CITE\]](#) It do works man .
then post a screenshot or video on a website like www.ip-adress.com

with the ip 1.2.3.4 :/

0x45 - May 24, 2010, 4:25 pm

Anything on linux?

{short}

davd-secure - May 24, 2010, 6:48 pm

(May 14, 2010 09:16 AM)dizzy Wrote: [\[CITE\]](#) then post a screenshot or video on a website like www.ip-adress.com

with the ip 1.2.3.4 :/

This can not work because www.ip-adresss.com server will try to send this screen to 1.2.3.4 !

Like it has been sayed before his is only for sendig packets.

(like disconnect someone from a server and so ?)

Bakedman - May 27, 2010, 8:54 am

so can you use this for xbox live? so you cant get ddosed

tipleddown - May 27, 2010, 9:44 am

thanks very nice guide.....

Tooth Fairy - May 28, 2010, 6:23 am

Thanks for the feedback .