

Re: Anonymizing Packets yet ensuring 0 % packet loss

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2007-09/msg00090.html>

- *From:* "Vivek P" <iamherevivek@xxxxxxxx>
 - *Date:* Fri, 14 Sep 2007 02:11:39 +0530
-

hi

it was quick & impressive

we had worked on socks proxy! there are some merits & demerits

the network on which we are testing (80 % target simulation) has some filters which blocked it..

Are you aware of some technology though which i can employ dns poisoning to route it to a virtual location !! where i have control !!

I am interested to do something at packet level cos setting up a proxy also can be traced at the ISP level!!

Any suggestion to go about it would be appreciated!

thanx

On 9/14/07, Utmost Bastard <utmostbastard@xxxxxxxx> wrote:

Other than delivering a payload with a forged packet you will have to proxy through something.

If you are reverse tunneling a shell it will need to relay through a proxy of sorts also if you truly need the originating IP concealed.

Basically anything other than a one way connection is going to need a valid address to relay the data back and forth from.

The first and only truly reliable thing I can think of is a good fast socks proxy.

----- Original Message -----

From: "Vivek P" <iamherevivek@xxxxxxxx>

To: "Utmost Bastard" <utmostbastard@xxxxxxxx>

Cc: <security-basics@xxxxxxxxxxxxxxxxxxxx>; "Pen-Testing" <pen-test@xxxxxxxxxxxxxxxxxxxx>

Sent: Thursday, September 13, 2007 4:15 PM

Re: Anonymizing Packets yet ensuring 0 % packet loss

Subject: Re: Anonymizing Packets yet ensuring 0 % packet loss

hi
thanks for the quick reply

my goal is to hide my ip adress, the n/w packets will be pentest related & general stuff!

there is no torrent, but FTP, HTTP & regular communications will take place from the setup!

I am looking for a solution with which i can permanently show a different IP adress! (not actual)

i did try creating packets, the problem is that the reply doesnt come back to me!!

I was successful to broadcast a packet outside & it came back too.. but it was traceable (i used a carrier)... :-(

i would appretiate some one discussins techncalities. I am okay with coding a program fr the same!

On 9/14/07, Utmost Bastard <utmostbastard@xxxxxxxxxx> wrote:

PeerGuardian just uses preset "block lists" of IP addresses to function.

If
an IP address is met any protocol/port transferring or receiving data is blocked at the network layer.

I do not think that is the goal you are trying to achieve.

If this is for traffic such as torrent your IP will still be known from the tracker itself but you will not be sending or receiving data from any of the IP addresses you have in your list.

<http://www.bluetack.co.uk/forums/index.php> ironically has a torrent to download the latest blocklist set.

Hopefully this clears any questions up.

Re: Anonymizing Packets yet ensuring 0 % packet loss

UB

----- Original Message -----

From: "Vivek P" <iamherevivek@xxxxxxxx>

To: <security-basics@xxxxxxxxxxxxxxxx>;

"Pen-Testing"

<pen-test@xxxxxxxxxxxxxxxx>

Sent: Thursday, September 13, 2007 1:52 PM

Subject: Anonymizing Packets yet ensuring 0 % packet loss

hi all

I am on a lookout for IP hiding & anonymity
for a project of mine!

I was googlin for some time now! most
amusing one that i came across
was that of Peer Guardian..

I wanted to get directions frm hw best can i
get my identity hidden!
atleast without using a proxy server from
some providers (like
anonymiser)...

the link for Peer Guardian is here:

<http://phoenixlabs.org/pg2/>

I m pretty sure someone would have tried it..

I am testing it as i am writing this query...

thanks in advance

Vivek P Nair
VP Tech
Appin Group Of Companies
Appin Security Group
Module III TBIU
IIT DELHI
Hauz Khaus
New delhi
India
www.appinlabs.com
vivek.p@xxxxxxxxxxxxxxxx

We explore... and you call us criminals.
We seek after knowledge... and you call us
criminals.

Re: Anonymizing Packets yet ensuring 0 % packet loss

We exist without skin color, without
nationality, without religious
bias... and you call us criminals.
You build atomic bombs, you wage wars,
you murder, cheat, and lie to
us and try to make us believe it's for our own
good, yet we're the
criminals.

Yes, I am a criminal. My crime is that of
curiosity.
My crime is that of judging people by what
they say and think, not
what they look like.
I am a hacker, and this is my manifesto.
You may stop this individual, but you can't
stop us all!

This list is sponsored by: Cenzic

Need to secure your web apps NOW?
Cenzic finds more, "real" vulnerabilities fast.
Click to try it, buy it or download a solution
FREE today!

<http://www.cenzic.com/downloads>

Vivek P Nair
Vice President Technology
Appin Group Of Companies
Appin Security Group
Module III TBIU
IIT DELHI
Hauz Khaus
New delhi
India
www.appinlabs.com
vivek.p@xxxxxxxxxxxxxx
+919910924675

We explore... and you call us criminals.

Re: Anonymizing Packets yet ensuring 0 % packet loss

We seek after knowledge... and you call us criminals.
We exist without skin color, without nationality, without religious bias... and you call us criminals.
You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity.
My crime is that of judging people by what they say and think, not what they look like.
I am a hacker, and this is my manifesto.
You may stop this individual, but you can't stop us all!

--

Vivek P Nair
Vice President Technology
Appin Group Of Companies
Appin Security Group
Module III TBIU
IIT DELHI
Hauz Khaus
New delhi
India
www.appinlabs.com
vivek.p@xxxxxxxxxxxxxxxx
+919910924675

We explore... and you call us criminals.
We seek after knowledge... and you call us criminals.
We exist without skin color, without nationality, without religious bias... and you call us criminals.
You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity.
My crime is that of judging people by what they say and think, not what they look like.
I am a hacker, and this is my manifesto.
You may stop this individual, but you can't stop us all!

This list is sponsored by: Cenzic

Need to secure your web apps NOW?

Re: Anonymizing Packets yet ensuring 0 % packet loss

Re: Anonymizing Packets yet ensuring 0 % packet loss

Cenzic finds more, "real" vulnerabilities fast.

Click to try it, buy it or download a solution FREE today!

<http://www.cenzic.com/downloads>
