

RE: bypassing employer's proxy to surf anonymously

RE: bypassing employer's proxy to surf anonymously

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-06/msg00235.html>

- *From:* "Levenglick, Jeff" <JLevenglick@xxxxxxxxxxx>
 - *Date:* Tue, 13 Jun 2006 13:46:56 -0400
-

Gimeshell,

Your question is a little confusing ...

1) Is there any other way for you to send your data or must you go through a proxy? (ie: firewall blocking all traffic except The proxy box)

If you can send your data, then just avoid the proxy. If not, then the only thing you could do is try to spoof the ip/mac of the Proxy and send your data. (unless you know what your doing then this is not an option for you :))

2) What is nasty traffic? Are you not allowed ssh? Ssh is encrypted, so they can't view your data.

3) hide data? (Karyn) There really is no such thing. Yes, you can change ports, but that would just set off more Alerts. On top of that, he is going to another box so he must use the port that the host is listening on.

You can mess around with the payload, but ssh is an encrypted prot, so your going to end up with more problems then it

Is worth. If you think about it: If he is on a company network and I'm an admin who wants to find out who is

Sending the traffic, I can track you down to your port. (ie: you change your ip or mac address to hide yourself)

Bottom line.. Surf at home.

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

From: Karyn Pichnarczyk [<mailto:karyn@xxxxxxxxxxxxxxxx>]

Sent: Tuesday, June 13, 2006 12:49 PM

To: gimeshell@xxxxxx

Cc: pen-test@xxxxxxxxxxxxxxxxxxx

Subject: Re: bypassing employer's proxy to surf anonymously

Gimeshell,

RE: bypassing employer's proxy to surf anonymously

RE: bypassing employer's proxy to surf anonymously

If a network is being used to transfer traffic, and something is physically monitoring all traffic (regardless of source/destination port, regardless of protocol, etc) then there's no way to prevent them from monitoring your traffic over that network. You're talking about bypassing something in a lower network layer (physical) with something in a higher network layer (i.e. Data or Network). It's not going to happen.

Now hiding data in unsuspecting packets....depends on your definition of "unsuspecting" and the level of detail of the network admins are who are monitoring the traffic. If the net admins are using a network forensics analysis product you have to get fairly creative to hide your data.

karyn

gimeshell@xxxxxx wrote:

Question:

Is there a solution to prevent proxy traffic monitor (and therewith big brother) to see SSH traffic to dynamic ip? So that there isn't any

suspicious line in proxy traffic monitor's output? The best: Proxy doesn't get notice of nasty traffic at all.

Perhaps there is some technique to hide data in unsuspecting packets?

regards,
gimeshell

--

Karyn Pichnarczyk
Sandstorm Enterprises, Inc.

Be advised that all electronic communication with Sandstorm Enterprises(R) is subject to monitoring by NetIntercept(R), our full-content network forensics analysis tool. More information about NetIntercept can be found at www.sandstorm.net. Please direct any questions to privacy@xxxxxxxxxxxxxxxx

RE: bypassing employer's proxy to surf anonymously

RE: bypassing employer's proxy to surf anonymously

This List Sponsored by: Cenzic

Concerned about Web Application Security?

Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you:

http://www.cenzic.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.

This e-mail message is private and may contain confidential or privileged information.

This List Sponsored by: Cenzic

Concerned about Web Application Security?

Why not go with the #1 solution – Cenzic, the only one to win the Analyst's Choice Award from eWeek. As attacks through web applications continue to rise, you need to proactively protect your applications from hackers. Cenzic has the most comprehensive solutions to meet your application security penetration testing and vulnerability management needs. You have an option to go with a managed service (Cenzic ClickToSecure) or an enterprise software (Cenzic Hailstorm). Download FREE whitepaper on how a managed service can help you: http://www.cenzic.com/news_events/wpappsec.php

And, now for a limited time we can do a FREE audit for you to confirm your results from other product. Contact us at request@xxxxxxxxxx for details.
