

Re: firewall question

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-02/0060.html>

From: Michael Starr (mstarr@ampeisch.com)

Date: 02/14/02

From: "Michael Starr" <mstarr@ampeisch.com>
To: "leon" <leon@inyc.com>, pen-test@securityfocus.com
Date: Thu, 14 Feb 2002 15:05:43 -0500

Leon;

The technique you are talking about has been called "reverse telnet", "reverse www exploit", or "shell shoveling". Unfortunately, it is extremely difficult to defend against. However, it does require that the attacker has the ability to launch the attack from inside your network. The answer in this case, is not in the firewall rules sets. You'd be better off spending your time guarding against trojan software, and "fairly" benign tools like NetCat (which many virus scanners won't pick up), and making sure that your internal users aren't conspiring against you. =8->

M.

On 13 Feb 2002 at 20:44, leon wrote:

> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
> Hi,
>
> I posted this to the security basics list but nobody answered the
> question. I thought maybe the people on this list would know the
> answer since they are the ones who have to get around firewalls.
>
>
> I have a question regarding stateful inspection firewalls
> (specifically pix and checkpoint).
>
> It seems to me that a lot of people use either nat or pat and that
> these types of firewalls by default drop unsolicited connection
> attempts (meaning packets that arrive with the syn bit set). Any
> packet that leaves the network is put in the state table so that the
> return packets can come back in. My question is this; if I were to
> exploit a client-side buffer overflow and I got the system to make a
> connection to me via netcat with a destination port of 80, would I
> circumvent a majority of the stateful inspection firewalls? It seems
> that these firewalls trust that ALL connections originating from the
> inside are good. Now I know we could block off destination ports of

SecurityFocus Penetration: Re: firewall question

- > services we don't want to allow access to (say no port 23 traffic
- > leaves the network because we don't allow telnet) but I am wondering
- > if either of these firewalls have a method of filtering based on
- > protocol (for example allow 80 to be a destination port but only http
- > traffic can cross it. No netcat, no aim, no limewire just http.
- >
- > I have seen a ton of networks where I came in and I found people
- > using things like aim even though the firewall specifically only
- > permitted port 80 traffic out (obviously these people switched the
- > port from 5190 to 80).
- >
- > So to reiterate; is there a way to configure pix or checkpoint to
- > judge the connection based on protocol as opposed to arbitrary things
- > like source ip, destination IP or port numbers?
- >
- > Cheers and thanks in advance,
- >
- > Leon
- >
- > PS: Links are appreciated if possible.
- >
- >
- > -----BEGIN PGP SIGNATURE-----
- > Version: PGPfreeware 6.5.8 for non-commercial use <<http://www.pgp.com>>
- >
- > iQA/AwUBPGsWcNqAgf0xoaEuEQIxyQCgkNOVREzUZDZxaD6bvvxhi5J5MeMAnjmH
- > 87LbvB+D88XdIzKulw6uR4n
- > =6Pir
- > -----END PGP SIGNATURE-----
- >
- >
- >

> ----- This list is provided by the SecurityFocus Security
> Intelligence Alert (SIA) Service. For more information on
> SecurityFocus' SIA service which automatically alerts you to the
> latest security vulnerabilities please see:
> <https://alerts.securityfocus.com/>

"Even if a samurai's head were to be suddenly cut off, he should still be able to perform one more action with certainty, If one becomes like a revengeful ghost and shows great determination, though his head is cut off, he should not die." -- Hagakure

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- *Previous message:* [Rzac`](#): "Re: firewall question"
- *In reply to:* [leon](#): "firewall question"
- *Next in thread:* [John Adams](#): "Re: firewall question"
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)