

## Re: Ports getting hammered?

---

*Source:* <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2006-01/msg00153.html>

---

- *From:* "Duane Arnold" <No@xxxxxx>
  - *Date:* Fri, 06 Jan 2006 02:32:05 GMT
- 

"Somebody." <somebody.@xxxxxxxxxxxxxxxxxxxxxx> wrote in message  
[news:oIjvf.8537\\$43.4005@xxxxxxxxxxxxxxxxxxxx!nnrp1.uunet.ca...](mailto:news:oIjvf.8537$43.4005@xxxxxxxxxxxxxxxxxxxx!nnrp1.uunet.ca...)

>

> "Duane Arnold" <No@xxxxxx> wrote in message

> [news:u1Wuf.5849\\$nu6.3112@xx](mailto:news:u1Wuf.5849$nu6.3112@xx)

>>

>> "Somebody." <somebody.@xxxxxxxxxxxxxxxxxxxxxx> wrote in message

>> [news:hYSuf.8388\\$43.1353@xxxxxxxxxxxxxxxxxxxx!nnrp1.uunet.ca...](mailto:news:hYSuf.8388$43.1353@xxxxxxxxxxxxxxxxxxxx!nnrp1.uunet.ca...)

>>>

>>> "Duane Arnold" <No@xxxxxx> wrote in message

>>> [news:YfSuf.3070\\$H16.311@xx](mailto:news:YfSuf.3070$H16.311@xx)

>>>>

>>>>>

>>>>> 1. it's not on the list of allowed outbound ports/protocols

>>>>> 2. it's on the list of blocked outbound ports/protocols

>>>>> 3. it's not on the list of allowed destinations

>>>>> 4. it's on the list of blocked destinations

>>>>> 5. it contains traffic that can be identified as problematic based on

>>>>> signature (deep inspection)

>>>>> 6. the behaviour of the traffic can be identified as nefarious

>>>>> (metrics, thresholds, or profiling)

>>>>> 7. combinations of the above methods

>>>>>

>>>>> Not to be smart here but my Watchguard is not just going to start

>>>>> blocking outbound from some machine that it has determined that

>>>>> outbound traffic is dubious in some nature – automatically. Maybe some

>>>>> of the higher end models can do it but I don't have one of those. The

>>>>> only PFW solution that I know about that will stop outbound on its own

>>>>> based on some kind of traffic analysis of protocols being broken is

>>>>> Blackice in conjunction with using IPsec running on the machine. That

>>>>> traffic that was being blocked outbound just happened to be the query

>>>>> by the XP O/S to the MS site for time sync that the XP O/S was having

>>>>> trouble at the time, which I told BI to accept the traffic and forget

>>>>> about it.

>>>>>

>>>>> I am aware of ZA and have used it. And I know that ZA is not stopping

>>>>> outbound on its own unless some rules are being set to stop it. It's

>>>>> not just going to start blocking outbound on its own and many of them

## Re: Ports getting hammered?

>>>> cannot do it.

>>>>

>>>> Duane :)

>>>>

>>> Well to be honest I'm not fully up on most software firewalls as I don't  
>>> believe in them as a genre. I run one sometimes to support clients that  
>>> in fact does inspect traffic for nefarious content and can utilize most  
>>> of the techniques I noticed including recognizing signatures of outbound  
>>> traffic. It's the FortiClient which is the FortiGate's IPSec client.  
>>> That's what my comments were based on.

>>>>

>>> If your Watchguard can't stop outbound traffic... is it really useful?

>>> Would not the Windows XP firewall do exactly the same work?

>>>>

>> My WG can stop inbound or outbound by setting rules by port, protocol and  
>> IP WAN or LAN IP(s). What it can't do is start doing some kind of  
>> protocol analysis to see if protocols are being broken only a IDS  
>> application in system can do that. Now if the FW solution host based or  
>> otherwise has an IDS element to it, then more power to it.

>>>>

> My PFW has an IPS built in, supporting around 1300 attacks. So, it can  
> recognize and stop nefarious traffic that is going over allowed ports,  
> protocols and IPs.

>>>>

>>> As far as the appliance-based approach, the FortiGate firewall line in  
>>> fact uses all the methods I mentioned and more to stop outbound traffic,  
>>> no matter who solicits or initiates it, and it can't be compromised by  
>>> the malware itself. Which is what makes that approach superior to a  
>>> software based firewall approach.

>>>>

>> I am not going to be depending upon any solution appliance, host based  
>> or otherwise to be making some kind of decision as to when it's going to  
>> stop inbound or outbound based on some algorithm it maybe using on its  
>> own that has been predetermined by some programmer. BTW I am a programmer  
>> that's what I do for a living is write programs. If I set rules for a FW  
>> host based, appliance or otherwise to do something to filter packets  
>> inbound or outbound, then it had better well do it.

>>>>

>> I am the one who is the determining factor by reviewing logs for traffic  
>> patterns, what's dubious or not dubious in nature and where traffic is  
>> being sent to or coming from.

>>>>

>> The buck stops with me and not some program in the determination as to  
>> what is happening.. I may use tools to help me make that determination.  
>> But the buck stops with me and no where else.

>>>>

>>>> Duane :)

>>>>

> On the appliance, the entire set of attacks can be fully customized, one  
> by one. They can be enabled or disabled, they can be set to drop the bad  
> packets, kill the session, or send a reset to one or both ends. Smart

Re: Ports getting hammered?

## Re: Ports getting hammered?

- > people review their logs and the default configurations to decide what
- > they want to let through and what they don't. Some data types are
- > exempted from scanning, some are not. Some are subjected to deeper or
- > different scans than others.

Look, I am a home user with some professional expertise. I know how to protect my setup. And I'll dare say that I would know what to do protect a small business too and do it well.

- >
- > You are taking the position that you don't want to see or know about these
- > things, because your tools cannot inspect the data going over the
- > permitted ports and protocols. All your programming skill in the world
- > will not save you from in-band attacks when zero-day exploits hit the wire
- > for products you use.

For the moment, my machine is setting behind BlackIce and IPsec on the machine while on the road. And while at home, the machines are setting behind that WG. I have learned a lot from the Top Guns in the NG and in a couple other NG(s) on how to protect my setup along with other things I have learned on my own, like going to the O/S where I should go and configure the O/S and solutions such as IIS for better protection. I got it covered and I know how to look.

- > Until the vendors release patches, you're open. In the other direction,
- > nefarious software installed by nefarious means or rouge users on your
- > machines are free to communicate out over common ports such as 80 without
- > impediment, in plain view of your logs.

A rouge user is never going to get on my machines. I know how to go look for such things, if it ever does happen and I do look from time to time with the proper tools, I'll take care of it. The FW appliance knows the difference between FTP coming down port 80 as opposed to HTTP coming down port 80 so it is protocol aware. And so is BlackIce along with IPsec that's implemented on this laptop I am using.

- >
- > I trust people that do this for a living to help me with such things while
- > the software vendors tell us that the vulnerability is theoretical only.
- > I gain visibility into the data streams and types going through my
- > firewalls, be they common ports or not.

I learned long ago not to trust anything or anyone and Human Beings are fallible to say the least about it.

- >
- > I temper that with a dose of reality and the ability to read the logs and
- > modify the configuration as need be, based on what really is and is not
- > allowed over the wire by the firewall rules and the data types traversing
- > them.
- >

Re: Ports getting hammered?

Re: Ports getting hammered?

OK, if that's what you do that's what you do.

I know what I am doing and I can take care of myself — count on it. :)

Duane :)

---

• **References:**

- ◆ **Ports getting hammered?**  
◇ From: SHRED
  - ◆ **Re: Ports getting hammered?**  
◇ From: Duane Arnold
  - ◆ **Re: Ports getting hammered?**  
◇ From: SHRED
  - ◆ **Re: Ports getting hammered?**  
◇ From: Duane Arnold
  - ◆ **Re: Ports getting hammered?**  
◇ From: SHRED
  - ◆ **Re: Ports getting hammered?**  
◇ From: Somebody.
  - ◆ **Re: Ports getting hammered?**  
◇ From: Duane Arnold
  - ◆ **Re: Ports getting hammered?**  
◇ From: Somebody.
  - ◆ **Re: Ports getting hammered?**  
◇ From: Duane Arnold
  - ◆ **Re: Ports getting hammered?**  
◇ From: Somebody.
  - ◆ **Re: Ports getting hammered?**  
◇ From: Duane Arnold
  - ◆ **Re: Ports getting hammered?**  
◇ From: Somebody.
- Prev by Date: **Re: Ports getting hammered?**
  - Next by Date: **Re: Is there a firewall that can block a particular connection?**
  - Previous by thread: **Re: Ports getting hammered?**
  - Next by thread: **Re: Ports getting hammered?**
  - Index(es):
    - ◆ **Date**
    - ◆ **Thread**