

Re: [fw-wiz] httpport 3snf

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2002-10/0957.html>

From: Robert E. Martin (rmartin@fishburne.org)

Date: 10/22/02

From: "Robert E. Martin" <rmartin@fishburne.org>

To: "R. DuFresne" <dufresne@sysinfo.com>

Date: Tue Oct 22 10:13:19 2002

R. DuFresne wrote:

>On Mon, 21 Oct 2002, Ryan M. Ferris wrote:

>

>

>

>>Paul:

>>

>>Great Comments! But is this really realistic?:

>>

>>

>>

>>>If tunneling is (a) against policy, and (b) requires active and considered
>>>engineering to achieve, then the technology has done its part. After
>>>that, it's a monitoring and enforcement issue, not a firewall issue. If
>>>you can show active anti-policy malice in achieving the connection- then
>>>it's time to move into the penalty phase.

>>>

>>>

>>[Bigger question coming...]

>>

>>At what point does monitoring and enforcement become unrealistic? In
>>Robert's case, he could be the network administrator of thousands of
>>individually configured Windows laptops running some kind of tunneling. It
>>could end up as pervasive as napster. Isn't the penalty phase really just
>>reserved for very criminal cases?! I have worked at some pretty big places.
>>My experience was always that you would have to do something really bad to
>>reach "penalty phase" - a hand slap usually at most. If you had ten users
>>doing something against policy, you didn't get ten "penalty phases", you got
>>a meeting with your boss to help provide alternate functionality so there
>>were no desktops users "against policy".

>>

>>For example, if AIM and ICQ were bad, I can imagine a mandate to provide
>>secure messaging or else the masses might riot. It is true the security
>>groups had more power to slap hands than us network/desktop administrators
>>types - but we usually took more "user heat" for reduced functionality.

>>

>>

>

>

>Don't limit your thinking and discussion of "against policy" to merely AIM
>and the various IM toys. There was a recent thread on a few other related
>lists, vuln-dev being one, about the DCMA(BAD TM), but there to deal
>with>, and the P2P toys that allow trading in copywrited material. Some
>of those P2P networks are actively monitored to an extent, and violators
>as well as their hosting sites <ISP's and even universities> are sent
>nasty grams from the copywrite holders warning them of committing offenses
>and fiscal liability. The AUP here is the universities friend here, as
>well as the network admins best buddy in dealing with these infrations
>that might well dig into campus pockets for negligence. Additionally,
>75+% of the DDOS attacks we've looked into have been launched via
>compromised uni systems, oftem sitting in the student dorm residences and
>lounges, but, still on the university backbone. Paul's mention of
>specialised firewalls/IDS' to enforce policies, contain, and monitor these
>subnetworks is great advice. You need this to keep the students out of
>areas of the campus networkk they should not be playing in anyways, a
>seperation of zones of authority if you will, afterall there has been
>alot of mention of students altering thier academic status in various
>institutions of learning, so some seperation is madatory anyways, just
>take it a step further and deem the renets as internal DMZ's. I'd
>additionally advise that the AUP be backed up by a minimal use policy,
>requiring proper anti-virus and perhaps personal firewall software as an
>additional et of protections. Of course, your other wories are going to
>be in the wireless realm these days and folks providing access freely to
>those not intended for the campus networks.

>

>SECURITY WIRE DIGEST, VOL. 4, NO. 76, OCTOBER 10, 2002

>*UNIVERSITY BANS WINDOWS NT/2000

>Citing security reasons, the University of California at Santa Barbara
>(UCSB) has banned the use of Microsoft Windows NT/2000 on its residential
>network, ResNet. In a posting on the ResNet site, UCSB officials blame the
>OSes for "hundreds of major problems on UCSB's residential network during
>the 2001-2 academic year," including exploited vulnerabilities,
>denial-of-service attacks, port scanning, and infections by Code Red and
>Nimda. UCSB recommends that ResNet users switch to Windows XP Home.
><http://www.resnet.ucsb.edu/information/win2k.html>

>

>

>Thanks,

>

>Ron DuFresne

>

>

Boy, I didn't think I'd be opening a can of worms here. I gotta hand it to you all, there is a lot going on here that I have thought of without the fancy degree and years of Unix experience. AUP here is strong but maybe this will put things into perspective:

Firewall-Wizards: Re: [fw-wiz] httpport 3snf

This is a military School for 8-12 graders.. The key here is discipline. Most of the kids here are on some sort of chemical to keep them on the ground. (doggie downers) As you all are aware of, some of the "users" come in with enough knowledge to be dangerous so I get a lot of"so how does the network work"types of pre-adolescent questions. And then there is always one guy who thinks he is above all this and has GOT to hack the network. That is what we have here. Here are a couple of snippets I found applicable during this thread:

----No, administrative penalties are an appropriate thing. That may be as small as "temporarily losing legitimate access" or a letter of reprimand for the first offense. Subsequent offenses should of course escalate in punishment. *Heck, if we don't teach the kids that in school, they're sure gonna find out about it in the real world.*

This is the main reason I have got to solve this somehow. If I send the message to these types of kids that they CAN get away with hacking a network, You all in bigger business have guys like me to thank for the problems that arise in the future. Our network for the cadets is on it's own subnet from the admin so security is good. Making changes to the infrastructure of the network is in the works and all of the content of this and other discussions dealing with network security and AUP will play a major role in the redesign. Thanks to everyone for your input.

----Fo*r example, if AIM and ICQ were bad, I can imagine a mandate to provide*
secure messaging or else the masses might riot. It is true the security groups had more power to slap hands than us network/desktop administrators types - but we usually took more "user heat" for reduced functionality.

The masses might riot. Hummmmm. I can imagine that a riot over AIM or it's equal could most likely escalate to a grating whine but not a riot. This was the whole reason this came up to begin with. I stopped all chat programs here due to abuse. The cadets would use this to communicate plans to_ really _riot within the school, talking more to their girlfriends and friends and lewd content when they did use the application. So I stopped it. The whining was unbelievable. Then the hacking started. Now the chat programs are working again. Crap!!! Coming into the school the AUP is clear.....Chat programs are forbidden. Now I am at the "dealing with the parents" stage. Billy can't do his homework because he doesn't have his computer in his room anymore.....Well, you should tell him the AIM is not allowed.....The parent I believe was the one who gave him this application to begin with. Let's not get into the modems in the rooms....

----When I was the evil firewall BOFH in a large stupid company, your friends wouldn't have gotten SSH out of my firewall.

Ok. I believe you. Did you also have web based e-mail accounts and if you did, how was authentication taking place without 443 open?. There are plans to change the e-mail accounts here to something more web based. There are a slew of mail applications out there that look and feel a lot like hotmail and yahoo mail. Outlook has a great web based

Firewall-Wizards: Re: [fw-wiz] httpport 3snf

app that costs more and really does a nice job. Who invented AOL anyway and why are the masses so caught up in it??? I think it's the Pied Piper syndrome. That will be the next issue with the parents. "Why can't billy use his AOL mail?????" I am interested in hearing about the kind of firewall you used and how it was set up.

I really appreciate all the discussion as I am a 3 year newbie to the industry. I have learned a lot and there still is a lot to learn. Again, this discussion started by asking you all how I can stop traffic generated by software that tunnels out the firewall. The message is clear, NOT MUCH. I have sniffed packets, blocked ports, stopped services and almost made a mess out of the ipchains rules in our firewall. There is no smoke yet, but there is fire to re-think the network security implementation here. This is great stuff. Keep going.

Robert E Martin
IT Manager
Fishburne Military School
rmartin@fishburne.org
540.946.77