

Re: Probes on Port 135 and 445 continue

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2004-10/0319.html>

From: Leythos (void_at_nowhere.org)

Date: 10/17/04

Date: Sun, 17 Oct 2004 15:27:19 GMT

In article <slrncn3p10.njk.ibuprofin@atlantis.phx.az.us>, ibuprofin@painkiller.example.tld says...

> In article <MPG.1bda6c0588d983b98986e@news-server.columbus.rr.com>,

> Leythos wrote:

> >In article <slrncn0vjt.k70.ibuprofin@atlantis.phx.az.us>,

> >ibuprofin@painkiller.example.tld says...

>

> >> *I'm curious how someone managed to educate them into such an*

> >> *enlightened position*

>

> >*The Sorority has an AUP that I designed and passed through our legal*

> >*department, it's the same type of AUP that we use for commercial /*

> >*corporate accounts when they don't have one of their own.*

>

> *OK "imposed"...*

Yea, they had nothing before, free, unrestricted use of the service without any consequences – at least until the ISP threatened to cut off their service for spam abuse.

> >*Since there is no benefit to the Sorority to allowing external users to*

> >*access services inside the house, such as P2P systems, there is no*

> >*reason to permit it. The house has a slow DSL connection, in order to*

> >*provide quality access to the largest number of users, all forms of*

> >*"servers" are prohibited.*

>

> *This is more what I was asking about – what caused them to buy into it.*

> *A slow connection is a very good reason.*

Slow and security were the main reasons.

> >*Since the network is monitored 24/7, it could be construed that the house*

> >*would know of P2P activity and could be sued by the RIAA should one of*

> >*the ladies start offering pirated material to the public.*

>

> *Monitored with their permission? Otherwise there are invasion of privacy*

> *issues. The RIAA has no right to monitor the connections, and could*

> *themselves be sued in the event that they did. A good landshark could*

> *make money out of that kind of stupidity.*

Actually, with P2P you can see where the source is from, so it would be easy to determine that a person offering pirated material is at a specific IP and then follow that to the ISP, etc... About 5 of the systems had P2P apps installed, every file they had in the sharing folders was pirated, we removed the P2P app, but left the material – it was not our mission to remove files, only apps, viruses, trojans, worms that violated the AUP.

> >*The blocking of the ports, 135 through 139, 445, 1433, 1434 and 2500 was presented to the board, checked by a senior Bank IT manager against their firewall design (since a bank member is on their board), and approved without concern.*

>
> *I see no reason to have most ports below about 1030 open – that might also reduce Messenger spam. Depending, they may need 113 inbound, but I've not seen that one exploited yet. We normally forward related port 113 requests to a server running fakeidentd anyway.*

If Ident was to become a problem, we have a monitoring server installed that we could setup an ident service on, but it's not been an issue as of yet.

> >*As it is, the entire house generated about 8MB in logs per 24 hour period. For 40 users of the network, this is considered very small. Most all activity is AIM and Web related.*

>
> *What all are you recording to generate that much? That's like 100000 lines of text.*

As I mentioned earlier, they have a NAT box, not a real firewall, and the logs track all in/out bound TCP/UDP traffic source, destination, local/remote port, time/date, etc... We have a couple scripts that process the logs to red-flag items so that we can quickly respond. More than half of the logs are inbound attempts that fail.

> >*The monitoring also lets us detect a virus outbreak as soon as it happens*
>
> *Obviously would have been better to prevent the infection, but the concept is otherwise OK.*

We removed more than 3000 viruses from their machines when they arrived at the house this year, many of them were infected while living in the dorms. The University offers free AV software, but you have to know about it, and you have to believe you need it, to install it. There were only 3 clean machines in the entire batch of them, and one was a MAC (but it didn't have all the OS/X updates).

Every machine was updated with the latest service packs, latest Office service packs, new AV software was installed, spyware detection software was installed, and all machines were certified clean before letting them on the house network. It's been over a month now and everyone's systems are running smooth and we're starting to get calls from other houses – due to the ladies talking to them about how smooth things are running in their house.

> > *which is how we got involved with them in the first place.*
>
> *But this, I don't know how to parse. This sounds political, rather*
> *than technical.*

The old IT company gave up on them, didn't want to deal with an outbreak, and the ISP was going to shut them off due to a massive SMTP virus spammer infection – sending about 250 email's out from 6 infected machines (using the viruses SMTP engine) every few seconds. They called us (a Friday evening) and asked if we could fix it, and we did in about 2 hours from the time they first called. The next session we got the contract to clean and secure the network/systems.

--
--
spamfree999@rrochio.com
(Remove 999 to reply to me)