

What Hackers Know About Your Network - That You Don't!

Whether you call them hackers, crackers or cyber criminals doesn't matter. What does matter is whatever you call them - they're looking for a way into your network!

You may not realize it but hackers are scanning your Internet connection looking for an opening.

What will they do if they find one?

They'll launch an attack against that opening to see if they can exploit a vulnerability that will allow them to remotely execute some commands thereby giving them access to your network.

But it all starts with scanning your network.

Automated Tools Are a Wonderful Thing

Cyber criminals don't scan each individual network on the Internet one by one. They have automated tools that randomly scan every IP address on the Internet.

Hackers aren't lazy people - just very efficient. And very intelligent.

The tools they use can be preloaded with a range of Internet addresses to scan. As this tool finds an Internet address with certain openings it produces a list of the address and the opening.

This list is then fed into another tool that actively tries to exploit that opening with various programs. If no exploit works, the hacker's program moves on to the next potential victim.

When you see the scanning activity in your firewall logs, you'll know where you're being scanned from and what they're trying to target. Armed with that data your security person should check to see if you're running software that uses that port and if it has any newly discovered openings.

If you are using software listening on a scanned port and there is a patch available, you should have that patch applied immediately - because the hackers may know something you don't. It's been our experience that many businesses patch their Microsoft Windows software but rarely do they check for patches for all the other software used in the business.

As stated, you'll see this activity in your firewall logs - that is, if someone is actually reviewing your firewall logs.

Oh, my firewall has logs???

However, when most business owners are asked about their firewall logs, the typical response is usually something like, "Oh, my firewall has logs?"

Yes, all firewalls produce log files. Most of them only show what's been blocked, which is like showing pictures of all the thieves that are in prison, while the bank down the street is being robbed.

Wouldn't you want to see all traffic? This produces more work, but if your firewall only logs activity it knows about, you're security is totally dependent on the ability of your firewall and the way it's configured.

Many firewall companies want to reduce their number of tech support calls. Their business model revolves around having tech support available, but in the process they're also seeking ways of reducing the number of times people call in.

This isn't necessarily a bad thing, but when their products have fewer features, thus fewer benefits as a result - that is a bad thing.

Most firewalls designed for the small business market lack features that most small businesses would benefit from. Many of them have all the technical

buzzwords like "deep packet inspection", "spyware prevention", "intrusion detection" and many others, however they don't go into the level of detail needed to be effective.

First, many firewalls that are "designed" for small businesses start with companies that have 100 - 250 users. These might be considered small businesses by the Bureau of Labor Statistics, but for technology purposes companies of this size have their own IT staff (96% do).

Not just one IT person, but an IT staff which means that someone is probably responsible for security. If not, they'll have someone train them in the proper setup, installation and monitoring of security appliances.

The businesses we consider small have anywhere from 3 - 50 PCs. The companies at the higher end of this scale might have someone dedicated to handling IT issues. But this person is usually so inundated with PC support issues that they have little time "left over" to effectively monitor firewall logs. Toward the lower end of this scale, they usually have either an outside person or firm responsible or they have an employee who "is pretty good with computers" who has other responsibilities as well.

Rarely will these small businesses have someone watching the firewall logs on a consistent basis. Someone might look them over if there's an issue, but these logs rotate when filled so the valuable information might be lost before it's ever reviewed.

And that's a shame.

Without reviewing the logs you have no idea what or who is trying to get in with which or what.

An Example Log File

Let's review some logs.

This happens to be a log from a client. The columns are labeled accordingly. This report has been cleaned up to make it easier to explain and understand.

Date	Time	Source IP	Source Port	Destination IP	Destination Port
06/18/2007	12:04:03.416	218.10.111.119	12200	55.66.777.1	6588
06/18/2007	12:16:05.192	41.248.25.147	4925	55.66.777.1	5900
06/18/2007	13:08:02.256	218.10.111.119	12200	55.66.777.1	6588
06/18/2007	13:22:10.224	58.180.199.163	4637	55.66.777.1	2967

What is this showing?

Well the first source IP (Internet) address is from Heilongjiang, a province in China. The destination is our client (mangled to protect the innocent) but the important data is the destination port. That identifies what they're looking for.

Port 6588 can be a few different things. They could be scanning for a Trojan that uses that port. If their scan responds with the typical response of the remote access Trojan, they know they've found an infected system. Port 6588 can also be a proxy server (which we won't describe here) with a recent bug. This bug makes it easy for a hacker to exploit thereby giving them remote access to the system running the proxy server software.

The hackers system will tell them what service is listening on port 6588 so they know what tools to use to attack that port.

The second line in our log file above is from Africa. Port 5900 is VNC which is used by many, many system administrators to remotely connect to a system to perform maintenance on it. This software has had a few exploits and one just last year allowed the attacker to have remote control of the system with VNC installed without having to crack any passwords!

Line 3 has our friend from China back trying again. Same port. They must be trying a few exploits against this port. Maybe they know something that the general security community isn't aware of yet.

On line 4 in our logs we see a new IP address in the source. This one is from Korea but notice it's scanning port 2967. This happens to be the port that Symantec's Anti-virus software listens on for new updates. There is a known exploit which allows remote attackers to execute arbitrary code via unknown attack vectors. When hackers find this port they know exactly what exploit to try.

In other words, the security software that is designed to protect systems is actually a way in for hackers due to a software bug.

It could be that there is a new "hole" in Symantec's software that hackers know about but Symantec doesn't. The previous hole was patched so either the hackers are looking for yet unpatched Symantec software or they know of a new hole and are looking for ways to infect them.

Without reviewing your logs you have no idea what is trying to get into your network.

Without a properly configured firewall, this type of attack would surely get through. This happens to be a firewall we configured so we know of ports like this and we blocked outside access because this client does not use Symantec products.

When talking security with a business owner I always ask, "When was the last time your network was scanned for openings?" They usually respond with, "Never". To which I reply, "Oh you're wrong there. You've been scanned, you just don't know by who!"

Regular scans of your network show you what the hackers are seeing of your network. It's a simple process and should be performed at least once a month. The results should be presented to you in a very readable, understandable report.

What to Do Next

The first thing you should do is check your firewall to make sure it's logging all activity.

Then, your job is to start reviewing the logs either everyday or at a bare minimum, once a week.

Some routers have the firewall "built-in". I've often found these are very limited in their ability to protect. Even more limiting is their logging functionality. Typically these devices will only show what's blocked.

Often these router/firewalls have the option to have the logs emailed to someone when they're filled up with entries. This is a nice option as you can have them directed to someone who will (should) review them in detail and notify you of any entries to be concerned with.

If your firewall doesn't provide the level of detail described in this article, you should seriously consider upgrading. You can keep your existing router just turn off the firewall feature and buy a dedicated firewall.

Then you'll know what the hackers know about your network.

Source: <http://www.articlecircle.com>

About the Author

Thomas J. Raef has been protecting the informational assets of businesses with 3 to 50 PCs for the last 11 years. His knowledge of computer security has led to numerous speaking engagements in front of thousands of small business owners. e-Based Security was formed to provide businesses with an affordable security system designed specifically for businesses with 3 to 50 PCs.