

# Why You Need A Network Services Audit

Michael J. Martin

This month we begin a series on network service auditing. Over the next few months, we will discuss how and why you should perform an inventory services audit. If you've never conducted one, you'll see that an audit can be quite enlightening.

Now, for many people, the idea of auditing anything is about as much fun as a root canal. In today's world of never-ending security alerts, we all know we should be conducting security audits, but we don't. I suspect there are a few reasons for this. The first one has to do with knowledge. Many network administrators have no background in systems or security. So while many would like to conduct an audit, for them the devil is in the details, which they are missing.

There are a number of great tools out there, such as Nessus and NMAP, not to mention all of the data that can be plucked off routers, switches and servers, which can help a great deal. Collecting and using this data is a double-edged sword, however. First, you need to have some understanding of the how to use the data; collecting for collecting sake is a waste of time. The other, more deadly, edge is that collecting this data can destabilize your network and crash systems. Care needs to be taken when using auditing tools. Running effective audits requires a documented, carefully planned methodology. Failing to develop a plan will put your network environment at risk and provide very little in terms of useful data.

That leads us to the second reason administrators resist auditing, the "my network is secure, I don't need to audit" mindset, or what I like to call denial (and I am not talking about a river in Egypt). This is simply a lie. Today, no network is secure. Computers are portable devices that travel from network to network. On average, most computer users use at least two or more networks to access data services on a consistent basis. Couple this with the, "hard on the outside, squishy on the inside" architecture many enterprise networks are still modeled on, security events are not are matter of if, but when.

In addition to insecure users, defects in the operating systems your servers run on are the most common source of network attack these days. Insecurity is built right into the OS. If you still think your network is secure, ask yourself these questions:

- If a virus attacked your network today and exploited microsoft-rdp (terminal services) or SSH v1.3.3, would you know which servers were running these services?
- Do you know the hardware vendor and operating systems of your network's critical service components?
- Would you be able to tell if someone attached a wireless access point to the LAN?
- Would you be able to detect if someone redeployed a "known" server to perform a new function?
- Do you know what network services are running on each of your servers and which ones are active?

If you answered "no" to any of these questions, then you can feel pretty confident that your network is not secure. But don't feel bad, even if you answered yes to each question your network is probably still not secure. But, you do have the advantage of being in an excellent position to identify and mitigate a network security event when it comes. When running an audit you need to work from the perspective that the network is insecure. Once the initial baseline audit is complete, you will need to verify your findings. Be prepared to work with your system administrators and application developers to make sure what you are finding is what should be in place. If they can't help, then contact the product vendor. If you're unable to discern between what should and should not be running on the network, you cannot secure it.

# Why You Need A Network Services Audit

Michael J. Martin

The third and final reason for audit neglect is to blame for many things: time (or lack of it). A network audit does take time. To make matters worse, you need to repeat them frequently and consistently. One of the most common responses to a good security audit is, "We conducted one. We found nothing. Case closed." This is a mistake. You need to think of network audit results are highly perishable.

You can assume that the results will be valid until you make a change in the network (if you run DHCP, this can be daily) or until the next vulnerability is announced for one of the platforms running on your network. Network audits need to be run on a regularly scheduled basis, and the data needs to be historically compared. Many security events are not detectable when they occur. Historical audit data can be used to identify when systems have been compromised, because often the operational characteristics will have changed. Without consistent auditing and results comparison, these changes in systems are hard to detect.

In an ideal world, you could build your network, connect all of the servers, and run a baseline of network services before any users had access. While ideal, this is also impractical, since without users you would never be able to know what services on the servers were actually being accessed. That said, once you have established auditing, new nodes should be audited when they are first introduced into the network. A typical network services audit collects the following data for each node:

- ARP address
- IP address
- DNS name and aliases
- Operating system
- Running network services (with version if possible)
- Active network services

A node can be a server, router, switch, wireless access point, or anything that is constantly connected to the network. While auditing user nodes has value, unless they are locked down and not modifiable by users, building useful profile data becomes a very burdensome task. The safe perspective to take is that all hosts not under a centralized administrative control should be considered hostile and to be defended against. Collecting the audit data is handled in three phases:

- Host identification: This process involves building databases of the active hosts connected to the network. This data is collected from three sources: switch ARP tables, active ICMP scans and DNS zone lookups.
- Host profiling: This process involves scanning the hosts to identify operating system, running network services and version info. Data is collected by running port and/or vulnerability scanners against the list of active hosts.
- Service profiling: This process involves monitoring inbound traffic flow to identify what network services are active. Using the host profile, data traffic monitoring access lists can be created and installed to monitor and detect network traffic patterns.

Next time we will pick up with the host identification process, which, with the right tools, is easy to accomplish. Before you go, let me leave you with this thought: Network auditing may be a time-consuming chore that you probably don't have time for. It's more than likely, however, that someone has already gone to the trouble and is scanning your network for weak points to attack. It could be someone within your organization; FBI statistics show that more than 60% of computer crimes

## **Why You Need A Network Services Audit**

**Michael J. Martin**

originate inside the enterprise. So remember that the best defense is a good offense, and you cannot raise a good defense unless you know where your network is weak.