Realtime publishers

Security Management Tactics for the Network Administrator

The Essentials Series

Using Network Management Tools to Identify a Network Attack

sponsored by

Mike Danseglio

Using Network Management Tools to Identify a Network Attack 1
What Does a Network Attack Look Like? 1
How Can Network Management Tools Identify an Attack? 3
How Should I Respond to the Attack? 5
Summary 5

Copyright Statement

© 2010 Realtime Publishers. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtime Publishers (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtime Publishers its web site sponsors. In no event shall Realtime Publishers or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtime Publishers and the Realtime Publishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtime Publishers, please contact us via e-mail at info@realtimepublishers.com.

Using Network Management Tools to Identify a Network Attack

Network attacks are a persistent and virtually continuous threat. Attackers are working 24 hours a day to compromise virtually every network connected to the Internet. And attackers have gotten better at their job over time. Gone are the days of random poking and prodding on a network. Today's attacker is well-trained, well-equipped, and has a specific task list. He is attacking for a specific reason, be it profit, political ideology, industrial espionage, or any other reason. He will not stop attacking until he is successful or until some other target becomes more tempting. And catching him is exceptionally difficult, considering that he's probably on the other side of the world.

But you can put a stop to his shenanigans and protect your network. And you might even be able to use the tools already deployed on your systems to do it.

What Does a Network Attack Look Like?

If you watch movies, you've undoubtedly seen the same basic scene repeated over and over: an evil attacker, wearing all black, skulking behind a terminal; a data center erupting with lights, sirens, and people running everywhere; a hero boldly thwarting the attack just as a SWAT team breaks in and arrests the attacker; a happy ending. That's a great story. But it never really happens.

There are two facts about network attacks that you should understand up front:

- Someone is attacking your network right now, and
- You probably don't know about it

Luckily, most network attacks are unsuccessful. This is largely thanks to IT departments paying more attention to security as well as improvements in most technologies that help keep systems better protected by default. But that doesn't mean you can safely ignore the unsuccessful attacks. They provide a wealth of information about how your network is affected, how you can defend it in the future, and even when a detected unsuccessful attack becomes an undetected but successful one. The easiest way to spot a network attack is to watch key network statistics (see Figure 1).

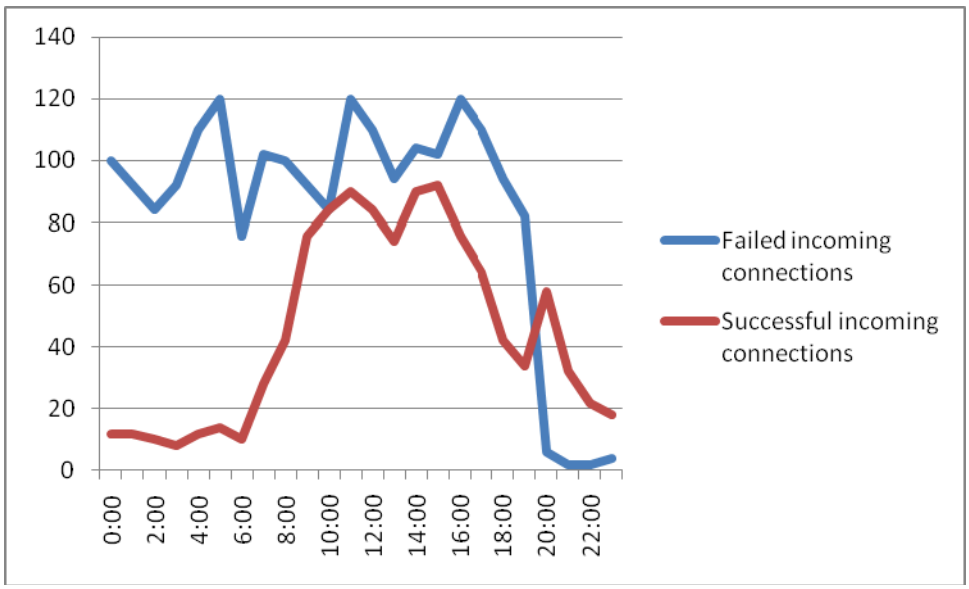

Figure 1: An attack in progress.

Notice in Figure 1 that there is an interesting event happening around 19:00. The number of failed incoming connections drops dramatically from the daily average and actually bounces off zero for a bit. By itself, that data might not mean anything. The drop could be the attacker going out for dinner, or an intermediate security device that temporarily throws off this type of attack. Now correlate that drop with another important measure of network performance (see Figure 2).

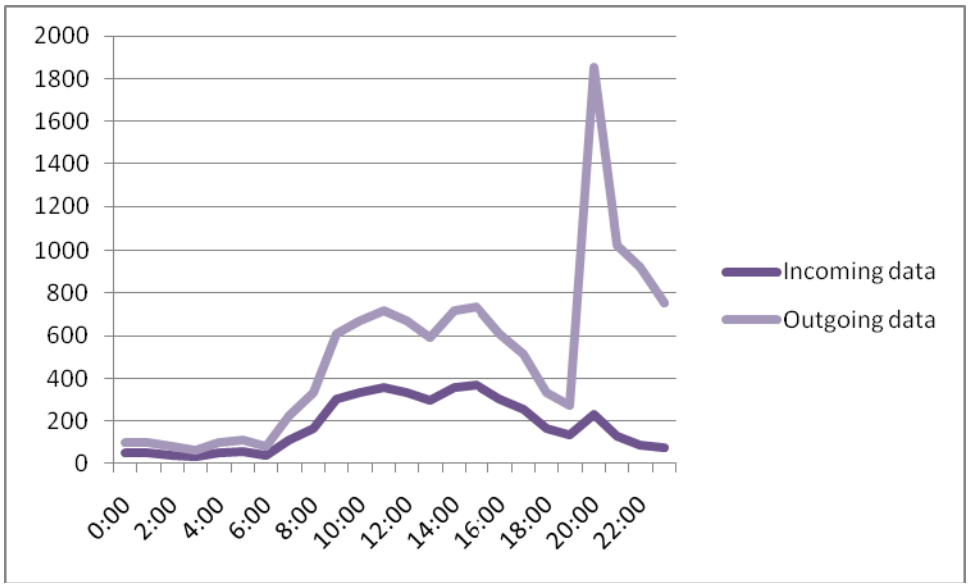

Figure 2: Data flow during an attack.

The information in Figure 2 shows the amount of data coming into and going out of the corporate network. Network utilization spikes of this nature are common when certain behaviors occur, like a user uploading a new product video to a marketing site. But the times seem to correlate very closely. At around the same time the unsuccessful network attacks dropped, the amount of outgoing traffic skyrocketed. This is a very typical pattern seen when an attacker achieves success. As soon as they have access to the resources they're looking for, they begin extracting it as quickly as possible. The attacker doesn't want to stay on the network any longer than necessary and so will download everything and go through it later.

> **Note**
>
> Although the aggregate data in Figure 2 is useful, it is difficult to mitigate an attack without more details. Details like the identity of the network host sending the data spike are critical. Information like this is best obtained through flow monitoring tools, which are described in the next section.

The data correlation between these two events might be coincidental. But it is worth investigation. Most security analysts would immediately pour through authentication logs for that timeframe and then work on identifying the source and destination of the outgoing data traffic.

How Can Network Management Tools Identify an Attack?

Most network attacks exhibit a specific pattern. One of the most common patterns is illustrated in Figures 1 and 2. Most frequently, a network attack shows up as a drastic change in network statistics.

Almost by definition, network management tool suites monitor and report on network statistics. The suites do so in a variety of ways. Some of the most powerful tools use a technique called *flow monitoring*, where data is gathered from devices and then analyzed based on a number of criteria to generate custom views and reports.

Flow monitoring is implemented by a variety of network hardware vendors, many of whom have different data storage and reporting formats. Some of these vendors and formats include:

- Cisco NetFlow v1, v5, and v9
- Cisco NetFlow Secure Event Logging (NSEL)
- Juniper Networks J-Flow
- IP Flow Information Export (IPFIX) originally defined by RFC 3917, which eventually became Cisco NetFlow v9

Similar to other tools described in this series, the more advanced flow monitoring tools enable richer functionality. The more advanced tools support features like:

- Identification and ranking of largest network bandwidth consumers by protocol, source, and destination
- Network traffic classification for baseline creation and subsequent comparison against baseline metrics
- Timeline-based reporting to analyze busy and slow network times and comparison to identify atypical network traffic flow
- Real-time administrative alerting when flows exceed defined threshold or approach maximum capacity

Flow monitoring tools are useful in a number of business analytics including the determination of network use based on protocol, application, server, or user, or even to verify proper configuration of network-centric processes like quality of service (QoS). This kind of deep network flow monitoring can be invaluable to all aspects of a business, not just security. In addition, verifying transparent-yet-important network processes like QoS can be very difficult and time-consuming without automated systems.

Other monitoring tools use various techniques including dedicated network agents, queries against switches and routers, active monitoring, polling system event logs, and more. And they aggregate all of this data in an analyzable way. This makes network management suites a natural resource to use to identify attacks as they already have all the data necessary to perform the task.

Virtually all of these tool suites have an automated data monitor and alerting system. The system watches the reported data for defined patterns—such as a dramatic increase in outgoing traffic at the same time there is a dramatic decrease in incoming failed connection attempts—and takes one or more actions. These actions usually include running defined scripts, alerting administrators, or provisioning resources to meet demand.

You should ensure that your network management tools, at a minimum, alert an on-call administrator when any suspicious traffic patterns take place. These alerts are often preconfigured in the software but can be fine-tuned to eliminate the majority of false alarms. You can also add and modify network monitoring alerts as threats evolve to give you early indication of trouble.

An early warning like this can easily make the difference between a successful and unsuccessful attack if your response is swift and sure.

How Should I Respond to the Attack?

Your cell phone rings at 2AM to alert you to a network traffic pattern matching a new, widely successful attack. Arriving at the office moments later, you can see that the traffic pattern does indeed indicate an attacker that has finally succeeded in breaching your perimeter. You can see the outgoing traffic volume to the attacker's IP address slowly increasing. What do you do?

If a criminal were breaking into your car and stealing your stereo, you'd call the police, stand back, and perhaps take photos or video with your phone. This situation isn't much different. In most cases, the prudent response is to simultaneously contact law enforcement and try to capture as much information about the attack as possible.

That doesn't mean the criminal will be brought to justice. Many attackers are never caught. And law enforcement's response to your call may be instructions to simply disconnect the attacker to stop the intrusion, then remediate the vulnerability that allowed the attacker to succeed. Realistically, your primary concern should be the protection of your assets. So closing down the Internet connection to prevent sensitive data compromise might be the best response. After all, defending your assets is likely the most important thing you can do, even if it results in a lack of evidence or a less-than-clear identification of the intrusion method.

If law enforcement does want detailed information, you should ensure that you get instructions on what components in your infrastructure should not be touched until law enforcement officials arrive. The preservation of digital evidence through forensics can be tricky. When in doubt, ask the professionals.

Summary

The digital landscape gets more dangerous every day. As the world gets more connected, speed increases, technology evolves, and the attacks get more complex, there is always an attacker waiting out there to compromise your security to make a profit or a statement. Defending against classic attacks of yesterday isn't any less important, but detecting and responding to future threats is a critical need.

Most network monitoring systems have the capability to perform very advanced security monitoring. It is worth a look to see if you can implement this level of network security for no additional cost beyond your existing investment.