University Security

Douglas Brown

Name: Douglas P. Brown
Version: GSEC 1.2e
Title: University Security

Our Universities are under attack. Networks comprised of heterogeneous hosts with fast Internet connections make universities desirable targets to a wide variety of attackers. Members of university communities are often not concerned with security because they assume that hackers attack systems to obtain confidential information. These academics have not realized that many attacks are instead quests for disk space or processor time and that the information stored on a server is sometimes irrelevant to the attacker. The resulting lack of system security at universities has allowed attackers to quickly make universities the preferred staging areas for distributed denial of service attacks. Decentralized structure and large size make many university networks difficult, but not impossible, to secure. By using a combination of security tools and procedures universities can provide a more secure computing environment than has generally been available.

Firewalls are the first option that comes to mind when many people think of network and system security. Stephen Northcutt, head of the SANS Institute's Global Incident Analysis Center, said in response to recent attacks on universities, "Why were universities so involved in these attacks? Because they're naked. They're sitting out there on the Internet with no firewalls or anything" (quoted in Borland). Universities are certainly open to the Internet, but border firewalls are often not an option for many university environments. Only recently have firewalls developed to the point where they can handle the bandwidth requirements of some universities' 40,000 (or more) hosts. As learning institutions, universities often wish to encourage academic freedom. Having to request a firewall conduit to allow access to your departmental web server is often seen as stifling to this freedom. Operation of the firewall would also pose an administrative and maintenance juggernaut for a large environment, requiring technology staff that many universities cannot easily spare or justify.

Many universities also connect student housing to the network. The firewall requirements for a student residential network are vastly different than the requirements for a university business network. Students may be reluctant to use a network where a firewall blocks many of their favorite applications, and a business network would be less than secure with some of these student applications open through the firewall. Balancing the conflicting firewall needs between students and business often fails to satisfy either community.

In contrast to firewalls, Intrusion Detection Systems (IDS) can be effectively used for these large university environments. Intrusion Detection Systems do not inhibit traffic, but rather allow a trained staff to react to attacks and provide early identification of compromised hosts. An IDS does not necessarily require the same level of administration or maintenance as a firewall. Daily monitoring and log response for an IDS can take less time and staff than the maintenance of a firewall for a similarly sized environment. While daily monitoring of the IDS would be ideal, it would not be necessary should a pressing matter take away resources. Cost is often an issue for Universities, but with IDSs such as Snort available for free, many factors make the IDS a desirable option.

Unfortunately a uniform out-of-the-box solution does not exist for every large environment. Using an IDS in a university environment requires some configuration. Knowing the environment and writing custom rules to look for new attacks are only part of the battle. It is important that the IDS be positioned on the network such that it will see all inbound and outbound traffic. The systems running the IDS must also have the processing power necessary to analyze all traffic. Although the free IDS Snort is considered a lightweight intrusion detection system for small networks, I will explore the use of this product in a large and demanding University environment.

A sample of the top 11 alerts from a University's IDS:

Signature (click for sig info)	# Alerts	# Sources	# Destinations	Detail link
INFO Possible IRC Access	859	58	67	Summary
WEB-MISC Invalid URL	961	128	410	Summary
WEB-FRONTPAGE fpcount.exe access	1062	580	301	Summary
RPC portmap request rstatd [arachNIDS]	2456	43	207	Summary
WEB-MISC count.cgi access [CVE]	3856	2398	393	Summary
WEB-MISC 403 Forbidden	5285	565	1115	Summary
WEB-MISC http directory traversal [arachNIDS]	8062	638	485	Summary
WEB-IIS msadc/msadcs.dll access [BUGTRAQ]	8082	4	3	Summary
WEB-MISC L3retriever HTTP Probe [arachNIDS]	8095	5	181	Summary
CUSTOM tcp traffic contains bin_sh	16039	21	2170	Summary
SCAN synscan portscan [arachNIDS]	23599	1	23554	Summary

(Snort)

When examining the IDS results comparing numbers for alerts, sources, and destinations is often very telling in determining the legitimacy of traffic. For example, the portscan in the bottom signature is clearly a pre-attack portscan of the subnet. One source creating 23,599 alerts to 23,554 destinations often typifies the type of traffic that administrators of large networks like to avoid. The recent proliferation of scripts and other automated attack tools has increased this type of activity; such high volume can be devastating to a small network.

Other results track signatures that are normally legitimate; for example, the IRC access signature may be a user legitimately using IRC. The IRC signature may also be a recently trojaned system advertising itself in an IRC channel. The combination of this signature with others, such as the subseven signature, may serve as a clear indication of a trojaned host. The IDS is a very effective tool to give the staff an overview of the activity for the entire network or an individual host. Multiple suspicious signatures from or to a single host can be a clear indication of trouble.

The web-related signatures have numbers that can be expected for an environment of this size. Further examination reveals that all alerts seem to be the result of normal web browsing both to and from this University's network. Knowing which systems on the network are high traffic web servers helps separate attacks from normal traffic.

Investigation of the RPC signature reveals one off-campus host with 393 alerts directed at 183 different on campus systems. A sample of the traffic seen:

Jul 5 02:52:14 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:816 -> *.*.5.129:111
Jul 5 02:52:14 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:817 -> *.*.5.130:111
Jul 5 02:52:14 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:818 -> *.*.5.132:111
Jul 5 02:52:14 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:819 -> *.*.5.133:111
Jul 5 02:52:15 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:821 -> *.*.5.136:111
Jul 5 02:52:15 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:821 -> *.*.5.137:111
Jul 5 02:52:15 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:822 -> *.*.6.138:111
Jul 5 02:52:15 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:823 -> *.*.7.64:111
Jul 5 02:52:15 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:824 -> *.*.7.65:111
Jul 5 02:52:15 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:825 -> *.*.7.66:111
Jul 5 02:52:16 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:826 -> *.*.7.67:111
Jul 5 02:52:16 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:827 -> *.*.7.68:111
Jul 5 02:52:16 snort-in snort[15876]: RPC portmap request rstatd: *.*.206.2:828 -> *.*.7.72:111

(Snort)

The small sample of the traffic shows that the attacking host attempted to connect to the RPC port on each machine within a subnet. Due to the small time between each attempt, the attacking system probably used another automated attack script to look for vulnerable RPC hosts within the University's subnet. RPC is a favorite service for attack. Many vulnerabilities and exploits are available for this service, and most users gain nothing from running the RPC service. Like echo and chargen, RPC is a service that many users fail to disable.
A sample of the TCP traffic contains /bin/sh signature:

Source	# Alerts (sig)	# Alerts (total)	# Dsts (sig)	# Dsts (total)
..*.3	11194	11272	110	113
..*.81	4746	4771	2007	2014
..*.240	26	714	19	72
..*.1	23	8508	14	417
..*.126	11	17	6	12

(Snort)

Knowledge of the network continues to be important. This university mirrors several sites for the distribution of software. Knowing which servers are the mirrors, we can see that the top five sources in the summary are all software mirrors. This traffic is not suspicious. If the source for the traffic were a surprising on-campus host or an off-campus host, then an attack or compromise would be suspected.

Monitoring what is seen in an IDS and responding to attacks will serve the average university environment well. These responses should be two-way, to both the sources of the attacks and the destinations of the attacks. While a diligent administrator should be monitoring system logs, not every attack captured by the IDS will also appear in these logs. Warning that a system is running a targeted service may at least prompt the administrator to check their patch levels.

An IDS serves a role similar to that of the closed circuit television camera systems used in banks; it will record the bad guys, but it will not stop them. Cisco states that the best approach is, "Implementing network security technologies in a comprehensive and layered approach so that the enterprise does not rely upon only one type of technology to solve all security issues" (Cisco). As security is best accomplished through a layered approach consideration must be given to the individual hosts on a network. A firewall or IDS is not a panacea for network security. Both of these items are tools that are best used in conjunction with other tools. Considering the tools used from an overall perspective allows the pieces to fit; just as a hammer works best with nails, it best not to end up with screws to use with your hammer.

A site license by a university for an anti-viral product that is installed on all file servers, mail servers, and client hosts is an excellent security layer to add to the environment. Government agencies recognize the importance of anti-viral programs. According to Brookhaven National Laboratory,

> "Anti-Virus procedures are an important component of BNL's host-based security architecture. Anti-Virus software is the component of this architecture that provides a protection mechanism against malicious code. Malicious codes are programs, such as Trojan horses or viruses, that run on a host system without the authorization of the system user." (Brookhaven)

Every day more viruses are written and more holes found to load Trojans onto unsuspecting machines. A good anti-viral product with current definitions can protect against most, but not all of this traffic.

User and administrator security education is critical, but it is also important to avoid creating an environment where paranoia prevents people from doing their jobs. Encouraging users to keep their virus definitions current is part of this security education. Other steps necessary for host security have been described as:

- *Understanding the functions the system will perform*
- *Applying all the vendor recommended security patches*
- *Removing all the unneeded services*
- *"Tightening" directory and file permissions*
- *Installing "watchdog" host and network programs*
- *Designing backup and recovery procedures* (msh.com).

These items may sound like common sense to many people, but a surprising number of users and administrators in university environments do not follow these simple steps. Commonly graduate students are drafted to administer research systems, and these students receive little or no training; security is often not a concern. Making the education available for these users to learn how to shutdown services, how to setup TCP wrappers, and how to install a product similar to Tripwire can enhance security. Although hackers are often not interested in the data on a compromised system, loss of this data is always a concern. The ability to quickly restore from backup in the event of a compromise will lessen downtime, but only if the initial steps are taken to provide for security and disaster recovery.

When the messages sent in complaint receive no response, and the attacks against a network continue, placing filters on the border router to block subnets that are known sources of multiple attacks is a good option. Many organizations avoid this action fearing that they may interfere with legitimate work. A university recently blocked a subnet from China, only to find that this block interfered with a professor's access to his colleagues. Fortunately the professor had good contacts in China, was able to stop the attacks, and the block was removed.

Router blocks are not something to be taken lightly, but they are also not something to rule out. Recently there have been a number of LPR exploits. Router filters to block TCP traffic directed at port 515 would have stopped many of these attacks, but in some cases legitimate print jobs do originate from off campus sources.

A sample router access list:

deny ip *.*.9.0 0.0.0.255 any (354 matches)
deny ip *.*.228.0 0.0.0.255 any (127 matches)

deny ip *.207.0.0 0.0.255.255 any (156180 matches)
deny ip *.13.0.0 0.0.255.255 any (47835 matches)
deny ip *.75.0.0 0.0.255.255 any (496633 matches)
deny udp any range snmp snmptrap any (1696609 matches)
deny udp any any range snmp snmptrap (776719 matches)
deny ip any 0.0.0.0 255.255.255.0 (174212 matches)
deny ip any 0.0.0.255 255.255.255.0 (193064 matches)
deny ip *.2.0.0 0.0.255.255 any (110427 matches)
deny ip *.19.0.0 0.0.255.255 any (2815 matches)
deny ip 10.0.0.0 0.255.255.255 any (1015028 matches)
deny ip 172.16.0.0 0.15.255.255 any (894354 matches)
deny ip 192.168.0.0 0.0.255.255 any (4698863 matches)
deny ip any 10.0.0.0 0.255.255.255
deny ip any 172.16.0.0 0.15.255.255
deny ip any 192.168.0.0 0.0.255.255
deny ip *.*.191.0 0.0.0.255 any
deny ip *.*.192.0 0.0.0.255 any (7044 matches)
deny ip 127.0.0.0 0.255.255.255 any (5071 matches)
permit ip any any (226937983 matches)

This access list includes blocks of known bad subnets. It also blocks any traffic destined for the campus that appears to be originating from an on campus IP Address (spoofed), and it blocks the private addresses mentioned in RFC 1918. The importance of these filters has been outlined in several articles,

> "[user organizations] should also ensure that no traffic from "unroutable addresses" listed in RFC 1918 are sent from their sites. This activity is often called *egress filtering*. User organizations should take the lead in stopping this traffic because they have the capacity on their routers to handle the load" (Sans.org)

Taking these proactive measures now, to prevent attacks on the network, or from the network, can make the job of security easier for universities. Knowing the network, and having a good set of tools, will allow an appropriate response from universities to new security threats.

Lack of network security is giving our universities a reputation as hacker havens. Tools are now available that work with large numbers of heterogeneous hosts, and fast Internet connections, without stifling academic freedom. Universities can provide a more secure computing environment. Firewalls may not be a good option, but the use of an Intrusion Detection System combined with user education in host security, university licensing of key security products, and an overall awareness of best practices will enhance network security at these institutions.

Works Consulted

Borland, John. “Universities likely to remain Net security risks.”
February 15, 2000. July 3, 2000.
<http://news.cnet.com/news/0-1005-200-1550326.html?tag=st.ne.1002.tgif?st.ne.fd.gif.f>

Brookhaven National Laboratory. “Anti-Virus Procedures.”
June 15, 2001. July 6, 2001.
<http://www.bnl.gov/cybersecurity/antivirus.asp>

Cisco, Inc. “Network Security.”
July, 6, 2001.
<http://www.cisco.com/warp/public/779/largeent/issues/security/>

Criscuolo, Paul J. “Distributed Denial of Service – CIAC-2319.”
February 14, 2000. July 6, 2001.
<http://www.ciac.org/ciac/documents/CIAC-2319_Distributed_Denial_of_Service.pdf>

Educause Quarterly. “Top Campus IT Challenges for 2001.”
Number 2 2001. July 9, 2001.
<http://www.educause.edu/ir/library/pdf/eqm01211.pdf>

MSH Consultants. “Host / System Security”
July 6, 2001.
<http://www.msh.com/host.html>

Radcliff, Deborah. “University Computers Remain Hacker Havens”
February 12, 2001. July 6, 2001.
<http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57605,00.html>

Sans.org. “Consensus Roadmap for Defeating Distributed Denial of Service Attacks”
February 23, 2000. July 9, 2001.
<http://www.sans.org/ddos_roadmap.htm>

Snort – Tables provided from Snort-Snarf system used at a large university.
July 6, 2001.
<http://www.snort.org>

Stanford University. “Host Security for E-Commerce and Critical Infrastructure Services”
Jan 25, 2001. July 6, 2001.
<http://www.stanford.edu/group/itss-ccs/security/critical/hostsec.html>