GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

The University has a firewall – isn't that enough?

Why users still need to be concerned about computer security

Sherry Cummins
May 13, 2002
GSEC Practical Assignment Version 1.3

Abstract

As the risk of attack against computer systems rises, firewalls of various types are frequently used as part of the overall security infrastructure of many institutions, including universities. There is evidence to show that universities are even more at risk for attack and compromise than other types of institutions. Users and system administrators of university systems do not always understand that a firewall is not by itself an entire security solution, but must be a part of a layered defense.

Firewalls are not perfect and do not protect against all forms of attack. They can be configured too openly, have limited ability to stop viruses, and can be bypassed by various methods. In addition, hackers from inside the institution and employees who are taken in by social engineering techniques cause security problems no firewall can help. Users must be aware of security risks and understand that in addition to the protection provided by their firewall, they must also help to maintain the university's computer and network security.

Introduction

In the past several years, computers have become such an integral part of the workplace that it is rare to find anyone in an average office who does not have access to a computer for at least some part of their daily tasks. As employees learn how to utilize computers to help them in their jobs, they must also become increasingly aware of the risks that hackers, viruses, and other threats pose to their computers and the data they contain.

Any device that can be connected to a network of any type can be attacked. This includes everything from mainframes and large servers to routers, desktop workstations, PDA's, and even mobile phones. Usually attacks are aimed at the most common types of computers and their software, namely Windows PC's and servers, and computers running some form of Unix. This is probably because the number of potential targets and their relatively well-known vulnerabilities make the attacker's effort more likely to pay off. However, I have seen networked printers that were made to spew out pages of useless and unreadable printout when probed from outside the network.

At the university where I work, I have often heard questions and comments such as "If we have a firewall, aren't we already safe?" As a system administrator of computers on the university's network, this is a question I have had to investigate with regard to the safety of my own systems. After some reading and a lot of consultation with the experts,

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

the answer, I have found, is quite bluntly "no". This paper explains ways in which a firewall might be bypassed or penetrated and why individuals must do their part in helping to maintain computer and network security.

A university network is a high-risk environment

University computer systems are a favorite target for hackers. At first glance, it may not be clear why these systems are attacked so frequently. Although some university systems contain sensitive student, financial, and research data, most computers connected to an academic network do not generally hold secret strategic, defense, or weapons information, provide privileged access to large credit card databases, or otherwise have information that anyone would be interested in going to a lot of trouble to steal. Nevertheless, it is widely understood that a computer with a network address ending in .edu is more likely to be a hacker's victim of choice than computers residing in other types of network domains.

The primary reason for this is fairly simple. Hackers have discovered that university computers and networks are often easier to gain entry into and exploit than computers and networks belonging to military or commercial sites. Although hackers are less likely to be interested in the actual data they contain, computer systems at universities are attractive to hackers for other purposes. Among these are:

- Obtaining easy access to the thrill of success for novice hackers while they learn their hacking skills
- Stealing resources for the hacker's own processing needs
- Using a compromised system as a stepping stone to other potential victims
- Establishing a 'testing ground' for experimenting with attacks that might later be used against commercial or government sites
- Using a compromised system as a zombie attacker in a DDOS or other external attack

By some accounts, attacks on universities are so common that the addresses of compromised university computers are frequently bartered between hackers for other addresses, information, or items that the hackers want.

The overall threat of malicious attacks is growing worse

Historically, university computer systems and networks have conformed to an open architecture to allow free flow of information into and out of the network without putting too much limitation on the freedom and creativity of the academic enterprises they support. This openness, coupled with a chronic lack of resources and manpower at most universities, causes computer and network security to be a big enough challenge. In the past several years, however, two changes have occurred simultaneously to further complicate the task of trying to provide a reasonable measure of computer security within this traditionally open architecture. The first change is the movement from a centrally managed mainframe-dependent system to a system of decentralized, locally managed

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

servers. In the older, mainframe-centered system a small specialized group with specific skills and training managed data protection, access to resources, and networking from within a centralized computing facility. Today it is very common for a large part of the total computing power of a university to reside in decentralized computer systems, where management often falls to isolated departmental system administrators whose primary function may not be computer support, and who may not have the time necessary, knowledge, or funding to devote to the increasingly complex task of keeping their computers and networks secure.

The second change that has taken place is the drastic increase in the use of the Internet to attack remote computer systems. According to records kept by the Computer Emergency Response Team (CERT) Coordinating Center at Carnegie Mellon University, the number of security incidents reported to CERT by various sites increased from a total of 6 in 1988 to 52,658 in 2001. As of the end of the first quarter of 2002, the total number of incidents reported so far is 26,829. If incidents continue to be reported at the same rate throughout 2002, the final total for the year (107,316 or more) will exceed the cumulative total of incidents reported to CERT in all preceding years. A summary of the total number of attacks reported to CERT annually since 1988 is shown below in Table 1.

YEAR	INCIDENTS
1988	6
1989	132
1990	252
1991	406
1992	773
1993	1,334
1994	2,340
1995	2,412
1996	2,573
1997	2,134
1998	3,734
1999	9,859
2000	12,756
2001	52,658
Q1, 2002	26,829

Table 1. Number of Incidents Reported, 1988 – 2002. (Source: CERT/CC Statistics 1988 – 2002)

In the Internet Software Consortium's January 2002 survey of top-level domain names by host count, .edu hosts accounted for 7,754,038 hosts out of a total of 147,344,723 total hosts queried, or just over 5% of all computers that could be counted via the Internet. (Source: Internet Software Consortium (http://www.isc.org/.)) Based on these figures, and given the projected number of incidents for 2002 from above, university computers

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

can be expected to be the target of at least 5,366 reported incidents this year – more than the total number of incidents reported to CERT in any single year prior to 1999. Since it is believed that universities are targeted more frequently than other types of domains, we must assume that the actual number will be even higher.

When examining these horrifying trends, it is important to keep in mind that some of the rise in reported attack rates is probably explained by the fact that increased awareness of security and hacking causes victims of attacks to report them more frequently than in the past. On the other hand, what is reported to an official agency such as CERT almost certainly represents a fraction of the total number of incidents that occur.

A firewall is just one part of a layered security plan

A memorable comment by Bill Cheswick, noted security expert from AT&T and co-author of "Firewalls and Internet Security: Repelling the Wily Hacker", describes a network protected by a firewall as "a crunchy shell around a soft, chewy center" (McClure, p.394). What this implies is that if a firewall is used as a network's only defense, once it is penetrated intruders are home free, with no further obstacles to obtaining access to whatever they want to do.

The popular visual image of a firewall is of a solid brick wall placed between the internal network and the outside world. If this image is carried a bit further, the network inside the firewall could be represented as a city, with individual computers as the houses and buildings and the brick wall around it for protection. In our modern Internet world, this walled city is under constant attack, with the number of attackers increasing daily. Imagine that the inhabitants of the city rely on the brick wall as their only defense, hoping that their enemies neglect to bring a ladder or a rope, forget to pick the lock on the gate, and don't notice the places in the back of the wall where the bricks don't quite meet or no mortar was used. No sentries are posted, and homeowners do not bother to lock their doors or carry weapons because the wall is there to protect them. With such meager defenses, this imaginary city would be quickly overrun, as will any network where a firewall is used as the only defense.

If, however, other layers of defense are used in conjunction with a good firewall, the intruder's job becomes much harder. Virtual LAN's, access control lists, personal firewalls, virus scanners, and monitored system logs are just a few of the other tools that can be used to improve the security throughout a network. Some of these additional layers of security may be set up and maintained by institutional networking personnel, but others are implemented on individual computers that are not under direct institutional management. Unfortunately, the existence of a firewall at the network perimeter can lead users and system administrators within the network to have a false sense of security. They may not understand the need for continuing vigilance on their part or may simply become less concerned about maintaining the parts of the overall security infrastructure for which they are responsible.

A firewall that is too open is limited in its effectiveness for protecting the network

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Firewalls are put in place for the purpose of monitoring and controlling electronic traffic into and out of a network. The most common form of firewall technology currently in use achieves its purpose with packet filtering. As packets come into the firewall, the source and destination IP addresses and ports in the packet header are examined. Each packet is allowed or denied passage through the firewall depending on whether its IP address and port information match the deny (block) and allow (pass) rules written into a ruleset configured by the firewall administrators.

Properly configured and monitored, a firewall can do a good job filtering traffic coming into a network (ingress filtering), protecting the computers and the network from malicious probing and unauthorized connections from the outside. Some firewalls are also configured to control what is allowed to pass out of a network (egress filtering). This is done to help reduce leakage of information to the outside, and to prevent compromised computers or unscrupulous users inside the network from attacking other sites.

Traditionally, rulesets have been written to be very open, with an "allow all/deny specific" approach to packet filtering. Firewalls with this type of open ruleset allow all traffic to pass through except those whose header information contains particular addresses or ports that have been determined to be undesirable. In recent years, the increased threat of external attacks has caused the opposite of the open approach, a "deny all/ allow specific" ruleset, to become increasingly common. This more closed ruleset improves security by blocking all packets except those that contain specific addresses or ports in their headers. In spite of the increasing popularity of the closed approach, however, some organizations, including many universities, continue to use more open, less secure rulesets.

Determination of the appropriate filtering rules for any firewall is dependent on many considerations and the decisions must be made with the purpose of the network and its users in mind. Nevertheless, allowing the ruleset to be written in a way that is too open can increase a network's vulnerability, and can make the firewall seem less like a brick wall and more like a chain link fence.

A firewall is not intended to protect against all potential threats

Although useful in preventing certain types of malicious traffic from passing into a network, there are some things firewalls do not do well. For instance, because they filter traffic by inspecting packet header information, traditional firewalls cannot be made to block viruses and other exploits that are written into computer code and travel in the data portion of multiple packets. With most firewalls, the best that can be achieved in protection against viruses is to block potential network access by a particular virus exploit based on an external IP address or port that the virus is known to use. This prevents the virus from infecting other computers, contacting a site where further exploit code can be obtained, or sending out sensitive information about the computer or network it has infected. Because this type of filtering on the firewall is somewhat haphazard and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

difficult to maintain, virus protection is best done at other levels in the overall network architecture. Virus scanners on incoming e-mail gateways, endpoint servers, and individual workstations are much more effective in combating the virus code itself, and can often be kept up-to-date much more reliably than any type of firewall filtering that could be established.

Firewalls also cannot prevent attacks that occur through ports or IP addresses that appear legitimate. Even if a firewall is very closed, some ports and addresses will be allowed through. If the ruleset on a firewall specifies that telnet traffic must always be passed, any exploit that utilizes the telnet port will pass into the network unchallenged. If packets are always accepted from a particular IP or domain, any exploit from that source will be allowed through to wreak its havoc. To guard against threats of this type, the administrators of servers and pc's inside the network must pay attention to software patches and such hazards as default passwords and accounts that could be exploited.

A firewall is often not the only way into a network

Either accidentally or deliberately, there often exist several alternative routes into a network that bypass the firewall. Some of these routes, such as virtual private networks and wireless access points, are useful resources offered for the convenience of the organization's user population, but which have inherent security risks and can be misconfigured. Other routes, such as network-connected computers with modems and laptops used both in and out of the office, are sometimes unexpected threats and can be difficult to detect and manage. In the following sections, we will examine these routes and why they can be a hazard to security.

Virtual Private Networks (VPN's):

VPN's allow a user on a computer outside of a network to run a client program on their remote machine to establish an encrypted login to a network. The user is authenticated on the network by a VPN server and enjoys all of the same network privileges the user would have if they were logged on locally. Ironically, it is this function of a VPN that both makes it a valuable tool for remote access to a network and creates its primary threat to network security.

Physically, VPN's can be set up several different ways: with the VPN server inside, in parallel with, or outside the firewall, or in some cases with a specialized device that is a combined VPN server/firewall. In most cases, the VPN server is located inside the network, technically behind the firewall. Because the VPN client and server have established an encrypted tunnel between themselves, traffic that passes from one to the other cannot be examined by the firewall as it goes through. This means that packets that would normally be blocked by the firewall because of an undesirable IP or port can pass through into the network unhindered via the VPN server.

The computers being used at home to access a VPN are usually not under the control of the corporate IT administrators, but are instead administered by their individual owners

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

and can be expected to vary widely in their software patch status and virus protection. If the remote computer is compromised, or if a malicious user can gain access to a VPN-authenticated computer, the VPN becomes an unobstructed free ride into the local network for destructive network traffic. This risk is increased if the VPN software allows split tunneling (connecting to the VPN and to a separate non-VPN network site simultaneously) which might allow a hacker to use the Internet to gain control of the remote pc and use it to bypass the firewall into the network.

Wireless Networking:

The security challenges presented by wireless networks are somewhat different from those associated with most other network access methods. In a wireless network, access points are connected to the traditional wired network, and are then configured to accept connections from computers with wireless network cards just as if the computer were plugged in via a physical network cable and wall jack.

The access points and the network cards communicate with each other through radio waves. An access point transmits a signal that broadcasts certain information about the wireless network, and waits for a connection to be requested from a computer with a wireless network card. The radio waves create a network "cloud" around the access point. Depending on the antenna strength, this cloud of network accessibility typically ranges from about 75 to 150 feet from the access point in an office environment.

Unfortunately, the radio waves that make up this network cloud recognize few boundaries aside from signal strength and distance. The walls of most buildings cannot contain this type of network. Often the signal from a wireless access point can be picked up in the next office suite, in the parking lot, or even across the street. This gives would-be attackers the chance to try and connect to a network without having to have a physical connection to the wired network. Since the access points are located inside the firewall, this can create a back door into the network. Hackers sometimes do "war driving", using a laptop with wireless capability and one of several exploit products such as Netstumbler to move about, and gather information on vulnerable wireless networks.

In his article "Exploiting and Protecting 802.11b Wireless Networks", Craig Ellison describes an experiment in war driving that he conducted with some of his associates. They used a laptop with a wireless network card connected to slightly more sensitive but still inexpensive antennae, and Netstumbler to sniff for wireless networks. In the course of a few weeks, they checked various points in four metropolitan areas of the U.S. including Manhattan and the Silicon Valley, looking for wireless networks and checking whether or not the network had Wired Equivalent Privacy (WEP) encryption and other security features, and testing whether or not they were given unchallenged access. They logged a total of 481 access points, of which only 211 had WEP encryption enabled (Ellison, pp.1-9). In a similar experiment during a shared shuttle ride through the downtown area of a major metropolitan city, I once observed a colleague with a laptop and wireless network card pick up an average of about one connection per city block.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Some measures can be taken to try to reduce the chance of unauthorized users connecting to the wireless network, such as enabling built-in WEP with 128-bit encryption or maintaining an access control list. However, many times security considerations are not given enough attention when wireless networks are installed, and access points are frequently set up with default settings, which are very low security. Even worse, wireless networking equipment is becoming so inexpensive and easy to install that unauthorized "rogue" wireless LAN's are popping up wherever enterprising users choose to plug them into the network.

Modems on Network-Connected Computers

Servers and desktop workstations that are attached to a network can also be connected to the outside world via a dialup modem. The dialup modems are often forgotten, ignored, or not adequately protected against intrusion by hackers who connect to the computer via the modem and vulnerable dialup applications. These computers can become the target of a hacking technique called war dialing.

War dialing is the process of using a computer program to automatically call a list of phone numbers and keep a log of those numbers that are answered by potentially exploitable electronic equipment. The exploitable numbers are then called by a hacker who tries to use the dialup connection to break in. Although computers are not the only type of equipment that can be compromised this way, most often the intent of the war dialer is to find computers that can be broken into.

If a computer can be compromised by way of a dialup modem, this gives a hacker a way inside the network without having to go through the firewall. The hacker then has free rein in the computer and can do many things such as set up backdoors to allow later connections by other routes and use the computer to gain access to other computers within the network. Historically, war dialing was one of the first forms of illegal computer access, and still constitutes one of the greatest vulnerabilities in many networks. Because of the great risk, many companies and institutions are now prohibiting the use of dialup modems on computers that are connected to the internal network.

Laptops

Laptop computers that are used both in the office and at home or in the field can be a security threat in a couple of ways. The first of these is the potential for an infection or compromise to occur outside the network and then be brought back in. Laptops may at some times be connected to networks that do not have adequate security measures in place. If the laptop is not configured well or has vulnerable applications running, it may be compromised by a virus, trojan, or other malicious software that would normally not make it past the security used in the home network. When the laptop is brought back and plugged into the network at the users desk, the virus or trojan could activate and infect other computers or open a back door for an intruder to connect to.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Second, a laptop computer that is stolen may have applications that are set up to remember the user's login username and password for remote access to servers, e-mail, VPN, and other services that require authentication within a network. If the laptop can be used to gain access to accounts with stored passwords, the hacker has no need to break in – he has been given a free pass into the network with the unfortunate user's identity linked to anything the hacker tries to do. This risk can also apply to regular desktop workstations with stored passwords if they are stolen out of an office, or if a computer that has been retired from use and sold to an external buyer did not have its hard drive properly sanitized.

Some hackers do not need to break into a network, because they are already inside

According to an article in Business Week Online, experts say that insider hacking represents about 70% of all malicious attacks and causes $1 billion in damages to U.S. businesses each year (Blank, p.1). Hacking and other malicious or illegal activity by persons inside an institution can come in many different forms, including:

- Retaliation by employees who have been terminated or suffered some perceived slight (especially information technology staff, who are more likely to have the necessary skills)
- Intentional or accidental intrusion by employees who are exploring the network or trying out their system
- Deliberate use of computer systems for unauthorized activities such as distributing pirated videos or pornographic images
- After-hours use of unsecured workstations by employees other than the authorized user
- Unauthorized access to accounts with stored passwords, or to accounts that have been left logged in while the user is away

Some of these hazards are difficult to protect against. Predicting when a user is likely to indulge in illegal activities is hard, and sometimes these incidents take place a long time before the perpetrators are caught, if ever. In the case of some of the other types of insider threats, definite steps can be taken to reduce them. Promptly disabling access to accounts for terminated employees, using password protected screen locking and authenticated logins for workstations, not storing passwords on the machine, and auto-disconnect software for idle logins would help to alleviate some of the risk. The other thing that helps guard against insider hacking is alertness of co-workers and managers to any suspicious activity or behavior.

Sometimes all a hacker has to do is ask

Security experts who do risk assessment frequently report that one of the easiest methods of getting unauthorized access to systems is simply to convince users to give them the information they need. Many people tend to be helpful by nature, and some users are uncertain of or at least slightly intimidated by their computer technology and the "gurus" who support it. These facts work together to make it fairly simple for an intruder to trick

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

users into telling what they know, including usernames, passwords, and other bits of vital information that can be used to compromise a computer system or network. The practice of finding ways to con information directly from users is called social engineering.

Social engineering shows up in an infinite variety of interesting forms. Some of the most common stories of social engineering attacks usually involve one of two scenarios: 1) A "technician" who calls asking for a user's login information so he can fix a problem with the user's account, or 2) a "desperate executive" who calls asking for changes to login information or special privileges because he is out of town and in dire straits, with the success of a big project dependent on his ability to gain immediate access to the computer. In social engineering, the success of the attack lies not in the attacker's technical expertise, but in his acting and his ability to convince the user of both his authority and sincerity.

Administrator access to a computer is a powerful thing. Anyone who genuinely has the ability to fix whatever is wrong with user accounts does not need the user's password to get where they need to go. There are extremely few legitimate reasons why an administrator would ask a user to divulge a password, and users should always be very suspicious when they are asked for this type of information. Likewise, the administrators of a computer system must have access policies in place to deal with remote access emergencies and must be very suspicious when this type of request occurs.

One type of social engineering attack that is on the rise currently is in the form of electronic messages that convince the user to sabotage their own system. Recently, there have been reports of AOL Instant Messenger users receiving messages from someone who tells them that their computer is showing signs of being infected with a virus, and that the user should immediately download and run a cleaning utility from a particular web address (CERT, March 19, 2002). In other cases, chain e-mail warning of a virus is distributed, with an attached utility that is supposed to rid the computer of the virus. In either of these cases, if the user complies with the instructions, it usually turns out that the "cleaning utility" was actually the virus program, and the user has infected his own machine

Conclusion

There are many different ways to gain unauthorized access into computers and networks. For many reasons a university is at greater risk for compromises of the network than in many other types of organization. A firewall alone cannot eliminate this risk, but must be used in conjunction with other tools as a first line of defense against attacks. However the most important and most effective part of network defense lies inside the firewall, with system administrator and user awareness of security issues and a concerted, continuous effort by everyone involved to maintain a high standard of security on the part of the overall computer infrastructure that they are responsible for protecting.

References

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

1. Author Unknown. "Drive-by Hacking: Addressing Wireless Security Vulnerabiliteis". Entrust. Date Unknown. URL: http://www.entrust.com/products/vpn/wireless.htm (April 28, 2002).

2. Author Unknown, "Why Choose Integrated VPN/Firewall Solutions over Stand-Alone VPN's". Check Point Software Technologies Ltd. July 2000. URL: http://www.checkpoint.com/products/security/whitepapers/firewall-1_integrated.pdf. (April 20, 2002).

3. Blank, Dennis. "When the Hacker is on the Inside". Business Week Online. December 13, 2000. URL: HTTP://www.businessweek.com:/print/bwdaily/dnflash/dec2000/nf20001213_253.htm?mainwindow (April 20, 2002).

4. Bradner, Scott. "OPINION: A Firewall Can't Do It All". CNN.Com. July 30, 1999. URL: http://www.cnn.com/TECH/computing/9907/30/firewall.ent.idg (April 28, 2002).

5. Carlson, Christopher J. "Tunnel of Secure Transmission". Security Management Online. Date Unknown. URL: http://www.securitymanagement.com/library/000696.html (April 28, 2002).

6. CERT/CC. "CERT/CC Statistics 1988-2002". CERT Coordination Center. April 5, 2002. URL: http://www.cert.org/stats/cert_stats.html (May 5, 2002)

7. CERT/CC. "Social Engineering Attacks via IRC and Instant Messaging". CERT Coordination Center. March 19, 2002. URL: http://www.cert.org/incident_notes/IN-2002-03.html (May 10, 2002).

8. Edwards, Mark Joseph. "Frequently Asked Questions About Firewalls". Windows IT Library. December 1997. URL: http://www.windowsitlibrary.com/Content/121/19/1.html (April 28, 2002).

9. Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks". ExtremeTech. September 4, 2001. URL: http://www.extremetech.com/print_article/0,3428,a=13880,00.asp (May 9, 2002).

10. Goral, Tim. "Network Security: Unwelcome Visitors". University Business. Date Unknown. URL: http://www.universitybusiness.com/story.asp?txtFilename=features/hackers.htm (April 21, 2002).

11. Granger, Sarah. "Social Engineering Fundamentals, Part I: Hacker Tactics". SecurityFocus Online. December 18, 2001. URL: http://online.securityfocus.com/infocus/1527 (April 21, 2002).

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

12. Greene, Tim. "Remote Users – Don't Let Them Become Your VPN's Security Weak Link". NetworkWorldFusion. July 7, 1999. URL: http://www.nwfusion.com/newsletters/vpn/0705vpn2.html (April 5, 2002).

13. Hopper, D. Ian. "University Computers are Prime Targets for Hackers". The Detroit News.Com. June 2, 2001. URL: http://detnews.com/2001/technews/0106/02/technology-231328.htm (April 21, 2002).

14. Internet Software Consortium. "Distribution of Top-Level Domain Names by Host Count: January 2002". Internet Software Consortium. January, 2002. URL: http://www.isc.org/ds/WWW-200201/dist-bynum.html (May 5, 2002).

15. Kingpin. "Wardialing Brief". AtStake, Inc. 2000. URL: http://www.atstake.com/research/reports/wardialing_brief.pdf (April 21, 2002).

16. Mackenzie, Elizabeth. "Perimeter Filtering in a University Setting". SANS Information Security Reading Room. September 11, 2000. URL: http://rr.sans.org/firewall/perimeter_filter.php (April 28, 2002).

17. Marchany, Randy, & Olsen, Florence. "Colloquy Live: The Growing Vulnerability of Campus Networks". The Chronicle of Higher Education. March 13, 2002. URL: http://chronicle.com/colloquylive/2002/03/networks (April 28, 2002).

18. McClure, Stuart, Scambray, Joel, & Kurtz, George. Hacking Exposed, Third Edition. Berkley: Osborne/McGraw-Hill, 2001. 394-412, 434-437, 474-475.

19. Olsen, Florence. "Universities Should Plug 'Top 10' Network-Security Holes, Report Says". The Chronicle of Higher Education. June 22, 2000. URL: http://chronicle.com/free/2000/06/2000062201t.htm (April 28, 2002).

20. Radcliff, Deborah. "University Computers Remain Hacker Havens". Computerworld. February 12, 2001. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO57605,00.html (March 30, 2002).

21. Rezmierski, Virginia E., & St. Clair, Nathaniel. "Final Report NSF-LAMP Project: Identifying Where Technology Logging and Monitoring for Increased Security End and Violations of Personal Privacy and Student Records Begin". American Association of Collegiate Registrars and Admissions Officers. 2001. URL: http://www.aacrao.org/publications/catalog/NSF-LAMP.pdf (April 10, 2002).

22. Rueffer, James, Rooney, David, & Rollenhagen, Erin. "Network Security: Analysis of Firewall Systems". University of Iowa Dept. of Data

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Communications. December 13, 2001. URL: http://kwel.biz.uiowa.edu/datacomm/Group%20H/NTSecurFW.htm. (April 28, 2002).

23. Sample, Char, Nickle, Mike, & Poynter, Ian. "Firewall and IDS Shortcomings". SecurityFocus Online. October, 2000. URL: http://downloads.securityfocus.com/library/072400firewall.pdf (April 21, 2002).

24. Satten, Corey. "NAT Intro and Firewall Limitations". Washington University. Date Unknown. URL: http://staff.washington.edu/corey/fw/nat.html (April 28, 2002).

25. Schenk, Rob, Garcia, Andrew, & Iwanchuk, Russ. "Wireless LAN Deployment and Security Basics". ExtremeTech. August 29, 2001. URL: http://www.extremetech.com/print_article/0,3428,a=13521,00.asp (May 9, 2002).

26. Shunn, Arjuna. "Managed Security: Build It Right the First Time". DevX. Date Unknown. URL: http://www.devx.com/security/articles/WebServices/partI/AS0102-1.asp. (May 11, 2002).

27. Thurman, Mathias. "VPN Security Review Moves To the Front Burner". September 10, 2001. URL: http://www.computerworld.com/cwi/community/story/0,3201,NAV65-663_STO63621,00.html (April 28, 2002).

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: April 27th, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS