Global Information Assurance Certification Paper

Identification and Classification of Measures to Minimise Security Threats.

A small business and new internet users guide

Table of Contents

Table of Contents 2
Introduction 3
The Classifications 4
Hardware Security 5
  Integrated Hardware Security (Now and the Future) 5
  Hardware Firewalls. 5
  Hardware Security Recommendation 7
Software Security 7
  Personal Firewalls (Software Firewalls) 7
  Virus Scanners (Anti Virus Software) 8
  Intrusion Detection Systems (IDS) 9
  Honey Pots 10
  Software Security Recommendations. 10
Operating Systems Inherent Security 11
  Windows XP Internet Connection Firewall (ICF) 11
  Windows XP Remote Assistance 11
  Windows Restore Point Feature 12
  NTFS (user authentication) 12
  NTFS Auditing 13
  OS Security Recommendation 13
Encryption and Authentication 13
  Encrypting File System (EFS) 13
  PGP 14
  AES DES and Other Encryption 14
  Encryption Recommendation 15
User Education 15
  User Dos and Don'ts 16
  Strong Passwords 16
  Software Update Patches 17
  Data Backups 17
  User Education Recommendation 17
Glossary 18
References 23

Introduction

Countermeasures are becoming an essential ingredient in the operation of every business connected to networks and the Internet. In May 2003 AusCert, (Australian Computer Emergency Response Team), released a year long survey called computer crime and security survey. It states “of all attacks on business computers for 2002 the Internet was the worst means for security breaches. With 60% of all reported breaches being Internet related and 22% of business having more than 10 serious attacks within a 12-month period. Interestingly 2003 had already claimed 54% of this trend within only 5 months” (AusCert Australian Computer Emergency Response Team, 2003).

New Computer and internet home users are the testing grounds where hacker’s trial their skills before they attempt exploits upon businesses like those within the Auscert survey. New hackers, in particular script kiddie hackers, can hone their skills against the unsuspected home user, without the fear of a computer specialist being able to track them down and so they increase their black hat learning experiences. “Many well-known security vulnerabilities remain open on home machines and networks and there is less risk to hackers of getting caught” (Lyman 2002). Home computers are becoming more powerful and coupled together with firewalls and antivirus software they provide an extensive testing environment with the safety net of not being traced by corporate experts and thus elude a jail sentence. However because of the total integration of computers into family living and small office home users information stored on home computers is now at a level which could be on par with sensitive company information.

As already mentioned this report is designed for the utilisation of small business helpdesk staff or individual home users. Its aim is to provide the basic understanding of these countermeasure security classifications and to be able to identify some countermeasures with the view of being able to provide well informed recommendations and countermeasure advice for customer's systems.

The Classifications

Rather than choose the usual categories of Confidentiality, Integrity and Authentication this report relies on an easier classification solution. The classification categories are

- Hardware Security
- Software Security
- Operating System Security (predominantly Windows)
- Encryption and Authentication
- User Education

The reason I have used this classification is because help staff are predominately dealing with users the level of knowledge and related questions from the customers will fall directly within one of these categories making it a user-friendly guide to countermeasures.

Hardware Security

Integrated Hardware Security (Now and the Future)

"Microsoft Intel AMD are promising that future components of the PC will itself be security conscious and looking out for you from initial start-up …"(Flynn, 2003, p. 84.) . Already some parts of hardware are already protected from such things as boot sector viruses within the bios programs of newer motherboards; users are unfamiliar and unaware that these security measures are in place. It is suggested that users leave this security option enabled. As technology develops newer integrated security will develop.

Hardware Firewalls.

Firewalls are now a necessity for users and provide the base line protection especially for ADSL or cable internet users whom are always connected to the internet and therefore always vulnerable as opposed to dialup users.(Searchlores Org, 2003; Vicomsoft, 2003)

"There are basically four types of firewalls techniques which hardware firewalls utilise. Packet filters, circuit level gateways, application level gateways and stateful multilayer inspection firewalls" (Vicomsoft, 2003).

Each of these firewalls has its strengths and weaknesses. There are also different hardware options ranging from proxy server firewalls to standalone firewall boxes and multipurpose peripherals, which include firewall technologies. For a home user the only viable option would be a home personal standalone firewall, a multipurpose peripheral or a standalone computer acting as a firewall. This is mainly due to the

costs involved and the knowledge base required in setting up more sophisticated systems. Refer to standalone corporate firewall boxes like Cisco or Watch guard Firebox V200 which is priced at about $60000 (Newman, 2003)

The stands alone computer system firewall has become more viable over the past year or so. The predominant operating system for doing this is the OS (Operating System) Linux, which is freely available via download or on CD within many computer magazines. Linux will run on older type of machines, which give value to old discarded and updated system. The biggest resource consumer for this type of firewall is the users own time and education there are many web sites which can guide the setting up of a Linux box firewall (eg. Ippolito, 2000), and many good books such as Linux Firewalls (Ziegler, 2001).

However the user must learn a new operating system, which may not be viable to the part-time or new computer user's needs nor inclination.

Manufacturers are now providing multipurpose peripherals which incorporate routers, switches and in some cases cable/DSL modems as an all in one peripheral. The beauty of this is that they all utilise firewall technologies and often utilising NAT and VPN technologies.

"NAT is used in the router to prevent hacking into the local area network (LAN). NAT substitutes the "private" IP address of devices located on the LAN side of the router with a new "public" IP address that is visible on the "internet side" of the router. By virtue of this simple implementation, any device, up to 253, located on the

LAN will be hidden, or “masqueraded” from internet hackers trying to get to a specific PC” (Netgear Inc Support Team, 2003).

“Its Important to note that no firewall by itself will provide 100% cover and secure a system from all exploits and vulnerabilities, Firewalls merely serve as a barrier to attack” (Gaylord, 2003). Firewalls only protect your network on there own level they do not guarantee complete security on all levels and should be used in conjunction with other levels and types of security countermeasures.(Cheswick & Bellovin, 1994; Hare & Karanjit, 1996)

Hardware Security Recommendation

For ADSL / CABLE users it is recommended that any motherboard security such as boot sector protection be enabled, also an ADSL Ethernet router/switch with NAT firewall technologies be used in conjunction with their ADSL modem. This is a good standard to utilise and provides the user with the option of connecting more than one computer to the network and internet providing all connections with the same level of security and providing the user secured internet sharing and file share capabilities for up to 253 users for a very acceptable financial outlay of approx $300 AUD.

Software Security

Personal Firewalls (Software Firewalls)

Personal firewalls are software-based firewalls, which in essence do similar actions as their hardware counterparts. They can be used to filter headers; and in some cases content, of all incoming traffic data packets. From here a set of rules or polices established within the program will determine what packets are allowed to proceed to

their destination and what packets will be dropped. This can be configured for traffic from the outside world via an internet connection or within an internal network where trusts are set-up (Pfleeger & Pfleeger, 2003).

Because ADSL users are constantly connected to the net their vulnerability is of course increased (Broughton, 2000), if the computer is not physically switched off then the IP once known to an attacker can constantly be attacked 24 hours a day 7 days a weeks with a personal firewall at least the risk protected at a level that keeps the honest thieves at bay. It is becoming the basic thoughts of many leading experts in the area of Internet security that if you use the Internet, a firewall is an essential tool like antivirus software, the only time you don't need a firewall is when you are not on the internet and not connected to a network. (Lemos, 2001)

Virus Scanners (Anti Virus Software)

One area that all Internet users seem to be aware of is the security breach associated with Viruses. Most users will have a virus protector but that is where the problems begin. However some users will not read the help files to set-up their software to protect them from viruses correctly, they use free downloads which expire and then they do not renew them or else they do not update the virus definition list regularly leaving them vulnerable to new viruses, Trojan worms and other exploits within the wild. Most of these security features are maintained within their antivirus-email program settings but are not activated correctly. All this can create a false sense of security for the user if their antivirus software is not properly maintained.

"Antivirus programs look at the contents of each file, searching for specific patterns that match a profile -called a virus signature – of something known to be harmful. For

each file that matches a signature, the anti-virus program typically provides several options on how to respond, such as removing the offending patterns or destroying the file" (Cert Coordination Centre, 2003a). If these virus definition signature files are not downloaded and updated on the antivirus software regularly the software will not recognise new threats and think they are legitimate files and allow infection to your computer system breaking your computers confidentiality, integrity and authentication..

Users whom do not utilise antivirus software should be directed to connect to an online antivirus scanning source and scan their systems then purchase a new antivirus program and install the latest updates immediately. This will provide a rudimentary protection barrier from malicious code and emails.(Landesman, 2003)

Intrusion Detection Systems (IDS)

Intrusion detection systems (IDS) do not work on the principal of my box is secure and no one is getting in rather they work on the idea, my box is insecure and at some stage it will be compromised. What they do is detect attempted and successful intrusions and alert the user. They also have the ability to log the actions of the perpetrator for tracing purposes as well as noting security weaknesses so improvements can be made to the current security architecture at review times.(Graham, 2001)

One of the most popular software IDS is SNORT from www.snort.org which is available predominantly in a Linux based source however there is also a windows based version available for download. If users are familiar with Linux then IPTables

or Tripwire www.tripwire.com would be excellent IDS choices but Linux is not the predominant operating system so most users will lean towards Microsoft windows OS solutions.

Honey Pots

Honey pots are usually used in conjunction with IDS software and firewall. Their task is to create an illusion of a real system hoping that the hacker gains entry into the Honey pot system. The hacker will search through the system find nothing of interest then leave thinking he has hacked the entire system whilst not being aware that the real valuable system is still invisible to him behind a firewall of some type.

Whilst this is all going on IDS software running on the honey pot system is tracking the path, which the hacker has used and can be used as a good learning tool to educate the user in tracking down hackers. (Stephens, 2000)

However please be aware that there are legal issues related to Honey pots in some parts of the world which if used as computer forensic evidence in entrapping hackers may backfire and be counted as an illegal action.(Poulsen, 2003) I would therefore suggest this only be employed as a deterrent or learning experience.

Software Security Recommendations.

It is recommended that the user purchases one of the bundled software packages from a commercial provider like Norton's Internet Security Utilities, these contain various personal firewalls, antivirus software and email utilities to secure the users system

with little or no maintenance as most updates can be automatically engineered. The added incentive is the low bundled price coupled with the ease of use and deployment as all systems are integrated and tested to work with one another.

Operating Systems Inherent Security

With the notion that components will integrate security directly into the computers hardware also comes the next layer, which all computers require to interact between the computer components and the user, "*the operating system*".

Windows XP Internet Connection Firewall (ICF)

Windows XP actually has its own firewall program built directly into it system. Windows XP has been built with the idea of broadband Internet being the rule rather than the exception and therefore the user has the choice to activate this powerful applet Internet Connection Firewall (ICF) (Honeycutt, 2003).Its is recommended that this option be turned on but not used as a primary firewall rather as a backup to other commercial or hardware firewalls to increase the security n a different layer.

Windows XP Remote Assistance

Users should be made aware of OS exploits, which if not remedied will make their system vulnerable. "Remote Assistance is an XP innovation which is intended to allow another user to take control of your computer to enable problem diagnosis and solution. This is obviously open to misuse, however potentially helpful it may seem at first sight" (UK Security online, 2003). Although this is a great tool for new users to have their computers fixed by online experts the potential for someone to take over

their system and load exploits such as Trojan for later use are indeed a sever security risk. The counter measure is simple and obvious, turn off this feature and only activate it when the online expert is known and trussed and when the system has been fixed then disable this feature again.

Windows Restore Point Feature

Since Windows Millennium Edition windows has contained a great feature, which can be used as a good security countermeasure. One aspect within security is the protection of the integrity of data. A way to ensure the integrity of the Operating system is by using the windows restore point feature. This is accomplished by the following, windows creates periodically creates restore points. When a systems OS integrity has been compromised these points can be accessed and restore the OS prior to the compromised state. Although some data may be lost not all the majority will be saved. Restoration points are made; at the initial installation of the OS, every time new software is installed, periodical and scheduled restore points and the user can also create manual restore points (Benson, 2003).

NTFS (user authentication)

On installation Windows XP has the options of installing onto three types of file systems Fat16, Fat32 and the file system format known as NTFS (new technology file system). NTFS contains various file permissions and policies which can be set-up by the user allocating himself administration rites to determine whom has what level off access to the directories and file s contained within the computer. Access to resources

is granted via a authentication of users via username and password encryption process. (Microsoft, 2003).

NTFS Auditing

When Windows has been installed onto a NTFS partition the OS also has available a valuable security tool for auditing processes, network commands and directory and file access. Similar to IDS the auditing process can track the path of an intruder and log their actions , processes and files accessed.(Scambray, McClure, & Kurtz, 2001)

OS Security Recommendation

It is recommended that all users activate the Windows XP Internet Connection Firewall (ICF) and remote assistance be deactivated.

Encryption and Authentication

There are a number of encryption and authentication programs and processes available for use with some of the better standards being hash programs such as MD5 and encryption processes as DES (data encryption standards) and AES

Encrypting File System (EFS)

Another advantage of Windows installed on NTFS partitions is the Encrypting File System (EFS). You can instruct windows to encrypt a single file as you work on it, when you have completed it or make this a default setting so that all files access on this computer are encrypted. That way if your important data is stolen the thief will not be able to access the data without firstly breaking the encryption protecting the

confidentiality of the data. EFS is based on public key encryption and therefore keys are installed on the system for encryption and decryption purposes. As an added security measure the recovery agent certificate should be exported to a floppy disk and kept in a secure locked area. As the encryption/decryption key process is installation specific, should you need to recover your data then this file will be required to perform the function.(Microsoft, 2003; Schmied, 2002)

PGP

"PGP stands for pretty good privacy, developed in 1991 by Phil Zimmerman originally a free encryption program until it was purchased by Network associates in 1996 and made a commercial program" (Pfleeger & Pfleeger, 2003, p. 478.). Pgp is predominantly used for encrypting e-mail. You have two keys a public and a private key. If someone needs to send you an email they encrypt it with your public key which you may have posted on a website. The only key to decrypt it is the private key which only you have access to on your computer; if the email is intercepted by someone not authorised then they will not be able to open it as they do not have the private key to do so.(Vacca, 1996)

AES DES and Other Encryption

No matter how secure users feel that their system is secure there is always the risk that data will be compromised. Today people are using their personal computers more and more to keep important and personal and highly confidential data, things like finances, internet banking, taxation records and even medical records. All this data may be financially crippling or embarrassing if the wrong people got their valuable data. For this reason encryption tools of any description are better than none but some of the more renown are Data Encryption Standard (DES) and Advanced Encryption

Standard (AES). Des is a 64bit encryption program and AES algorithm converts a block of 128 bits (referred to as plain text) to a 128-bit block of encrypted data. (Allman, 2002, p. 26-30.) By using these types of encryption, the user countermeasures the problem associated with confidentiality, by rendering the stolen data useless to the thief and thus ensuring confidentiality.

Encryption Recommendation

It is recommended that the all email be encrypted via a third party utility such as PGP or one of the utilities already mentioned like Norton's Internet Security Utilities.

User Education

I recently was lucky enough to attend a computer forensic seminar with guest speaker Andy Rosen of ASR Data Inc. USA. Mr Rosen is a renowned expert within the area of computer security and computer forensics. Mr Rosen gave the following analogy on educating users, " I have educated my daughters with the fear of stranger danger ", he said, " I tell them no adult looses a puppy in the park and then comes up to a child asking them to help find that puppy they are there to do you harm, run for your life" , he went on to say " No ISP or security specialist rings up saying we are just checking your account and need your system passwords , if they do they are there to do you harm , run for your life." Users should be educated with and given good points of reference like magazines, newsgroups and websites like www.auscert.com.au which contain valuable education for all internet and computer users and provide latest bugs and security breaches like the Alcatel ADSL modem vulnerability (AusCert, 2001a).

User Dos and Don'ts

Small business help desk staff should always take a little effort when speaking to users about ADSL Internet security issues. What seems obvious to the educated can somewhat appear daunting to the non experienced. One of the best countermeasures within any security related matter is education. Educate users not to open emails from persons they don't know, and don't fall victim of the Social Engineering techniques employed by hackers. (Mitnick & Simon, 2002).

Strong Passwords

Encryption and authentication is a good security start but what is the point when so many people use passwords, which are so easily compromised or guessed. A good countermeasure is to use a strong password. They are called strong because they are harder to crack. Users should be encouraged not to use real dictionary names but rather a series of letters and numbers, which has no real meaning when looked at. Passwords should be a minimum of 6 – 8 characters and numerals, but at the same time be something, which is not easily forgotten by the user. Don't use family or friends names, pet's names or birth dates; these are all too easily broken. A good method is have a phrase eg ***before you run ok*** then change characters which make up the phrase and swap case between words , and swap any numerals for similar letters ***B4uRun0k*** and then if you add the month number to the front or rear of this you have a set of passwords easy to remember which you can change on a regular basis each month and yet easily remember it. Eg for may ***B4uRun0k05*** (AusCert, 2001b)

Software Update Patches

One area where users are particularly uneducated in yet one that is an essential countermeasure is the appliance of security patches to software. This task is now a lot easier and automated with the Windows XP Home and Professional series and should be encouraged. However users should be advised to use the windows restore point prior to applying patches as "In some cases, installing a patch can cause another seemingly unrelated program to break."(Cert Coordination Centre, 2003b)

Data Backups

The last Bastille of security is contained within the process of regularly and properly backing up your data. When integrity of your system has been compromised and there is no way to ensure the data is correct any longer only good solid backups will provide a good security countermeasure for this scenario. Windows NT , 2000 and Windows XP has the built in tape backup option of with daily , incremental , differential and full backups but now with CD writers being so cheap and media being so cheap this is proving a easy and cheap backup medium (Cert Coordination Centre, 2003c).

User Education Recommendation

If users were guided to utilise strong passwords and engage in a good backup strategy and implement the other countermeasures as already recommended, then their system would be at a good security standard and free from the majority of exploits and cyber terrorism.

Glossary

Adware or Ad ware (see also Spyware) – "Software, which downloads and displays ads. This kind of software is often bundled with Free ware available on the web, the software license will usually say that by installing the software you will accept advertising" (Computer Associates, 2003).

Application Gateway (firewall) – "Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation" (Cert Coordination Centre, 2003d).

Circuit-level gateway (firewall) – "Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking" (Cert Coordination Centre, 2003d).

Denial of Service – "An attack on a computer system intended to reduce, or entirely block, the level of service that 'legitimate clients' can receive from that system. These range in scope from network bandwidth wasting and/or swamping through exhausting various machine resources (memory, disk space, thread or process handles, etc) required by the process(es) providing the service. They usually work by exploiting vulnerabilities that eventually crash the service process or the underlying system. Although not commonly associated with viruses, denial of service components are included in some viral payload routines" (Computer Associates, 2003).

Encryption – "Set of mathematically expressed rules for rendering data unintelligible by executing a series of conversions controlled by a key"(National Information Security Systems, 2003).

Firewall – "A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a

combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria." (Cert Coordination Centre, 2003d)

Hoax – "A chain letter that usually spreads a false virus warning" (F-Secure, 2003).

In the Wild – "A term that indicates a virus has been found infecting systems in several organizations around the world. Ideally, the term is reserved for viruses that currently are (or, that have been) in the 'top half' of the WildList. This contrasts the virus with those that have only been reported by antivirus researchers, and which are sometimes referred to as 'zoo viruses' or 'collection viruses'"(Computer Associates, 2003) .

Key Logger – "Any program that records keystrokes is, technically, a key logger. Commonly these log files are e-mailed to the person who planted the logging software, but on public access machines (in cyber-cafes, school and university computer labs, etc) that level of sophistication is not necessary as the 'attacker' can simply access the log file from the compromised machine at a later date, revealing usernames and passwords for accessing other systems and other potentially sensitive information. Although more common in Trojan Horse programs and remote access Trojans, key loggers are sometimes used in the payloads of viruses" (Computer Associates, 2003).

Macro Virus – "Consist of instructions in Word Basic, Visual Basic for Applications and other application macro languages. They often reside in documents or other file types that are traditionally thought of as 'just data', and although that is not critical to

determining whether something is a macro virus or not, it has been a crucial factor in the relative success of certain kinds of macro viruses. Another factor contributing to the success of macro viruses in the popular Microsoft Office application suite and related products (such as Microsoft Project) is that not only can the document files of these applications carry macro code, those macros can automatically run when certain basic events" (Computer Associates, 2003).

Malware – "A common name for all kinds of unwanted software such as Viruses, Worms, Trojans" (F-Secure, 2003).

Multipartite virus - "A virus composed of several parts. Every part of a multipartite virus needs to be cleaned away, to give assurance of non-infection" (F-Secure, 2003).

Nuker – "Now a generic term for several TCP/IP DoS attacks, but originally made (in)famous by the WinNuke DoS attack which crashed Windows machines that had not been suitably patched or firewalled" (Computer Associates, 2003).

Packet Filter (firewall)- "Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing"(Cert Coordination Centre, 2003d).

Packet Sniffer – "Is a program that captures data from information packets as they travel over the network. That data may include user names, passwords, and proprietary information that travels over the network in clear text. With perhaps hundreds or thousands of passwords captured by the sniffer, intruders can launch widespread attacks on systems. Installing a packet sniffer does not necessarily require

privileged access. For most multi-user systems, however, the presence of a packet sniffer implies there has been a root compromise"(Cert Coordination Centre, 2003e).

Proxy Server (firewall) – "Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses"(Cert Coordination Centre, 2003d).

Payload - "If a virus has any damaging routines (other than apparently unintended side-effects or bugs), they are known as payloads or warheads" (Computer Associates, 2003).

Resident

A property of most common computer viruses. A resident virus is one which is normally running and active in the environment in which it is infective. Thus, resident DOS executable infectors load into memory, hook one or more interrupts and remain in memory, waiting for some trigger event such as a file being opened. (Computer Associates, 2003)

Spyware or Spy Ware

A program that gathers information and can be 'silently' installed and run in 'stealth' mode. This kind of software is used to gather information from a user's machine, such as recorded keystrokes (passwords), a list of websites visited by the user, applications installed on the machine, the version of operating system, registry settings, etc. (Computer Associates, 2003)

Sniffers - A program and/or device that monitors data travelling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous

to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favourite weapon in the hacker's arsenal

(Cert Coordination Centre, 2003e)

Spoofing – "Unauthorized use of legitimate Identification and Authentication data, however, it was obtained, to mimic a subject different from the attacker. Impersonating, masquerading, piggybacking, and mimicking are forms of spoofing" (National Information Security Systems, 2003).

Trojan Horse –"A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program" (SANS Institute, 2003).

Virus – "A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting - i.e., inserting a copy of itself into and becoming part of - another program. A virus cannot run by itself; it requires that its host program be run to make the virus active" (SANS Institute, 2003).

Worm – "A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively" (SANS Institute, 2003).

References

Allman, S. (2002). Encryption and security: The advanced encryption standard. *EDN Boston, 47*(24), 26-30.

AusCert, A. C. E. R. T. (2001a). *ADSL Alcatel modems vulnerability*. Retrieved 31st March 2003, 2003, from http://www.auscert.com.au/render.html?it=1257

AusCert, A. C. E. R. T. (2001b, 1st Feb 2001). *Choosing good passwords*. Retrieved 13th May 2003, 2003, from http://www.auscert.org.au/render.html?it=2260&cid=1920

AusCert Australian Computer Emergency Response Team. (2003). *Computer crime and security survey*. (Survey). Brisbaine , Qld: University of Queensland : AusCert.

Benson, R. (2003). *Now if something goes wrong just turn back the clock*. Retrieved 13th May 2003, 2003, from http://www.bcentral.co.uk/technology/Windows/tips/P20970.asp

Broughton, J. (2000, April-May 2000). *Cable modem and DSL security issues and solutions*. Retrieved 20th April 2003, 2003, from http://istpub.berkeley.edu:4201/bcc/Apr_May2000/sec.dsl.html

Cert Coordination Centre. (2003a). *Home Computer Security*. Retrieved 11th April 2003, 2003, from http://www.cert.org/homeusers/HomeComputerSecurity/#8

Cert Coordination Centre. (2003b). *Home computer security :Apply security patches*. Retrieved 11th April 2003, 2003, from http://www.cert.org/homeusers/HomeComputerSecurity/#what

Cert Coordination Centre. (2003c). *Home computer security :Make backups of important files and folders*. Retrieved 11th April 2003, 2003, from http://www.cert.org/homeusers/HomeComputerSecurity/#what

Cert Coordination Centre. (2003d). *Home computer security glossary*. Retrieved 15th May 2003, 2003, from http://www.cert.org/homeusers/HomeComputerSecurity/glossary.html

Cert Coordination Centre. (2003e). *Security of the internet*. Retrieved 15th May 2003, 2003, from http://www.cert.org/encyc_article/tocencyc.html

Cheswick, W. R., & Bellovin, S. M. (1994). *Firewalls and internet security :Repelling the wily hacker*. Reading, Massachusetts: Addison-Wesley Publishing Company.

Computer Associates. (2003). *Virus information centre: Glossary of terms*. Retrieved 4th April 2003, 2003, from http://www3.ca.com/virusinfo/glossary.aspx

Flynn, D. (2003, February 2003). An all-secure PC? *Australian Personal Computer*, 84-85.

F-Secure. (2003). *Corporation virus glossary*. Retrieved 3rd April 2003, 2003, from http://www.f-secure.com/virus-info/glossary.shtml

Gaylord, K. (2003). Free security measures you can take to guard your computers from intruders. *Inside the internet, 10*(5), 5.

Graham, R. (2001). *FAQ:Network intrusion detection systems*. Retrieved 3rd May 2003, 2003, from http://www.robertgraham.com/pubs/network-intrusion-detection.html#1.1

Hare, C., & Karanjit, S. (1996). *Internet firewalls and network security* (2nd ed.). Indianapolis, IN: New Riders Publishing.

Honeycutt, J. (2003, 20th March 2001). *Windows XP prefers broadband*. Retrieved 30th March, 2003, from http://www.microsoft.com/windowsxp/expertzone/columns/honeycutt/june11.asp

Ippolito, G. (2000). *Linux tutorial network gateway*. Retrieved 11th May 2003, 2003, from http://www.yolinux.com/TUTORIALS/LinuxTutorialNetworkGateway.html

Landesman, M. (2003). *Before you use an online scanner*. Retrieved 11th May 2003, 2003, from http://antivirus.about.com/library/reviews/winscan/aabybonsc.htm

Lemos, R. (2001, 28th August 2001). *Home PC users wake up to need for firewalls*. Retrieved 11th May 2003, 2003, from http://news.com.com/2100-1040-272286.html

Lyman , J. (2002). *Home is where the hacker is*. Retrieved 15th May 2003, 2003, from http://www.newsfactor.com/perl/story/16035.html

Microsoft. (2003). *Choose the file system that suits your needs*. Retrieved 25th March 2003, 2003, from http://www.microsoft.com/windowsxp/pro/evaluation/overviews/filesystem.asp

Mitnick, K. D., & Simon, W. L. (2002). *The art of deception: Controlling the Human Element of Security*. Indiapolous, Ind: Wiley and Sons.

National Information Security Systems. (2003). *Infosec glossary*. Ft Meade: National Security Agency.

Netgear Inc Support Team. (2003). *Netgear support team FAQs*. Retrieved 22nd April 2003, 2003, from http://www.expressresponse.com/cgi-bin/progsnp/netgear2/srchjnnp?search_type=vdocument&search_input=N100488.htm&session_id=1052563932.10615.5&level=main&prodfamily=&product=&search_erproduct=&template=viewmoretest%2ehtml&submit=Submit+Query

Newman, D. (2003). Watchgaurd firebox V200 firewall/VPN. *Network World, 20*(17), 69.

Pfleeger, C. P., & Pfleeger, S. L. (2003). *Security in computing* (Third ed.). Upper Saddle River, New Jersey: Prentice Hall.

Poulsen, K. (2003, 16th April 2003). *Use a honeypot, go to prison?* Retrieved 12th May 2003, 2003, from http://www.securityfocus.com/news/4004

SANS Institute. (2003). *SANS glossary of terms used in security and intrusion detection*. Retrieved 15th May 2003, 2003, from http://www.sans.org/resources/glossary.php

Scambray, J., McClure, S., & Kurtz, G. (2001). *Hacking exposed: Network security secrets and solutions* (Second ed.). Berkeley , California 94710: Osborne / McGraw-Hill.

Schmied, W. (2002). *Encrypting file system: Data security comes mainstream*. Retrieved 12th May 2003, 2003, from http://itresources.brainbuzz.com/TechLibrary/GetHtml.asp?ID=987&CatID=230

Searchlores Org. (2003). *Firewall definitions and links*. Retrieved 11th May 2003, 2003, from http://www.searchlores.org/fiatlu/firewalls.html

Stephens, A. (2000, 13th November 2000). *Script Kiddies: - What are they and what are they doing?* Retrieved 12th May 2003, 2003, from http://www.sans.org/rr/hackers/kiddies.php

UK Security online. (2003, 2002). *Windows XP - home user self-defence*. Retrieved 30th March, 2003, from http://www.uksecurityonline.com/husdg/windowsxp.php

Vacca, J. (1996). *Internet Security Secrets*. Foster City, CA 94404: IDG Books Worldwide INC.

Vicomsoft. (2003). *Firewall software white paper*. Retrieved 10th May 2003, 2003, from http://www.firewall-software.com/firewall_faqs/types_of_firewall.html

Ziegler, R. (2001). *Linux firewalls* (2nd Edition ed.). Indianapolous ,Indiana 46290: Que; New Riders.

Last Updated: July 25th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event