Global Information Assurance Certification Paper

A Basic Security Arsenal at No Cost

GSEC Version 1.4b Option 1

Tim Roper

A Basic Security Arsenal at No Cost

Abstract:
All network security individuals and users with always-on internet connections should be familiar with or at least have in their arsenal a few tools in which to perform security assessments and/or improve security measures. This paper is intended for any user who wishes to improve the security on their home computer system or a security administrator wanting to verify that some of the basic security steps have been taken or implemented throughout his/her network. Most of the tools or ideas hereafter will require little or no investment from the organization or individual.

A section on passwords will include creation, replacement schedules and password tests. Education and applications about virus protection will be covered. A section regarding firewalls will include information about address translation, proxy services, perimeters/demilitarized zones and stateful packet inspection. Scanners will include why and when they should be used as well as a few examples. Information regarding analyzers will include topics such as uses, importance and a few examples. The section on logging servers will cover importance and a few examples. Finally, intrusion detection systems will be described and a few solutions and vendors will be listed. After deploying or using some of these security techniques, an organization or individual will feel more comfortable about the security of their system(s) or network at no additional cost. One should never get too comfortable in the world of security, however, because it changes every day.

A Basic Security Arsenal at No Cost

Introduction:
Many organizations deploy minimal security due to monetary and resource restrictions. Many essential security procedures or hardware can be attained and put into production at little or no cost. Passwords, virus protection, firewalls, scanners, analyzers, logging servers and intrusion detection systems will be covered with a few suggestions for use, selection and a little configuration.

Passwords:
Although passwords are usually the last line of defense in a network, they can sometimes be the most important. Passwords are used in almost every aspect of computing such as an administrator's system password, an 'enable' password on a Cisco device and a home user's KaZaA password. One must determine how valuable the information or system being protected is before a password is chosen. As learned in the GIAC Security Essentials Certifications course, a qualitative, quantitative and/or best practices method can be used to determine the value of information or a system. The next step is to select or generate a password, which will be described below. Optional yet just as important, education for end-users and verification of password strength should also be considered.

Many choices exist for passwords; however, dictionary words and personal information should be avoided at all costs because an attacker is able to crack these types of passwords rather quickly. The strength of a password increases when using capital letters, lowercase letters, numerals and special characters. When dictionary words are avoided, an attacker is usually forced to resort to a brute force attack where all combinations of character(s) must be tried (WinGuides).

Example 1: Character Set = [a-z]. Length = 1. Passwords = 26.
Example 2: Character Set = [A-Za-z]. Length = 1. Passwords = 52.
Example 3: Character Set = [A-Za-z0-9]. Length = 1. Passwords = 62.

As one can see from the examples above, the more possible characters in each password's character set, the more diverse a password becomes. Another variable that usually increases the strength of a password is its length.

Example 4: Character Set = [a-z]. Length = 1. Passwords = 26.
Example 5: Character Set = [a-z]. Length = 2. Passwords = 676.
Example 6: Character Set = [a-z]. Length = 3. Passwords = 17,576.

With the addition of password length as a variable as seen above, password combinations also increase. Common password lengths should be avoided which could aid a brute force attack. When combining a diverse character set and a length of more than 1 character, the total possibilities are computed as <number_of_possible_characters> raised to the <length_of_password>.

Example 7: Character Set = [a-z]. Length = 2. Passwords = 26^2 = 676.
Example 8: Character Set = [A-Za-z]. Length = 2. Passwords = 52^2 = 2704.

Example 9: Character Set = [A-Za-z0-9]. Length = 10. Passwords = 62^10 = 839,299,365,868,340,224 (approximately 839 quadrillion).

Strong passwords should be in excess of 8 characters and should include alphanumeric characters at least (Network). Obviously, users will not use such passwords on all types of information or systems, and such passwords are sometimes hard to generate. One way to generate such a password is using a device that generates encrypted strings such as a router or firewall. When the configuration on a Cisco PIX firewall is changed, the crypto checksum also changes, and this crypto checksum may be used as a possible password. Windows Security Guide also provides a random password generator which aids in the process of producing secure passwords (WinGuides).

A password issue that needs to be addressed is a system or software's default password or lack thereof. These default passwords should be changed immediately, and a blank password should be assigned a password. Another important item to consider with passwords is the people that will be using them. A system or security administrator must educate his/her employees not to distribute their password to anyone at anytime and not to write a password on paper or in a computer document. Also warn users against using a network or organizational password for personal uses such as a bank account or another personal interest site. End-user passwords should be changed or users should be required to change passwords at least every 6 months (the sooner the better from a security standpoint) in order to deter attacks (Network). Highly critical passwords should be changed more frequently. A system administrator or home user may want to check the strength of a password by using a password cracking piece of software such as 'lOphtcrack' or 'John the Ripper'. These applications must always be used with permission and normally a dictionary or hybrid attempt is all that is necessary because a brute force attack will eventually determine a password. Passwords might be the last thing between secure information or a secure system and an attacker, but a good password policy is sometimes the best place to start; and with nothing to invest, the cost of this security arsenal initially starts at $0.00.

Virus Protection:

Virus protection will only be covered briefly because most users are already educated about the importance of good virus protection after seeing many virus warnings and reports broadcast on international news stations, radio stations and e-mails. The term 'virus' for the extent of this paper will also include trojans, worms and other types of malicious software or code; one can get a more detailed explanation of these different types of malicious software or code from CERT at http://www.cert.org. With over 57,000 viruses reported today and many hoaxes, virus education and protection of systems is a very important task in securing a system (McAfee).

One important step to take when protecting a system from viruses is education. Educating end-users to be more aware of what actions they take on a computer

is an important task. Users need to be informed not to open any e-mail received from an unknown user. Also they need to realize that attachments are one of the most popular methods for transferring viruses among the computer society. Users should never open any executable attachments with file extensions such as .exe, .bat, .com, .msi and .vbs (to name a few) unless they are expecting these attachments from a reliable source or system administrator. Even when an attachment is received, it does not hurt to have the end-user call the sender and verify the attachment was sent on their behalf. Macros or other embedded code within a document should raise the curiosity of end-users, and once again, they should verify this code with the sender/author, ask for a text-only version of the document and/or disable the macros within the document. Users should also be discouraged from downloading software or other forms of code from the internet such as 3rd party software or screen savers. Another step users can take to stop unintentional infection of his/her computer is to turn off any options that automatically display or open e-mails as they arrive. Users must be aware of all actions they take on a computer and whether these tasks are potentially hazardous to an individual computer, an organization and/or the internet community.

Another step in virus protection which is usually required by organizations and highly recommended to all computer users is the installation of anti-virus software on all computers. Even when an end-user states the machine is standalone, one question to be asked is whether he/she ever uses a floppy disk, compact disc (CD) or other removable media. If so, the computer is also susceptible to viruses. Many anti-virus applications and resources are available on the internet or at stores that sell computers (CERT). One of the most popular anti-virus software suites is Norton AntiVirus from Symantec which can be purchased online or from stores that sell computers. Norton AntiVirus usually can be found for less than $50 per license. Another popular anti-virus software application is VirusScan from McAfee which can also be found for less than $50 per license. Many free anti-virus applications are also available; however, end-users need to research these applications before relying on them (TheFreeSite). After selecting and installing anti-virus software, the end-user or security administrator must keep the virus definitions, files which describe current and former viruses, up to date. Most anti-virus definition updates can be scheduled to run automatically and/or behind the scenes without any user intervention whatsoever. Virus definitions should be checked regularly at least once a week, usually at no cost. Operating system updates should also be updated at the same time in order to fix any vulnerabilities within the operating system itself. These anti-virus applications will usually protect a system from viruses with all of the default settings; an end-user should find installation very simple.

Virus protection is a must on any computer connected to the internet or any standalone computer that uses removable media. With the number of viruses present today, it is next to impossible to educate end-users about all the manifestations of a virus, so having the computer automatically check for viruses

is a must. With a little education and some free anti-virus software such as AVG Free Edition and SurfinGuard, this security arsenal has now reached a running total of $0.00 (TheFreeSite).

Firewalls:
Firewalls are another important security device or application that always-on internet computers and organizations must have. Firewalls have features that protect computers or networks from attacks that originate from the internet or other connected computers or networks. Some features available on a firewall include Network Address Translation (NAT), Port Address Translation (PAT), proxy services, perimeter/DeMilitarized Zone (DMZ) and stateful packet inspection.

First, a few terms must be described. Host is a term used to describe any computer or network device attached to a network. The term internet, for this discussion, will be used to describe any external entity's network. Inside refers to any host or network that is on the protected side of the firewall. Outside or global refers to any host or network on the unprotected side of the firewall such as the internet. An IP address is similar to a person's home address where mail is sent…hosts have an IP address in order for data to be sent from one device to another. Ports can be thought of as places where applications can connect similar to a ship that has access to a port in order to load or unload shipments; FTP uses port 21 to make connections for example. Scanning is a term used to describe the process of one host (the scanner) attempting to make a connection to another host using different ports. Scanning also allows one host to determine if another host is currently operational (responding to a ping packet).

PAT is a many-to-one translation in which many inside hosts can use one global IP address to access the internet. PAT saves money by allowing an organization or small home network to connect to the internet without having to purchase more than one IP address. NAT is a one-to-one translation where each inside host is given a global IP address. Many of the firewall products claim to provide NAT; however, they are truly providing PAT. Since many firewall products refer to this terminology as NAT, NAT will also be used to describe PAT for the remainder of this paper. Generally, the default rules on a firewall will not allow any internet host to connect to an inside host nor distinguish whether an inside host is up and running which protects inside hosts from very common attacks or scans.

Proxy services are offered by some firewall devices to also increase the security of inside hosts. An example with proxy services enabled is a host trying to make a connection to a web server such as Yahoo. When the host attempts to contact Yahoo, the host actually makes a connection with the proxy device/server, and the proxy server makes a connection with Yahoo. The connection to Yahoo is made from the proxy server on behalf of the host which strengthens the security

for the host because additional security measures can be taken on the proxy server in order to 'weed out' potential threats.

Perimeters/DMZ's are generally used in organizations where web or e-mail servers or any other inside host might need to be accessed from the internet. DMZ's are usually implemented using a separate Ethernet interface on the firewall appliance which adds additional cost. The extra interface is on a different network than the inside and the global networks, so security can be set up differently for each network. The DMZ is viewed by the firewall as an external network that should have restricted access to the inside network. For example: all hosts from the inside have access to the DMZ and the internet; all hosts from the DMZ have access to the internet, but they have restricted access to the inside network; and all hosts from the internet have restricted access to the DMZ and even more restricted access to the inside network. The reason for separating an e-mail or web server from an inside network is because these hosts need direct access from the internet which causes more vulnerabilities. If the e-mail or web server gets attacked, the chances of the attack propagating throughout the entire inside network is reduced because the firewall restricts access from the DMZ to the inside network. For the remainder of this document, the outside network will also include the DMZ due to the restrictions placed on each network. Creating a DMZ does enhance the security in cases where outside access to an internal host exists, normally enterprise type networks.

Stateful Packet Inspection (SPI) is a term that many firewall devices use today in order to describe the dynamic protection they can provide. The firewall keeps a table of all current connections/sessions originating from an inside host to an outside host. If a current connection exists in the firewall's tables, then a packet with the same or related properties may return to the inside host from the outside host. For example: an inside host connects to the web server at Microsoft.com using http (web access); the firewall adds the connection entry into its table source: INSIDE_A destination: MICROSOFT.COM protocol: TCP port: 80; when MICROSOFT.COM sends INSIDE_A its web page, the firewall looks in its table to see if this connection was originally established from an inside host. Since the connection was established from INSIDE_A, then the firewall allows the web page data to enter the inside network and go to the inside host. One way a firewall prevents future attacks from MICROSOFT.COM, using the example above, to INSIDE_A on port 80 is to delete the entry in its table after a specified amount of idle time. If INSIDE_A does not keep requesting web pages from MICROSOFT.COM for a period of 5 minutes, for example, then the entry gets deleted, and MICROSOFT.COM no longer has access to INSIDE_A using port 80. SPI is a feature that can be found on many firewalls today, and should be considered a requirement when choosing firewall software or a firewall device.

The range of firewall appliances and applications is vast, so all options must be considered appropriately. Some firewalls with extravagant features are available with high price tags such as Cisco's PIX Firewall or Check Point's Firewall

ranging anywhere from $1000 to $20,000 and up. One firewall device that organizations are looking at in order to cut costs is a computer running the Linux operating system which is a free operating system with a built-in firewall application such as iptables (Linux). The only cost is the computer, which is usually nothing because organizations typically rotate computers out of production. At the end of a computer's organizational life cycle, it is usually discarded or donated to a non-profit entity, but the computer can still be used for a firewall because its specifications will easily exceed the minimum requirements of Linux. For home use, many free personal firewall applications can be found. One simple search on Google for 'free personal software' returns over 300,000 hits with personal firewalls such as Zone Labs' ZoneAlarm, Tiny Software's Firewall and Sygate's Firewall (Google). Since a firewall is very important for an always-on computer or organization, the cost should not matter when implementing this security feature; however, with no cost associated with a recycled computer or free software, the running total of this security arsenal is still $0.00.

Scanners:
Scanners, as described in the firewall section, are tools used to determine if a host is active (replies to an icmp request), what applications a host is running, and/or what vulnerabilities are associated to an open port (Insecure). Scanners can be used maliciously or they can be used to increase a system's security by informing the administrator/owner of potential vulnerabilities. Scanners should always be used with administration's permission and/or the permission of the owner.

One of the most popular and powerful scanners today is Nmap. Nmap is distributed freely from Insecure.org (Insecure). Scanners should normally be used by security professionals in order to reduce the risk of violating organizational, governmental or personal security policies. Nmap will run on most Windows versions, Mac OS X, Solaris, most Linux versions as well as UNIX versions. Not only will Nmap report open/running services, but it can also detect the host's operating system.

For home users, a scanner might not be possible because it would have to be installed on a separate computer in order to scan the primary computer or host. Some organizations will scan a computer as long as they are given permission such as Sygate; however, most of these scans are not as extensive as Nmap (Sygate).

Once the open services and/or vulnerabilities have been determined, a host can be updated to reduce its vulnerabilities and scanned again. If an organization recycles another computer that is about to be discarded and installs Linux and Nmap, the cost of this scanning device is nothing. A personal user can have their home computer scanned from companies such as Sygate at no cost as well.

For the scanner implementation, the updated total of this security implementation is $0.00.

Analyzers:
An analyzer is an application used to monitor data traffic on a network link or a host. Analyzers can be useful at home or on a network in order to troubleshoot connectivity problems or view potential threats. Analyzers can also be used maliciously to learn passwords and other sensitive information from a host or network, so users should attain permission before using an analyzer in an enterprise network. A good analyzer must be able to efficiently and easily filter data traffic. Filtering packets is the process of selecting a few packets that match a given criteria from hundreds or thousands of packets in order to make troubleshooting more efficient.

A very popular and powerful analyzer suite is Sniffer from Network Associates Technology (Sniffer). The Sniffer product comes in many different varieties including but not limited to a distributed version, multiple analyzing hosts reporting back to one centralized analyzer, and a wireless version, which is capable of analyzing packets transmitted across airwaves. Sniffer provides a very user-friendly graphical user interface (GUI) in order to make analyzing data packets easy enough for beginners. The cost of some Sniffer modules, however, can easily be more than $5000.

Another popular and very efficient analyzer application is Ethereal which has many known and anonymous authors (Ethereal). It is distributed as freeware which also adds to very extensive signature files, files used to recognize data packets. Ethereal does not have a GUI that is as user-friendly as Sniffer, but the speed in which Ethereal on a Linux machine can process packets is extraordinary. Ethereal can capture packets and display the output in real-time, or it can display the output after capturing has been completed. This feature allows the host processor to use more resources in order to gather packets, and when capturing has ceased, the processor can display the packets, which also may include name resolution if desired (exchanging IP or MAC addresses with host names). Ethereal is supported on Microsoft Windows (one of the most common operating systems) as well as Linux which keeps the cost down.

And still one more very popular application is Snort. Snort is another application which is freely distributed adding to its extensive support, and it is also covered in the Intrusion Detection System (IDS) section because it is best known for its performance and features as an IDS (Caswell). However, Snort can also be used as a network analyzer in order to capture packets traveling across a network segment. Snort is also supported on Microsoft Windows platforms and Linux versions.

When analyzing a switched network, a port on the switch must be dedicated as a mirror or monitor port in order to capture all of the necessary packets passing

through the switch because switches by nature do not send all packets through every port (other restrictions such as virtual local area networks must be considered as well). Filtering with Ethereal is a little easier to implement than with Snort because it is more modular. Ethereal and Snort perform very efficiently on low-end computers at absolutely no cost. Ethereal has a slight learning curve; however, it also has a very large support base. With all of the features and benefits listed above, Ethereal is a fine choice to implement in an organization or on a home computer when analyzing the data traffic is desired or necessary. This application is free and can also be installed on a standalone machine that has been rotated out of production which keeps the cost of the security arsenal at $0.00.

Logging Servers:
Standalone computers should be used as logging servers in an organization where security is considered critical. Not many home users will find a need for a dedicated logging server because not many devices that generate system log (syslog) messages such as firewall appliances, routers, switches or servers are used in a home environment. Logging applications have been created in order to capture syslog messages and usually store the information in text files based on the priority of the message. Applications exist to create syslog servers on virtually any operating system or device such as Windows, Linux, Solaris, Mac OS, and even a Pocket PC (Adiscon).

Once again, the Linux operating system can be used to deploy a syslog server or even a distributed syslog system where multiple syslog servers report back to one centralized syslog server. A Linux server is a very effective configuration for a syslog server because of its cost (nothing for the operating system and nothing for a recycled computer) and some of the default features of Linux. One of the default features of Linux is a built-in firewall which is very important on a syslog server in order to reduce any possible availability attacks or false messages from an attacker. When the messages are received and stored in files, the files can then be filtered using shell scripts or other applications, and the results can be presented to the user in numerous methods.

Free applications also exist for the Windows operating system (Kiwi). They operate in a similar fashion to those created for Linux. One advantage of using a Windows based syslog server is usually the ease of installation and setup. While the installation and setup is usually easier, customizing the syslog server is a little more difficult. Custom filtering is not as easy as the Linux syslog server, and it is more difficult to sort or filter text files with some of Windows default text tools such as Notepad or WordPad.

An organization must weigh the pros and cons of using a Windows, Linux or even a handheld based syslog server for their own applications and purposes. The cost is still nothing unless licenses are required for the operating system or an extra computer is not available. For many organizations, the benefits of using

Linux far outweigh the benefits of other choices due to the facts that the cost is nothing, Linux will operate very efficiently on older, recycled machines, and the built-in firewall that comes standard with Linux. The cost for this security arsenal can still be kept at $0.00 with the recommendations above.

Intrusion Detection Systems:
A device or application with the ability to inform a security administrator or end-user that an attack is occurring and shut down the attack by itself, Intrusion Detection System (IDS), is the hot topic in security. An IDS can change rules on a firewall or stop an attack dead in its tracks with only a few configuration changes. The problem with an IDS is the initial installation and configuration because a 'happy' medium must be found between too sensitive and not providing enough alerts. If an IDS is set too sensitive, it will pick up many false alerts such as computers requesting information from a Domain Name Server (this is not an attack, simply a computer needing an IP address for a web site or other host). Two types of IDS's exist, a Network based IDS (NIDS) and a Host based IDS (HIDS). The NIDS takes information from a monitor port on a switch or hub and can report back to a centralized IDS for review and action, or it can be placed on a network tap (device used to monitor fiber, copper, etc. without disrupting service). The HIDS specifically runs on one host and generates logging information as well as stopping the attack by closing the service or denying the attacker access. For the remainder of this topic, IDS will refer to a NIDS, but it is not limited to the network solution.

One of the most popular and well-revered IDS solution has become Snort installed on a Linux computer. Because Snort is distributed freely, updates to new attack signatures come quite often and are usually very well described. An end-user also has the ability to customize the Snort application or contact the authors in order to gain support for a new found signature. Snort is very efficient while processing thousands or millions of packets even if it is installed on a low-end computer with a 486 Mhz processor. After processing the packets and determining that an attack has occurred, Snort can perform many actions, such as logging the attacks to a text file, storing the information in a database or sending the information to the syslog facility. After Snort has processed and stored the attack information, many applications exist which will filter, sort and present the data in a user-friendly method such as SNARE and RazorBack (InterSect). Other applications interact with Snort to provide updated web pages in order to view possible intrusion attempts such as SnortSnarf (Hoagland). Snort has a very large support base, and it is growing every day.

Many other devices exist which can provide intrusion detection services; however, they can not be customized in the same manner that Snort can. Some other vendors include, but are not limited to, Cisco, CyberSafe, Internet Security Systems, Network Flight Recorder, Network Ice and Network Security Wizards (Shipley). Most of these vendors' devices are based on the same principles as other IDS's…recognize an attack and notify and/or stop the attack. However,

these devices can be quite expensive with some over $10,000. With cost in mind, Snort installed on a Linux computer with another selected application as a front-end will prove more than enough for any organization. The final cost figure to implement this security arsenal is $0.00.

Conclusion:
Passwords should be selected carefully depending on the security required for the application, and they should be tested regularly. Virus protection should be installed on all computers with few exceptions, and the virus definitions should be kept up to date. Firewalls provide a first line of defense against possible threats, yet they still have their limitations. Scanners should be used to assess possible vulnerabilities on systems in order to give the end-user or administrator an idea of what needs to be fixed. Analyzers are very important tools when it comes to troubleshooting and/or determining what possible threats are occurring at a given time. Logging servers are used to document possible security breaches and should be implemented in most networks in order to review such problems. Intrusion detection systems might be a little difficult to install and configure; however, they are a major factor in becoming proactive in security.

Home users with always-on internet connections and security professionals should have or plan to implement some of the items covered in this paper. Not only are most of these solutions free, but they will help guarantee the security of a computer or network. A user should never become lax about security, so if these security solutions are already in use, one should keep updated with security solutions or implementations by reading or subscribing to security journals and/or newsgroups.

References:

Adiscon GmbH. "Product Features – PocketSyslog." Adiscon GmbH. URL: http://www.pocketsyslog.com/en/Product (4 September 2002).

Caswell, Brian and Roesch, Marty. "Snort.org." Snort.org. 4 September 2002. URL: http://www.snort.org/about.html (4 September 2002).

CERT. "CERT/CC Computer Virus Resources." CERT Coordination Center. 1 March 2002. URL: http://www.cert.org/other_sources/viruses.html (4 September 2002).

Ethereal.com. "The Ethereal Network Analyzer." Ethereal.com. 2 September 2002. URL: http://www.ethereal.com (4 September 2002).

Google. "Google Search: free personal firewall." Google. URL: http://www.google.com/search?hl=en&lr=&ie=ISO-8859-1&q=free+personal+firewall (4 September 2002).

Hoagland, James; McAlerney, Joe and Staniford, Stuart. "SILICON DEFENSE SnortSnarf snort alert browser." Silicon Defense. URL: http://www.silicondefense.com/software/snortsnarf (4 September 2002).

Insecure.org. "Nmap – Free Stealth Port Scanner For Network Exploration…." Insecure.org. 10 August 2002. URL: http://www.insecure.org/nmap (4 September 2002).

InterSect Alliance. "InterSect Alliance – Information Technology Security." InterSect Alliance. URL: http://www.intersectalliance.com/projects (4 September 2002).

Kiwi Enterprises. "Syslog Daemon for Windows, Free Syslog Server, Firewall logging, Kiwi Syslog Daemon." Kiwi Enterprises. 4 September 2002. URL: http://www.kiwisyslog.com (5 September 2002).

Linux Online, Inc.. "The Linux Homepage at Linux Online." Linux Online, Inc.. URL: http://www.linux.org (4 September 2002).

McAfee.com. "McAfee.com – Virus Information Library." McAfee.com Corporation. URL: http://vil.mcafee.com (4 September 2002).

Network Security Center. "NSC: Guidelines on Securing Passwords." The University of Chicago. URL: http://security.uchicago.edu/docs/passwdguide.shtml (3 September 2002).

Shipley, Greg. "Intrusion Detection, Take Two | Page 1 | November 15, 1999." CMP Media LLC. 15 November 1999. URL: http://www.networkcomputing.com/1023/1023f1.html?ls=NCJS_1023bt (5 September 2002).

Sniffer Technologies, Inc.. "Sniffer Technologies – Network Monitoring Tools and Network Management Software." Network Associates Technology, Inc.. URL: http://www.sniffer.com/products/default.asp (4 September 2002).

Sygate Technologies, Inc.. "Security Scan – Sygate Online Services (sos)." Sygate Technologies, Inc.. URL: http://scan.sygatetech.com (4 September 2002).

TheFreeSite.com. "TheFreeSite.com: Free Software: Free Anti-Virus software, freeware to protect your computer…." TheFreeSite.com. URL: http://www.thefreesite.com/Free_Software/Anti_virus_freeware (4 September 2002).

WinGuides.com. "Windows Security Guide – Random Password Generator." WinGuides.com. 13 September 2001. URL: http://www.winguides.com/security/password.php?guide=registry (3 September 2002).

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
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
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
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
SANS Cyber Defence Singapore 2017	Singapore, Singapore	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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event