Impact of Network Security Vulnerabilities Management

2016 spring ICTN6865

Due 4/5/2016

Robert Underwood

3/28/2016

Abstract

Managing cyber security vulnerabilities in a large network is a big challenge where the implementation of cyber security techniques can create network slowdowns that negatively impact customers and the delivery of service. The challenge of managing cyber security for a large network is monumental because of the complexity of cyber security associated with multifaceted and interrelated systems to which data, voice, and video may be imbedded. Since all computers in the network are interconnected and their cyber security is independent the total effort required for the entire network the effort to manage cyber security becomes multiplied by a colossal scale.

Managing and mitigating cyber vulnerabilities within a network require device scanning to identify the network vulnerabilities, data encryption techniques, vulnerability mitigation techniques, authentication methods, virus protection, and intrusion detection techniques all to which take up valuable network bandwidth.

Managing the vulnerability threat also needs to consider the types of network traffic that is required to maintain the network operation and the effects of network manager's interactions with network users.

This paper will examine the techniques implemented to reduce the impact to the network and network customers by mitigating vulnerabilities effectively and efficiently through technics implemented by industry such as those seen in network equipment life cycle management and by examining some of the issues Lucent Technologies faced as they tackled these issues.

Costs in Lost Services

Security methods and their applications hog our network resources, why do we need security and why do they need so much of our time and resources? Network security prevents down time and according to a survey conducted by Computer Associates (CA) Technologies industry lost approximately $25.6 billion in revenue due to information technology (IT) downtime (CA Technologies, N.D.). A note about the survey, it was conducted over a cross section of 200 small, medium, and large businesses in 2010. Within the survey CA Technologies does not list the reasons for the outages so we don't know how much network downtime is related specifically to security. According to a TechTarget article downtime related to IT security issues are estimated at around $30 million a year (Hickey, 2007).

Network Related Security Issues

There seems to be about 95% of all network downtime contributed to operational security issues with 55% related to hardware failures; 22% related to human error; and 18% related to software failures. According to Quorum's disaster Recovery Report in 2013 (Quorum, N.D.) about 55% of IT downtime was caused by hardware failures.

Hardware Failure

Can we prevent hardware failures that caused 55% of IT failures? If we approach the issues with preventive maintenance we can prevent many hardware failures by replacing hardware before the end-of-life of the equipment life cycle. In addition if we monitor the health of a device through manufacture given performance metrics we can predict early failure which fall under IT asset management which is a subdivision of IT security management (Calder, 2005). Replacing IT equipment such as network equipment, switches, routers, and network

computers can cause serious hardships on device traffic causing issues with network users but if performed correctly a plan can limit impact to an organization as well as customers. A much more serious problem would be the loss of functionality of equipment due to a failure, reaction to emergencies can be much more costly. The process of monitoring network equipment can also present can increase traffic and reduce network response if not planned and managed properly, which we will examine later in this paper.

Human Error

The next highest IT downtime contributor was with the human error factor which was ranked second in the impact report by (Quorum, N.D.)' and was reported as 22% of IT downtime. Calder's book about Information Security confirms the importance of mitigating the threats to computer systems which are composed of incompetent users (Calder, 2005, p. 2). It would seem that there is no impact to the network traffic regarding the mitigation of user incompetents but if we consider the type of training used as the mitigation effort such as Computer Based Training (CBT), designed with video streaming and multi-media in most cases, the impact could be significant.

Software Issues

Quorum lists 18% of downtime as attributed to software issue such as operating system (OS) and application failures which could be mitigated through patching and updates which are another function that falls under the domain of IT security. Although software issues only attribute to 18% of our total down time it is one of the most network traffic intensive computer system security processes on the network because the process are related to audits, pushing software patches and updates across the network to computer and network devices.

Impact of Security

Overall the greatest risk to network operations is the loss of service and there are certain types of vulnerabilities that are directly related to this type of event such as a Denial of Service attack (DoS) which if mitigated by a reverse proxy (Weiss, 20122) offers improvements to our customer network traffic. The improvements are seen through the reverse proxy in which the type of traffic entering the network from another domain is controlled. This is possible through the implementation of a reverse proxy and the types of configurations that the reverse proxy allows (Amna Hashim Mohauued, 2014). On the other side of completely killing access to networks to stop a DoS attack are the different levels of traffic that increase related to the traffic produced by security methods such as monitoring, auditing, patching, updating, authentication, intrusion detection, and virus protection.

Network Security and Network Performance

Network traffic is increased through security mitigation processes such as monitoring, patching, updating, authentication, intrusion detection, auditing, and virus protection. Each mitigation process impacts traffic for a different reason at the same or different times which is dependent on when the security policy is applied. As an example of poor planning an organization IT administrators could pushing virus scans; network sans; computer vulnerability scans; network devise audit reports; computer patches; and computer updates all the same time to the entire network at the moment the organization doors open and everyone begins work by starting their computers and opening their applications. The processes listed above can cause some serious network lag issues in just one even occurrence, but all if all the events occur at the same time the when entire organization jumps onto the network then serious lag is not a well

enough defined word to describe the event. The point is planning security mitigation events is an important concern and dependent on current network traffic peek user and customer traffic times.

Network Size Traffic Impact

The size of a network has a critical effect on traffic. Large networks such as Lucent Technologies are composed of more than 100,000 computers (Chang, 1999). In general the greater the size of your network the harder the traffic will be to control and the greater the impact will be to network traffic. The question about size boils down to how we identify and mitigate vulnerabilities on such a large network in the most effective way.

Vulnerability Impact

Vulnerabilities can be defined as the weaknesses within our network. In order to identify the number total potential vulnerabilities the network may have is defined by the number of weaknesses found in each computer or devise and is a multiple of each system to which the vulnerability effects which a gives potential magnitude to the number of systems it may impact, this potential number is then multiplied by the number of systems. As an example Lucent Technologies identified 1,250 different vulnerabilities in there systems which were composed of computers and network devices which equals a potential magnitude of 125,000,000 (1,250 X 100,000) vulnerabilities in their network (Chang, 1999).

With a number as large as 125,000,000 potential vulnerabilities the challenge is to find the vulnerabilities before the vulnerability becomes an incident. We assume an incident in this case is a vulnerability that has been exploited or is exploiting our system and is actively performing some nefarious action on our network or computers, such as with worms, viruses, or hackers. As we have identified the problem with identifying vulnerabilities on large networks

can be overwhelming so where do we start? Lucent Technologies took an approach of vulnerability impact prioritization against zone control. This technique attempts to identify the highest priority vulnerability which is defined by the vulnerability with the highest negative impact. Once the vulnerability priority has been set then a segment of the network in a zone and its sub-zones is identified to which the priority vulnerability is searched. Lucent Technology's methods show that they were able to establish a hit rate with confidence level of 95% in identifying network vulnerabilities (Chang, 1999). This method applied by Lucent Technology was able to reduce the overall impact to the network by restricting vulnerability identification to defined zones.

Vulnerability Tools

There are several types of tools currently used on the todays networks that help identify vulnerabilities some of the industry most popular tools are listed in Table 1, data provided by (Sectools).

Table 1

Vulnerability Tools

Product Name	Systems	Vendor
Nessus	Windows, Linux	Tenable
OpenVAS	Windows, Linux	OpenVAS
Core Impact	Windows, Linux	Core Security
Nexpose	Windows, Linux	Rapid 7
GFI LanGuard	Windows	GFI
QualysGuard	Windows, Linux	Qualys

Managing the way the tool is used is important as was identified in the method implemented by Lucent Technology and shown in the previous section. Once we have identified the vulnerabilities the next step is mitigation, so what is the plan?

Mitigation Impact

The problem with mitigating 125,000,000 potential vulnerabilities involves more that the methods used to identify them. In the mitigation phase planning our first priority, as seen in the Lucent Technology method of vulnerability identification, we would need to establish a migration critical path by establishing a priority metric for the most critical vulnerabilities, those vulnerabilities that have the potential to have the highest negative impact to the network. Once the mitigation priority critical path has been established a network zone should be establish, which should also be identified by priority and include those zones that exist within the network that maintain critical operational functionality, such as network control planes, or data centers.

The techniques involved with mitigation increase network traffic to which the degree of increase is related to the type of mitigation as in a light or heavy impact to network traffic. A light impact mitigation could be a simple update to computer policy such as those policies pushed by Active Directory (AD) that change the base settings of a computer's operating system, an example would be a change to computer policy that forces the web browser to deny pop-ups. A heavy impact mitigation could be a software update where sizable data would need to be sent from a source server to other computers or devices on the network. Some updates many be several hundred megabytes (MB) in size and if these updates were put on the Lucent Technology's network of over 100,000 computers the total update requirement would be over 20,000,000 MB (200 MB X 100,000 Lucent computers) or 200,000 gigabytes (GB), this magnitude of impact would need to be planned and need to occur at the time of lowest usage on the network to avoid interfering with high volume network usage.

Authentication Impact

The impact of authentication starts at the access point when system logs onto the network and the user logs onto the computer. The process of authentication usually is to establish and validate the identity of a computer and the person operating the computer to which the access is requested to the network. A network can be configured through several methods that manage an access request from a computer such as IP filtering, MAC filtering, Network Access Control (NAC), or computer object membership controls. A user's requests to the network are usually processed by methods of computer access control where data about the user is stored such as in Windows Active Directory where a database of users are populated and user information is stored including a unique password established by the user. Once a connection is established by a user their continued authentication is not required a user only needs to authenticate once every time the user logs on. Some systems will log the user off for a certain time of inactivity as a matter of security policy which means you could be logging onto your system many times a day if you walk away from your computer often.

The basic authentication process does not take many network resources or create excessive traffic without encryption but almost all authentication methods include some type of encryption. The impact to traffic related to encryption can be significant because encryption uses a cryptographic algorithm which encodes the contents of a message in a way to prevent anyone, other than the authorized decoder, from reading the message, this encoded message is called cipher text. One method of key encryption uses the process of encryption with a key to encrypt the message before it is delivered to its destination. Once the cipher text reaches the destination a copy of the original key is used to decode the message. Since the encryption work is done by the originator and the receiver it would appear that there is not additional load to the network but the

mechanics of encryption add additional bocks to the message and those blocks can become large. A standard Advanced Encryption Standard (AES) encryption method adds bocks in sizes from 128, 192, 256 bits keys (Krishnamurthy, 2006) with the total size of the encrypted block being as large as 3 MB. This number does not seem large in itself but on the Lucent network with over 100,000 computers that is 300,000 MB (3 MB X 100,000 Lucent computers) going to authentication servers.

The biggest issue with authentication comes from the process of decryption where the cipher text is decrypted. The reason for this additional overhead is that the traffic that the authentication server has is a one to many relationship. meaning that all traffic in a designated are will be converged by the network to the authentication server. In general as an example a domain controller, a network user authentication device, reaches its upper capacity around 10,000 users (Microsoft, N.D.). The user numbers that exceed 10,000 users, in poorly designed networks, could cause authentication lag or network lag in general. Additionally if there are other security activities occurring on the network such as patches or updates which would additionally tax the domain controller there could be a loss of service causing users to be unable to authenticate or network lag.

Virus Protection

The impact from virus protection has two components scanning and updates. Virus protection, also known as antivirus, scanning is usually not a traffic issue because of the mechanics involved with virus protection software. Normally on a network virus protect is an application that is pushed out to client computers or installed on a computer during the initial setup of a user computer. When the virus protection application is activated it runs a scan on the computer it is hosted on. The user may experience a performance hit during scanning but the

issue is remote to the user and not caused by the network since the virus protection application usually runs remotely on the host machine.

Virus protection and network devices are a tricky issue since most network devices are very limited in computing power and functional governed, limited to managing network traffic, but there are those devices which manage certain aspects of the network that require server functionality and require a current operating system (OS) to complete their network operational purpose, these types of devices will require virus protection and the scheduling of scanning will need to be managed as not to interfere with network traffic. For those devices mentioned of little processing power like routers and switches do not have the capacity to load a host virus protection program, unless specifically designed to support it, so these devices require another technique or method of inspections to determine if they are compromised with malware.

Malware the all-encompassing definition of our generalization of viruses because the clever attacks from our enemies come in many ways and present specific attack vectors we need to encompass the meanings within a single word, malware. This matters because our virus protection is actually malware protection by definition, confused, let's clarify. The word virus has two meanings for instance one meaning used in the phrase Virus Protection which means malware this is because the meaning of the word malware includes Trojan horse, worms, adware, spyware, ransomware, scareware, and other malicious programs (Techtarget, N.D.). The other meaning of virus is specific to how a malicious program works and the way it works is that a hidden or innocent looking program delivers a payload to a system, as in a Trojan horse. So as we see malware covers the gambit of malicious programs and a virus is just a specific type of malware.

Finding malware in our network devices may not be that hard. Since most network devices are limited in space, processor, data storage, and function. With these devices such as router and switches the manufactures make sure they optimize every bit, byte, and feature for performance so there is little to no chance a virus will have room to reside in a device like a router or a switch but that is not to say cannot be hijacked. Hijacking is taking control of the device and reprograming it to anything else other than what you want it to do, redirect traffic, block traffic, interfere with traffic, or add new traffic routs. A major sign that our network devices have been compromised is network performance, to be more specific for malware we need to discuss specific tools. To detect situations of malware or hijacking monitoring can be used like a network tool such as snort (Routing & Switching (CCNA) Discussion, 2012).

NIDS

Snort is a Network Intrusion Detection System (NIDS) that uses the methods discussed about viruses with virus definition files to detect malware on our network specifically moving from one device to another. Snort scans packets sent over the network by the focus on transfer points, ports. Aa type of traffic sniffer, these scans are measured against different network malware definitions of the NIDS to determine if network traffic contains malware such as buffer overflows, denial of service, Stealth Port, or Small Message Block (SMB) Probes to mention a few (TechTarget, N.D.a). NIDS can have significant impact to our network if not managed properly along with other packet analyzing methods which we will discuss later in this paper as we bring all the traffic analyzers together under one heading of traffic monitoring.

The second component of virus protection is updates. Updates come in a few flavors such as client updates and definition updates. When we talk about client updates we are talking about the changes made by the vendor or manufacture of the virus protection application that need to

be installed on the network computers. When we talk about definition updates we are speaking to the process of distributing virus definitions. The virus definitions are the footprints that our virus protection client applications use to scan on our computers for malware. These definitions are designed by our virus protection application developers. Let's take a moment and look at how virus definitions work with our virus protects because as you will see intrusion detection system (IDS) uses the same process. Unlike virus protection scanning which has little consequence to network performance, due to the fact it runs locally or can be schedule to run against network devices at low traffic times, IDS can have significant impact because can active on the network and scanning all network traffic as it passes through.

Once an update for the virus protection is available for the network customer to distribute across the network some planning will need to be made to prevent issues such as a network traffic congestion or computer failures due to compatibility issue. Some products such as Symantec Norton antivirus products provide an antivirus server which can deploy and monitor all the client computers that the Symantec Norton antivirus products have been installed on (Symantec, N.D.).

This is type application offers a central management method which allows the monitoring and scheduling of updates from one location. There are others vendors who can provide a similar product but other options involve system administrators who will need to use software distribution products or manually push the antivirus definition updates to each individual server. Regardless of the method there is an increase in traffic on the network that will need to be planned for. Currently the size of the virus protection definition files from McAfee antivirus (McAfee, N.D.) is over 130 MB which would be substantial traffic if Lucent were to push updates across the network as in 13,000,000 MB (130 MB * 100,000 Lucent computers).

Blame it On the Network

Impact on network performance from blame can have a large impact because of the time it takes to resolve non-network related issues. It is important for network stake holders, i.e., engineers, administrators, or anyone responsible for design and care of the network, to be positive when responding to the blame game. Most users and even IT people blame slow computer application response on the network as reported from SolarWinds lead geek Adaton (Adaton, 2015). As network professionals our teams need to be diligent and listen and provide positive feedback to our customers to promote a better working environment (Batista, 2013). Often our customers, end users of the network, have very little awareness of what is causing them hardship, technology as we all know can be very perplexing, if you have not been perplexed by technology then you have never used it.

Educating our network users needs to be a positive re-assuring event so we do not perpetuate the anger felt for loss of service which is not an easy task since we as network managres are generally composed of technically skilled individuals are not always the best social communicators, as stated on the Science Forum of Natural Sciences and Behavior and Psychology (Science Forum, N.D.). The forum indicates there is a correlation between highly functioning technically skilled people and their ability to communicate effectively socially.

Technology and network professionals need to take time and evaluate, study, and change the way we communicate with our customer to give the best possible outcome for the benefit of the organizations to which we work. Batistan mentions a few benefits of positive feedback such as safety and trust which establishes a feedback mechanism of truth and candidness without emotional bias.

Impact to network performance through blame can have a large impact because it takes our focus away from current network tasks and causes us as network managers to chase ghosts, phantoms, and boogeymen so when these situations occur it is important to educate network users in a positive and constructive manner as to help limit unnecessary blame. In many cases help desk personal are the first line of defense and can significantly reduce the service request calls to network personnel but again when responding and interacting with a customer the communication skills are important to a positive experience. There are situations that occur that are definitely network related so how do we determine where the issues exists.

Root Cause Analysis

Root cause analysis is the process of determining the underling failure that is causing the issues or symptoms. Issues can be directly related to the root cause or they may be symptoms created by the root cause, as an example a doctor will ask a patient what their symptoms are so the doctor can determine what the root cause of their fever is. Symptoms are import because they are indicators to the root cause but some of these issues may need immediate attention before you can begin an investigation to find the root problem, as an example someone may be bleeding severely so your first action is to stop the bleeding (Harvard Heath, 2005). Symptoms can be documented and stored in a knowledge base as with the Information Technology Information Library (ITIL) methodology which stresses the uses a known error database (Morris, 2012) for troubleshooters to utilize in diagnosis. The advantage of using a knowledge base is that symptoms common to a specific organization can help identify issues and accelerate the resolution if not identify the root cause immediately (Morris, 2012).

They key to successful troubleshooting is in identifying the problem for it may not always be obvious what the scope of the problem is so identifying the scope of the problem is

essential. Six Sigma, a method that strives to improve the quality of service (Six Sigma, N.D.), defines the first step in root cause analysis as defining and measuring the problem. In regard to Lucent's issue as stated earlier in this paper there was a problem in identifying the network vulnerabilities do to the oversized network and the number of vulnerabilities being searched for. Lucent used a root cause methodology then scoped the problem with analyzed traffic and user impact which lead to their overall solution (Chang, 1999).

Traffic Monitoring

In this section we will discuss network performance monitoring which consists of traffic analyzers. Traffic analyzers serve two main functions, monitoring traffic flow and security IDS. Traffic analyzers that monitor network traffic flow are part of performance monitoring. Performance monitoring uses traffic analysis to determine where the network traffic by measuring response time, device up-time, and availability. Understanding the traffic flow can better help network managers to understand what the network overall traffic topology looks like so that zones of convergence can be reviewed and protocols can be assessed.

The type of protocols that manage network traffic are called network routing protocols and there are many types of protocols designed to meet certain needs of a network. Most Internet communications protocols fall under Unicast (Microsoft, N.D.a) as where Multicast is used less often.

Unicast is a one to one communicator as where the Multicast method is a one to many communicator. The advantage of Multicast is found in data streaming where several sites are connecting to one source of information like a data stream (Microsoft, N.D.a). There are currently several network protocols utilized on the market CISCO lists the current basic routing protocols as seen below.

Boarder Gateway Protocol (BGB)

BGB routs traffic between autonomous systems which are grouped together by common routing policies. BGB is mainly used in large network deployments where more than one Interior Gateway Protocol (IGP) is used such as with those organizations that connect between Internet Service Provider (ISPs). "BGP is a very robust and scalable routing protocol, as evidenced by the fact that it is the routing protocol employed on the Internet. To achieve scalability at this level, BGP uses many route parameters, called attributes, to define routing policies and maintain a stable routing environment. BGP neighbors exchange full routing information when the TCP connection between neighbors is first established. When changes to the routing table are detected, the BGP routers send to their neighbors only those routes that have changed. BGP routers do not send periodic routing updates, and BGP routing updates advertise only the optimal path to a destination network." (CISCO, N.D.a).

Multiprotocol BGP

MP-BGP adds function to BGP by providing multicast routing that can be utilized with unicast routing. "MP-BGP is an enhanced BGP that carries IP multicast routes. BGP carries two sets of routes, one set for unicast routing and one set for multicast routing. The routes associated with multicast routing are used by the Protocol Independent Multicast (PIM) to build data distribution trees." (CISCO, N.D.a).

Open Shortest Path First (SSPF)

OSPF is a routing protocol for IP networks which routes network traffic to its destination by a shortest path algorithm. "OSPF is a link-state routing protocol that calls for the sending of link-state advertisements (LSAs) to all other routers within the same hierarchical area. Information on attached interfaces, metrics used, and other variables are included in OSPF LSAs.

As OSPF routers accumulate link-state information, they use the SPF algorithm to calculate the shortest path to each node." (CISCO, N.D.a).

Enhanced Interior Gateway Routing Protocol (EIGRP)

EIGRP is a CISCO proprietary routing protocol and is a distance-vector protocol. The algorithm is designed to minimize the routing instability that occurs through topology changes. "Most of the routing optimizations are based on the Diffusing Update Algorithm (DUAL), which guarantees loop-free operation and provides fast router convergence." (CISCO, N.D.a).

Routing Information Protocol (RIP)

RIP is widely used and is a distance routing protocol that uses an algorithm of hop counts to adjust routing traffic. RIP prevents loops by implementing a limit on the number of hops allowed from a source or destination path. RIP "also implements split horizon, route poisoning and hold-down mechanisms to prevent incorrect routing information from being propagated." (CISCO, N.D.a).

Intermediate System to System (IS-IS)

IS-IS is a link state routing protocol which operates by flooding the network topology throughout the network of routers which allows each router to build its own picture of the networks topology. IS-IS uses an algorithm of computing the best path, Diikstra's algorithm. IS-IS was intended to be used on one domain of networks (CISCO, N.D.a).

Routing Impact

Each routing protocol has its own set of pros and cons and it cannot generically be said that one is not better than the other. Determining which protocol is best for the network should be determined by the network use and what protocol will perform better than the other.

Monitoring can give us traffic information that can validate or suggest a change but we also need to consider the impact on security. The impact of monitoring can interfere with network traffic if we pole devices too frequently which can cause network lag or if the device is already at capacity and we stack on additional request we can causing network lag, in the case just mentioned we definitely want to know there is an issue.

Performance monitoring is something the needs to be planned such that inventory scans, traffic scans, discovery scans, are done within network windows of lightest loads as to prevent network interruptions.

IDS Impact

IDS scans can cause some serious network lag due to the nature of the packet inspection. Fortunately not all IDS are so intrusive such as those passive IDS (Omni Secu, N.D.). Non-intrusive IDS systems passively capture network traffic and perform analysis on the data comparing their captured data against the intrusion detection definitions provided by their vendor, such as with Snort mentioned earlier. If we use a passive IDS we can expose our network to a possible attack as with malware or being hijack. This is due to the way passive IDS works which is reactionary after the traffic has passed which leads to a delay in notification. As opposed to active IDS where it can alert the system to the presence of and attacker as soon as the attack happens and with certain settings IDS alarms can trigger a network response such as closing firewalls or rerouting traffic (CISCO, N.D.b). With active IDS comes at a higher cost, this cost is to network traffic because active IDS captures and analyzes in real time with no delay in analysis.

Conclusion

We just began to scratch the surface of all the things that compose network traffic that affect our ability to secure the network and keep the network performing optimally. Hopefully there is a better understanding about of the important issues involved with identifying and mitigating network vulnerabilities. In addition we took a look at how communications between users and network managers affected our performance which in turn impacted the network performance. Overall with careful planning and consideration the types of impacts reviewed shows ways to reduce impact to our networks so our teams can better design and operate networks and provide a reliable and well performing infrastructure for business operations.

References

Adaton, L. (2015, February 14). *'IT MUST BE THE NETWORK': HOW TO AVOID THE BLAME GAME AND REDUCE DOWNTIME IN AN APP-CENTRIC IT ENVIRONMENT*. Retrieved from Continutiy Central Archive: http://www.continuitycentral.com/feature1279.html

Amna Hashim Mohauued, A. (2014). Proxy Impact on Network Performance. *International Journal of Innovateive Research inscience, Engineering and Technology*, 17107 - 17113.

Batista, E. (2013, December 24). *Building a Feedback-Rich Culture*. Retrieved from Harvard Business Review: https://hbr.org/2013/12/building-a-feedback-rich-culture/

CA Technologies. (N.D.). *CA Technologies Survey Reveals IT Systems Failures Cost Businesses 127 Million Lost Person-Hours*. Retrieved from CA Technologies: http://www.ca.com/us/news/press-releases/na/2011/ca-technologies-survey-reveals-it-systems-failures-cost-businesses-127-million-lost-person.aspx

Calder, A. (2005). A business guide to information security : how to protect your company's IT assets, reduce risks and understand the law / Alan Calder. London, Sterling, VA.

Chang, E. S. (1999). Managing cyber security vulnerabilities in large networks . *Bell Labs Technical Journal*, 252-272.

CISCO. (N.D.a). *Routing Protocols*. Retrieved from CISCO: http://www.cisco.com/c/en/us/td/docs/net_mgmt/active_network_abstraction/3-7/reference/guide/ANARefGuide37/routpro.html

CISCO. (N.D.b). *Configuring Cisco IOS Firewall Intrusion Detection System*. Retrieved from CISCO: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfids.html

Harvard Heath. (2005, September 1st). *Emergencies and First Aid — Direct Pressure to Stop Bleeding*. Retrieved from Harvard Heath Publications: http://www.health.harvard.edu/family_health_guide/emergencies-and-first-aid-direct-pressure-to-stop-bleeding

Hickey, A. R. (2007, March 14th). *Network downtime from security attacks proves costly*. Retrieved from TechTarget: http://searchnetworking.techtarget.com/news/1247369/Network-downtime-from-security-attacks-proves-costly

Krishnamurthy, A. (2006). *Performance impact of encryption algorithms on Kerberos network authentication protocol.* Oklahoma City: ProQuest Dissertations Publishing.

McAfee. (N.D.). *Security Updates*. Retrieved from McAfee: http://www.mcafee.com/apps/downloads/security-updates/security-updates.aspx?region=us

Microsoft. (N.D.). *Capacity Planning for Active Directory Domain Services*. Retrieved from Microsoft Technet: http://social.technet.microsoft.com/wiki/contents/articles/14355.capacity-planning-for-active-directory-domain-services.aspx#Baseline_Requirements_for_Capacity_Planning_Guidance

Microsoft. (N.D.a). *Differences Between Multicast and Unicast*. Retrieved from Microsoft: https://support.microsoft.com/en-us/kb/291786

Morris, S. (2012, April 16th). *7 Benefits of Using a Known Error Database (KEDB)*. Retrieved from The ITSM Review: http://www.theitsmreview.com/2012/04/7-benefits-of-using-a-kedb/

Omni Secu. (N.D.). *Types of Intrusion Detection Systems (IDS)*. Retrieved from Omni Secu: http://www.omnisecu.com/security/infrastructure-and-email-security/types-of-intrusion-detection-systems.php

Quorum. (N.D.). *Quorum Disaster Recovery Report Exposes Top Causes of Downtime*. Retrieved from Quorum: https://quorum.net/news-events/press-releases/quorum-disaster-recovery-report-exposes-top-causes-of-downtime/

Routing & Switching (CCNA) Discussion. (2012, Februrary 14th). *How to know if there is a virus in my switch , router and my network ?* Retrieved from CISCO: https://learningnetwork.cisco.com/thread/39762

Science Forum. (N.D.). *Intellectuals and Social retardation*. Retrieved from Science Forum: http://www.thescienceforum.com/behavior-psychology/763-intellectuals-social-retardation.html

Sectools. (n.d.). *SecTools.Org: Top 125 Network Security Tools*. Retrieved from Sectools.org: http://sectools.org/tag/vuln-scanners/

Six Sigma. (N.D.). *Wha is Six Sigma*. Retrieved from Six Sigma: http://www.isixsigma.com/new-to-six-sigma/getting-started/what-six-sigma/

Symantec. (N.D.). *Symantec Antivirus Corporate Edition*. Retrieved from Symantec: https://www.symantec.com/page.jsp?id=eol_av_ce

Techtarget. (N.D.). *malware (malicious software)*. Retrieved from Techtarget: http://searchmidmarketsecurity.techtarget.com/definition/malware

TechTarget. (N.D.a). *Snort*. Retrieved from TechTarget: http://searchmidmarketsecurity.techtarget.com/definition/Snort

Weiss, A. (20122, July 2nd). *How to Prevent DoS Attacks*. Retrieved from eSecurity Planet: http://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html