Applying Penetration Tests on a Highly Secured Cooperative Network

Qutaiba Ali, and Salah Alabady
Computer Engineering Department, University of Mosul, Iraq

Abstract*: Security plays a vital role in the design; development and practical use of the distributed computing environment, for greater availability and access to information in turn imply that distributed systems are more prone to attacks. The need for practical solutions for secure networked system management is becoming increasingly significant. Any cooperative network should be supplied with different security techniques and tools. This paper deals with subjecting a highly secured cooperative network to successive penetration tests. An experimental network is built to represent a typical layout for a cooperative network and it is supplied with a variety of security techniques such as, Virtual Local Area Networks (VLAN), Virtual Private Network (VPN), Intrusion Detection System (IDS), Authentication, Authorization, and Accounting (AAA) server, Secure Shell Header (SSH), Access Control List (ACL), WLAN security Techniques and Network Address Translation (NAT). Our tests focus on the evaluation of the importance of each security technique and the effect of their absence on the security level of the network. This work could assist the future introduction of security evaluation matrices.*

Keywords*: Network security, Virtual Local Area Networks, Virtual Private Network, Intrusion Detection System, Authorization, and Accounting server, Secure Shell Header, Network Address Translation.*

Received December 15, 2008; Accepted June 7, 2009

1. Introduction

As the role of enterprise networks keeps expanding in its support of both internal and external connectivity in the form of emerging Internet, intranet, and extranet applications, network components are being exposed more and more seriously to malicious as well as unintentional security breaches. Network security becomes an ever increasingly critical element of enterprise network designs and implementations. A typical network security exercise involves the planning and design of a networks and information technology (IT) security infrastructures so as to protect its valuable applications, sensitive data, and network resources from unauthorized access that results in either intentional or unintentional misuse or malicious alterations of the company's assets. Traditionally, there are four primary classes of threats to network security [1, 2]:

- **Unstructured threats**: Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers.
- **Structured threats**: Structured threats come from hackers that are more highly motivated and technically competent.
- **External threats:** External threats can arise from individuals or organizations working outside the network. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.
- **Internal threats**: Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. This threats occupies for 60 to 80 percent of reported incidents.

Network security estimation is to detect computer system or network facilities to find security holes and vulnerability possibly imposed by hacker, take measures earlier, and protect network system from threats. The current methods of risk evaluation on information security are basically related to qualitative and quantitative ones. Researches on network security situation have two great classes based on system deployment and running information according to data resources [9]. The former is about system design, deployment, service and hidden trouble in the system. The latter is about attacks situations on the system mainly from IDS logs database.

2. Literatures Review

Security situation estimation work based on system running information is mainly about threat estimation from single event on the system. Bass [2, 3] presented that next generation cyberspace intrusion detection systems will fuse data from heterogeneous distributed network sensors to create cyberspace situational awareness, and multi-sensor data fusion technology is an important avenue on the road toward the development of highly reliable intrusion detection and security decision systems that identify, track, and assess cyberspace situations with multiple complex threats. But he only offers small steps in the process of setting the engineering requirements to design and develop cyberspace situational awareness systems. Chen Xiuzhen [9] developed a quantitative hierarchical threat evaluation model and computational method based on the structure of the network and the importance of services and hosts to evaluate security threat status of a computer network system. Because attacks are dynamic, if analysts can't absorb and correlate the available data, it is difficult for them to detect sophisticated attacks. Developing tools that increase the situational awareness and understanding of all those responsible for the network's safe operation can increase a computer network's overall security. System administrators are typically limited to textual or simple graphical representations of network activity. There is a growing body of research that validates the role of visualization as a means for solving complex data problems. Yarden and Stefano [4, 5] focus on visual correlation of network alerts and situational awareness. The National Center for Supercomputing Applications (NCSA) has developed two applications for the detection of network incidents: VisFlowConnect [12] and NVisionIP[10]. They obtain Internet security situation according to visualization of connection analysis and system status.

This paper deals with developing a penetration test procedure for security levels in a cooperative network. An experimental network is built to represent a typical layout for a cooperative network and it is supplied with a variety of security techniques. Our tests focus on the evaluation of the importance of each security technique and the effect of their absence on the security level of the network.

3. Building an Experimental Secured Network

The ultimate objective of network security is to ensure that protected applications and the information used as input and generated as output by these applications are not compromised by malicious or unintentional security breaches. As a result, it is possible to define the major basic network security functional elements that are needed to build a network security system, in terms of the following well-known security services needed for secure message exchanges: confidentiality authentication, authorization, message integrity, and non-repudiation. These five network security functional elements are implemented as hardware and software in network devices (e.g., routers and servers) that are found in places over the end-to-end path of a connection between two communicating endpoints (typically, a client computer and a server or host)[8].

Building on the above concepts, an experimental network is built to be the test bed of our work. The layout of the network could be explained as follows see figure 1.

The network consists of (Cisco2960) switches connected (via Fast Ethernet links) to the Cisco 3720 core switch. These switches represent different network departments. Each switch is connected down to other layer 2 switches and numerous hosts. The connection to the internet is achieved through the Private Internet eXchange (PIX515E) device (which act as a firewall) and the Cisco2811 Network Address Translation (NAT) router. The internet service of the network could also be accessed through several IEEE802.11b WLAN connections.

In order to achieve a high degree of protection, our suggested security model presented in [9] was adopted. In this model, the first dimension is to protect the network against the internal threats. This was achieved using the following techniques:

- Any access to the network must pass through the AAA server. AAA is the acronym for authentication, authorization, and accounting Authentication controls access by requiring valid user credentials, which are typically a username and password. Authorization controls access *per user* after users authenticate. Accounting tracks traffic that passes through the security appliance, gives the ability to have a record of user activity [12]. The AAA server is configured to have two administrators groups: sub administrators and main administrators (for the whole network). The sub administrators have limited access and authorities to the network devices in their departments only. The main administrator has unlimited authorities and can access any portion of the network with configurations privileges over the sub administrators. Also, The AAA server has different groups and accounts for the different users.
- The (Wired & Wireless) LAN connections of the main administrator are protected using Virtual Private Network (VPN). It was found that VPN connection decrease the channel throughput by (70%) [11], for that reason it is used for the administrator communications only. The following VPN parameters are chosen: The authentication method is pre shared keys, AES encryption method, MD5 Hashed Message Authentication Codes (HMAC), Diffie-Hellman Group 2 (1024-bit) and 12 hour policy lifetime. Also, the VPN authentication was enhanced using One Time Password (OTP).
- Installing Intrusion Detection System (a PC supplied with *Snort* software) devices in front of the supposed, sensitive data, locations.
- Splitting the network into several ports based Virtual Local Area Networks (VLANs). It is known that access is denied for a cretin VLAN except their

members. The other benefit of using VALN it to limit the damage caused by viruses or worms to the members of the VLAN.

- Each network device is protected using an '***encrypted User Name & Password'*** assigned by the administrator with two attempts. Also the IP address of the authorized person (administrator) is checked by enabling the access list of the VTY property [12].
- For further protection, the TELNET service and PING command is disabled in all the switches ports (using Access List rules). Alternatively, Secure Shell Header (SSH) is used instead of TELNET. SSH is an application running on top of a reliable transport layer, such as TCP/IP, that provides strong authentication and encryption capabilities [8]. SSH is configured to have a key modulus size of (1024bit). This key is used by the RSA ciphering.
- The WLAN security is achieved using: Rotated 64bit WEP keys (for better performance), MAC address filtering in each access point and network access is achieved through the AAA server. Also VPN is used for administrator's WLAN connections as mentioned earlier.
- The core switch, AAA server and VPNs are supplied with an Extended access lists. These lists are made up of one or more Access Control Entries (ACE). An ACE is a single entry in an access list that specifies a permit or deny rule, and is applied to a protocol, a source and destination IP address or network, and the source and destination ports [12]. Each device has its own rules on which the access lists were written in order to control the traffic inside the network.
- Disabling any unnecessary services on the network devices.
- Using central viruses' server. Symantec Norton Antivirus corporation edition is installed at the server and each client has its own copy which is updated periodically by the server.

Also, the following techniques are used to protect the network against external threats:

- Using AAA server. Any connection request is checked by the AAA server and only the authorized users can access to the network according to their policies.
- In order to access the network remotely, the administrator must use Remote Access VPN connection. This allows the administrator to connect to the management server through a secure connection over a TCP/IP network such as the Internet. This connection has the same VPN parameters mentioned earlier while setting the dynamic Crypto Map. These dynamic crypto maps let the security appliance receive connections from peers that have unknown IP addresses [7].
- Enabling Network Address Translation (NAT) control. Address translation substitutes the real address in a packet with a mapped address that is routable on the destination network. NAT is comprised of two steps: the process in which a real address is translated into a mapped address, and then the process to undo translation for returning traffic [7]. The security appliance translates an address when a NAT rule matches the traffic. If no NAT rule matches, processing for the packet stops. The benefits of NAT are preventing private addresses from being routable on the Internet and NAT hides the real addresses from other networks, so attackers cannot learn the real address of a host. In order to apply Remote administration through VPN connection, static NAT is used.
- In addition to the Extended access lists mentioned earlier, The PIX device (Firewall) is also supplied with an extended access lists. These lists control the traffic in both directions (inside and outside the network) according to predefined rules.
- The whole network is protected against external attacks using another IDS device connected to the *inside* portion of the firewall.
- SSH is used by the administrator only for remote access to the system. It has the configuration mentioned earlier.

4. The Test Procedure

In this paper, *penetration test* is used to discover the importance of each security technique and to evaluate the whole system response. This *test* is designed to evaluate an information system's defense and discover weaknesses in the network and its resources. A penetration test can determine how a system reacts to an attack, whether or not a system's defenses can be breached, and what information can be acquired from the system [8].

Penetration tests can be classified in a number of ways. The most common categories of penetration tests are as follows:

4.1. Internal penetration test

This type of penetration tests tries to complete the following activities while operating from inside the network perimeter:

- Obtain unauthorized connection and access to the network
- Determine the network architecture
- Identify the OS
- Identify OS vulnerabilities
- Obtain protected information from the network and its associated resources
- Evaluate response of any installed intrusion detection systems

- Determine if there are any unauthorized items connected to the network

4.2. External penetration test

An external penetration test attempts to obtain network information while operating outside of the network perimeter. The following types of actions are performed during this type of test:

- Determine the network OS
- Determine OS vulnerabilities
- Obtain unauthorized entry to the internal network
- Gather information about the internal network
- Obtain information stored on internal network resources
- Test the external intrusion detection system (IDS)
- Test the firewall

Using several packet sniffing and network hacking tools (super scanner, port scan, Packer Sniffer, Trinoo and TFN2K), numerous internal & external *supposed* attacks were applied on the network to emulate real world scenarios. The following procedures were taken to examine the network operation (The details of the test procedure are listed in Table (1), which shows the attack type, direction and the effective defense technique(s) against this threat):

- Monitoring the network traffic: attempts were made to monitor the network traffic (as the hacker does before his attack).It was assumed that packet sniffing procedure (using Ping Sweep & Telnet) is done by an authorized user (internal threat) at different locations (inside and out side the network). Trying to use the TELNET service or PING command was stopped by the switches access lists, SSH and AAA server. Also, the IDS prevent any suspicious packet from entering the network.
- The illegal log in to the network (IP Spoofing attack) as well as unauthorized access to some services and resources (Password attacks) was prevented by the AAA server.
- Any attempt to discover the real IP addresses of the network was stopped by the NAT policies.
- SYN flood (randomly opening many TCP ports and tying up the network equipment or computer with so many requests that sessions are thereby denied to others) was stopped by Firewall and IDS devices.
- Misconfiguration attempts to sensitive devices (Core switch) was prevented by SSH, ACL and AAA server.
- VPN technique was very effective in hiding the administration packets from the eyes of the eavesdroppers.
- Worms, Viruses, and Trojan Horses were removed by the distributed Anti virus software.

5. Conclusions

In this paper, penetration tests were used to evaluate the security situation of a highly secured network. It was found that some security techniques were very effective in protecting the network from the reconnaissance attacks in which unauthorized discovery and mapping of systems, services, or vulnerabilities is achieved (which. precede an actual access or Denial of Service (DoS) attack). Other techniques were useful in preventing other types of attacks such as unauthorized system access (the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password) and Denial of Service (DoS) attacks. From this study, it was concluded that protecting a network could not be achieved by a single technique but with an integrated bundle of parallel active solutions.

References

[1] Ali Q., and Alabady S., “Design And Implementation Of A Secured Remotly Administrated Network, " *ACIT07 Conference*, 2007.

[2] Bass T., “Intrusion systems and multisensor data fusion: Creating cyberspace situational awareness, " *Communications of the ACM*, vol. 43, no. 4, pp. 99 -105, 2000.

[3] Bass T , ”Multisensor data fusion for next generation distributed intrusion detection systems”, *1999 IRIS National Symp on Sensor and Data Fusion Laurel*, pp. 24 27, 1999.

[4] Bearavolu R, Lakkaraju K, Yurcik W. , “NVisionIP: An Animate State Analysis Tool for Visualizing NetFlows," *FLOCON Network Flow Analysis Workshop (Network Flow Analysis for Security Situational Awareness)*, Sept. 2005.

[5] Chen XZ, Zheng QH, Guan XH, and Lin CG., “Quantitative Hierarchical Threat Evaluation Model for Network Security," *Journal of Software*, vol. 17, no. 4, pp. 885-897, 2006.

[6] Cisco Inc., “Cisco Security Appliance Command Line Configuration Guide”, 2006.

[7] Cisco Inc., "Cisco Product Catalog", http://cisco.com/univercd/cc/td/doc/pcat

[8] Cole E., Krutz R., and Conley J., *Network Security Bible*, 1’st Edition, Wiley Publishing Inc., 2005.

[9] Foresti, S a , Agutter, J b , Livnat, Y c , Moon, S a , and Erbacher R d., ”Visual correlation of network alerts," *IEEE Computer Graphics and Applications*, vol. 26, no. 2, pp. 48-59, 2006.

[10] Livnat Y a. , Agutter, J b. Moon S b. , and Foresti S c., “ Visual correlation for situational awareness," *Proceedings - IEEE Symposium on Information Visualization*, INFO VIS, pp. 95-102, 2005.

[11] Riedmüller S., Brecht U., and Sikora A., "IPsec for Embedded Systems," *in: H. Weghorn (Ed.), Proceedings of the 2ndAnnual Meeting on Information Technology & Computer Science,* the BA-University of Cooperative Education, ITCS 2005.

[12] Yin X., Yurcik W, and Slagell A., " The Design of VisFlowConnect -IP: a Link Analysis System for IP Security Situational Awareness," *In: Third IEEE International Work shop on Information Assurance (IWIA)*, 2005

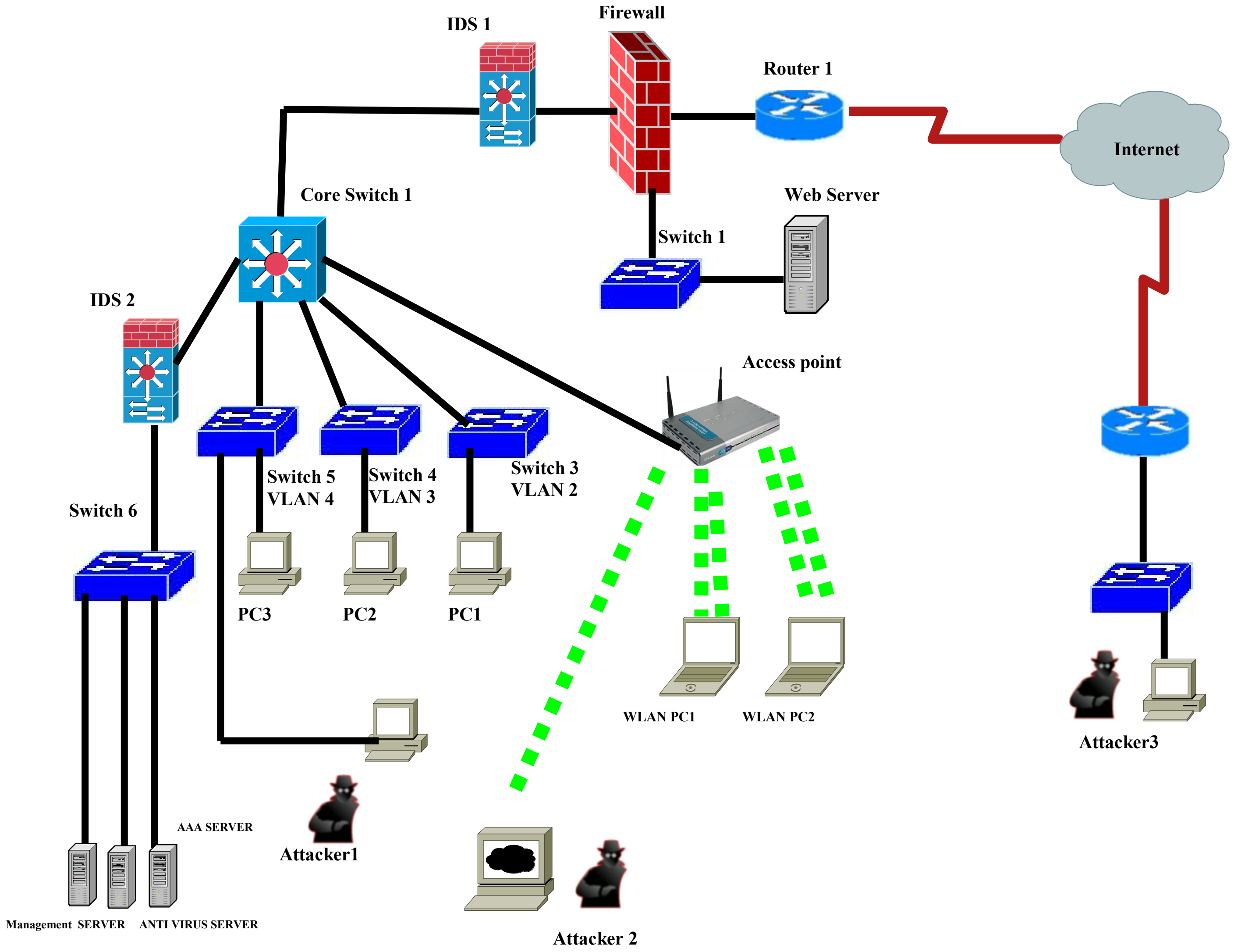

Figure 1. The experimental Network Layout.

Table 1. The test procedures

Threat Type	Attack Name	Source	Target	Security Defense
Internal	Ping Sweeps	Attacker 1	All PC's in other VLAN's	• ACL • VLAN operation
Internal	Telnet	Attacker 1	Switch 5	• AAA Server • SSH • ACL
Internal	Telnet	Attacker 1	Switch 4	• AAA Server • SSH • ACL
Internal	Telnet	Attacker 1	Switch 3	• AAA Server • SSH • ACL
Internal	Telnet	Attacker 1	Core Switch 1	• AAA Server • SSH • ACL
Internal	Telnet	Attacker 1	AAA Server	• AAA Server • SSH • ACL
Internal	Telnet	Attacker 1	Switch 6	• AAA Server • SSH • ACL
Internal	Ping Sweeps	Attacker 2	Core Switch 1	• ACL • VLAN operation
Internal	Ping Sweeps	Attacker 2	WLANPC1 WLANPC2	• ACL • VLAN operation • AP security techniques
Internal	Telnet	Attacker 2	Access point	• AAA Server • ACL • VLAN operation • AP security techniques
Internal	Telnet	Attacker 2	Core Switch 1	• AAA Server • SSH • ACL
External	Ping Sweeps	Attacker 3	Router 1	• NAT • ACL
External	Ping Sweeps	Attacker 3	Firewall	• NAT • ACL
External	Telnet	Attacker 3	Router 1	• NAT • SSH • ACL • AAA server
Internal	Password Attacks	Attacker 1	All network devices (sequentially)	• AAA server • SSH • ACL
Internal	SYN flood attacks	Attacker 1	Web server	• Firewall • Local IDS software(Installed on the server)
Internal	Misconfiguring router	Attacker 1	Core switch1	• SSH • ACL • AAA server
Internal	Password Attacks	Attacker 1	Management server	• IDS 2 • SSH • ACL control
Internal	Password Attacks	Attacker 2	All network devices (sequentially)	• AAA server • SSH • ACL • AP security techniques

Internal	SYN flood attacks	Attacker 2	Web server	• Firewall • Local IDS software (Installed on the server) • AP security techniques
Internal	Misconfiguring router	Attacker 2	Core switch1	• SSH • ACL • AAA server • AP security techniques
Internal	Password Attacks	Attacker 2	Management server	• IDS 2 • SSH • ACL control • AP security techniques
External	IP Spoofing	Attacker 3	Router 1	• NAT • SSH
External	SYN flood attacks	Attacker 3	Web server	• SSH • firewall • NAT • ACL
Internal	Packet sniffing on administrator's VPN traffic	Attacker 2	Administrator's VPN traffic over WLAN	• VPN technique • AP security techniques

Qutaiba Ali was born in Mosul, Iraq, on October ,1974. He received the B.S. and M.S. degrees from the Department of Electrical Engineering, University of Mosul, Iraq, in 1996 and 1999, respectively. He received his Ph.D. degree (with honor) from the Computer Engineering Department, University of Mosul, Iraq, in 2006. Since 2000, he has been with the Department of Computer Engineering, Mosul University, Mosul, Iraq, where he is currently a lecturer. His research interests include computer networks analysis and design, real time networks and systems, embedded network devices and network security and managements. Dr. Ali has attended and participates in many scientific activities and gets membership in many respectable Network Academy, and he is working as Instructor, Curriculum Leader, and Legal Main Contact in Mosul organizations such as IEEE, IENG, ASTF and many others. Currently, he and has more than 20 published papers.

Salah Alabady was born in Mosul, Iraq, on October, 1972, he received the B.Sc. degree in Electronic and Communications Engineering from the University of Mosul, Iraq in 1996, and in 2004 he received the M.Sc. degree in Computer Engineering from University of Mosul. From 2004 till now he is being a lecturer in Computer Engineering Department, Mosul University. His research interests include optical fiber communications, optical network architecture, network security and computer networks design. Alabady gets 10 certifications from Cisco University Regional Academy for Cisco Network Academy program.