SECURITY CONCERNS OF THE CISCO ASA USING MICROSOFT IAS RADIUS

Christopher Landman
Center for Cybersecurity Education
College of Business, University of Dallas
2324 Tall Grass Circle, Bossier City, LA 71111
318-617-7125 clandman@gmail.com

Brett J. L. Landry
Center for Cybersecurity Education
College of Business, University of Dallas
7460 Warren Pkwy, Suite 100, Frisco TX 75034
972-636-8633 blandry@gsm.udallas.edu

ABSTRACT

With today's security threats, Virtual Private Networks (VPNs) have become increasingly important. Security threats are lurking everywhere, so it is important to have a secure connection when a user remotes into a companyôs private network. This experiment tested to see if obvious security holes existed when the Cisco Adaptive Security Appliance (ASA) used a Windows 2003 IAS server for RADIUS. The results showed that some issues such as user and group names passed in clear text, but for the most part, it is secure. The data captured on the outside only showed the VPN group name. The data captured on the inside showed the ACLs pushed from the RADIUS server to the ASA, the user name, and the calling IP address. Nevertheless, on both occasions, the passwords were encrypted.

INTRODUCTION

With today's security threats, Virtual Private Networks (VPNs) have become increasingly important. Security threats are lurking everywhere, so it is important to have a secure connection when a user remotes into a companyôs private network. According to Deal (2006), ñA VPN is a connection, typically protected, between two entities that are not necessarily directly connected" (p. 7). Before VPNs existed, organizations leased dedicated lines between offices to exchange sensitive data which were expensive and complicated to set up. VPNs took away the need for the dedicated lines and created a virtual connection across the publicly used internet (Osipov, Sweeney, & Weaver, 2002). The Adaptive Security Appliance (ASA) is Ciscoôs version of a firewall and/or security appliance. Cisco is moving away from the term firewall and moving towards the term security appliance due to the extended features of the ASA; though they are still used interchangeably (Hucaby, 2008), in this paper the ASA is referred to as a firewall. The ASA is a very popular firewall and VPN device in today's market and comes in many sizes to accommodate small and large networks. The ASA series devices range from ASA5505 for the smaller networks to ASA5540 for the large networks. VPN functionality ranges from 5 to 5000 connections (Frahim & Santos, 2006). The VPN functionality is also very scalable and configurable and can use many types and sources of Authentication, Authorization, and Accounting (AAA) (Hucaby, 2008).

Protection Strategies and VPNs

Protecting internal data from outside sources is critical. In 2008, 74% of all reported network breaches came from the outside, and 99% of all compromised records came from online devices (Sachs, 2009) such as servers and applications. These numbers show that network security is a real threat that Information Technology (IT) departments face every day, and security does not always take priority over money worries or concern about the ability to do oneôs job when away from the office. VPNs play a huge role in helping secure these networks and in defeating unauthorized access and eavesdropping on data being transferred between the network and a remote user.

VPNs are very important to the workforce in today's world. Many organizations rely on VPNs to help remote users communicate securely from anywhere in the world that has an internet connection. The two types of VPNs that are most used today are Site-to-Site and Remote-Access. The Site-to-Site VPN allows two network devices like the ASA to connect two separate networks as if they were the same network subnet. The need for leased lines is eliminated, because it works over the public network. This type of VPN would be used in a business environment where there are different offices in the same company that would like to share resources or be able to communicate in a secure environment. It is accomplished by connecting two VPN devices through an exchange of keys and encryption information to set up a tunnel that the data will pass through (Deal, 2006). The Site-to-Site VPN is good for sites, but not for remote users, since they normally do not carry VPN devices around with them.

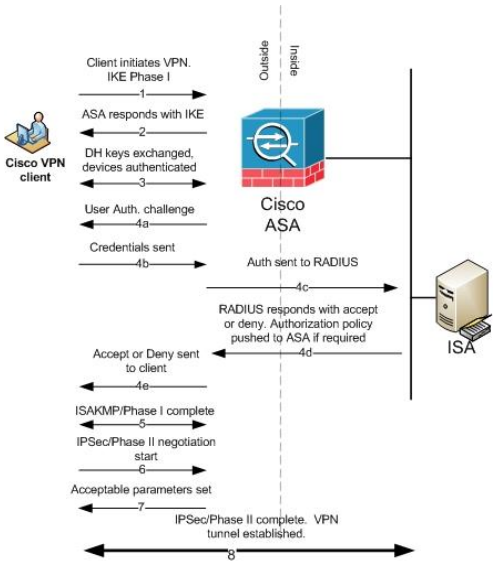

Figure 1: Remote-access VPN using RADIUS

The Remote-Access VPN is used primarily for remote users wanting to connect into a protected network and is the type of VPN this research paper will cover (Frahim & Santos, 2006). These two VPN types primarily go through the same procedures when it comes to creating the tunnel, except for when they get to authenticating the user (Deal, 2006). The Remote-Access VPN can use a RADIUS server to perform the authentication. It normally consists of a VPN device at the edge of the protected network and client software on the remote user's computer or device (Hucaby, 2008). Figure 1 shows how the Remote-Access VPN is set up.

Deal (2006) explains the steps in a Remote-Access VPN using RADIUS as:

1. Remote client initiates the Remote-Access VPN with Internet Key Exchange (IKE) Phase I Security Association (SA) proposal.
2. The ASA responds with acceptable SA proposal.
3. Diffie-Hellman (DH) keys are exchanges, and the devices authenticate each other.
4. User authentication. (This is where Site-to-Site and Remote-Access VPNs differ.)
    a. Initiated with a user/password challenge from the ASA.
    b. Credentials sent from user to ASA.

c. ASA forwards credentials to the RADIUS server along with the requirements for the connection (i.e., authentication, authorization).
d. RADIUS responds to the ASA with an Accept or Deny, and if requested, any authorization that user has in the form of downloadable Access Control Lists (ACL). This is also where any extra items that are configured in RADIUS are sent to the ASA (e.g., IP pool or address, DNS, gateways, etc.)
e. ASA forwards the Accept or Deny to the user and inserts any extra settings such as ACL or IP into its memory for this session.

5. Phase I Internet Security Association and Key Management Protocol (ISAKMP) SA complete.
6. IPSec/Phase II negotiation initiated and proposed SAs are sent.
7. Acceptable SAs are set.
8. IPSec/Phase II completed. VPN tunnel established.

There are several protocols that are used in Remote-Access VPNs, such as Point-to-Point Tunneling protocol (PPTP), Layer 2 Forwarding protocol (L2F), Layer 2 Tunneling protocol (L2TP), and Internet Protocol Security (IPSec). IPSec is the protocol examined in this paper. Phase I starts with two devices that need to set up a connection but do not have the correct keys. There are two modes in phase I, main and aggressive. The two are very similar, but main mode is more secure, because it sets up a secure tunnel to encrypt the IP headers that show the source and destination. Aggressive mode takes much less time to set up the phase I tunnel, because it does not establish a secure tunnel to start the exchange of information (Bhatnagar, 2002). Aggressive mode is the mode used with the Cisco VPN remote-access client, so it was the mode used in this experiment.

In aggressive mode, an ISAKMP SA is negotiated and set up so it can use it to handle phase II negotiation (Cisco, 2006). During phase I, the remote user sends a set of possible parameters to the VPN device. These include encryption type (DES, 3DES, AES 128, etc.), hashing (MD5 or SHA), authentication method (Preshared Key, RSA, etc.), and DH exchange group (1 or 2). DH is a key exchange protocol and hashing is a one-way mathematical function that, when applied to data, creates a very large hash file called a digest. It is almost impossible to recreate that digest unless you use the exact key, and it is not reversible. However, if not protected, the hash can have attacks run against it (McClure, Scambray, & Kurtz, 2005). The VPN device then chooses set parameters that match what it can use from the offered set. If it does not have a matching set, then the tunnel cannot be established (Osipov, Sweeney, & Weaver, 2002). Once the parameters are set and the phase I tunnel is established, then the two sides authenticate each other by the method chosen in the above exchange: ñpublic keys signatures, public key encryption, or a pre-shared key. This exchange is also protected by an encryption method that was selected in the first exchange (Osipov, Sweeney, & Weaver, 2002, p. 341)".

Now that a phase I tunnel is established and the shared secret key is confirmed on both sides, then phase II, Figure 1 step 6, starts to set up IPSec SAs using the already established ISAKMP SAs. With ISAKMP SAs, there is only one tunnel, but IPSec SAs have at least two per device or network, and they are only one-way. For a bidirectional tunnel, there would be two SAs, one for each direction (Frahim & Santos, 2006). Some of the more important attributes negotiated

during phase II are encryption (DES, 3DES, AES128, none, etc.), hashing (MD5, SHA, or null), and mode (tunnel or transport) (Frahim & Santos, 2006).

Security Protocols

The two main security protocols that are used to authenticate users are Terminal Access Controller Access System (TACACS) and RADIUS. TACACS is a Cisco protocol, and TACACS+ is the most up-to-date version (Knipp, et al., 2002). Since this protocol is proprietary, RADIUS is a more widely used choice. RADIUS is a client/server protocol that authenticates users to a VPN device such as an ASA. The ASA would be a Network Access Server (NAS), and it would contact the RADIUS server through UDP (Cisco, 2006). Frahim and Santos (2006) have a good example of the sequence that an ASA and RADIUS server takes to authenticate a user. In Figure 2, they show how the user authenticates to the RADIUS server. They show the RADIUS server as a Cisco server, but any RADIUS server can be substituted there.

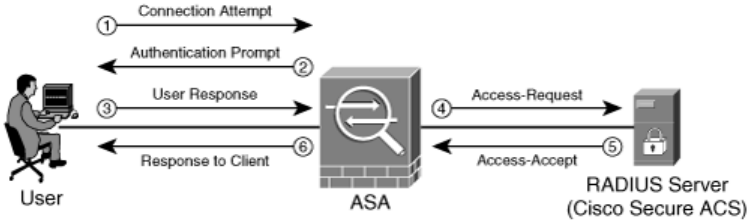

Figure 2: Basic RADIUS Authentication Process (Frahim & Santos, 2006, p. 216)

1. "A user attempts to connect to the Cisco ASA (i.e., administration, VPN, or cut-through proxy).
2. The Cisco ASA prompts the user, requesting his username and password.
3. User sends his or her credentials to the Cisco ASA.
4. The Cisco ASA sends the authentication request (Access-Request) to the RADIUS server.
5. The RADIUS server sends an Access-Accept message (if the user is successfully authenticated) or an Access-Reject (if the user is not successfully authenticated).
6. The Cisco ASA responds to the User and allows access to the specific service" (Frahim & Santos, 2006, p. 216).

The RADIUS server and the NAS authenticate to each other by a shared secret, and the exchange uses port 1812. This is the same port for the user name and password sent between the user and RADIUS (Cisco, 2006). It can use several protocols to make this authentication happen, including PPP, PAP, CHAP, and MS CHAP (Cisco, 2006). Windows IAS server is just one version of RADIUS among many. However, since Windows is widely used, clients already have access to this protocol without additional cost. The ASA can use a local database for AAA (Frahim & Santos, 2006), but that would mean that the organization would need a full-time Cisco professional on staff, which could be very expensive. It would also be more time consuming to add or remove a user's VPN access. The ASA can use RADIUS to query AD for authentication, and it can be managed directly from a domain server (Microsoft, 2004). It can

also use RADIUS to implement AAA and can even provide the ACLs to the ASA for that user during the session. These are called downloadable ACLs (Hucaby, 2008).

Network Policy Server (NPS) is Windowsô current RADIUS server (Microsoft, 2010), but in Windows 2003 it was called IAS. IAS allows RADIUS clients to use AD to authenticate users, but it also allows some clients to set up authentication and accounting (Microsoft, 2004). For the ASA to connect a client IP address to the device, the IP of the ASA has to be entered with a shared key. Then, policies for users or groups that are allowed to have remote access have to be configured. It is always best to use Windows groups for access, because it is easier to add and remove users from groups when you want to allow or disallow remote access (Microsoft, 2005). The group will also need to specify what type of authentication, such as CHAP or MSCHAP, should be used. For this experiment, MSCHAP was used. To use authorization with the ASA, the Cisco-AV-Pair should be chosen from the options. This will allow downloadable ACL to be entered and sent to the ASA once the user is authenticated (Cisco, n.d.). Accounting can also be set up with this server to push to a text file or to a database server.

Vulnerabilities

Sniffers, devices or programs that capture raw packets off the network to be analyzed, can be used to capture traffic passed between the user, ASA, and RADIUS. If the traffic is not encrypted or authenticated, it might be possible for the attacker to gain access to one or all of these devices or accounts (Harris, Harper, Eagle, Ness, & Michael, 2005). If an attacker can masquerade as the RADIUS client and a user tries to connect to him, then the attacker could pass traffic as if he were the client and RADIUS. This is called the man-in-the-middle attack (MITM), and it could capture the traffic (Scambray & McClure, 2003).

Research Questions

This research will answer two research questions: What data is passed between the ASA and the IAS server and can that data be used to manipulate or gain access to either device? This research is important to any organization that uses the ASA, because this configuration could limit the VPN ACL and it could expose data with weak encryption or clear text. If this is the case, an attacker could gain control of the ASA and/or the AD structure (Scambray & McClure, 2003), in which case the attacker could have full control of the network and domain security features.

Methodology

This Remote-Access VPN experiment analyzed how the ASA uses the IAS for RADIUS configuration as it relates to VPNs. It also looked at what data is passed between the two during the information transfer, if it is encrypted, and how the ASA will use that information. The ASA5505 v8.2 had a basic setup with inside and outside networks. The inside, or trusted, network had a Windows 2003 server that is loaded with IAS and serving as a Domain Controller (DC). There was a Windows XP machine on the outside, or untrusted, network that will perform the authentication attempt with Wireshark loaded on it to capture the traffic between the client, Windows XP, and the ASA, which is the VPN endpoint. The communication between the XP machine and the ASA is being examined to see if the traffic is able to be deciphered and

used against either device. There will also be a device with Wireshark on the inside network capturing the traffic between the ASA and the IAS server. This data is important because there could potentially be passwords or shared secrets being passed between the two devices in clear text.

The experiment mimicked the ASA in a corporate environment using the IAS server for RADIUS and AAA. The Cisco ASA 5505 firewall device had a basic security configuration to include some ACLs, VPNs, and separate Virtual Local Area Networks (VLANs), which represent the inside and outside of a network (Cisco, 2008). The network had specific settings to help differentiate the data that is being analyzed as inside or outside the network. The inside IP addresses were in the 192.168.50.0 network with a 255.255.255.0 subnet mask. The outside were in the 10.0.0.0 network with a 255.255.255.0 subnet mask. Since the ASA was at the edge of the network, it had an outside address of 10.0.0.1 and an inside address of 192.168.50.1. The remote user was set at 10.0.0.100 and the IAS server was on the inside at 192.168.50.20.
The experiments contained interactions between a VPN client, the ASA, and the IAS server. The first part of the experiment consisted of connecting to the inside network through a VPN, requiring the ASA to communicate with the IAS server with a RADIUS configuration such as authentication, authorization, assigning an IP address that overrides what the ASA assigns, and duration of connection time. During the connection process, the traffic between the two devices were monitored. To capture the external traffic, there was a Windows XP SP3 machine on a mirrored port for the ASA.

Network Setup

The network equipment used for the experiment was a Cisco ASA, a Cisco 2950 switch, a server, a client, and a computer with Wireshark installed. The ASA was set up with an inside and outside network that served as the testing grounds. The inside network simulated the trusted network. It had an IP address of 192.168.50.0 and a subnet of 255.255.255.0. The outside network simulated the untrusted network. It had the IP address of 10.0.0.0 with a subnet of 255.255.255.0. These two subnets represented the two networks trying to gain access to each other through the VPN. On the outside network, there were two IP addresses in use. The first one was the IP of the outside interface of the ASA. It had the address of 10.0.0.1. This was the entry point to the ASA and the inside network through the ASA. The VPN client had the IP address of 10.0.0.100. The client was a Windows XP SP3 machine with the Cisco VPN client v.50 installed. The client was where the VPN is initiated and the ASA outside interface is the VPN endpoint. The endpoint stopped the client outside the network until the authentication and authorization took place. The ASA, named ASA-8395, was set up with an inside and outside interface. On the basic configuration, the traffic can flow from the inside network to the outside network without much configuration. This is because it is considered normal by most companies to go from an inside network to an outside network, e.g., from the corporate network to the internet for websites. It is not allowed for devices outside the network, such as on the internet, to come into the inside network. This is where the ASA and a VPN come into play. After the basic configuration was set up, the VPN configuration was implemented. In this case, the Remote-Access VPN was set up for remote authentication and authorization from a RADIUS server that sits inside the network. Once the user connects, the ASA assigned the client an IP address that is not in the range of the IP address on the inside or outside network. This is for security and

routing reasons that are beyond the scope of this paper. The IP address range was from 172.16.1.10 to 172.16.1.20 with a subnet mask of 255.255.255.0. The pool had eleven IP addresses, more than enough for this experiment.

A point of interest in the configuration is the actual VPN setup, which includes the protocols, IP address pool, and other general attributes of the VPN. These attributes show how the VPN will connect and communicate. In this case, the Crypto Map shows that it used IPsec with several configurations to accommodate the client. It also shows that the group name is Test_VPN. The shared secret is Cisco111, but it is encrypted. This is how the client authenticates with the ASA for the first round of authentication. If the group name and shared password are wrong, the ASA will immediately drop the connection without initiating either phase of the VPN tunnel. If these two are correct in the client, then Phase I is established and the ASA will then connect to the RADIUS server for user authentication and authorization. For this step to happen, the ASA is set up to communicate with the Windows 2003 server running IAS on the inside network.
The inside network had two IP addresses in use, 192.168.50.1 for the ASA inside interface and 192.168.50.20 for the Windows 2003 server (w2k3) with service pack 2. A basic user, clandman, with the password of Password111 was created and was in the User OU, had basic user rights as a domain user, and the Dial-In permission in the user attributes is set to Control Access through Remote Access Policy. A group called VPN-Group1 was also created and clandman was added to this group. The group has no special access rights to the server in the experiment; it is only used to identify VPN users for an ACL.

The IAS was configured as a RADIUS server to allow connections from the ASA inside address and to authenticate to each other with a shared secret of cisco1234. The main configuration was in the Remote Access Policies section on the IAS server. The profile itself is where other options are added to the connection setup. These options include authentication, encryption, advanced, dial-in constraints, IP, and multilink. The four that are relevant to this experiment are authentication, encryption, IP, and advanced. The authentication tab shows methods of authentication allowed by IAS server for the VPN user. The encryption tab is next in the setup. This tab is where the encryption type is set up. If the site needs to be locked down, then a specific encryption method were chosen to assure proper encryption. The logs will show if encryption is used between the ASA and the RADIUS server. The last items that was set up for this experiment are the Cisco 2950 switch with VLANs to simulate two separate networks and the Windows XP machine with Wireshark.

THE EXPERIMENT RESULTS

The experiment found some mixed results. In the first packet is listed the proposed encryption/hash transport sets that are available to the client. It is the first step in the Phase I key exchange. The payload does have the group name, which is Test_VPN, but the password is encrypted. The second packet shows where the ASA agrees on the encryption transport set and starts to build the Phase I and shows that the IKE Phase I tunnel protocols were 3DES-SHA. The preshared key from the VPN group were sent in the next packets from the client to the ASA encrypted. From this point on, it is very difficult to read the packets, because the payload is encrypted. The connection does go on to finish the Phase I tunnel and then creates the Phase II

tunnel with IPsec. Since most of the data is encrypted and this is the view only from the outside, it is not visible as to where the Windows user/password is sent.

Based on Deal's (2006) research, we know that it is sent before the IPsec Phase II tunnel is created. From the inside, most of the data was encrypted, as well. From the packet capture we see that packet 1 does list in clear text the user name clandman, but the password is encrypted. The packet also shows the calling station of 10.0.0.1 and 10.0.0.100, the clientôs real IP, and the outside address of the ASA. It shows the Network Access Server (NAS) as 192.168.50.1, which is the inside address of the ASA. The second packet, from IAS to ASA, is a rejection. This error shows that an unknown user or incorrect password was used. The third packet is a second attempt to authenticate, which is successful. In addition, here are two inserts from the second and fourth packet, where it deals with user/password. Of course, the encrypted passwords will never show up as the same twice due to how encryption works, which is obvious when you look at more packets. Once the user is authenticated, the Cisco-AV-Pair sends over the attributes that were configured in the advanced tab on the IAS setup. This includes the downloadable ACLs that are used for authorization. The ACLs showed that there was one ACL downloaded as denoted by the AAA. The first entry is just the name and the second entry is the actual ACL. The one item that did not seem to work the way expected was the IP address push from the IAS to the client. In the setup, the ASA was configured to override the ASA VPN IP pool of 172.16.1.10 to 172.16.1.20 and issue an IP address of 172.16.1.25. Unfortunately, this did not happen and the VPN client was issued an IP address of 172.16.1.10. The ipconfig results from the client shows that the clientôs real IP address is 10.0.0.100 and the VPN, Connection 9, is 172.16.1.10. As mentioned earlier, 172.16.1.10 is part of the VPN IP pool from the ASA. This IP address shows that the IAS server was not able to push the IP address as configured.

CONCLUSIONS

The experiment showed that from the outside, the communication from the client to the ASA is secure. It did show the VPN group name, which is considered half of the password, but the actual password was encrypted. There was no other useful data collected from the communication on the outside network. From the inside, the sniffer was able to collect much more information than the outside communication. It showed the user name, the true IP address of the client, as well as the IP address that it was given, the protocols being used, and the ACLs that were pushed to the ASA, to name a few. The data capture also showed that hashes are used so that data integrity can be enforced. The data passed during the exchange is encrypted and hashed to preserve the confidentiality and integrity of the data. The moderately easy setup of these two devices makes this a very time and cost effective option for companies that need secure VPNs but do not have the resources to configure the whole thing on the Cisco device.

Recommendations to Network Administrators

This combination of ASA and IAS for RADIUS allows the network administrator to use the already built domain users database for VPNs. It is our recommendation that a strong shared secret is used for the authentication between the ASA and the IAS. User accounts should also have very strong passwords, because the Windows password grants the user access to the network remotely and to internal resources.

REFERENCES

Cisco. (2006). *Cisco IOS Security configuration Guide: Release 12.2.* http://www-search.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfbook.pdf

Cisco. (2006, January 19). *How Does RADIUS Work?: Document ID: 12433.* www.cisco.com/application/pdf/paws/12433/32.pdf

Cisco. (2008, Febuary 25). *PIX/ASA as a Remote VPN Server with Extended Authentication using CLI and ASDM Configuration.* www1.cisco.com/application/pdf/paws/68795/asa-remotevpn-asdm.pdf

Cisco. (n.d.). *PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS (Against Active Directory) Authentication Configuration Example: Document ID: 70330.* http://www.cisco.com/application/pdf/faws/70330/pix7x-vpn4x-w2k-ias.pdf

Deal, R. (2006). *The Complete Cisco VPN configuration Guide.* Indianapolis: Cisco Press.

Frahim, J., & Santos, O. (2006). *Cisco ASA: All-in-One Firewall, IPS, and VPN Adaptive Security Appliance.* Indianapolis: Cisco Press.

Harris, S., Harper, A., Eagle, C., Ness, J., & Michael, L. (2005). *Gray Hat Hacking: The Ethical Hacker's Handbook.* Emerybille: McGraw-Hill/Osborne.

Knipp, E., Browne, B., Weaver, W., Baumrucker, C. T., Chaffin, L., Caesar, J., et al. (2002). *Managing Cisco Network Security, Second Edition.* Rockland: Syngress Publishing.

McClure, S., Scambray, J., & Kurtz, G. (2005). *Hacking Exposed Fifth Edition: Network Security Secrets & Solutions.* Emeryville, CA: McGraw-Hill/Osborne.

Microsoft. (2004, October 13). *Microsoft Windows Server 2003: Enterprise Deployment of Wireless & Remote Access with RSA and Microsoft Internet Authentication Service.* http://www.microsoft.com/downloads/details.aspx? FamilyID=2466F0E3-231B-46B5-AE1E-0E5D3C3CACAD&displaylang=en

Microsoft. (2005, January 21). *Microsoft Technet: Internet Authenticaion Service.* http://technet.microsoft.com/en-us/library/cc787275(WS.10).aspx

Microsoft. (2010). *Microsoft Technet: Networking and Access Technologies*. Retrieved June 26, 2010, from Microsoft: http://technet.microsoft.com/en-us/network/bb629414.aspx

Osipov, V., Sweeney, M., & Weaver, W. (2002). *Cisco Security Specialist's Guide to PIX Firewall.* Rockland: Syngress Publishing, Inc.

Scambray, J., & McClure, S. (2003). *Hacking Exposed Windows Server 2003: Windows Security Secrets & Solutions.* Emeryville: McGraw-Hill/Osborne.