Global Information Assurance Certification Paper

John Kresho
Version 1.4b (amended August 29, 2002)
GSEC Option 1
May 11, 2004
The Security Policy, Only Half of the Story: Ensure the Words are Put into Action

Abstract

An organization can have an excellent security policy, but unless it is implemented across the organization's information infrastructure, the policy may as well have never been written. This paper is intended to show excerpts from actual security policies, describing topics such as password settings, auditing requirements, the use of the New Technology File System (NTFS), and patch management.

Several tools, such as ManTech's Baseline Toolkit (BTK), netVigilance SecureScout NX, and Microsoft's Software Update Services can help an organization ensure the written policy is put into action. A brief discussion about different topics from a security policy will be followed by a short description of each of these tools. Sample results from the tools mentioned above will be used in describing how actual implementation failed to comply with the written policy.

I have been involved several security assessments recently, and the disconnect between written policy and actual implementation has frustrated me. Hopefully this paper will help organizations realize that self-assessments with the proper tools can focus efforts of local administrators on important security issues and reduce their overwhelming workload.

Introducing the Organization's Network

The network being focused on in this paper is located in an organization's headquarter building, and it has a single Windows 2000 Domain. The servers that are on this network are:

- PDC_1 – The Primary Domain Controller for the organization's network, running Windows 2000 Advanced Server
- BDC_1 – The Backup Domain Controller for the organization's network, running Windows 2000 Advanced Server
- Exchange_1 and Exchange_2 – Both servers are running Windows 2000 Advanced Server with Microsoft Exchange 5.5. The primary purpose of these platforms is to serve mail to the organization's users and to share public folders.
- MEMBER_1 – This server has Windows 2000 Advanced Server installed and is acting as a Member Server. It has the Microsoft Internet Information 5.0 service running. It also acts as a file and printer server.

This network has 156 client workstations, each of which is a member of the company's Windows 2000 Domain. Each workstation has recently been upgraded to Windows 2000 Professional. Finally, there are 8 networked HP printers within the headquarters building.

The above description is generalized based on several assessments that I have conducted. In order to protect the identity of the assessed organizations, let's

assume that a single IP address range of 192.168.1.1-255 is used, and the Windows Domain name is EXAMPLE_DOMAIN.

The Security Policy

When the organization's president asks "How safe is our computer network and the data that is stored on it?" where does the Information Technology (IT) staff or hired assessment team start? "An important first step for most corporations is a security policy that establishes acceptable behavior (Palace Guard Software). " This acceptable behavior should be defined for both system administrators and users. The following topics are based on excerpts from a security policy based on the above network. After describing some of the common items found in the policy, the discussion will switch to verifying the implementation of these items.

Password Requirements

"Gone are the days of using your goldfish's name as a password. The spiraling power of computers makes strong passwords a must (Hurley)." But what is a strong password? In the policy being reviewed, a strong password is defined as being at least eight characters in length and using four of the five following characteristics:

- Upper-case letters
- Lower-case letters
- Letters
- Numbers
- Symbols (e.g. !, @, $, ^)

Passwords must not contain common dictionary words or names, birthdays, phone numbers, or user identifications (USERID). Passwords will be changed every 60 days, and cannot be changed until at least 7 days have elapsed. Accounts will be locked out after no more than three failed logon attempts. Locked out accounts will remain locked out for at least 45 minutes. The failed logon count will be reset every 45 minutes. Accounts locked out for failed logons will not be locked out indefinitely, as this renders the system vulnerable to Denial of Service attacks.

After reviewing the article by Edward Hurley from SearchSecurtiy and the SANS Sample Password Policy, it appears that the above policy statements provide a very good guide for users and administrators to follow. Additionally, this password policy can be used to implement the Account Policy Section within a Microsoft Windows Security Template, giving an assessment team a baseline configuration to check against.

File Management

After a user is authenticated to the network, a method must be established to control what data a user may see and/or change. In a Microsoft Windows

environment, file access can be controlled by using file systems formatted with NTFS. The organization's policy states that all machines running Windows 2000 will format all hard drive volumes using NTFS. The policy also goes on to describe specific permissions on the %NTDIR%\System32 folder. This folder should give the Administrators, Creator Owner, and System groups Full Control and the Authenticated Users group Read permissions. Checking for these correct file permissions will verify another layer in the organization's Defense in Depth strategy.

Network Services

The organization's policy states that a network that has a multiplicity of network services is more vulnerable to cracking than a network with a reduced set of network services. When running, a network service exposes itself to the network by advertising on a "port". For example, a default installation of Microsoft Windows 2000 Advanced Server will have the Network News Transport Protocol (NNTP) listening on Port 119. When a Network News Reader such as Outlook Express attempts to retrieve newsgroup information from this Microsoft Exchange server, it will connect to Port 119. An assessment team will look for open ports such as 119 and ask if it is necessary. If the organization does not use the NNTP service, then NNTP should be shutdown, closing Port 119. Leaving Port 119 open unnecessarily gives an attacker an entry point, allowing for a possible Denial of Service attack to which the Microsoft NNTP service can be susceptible.

Activity Logging

The Event Viewer, which is a part of all Microsoft Windows Server operating systems, is another useful tool to be used in an organization's Defense in Depth Strategy. The Event Viewer's Security Log can identify suspicious behavior, helping system administrators react faster to password cracking attempts and even virus outbreaks. However, in order to be useful, there must be an auditing policy in place that gives the system administrators useful log information and the time to review this information.

In our organization's auditing policy, the following items will be recorded for all servers:

- Success and failure of logon attempts
- Failures of any access to files and printers
- All events related to user and group account administration
- Any Security Policy changes
- All attempts to Shutdown or Restart
- Failed attempts to perform special User Rights
- Failed attempts of processes that attempt to execute.

Additionally, the audit logs must be reviewed twice daily, and will be cleared manually.

If the above policy is followed, system administrator's will have the opportunity to recognize if a hacker is attempting to crack passwords, a user is illegally attempting to access sensitive files, or a virus is attempting to modify EXE or DLL files.

Compliance with US-CERT Recommended Patches

In the organization's policy, it is stated that all servers, workstations and other devices connected to the Internet will be updated with current software patches. But how are the system administrators supposed to know which systems need updating?

The majority of exploits are due to missing patches on computers and other systems that are connected to the Internet. If an organization has a policy in place that allows a system administrator the time and authority to consistently monitor and apply software updates, it will go a long way to preventing a major disaster due to a destructive virus or Denial of Service attack from a well placed Trojan program.

The United States-Computer Emergency Response Team (US-CERT) provides email lists (http://www.us-cert.gov/cas/index.html) to help system administrators stay current with vulnerability information and other security issues. US-CERT Technical Cyber Security Alerts provide system administrators an excellent starting point for gathering information on specific software updates that are needed to address the high level threats against their systems. Additionally, the US-CERT Vulnerability Notes Database provides information for less severe threats, but it should also be monitored.

Self Assessment Tool – Helping Verify the Written Policy

The above discussion points out several topics that are covered in our generalized organization's security policy. Each of these topics can be implemented via technical means. With so many items to track on each computer, and with so many computers, a system administrator requires tools that help ensure each of the technical solutions are in place. Below are three tools that help perform self assessments.

Verifying Windows Security Templates – The Base Line Tool Kit

In a Microsoft Windows 2000 networked environment, it is recommended that a Windows Security Template be used. The Windows Security Template allows a system administrator to setup a single policy file that dictates how security settings are configured on each Windows computer. Items such as the password policy discussed above are included in a security policy. Additional items include an Account Lockout Policy, Auditing Policy, Registry Permissions, and Permissions on System Services.

After configuring a security template, the system administrator applies it to all of the networked computers. In a Microsoft Windows 2000 environment, Active Directory can be used to apply the security template automatically across each computer. Even though Active Directory can do most of the work for the system administrator, security settings should be regularly verified on each computer to ensure there is no abnormal behavior on the network.

The Baseline Tool Kit (BTK) from ManTech Security Technologies Corporation (http://www.mantech.com) is a tool that will enumerate a Microsoft Windows Domain and check each computer against a predefined security template checklist. BTK requires Domain Administrator level access in order to read all items associated with a security template, such as the registry settings and user/group account information.

Local results are normally viewed in an Excel Spreadsheet format. BTK results can be centrally imported into a database that can track overall scan results from different administrators across a large organization. This central reporting method can help show management the continued progress in securing the entire organization. To receive a demonstration of BTK, send email to Keith Ferguson at kferguson@mstc-mantech.com.

Looking for Open Ports– Foundstone SuperScan

Foundstone Inc. distributes a free Microsoft Windows port scanning tool called SuperScan 4.0. To download SuperScan 4.0, point your Internet browser to the following link: http://www.foundstone.com/index.htm?subnav=resources/navigation.htm&subcontent=/resources/termsofuse.htm%3Ffile%3Dsuperscan4.zip.

SuperScan's most popular feature allows a system administrator to scan specific network devices or an entire IP network range, listing open ports found on each device. Reports are generating using HTML, providing an easy to read snapshot of what devices are currently running on a network. By default, SuperScan will check a list of well known TCP and UDP ports on each network device. For example, TCP ports 7 (Echo), 21, (FTP), 25 (SMTP), and 80 (HTTP) are scanned, as well as UDP ports 53 (DNS), 123 (NTP), and 161 (SNMP). Additionally, a custom list of TCP and UDP ports can be entered, including the entire range of 1-65535.

Another option includes "Banner Grabbing". This option will instruct SuperScan to send commands to a well known port in order to gather information. For example, when scanning port 21 (FTP), SuperScan will attempt to logon using "anonymous". If allowed to connect, SuperScan retrieves the Operating System version of the device on which this FTP service is running by executing the SYST command, and then terminates its FTP connection.

SuperScan also allows the system administrator to control how fast packets are sent across the network to conduct the scans. For networks that have high bandwidth (10/100/1000 Mbps), a 10 ms delay or less should not unduly stress the network, but during a scan the additional traffic can be intrusive. Longer delays between scan packets will allow the system administrator to control the intrusiveness of the scan.

Where are the other Vulnerabilities? – Using SecureScout NX

SecureScout NX is a vulnerability assessment tool that attempts to locate known vulnerabilities on a device. The tool can assess any device that has an IP address on a network. When using SecureScout NX to perform a scan of your network, it is usually best to perform a "Safe" scan of your network as a Domain Administrator. SecureScout NX actually performs a test script against a system to determine the existence of a specific vulnerability. The "Safe" scan does not attempt to perform Denial of Service tests on your network, avoiding the more dangerous scans that crash computers. Performing scans with Domain Administrator rights allows a system administrator to see the full list of possible vulnerabilities that exist on his network. As new vulnerabilities are found, the database of test scripts is updated and the SecureScan NX can automatically receive these updates when connected to the Internet.

After performing a vulnerability scan, SecureScout NX produces reports in PDF and HTML formats. Discovered vulnerabilities are broken down into three levels of risk: High, Medium, and Low, giving the system administrator a good starting point to begin closing vulnerabilities. When listing a vulnerability, SecureScout NX describes the problem and provides a recommended solution for the reported vulnerability. By following a regular scanning schedule, the system administrator can stay on top of the patches that are needed to keep his network secure. To get a free trial of SecureScout NX, visit the netVigilance website at http://www.netvigilance.com/trial. netVigilance teams with a Japanese company named NexantiS (http://www.securescout.com/) to maintain the SecureScout NX product.

Using the Tools – What is the Current Status of the Security Policy?

Now that items in the written security policy have been described, and tools that can check the technical implementation of the written policy items have been reviewed, let us assess the organization's progress of putting words into action. SuperScan's results will first be reviewed. This will give an overall picture of the network, showing which doors are open on each network device. Second, the security templates on each computer will be reviewed, checking for password policy compliance, auditing compliance, account lockout policy, and many other settings. Finally, a check for known vulnerabilities will be performed, focusing on existing problems that can be mitigated with currently available patches.

SuperScan Results

For the assessment, the Foundstone SuperScan tool was configured to scan the entire address range (192.168.1.1-255). The scan was performed after working hours so as not to interfere with the daily network traffic. After the scan was complete, the HTML results were viewed. Figure 1 shows two examples from the SuperScan tool. As you can see, the first computer is a Microsoft Exchange mail server. Note that port 119 (NNTP) is open and active. After discussing the report with the organization, it was determined that NNTP is not used internally. This goes against the written policy that instructs the system administrators to stop all unnecessary services. In this case, using the Microsoft Management Console Services Snap-In for Windows 2000, the NNTP service can easily be stopped.

IP	**192.168.1.36**
Hostname	Exchange_1.example_domain.com
Netbios Name	EXCHANGE_1
Workgroup/Domain	EXAMPLE_DOMAIN
TCP Ports (13)	
25	Simple Mail Transfer
53	Domain Name Server
80	World Wide Web HTTP
110	Post Office Protocol - Version 3
119	Network News Transfer Protocol
135	DCE endpoint resolution
139	NETBIOS Session Service
143	Internet Message Access Protocol
389	Lightweight Directory Access Protocol / Internet Locator Service (ILS)
563	nntp protocol over TLS/SSL
593	HTTP RPC Ep Map
636	ldap protocol over TLS/SSL
1030	BBN IAD
UDP Ports (4)	
53	Domain Name Server
135	DCE endpoint resolution
137	NETBIOS Name Service
2967	SSC-AGENT / Norton Antivirus
TCP Port	**Banner**

25 Simple Mail Transfer	220 Exchange_1.example_domain.com ESMTP Server (Microsoft Exchange Internet Mail Service 5.5.2653.13) ready --> HELO anon.com 250 OK --> HELP 214-Commands: 214- HELO MAIL RCPT DATA RSET 214- NOOP QUIT HELP VRFY ETRN 214- XEXCH50 STARTTLS AUTH 214 End of HELP info
80 World Wide Web HTTP	HTTP/1.0 403 Forbidden! Content-type: text/html Content-length: 35
110 Post Office Protocol - Version 3	+OK Microsoft Exchange POP3 server version 5.5.2653.23 ready --> USER root +OK --> PASS password -ERR Logon failure: unknown user name or bad password.
119 Network News Transfer Protocol	200 Microsoft Exchange Internet News Service Version 5.5.2653.23 (posting allowed)
143 Internet Message Access Protocol	* OK Microsoft Exchange IMAP4rev1 server version 5.5.2653.23 (Exchange_1.example_domain.com) ready
389 Lightweight Directory Access Protocol / Internet Locator Service (ILS)	0....a. ......
563 nntp protocol over TLS/SSL	[Connection closed by remote host]
593 HTTP RPC Ep Map	ncacn_http/1.0
636 ldap protocol over TLS/SSL	[Connection closed by remote host]
UDP Port	**Banner**
137 NETBIOS Name Service	MAC Address: 00:05:C3:33:2B:F3 NIC Vendor : Intel Corporation Netbios Name Table (9 names) EXCHANGE_1 00 UNIQUE Workstation service name EXCHANGE_1 20 UNIQUE Server services name EXAMPLE_DOMAIN 00 GROUP Workstation service name EXAMPLE_DOMAIN 1C GROUP Domain controller name EXAMPLE_DOMAIN 1E GROUP Group name EXCHANGE_1 03 UNIQUE Messenger name EXCHANGE_1 6A UNIQUE EXCHANGE_1 87 UNIQUE ADMINISTRATOR 03 UNIQUE Messenger name

IP	**192.168.1.119**
Hostname	Workstation_81.example_domain.com
Netbios Name	WORKSTATION_81
Workgroup/Domain	EXAMPLE_DOMAIN

UDP Ports (3)	
7	Echo
137	NETBIOS Name Service
2967	SSC-AGENT / Norton Antivirus

TCP Ports (8)	
7	Echo
9	Discard
13	Daytime (RFC 867)
19	Character Generator
135	DCE endpoint resolution
139	NETBIOS Session Service
445	Microsoft-DS
1029	[Unknown]

TCP Port	Banner
13 Daytime (RFC 867)	11:14:37 AM 2/26/2004
19 Character Generator	!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefg !"#$%&'()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefgh "#$%&'()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghi #$%&'()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghij $%&'()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijk %&'()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijkl &'()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklm '()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmn ()*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmno )*+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnop *+,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq +,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqr ,- ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrs - ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst ./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst u /0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu v 0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuv w 123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvw x 23456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwx y 3456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxy z 456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz { 56789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{

	| 6789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{| } 789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|} 89:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|} ! 9:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|} !" :;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|} !"# ;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|} !"#$ <=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|} !"#$=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopq

UDP Port	Banner
137 NETBIOS Name Service	MAC Address: 00:0D:60:12:D8:65 NIC Vendor : Unknown Netbios Name Table (6 names) WORKSTATION_81 00 UNIQUE Workstation service name EXAMPLE_DOMAIN 00 GROUP Workstation service name WORKSTATION_81 03 UNIQUE Messenger name WORKSTATION_81 20 UNIQUE Server services name EXAMPLE_DOMAIN 1E GROUP Group name ADMINISTRATOR 03 UNIQUE Messenger name

Figure 1: SuperScan Results

The second computer shown appears to have the chargen and daytime services running. Even though the risk against these services is considered low, they are usually not needed and should be shutdown. The chargen service is susceptible to Denial of Service attacks, and the time service can give the attacker an idea of which operating system is being used. Both services can be shutdown by modifying the registry.

Solution for chargen (E-Soft, Chargen)
Set the following registry keys to 0
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpChargen
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpChargen

Solution for daytime (E-Soft, Daytime)
Set the following registry keys to 0
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableTcpDaytime
HKLM\System\CurrentControlSet\Services\SimpTCP\Parameters\EnableUdpDaytime

SuperScan provides a quick snapshot of what the network looks like at the surface. Its reports can help close some of the doors that attackers routinely look for, and they can help the system administrator put the written policy words into action.

BTK – Security Template Impementation Checks

BTK was configured to enumerate the EXAMPLE_DOMAIN by pointing it to an existing WINS server. In order to conduct the scans, a system administrator entered a password into BTK to give it Domain level administration privileges. The scan was conducted against the five Windows 2000 servers. As can be seen from the Account Policy section shown in Figure 2, items failed for each server.

	PDC_1	BDC_1	Exchange_1	Exchange_2	MEMBER_1
ACCOUNT POLICIES					
Max Password Age	**Passed**	**Passed**	**Passed**	**Passed**	**Passed**
Min Password Age	**Passed**	**Passed**	**Passed**	**Passed**	**Failed** Invalid value. Value data required (86400) Value data setting (0)
Min Password Length	**Failed** Invalid value. Value data required (8) Value data setting (6)	**Failed** Invalid value. Value data required (8) Value data setting (6)	**Failed** Invalid value. Value data required (8) Value data setting (6)	**Failed** Invalid value. Value data required (8) Value data setting (6)	**Failed** Invalid value. Value data required (8) Value data setting (0)
Password Uniqueness	**Passed**	**Passed**	**Passed**	**Passed**	**Passed**
Account Lockout	**Passed**	**Passed**	**Passed**	**Passed**	**Failed** Invalid value. Value data required (1) Value data setting (0)
Lockout Threshold	**Failed** Invalid value. Value data required (3) Value data setting (5)	**Failed** Invalid value. Value data required (3) Value data setting (5)	**Failed** Invalid value. Value data required (3) Value data setting (5)	**Failed** Invalid value. Value data required (3) Value data setting (5)	**Passed**
Reset Count	**Passed**	**Passed**	**Passed**	**Passed**	**Passed**
Lockout Duration	**Passed**	**Passed**	**Passed**	**Passed**	**Passed**
Force Logoff	**Passed**	**Passed**	**Passed**	**Passed**	**Passed**

Figure 2: BTK Account Policy Results

The most severe violation of the written policy is the Minimum Password length. It is currently set at 6, where it should be 8. The other violation is related to how many failed logon attempts are allowed before a user account is locked out, called the Lockout Threshold. This is set for 5, where it should be 3. Both of these setting can be fixed by using the Group Policy Snap-In when using Windows 2000.

Figure 3 displays the Audit Policy section from the BTK report. Almost all of the items Failed, meaning that the written policy has been ignored. The organization cannot determine if an attacker, or an insider, is attempting to gain unauthorized access to the servers. Even if the system administrators had an idea that suspicious activity was occurring, there would be little proof, if any, due to the lack of auditing. Another item corresponding to the Audit Policy is the Event Viewer. Viewing Figure 4 shows that even if the logs were generated, they would be overwritten quickly, having only a 512KB size limit. The Audit Policy can be corrected by using the Group Policy Snap-In when using Windows 2000. The

system administrator should ensure that the Event Viewer is used to set the correct maximum log size, and that the logs are not overwritten.

	PDC_1	BDC_1	Exchange_1	Exchange_2	MEMBER_1
AUDIT POLICIES					
File Object Access	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Passed**
Logon Logoff	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)
Process Tracking	**Passed**	**Passed**	**Passed**	**Passed**	**Passed**
Restart Shutdown	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Passed**
Security Policy Changes	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)
System Events	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)
User Group Management	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Success, Failure) Value data setting (No Auditing)
User Rights	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)	**Failed** Invalid value. Value data required (Failure) Value data setting (No Auditing)

Figure 3: BTK Audit Policy Results

	PDC_1	BDC_1	Exchange_1	Exchange_2	MEMBER_1
EVENT VIEWER					
Check Overwrite	**Failed** Required(Do Not Overwrite: Retain Logs days).Settings(Application=Overwrite: Retain Logs 0 days;Security=Overwrite: Retain Logs 0 days;System=Overwrite: Retain Logs 0 days).	**Failed** Required(Do Not Overwrite: Retain Logs days).Settings(Application=Overwrite: Retain Logs 0 days;Security=Overwrite: Retain Logs 0 days;System=Overwrite: Retain Logs 0 days).	**Failed** Required(Do Not Overwrite: Retain Logs days).Settings(Application=Overwrite: Retain Logs 0 days;Security=Overwrite: Retain Logs 0 days;System=Overwrite: Retain Logs 0 days).	**Failed** Required(Do Not Overwrite: Retain Logs days).Settings(Application=Overwrite: Retain Logs 0 days;Security=Overwrite: Retain Logs 0 days;System=Overwrite: Retain Logs 0 days).	**Failed** Required(Do Not Overwrite: Retain Logs days).Settings(Application=Overwrite: Retain Logs 0 days;Security=Overwrite: Retain Logs 0 days;System=Overwrite: Retain Logs 0 days).
Check Log Size	**Failed** Required(4194240 KB).Settings(Application=512 KB;Security=512 KB;System=512 KB).	**Failed** Required(4194240 KB).Settings(Application=512 KB;Security=512 KB;System=512 KB).	**Failed** Required(4194240 KB).Settings(Application=512 KB;Security=512 KB;System=512 KB).	**Failed** Required(4194240 KB).Settings(Application=512 KB;Security=512 KB;System=512 KB).	**Failed** Required(4194240 KB).Settings(Application=512 KB;Security=512 KB;System=512 KB).

Figure 4: BTK Event Viewer Results

Another section to look at is the File Directory Permissions. Based on Figure 5 below, the Everyone group has Change permissions for the %NTDIR%\SYSTEM32 folder on some servers, and Read Permissions for the same folder on other servers. Again, this is against written policy and can create a security risk. The Everyone group can include any anonymous user that connects to the network (e.g. Web user). Such a user having Change permission to the System32 folder is very dangerous because actual Windows applications can be replaced with Trojan programs.

	PDC_1	BDC_1	Exchange_1	Exchange_2	MEMBER_1
FILE DIRECTORY PERMISSIONS					
Permissions: %NTDIR%\SYSTEM32	**Failed** Invalid number of trustees. Required (4) Settings (5); **DIR: \\IIMEFDMN01C\c$\WINNT\system32** : Administrators - Full Control (All)(All), Everyone - Change (RWXD)(RWXD), CREATOR OWNER - Full Control (All)(All), Server Operators - Change (RWXD)(RWXD), NT AUTHORITY\SYSTEM - Full Control (All)(All)	**Failed** Invalid number of trustees. Required (4) Settings (5); **DIR: \\IIMEFDMN02E\c$\WINNT\system32** : Administrators - Full Control (All)(All), Everyone - Change (RWXD)(RWXD), CREATOR OWNER - Full Control (All)(All), Server Operators - Change (RWXD)(RWXD), NT AUTHORITY\SYSTEM - Full Control (All)(All)	**Failed** Invalid number of trustees. Required (4) Settings (5); **DIR: \\IIMEFDMN03E\c$\WINNT\system32** : Administrators - Full Control (All)(All), Everyone - Change (RWXD)(RWXD), CREATOR OWNER - Full Control (All)(All), Server Operators - Change (RWXD)(RWXD), NT AUTHORITY\SYSTEM - Full Control (All)(All)	**Failed** Invalid number of trustees. Required (4) Settings (5); **DIR: \\IIMEFDMN04E\c$\WINNT\system32** : Administrators - Full Control (All)(All), Everyone - Change (RWXD)(RWXD), CREATOR OWNER - Full Control (All)(All), Server Operators - Change (RWXD)(RWXD), NT AUTHORITY\SYSTEM - Full Control (All)(All)	**Failed** Invalid number of trustees. Required (4) Settings (5); **DIR: \\IIMEFDMN04E\c$\WINNT\system32** : Administrators - Full Control (All)(All), Everyone - Change (RWXD)(RWXD), CREATOR OWNER - Full Control (All)(All), Server Operators - Change (RWXD)(RWXD), NT AUTHORITY\SYSTEM - Full Control (All)(All)

Figure 5: BTK File Directory Permission Results

The last BTK item to be reviewed is from the scan of a Windows 2000 Member Server. Remember from the description of the network above that the Windows 2000 Member Server is running Web Services and shares files and printers.

	PDC_1	BDC_1	Exchange_1	Exchange_2	MEMBER_1
DISK ADMINISTRATOR					
Check Dual Boot	**Passed**	**Passed**	**Passed**	**Passed**	**Passed**
Check NTFS	**Failed** Volume(s) not formatted NTFS: G$	**Passed**	**Passed**	**Passed**	**Failed** Volume(s) not formatted NTFS: G$, H$

Figure 6:BTK Disk Administrator Results

Based on Figure 6, BTK performed a check on the Disk Administrator and found that two volumes on MEMBER_1 and one volume on PDC_1 where not formatted with NTFS. Again, this is not compliant with the written policy. Files located on these volumes are not protected using the Windows NTFS permissions. The Windows 2000 *convert.exe* utility can convert a FAT32 volume to NTFS without reformatting the volume.

BTK has done its job and pointed out the areas to where the system administrator needs to focus his immediate attention.

SecureScout NX Results - There's More Vulnerabilities?

Finally, SecureScout NX was run to check for other known vulnerabilities that are not covered by SuperScan or BTK. The SecureScout "Safe" scan was used to evaluate all of the network servers, workstations, and printers (192.168.1 – 255). Figure 7 displays a few samples of what the scans discovered:

Vulnerability name:	Microsoft Windows RPC DCOM Interface Buffer Overflow Vulnerability
Vulnerability description:	Remote Procedure Call (RPC) is a protocol used by the Windows operating system. RPC provides an inter-process communication mechanism that allows a program running on one computer to seamlessly execute code on a remote system. There is a vulnerability in the part of RPC that deals with message exchange over TCP/IP. The failure results because of incorrect handling of malformed messages. To exploit this vulnerability, an attacker would need to send a specially formed request to the remote computer on port 135. By exploiting this flaw a remote attacker is able to overflow a buffer and then obtain local system privileges to execute arbitrary code.
List of vulnerable hosts	192.168.1.34 (PDC_1.example_domain.com) 192.168.1.35 (PDC_2.example_domain.com) 192.168.1.36 (Exchange_1.example_domain.com) 192.168.1.37 (Exchange_2.example_domain.com) 192.168.1.38 (Member_1.example_domain.com) 192.168.1.39 (workstation_1.example_domain.com) 192.168.1.57 (workstation_19.example_domain.com)

Vulnerability name:	Microsoft Exchange Server Buffer Overflow Vulnerability
Vulnerability	The Internet Mail Service in Exchange Server 5.5 and Exchange 2000 allows

description:	remote attackers to cause a denial of service (memory exhaustion) by directly connecting to the SMTP service and sending a certain extended verb request, possibly triggering a buffer overflow in Exchange 2000.
List of vulnerable hosts	192.168.1.36 (Exchange_1.example_domain.com) 192.168.1.37 (Exchange_2.example_domain.com)

Vulnerability name:	NetBIOS Null Session Vulnerability
Vulnerability description:	A NetBIOS null session is possible. A null session is established with username "", password "", domain "" (no authentication). It is normally used to list resources (shares). This may allow access to usernames and to the registry database.
List of vulnerable hosts	192.168.1.34 (PDC_1.example_domain.com) 192.168.1.35 (PDC_2.example_domain.com) 192.168.1.36 (Exchange_1.example_domain.com) 192.168.1.37 (Exchange_2.example_domain.com) 192.168.1.38 (Member_1.example_domain.com) 192.168.1.39 (workstation_1.example_domain.com) 192.168.1.57 (workstation_19.example_domain.com) 192.168.1.60 (workstation_22.example_domain.com) 192.168.1.61 (workstation_23.example_domain.com) 192.168.1.102 (workstation_64.example_domain.com) 192.168.1.119 (workstation_81.example_domain.com) 192.168.1.123 (workstation_85.example_domain.com) 192.168.1.125 (workstation_87.example_domain.com) 192.168.1.128 (workstation_90.example_domain.com) 192.168.1.152 (workstation_114.example_domain.com)

Figure 7:SecureScout NX Results

The first vulnerability noted is a Microsoft Windows RPC buffer overflow. Several systems on the network are affected by this vulnerability and are missing an available patch that will mitigate this issue. By clicking on the Vulnerability Name link in the SecureScan NX report, a description and recommended action is shown to the system administrator. An advisory from the CERT was published on 17 July 2003 (http://www.cert.org/advisories/CA-2003-16.html) to alert system administrators of this problem.

The next vulnerability was only found on a single server, but it is a vital Microsoft Exchange server. This known vulnerability was published by the CERT on 16 October 2003 (http://www.cert.org/advisories/CA-2003-27.html), and is considered a high risk. As with the RPC vulnerability mentioned first, there is an available patch from Microsoft that will mitigate this risk.

The final vulnerability discussed from the SecureScout NX results is found on almost 20 devices connected to the network. This is the NetBIOS Null Session Vulnerability as discussed in the SANS Top 20 List. If not mitigated, information

regarding a computer's shared folders, users, groups, and other registry resources can be gathered by a non-authenticated user. Recommended solutions can be found in the SecureScout NX report, as well as in the SANS Top 20 List.

The above results show that only a fraction of the devices on the network are exposed to the vulnerabilities found by SecureScan NX. This demonstrates that some patching has occurred and that the system administrator has kept up with the CERT advisories and other publicly available security information (e.g. the SANS website). Maintaining the correct patches on all computers can be very time consuming and some computers may be missed unless the process can be automated. One method of keeping up with current patch releases in a Microsoft environment is by implementing Microsoft's free Software Update Services (SUS) and the new Windows Update Services (WUS). Both of these services provide the system administrator a method of controlling when specific patches are applied to network devices. Both SUS and WUS download updates that Microsoft provides for its operating systems, Exchange and SQL products, and Office applications. Once these updates are downloaded a system administrator can test them and specify which updates are applied to his organization's assets. Each client's Windows Update service is now pointed to a local SUS or WUS resource vice the Microsoft website, automatically downloading the organization's approved updates.

Conclusions

As described at the beginning of the paper, the written policy appears to be a good start in providing a Defense in Depth strategy for the organization. It covers password, file protection, auditing, and patch management policies. However, having the written policy is only half of the battle, action must be taken, and actually implementing the written policies can be a daunting task. Even if a system administrator attempts to keep up with the constant releasing of new patches and security recommendations, some devices may be missed. A method must be established for ensuring the technology is applied in order to comply with written policy. Performing a self-assessment with existing tools that shows a current snapshot of the network, checking for security template compliance, and scanning for known vulnerabilities can help focus the system administrator on what tasks need to be completed in order to keep the organization's network secure.

References

Palace Guard Software. "Security White Paper". URL: http://www.pgsas400.com/whitepaper.htm (7 May 2004).

SANS Institute. "Password Protection Policy". The SANS Security Policy Project. URL: http://www.sans.org/resources/policies/Password_Policy.pdf (6 May 2004).

Hurley, Edward. "Proper password policy is imperative". 8 Jul 2002. URL: http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci837272,00.html (18 April 2004).

Aitken, Robert. "Taking the Confusion Out of Security Templates". 27 March 2003. URL: http://www.sans.org/rr/papers/67/989.pdf (8 May 2004).

Gibson, Steve. "Evil Port Monitors?". "Internet Connection Security for Windows Users". URL: http://grc.com/su-evilportmon.htm (6 May 2004).

Microsoft Corporation. "Microsoft Security Bulletin (MS98-007): Potential SMTP and NNTP Denial-of-Service Vulnerabilities in Microsoft Exchange Server". Microsoft Technet. 9 September 1998. URL: http://www.microsoft.com/technet/security/bulletin/ms98-007.mspx (10 May 2004).

Microsoft Corporation. "Best practices for auditing". Microsoft Windows 2000 Server Documentation. URL: http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_SEconceptsImpAudBP.htm (3 May 2004).

Merrion, Sarah. "Is Patching a priority?". 29 March 2004. URL: http://www.computeruser.com/articles/daily/8,10,1,0329,04.html (9 May 2004).

"Useless Services: Chargen". URL: http://www.securityspace.com/smysecure/catid.html?id=10043 (7 May 2004).

"Useless Services: Daytime". URL: http://www.securityspace.com/smysecure/catid.html?viewsrc=1&id=10052 (7 May 2004).

SANS Institute. "W5 Windows Remote Access Services". The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus. Version 4. 8 October 2003. URL: http://www.sans.org/top20/#w5 (8 May 2004).

CERT. "vulnerabilities, incidents, and fixes". URL: http://www.cert.org/nav/index_red.html (10 May 2004).

Thurrott, Paul. "What You Need to Know About Windows Update Services". Windows &.NET Magazine. April 2004. URL: http://www.winnetmag.com/Windows/Article/ArticleID/41969/41969.html (9 May 2004).

Last Updated: May 29th, 2017

Upcoming Training

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 San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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 Munich Summer 2017	Munich, Germany	Jul 10, 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
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 Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
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
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event