Global Information Assurance Certification Paper

SANS Security Essentials
GSEC Practical Assignment
Version 1.2e
December, 2000 (Amended May 22, 2001)

Developing the Network Operations Center in Support of the NT 4.0 Wide Area Network.

David C. Peterson
March 25, 2001

Introduction:

I believe the greatest challenge for a Network Operations Center (NOC) is to balance the following three desired outcomes with respect to a communications network: the organizations mission, the support to the individuals, and network security. The fulcrum for this triangular shaped plate is that of a pinhead and these tasks are constantly outweighing each other. This paper is not intended to identify the perfect formula for this balance but only to show some real life concepts and solutions as well as some technical points.

To manage all three outcomes requires a fair amount of knowledge, experience, and resiliency on the Network Operations Center Staff. This process involves the proper planning and configuration of resources, to include personnel, training, equipment, end-user awareness, and manageable policies.

Background:

I was selected as the Network Security Manager for my federal agency in December 2000, just weeks before the…much anticipated Y2K challenge. Upon surviving Y2K and the next nine months of learning the functions of the Network Security Manager, I was promoted to the Information Management Branch Supervisor. With this…promotion…I took with me the responsibilities of the Network Security Manager. I was told that because of the funding constraints, the directorate would not backfill this position so I would balance both positions.

My first task given to me by my supervisor was to build a Network Operations Center so that any IT savvy person could look at the checklist and maintain the Network on a recurring basis. I have conducted much personal research via the Internet, books, magazines, and interviews with my sister agencies and have built a NOC that fits my networks needs.

The functions of the NOC deal with the three demands that I mentioned above and the "all-inclusive checklist is evolving daily as I and my subordinates get smarter about the Network. This "Checklist" is a tool that maximizes the performance and products of the NOC. My attendance at the SANS eCoast conference in March really aided in identifying the details necessary to be performed in the NOC.

I recently found the following NOC description, which I think, is very fitting. It's from University of Indiana's "University Information Technologies Services (UITS):

"The Network Operations Center (NOC) monitors, documents and troubleshoots resource connectivity in an open systems environment. In the process of network support, the NOC develops, maintains, and implement service methodologies on a continuous operating schedule of seven days a week, 24 hours a day. The focus of the NOC's functions includes fault prevention, detection and correction of component failures, reporting, and statistic gathering. The NOC facilitates the coordination, notification, and scheduling of network installations and enhancements, as well as managing internal resources for continuous network support."

In this paper, I will describe the sanitized process that I went through and I would recommend that someone go through in the development of a fully functional Network Operations Center. I will detail some points and just skirt other ideas for future research. This, by no means is an "all inclusive" document.

Assessment:

The first step in building a NOC is to assess what it is that you have to control and monitor. In my assessment, I looked at the wide area network (WAN) architecture and the associated equipment, and each local area network. Other areas of concern were the Information Technology Personnel assigned to the directorate, the training level of the individuals, the threat environment, the current level of awareness of the end-users, the network access policy, the network security policy, and the physical security policy.

A critical task is to identify the baseline for the network configurations. This I was able to do by researching through notes, logbooks, and within components themselves to determine our baseline. Interviewing key personnel was necessary to interpret many inconclusive notes.

The Baseline: It is imperative in establishing the baseline to focus on the following areas. This will also be the starting point when building the Network Operations Center (NOC).

The Network Architecture - The scale of the network is important. In this federal agency, the Wide area Network that I am responsible for lies within the bounds of the State of New Hampshire. But I do have to report to a higher Headquarters who's WAN consists of its own headquarters, and 54 States and Territories. Most of these are larger than New Hampshire's and a few are much smaller. The Headquarters itself is a campus that is a viable part of the National WAN. It is important to note that the configuration of the New Hampshire WAN must be in accordance with the National Headquarters standards as well as good industry standards. Any uniqueness that I configure my WAN for must be in compliance with them.

The Wide Area Network - As I previously mentioned the WAN in NH is basically 28 LANS in twenty-one different localities. The WAN consists of one large site, a campus consisting of seven LANS, and twenty small sites. The large site and three small

sites have a T1 (1.545 Mbps) capacity in bandwidth and the remainder of the small sites are presently connected with 56K modems. (I am presently managing a project to change the terrestrial based network over leased lines to a microwave broadband network that will send voice, data, and video across it at T1 capability as a minimum to the small sites and from two to five Mbps to the larger sites).

The Local Area Networks - The LANS support a minimum of ten workstations at the remote sites to a couple of hundred workstations in the seven LANS at the campus.

The Campus - The Campus consists of seven buildings each with its own LAN. When the microwave broadband system enters the picture, this campus will retain the terrestrial system between all its LANS and will connect to the other LANS via microwave.

The New Hampshire Network presently supports approximately 725 end users, which we anticipate to grow to approximately 1200. We support about 550 servers and workstations to include notebook computers. We are standing up a Virtual Private Network (VPN) that will account for the growth of end users. Individuals are expected to use privately owned Personal Computers to gain access to the Network via the VPN. Virtual Private Networks create a whole different set of issues with respect to bandwidth consumption, customer service, and network security.

Personnel staffing - The Network Operations Center consists of a combination Information Management Branch Supervisor/Network Security Manager, a Network Manager, a Network Engineer, and a Senior Wide Area Network manager who also has the responsibilities of the Telecommunications Manager. I have a Visual Information Manager working for me but she is not an operational asset of the NOC.

Personnel Qualifications - Personnel Qualifications of those in the NOC range from no formal classroom/lab training to personnel trained in most every aspect of Windows NT 4.0 and Cisco Routers. Experience also ranges from those who can do elementary Administrator and Workstation functions to those with much formal training and have great experience. I recommend that new personnel to the NOC staff be assessed as to their competencies and a combination formal schooling plan and on-the-job training plan be devised to maintain their momentum along the learning curve. According to a study done by the Gartner Group, Inc. in 2000 an untrained It person would likely take 45 hours to accomplish the same skill level that a trained employee will take ten hours to achieve (including training).

24x7 Operational Capability - What is the requirement for the NOC to maintain continuous operations? Can the NOC be monitored in a 24x7 configuration? With minimal manpower this may be impossible to physically man the seats. With the proper use of remote stations and alerts being sent to pagers, problems can be noted during the off-hours with a contingent plan being placed into effect before the start of the normal duty day.

The Operating System of the Network - This network is comprised of primarily a Windows NT 4.0 operating system with its entire supporting infrastructure. There are fourteen (14) different stovepipe systems are basically databases that are linked to via NT 4.0 and are reportable to higher headquarters via the network. Not all these systems are windows based or other GUI type. Some are command line interface so the NOC personnel have to maintain a certain level of competence in these systems as well. Most of this training is via informal on the job training. It is imperative that the system administrators monitor the technical Websites to keep informed of the latest service packs, patches, and information notices. There should be routine updates of vulnerability information related to the operating system, email system, and web server system. The email system for my organization is Outlook running on Microsoft Exchange 5.5. Presently we are supporting Outlook 97, 98, and 2000.

Network Security

Information Awareness Vulnerability Alert (IAVA) Compliance - It is mandated that all Department of Defense (DOD) networks maintain IAVA compliance. IAVA messages are routinely distributed to each state as threats and associated vulnerabilities are identified. It is the NOC personnel function to acknowledge the message, make the correction, and to notify the higher headquarters of the corrected action.

The Intrusion Detection System - The Intrusion Detection System (IDS) can be a Network-based system, a Host-based system, or a hybrid of the two systems working in concert with one another. We are running a Network based ID system to monitor attempts outside our perimeter. We are presently standing up some host based ID systems on critical servers and in areas of high traffic usage to monitor inside network attempts at violating components of the system.

Firewalls - We have firewalls stood up at each point of entry into the New Hampshire Network. All accesses to the Internet travel through two additional layers of security through our higher headquarters before actually touching the outside world. The firewalls are configured to deny all and as we determine a need we then open the appropriate port.

Scanners - We have deployed the additions of a Network scanner, a network monitor, and a network sting software packages in testing the vulnerabilities of our defenses. Using good third party software is imperative in getting the "honest broker" assessment of our defenses. We run this suite of tools once every three months to determine the critical vulnerabilities.

End-User Awareness and Training - This is critical as the final line of defense in the rings of defense when it comes to the network. Users are trained in using the NT 4.0 workstation, email, file shares, virusware, and backups. Even with the best security in place, a careless end-user can cause great chaos in a network. Keep them well

trained and well informed. Create an environment of anonymity when bringing issues forward. Forgiveness will go a long way in network security.

Web surfing software monitoring - It is important to track Internet usage and to publish it throughout the organization. We do not publish it in a name-by-name method but in a generic way that will show when bandwidth is being consumed the most and what types of Websites are being accessed at these times. Publishing names or offenders can have legal implications.

Network Usage Policy - This is the contract between management, or the owner, and the end-user. It consists of the can-does and don'ts and the repercussions if they must. This is what the administrator using in establishing the baseline.

Network Security Policy - This is the contract between Management and the administrators, especially the Network Security Manager. This allows the audit to be conducted. This allows the auditor to "attempt" to access areas where they as a normal end-user should not be. This is what allows the auditor to challenge the level of end-user passwords…even the CEO. This is what covers the administrator legally! Be the author!

Information Technology Training: Information technology training is imperative for the NOC personnel. Assessing which schools they have been to as well as which schools they must go to is imperative. A good recurring program informal training and required professional reading is also a must in keeping up in the IT world. The risk with too much education is that you are constantly making the individual more "marketable". A good way to counter this is with some very proactive, interesting training…constantly!

The Network Operations Center (NOC) Checklist:

1. Check the physical security of the servers, routers, and other critical connections. Ask yourself if they look like they have been tampered with? Is there an in-place physical security policy?

2. Log into the system as yourself (not as an administrator). Does the terminal act as it did the last time.

3. Check Network Neighborhood for Servers and workstations. Do all critical servers display in the window? Check your baseline in your configuration manual.

4. *Check Cisco Watch (What's Up Gold) for Routers to all the LANs.*

5. Log on your stand alone administrator account.

6. Ping higher HQ.

7. Ping the small sites.

8. Traceroute to the default (gateway) router to determine the path.

9. Surf the Internet to a couple official sites (.mil and .gov.) Do they look tampered with?

10. Check Fsecure Website for updates on viruses and hoaxes.
http://www.f-secure.com/virus-info/hoax/ <http://www.f-secure.com/virus-info/hoax/>

11. Check Symantec Website for updates on viruses and hoaxes.
<http://www.symantec.com/avcenter/index.html>

12. Use some of the Networking Tools that are provide free with windows NT 4.0

Performance Monitor: The Performance Monitor allows the administrator four ways to view information generated by activity on the system: charts, alerts, logs, and reports. I will focus on the use of alerts, which will allow for immediate notification versus historical logs. The following alerts should be set to monitor for attempted security breaches:

Errors Access Permissions - Indicates whether somebody is randomly attempting to access files in hopes of finding an improperly protected file.

Errors granted access - Logs attempts to access files without proper access authorization.

Errors Logon - Displays failed logon attempts, which could mean password guessing programs are being used to crack security on a server.

Windows NT Diagnostics: In lieu of using the Performance Monitor, the administrator can use the following controls can be set using Windows NT Diagnostics:
-Server Password Errors
-Server Permission Errors.

Network Monitor: This monitors network traffic to and from the server at the packet level. The following information can be captured for later analysis: Expressions, Addresses, protocols, and properties of protocols. The simplest capture trigger to use for the Network Monitor is the Pattern Match although there are other options.

Auditing is a very critical part of effective security monitoring controls. System auditing needs to be turned on to be implemented. Auditing consumes many resources including hard drive space and personnel time. Things that can and should be audited are Files and directories, the registry, printers, remote access servers (RAS), and the Event Viewer, which will be discussed below.

Event Viewer: The Event Viewer captures events in one of three logs: system, security, and application. These logs forma the basis for legal and employment decisions.

System logs records, errors, warnings, and information generated by the Windows NT 4.0 Server.

Security logs record events such as valid and invalid logon attempts and others such as creating, opening, and deleting objects.

Application logs record errors, warnings and information generated by application programs.

Netstat -a- | more

This provides the current connection table for the system you are on. This is used to determine the ports open on the server.

NTLast

This command finds all logon information about a server. The use of switches can isolate information (i.e. -r, -f, -I, -s, -n, etc.).

Free Tools from the NT Resource Kit. This kit is a must for truly professional administrators. The following is a list of tools found in the kit that are extremely useful but it is imperative that the administrator use the tools consistently to get better with them. These commands are done at the Command Prompt.

-dumpel.exe (This utility is used to export the contents of Event Viewer to an ASCII file.)

-netsvc.exe (This utility allows you to manage services and drivers on remote machines.)

-adduser.exe (This utility is used to document all users and groups on a server.)

-sysdiff.exe (This utility allows an administrator to automate the installation of software.)

-regdmp.exe (This utility is used to create an ASCII copy of the registry.)

-xcacls.exe (This utility is used to query a single file for the access level of multiple users.)

-perms.exe (This utility is used to query multiple files for the access level of a single user.)

-rasusers.exe (This utility is used to list all users granted dial-in access.)

Finishing the audit and Reporting the results. The audit is continuous and methods to automate it should be considered. Sampling the same information different ways is as important as sampling different things the same way. Ask your peers to interpret some particular information as a way of determining that you are seeing what you think you are. Finally, document the information that you have found, and report what is not consistent with the baseline. Every Server should have a configuration management log and these should be routinely verified. This is the baseline. It is important to understand that this baseline changes as new components get added to the system as well as new configuration standards caused by patches that are applied because of the ever-changing threat.

Crises Management Plan:

It is important to have a Crises Management Plan to cover events that severely affect the network. This plan should cover disasters from natural and man-made causes. It should address Incidents and responding to them, Triage, containment, eradication, and recovery from this devastation. The near final step is the complete follow-up on an event to include documentation and after action reviews. The final step of creating a Crisis Management Plan is the actual implementation of it during a mock scenario. This is the absolute test for the plan.

Conclusion:

A working Network Operations Center (NOC) is a high speed, immediately responsive center that must operate in a proactive mode to be able to react to threats against the network at a moment's notice "Reaction". The NOC's environment should be that of a methodical, preventative maintenance one versus a crisis management mode. Although every attempt should be made to have created a Crises Management Plan (CMP) in place, the ultimate end is never having to remove it from the shelf other than only to test it. The audit within the NOC should be continuous to the point when you have identified an issue, decide if you must stop the audit to take corrective action. The audit should happen between the times established to improve the position of the defense. The audit must be scheduled and strictly enforced. Log the results

There are hundreds of tools available to better manage the NOC and to conduct administration and auditing. Software is available at a price or is free. What you decide to use is only as good as you make it.

References:

1. Jumes, J.G., N.F. Cooper,, P. Chamoun, and T.M. Feinman, "Microsoft Windows NT 4.0 Security, Audit, and Control", Microsoft Technical Reference, Microsoft Press, 1999.

2. National Guard Bureau Network Operations Center Website: <http://nocweb.ngb.army.mil/>

3. Harris, Inc. Security Threat Avoidance Technology: http://www.statonline.com/products/analyzer/analyzer.pdf <http://www.statonline.com/index.asp>

4. Internet Security Systems, Inc. (ISS) Intrusion Detection System (IDS) Manager: <http://www.iss.net/securing_e-business/security_products/intrusion_detection/realsecure_manager/>

5. Network Associates Incorporated, McAffee AsaP: <http://www.mcafeeasap.com/content/virusscan_asap/default.asp>

6. CISCO Corporation What's Up Gold: <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/cwfw/cww_6_0/use_6_0/cww60dt.htm#xtocid1276620>

7. Poor Man's NT Auditing, Track 1: Security Essentials Curriculum 1.3.6, The SANS Institute : http://www.sans.org/momaudio/s=1.3.5/a=i9CTZWKsSAC/audit

8. Fsecure Website: http://www.f-secure.com/virus-info/hoax/ <http://www.f-secure.com/virus-info/hoax/>

9. Symantec Website: http://www.symantec.com/avcenter/index.html

10. University of Indiana's "University Information Technologies Services (UITS): http://www.indiana.edu/~uits/telecom/masterlos.html

11. Aldrich, C, The Justification of IT Training, Decision Framework, DF-11-3614, @2000 by the Gartner Group, Inc., 10 July 2000.