Global Information Assurance Certification Paper

External Name Server Security Audit: An Auditor's Perspective

GIAC Systems and Network Auditor Certification
Practical Assignment 3.1, Option 1

Prepared by:
Jennifer M. Marek
2 May 2004

Table of Contents

Executive Summary

Objective

A security audit was performed on the GIAC Enterprises Inc., external name server (NS), DMZDNS, to determine if the sever is securely configured and maintained using current company policy and industry best practices

Name server overview

The GIAC external name server performs the role of directing incoming Internet traffic to the correct GIAC server once the traffic reaches the outside of the GIAC network. All Internet traffic coming into GIAC Enterprises is sent to the same address "giacenterprises.com" or XXX.XX.30.11 translated into the Internet Protocol (IP) addressing scheme. The external name server then decides which internal network server needs that traffic: (1) email server for email; (2) web server for access to the GIAC web site; (3) authentication server for users who want to authenticate and have remote access to the GIAC intranet, etc.

There are two ways to compromise a server: (1) a vulnerability in the base operating system that runs the server and the name server "sits on"; or (2) through a vulnerability in the name server itself. These vulnerabilities could be exploited through configuration flaws (intentional or unintentional), bad design, or through changes made through during maintenance – again intentional or unintentional.

The secure operation of the external name server is important. If the server was compromised the unauthorized person could gain access to the internal network and servers that store sensitive information, the company's network could be used to launch attacks against other companies, or the network could be used to store illegal information (e.g., stolen credit card numbers, pornography, etc.), denial of service or hijacking of the web address.

Process

The audit was performed to determine if the server was being securely maintained in accordance with company policy and best business practices.

The results and the process of this audit are documented in this report. For confidentiality, all company and network specific information has been omitted, blacked-out or modified in all screen shots.

During the audit process, the high risk items were identified, interviews were held with the network engineers and the server was subjected to several behavioral tests to determine if the server acted in accordance with policy, procedures and expectations.

Results

The major gap identified was the lack of formal procedures and documentation of the name server's configuration, maintenance and operation. However, the configuration and behavior of the name server is as expected – no major gaps, which is surprising considering the lack of formal procedures. An additional gap was noted in the server is not "hardened". There is no antivirus installed and unneeded services were found running.

While the there is only one external name server which is a single point of failure, there are two Internet Service Providers that supplies the network with Internet traffic. Additionally, the design splits out the external name server role and the internal name server role.

Overall, the external name server should be hardened and formal procedures developed, issued and followed.

Part 1: Research in Audit, Measurement Practice and Control

Method

In evaluating the NS, the following steps were followed:

1. *Characterization*. Overview of the company, the external NS and the information assets being protected was developed.
2. *Risk evaluation.* A basic risk evaluation was performed to determine the major threats and risk to GIAC information. The risk evaluation was performed using the National Institute for Science and Technology (NIST) Risk Assessment Guide, SP 800-30:
   a. *Threat identification*[1]*.* Identification of the threat-source, motivation, and threat action was performed for the information assets being protected.
   b. *Vulnerabilities*[2]. Identification of any flaws or weaknesses in the external NS configuration or network design was performed. This includes flaws or weaknesses that could be exploited (accidentally or intentionally) that would create a security breach or a violation of the security policy of the NS.
   c. *Identification and Analysis of the controls.* Controls are put into place to mitigate risks to the NS and the information it is protecting was analyzed. The likelihood[3], defined as the probability a threat-action would be successful was analyzed to determine if the controls in place are sufficient to reduce the risk to an acceptable level for given the information assets.

   d. *Impact*[4]*.* Identified possible effects to the company in the event the threat threat-action was successful.

3. *Degree of Exposure*. The Degree of Exposure is the measurement which the information is at risk assuming given the vulnerability is exploited.
4. *Checklist development and system testing.* A checklist was developed using the risk evaluation and degree of exposure to identify high and medium risks. Industry best practices were then identified for these higher risk items and which were compared to the policies, procedures and network design of GIAC Enterprises. Tests outlined on the checklist were performed.
5. *Findings.* Findings from the tests are outlined in the Finding Tables.

Characterization

Company

The company audited, GIAC Enterprises, is a *medium-sized consulting company* that relies heavily on name recognition and quality of work product (e.g., not being the "lowest bidder") in a highly competitive, small-niche market. The customer base is world-wide which requires *up to 80% travel* for some of the staff. Due to the travel requirements, staff members routinely connect remotely to the network through a SecurID / VPN combination to retrieve work products and to access resources that are only available in the corporate office (access to intellectual property, editors, legal counsel, etc.).

Device being audited

The device being audited is the external NS for the company. This NS provides DNS service to GIAC Enterprises. GIAC Enterprises has two Internet Service Providers that enter the network though the Border router. The Border router is connected to a Firewall. The DMZ is off one of the firewall's interface which the NS being audited resides.

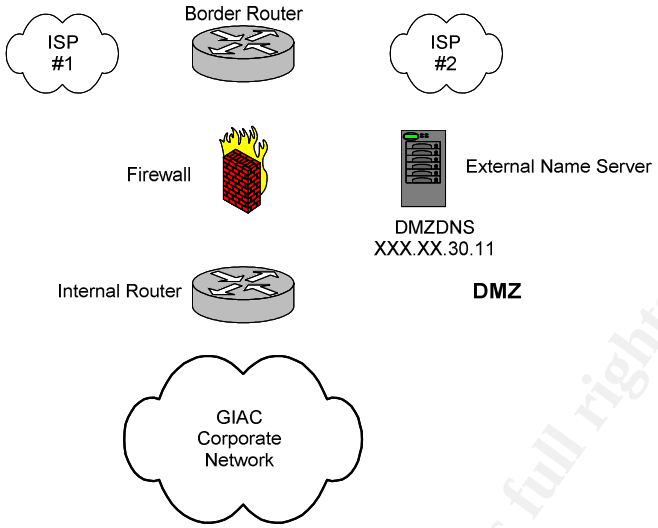


Figure 1: Network Diagram

Device characterization

The NS, DMZDNS, is a Compaq ProLiant DL 380 with a 1000 MHz Intel Pentium III. The server has 640 MB of installed memory. The server is running Windows 2000 Server, Service Pack 3 with Build 2195. A complete server characterization can be found in Appendix A: DMZDNS Characterization.

Role of the NS and how it affects the security of the network

The Name Server, DMZDNS, stores the Internet address information about GIAC Enterprises network [zone]. When a customer, business partner or anyone else wants to contact the GIAC Enterprises web site or send GIAC Enterprises email, the DMZDNS resolves the names to the IP addresses for the needed server (e.g., email server, secure web servers, etc.) the traffic at the network border to the right server. For example, it directs potential customers to the GIAC web site so they can learn more about the company.

As with any database, the DNS database "sits on top" of an operating system. If the database, the server hardware, or the base operating system, has a vulnerability that allows an attacker access to the DNS database or the operating system, the GIAC network could be at risk. The vulnerability could allow unauthorized individuals (possibility malicious) to read, access or use the company's information or electronic resources through the NS.

This name server also serves as an FTP and web server for the company. The audit is focused specifically on the NS portion of the server but the other roles of the server must be considered.

Information Asset being protected

The major information assets that are directed affected by the integrity of the external Name Server are:

	Information asset affected by the external DNS server
1	*Email.* The confidentiality, integrity and reliability of email are vital to a medium-sized consulting firm's profitability. Incoming email that could be directed/incepted routinely contains invoices, contracts, company pricing and bid information as well as company employee's names, personal data (social security numbers) and telephone numbers.
2	*Intellectual Property.* A company's IP integrity, confidentiality and availability rely on the secure working of the NS. While on travel, staff frequently needs to transfer work products / bid proposals and pricing information to inside the corporate network which can only be done through file transfers via VPN (files are too large to be transferred via email). If the traffic between the staff on travel (external user) to the company fileservers (internal to the network) is redirected to malicious people, profits of the company could suffer if the external user is transferring the intellectual property and this information is redirected to a competitor.

Table 1: Major information assets being protected

Threat Identification

A *threat* to a given IT device is defined as the potential for a *threat-source* (e.g., malicious hacker or ignorant user) to do harm, either intentionally or unintentionally depending on the motivation. The threat-source can be an *internal* or *external* source. The *threat-action* is the action that implements the threat.

Although there are many threats to the NS, the two threats identified that pose a significant risk to the company's network and information integrity, reliability and confidentiality are:

	Threat	**Threat-source / motivation**	**Threat-action**
1	*Misconfiguration.* At least 35% of all DNS servers on the Internet have a misconfiguration or are running outdated software that contains security bugs. Bugs and misconfiguration might vary in severity from giving out username information to allowing an attacker to start a privileged program.[5]	• Internal / unintentional o lack knowledge o careless o poorly or untrained o Unintentional errors • Internal / intentional o Ego o Blackmail o Exploitation o Revenge	Hacking Disgruntled user Untrained user Malicious user Careless user Terminated employee Former consultant Corporate espionage
			Disgruntled user

2	*Flawed design.* A network design must consider the security threats when it is being developed or modified. Without such consideration, the network and its information is more likely to be compromised. A high confidence configuration and maintenance program will not protect the network or its information from intruders or natural disasters.	• Internal / unintentional o lack knowledge o careless o poorly or untrained o Unintentional errors • Internal / intentional o Ego o Blackmail o Exploitation • Revenge • Natural disasters	Disgruntled user Untrained user Malicious user Careless user Terminated employee Former consultant Corporate espionage Major power outage that disrupts ISP service Fire Disruptive weather conditions (tornado, hurricane, flood, winter storm, etc.)

Table 2: Threat Identification

Vulnerability

Vulnerabilities are ways in which threats can be realized. NIST defines vulnerabilities[6] as a flaw or weakness in the security procedures, design, implementation or internal controls that could be exploited that would result in a breach of violation of the system's security policy. In summary, a threat is the potential for the threat-source to take advantage of a vulnerability.

Using this definition, the following vulnerabilities of a NS were identified:

Threat	Vulnerability	
1. Misconfig.	**Administrative misconfiguration vulnerabilities**	
	1.1	Patches not tested in a test environment before installing them in a production environment
	1.2	Lack of name server administration policies and procedures
	1.3	Lack of policies and procedures for device monitoring (logs, quantify of traffic, etc.)
	1.4	Lack of configuration management program, policies and procedures
	1.5	Lack of policies and procedures for incident management
	Server misconfiguration vulnerabilities	
	1.6	Latest service packs and revisions of the name server not being applied
	1.7	Authorized but unsecured transfer of zone information between name servers

	1.8	Unauthorized zone transfers to unknown / untrusted servers
	1.9	Services running unneeded on the name server
	1.10	Unsecured file system and registry
	1.11	Dynamic updates not disabled or restricted
2. Design Flaw	2.1	Single point of failure
	2.2	NS split design is not implemented
	2.3	NS not protected by a firewall and router
	2.4	Lack of adequate backup capability
	2.5	No antivirus installed or definitions not up to date
	2.6	NS being used for more than one service (e.g., web server)

Table 3: Vulnerability Identification

Likelihood

For the identified threats and vulnerabilities, the likelihood provides a *probability estimate* a vulnerability will occur in the given environment. In developing the likelihood rating, several factors need to be considered: (1) threat-source motivation and capability; (2) nature of the vulnerability; and the (3) existence and effectiveness of *current* controls.

The likelihood for each vulnerability was evaluated and scored. The likelihood is defined in the terms of High, Medium, or Low. The definitions of these ratings are:

Likelihood Level	Score	Likelihood Definition
High	> 0.5 and $\leq$ 1	The **threat-source is highly motivated** and sufficiently capable, and **controls** to prevent the vulnerability from being exercised **are ineffective**.
Medium	> 0.1 and $\leq$ 0.5	The **threat-source is motivated and capable**, but controls are in place that **may** impede successful exercise of the vulnerability.
Low	$\leq$ 0.1	The threat-source **lacks motivation or capability**, or controls are in place to **prevent, or at least significantly impede**, the vulnerability from being exercised.

Table 4: Likelihood Scoring and Definition

Impact

In the event a threat is successful, the resulting impact to the company was evaluated and scored considering the loss of availability, integrity, and/or confidentiality of the network or the data it stores or processes. The impact is defined in terms of High, Medium or Low which are is defined as follows:

Magnitude of Impact	Score	Impact Definition
High	> 50 and ≤ 100	Exercise of the vulnerability (1) may result in **the highly costly loss** of major tangible assets or resources; (2) **may significantly** violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human **death** or serious injury.
Medium	> 10 and ≤ 50	Exercise of the vulnerability (1) may result in **the costly loss** of tangible assets or resources; (2) **may** violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	≤ 10	Exercise of the vulnerability (1) may result in **the loss** of some tangible assets or resources or (2) **may noticeably** affect an organization's mission, reputation, or interest.

Table 5: Impact Scoring and Definition

Risk identification and evaluation

After considering the two identified threats and corresponding vulnerabilities, mitigating factors were identified. Based of these mitigating factors (e.g., process and procedures in place, network design and operation, etc.) a likelihood score was estimated. Next, it was considered if the vulnerability was successfully exploited, what the impact would be to GIAC Enterprises. The impact estimate was scored. The likelihood and impact scores were multiplied to determine the risk. In keeping with the NIST risk assessment process, risk (R) is defined as likelihood (L) x impact (I). The resulting score defined determined if the risk is High, Medium or Low. The resulting score is interpreted in the following way:

- High = (>50 to 100);
- Medium = (>10, ≤50);
- Low = (1 - 10).

Threat		Vulnerability	Mitigation	Consequences	Likelihood	Impact	Risk (= L * I)	Exposure
1 Misconfig.	**Administrative misconfiguration vulnerabilities**							
	1.1	Patches not tested in a test environment before installing them in a production environment	None; some changes are tested but there is no policy or procedure requiring this to occur	Applying patches prior to testing could "break" or disable security controls increasing the risk to the information	Medium (0.5)	High (95)	Medium (47.5)	Medium
	1.2	Lack of name server administration policies and procedures	None	Untrained administrators could change a security configuration which that would increase the risk to the information	High (1.0)	High (100)	High (100)	High
	1.3	Lack of policies and procedures for device monitoring (logs, quantify of traffic, etc.)	None	Without a program to monitor the network and its logs could increase the detection time for a security event which would increase the exposure time of the network.	High (1.0)	High (100)	High (100)	High
	1.4	Lack of configuration management program, policies and procedures)	Although the Change Control procedure identifies different change levels dependent on the risk and significance of the change, there is no mechanism for "double checking" the engineer when the change is actually made.	Without a formal configuration management program changes can lead to network misconfiguration (e.g., accidentally change network flow, improper change of security settings, etc.	Low (0.1)	High (100)	Low (10)	Low
	1.5	Lack of policies and procedures for incident management	None	Without a formal incident handling program could increase the response time once a security event is identified,	High (1.0)	High (95)	High (95)	High
	Server configuration vulnerabilities							
	1.6	Latest service packs,	The Security Officer,	Service packs, patches and	Medium	High	Medium	Medium

		patches and hotfixes not applied	Network Operations Manager and the Manager of IT all subscribe to multiple vulnerability lists. As a vulnerabilities are announces and patches released, they are applied after going through the change management process. A recognized Configuration Management Team is responsible for approving all changes.	hot fixes often fix vulnerabilities that directly impact the security of the network. If left unpatched then unauthorized individuals could take advantage of the known vulnerabilities.	(0.3)	(100)	(30)	
	1.7	Unsecured authorized transfer of zone information between name servers	Configured to prohibit all zone transfers	If the name server is tricked into a zone transfer the risk is evaluated in 1.8.	Low (0.1)	Low (10)	Low (0.1)	Low
	1.8	Zone unauthorized transfers to unknown / untrusted servers	Configured to prohibit all zone transfers	If the external NS is tricked into performing a zone transfer to an unknown or untrusted servers, the network internal addressing could be exposed to unauthorized individuals who could use the information to launch an attack against GIAC Enterprise and its information.	Low (0.1)	High (100)	Low (10)	Low
	1.9	Services running on server that are not needed	None; no routine reviews are performed on the server	For each additional service that is running, the probability an unauthorized individual could gain access to the network and its information is increased. It the services are turned off all known and unknown vulnerabilities will be eliminated.	High (.85)	High (100)	High (85)	High

		1.10	File system and registry not secured	None	Restrict access to only the users/groups who need access; eliminates the change of an accidental or intentional changing of the zone files and registry. This could result I the incoming Internet traffic being redirected.	High (.85)	High (100)	High (85)	High
		1.11	Disable or restrict dynamic updates	Dynamic updates are not enabled	Anyone who can change records can add, delete or modify existing records which can redirect all incoming Internet traffic.	Low (0.1)	High (100)	Low (10)	Low
2	Flawed Design	2.1	Single point of failure;	None. There is only one NS in the DMZ that supports the company.	If the singe point of failure of failure was to crash or be compromised, the inbound traffic could stop – either through Denial of Service or through traffic diversion. If the traffic was diverted but the rerouted back to the company, the network engineers might not be aware of the condition immediately.	Medium (0.3)	High (75)	Medium (22.5)	Medium
		2.2	NS split design not implemented	The network incorporates a split-design – internal and external NS functions are split to different servers	Internal hosts could be exposed to the Internet if the split design is not employed.	Low (0.1)	High (100)	Low (10)	Low
		2.3	NS not protected by a firewall and router	A firewall protects the DMZ NS	The NS would be open to all attackers.	Low (0.1)	High (100)	Low (10)	Low

	2.4	Lack of adequate backup capability	None	Down time will be increased if the NS needs to be rebuilt.	High (1.0)	High (100)	High (100)	High
	2.5	No antivirus installed or definitions not up to date	Antivirus is not installed.	No way to detect malicious software on the NS.	Medium (0.5)	High (75)	Medium (37.5)	Medium
	2.6	NS being used for more than one service (e.g., web server)	Operating system and services hardened; web server hosts static pages only.	The more services running on a server, the more possibilities for vulnerabilities and exploitation by an authorized person.	High (1.0)	High (95)	High (95)	High

Table 6: Risk and Exposure Identification

Current State of Practice

In researching the best practices for external NS configuration and design, several resources were used; all which can be found on the Internet. For specific references, consult the endnotes.

Configuration& Implementation Guides

1. System and Network Security (SANS)
   http://www.sans.org
   In addition to the course material for securing information systems and networks and step-by-step guides for securing operating systems, SANS also has a great deal of cyber security information on varied topics in their reading room.
2. National Institute for Science and Technology (NIST)
   http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
   Although NIST gets is funding and mandate from Congress to provide best practices and guidelines to the U.S. government information systems, these documents are available free to the general public. While a commercial company might have to adapt the guides for the commercial world, in general these are an excellent starting point.
3. Microsoft
   http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx
   From configuring external name servers and their base operating systems, to identifying the purpose and dependencies of services, the Microsoft web site has a lot of information including checklists for configuring secure servers.
4. CERT Coordination Center
   http://www.cert.org
   CERT Coordination Center is located at Carnegie Mellon University. CERT provides many free security documents that can be used for all operating systems.
5. National Security Agency (NSA)
   http://www.nsa.gov/research/resea00003.cfm
   NSA also provides free configuration guidelines for securing many network devices and operating systems. Again, although NSA mandate is to support government computer systems and networks, these guides are made available to the general public.

Web Resources

1. Google
   http://google.com
   The resource used the most while developing the best practices is Google. Google is a search engine that provides links to many resources like the ones already discussed, but for many that are not know.
2. WindowSecurity.com
   http://www.windowsecurity.com
   This web site provides many resources to the computer and network individual. On the web site are topics such as Email Security Test, Even Scan Log, Security FAQs, Software and White Papers.
3. Security Associates Institute
   http://sainstitute.org
   Security Associates Institute is an organization that provides education and certification in the area of cyber security.

Tools

1. Sam Spade
   http://www.samspade.org/ssw/features.html
   Sam Spade is freeware network query tool. The auditor used it to determine if the DNS server was behaving in accordance with the configuration.
2. NMapWin
   http://www.insecure.org
   NMapWin is the windows version of NMap for the *nix operating system. As described on the web site, NMap is "…designed to rapidly scan large networks, although it works fine against single hosts." NMapWin is a freeware tool.
3. WhatsUpGold
   http://www.whatsupgold.co.uk/
   WhatsUpGold is an easy way to scan the network to obtain an accurate map. It is a commercial product.

Part 2: Create an Audit Checklist

Checklist development

An Audit Checklist was developed which provides the auditor a road map for each of the vulnerabilities. The vulnerabilities are logically separated in to the following groups:

1. Administrative [A]: Administrative actions/items that are needed to ensure the secure operation and maintenance of the external NS; these items generally address procedures, policy, documentation and training;
2. Configuration [C]: Configuration actions that are needed to ensure the continued secure operation of the external NS; this is independent of the design of the network;
3. Design [D]: This audit group is based on the design of the network.

Then each item in the checklist includes:

1. Item Number: Unique identifier of the checklist item (e.g., A1)
2. Title: Unique title of the checklist item
3. Objective: Goal of the checklist item
4. References: Source used in developing the checklist item best practices
5. Vulnerabilities: Each vulnerability has a unique vulnerability number (Table 2: Vulnerability Identification); the complete description of the vulnerability and associated risk and exposure can be found in *Table 6: Risk and Exposure Identification* above.
6. Risk: Identifies the risk if the vulnerability is exploited
7. Compliance Criteria: Describes the criteria used to determine if external NS is in compliance with this item
8. Test procedure: Describes the steps test and the steps taken to determine if the item is in compliance; a grade of pass or fail will be given
9. Objective / Subjective: Categorizes the test as either objective or subjective

Checklists and testing procedures

Item Number: A1	**Title: Change and Configuration Management Policies and Procedures**
Objective: Adequate administrative procedures for change and configuration management	
References: 1. [WINDOWSECURITY-01][7] 2. [CIO-01][8] 3. [SANS-01][9] 4. [SANS-04][10] 5. [WINDOWSECURITY-02][11]	

Vulnerability:

(1.1) Patches not tested in a non-production environment before applying to a production environment could create additional security vulnerabilities for a specific environment by "breaking" a security feature of the design.

(1.2) Lack of name server administration policies and procedures could allow for untrained staff to make changes and negatively impact the security information

(1.4) Lack of configuration management program, policies and procedures can lead to network misconfiguration

Risk:

No formal and enforced policies and/or procedures for making, controlling testing, and documenting changes can lead to misconfiguration of the network which would increase the risk of unauthorized use or access to company sensitive information.

Compliance Criteria:

Are formal policies and procedures developed and being followed? If not, the system is not in compliance.

Test Procedure:

1. Interview Network Operations Manager for policies and procedures.
2. Interview network engineers to see if standards and/or procedures are being followed
3. Observe the change process (change control meeting, review documentation, etc.)
4. Determine if the policies and procedures are being followed and if they conform to best practices. At a minimum the following should be identified:
    - Who may make changes
    - When changes may be made
    - Testing of changes
    - Documentation of changes – before and after the change (e.g., what will be changed and if the change is successful)
    - Approval of changes
    - Notification of changes

Objective/Subjective? Objective & Subjective

The test is objective and subjective.

1. Either there are formal documented policies and procedures or not (objective).
2. Are the policies and procedures being followed? [If the policies and procedures are not well written, judgment must be used to determine if

they are being followed]. (objective and/or subjective)
3. Do the policy and process follows best practices with regards to the specific situation at the company. (subjective)

Item Number: A2	**Title: NS monitoring**
Objective Determine if formal policy and procedures exist and being followed for NS monitoring and log capture / review	
References: 1. [WINDOWSECURITY-02] 2. [SANS-02][12] 3. [NIST-02][13]	
Vulnerability: (1.3) Lack of policies and procedures for device monitoring (logs, quantify of traffic, etc.) could increase the detection time for a security event which would increase the exposure time of the network and its information	
Risk: Without a known baseline and operational logs, it is almost impossible to know if the NS is operating properly – either from malfunction or from malicious acts. Additionally, there is no way of knowing if the NS is under attack without these items.	
Compliance Criteria: Are formal policies and procedures developed and followed for NS monitoring and log capturing and review? If not, the system is not in compliance.	
Test Procedure: 1. Interview Network Operations Manager for standards and/or procedures to understand the required log and device monitoring procedures / requirements. 2. Interview network engineers/administrators to determine if they know and understand the policies and procedures for NS monitoring and log review. 3. Review work products from device monitoring / log reviews (e.g., incident report stating the incident found during review, etc.). 4. Observe a system administrator or network engineer performing a log review.	

5. Review the policies and procedures; are best practices implemented including:
   a. Identification of responsibility for monitoring
   b. Frequency of monitoring
   c. Method for monitoring
   d. Definition of an anomaly
   e. Actions if an anomaly found (can reference incident response / handling procedures)
   f. Development, storage and maintenance of baseline documentation

Objective / Subjective? Objective & Subjective

The test is objective and subjective.

1. Either there are formal documented policies and procedures or not (objective).
2. Are the policies and procedures being followed? [If the policies and procedures are not well written, judgment must be used to determine if they are being followed.]. (objective and/or subjective)
3. Do the policy and process follows best practices with regards to the specific situation at the company. (subjective):

Item Number: A3	**Title: Incident Handling Program**

Objective:

Determine if there is a formal incident handling program established and followed in the event the external NS is down or a compromise is suspected

References:

1. [NIST-03][14]

Vulnerability:

(**1.5**) Lack of policies and procedures for incident management could increase the response time once a security event is identified.

Risk:

Incident response and management has become a required part of an IT security program. Only through fast identification of and reaction to incidents, can the losses and destruction be minimized and services restored.

Compliance Criteria:

Do formal incident handling policies and procedures exist and being followed? If not, the system is not in compliance.

Test Procedure:

1. Interview Network Operations Manager for standards and/or procedures to understand the incident handling process.
2. Interview the network engineers / administrators to see if they understand the incident handling policies and procedures.
3. Review work products submitted that support the incident policies and procedures (incident reports, etc.).
4. Review the policy and procedures (general and desktop); do they include:
   a. Definition of incident including classifications
   b. Policy on sharing information with outside parties
   c. Roles and responsibilities
   d. Actions if incident identified including:
      i. Notifications, including timing
      ii. Time permitted to classify
      iii. Documentation
      iv. Analysis
      v. Evidence Gathering and Handling
      vi. Eradication and Recovery
      vii. Post-Incident Activity (Lessons learned, evidence retention)

Objective/Subjective? Objective & Subjective

1. Either there are formal documented policies and procedures or not (objective).
2. Are the policies and procedures being followed? Review documentation of a recent incident [if the policies and procedures are not well written, judgment must be used to determine if they are being followed.]. (objective and/or subjective)

Item Number: C1	**Title: Installation of service packs, patches and hotfixes**

Objective:

Determine if current service packs, patches and hotfixes that have been applied; determine if these are the latest and if not, rational for not having the latest applied.

References:

1. [WINDOWSECURITY-02]
2. [CERT-01][15]

Vulnerability:

(**1.6**) Latest software updates, service packs, patches and hotfixes not applied
Risk: Latest service packs, patches and hotfixes should be applied to keep known software vulnerabilities from being exploited.
Compliance Criteria: Are the latest software update, service packs, patches and hotfixes applied? If not the system might not be in compliance - there might be a valid reason not to apply the latest revision or patch.
Test Procedure: 1. Identify the revision and service packs and patches installed on the NS by using Belarc Advisor[16] that lists all of the installed service packs and patches. a. Purchase and download the tool Belarc Advisor[17] 2. Determine the latest revision and patch level using *Microsoft Security Bulletin Search*[18] 3. If the latest available revision and patches are not applied, talk to the Network Operations Manager to determine if there is a valid reason for applying them. 4. Search for published vulnerabilities on CERT at www.cert.org for the installed services and DNS version.
Objective / Subjective? Objective / Subjective 1. Are the latest revision and patches are applied (objective) 2. If the latest patches and revisions not applied, there might be valid reasons for not updating the system. (subjective)

Item Number: C2	**Title: Secure zone transfer between trusted NS only**
Objective: Secure zone transfer to authorized servers only	
References: 1. [SANS-03][19] 2. [WINDOWSECURITY-01]	
Vulnerability: (**1.7**) Unsecured transfer of zone information	

Risk:

The NS information contains all the network hierarchical configuration and addressing information for the internal network. If a malicious person could sniff zone information during a zone transfer, he/she could use this information to perform DNS spoofing / DNS poisoning.

Compliance Criteria :

Are the zone transfers encrypted using strong encryption? If not, the system is not in compliance.

Test Procedure:

1. Review the network configuration with the Network Operations Manager
   a. Are zone transfers permitted?
   b. What is the transfer path?
   c. Is the transfer encrypted? What algorithm?
2. Does the server configuration support the Network Operations Manager answers? Check the configuration:
   a. Start up the DNS Management Console

[Many times the administrator will put a short cut on the desktop. If it is not there, the default path is: C:\WINNT\SYSTEM32\dnsmgtm.msc]

   b. Expand the tree to see all the DNS zones
   c. Expand the zone you are interested in
   d. Right click on that NS and select "Properties"
   e. Look under the tab, ***Zone Transfer*** to see if the server is configured to perform zone transfers
3. If zone transfers are permitted, verify the zone transfer by sniffing the traffic using a tool such as ethereal.

(Note: This might require the auditor to go to other network devices. This will depend on the network and if the zone is being transferred inside the network or between WANs so detailed instructions not provided here.)

Objective/Subjective? Objective

If zone transfers are permitted, is the encryption algorithm used 3DES[20] or later? If not, the system is not in compliance.

Item Number: **C3**	**Title:** **Zone transfers to unknown / untrusted servers**

Objective:

Determine if zone transfers to unknown / untrusted servers is allowed

References:

1. [NSA-01][21]
2. [SANS-04]
3. [SANS-05][22]

Vulnerability:

(**1.8**) Zone transfers to unknown / untrusted servers[23]

Risk:

If the external NS does not specify trusted servers by IP address, that may receive a zone transfer, the NS might be tricked in to transferring zone information to an untrusted / unknown server.

*[Note: If a malicious person conveniences the external NS their server is a "trusted" server they can initiate a zone transfer. This is known as **zone stealing**.]*

Compliance Criteria:

Are untrusted / unknown servers allowed to initiate a zone transfer? If so, the system is not in compliance.

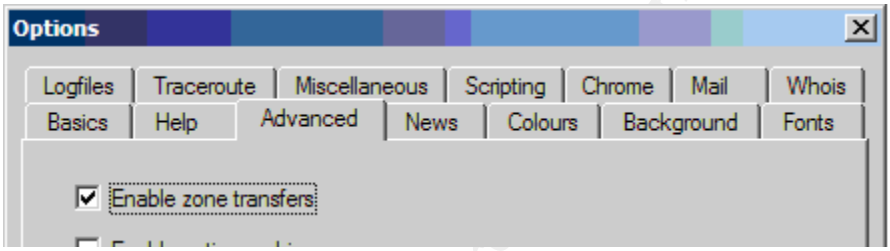
Test Procedure:

1. Look at the configuration:
   a. Start up the DNS Management Console

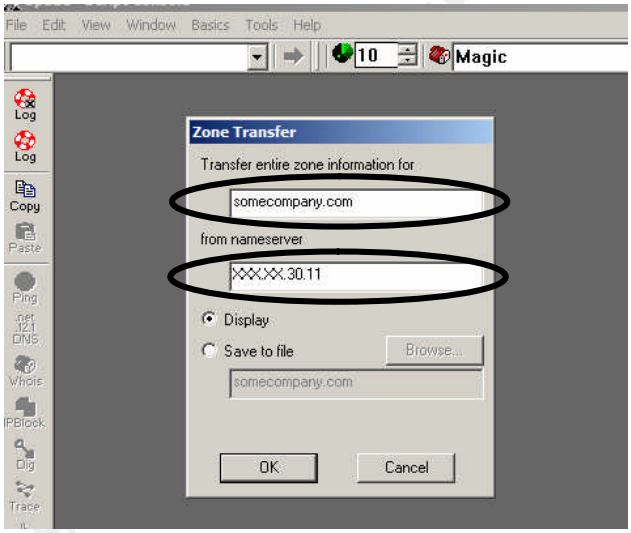
   [*Many times the administrator will put a short cut on the desktop. If it is not there, the default path is: C:\WINNT\SYSTEM32\dnsmgtm.msc*]
   b. Expand the tree to see all DNS zones
   c. Expand the zone you are interested in
   d. Right click on that NS and select "Properties"
   e. Look under the tab, ***Zone Transfer*** to see if the server is configured to perform zone transfers (box checked that says, "Allow zone transfers")
   f. If box is checked to allow zone transfers, the radio button "Only to the following servers" should be selected and list of IP addresses should be below.
2. If the server is not configured to allow zone transfers, test this through a ***nslookup*** command:
   g. From a computer with Internet access go to start => run, type in "cmd", <return>
   h. Type in "nslookup"
   i. Type in "server [server name] (e.g., DNSSERVER.somecompany.com)

j. Type "ls [domain name] (e.g., somecompany.com) *[Note: that is lowercase "L"]*
k. If the query is refused, the zone transfer is refused.

3. Another method of identifying the external NS allows zone transfers is to use the tool Sam Spade[24].
   a. Down load the free tool from: http://www.samspade.org/ssw/features.html
   b. Install Sam Spade and start it up
   c. Under *Edit* => *options* => *Advanced* tab check "Enable Zone Transfers"



   d. click OK
   e. Under *Tools* select *Zone Transfer*
   f. Enter the zone name and the IP address:



   g. Click OK and the results will either go to the screen or a text file depending on what you choose.
   h. If the results returned states "**Query refused",** the zone information will not be transferred.

Objective/Subjective? Objective

Either the NS performs zone transfer to untrusted/unknown servers or it doesn't. If a zone transfer to an untrusted source is permitted, the system is not in compliance.

Item Number: C4	**Title: Disable all unneeded services on the NS**

Objective:

Determine if all unneeded services are disabled.

References:

1. [NSA-01]
2. [WINDOWSECURITY-01]
3. [SYSTEMEXPERTS-01][25]

Vulnerability:

(**1.9**) Services running on server that are not needed

Risk:

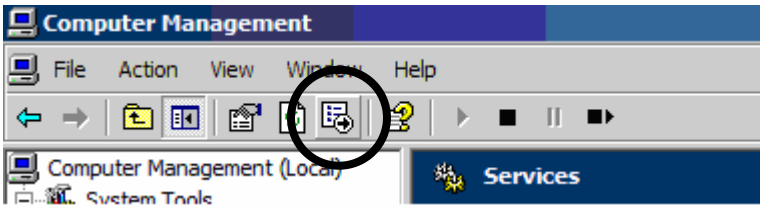
For every service that is left running on a NS which is no needed provides the malicious person an opportunity to exploit the server. May of the services (IIS) for example are not needed but are installed by default for Windows 2000 operating systems. IIS has many vulnerabilities and patching for IIS vulnerabilities for a NS would be easy to dismiss by a network administrator since it would not be intuitive that IIS should be running on a NS.

Compliance Criteria:

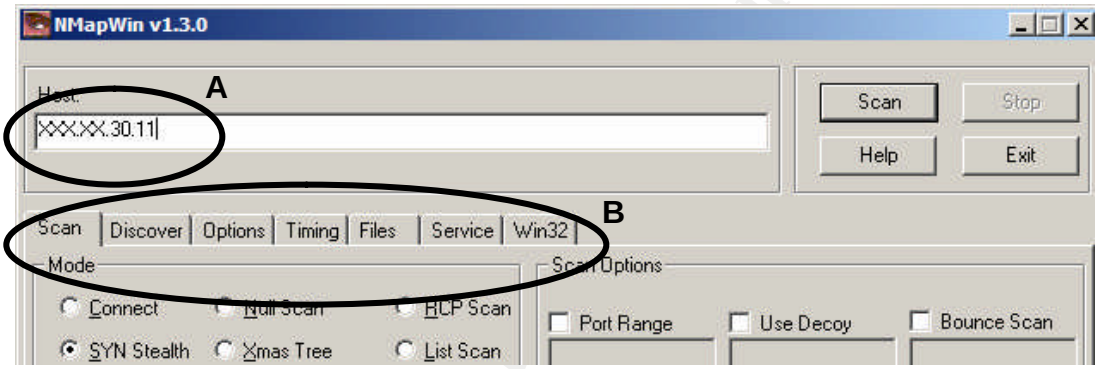
Are all unneeded services disabled? If not, the system is not in compliance.

Testing Procedure:

1. Talk to the Network Operations Manager and determine the services the server performs to determine which services are necessary[26]
2. Check the services under the operating system
   a. From the desktop of the Server, right click on the ***My Computer*** icon; (***Note:*** if the My Computer icon is not on the desk top, the default location is: c:Windows\System32\services.msc)
   b. Expand the tree to see "Services and Applications" listed; Expand the "Services and Applications" tree
   c. Double-click on "Services";
   d. You can export the services information for later reference by clicking on the export icon:



3. Run an external scan with NMapWin[27] to determine if any services are running with ports open that are not listed in the Computer Management Console – Services.
   a. Download and install the free tool NMapWin (windows based NMap)
   b. Run NMapWin with the following items entered / selected:



   - Enter the Host IP (**A**) that is desired to be scanned
   - Check the following options on the tabs (**B**):
     - Scan: Syn Stealth (-sS)
     - Discovery: TCP + ICMP (-PI –PT)
     - Options: OS Detection (-O)
     - Timing: Normal (-T 3)
     - No input for Files, Service, Win32

   c. Click "Scan"
4. Compare the external scan to the internal services listed.
5. How does the list compare to the best practices for the services the server performs? Ask Network Operations Manager if the reason for deviating from Best Practices.

Objective/Subjective? Objective

Either the unneeded services are disabled or they are not.

Item Number: C5	**Title: Security of the file system and registry**

Objective:

Security of the file system and registry of the NS

References:

1. [NSA-01]
2. [WINDOWSECURITY-02]

Vulnerability:

(**1.10**) File system and registry not secured

Risk:

To keep unauthorized users from identifying or modifying the locate of the zone files, the folder and registry settings should configured to limit permissions to *full control* to System and Administrator groups only.

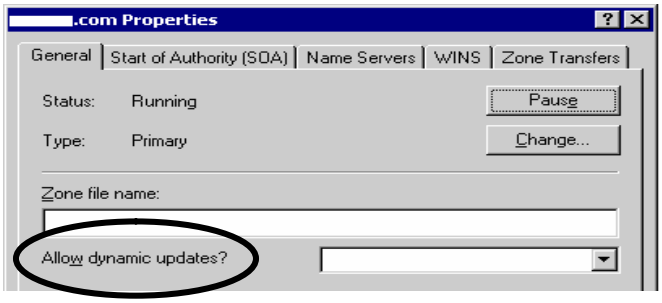
Compliance Criteria:

Is the file system and registry secured? If not, the system is not in compliance.

Testing Procedure:

1. Check the permissions on the *%SystemDirectory%\DNS* folder, subfolders and files – should only be System with Full Control
   a. Find the above folder on the server;
   b. Right click on the folder ad select "Properties";
   c. Select "Security" tab and then the "Advanced" button at the bottom of the pop-up window;
   d. This screen will show all users who have permissions to the folder and what those permissions are.
2. Check the Registry Key: *HKEY_LOCAL_Machines\System\CurrentControlSet\Services\DNS* with only the Administrator and System groups having Full Control. No other groups present.
   a. Find the above registry key:
      i. Start => run => type in "regedit" <return>
      ii. Locate the registry key by following the path above (e.g., *HKEY_LOCAL_ …)*
   b. Right click on the folder ad select "Properties";
   c. Select "Security" tab and then the "Advanced" button at the bottom of the pop-up window;
   d. This screen will show all users who have permissions to the folder and what those permissions are.

Objective/Subjective? Objective
Both the file system and registry are secure or not.

Item Number: C6	**Title: Disable dynamic updates for the NS**
Objective: Determine if dynamic updates are disabled.	
References: 1. [NSA-01] 2. [CERT-01]	
Vulnerability: (1.11) Disable or restrict dynamic updates	
Risk: If updates to the NS are automatic without any additional precautions, the risk is increased since an outside authorized updater could add, delete, or modify zone records.	
Compliance Criteria: Are dynamic updates allowed (Microsoft default configuration)? If so, the system is not in compliance.	
Testing Procedure: 1. Check the configuration: a. Start up the DNS Management Console; [*Many times the administrator will put a short cut on the desktop. If it is not there, the default location is: C:\WINNT\SYSTEM32\dnsmgtm.msc*] b. Expand the tree to see all the DNS zones; c. Expand the zone you are interested; d. Right click on that NS and select "Properties"; e. Under the tab "General" check to see if Dynamic Updates are performed per the configuration:  	

2. Confirm that configuration setting by using ipconfig:
   a. Configure the client computer to use the NS being audited to provide the IP address: My computer=> right click on "Local Area Connection" => Under "General" tab, select "Internet Protocol (TCP/IP) and click "Properties" => select "Use the following IP address:" and type in an address on the same subnet as the NS => select "Use the following DNS Server" and type in type DNS server address
   b. From the command prompt type "ipconfig /registerdns"
   c. If the NS responds, the NS automatically updates.

Objective/Subjective? Objective

Either the dynamic updates are allowed or not.

Item Number: D1	**Title: Single Point of Failure**

Objective

Review design to determine if a single point of failure exists

References:

1. [WINDOWSECURITY-01]
2. [SANS-04]
3. [CERT-01]

Vulnerability:

(2.1) Single point of failure;

Risk:

Single point of failure could affect the availability of the data by leading to a denial of service if there is a failure at the single point.

Compliance Criteria:

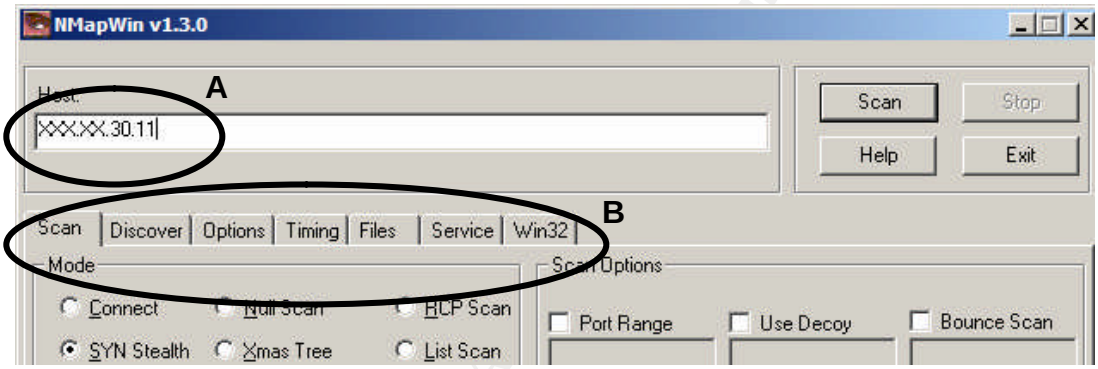
1. Is there a single point of failure? If so, the system is not in compliance.

Testing Procedure:

1. Review the network design with the Network Operations Manager
2. Look for these common Single points of failure:
   a. NS on a single subnet
   b. Behind a single router
   c. Behind a single leased line

d. DNS using the same server for internal and external server

3. Interview the IT Manager and determine if any identified single points of failure are know and acceptable to management.
4. Run NMapWin[2829] to map the network to determine of the external network is configured as the Network Operations Manager outlined
5. Download and install the tool NMapWin on your client machine;
   a. Configure the tool to scan the network, politely;
   b. Identify the network to scan under "Host"; to scan the entire network you can use a netmask (e.g., the auditor used 10.XXX.0.0/16 to scan the entire internal network);
   c. Run NMapWin with the following items entered / selected:



- Enter the Host IP (**A**) that is desired to be scanned
- Check the following options on the tabs (**B**):
  - Scan: Syn Steath (-sS)
  - Discovery: TCP + ICMP (-PI –PT)
  - Options: OS Detection (-O)
  - Timing: Normal (-T 3)
  - No input for Files, Service, Win32

   d. Click "Scan"

Note: While running the scan, the auditor noticed the scan type under the "Scan" tab reverted to the default. Check this tab again before you start the scan.

Objective/Subjective? Objective & Subjective

Either there is a single point of failure or there isn't (objective). Due to the disaster recovery plans and tolerance for down-time, a single point of failure might be acceptable to management.

Item Number: D2	**Title:** NS Split Design
Objective:	

Determine if the NS design employed is a split design

References:

1. [CERT-01]

Vulnerability:

([2.2](#)) Internal hosts could be exposed to the Internet if a NS split design is not used

Risk:

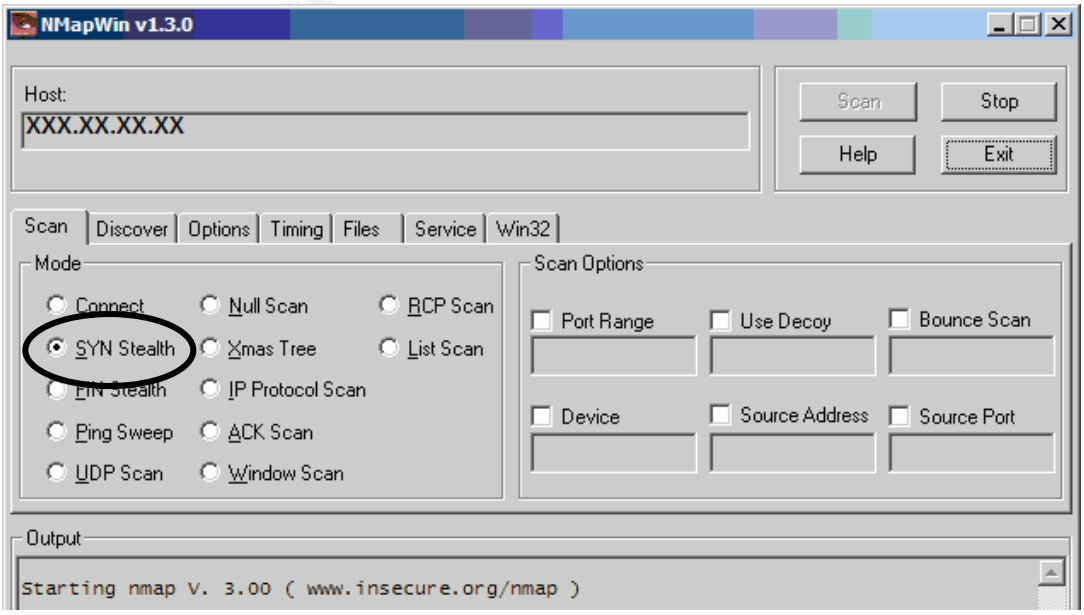
Unless different NS on the internal side of the network and one for the Internet, different policies for the different roles cannot be applied and therefore increasing the risk.

Compliance Criteria:

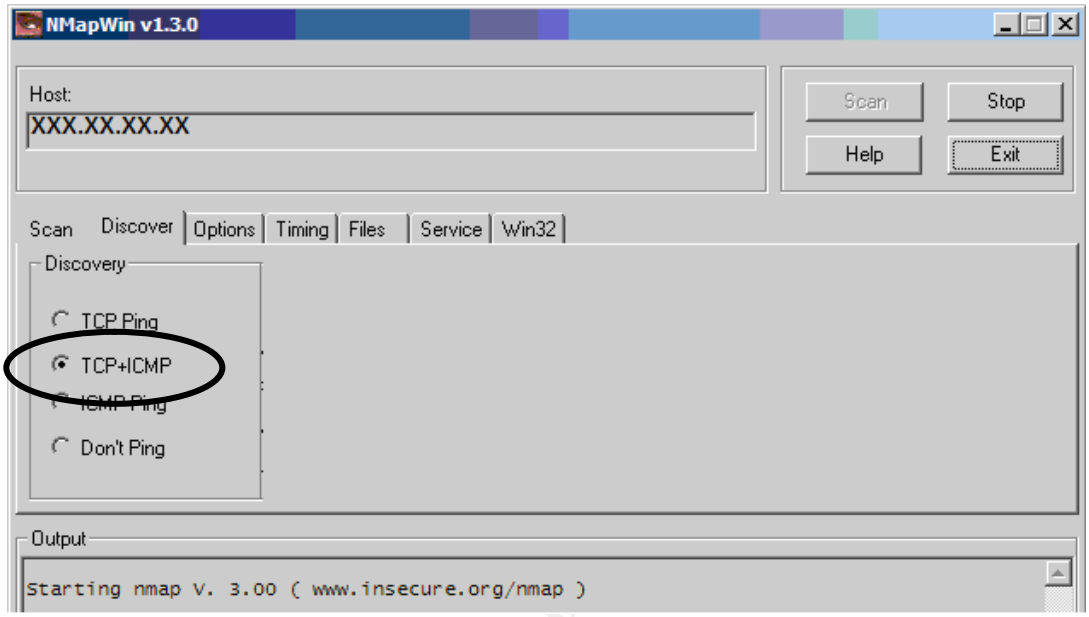
Is a split NS design implemented? If not, the system is not in compliance.

Testing Procedure:

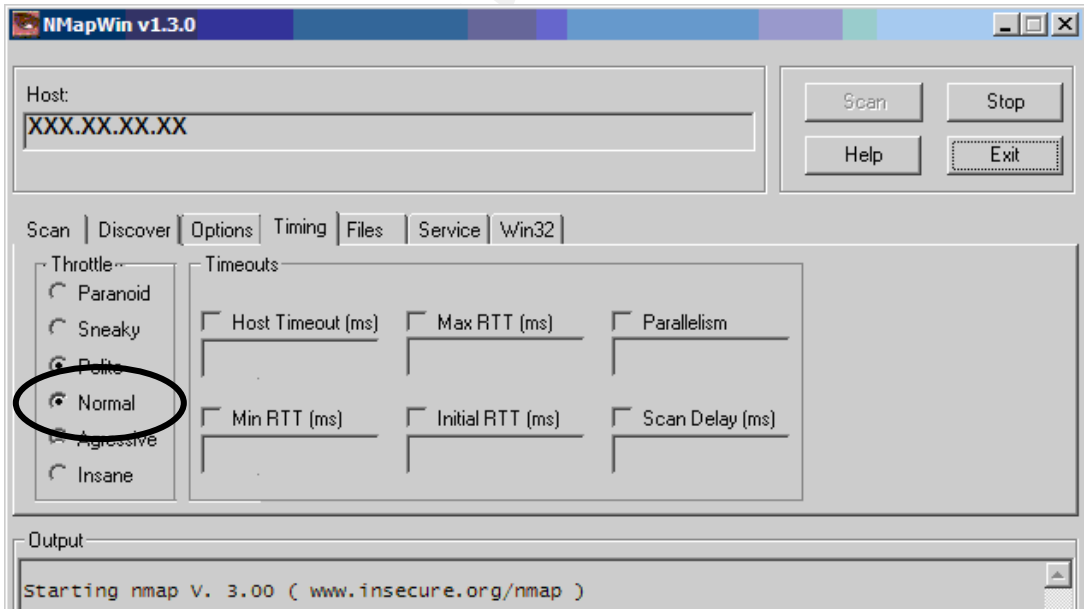
1. Run NMapWin[3031] to map the network to determine of the *external* border devices of network are configured as the Network Operations Manager outlined:
   a. Download and install the tool NMapWin on your client machine;
   b. Configure the tool to scan the network;
   c. Identify the network to scan under "Host"; to scan the entire network you can use a netmask (reference the NMapWin help ("man") pages for specific help);
   d. Under the "Host" tab: select "Syn Stealth".



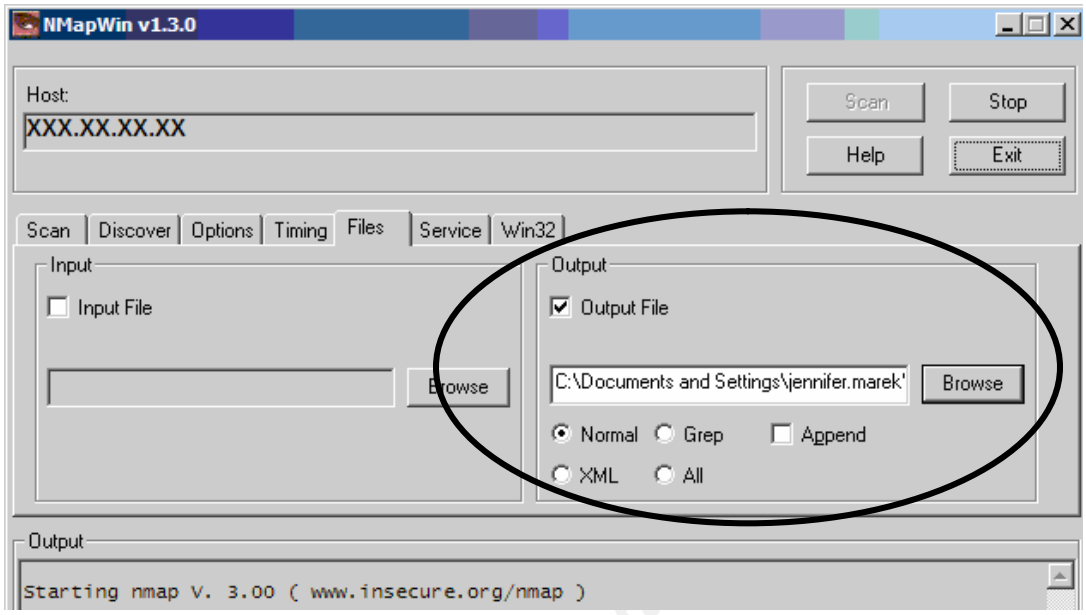
e. For the "Discover" tab, select the "TCP+ICMP" option. This will probe all devices without having they to send a "SYN" and tie up system resources in answering the scan.



f. Select "Normal" timing. The is the NMApWin default so not to overload the network but not skipping any ports either:



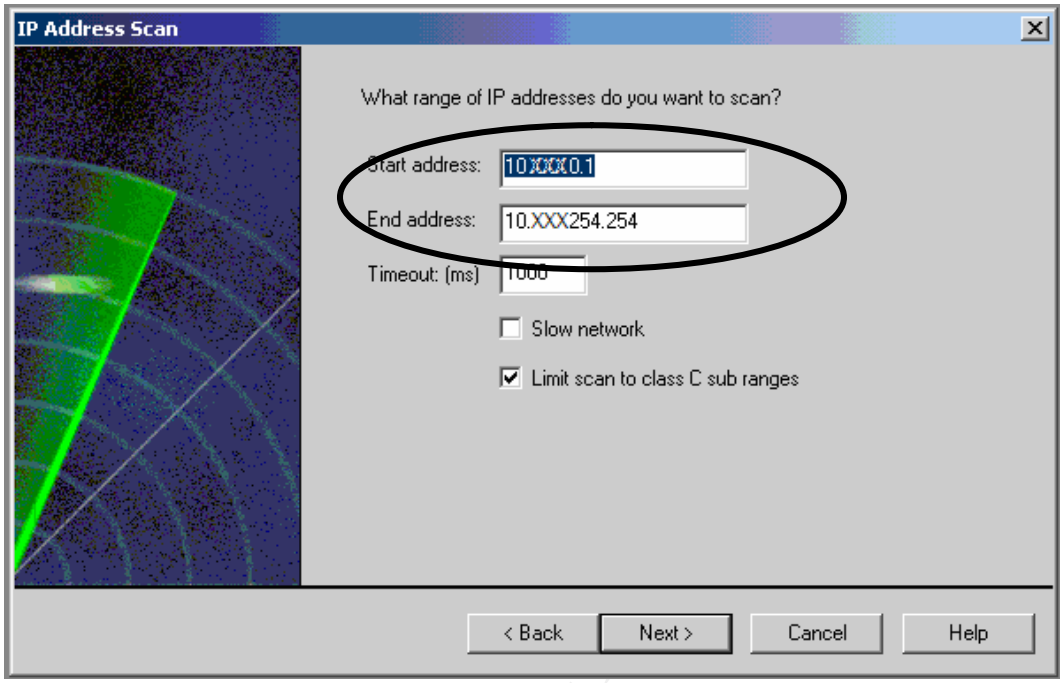
g. Direct the output to a text file so you can keep the results for reference later. Do this under the "Files" tab:



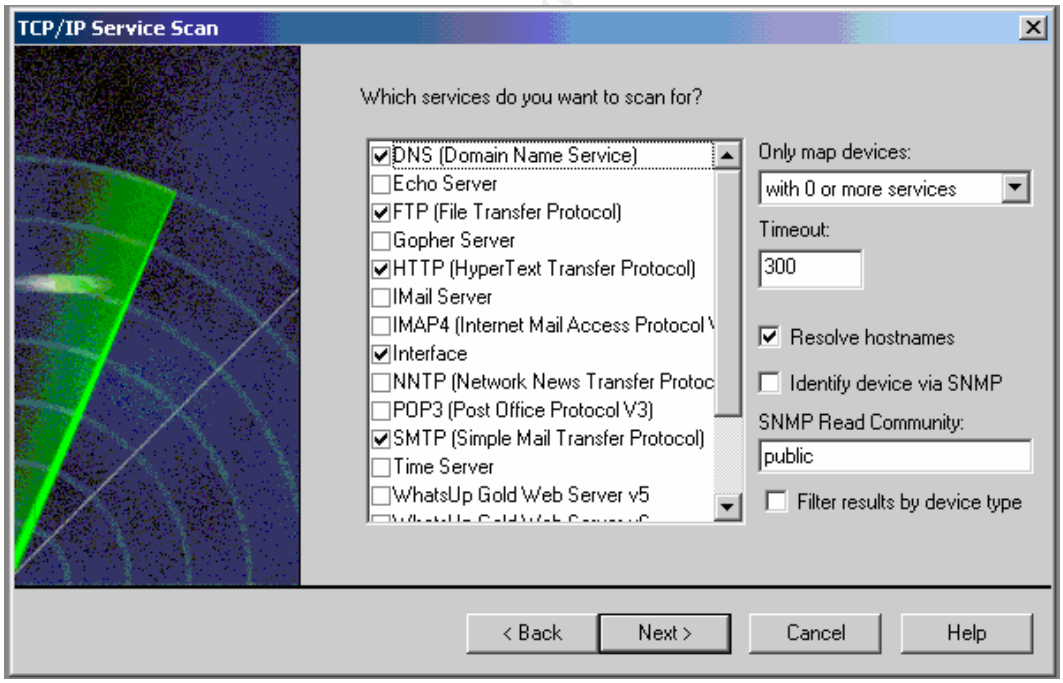
h. For the last two tabs, keep the NMapWin default settings.
i. Click "Scan" button.

Note: While running the scan, the auditor noticed the scan type under the "Scan" tab reverted to the default. Check this tab again before you start the scan.

2. To confirm the *internal* network configuration, run the tool *WhatsUpGold*[32].
   a. Start up the application;
   b. Follow the path: Tools => Discover Devices;
   c. Identify the network to scan:



d. Select the services you want to scan for:

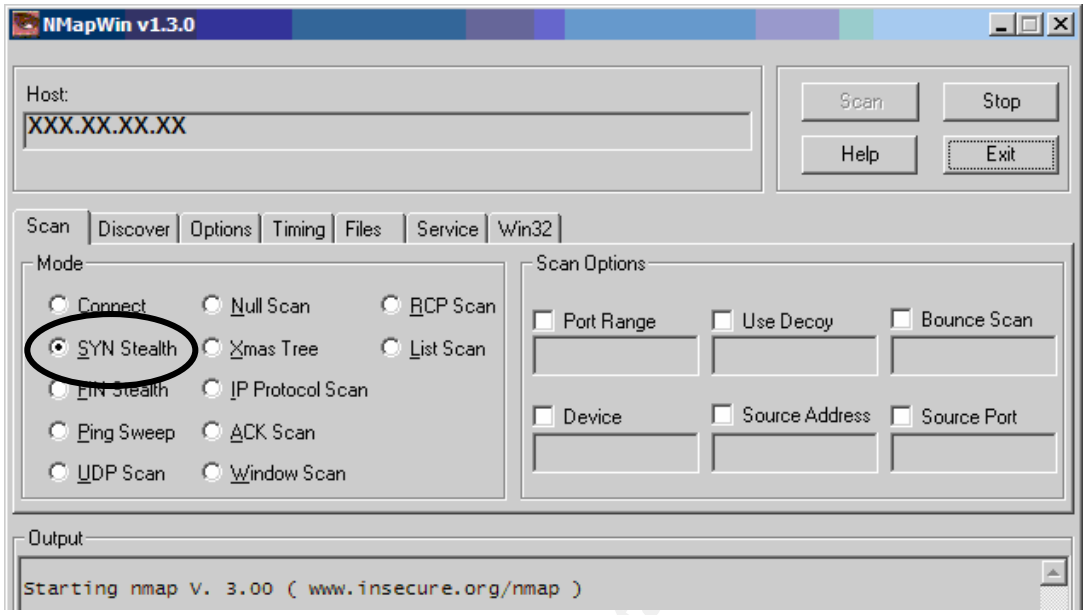


e. Follow the screens and start the scan

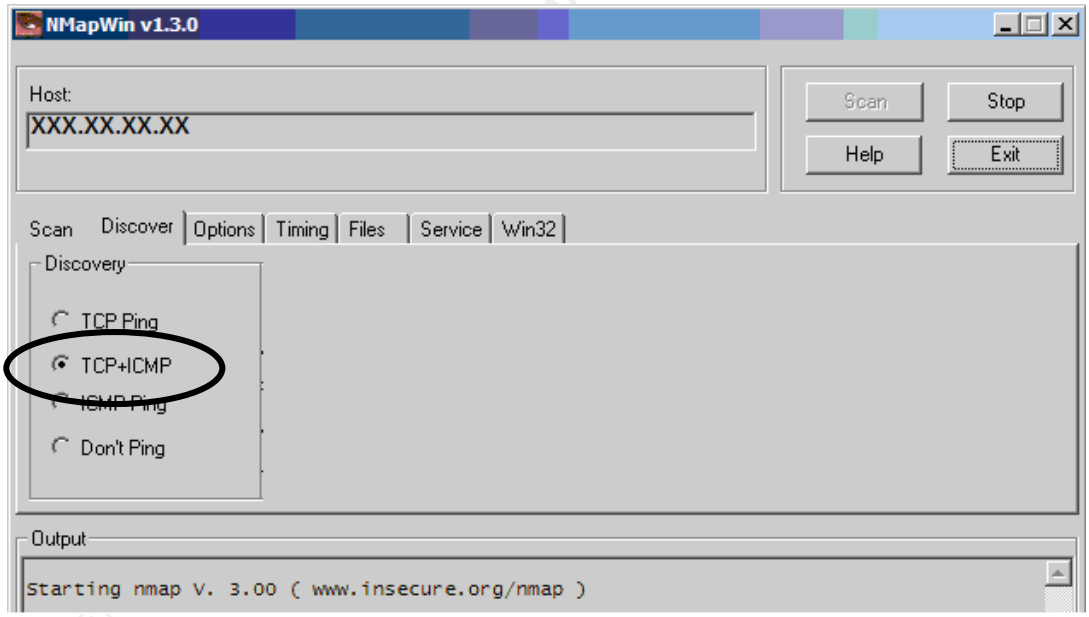
Objective/Subjective? Objective

Either the design is based on split NS operations or it isn't

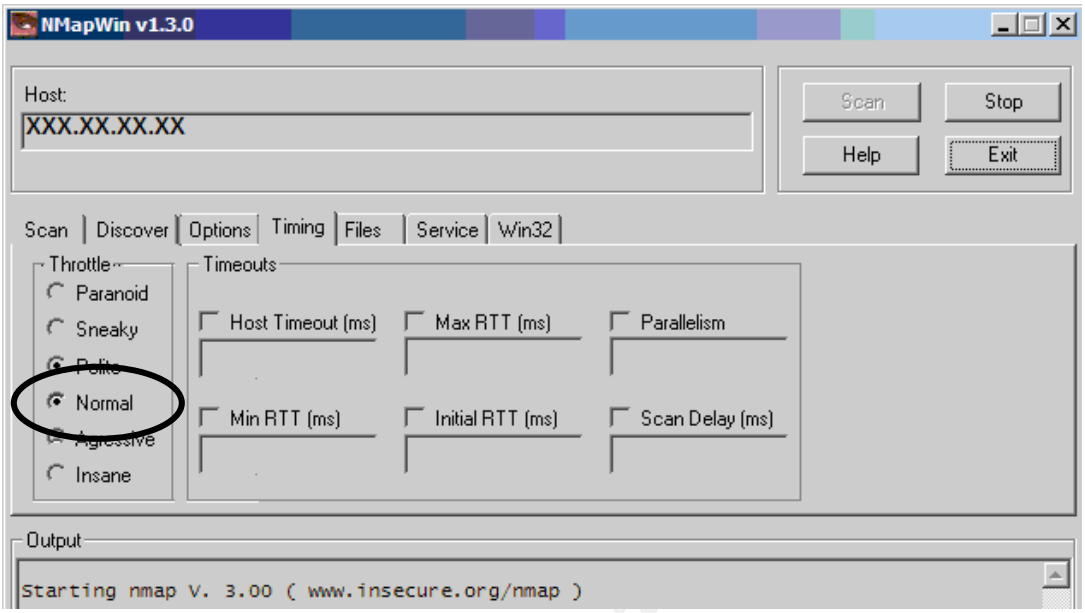
Item Number: D3	**Title: NS DMZ Protection**
Objective: Determine if the external NS is protected by a DMZ	
References: 1. [CERT-01]	
Vulnerability: (**2.3**) NS not protected by a firewall and router	
Risk: NS not protected by a firewall and router "may allow an intruder to compromise the name server and take control of the host. This often leads to further compromise of the network."[33]	
Compliance Criteria: Is the external NS protected in a DMZ by a firewall and border router? If not the system is out of compliance.	
Testing Procedure: 1. Review the network design with the Network Operations Manager 3. Run NMapWin[3435] to map the network to determine of the *external* border devices of network are configured as the Network Operations Manager outlined: j. Download and install the tool NMapWin on your client machine; k. Configure the tool to scan the network; l. Identify the network to scan under "Host"; to scan the entire network you can use a netmask (reference the NMapWin help ("man") pages for specific help); m. Under the "Host" tab: select "SYN Stealth".	



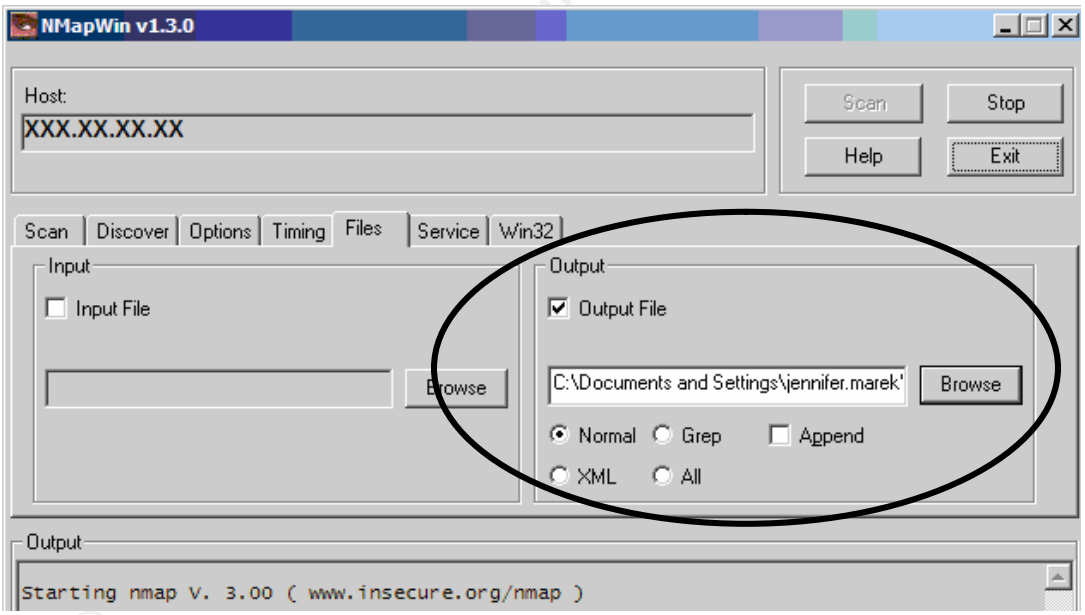
n. For the "Discover" tab, select the "TCP+ICMP" option. This will probe all devices without having they to send a "SYN" and tie up system resources in answering the scan.



o. Select "Normal" timing. The is the NMApWin default so not to overload the network but not skipping any ports either:



p. Direct the output to a text file so you can keep the results for reference later. Do this under the "Files" tab:



q. For the last two tabs, keep the NMapWin default settings.

r. Click "Scan" button.

Note: While running the scan, the auditor noticed the scan type under the "Scan" tab reverted to the default. Check this tab again before you start the scan.

Objective/Subjective? Objective

Either the external NS is protected by a firewall and router or it isn't.

Item Number: D4	**Title: NS Backup**
Objective Determine if the NS is being backed-up	
References: 1. [WINDOWSECURITY-01]	
Vulnerability: (**2.4**) Lack of a good backup	
Risk: Lack of a good backup will increase the down-time if the NS is compromised or fails	
Compliance Criteria: Is the NS being backed up on a regular basis? If not, the system is not in compliance.	
Testing Procedure: 1. Review the backup strategy, policy and procedures with the Network Operations Manager 2. Witness a backup and restore	
Objective/Subjective? Objective Either the NS is being backed up or it isn't	

Item Number: D5	**Title: NS Protected by Anti-virus**
Objective Determine if the NS is protected from malicious software by anti-virus and the definitions are up to date.	
References: 1. [SANS-06][36]	
Vulnerability: (**2.5**) No anti-virus installed or definitions not up to date.	
Risk:	

Without an anti-virus software program on the server with current definitions, there is no way to detect if malicious software infects the NS.
Compliance Criteria: Does the NS have anti-virus program installed? Are the definitions up to date?
Testing Procedure: 1. Interview the Network Operations Manager and determine if anti-virus is loaded on the server and how (and how frequently) the definitions are updated. 2. Confirm the results of the Network Operations Manager: a. Logon on to the NS and search the server for anti-virus. b. f anti-virus is installed, check the definition date (for the more popular anti-virus programs, double-click on the icon at the bottom right of the screen or go to the Programs folder and open the folder with the anti-virus program and get the definition date and revision number). c. Go to the anti-virus web page and get the latest definition date and revision number d. Compare the anti-virus manufacturer's definition date and revision number to the one on the NS.
Objective/Subjective? Objective Either the NS has anti-virus installed with updated definitions or not.

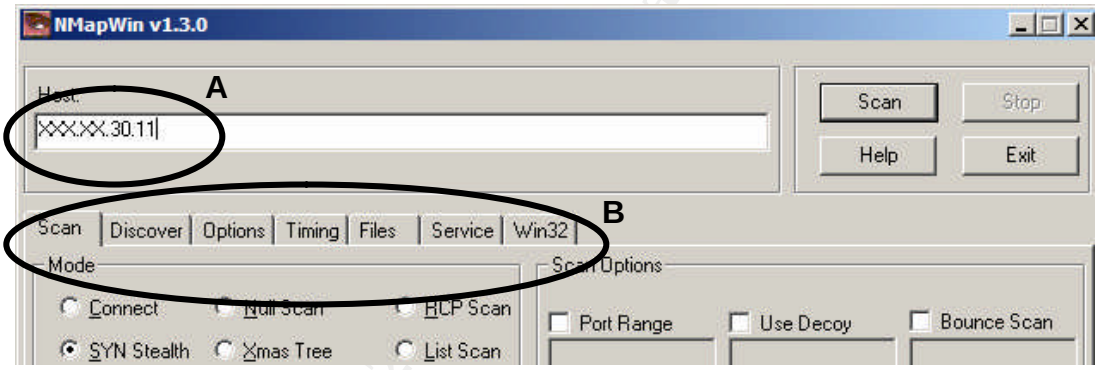
Item Number: D6	**Title: NS performing multiple roles**
Objective Determine if the NS is being used for more than one purpose.	
References: 1. Personal experience 2. [WINDOWSECURITY-01] 3. [NSA-01]	
Vulnerability: (2.6) The NS being used for multiple purposes.	
Risk: The more services running on a server, the more possibilities for vulnerabilities and exploitation by an authorized person.	

Compliance Criteria:

If the NS is being used to perform multiple roles, the NS is not in compliance.

Testing Procedure:

1. Interview the Network Operations Manager and determine if the NS is being used to perform multiple roles.
2. Look under the "Change or Remove Programs" service in the control panel.
3. Run a external scan with NMapWin[37] to determine what services are running with ports open:
    a. Download and install the free tool NMapWin (windows based NMap)
    b. Run NMapWin with the following items entered / selected:



- Enter the Host IP (**A**)
- Check the following options on the tabs (**B**):
    - Scan: Syn Steath (-sS)
    - Discovery: TCP + ICMP (-PI –PT)
    - Options: OS Detection (-O)
    - Timing: Normal (-T 3)
    - No input for Files, Service, Win32

4. Compare the notesfromthe Network Operations Manager interview, Hyena scan and the NMapWin scan to see if they all agree.

Objective/Subjective? Objective

Either the NS is being used only for a DNS server or it is not.

Part 3: Audit testing, evidence and findings

Item Number: A1	**Title: Change and Configuration Management Policies and Procedures**

Pass / Fail:

Failed

Test:

In interviews with the Network Operations Manager and network engineers it was determine there was no formal, approved change management or configuration management procedure(s) in place. There is a company policy signed by the company president that states change and configuration management will be formally implemented, but this has not happened.

Finding:

1) Change Management: A draft change management procedure (*IT-PROC-045*) has been written and being followed by the network engineers. Changes are submitted and reviewed at a weekly change management meeting. All changes are made a designated day of the week unless it is considered an emergency change ("emergency change" is defined in the draft procedure). Not all changes are tested in a lab prior to deployment.
2) Configuration Management: No procedure has been developed for configuration management. Configuration of the NS is maintained sporadically.

Not having formal change management and configuration management procedures can lead to misconfiguration of the NS. Maintenance relies solely on the memory of the engineer who built the server. If that engineer is not available when the server needs maintenance (emergency or routine) the other engineer must guess at why the server was configured the way it was. This could result in a flawless change or one which shuts down the Internet access for employees and not allow customers access to the GIAC web site. Successful changes are a product of chance.

However, the draft change control procedure that is being followed does require each engineer submit the changes to the Change Control Board and document: (1) who is making the change; (2) why the change is being made; (3) testing after changes are made; (4) security implications of the change; (5) documentation after the change is made.

Additionally, without a formal configuration management procedure that requires the server to maintain current on updates, known vulnerabilities can be exploited and the GIAC network and resources could be used /

accessed by unauthorized individuals, including competitors.

Evidence:

The findings resulted in the interview of the Network Operations Manager and the network engineers. Additionally, the draft procedure was reviewed and change control meeting was attended on April 4, 2004.

Item Number: **A2**	**Title:** **NS monitoring**

Pass / Fail:

Failed

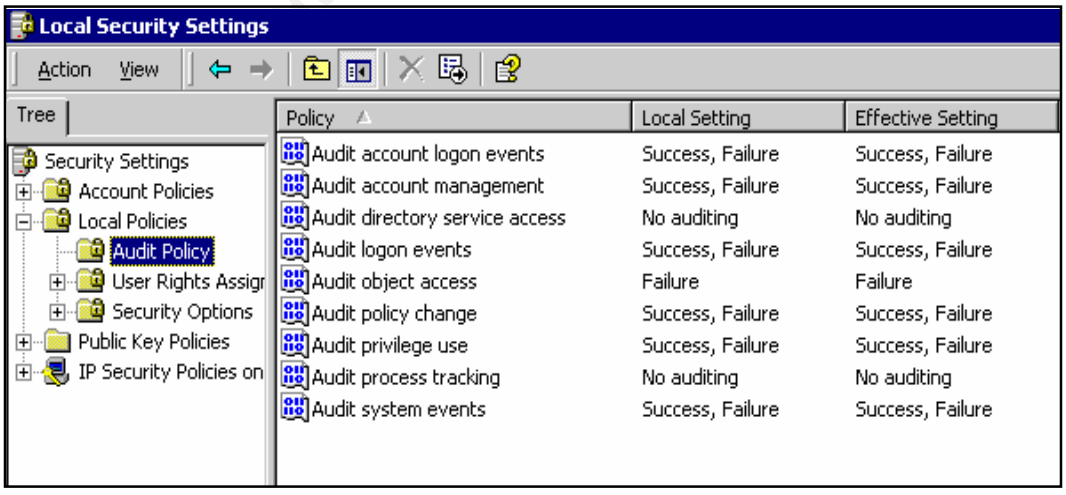
Test:

Interviews with the Network Operations Manager and network engineers and inspection of the auditing enabled on the NS.

Finding and Evidence:

As a result of an interview with the Network Operations Manager and the network engineers on 4-1-04, it was determined there is formal signed policy by the company's president (POLICY-001) that requires monitoring of the network and assigns responsibility for monitoring to the Network Operations Manager. However, there is no formal written procedure for monitoring of the NS. There were no work products of past log reviews to inspect.

Auditing is enabled so pertinent events could be reviewed if log review is needed. Log reviews are preformed on an as needed basis.



The auditing is enabled for the NS is above the NIST requirements:

	DMZDNS settings	NIST setting recommendation
Audit account logon events	Success/Failure	Success/Failure
Audit account management	Success/Failure	Success/Failure
Audit directory service access	No auditing	No auditing
Audit logon events	Success/Failure	Success/Failure
Audit object access	Failure	Failure
Audit policy change	Success/Failure	Success/Failure
Audit privilege use	**Success/Failure**	**Failure**
Audit process tracking	No auditing	No auditing
Audit system events	Success/Failure	Success/Failure

When asked why the level of logging is slightly higher than NIST, the Network Operations Manager said he wanted to know who was logging on to the server successfully – accountability for the engineering staff.

While it is commendable the level of auditing enabled, unless there is a formal and enforced procedure to review the logs, auditing will not alert a network engineer of a compromise. Only after a compromise is suspected will the logs be reviewed. If a compromise actually did occur, it is likely the unauthorized individual will clear the logs so no evidence remains.

Item Number: A3	**Title: Incident Handling Program**
Pass / Fail: **Failed**	
Test: Interviewed the Network Operations Manager and network engineers. Reviewed the company policy on computer security (POLICY-0001). There was no work product from past incidents to review.	
Finding & Evidence: As a result of an interview with the Network Operations Manager on 4-1-04, it was determined there is a policy that Incident Handling Procedures will be developed and followed and was signed by the company president (POLICY-001), formal procedures have not been written. When an incident does occur, corporate memory serves the IT staff on what they did last time if the event is a repeat. If it is a new event that is significant, an IT "War Room" has been set up for events where incident handling is controlled. While the network engineers are a close-knit group that works well together,	

relying on corporate knowledge to mitigate an ongoing event can increase the event response time which will increase the company's exposure from the event.

Item Number: **C1**	**Title:** **Installation of service packs, patches and hotfixes**

Pass / Fail:

Passed

Test:

The tool *Belarc Advisor* was used to scan the NS. The results from the scan and inspection of the Windows folder under the C: drive, a listing of applied service packs, patches and hotfixes was assembled. This list was then compared to the list on the Microsoft Security Bulletin Search.

Note: While the audit was going on, network engineers submitted a change request and after the change was approved, they performed a network-wide server update for patches and hotfixes. The update was performed manually on each server using Microsoft Updater. The results from the update confirmed the auditor's results.

Finding & Evidence:

Using Belarc Advisor scanning tool a report was run:

Installed Microsoft Hotfixes [Back to Top]

DataAccess
Q318203 on 3/25/2003 (details...)
Q329414-25 on 3/25/2003 (details...)
Internet Explorer
Q810847 (details...)
Q813951 (details...)
SP1 (*SP1*)
Windows 2000
SP3
Q282522[SP] on 3/25/2003 (details...)
SP4
✔ Q323172 on 3/25/2003 (details...)
✔ Q323255 on 3/25/2003 (details...)
✔ Q324096 on 3/25/2003 (details...)
✔ Q324380 on 3/25/2003 (details...)
✔ Q326830 on 3/25/2003 (details...)

Windows 2000
SP4 (continued)
✔ Q326886 on 3/25/2003 (details...)
✔ Q327696 on 3/25/2003 (details...)
✔ Q328310 on 3/25/2003 (details...)
✔ Q329115 on 3/25/2003 (details...)
✔ Q329170 on 3/25/2003 (details...)
✔ Q329834 on 3/25/2003 (details...)
✔ Q810030 on 3/25/2003 (details...)
✔ Q810649 on 3/25/2003 (details...)
✔ Q810833 on 3/25/2003 (details...)
✔ Q811630 on 3/25/2003 (details...)
✔ Q814033 on 3/25/2003 (details...)
✔ Q815021 on 3/25/2003 (details...)
Windows Media Player
✔ WM320920.1 (details...)

Click here to see all available Microsoft security hotfixes for this computer.

✔ Marks a HotFix that verifies correctly
✘ Marks a HotFix that fails verification
(note that failing hotfixes need to be reinstalled)
Unmarked HotFixes lack the data to allow verification

Then a Microsoft Security Bulletin Search was performed to determine what items were delinquent.

The name server was running service pack 3 but service pack 4 had been issued. Several hotfixes had not been applied.

Additionally, the services:

- Network connections
- Licensing Logging Service
- Distributed Link Tracking Client
- Network DDE
- Network DDE DSDM

all have vulnerabilities that were fixed with released patches that had not been applied.

The update performed by the network engineer during the audit brought the server up to date on all patches.

The patches that were applied were detailed in a report provided by the network engineer. These patches, hotfixes, etc. were:

KB831167	Critical update for Internet Explorer 6, SP 1	KB835732	Security Update for Microsoft Windows 2000
816093	Security Update Microsoft Virtual Machine	KB828741	Security Update for Microsoft Windows 2000
823559	Security Update for Windows 2000	KB837001	Security Update for Microsoft Windows 2000
KB824105	Security Update for Microsoft Windows 2000	KB828026	Critical Update for Windows Media Player Script Commands
KB826232	Security Update for Microsoft Windows 2000	KB832894	Cumulative Security Update for Internet Explorer Service Pack 1
KB825119	Security Update for Microsoft Windows 2000	KB837009	Cumulative Security Update for Internet Explorer 6 Service Pack 1
KB828035	Security Update for Microsoft Windows 2000	KB823182	Security Update for Microsoft Windows 2000
KB828749	Security Update for Microsoft Windows 2000	KB826232	Security Update for Microsoft Windows 2000
KB832483	Security Update for Microsoft Data Access Components		Windows 2000 Service Pact 4 Express Install for End Users

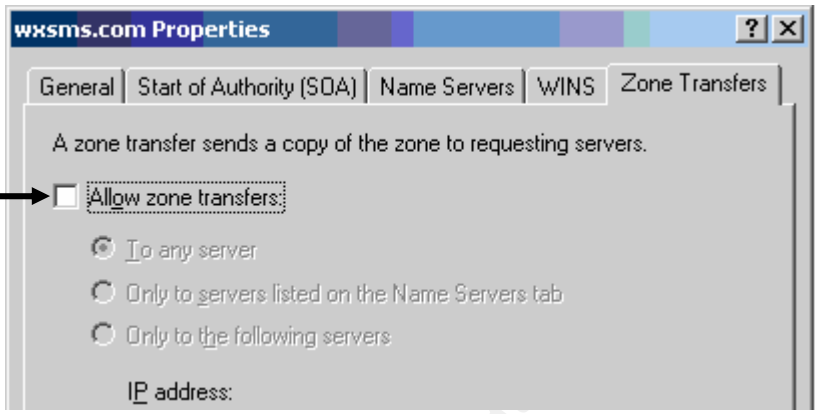
As a result of the server update performed by the network engineers, the name server is up to date on all patches, hotfixes and service packs.

Item Number: C3	**Title: Zone transfers to unknown / untrusted servers**
Pass / Fail: **Passed**	
Test: The NS Management Console was inspected to see if the server was configured to allow zone transfers and if so to which servers.	

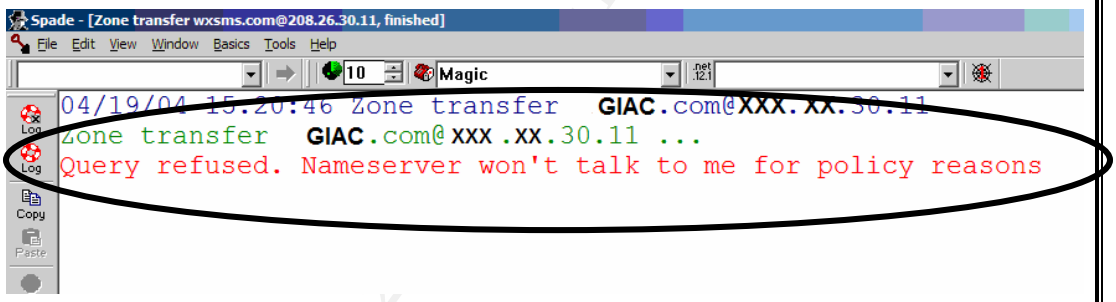
Next the NS was tested using the tool Sam Spade to confirm the NS would not respond to a zone transfer request.

Finding & Evidence:

The NS was configured to not allow zone transfers to **any server**.



This configuration was confirmed by the tool Sam Spade.



The risk from unauthorized individuals receiving a zone transfer, either from sniffing unencrypted traffic off the Internet, or from "tricking" the NS in believing the unauthorized server is allowed to receive the zone information is minimal. The configuration of the server doesn't allow the transfer and the scans run against the server confirmed this.

Item Number: **C4**	**Title:** **Disable all unneeded services on the NS**

Pass / Fail:

Failed

Test:

The services for the NS were identified through running the Management Console. Then NMapWin was run to determine if any services had ports open that were not listed in the Management Console.

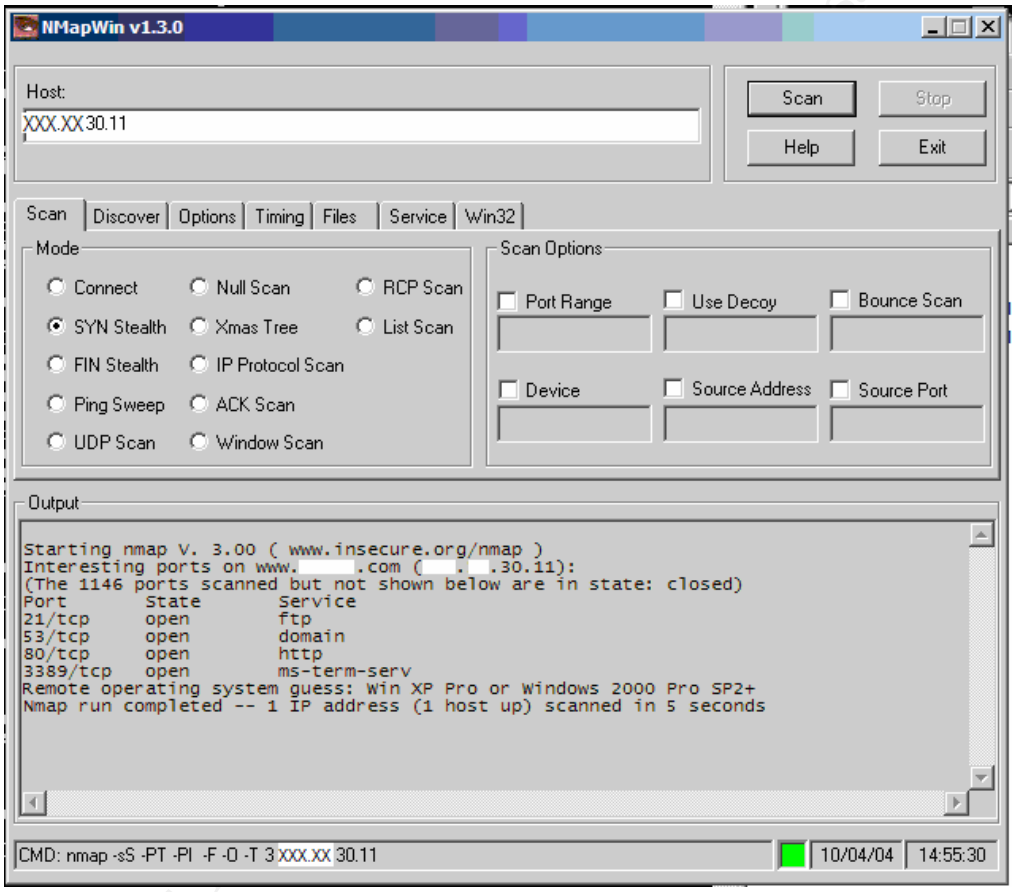
This list of services was then reviewed and the network manager was asked

the reason for the remaining services being open.

Finding & Evidence:

A complete listing of all the services running on the NS was exported to Microsoft Word and can be found in Appendix B.

Next NMapWin was run against the box. The scan and the service listing were consistent.



When the Network Operations Manager was asked why some services were not disabled since they were not being used. Specifically the Network Operations Manager was asked about the following services:

Utility Manager	Remote Procedure Call (RPC) Locator
DNS Client	RunAs Service
License Logging	Distributed Transaction Coordination
Distributed Link Tracking Client	

The services and the state of each service are listed in Appendix B.

The Network Operations Manager responded the servers were not turned

off because the box was never hardened. He felt the risk was low and if the box was compromised he would simply rebuild it.

While the server would have to be rebuilt, many times when the external name server is compromised this often leads to further compromise of the network.

Item Number: **C5**	**Title:** **Security of the file system and registry**

Pass / Fail:

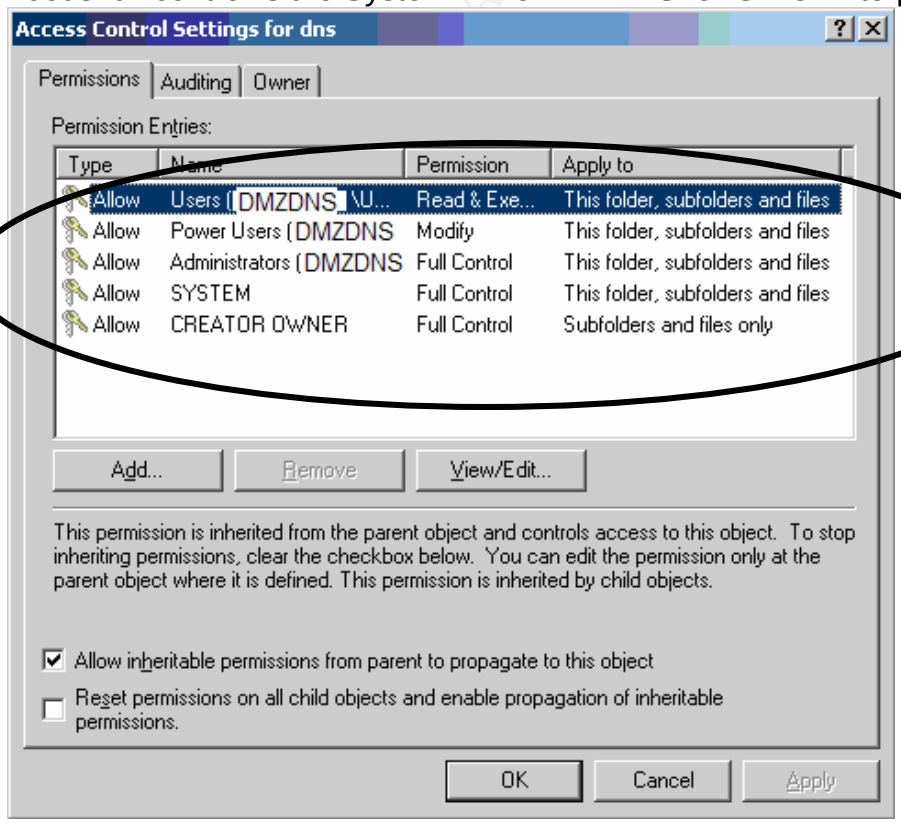
Failed

Test:

The permissions for the *%SystemDirectory%\DNS* folder, subfolders and files and for the registry key, *HKEY_LOCAL_Machines\System\CurrentControlSet\Services\DNS* were checked to see which users had permissions for these items.

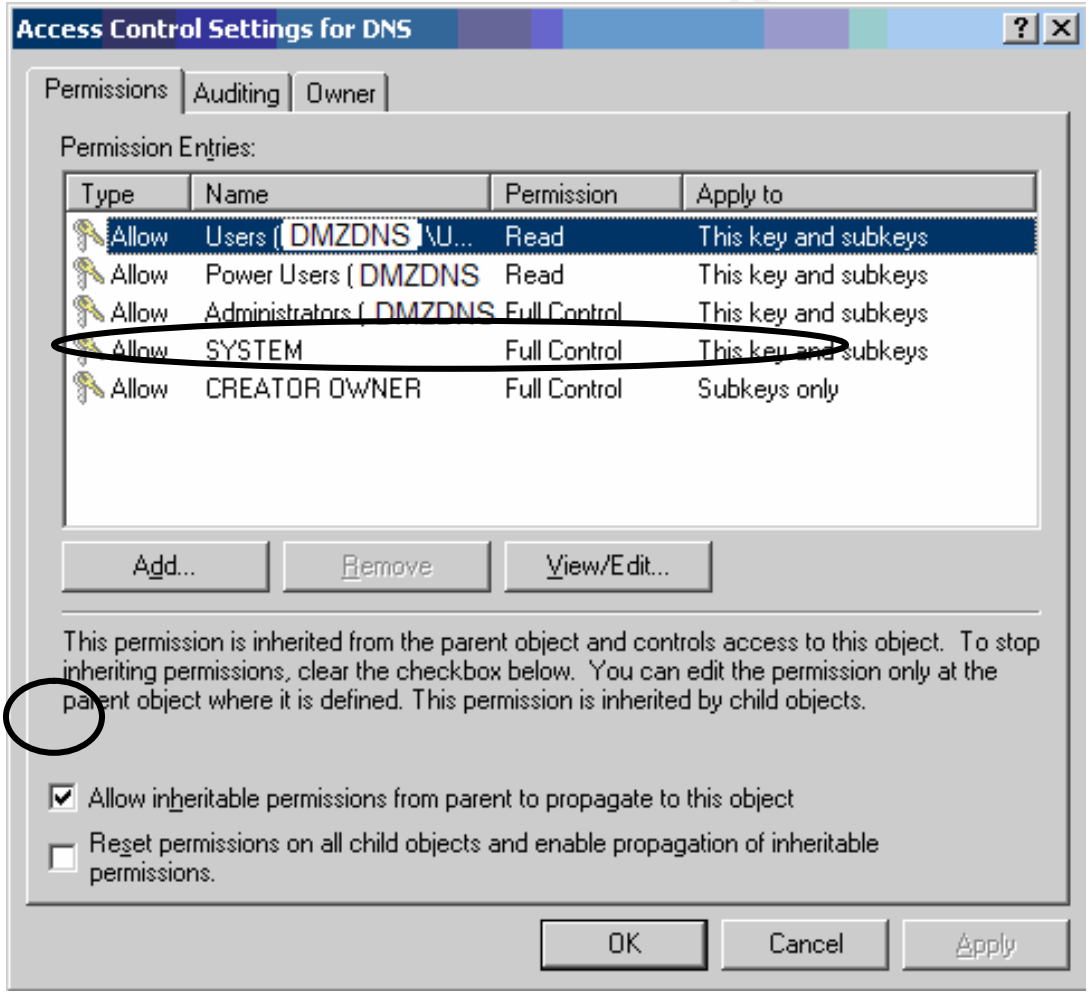
Finding & Evidence:

The ***DNS folder*** contains the DNS zone files. The only user group that needs full control is the System. The DMZDNS for GIAC Enterprises



is configured so all users have access. Therefore the DNS folders are not secured. If an unauthorized person is allowed to access and change the zone files, all incoming Internet traffic is at risk. Sensitive emails, transmittals of sensitive company information, contract and bid information etc. are all vulnerable to redirection if the zone files can be altered.

The ***registry key*** settings identify the location of the zone files. If a unauthorized person could identify or modify the location of the zone files, they would also be able to redirect incoming Internet traffic just as in the case of unsecured DNS folders. The current DMZDNS registry settings are not in compliance with best industry practices. Only the Administrator and the System should have full control of these entries.



Also note that inheritable permissions are turned on. With this feature enabled, the security settings are decided for the network engineer rather than the network engineer making conscious decisions on which users need what access. This is can lead to permissions and access that is not intended.

Item Number: **C6**	**Title:** **Disable dynamic updates for the NS**

Pass / Fail:

Passed

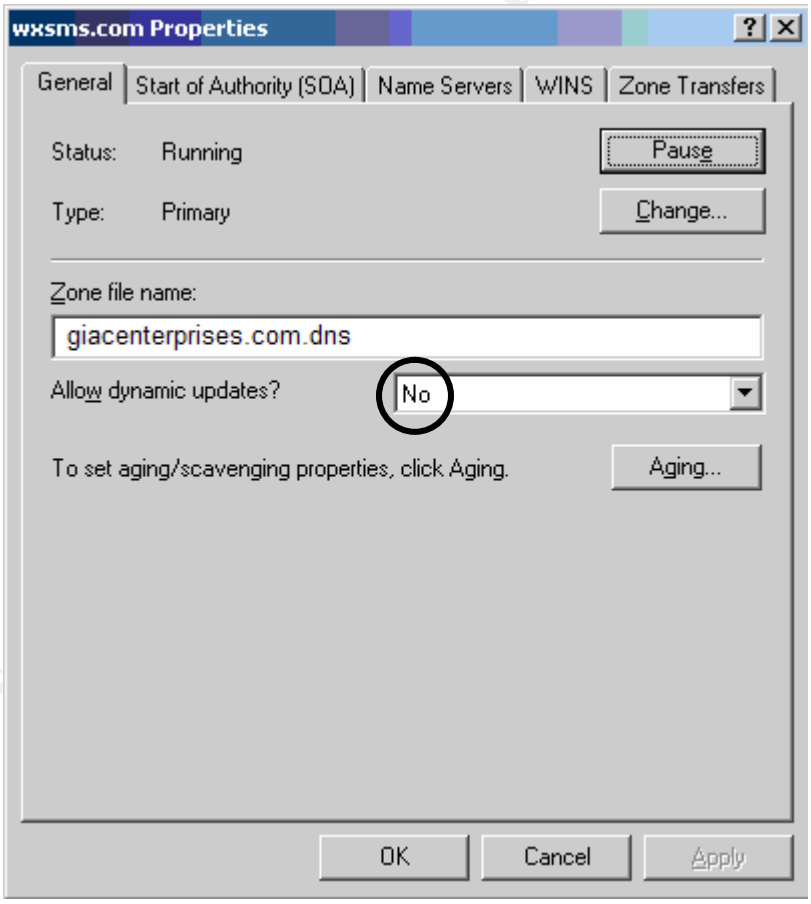
Test:

The DMZDNS is reviewed to see if the server configuration is compliance with best practices. Next the server is "tested" to see if the behavior of the server is consistent with the configuration.

Finding & Evidence:

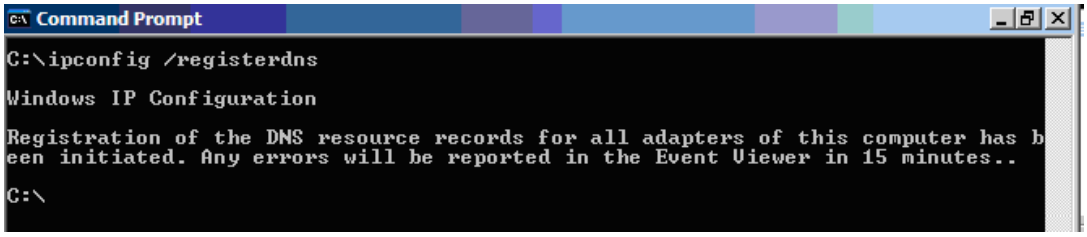
Anyone who can change records can add, delete or modify existing records which can redirect all incoming Internet traffic. This puts all of the incoming traffic at risk of being read or used by unauthorized individuals.

The DMZDNS server is configured not to allow dynamic updates.

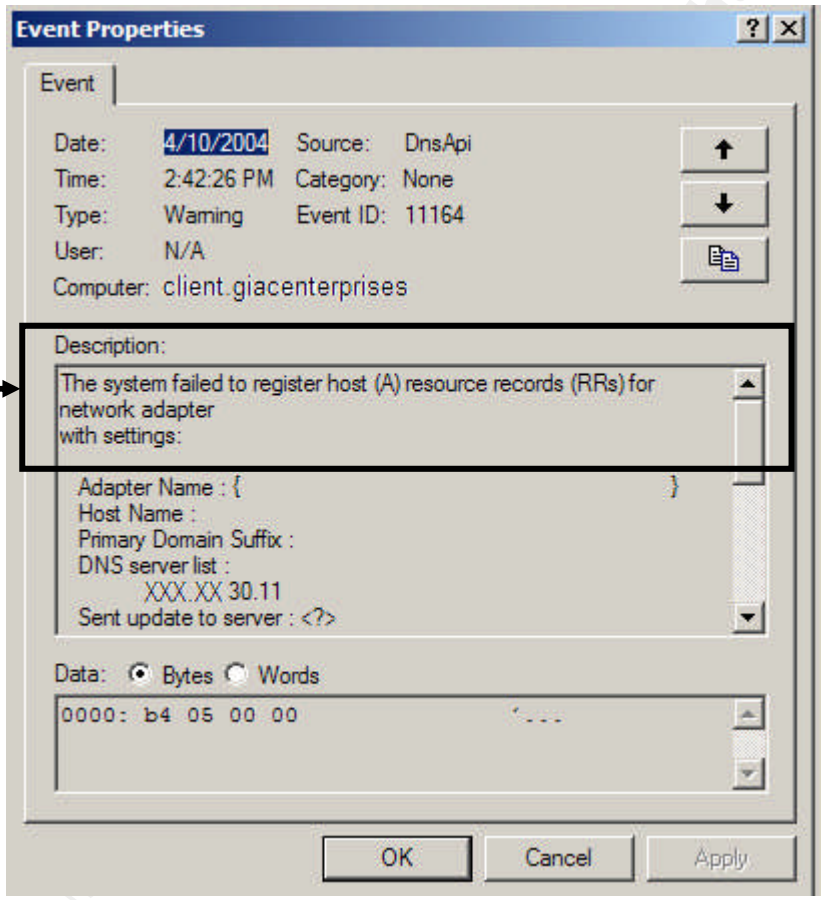


The configuration is in compliance with best practices.

When the server was tested to see if it allowed dynamic updates using the ipconfig / registerdns command from the computer "client.giacenterprises"



DMZDNS did not respond to the request. After 15 minutes the following event was recorded in the System event viewer:



The NS did not respond to the dynamic update request so the system passed this test.

Item Numbers:	**D1**	**Title:**	**Single Point of failure**
	D2		**NS Split Design**
	D3		**NS protected in a DMZ**

Pass / Fail:

Single Point of Failure - **Failed**

NS Split Design – **Passed**

SN Protected in a DMZ - **Passed**

Test:

An interview with the Network Operations Manager on 4-1-04 the network design and configuration was described.

1. There are **two** Internet Service Providers (ISPs) for giac.enterprises
2. **One** border router
3. **One** external name server and multiple internal name servers.

Several tests were performed. NMapWin was run in addition of WhatsUpGold to confirm the Network Operations Manager network design description.

Finding & Evidence:

NMapWin Findings[38]:

The NMapWin scan was run to address the possible risks of single point of failure and to determine if the external name server is protected in a DMZ by a border router and firewall.

(**D1**) If the external name server design ***has*** a single point of failure – only one ***external name server*** to support all of the incoming traffic into the GIAC network. The risk is if the name server is compromised all of the incoming traffic is at risk for (1) no delivery; (2) delivery to the wrong server; (3) be used in an attack against another target. The some of the information that comes into the network has already been described as sensitive to the company and the employees.

(**D3**) The NMapWin results concluded the Network Operation Manager's description of the network was accurate. There external name server is in a DMZ being protected by a border router and a firewall.

If the external name server is not protected by a border router, it is more likely to be compromised which usually results in further compromise of the network. Another risk is a denial of service against the name server which would stop all incoming traffic into the network. Or if the name server was compromised, an attacker could alter the DNS records and redirect all of the incoming traffic to a false web site or redirect sensitive emails to malicious servers.

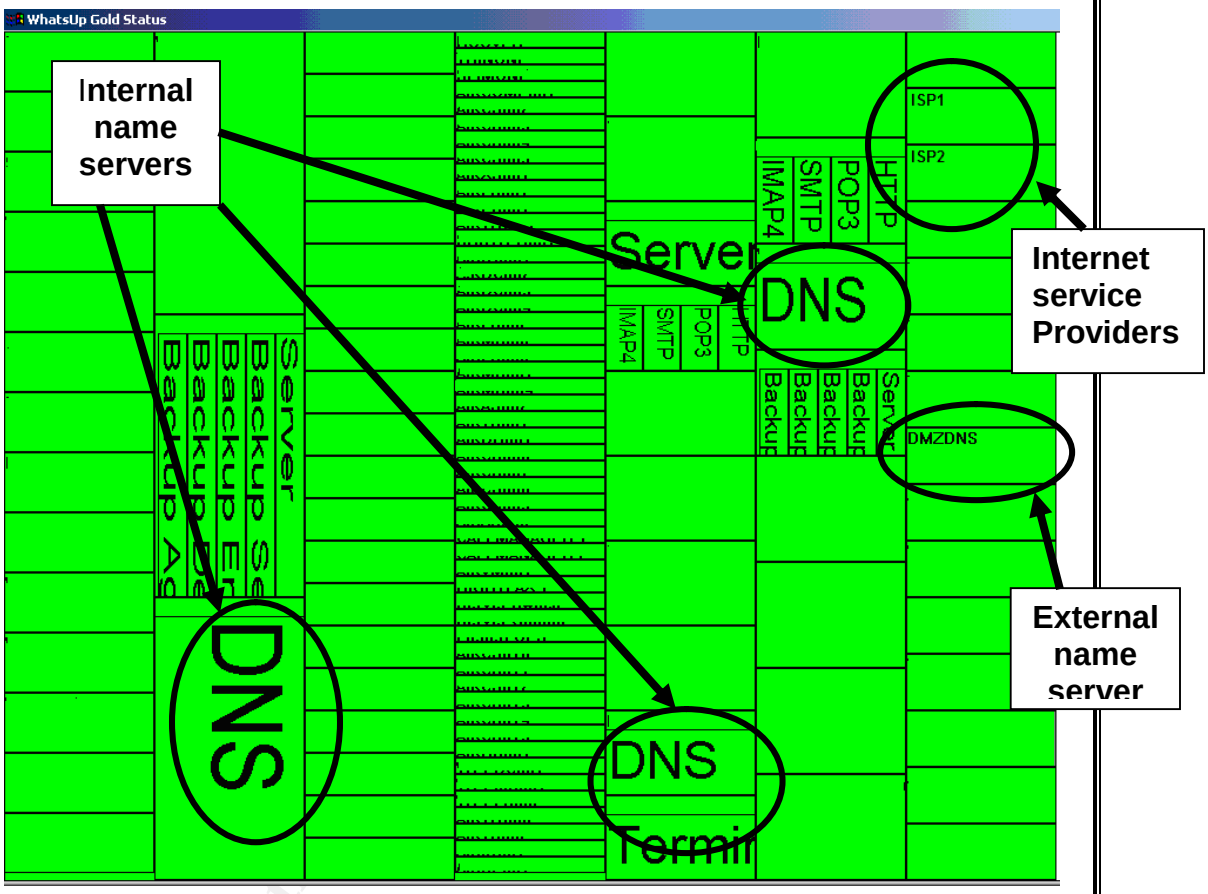
WhatsUpGold results:

The WhatsUpGold results of the internal network confirmed the Network Operations Manager's description of the network configuration.

(**D2**) If the DNS service for a network is not split the DNS server that is accessible from the Internet contains the network server's internal

addresses. If the server is compromised then the entire internal addressing scheme would be known to an unauthorized individual who then could target specific machines.

The DNS design for GIAC Enterprises is split between external and internal DNS servers. This can be seen in the graphical results[39]:



(**D1)** Additionally, the two Internet Service Providers were identified in the graphical representation. If one ISP were to go down, the second ISP would be able to deliver Internet traffic to GIAC Enterprises.

Item Number: **D4**	**Title:** **NS Backup**
Pass / Fail: **Failed**	
Test: The Network Operations Manager was interviewed on 4-1-04.	
Finding & Evidence:	

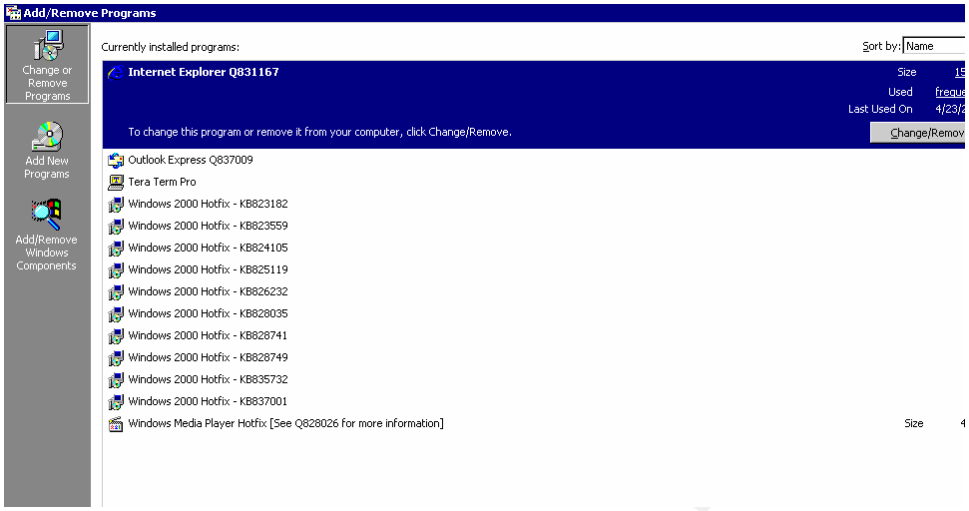
From the interview with the Network Operations Manager, the auditor learned the external name server, DMZDNS, is not backed up.

Not performing regular backups of servers increases the exposure of the company if the server every crashed – software or hardware failure. Even if there is redundant hardware readily available in the case of a hardware failure, the configurations that took time to create would have to be developed from scratch.

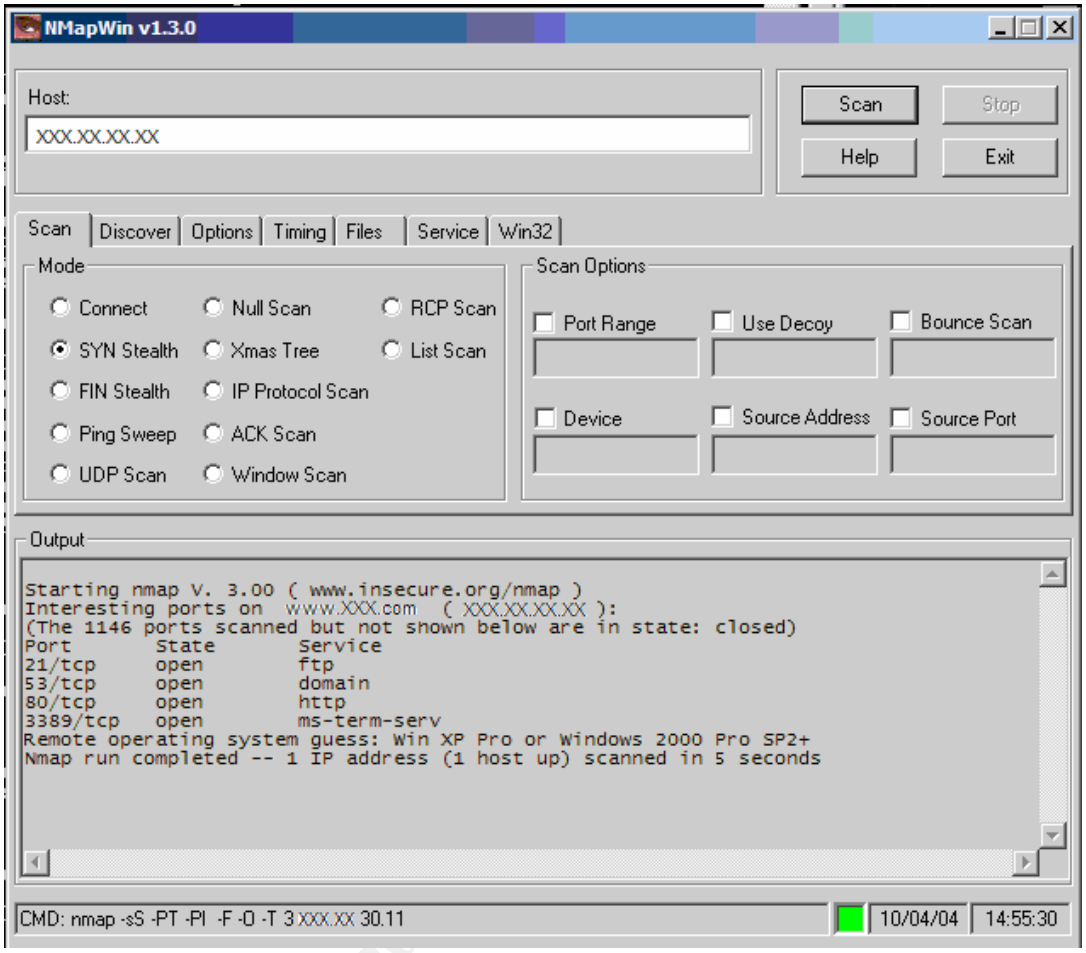
If the name server was compromised, there is no know "good" backup of the server so the server would have to reformatted and all the software from the operating system to the applications would have to be reinstalled and reconfigured.

If a good backup was available, the down-time would be the minimal time it would take to perform a restore.

Item Number: D5	**Title: NS Protected by Anti-virus**
Pass / Fail: **Failed**	
Test: The Network Operations Manager was interviewed and the external name server was searched to determine if anti-virus software was installed and to determine if it was installed, what the latest definitions were..	
Finding & Evidence: There was not anti-virus installed on DMZDNS. While the likelihood is Medium the server would get infected, because the server also is used as a FTP server (see C4, results from the NMapWin scan), there is a chance the server could become infected with malicious code. If this happens the results and dependability of the server are questionable. The malicious code could insert backdoors or Trojans that could allow unauthorized individuals access to the external name server. The "Change or Remove Programs" service was started and no anti-virus was found.	



Item Number: **D6**	**Title:** **NS performing multiple roles**
Pass / Fail: **Failed**	
Test: The Network Operations Manager was interviewed on 4-1-04. During this interview the role of DMZDNS was discussed. The results of the interview were confirmed by scanning the server with NMapWin. Open ports were compared to the roles indicated by the Network Operations Manager.	
Finding & Evidence: The Network Operations Manager indicated the server is being used for an external name server, static page web server, and an FTP server. These results were confirmed by the NMapWin run:	



Port 21 is open for the FTP server; Port 53 is open for the DNS server to talk to the firewall; port 80 is open for the HTTP traffic for the Web pages; and port 3389 is the remote desktop default port and Tera Term Pro is being used (Finding D5).

Using the external name server for other than a DNS server requires more software to be installed and more ports to be open. Both of these provide more opportunity / chance of a vulnerability to be exploited against the server. Especially since the web server is running IIS that is know for its vulnerabilities.

Part 4: Audit Report

Executive Overview

The audit objectives were achieved. The network engineering staff was interviewed to determine the administrative policies and procedures which the external name server, DMZDNS, is monitored and maintained. Next the server was tested and scanned to determine if the server behaved in accordance with expectations based on the interviews.

The interviews and tests concluded there is a lack of formal procedures to ensure the server is monitored and maintained on a regular basis. While the design ensures the name server is protected in a DMZ and incorporates a split-design for external and internal name servers, there is a single point of failure in the fact there is only one external name server for GIAC Enterprises.

Finally, the impact lack of anti-virus protection and lack of a high-confidence backup of the server is increased due to the external name server being used for multiple purposes including hosting the company's web site.

Formal procedures to identify roles and responsibilities should be developed. Additionally, the server should have malware protection installed. If the company believes there is no reason to back up the server, a separate risk assessment should be performed to ensure the Director of Operations, who accepts the residual risk for the company, understands the impacts of not having a good backup and from using the external name server as the host for the company's external web site.

Audit Findings

The audit objectives were identified by performing a basic risk assessment on the server. The items which were considered a Medium or High risk became the audit objectives. These objectives were then separated into three categories: (1) Administrative; (2) Configuration; and (3) Design. Each of the objective included subjective and objective tests. The Administrative category contained more subjective tests due to the nature of the control. However, the Configuration and Design objectives were mostly objective and the tests were design to confirm the network engineers input from the interviews.

Of the fourteen objectives, nine of the items failed to meet company policy or best practices.

The gaps are:

1) **Lack of formal procedures**.

   Although there are requirements in the company policy (POLICY-001) to have formal procedures (e.g., monitoring, change management, etc.), they have not been developed. There is a draft Change Management procedure that seems to be followed, but has not been approved (**A1**). A significant

procedure that is lacking is the Incident Handling Procedure. The lack of this procedure will increase the exposure time in the event of a significant event such as a server or network compromise. While the external name server is being audited this is a weakness that impacts the entire GIAC network (**A3**).

The development of "good" procedures can be expensive in terms of time. Procedures should identify what is to be done and who is responsible for performing the work. If the development of the procedures is hired out to a consultant, care should be taken to understand and confirm the validity of the procedures before the consultant is released from their obligation.

In house reviews after the procedures are developed and issued can ensure the roles and responsibilities are understood and followed and help determine if the procedures are "good" procedures.

The Administrative area is the area of most concern.

2) Unneeded services running on the server

Another are that needs work is the disabling of unneeded services (**C4**). The risk is the more services which are running the greater the possibility an unauthorized individual could take advantage of a vulnerability through one of the unneeded services. Defense in depth best practice is to disable all unneeded services to eliminate any possible vulnerabilities in the future. This gap can be directly linked to the lack of formal procedures. Who is responsible for turning off the unneeded services and who is responsible for ensure this is done?

Immediate correction of this gap is minimal in terms of initial and ongoing time and effort by turning off unneeded services. The bigger issue of development procedures is more costly and time consuming.

3) The DNS folder and DNS Registry Key should be secured

The DNS folder contains the zone information and the DNS Registry Key provides the location of the zone information. Access to these should be strictly controlled. If any engineer can access this information, the contents/values could be altered either through ignorance or malicious act.

Immediate correction of this gap is minimal in terms of initial and ongoing time and effort by securing the folder and the registry key. The bigger issue of development procedures is more costly and time consuming.

4) Single Point of Failure (D1) / Lack of backup (D4)/ Lack of Anti-virus (D5) / Name Server performing multiple roles (D6)

There is only one external name server that supports GIAC Enterprises. If this server was to become inoperable due to hardware failure or compromise, the incoming Internet traffic would be halted until server could be replaced or rebuilt.

The correction of this item is dependent on the GAIC's own tolerance for down-time. While it is best practice to have redundant external name servers,

fully backed up and protected by antivirus software and only performing one role, it is understood the size of the company might not be able to put the resources toward the "ideal". GIAC has to determine their tolerance and take mitigating steps to get the potential down-time within an acceptable time frame. For example, spare hardware could be purchased or high-confidence backup of the server available to minimize the down time could be implemented to mitigate the exposure.

It is the combination of all of the gaps which increases the concern. The concern of a lack of a good backup and the lack of anti-virus is increased since all incoming traffic depends on the operability of the one external name server.

Combined with the lack of good procedures including Incident Handling procedures, the exposure time for the company is significantly increased. How will the company know there is a compromise and when there is who has the authority to mitigate the incident? Who needs to be contacted and when? The corrective action, when identified, will take longer to implement which will increases the exposure time.

By themselves, the design gaps are minor to mitigate, with the exception of deploying a second external name server. Depending on the company's tolerance level if the name server should go down, spare parts and a good backup might be adequate. However, the bigger issue of no procedures and no single point of responsibility to perform the daily maintenance activities is a major concern.

Summary

The major gap identified was the lack of formal procedures and documentation of the name server's configuration, maintenance and operation. However, the configuration and behavior of the name server is as expected – no major gaps, which is surprising considering the lack of formal procedures. An additional gap was noted in the server is not "hardened".

While the there is only one external name server which is a single point of failure, there are two Internet Service Providers that supplies the network with Internet traffic. Additionally, the design splits out the external name server role and the internal name server role.

It is recommended formal procedures are developed, tested and then implemented at GIAC Enterprises. Good starting point to identify which procedures are needed and to what detail is SANS at http://www.sans.org and the National Institute of Science and Technology at http://csrc.nist.gov/publications/nistpubs/index.html, both of which give excellent suggestions on what type of procedures are needed and there are some example procedures to start from.

While there were gaps identified, it should be noted the external name server behaved in accordance with best practices. Zone information was not

transferred and dynamic updates were not permitted. Additionally a split design was implemented and the name server was protected in a DMZ.

The company is relatively new, less than 10 years, and is rapidly growing. When detailed procedures were considered an over-kill when there was one office with only 200 employees when the company was founded, this is no longer the case. There are multiple satellite offices and the company employs over 600 people. To help sustain the company's growth and to help it continue to grow, the network engineering processes need to be proceduralized so not to be so depended on one or two network engineers memory and availability, and addition to recording the company's expectations for all new network engineers.

Appendices

Appendix A: DMZDNS Characterization

Appendix B: Services

Appendix A: DMZDNS Characterization

Physical Characteristics

Operating System	• Windows 2000 Server; Service Pack 3, Build 2195
Processor	• 1000 megahertz Intel Pentium III • 32 kilobyte primary memory cache • 256 kilobyte secondary memory cache
Drives	• 18.16 Gigabytes Usable Hard Disk Capacity • 10.68 Gigabytes Hard Drive Free Space • COMPAQ CD-ROM SN-124Q • 3.5" format removable media [Floppy Drive] • Compaq Disk Array SCSI Disk Device (18.20 GB)
System Model	• Compaq ProLiant DL 380
Main Circuit Board	• 133 megahertz • BIOS: Compaq P17 04/02/2001
Memory Modules	• 640 MB Installed Memory
Local Drives	• c: 4.20 BG; 2.02 GB free • d: 13.97 GB; 8.66 GB free
Printers	• None
Controllers	• Secondary floppy disk controller • Primary IDE channel [controller] • Secondary IDE Channel [controller] • Standard Dual Channel PCI IDE Controller
Multimedia	• None
Bus Adapters	• Compaq Integrated Smart Array Controller
Communications	• Compaq NC3163 Fast Ethernet NIC • Network Card MAC Address: XX:XX:XX:XX:XX:XX • Network IP Address: XXX.XX.30.11/24
Other Devices	• Standard 101/102-Key or Microsoft Natural PS/2 Keyboard • PS/2 Compatible Mouse
Virus Protection	• None

Open Ports (identified through netstat from the command line)

Protocol	**Local Address**	**Foreign Address**
TCP	dmzdns001: ftp	XXX.XX.30.1:1066
TCP	dmzdns001: http	XXX.XX.30.1:
TCP	dmzdns001: http	XXX.XX.30.1:1182
TCP	dmzdns001: http	XXX.XX.30.1:1243
TCP	dmzdns001: http	XXX.XX.30.1:1260
TCP	dmzdns001: http	XXX.XX.30.1:6990
TCP	dmzdns001: http	XXX.XX.30.1:6992
TCP	dmzdns001: 3389	XXX.XX.30.1:1276

Appendix B: Services and their status for DMZDNS

Name	Description	Status	Startup Type
Automatic Updates	Enables the download and installation of critical Windows updates. If the service is disabled, the operating system can be manually updated at the Windows Update Web site.	Started	Automatic
COM+ Event System	Provides automatic distribution of events to subscribing COM components.	Started	Manual
Distributed Link Tracking Client	Sends notifications of files moving between NTFS volumes in a network domain.	Started	Automatic
Distributed Transaction Coordinator	Coordinates transactions that are distributed across two or more databases, message queues, file systems, or other transaction protected resource managers.	Started	Automatic
DNS Server	Answers query and update requests for Domain Name System (DNS) names.	Started	Automatic
Event Log	Logs event messages issued by programs and Windows. Event Log reports contain information that can be useful in diagnosing problems. Reports are viewed in Event Viewer.	Started	Automatic
FTP Publishing Service	Provides FTP connectivity and administration through the Internet Information Services snap-in.	Started	Automatic
IIS Admin Service	Allows administration of Web and FTP services through the Internet Information Services snap-in.	Started	Automatic
IPSEC Policy Agent	Manages IP security policy and starts the ISAKMP/Oakley (IKE) and the IP security driver.	Started	Automatic
License Logging Service		Started	Automatic
Logical Disk Manager	Logical Disk Manager Watchdog Service	Started	Automatic
Network Connections	Manages objects in the Network and Dial-Up Connections folder, in which you can view both local area network and remote connections.	Started	Manual
Plug and Play	Manages device installation and configuration and notifies programs of device changes.	Started	Automatic
Protected Storage	Provides protected storage for sensitive data, such as private keys, to prevent access by unauthorized services, processes, or users.	Started	Automatic
Remote Procedure Call (RPC)	Provides the endpoint mapper and other miscellaneous RPC services.	Started	Automatic
Removable Storage	Manages removable media, drives, and libraries.	Started	Automatic
RunAs Service	Enables starting processes under alternate credentials	Started	Automatic
Security Accounts Manager	Stores security information for local user accounts.	Started	Automatic
System Event Notification	Tracks system events such as Windows logon, network, and power events. Notifies COM+ Event System subscribers of these events.	Started	Automatic
TCP/IP NetBIOS Helper Service	Enables support for NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution.	Started	Automatic
Terminal Services	Provides a multisession environment that allows client devices to access a virtual Windows 2000 Professional	Started	Automatic

	desktop session and Windows-based programs running on the server.		
Windows Management Instrumentation	Provides system management information.	Started	Automatic
Windows Management Instrumentation Driver Extensions	Provides systems management information to and from drivers.	Started	Manual
World Wide Web Publishing Service	Provides Web connectivity and administration through the Internet Information Services snap-in.	Started	Automatic
Alerter	Notifies selected users and computers of administrative alerts.	Stopped	Disabled
Application Management	Provides software installation services such as Assign, Publish, and Remove.	Stopped	Manual
Background Intelligent Transfer Service	Transfers files in the background using idle network bandwidth. If the service is stopped, features such as Windows Update, and MSN Explorer will be unable to automatically download programs and other information. If this service is disabled, any services	Stopped	Manual
ClipBook	Supports ClipBook Viewer, which allows pages to be seen by remote ClipBooks.	Stopped	Disabled
Computer Browser	Maintains an up-to-date list of computers on your network and supplies the list to programs that request it.	Stopped	Disabled
DHCP Client	Manages network configuration by registering and updating IP addresses and DNS names.	Stopped	Disabled
Distributed File System	Manages logical volumes distributed across a local or wide area network.	Stopped	Disabled
Distributed Link Tracking Server	Stores information so that files moved between volumes can be tracked for each volume in the domain.	Stopped	Disabled
DNS Client	Resolves and caches Domain Name System (DNS) names.	Stopped	Manual
Fax Service	Helps you send and receive faxes	Stopped	Disabled
File Replication	Maintains file synchronization of file directory contents among multiple servers.	Stopped	Disabled
Indexing Service	Indexes contents and properties of files on local and remote computers; provides rapid access to files through flexible querying language.	Stopped	Disabled
Internet Connection Sharing	Provides network address translation, addressing, and name resolution services for all computers on your home network through a dial-up connection.	Stopped	Disabled
Intersite Messaging	Allows sending and receiving messages between Windows Advanced Server sites.	Stopped	Disabled
Kerberos Key Distribution Center	Generates session keys and grants service tickets for mutual client/server authentication.	Stopped	Disabled
Logical Disk Manager Administrative Service	Administrative service for disk management requests	Stopped	Manual
Messenger	Sends and receives messages transmitted by administrators or by the Alerter service.	Stopped	Disabled
Net Logon	Supports pass-through authentication of account logon events for computers in a domain.	Stopped	Manual

NetMeeting Remote Desktop Sharing	Allows authorized people to remotely access your Windows desktop using NetMeeting.	Stopped	Disabled
Network DDE	Provides network transport and security for dynamic data exchange (DDE).	Stopped	Manual
Network DDE DSDM	Manages shared dynamic data exchange and is used by Network DDE	Stopped	Manual
NT LM Security Support Provider	Provides security to remote procedure call (RPC) programs that use transports other than named pipes.	Stopped	Manual
Performance Logs and Alerts	Configures performance logs and alerts.	Stopped	Manual
Print Spooler	Loads files to memory for later printing.	Stopped	Disabled
QoS RSVP	Provides network signaling and local traffic control setup functionality for QoS-aware programs and control applets.	Stopped	Disabled
Remote Access Auto Connection Manager	Creates a connection to a remote network whenever a program references a remote DNS or NetBIOS name or address.	Stopped	Disabled
Remote Access Connection Manager	Creates a network connection.	Stopped	Disabled
Remote Procedure Call (RPC) Locator	Manages the RPC name service database.	Stopped	Manual
Remote Registry Service	Allows remote registry manipulation.	Stopped	Disabled
Routing and Remote Access	Offers routing services to businesses in local area and wide area network environments.	Stopped	Disabled
Smart Card	Manages and controls access to a smart card inserted into a smart card reader attached to the computer.	Stopped	Disabled
Smart Card Helper	Provides support for legacy smart card readers attached to the computer.	Stopped	Disabled
Task Scheduler	Enables a program to run at a designated time.	Stopped	Disabled
Telephony	Provides Telephony API (TAPI) support for programs that control telephony devices and IP based voice connections on the local computer and, through the LAN, on servers that are also running the service.	Stopped	Disabled
Telnet	Allows a remote user to log on to the system and run console programs using the command line.	Stopped	Disabled
Uninterruptible Power Supply	Manages an uninterruptible power supply (UPS) connected to the computer.	Stopped	Disabled
Utility Manager	Starts and configures accessibility tools from one window	Stopped	Manual
Windows Installer	Installs, repairs and removes software according to instructions contained in .MSI files.	Stopped	Manual
Windows Time	Sets the computer clock.	Stopped	Disabled
Workstation	Provides network connections and communications.	Stopped	Manual

[1] **[NIST-01]**: Gary Stoneburmer, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems", Special Publication 800-30, January 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf, (26 April 2004)

[2] [NIST-01]

[3] [NIST-01]

[4] [NIST-01]

[5] **[CISCO-01]**: Cisco, "What are the most dangerous Internet Services," http://www.cisco.com/warp/public/146/news_cisco/ekits/vulnerability_report.pdf, (26 April, 2004)

[6] [NIST-01]

[7] **[WINDOWSECURITY-01]**: Magalhaes, Ricky M., "Securing Windows 2000 DNS by design," March 13, 2003, http://www.windowsecurity.com/articles/Securing_Windows_2000_DNS_by_design_Part_1.html , (26 April 2004)

[8] **[CIO-01]**: Berinato, Scott, "FrakenPatch," http://www.computerworld.com.sg/pcio.nsf/0/25ECCA766A23F47F48256DF0003A9304?OpenDocument , (26 April 2004)

[9] **[SANS-01]**: Milroy, Derek P., "Implementing / Re-Implementing Change Control Policies, " 2001, http://www.sans.org/rr/papers/index.php?id=419, (26 April 2004)

[10] **[SANS-04]**: Hinshelwood, David, "DNS, DNSSEC and the Future," May 2003, http://www.sans.org/rr/papers/index.php?id=1054, (26 April 2004)

[11] [**WINDOWSECURITY-02]**: Magalhaes, Ricky M., "Securing Windows 2000 DNS by design," March 20, 2003, http://www.windowsecurity.com/articles/Securing_Windows_2000_DNS_by_using_configuration_Part_2.html, (26 April 2004)

[12] **[SANS-02]:** SANS GIAC Track 1: Security Essentials, Chapter 24, pg 113

[13] **[NIST-02]**: Murugiah Souppaya, Anthony Harris, Mark McLarnon, Mikoalos Selimis, "Systems Administration Guidance for Securing Microsoft Windows 2000 Professional System," http://csrc.nist.gov/itsec/download_W2Kpro.html , (26 April 2004)

[14] **[NIST-03]**: Tim Grance, Karen Kent, Prian Kim, "Computer Security Incident Handling Guide," http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf, (26 April 2004)

[15] **[CERT-01]**: Allen Householder, Brian King, "Securing an Internet Name Server," August 2002, http://www.cert.org/archive/pdf/dns.pdf , (26 April 2004)

[16] **[BELARC-01]**: Belarc, Inc., http://www.belarc.com/free_download.html, (26 April 2004)

[17] *Belarc Advisor* is a free tool to home users. For use in a corporate environment on a corporate network, a license must be purchased. For the purposes of this practical, the creators/distributors of *Belarc Advisor* generously agreed to allow the auditor to use the tool one time free.

[18] **[MICROSOFT-01]**: Microsoft Corporation, http://www.microsoft.com/technet/security/current.aspx, (26 April 2004)

[19] **[SANS-03]**: Lau, Steven, "Why is securing DNS zone transfer necessary?" March 17, 2003, http://www.sans.org/rr/papers/index.php?id=868 , (24 April 2004)

[20] **[NIST-04]**: NIST Federal Information Processing Standard (FIPS) 46-3, 25 October 1999, http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf, (26 April 2004)

[21] **[NSA-01]**: National Security Agency (NSA), "NSA Guide to securing Microsoft Windows 2000 DNS," Report Number C4-050R-00, April 9 2001, http://www.iup.edu/tsc/security/w2k-6.pdf, (26 April 2004)

[22] **[SANS-05]**: Pack, Jeff, "DNS and SMTP Server Security Audit: AN Auditor's Perspective," June 14, 2003, http://www.giac.org/practical/GSNA/Jeff_Pack_GSNA.pdf , (26 April 2004)

[23] Although the risk and exposure of this event was determined to be *Low*, because the impact of such an action is *High*, the event is being audited.

[24] **[SAMSPADE-01]**: SamSpade.org, http://www.samspade.org/ssw/features.html, (26 April 2004)

[25] **[SYSTEMEXPERTS-01]**: Cox, Philip, "Hardening Windows 2000," March 30, 2001, http://www.systemexperts.com/tutors/HardenW2K101.pdf, (26 April 2004)

[26] **[MICROSOFT-02]**: Microsoft Corporation, "Windows 2000 Services," http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/prodspecs/win2ksvc.mspx, (26 April 2004)

[27] **[NMAPWIN-01]**: Insecure.org, http://www.nmapwin.org/ (26 April 2004)

[28] Make sure to get permission from the Network Operations Manager before you start the scan. Also, run the scan during off-hours so not to impact system performance.

[29] For a complete explanation of the NMapWin settings, go to http://www.insecure.org/nmap/data/nmap_manpage.html

[30] Make sure to get permission from the Network Operations Manager before you start the scan. Also, run the scan during off-hours so not to impact system performance.

[31] For a complete explanation of the NMapWin settings, go to http://www.insecure.org/nmap/data/nmap_manpage.html

[32] Make sure to get permission from the Network Operations Manager before you start the scan. Also, run the scan during off-hours so not to impact system performance.

[33] [CERT-01]

[34] Make sure to get permission from the Network Operations Manager before you start the scan. Also, run the scan during off-hours so not to impact system performance.

[35] For a complete explanation of the NMapWin settings, go to http://www.insecure.org/nmap/data/nmap_manpage.html

[36] **[SANS-06]**: SANS Institue, "The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts Consensus", Version 4, October 8, 2003, http://www.sans.org/top20/ , (26 April 2004)

[37] [NMAPWIN-01]

[38] NMapWin was used to scan the external network. Because the report is so long and because after sanitization the report would not be helpful, it is not being included here. If it was a "real" audit report, the NMapWin report would have been included in its entirety as an Appendix item and the report would have been marked *Company Confidential*.

[39] Obviously the graphical representation had a lot more data in it. The graphic was sanitized for corporate security. If this was an actual audit report, the report would have been marked *"Company Confidential"* and all the information would have been presented.

Last Updated: July 24th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**