



Information Technology
Information and Systems Security/Compliance

Information Security Vulnerability
Assessment Program

Version: 1.1

Refer all questions and recommendations concerning this document to:

Jeff Holland
Security Vulnerability Analyst
Information & Systems Security/Compliance
Northwestern University
Phone: 847-467-3569
Email: [jholland \[at\] northwestern \[dot\] edu](mailto:jholland@northwestern.edu)



Revisions

Date	Version	Modified By	Comments
06/28/07	1.0	D. Kovarik	Initial publication
7/11/08	1.1	J. Holland and D. Kovarik	Updated to reflect vulnerability assessments do not require a signed agreement, but rather just a written request. Pen-tests still require a signed agreement.

Contacts

Jeff Holland, Security Vulnerability Analyst, IT Security/Compliance
jholland [at] northwestern [dot] edu

Dave Kovarik, Director, IT Security Compliance
david-kovarik [at] northwestern [dot] edu

Roger Safian, Information Security, IT Security Compliance
r-safian [at] northwestern [dot] edu

Colin Chisholm, Information Security, IT Security Compliance
Cchisholm [at] northwestern [dot] edu



Table of Contents

Revisions.....	2
Contacts.....	2
Overview.....	4
Focus of Vulnerability Assessment Program.....	5
Required Elements.....	5
Vulnerability Assessment Methodology.....	6
Resources/References	10
Vulnerability Assessment Profiles.....	11
Vulnerability Assessment & Remediation Agreement.....	13
Non Disclosure Agreement (NDA)	18
Appendix 1 - Sample Network Vulnerability Assessment	20



Overview

The NUIT Information Security Vulnerability Assessment Program is a University-wide and applicable set of policies, procedures, tools and services intended to audit, identify and help facilitate schools/departments (Clients) in the identification and remediation of security vulnerabilities. The program was created by, and is maintained and operated by the Information and Systems Security/Compliance (ISS/C) department. In particular, the program provides for:

- Consultation concerning the benefits of the Vulnerability Assessment Program
- Initial audit of a Client's network infrastructure through review of documents, configurations, network diagrams and interviews
- In-depth network-based assessment of workstations, servers, devices and the overall security of the network infrastructure
- Coordination, collaboration and general technical consulting before, during and after the Assessment
- Follow-up documentation/reports and additional consulting as needed after the Assessment
- On an ad-hoc available basis, educational presentations concerning topics relevant to computer Vulnerability Assessment (i.e. reducing vulnerabilities, secure coding, etc)

The program will incorporate several existing Northwestern programs and committees as needed and when appropriate, such as:

- Information Security Advisory Committee
(<http://www.it.northwestern.edu/about/committee/isac/index.html>)
- Information Security Coordinator Network
(<http://www.it.northwestern.edu/about/departments/issc/index.html>)
- NUSA – Network User Status Agent
(<http://www.it.northwestern.edu/network/nusa/index.html>)
- Northwestern Information Security Incident Response Protocol
(<http://www.it.northwestern.edu/transitions/2006/irp.html>)
- Northwestern Policies and Guidelines
(<http://www.it.northwestern.edu/policies/index.html>)

Note: This document will address both Vulnerability Assessments and Penetration Testing (pen-tests). These are defined as follows:

- Vulnerability Assessments determine whether a network device or an application is susceptible to a known vulnerability, often by testing for specific ports that are listening, operating system identification, etc. An Assessment typically does not actually exploit a vulnerability and gain access typically associated with the known vulnerability. Instead, it identifies the presence of a known vulnerability so that remedial action may be taken by the Client. While every attempt is made not



-
- to disrupt operations during the course of an Assessment, there is a possibility this could occur.
- Penetration Testing leverages Assessment information and actually attempts -- with the Client's permission -- to exploit a vulnerability found during the Assessment or at the beginning of the penetration test. Note that a Penetration Test should occur after an Assessment and the subsequent recommendations/fixes have been addressed by the Client. While every attempt is made not to disrupt operations, there is a possibility this could occur.
- A sample Vulnerability Assessment report is provided in Appendix 1.

Focus of Vulnerability Assessment Program

The focus of the Vulnerability Assessment Program is University-wide; however, special attention and prioritization will be given to the following:

- Clients receiving a SNAP-feed of NetID's and passwords to their departmental DC (Domain Controller).
- Clients that process University data identified and classified as "Legally/Contractually Restricted" [2] (see References, page 10)
- Clients requesting additional assistance with auditing/assessing their network infrastructure or specific devices for vulnerabilities.

Required Elements

The required elements for Vulnerability Assessments include, but are not limited to, the following:

- A request by a client, or a suggestion by ISS/C, to conduct an assessment on the client's network. An informal written request is sufficient.
- Timely and bi-directional coordination, collaboration and communication between ISS/C and the Client receiving the Assessment.
- Identification of, and authorization to assess, the range of IP addresses assigned to or "owned" by the Client.
- Appropriate network and/or physical access to the Client networks and resources, as agreed to by both parties.
- Sufficient notification by ISS/C as to when the Assessment will take place, what tests will be performed (e.g. Network scanning, Google hacking and a security policy review) and what source IP address range will be used in the execution of Assessment activities.
- Appropriate documentation of findings, results and recommendations so as to facilitate the remediation of vulnerabilities by the Client themselves or in



- conjunction with other NUIT resources (e.g., Telecommunications and Network Services), if required.

Vulnerability Assessment Methodology

Coordination of Assessment Activities

The coordination of the Vulnerability Assessment between ISS/C and the department/school (Client) receiving the Assessment is crucial. Without proper coordination of resources, when the Assessment may be performed, documentation and/or device configurations, and persons to be notified before and after the Assessment, the Assessment cannot be performed. The following items are required, at a minimum, to perform the Assessment:

- In the specific case of a **vulnerability assessment**, a written request by the client (or a written suggestion by ISS/C) to conduct an assessment on the client's network. A detailed agreement (as in needed in the case of penetration test, detailed below) is not necessary. Requests should include the IP range to be assessed, times to perform the assessment and who to contact with questions.
- In the specific case of a **penetration test** (pen-test), a written request and agreement between ISS/C and the Client receiving the pen-test detailing what will be required of the Client, what will be provided by ISS/C, when the pen-test will take place and when the resulting findings report will be made available to the Client. Specific requirements are detailed in the Penetration Test and Remediation Agreement (see page 13).

Client Requests should include, at a minimum:

- What Client personnel are the key contacts before, during and after pen-test?
- What steps were taken to fix any issues found during the previous assessment (which is mandatory)
- Why the Client is requesting the pen-test (e.g. compliance testing, assessment of networks handling sensitive data, etc)?
- What are the goals and expectations of the Client after receiving the pen-test and resulting report?
- What resources will be assessed (IP addresses, and hostnames if available)?
- What resources shall not be assessed (IP addresses, and hostnames required)?

ISS/C and Client Agreements should include, at a minimum:



- What steps were taken to fix the vulnerabilities found in the mandatory assessment conducted before the pen-test was requested
- What IP address range will be used to originate pen-test activities
- Dates and times the pent-test activities may be carried out
- A signed document that identifies and accepts the risk that is inherent to pent-test activities and describes the limitation of liability of personnel involved in the pent-test
- A Non-Disclosure Agreement, signed by ISS/C and Client personnel involved in the pent-test and report preparation and review.
- A final report of findings (see Appendix 1), to include recommendations based upon the pent-test
- Follow-up by ISS/C on technical issues or questions after the pent-test is completed, as well as follow-up on the Clients remediation progress on the identified vulnerabilities
- ISS/C will assist in the development of a remediation plan, at Client's request. However, remediation of vulnerabilities is the responsibility of the Client.

Education, Procedures, and Tools

The following describes the various components of a Vulnerability Assessment:

Education

Establishing and managing expectations of the Client receiving the Vulnerability Assessment is key to a successful Assessment. Active involvement in Assessment planning, design, execution and post-review allows all parties to effectively communicate status and any issues. In particular, educating the recipient of the scan on the following is of primary concern:

- What will the Assessment “look like” to the Client’s network, e.g., firewall and IDS alerts, bandwidth usage, IP’s the testing will originate from, etc.
- What kinds of Assessment testing will take place (i.e. port scanning, vulnerability network scanning, password cracking, web/application testing, etc)
- What level of detail will be provided in the resulting findings and recommendations report by ISS/C
- What level of support will be provided post-Assessment to the department/school (consulting support on remediation but not the remediation itself)

Procedures

The following procedures are meant as guidance for planning and conducting a Vulnerability Assessment. Since nearly every assessment will be different, these procedures are by no means exhaustive.

- Planning and Coordination/Collaboration



1. Establish contact with appropriate management and staff in department/school
 2. Create Assessment plan
 - Devices to assess/scan and date/time to perform Assessment
 - Configurations to audit/review
 - Any specific of deliverables documentation beyond the standard
 - Contact information
 3. Obtain agreement and sign-off on Assessment plan
 4. Coordinate and execute Assessment activities
 5. Provide Client with report of activities
- Vulnerability Assessment (individual tasks below may be combined based on the scanning/assessment requested)
 - Review configurations, documentation and networks diagrams (if applicable)
 - OS configurations
 - Network device configuration
 - Network topology review
 - Security policy review (for those policies that are in addition to, and not contradictory of, University security policies)
 - Perform ping/port scan
 - Perform vulnerability scans
 - Perform Web/Application scans
 - Perform password cracking test
 - Perform Google hacking
 - Perform spot checks for rootkits and spyware
 - Penetration Testing
 - Penetration testing is a separate and distinctly different set of testing activities and available upon request. Its primary focus is the exploitation (not just assessment) of security vulnerabilities and may be disruptive of operations (some exploits may cause operating systems to “crash”). Penetration testing is most beneficial when executed after an Assessment has been performed and the issues found by that Assessment have been remediated. See Penetration Test & Remediation Agreement (page 13).

Paraphrasing the SANS article at

http://www.coresecurity.com/files/attachments/SANS_Penetration_Testing.pdf

[1] (see References, page 10), penetration testing may be defined and delineated from vulnerability assessment as follows:

“Penetration testing is the process of attempting to gain access to resources without knowledge of usernames, passwords and other normal means of access. If the focus is on computer resources, then examples of a



successful penetration would be obtaining or subverting confidential documents, pricelists, databases and other protected information.

The main thing that separates a penetration tester from an attacker is permission. The penetration tester will have permission from the owner of the computing resources that are being tested and will be responsible to provide a report. The goal of a penetration test is to increase the security of the computing resources being tested.

In many cases, a penetration tester will be given user-level access, and in those cases, the goal would be to elevate the status of the account or use other means to gain access to additional information that a user of that level should not have access to. Some penetration testers are contracted to find one hole, but in many cases, they are expected to keep looking past the first hole so that additional vulnerabilities can be identified and fixed.

It is important for the pen-tester to keep detailed notes about how the tests were done so that the results can be verified and any issues that were uncovered can be resolved. It's also important to understand that it is very unlikely that a pen-tester will find all the security issues. As an example, if a penetration test was done yesterday, the organization may pass the test. However, today is Microsoft's "patch Tuesday" and now there's a brand new vulnerability in some Exchange mail servers that were previously considered secure, and next month it will be something else. Maintaining a secure network requires constant vigilance."

- Penetration testing can include, but is not limited to:
 - Testing servers and applications to attempt subverting the security controls and/or exploit vulnerabilities
 - Attempting password cracking to assess password strength
 - Attempting to subvert physical security controls
 - Attempting social engineering to subvert security policies/procedures

Assessment Documentation

- Reporting Findings and Recommendations
 - Review all findings and create a final report for the Client, which includes:
 - Executive/Management Summary
 - General description of recommendations for the remediation of findings
 - Description of tests conducted and tools used during the Assessment
 - Identification of positive findings



- Description of findings requiring remediation, prioritized by risk exposure (critical, high, medium, and low severity) and supported by documentation (e.g., logs, screen shots, etc.)

Resources/References

Policies, Standards and Bench Marks

- Center for Internet Security - <http://www.cisecurity.org>
- SANS – System Administration and Security
 - Sample Policies - <http://www.sans.org/resources/policies/>
 - Misc Resources - http://www.sans.org/free_resources.php
- CERT Vulnerability Remediation - <http://www.cert.org/vuls/>
- OWASP - http://www.owasp.org/index.php/Main_Page

References

[1] SANS Analyst Program, “*Penetration Testing: Assessing Your Overall Security Before Attackers Do*”, Northcutt S., Shenk J., Shacklefor D., Rosenberg T., Siles R., Mancini S., June 2006,
http://www.coresecurity.com/files/attachments/SANS_Penetration_Testing.pdf

[2] Northwestern University Data Access and Classification Policy
<http://www.it.northwestern.edu/policies/dataaccess.html>



Vulnerability Assessment Profiles

The following templates describe common types of security Assessments that may be performed. Custom combinations of profiles can be created as needed based upon Client and/or ISS/C requests and recommendations.

Profile 1: Security Policy Assessment

- Review Client's security policies and network infrastructure diagrams
 - ISS/C will provide recommendations upon reviewing Client security policies based upon industry best practices and common recommendations from compliance programs such as ISO 17799. (Note: ISS/C will not write or update the security policies for Clients.)
 - ISS/C will provide recommendations upon reviewing Client mobile device and/or PDA security policies

Profile 2: Network Infrastructure Assessment

- ISS/C will review network infrastructure through the auditing of network diagrams and/or interviews with the appropriate Client staff.
- When applicable, ISS/C will audit for network extensions (hubs, routers, switches) that were not installed by TNS (Telecommunications and Network Services) and is against NU's network policy.

Profile 3: Network Vulnerability Assessment

- Perform a network-based Vulnerability Assessment of the Client's network (a subset or all of the following may be performed based upon the Client's needs and/or the recommendation of ISS/C)
 - ISS/C will perform a network-based Vulnerability Assessment of the Client network using open source and/or commercial software.
 - Audit key device configurations (firewall(s), servers, etc)
 - Note that a network infrastructure assessment is often combined with the network Vulnerability Assessment, while a security policy assessment is optional.
 - Google hacking to uncover misconfigurations or sensitive data available on the web
 - Social engineering
 - Password strength/policy assessment
 - Wireless Network and Bluetooth assessment

Profile 4: Penetration Test

- Perform a penetration test of the Client's network (**NOTE: requires a prior Vulnerability Assessment and resolution of the Assessment's findings**)



- The penetration test shall be performed after the Client has addressed the findings from the Assessment to reassess the security of their network.

NORTHWESTERN
UNIVERSITY



Penetration Test (Pen-Test) & Remediation Agreement

1.0 Purpose

The purpose of this document is to set forth agreement regarding security assessment and scanning activities offered by NUIT's Information and Systems Security/Compliance (ISS/C) department to the Client. In exchange for these assessment services, the Client agrees to engage in activities for the remediation of Critical and High Risk findings as defined in Section 4.0, Agreement to Remediate Findings.

Penetration Tests may be conducted to:

- Insure the findings in the previously conducted vulnerability assessment were properly addressed and fixed
- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents and ensure conformance to the Client's security policies
- Assess the Client's network and devices for vulnerabilities
- Review the Client's policies and device configurations for security issues and/or configuration issues
- Monitor user or system activity where appropriate

2.0 Scope

This Agreement covers all computer and network devices owned or operated by the Client. This Agreement also covers any computer, network and mobile devices that are present on the Client's premises, but which may not be owned or operated by the Client. ISS/C will not perform Denial of Service (DoS) activities and due care will be taken not to create a DoS condition on the Client network. However, ISS/C makes no assurance that a networked device will not be adversely affected by assessment activities that results in a loss of connectivity and/or the need for a system reboot.

3.0 Authorization to Access Resources

When requested, the Client's consent to access resources shall be provided to ISS/C staff for the purpose of performing an Assessment. Client hereby provides its consent to allow ISS/C to access its networks, firewalls and other devices as designated in this Agreement to the extent necessary to allow ISS/C to perform the Assessment and scanning activities authorized. Client shall provide protocols, addressing information, device configurations, policies and network connections sufficient for ISS/C to execute the tools required to perform network scanning and other Assessment tasks.

This access may include:

- User level and/or system level access to any computing or network device
- Access to information (electronic, hardcopies of documentation, etc.) that may be produced, transmitted or stored on Client's equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)



- Access to interactively monitor and log traffic on Client networks as required and appropriate

3.1 Network Control. If the Client does not control their network, and/or Internet service is provided via a second or third party, these parties are required to approve scanning in writing if scanning is to occur outside of the University LAN. The Client is responsible for obtaining the written approvals from non-University parties; said approvals are to be made part of this agreement. Assessment activities will not commence until these approvals are obtained. Execution of this agreement by the Client along with the required approvals indicates that all involved parties acknowledge that they authorize ISS/C to use their service networks as a gateway for the execution of these tests during the dates and times specified.

3.2 Service Degradation and/or Interruption. Network performance and/or availability may be affected by the network scanning or other Assessment activities. The Client releases ISS/C of any and all liability for damages that may arise from network availability restrictions caused by the network scanning or other Assessment activities, unless such damages are the result of ISS/C's gross negligence or intentional misconduct.

3.3 Client Point of Contact During Scanning Period. The Client agrees to identify, in writing, a person to be available if the ISS/C department Assessment Team has questions regarding data discovered or requires assistance.

3.4 ISS/C Point of Contact During Scanning Period. ISS/C agrees to identify, in writing, the personnel performing and involved in the Assessment activities in the event the Client needs to contact them. This will include e-mail and phone numbers of the personnel performing the Assessment.

3.5 Assessment Period. The Client and ISS/C department Assessment Team agree to identify in writing the allowable dates and times for the scans and testing to take place (during normal M-F business hours), as well as what IP range the scans will originate from if the scan originates from a remote location on campus (see end of document).

3.6 Reporting. ISS/C agrees to create a final Vulnerability Assessment findings report and deliver it to the Client within 15 business days (unless otherwise noted). This report shall describe the findings and recommendations for remediation by Client personnel. ISS/C personnel will be available for assistance with explanations of the findings and recommendations. Note that ISS/C will inform the client of any Critical or High vulnerabilities found during the Assessment within 24 hours.

4.0 Agreement to Remediate Findings.

All remediation activities are the responsibility of and shall be performed by the Client or the Client's designee. The Client has engaged ISS/C to perform the Assessment and agrees to complete the following remediation activities upon written acknowledgement of receipt of the completed Assessment document:



- The Client agrees to immediately address all *Critical Severity Vulnerability* findings and institute the recommendation or an acceptable mitigating control within 2 business days
- The Client agrees to immediately address all *High Severity Vulnerability* findings and institute the recommendation or an acceptable mitigating control within 5 business days
- The Client agrees to address all *Medium Severity Vulnerability* findings and institute the recommendation or an acceptable mitigating control within 20 business days. The Client has the option to accept the risk imposed by this vulnerability and refrain from fixing it or implementing a mitigating control, with the exception of instances of illegally downloaded copyrighted material and unlicensed software.
- The Client agrees to address all *Low Severity Vulnerability* findings and institute the recommendation or an acceptable mitigating control within 120 business days. The Client has the option to accept the risk imposed by this vulnerability and refrain from fixing it or implementing a mitigating control.

A *Critical Severity Vulnerability* finding is one that imposes serious and immediate risk upon the Client and/or University and exists on a device that contains personal data such as social security numbers, or is associated with an “essential” device (e.g. a domain controller or mail server) infected with spyware or malware. Note that the existence of personal data on a machine that has a High vulnerability is what elevates the vulnerability to critical, not simply the existence of personal data on a device.

Nessus scans do not identify “Critical” vulnerabilities. For the purposes of Assessments at Northwestern University, Critical vulnerabilities will be designated upon inspection of the Assessment results by ISS/C using the following criteria:

- Any vulnerability will be deemed Critical if it fails a compliance test (such as HIPPA or PCI)
- Any vulnerability that could lead to a loss of personal information (such as social security number stored on a particular server)
- Services that are accessible from the Internet that provide open access for unauthorized users (e.g. an open mail relay to the internet, a telnet server with a weak or no password on a default account, etc.)

A *High Severity Vulnerability* finding is one that imposes serious but not immediate risk upon the Client and/or University. One such example is a workstation infected with a virus or spyware, or a misconfigured firewall allowing inappropriate access to sensitive data that has other security controls that prevented it from being accessed.

A *Medium Severity Vulnerability* finding is one that imposes moderate risk upon the Client and/or University, such as illegally downloaded copyrighted material found on a server, or unlicensed software installed on a server.



A *Low Severity Vulnerability* finding is one that imposes some risk upon the Client and/or University, but is not significant enough to require immediate attention and can be scheduled for future upgrades or maintenance windows. One such example would be a computer running Windows NT 4.0 without a host-based firewall installed (as Windows 2003, XP and Vista support natively).

5.0 Enforcement

Critical and *High Severity Vulnerabilities* findings represent significant exposure to the Client and Northwestern University, and require immediate attention.

Failure to take the remedial action identified in this agreement could substantially increase risk and exposure to the Northwestern University community at large, and may result in the suspension of the Client's network access until remediation activities have been completed. Failure to remediate in a timely manner may also expose the Client's environment to compromise across those systems identified in the Assessment and/or Penetration Test.

6.0 Non-Compliance

Non-compliance with Critical and High severity vulnerability remediation timelines, as outlined in this agreement, may result in ISS/C forwarding a report of non-compliance to the Northwestern University Office of Vice President for Information Technology, Office of General Counsel, and Audit and Advisory Services.

7.0 Specifics of Assessment

What IP address range will be used to originate Assessment activities?

What IP's are to be assessed?

Dates and times the Assessment activities may be carried out:



NUIT Senior Management

Client Senior Management NORTHWESTERN
UNIVERSITY

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____

Name: _____

Name: _____

Title: _____

Title: _____

Date: _____

Date: _____



Non Disclosure Agreement (NDA)

Information Security Vulnerability Assessment Program Mutual Confidentiality Agreement

This Mutual Confidentiality Agreement (“*Agreement*”) is effective this _____ day of _____, 20____, between Northwestern University Information Technology, Information and Systems Security/Compliance (“*ISS/C*”) and information security vulnerability assessment client _____ [**insert name of client**]_____ (“*Client*”).

In order to protect certain confidential information (“*Confidential Information*”) that may be disclosed between them, ISS/C and Client agree to the following:

1. Confidential Information. As used in this Agreement, Confidential Information includes:

- a) “Proprietary Information” - information relating to ISS/C and Client that is not generally known to the public, including, but not limited to information that relates to business affairs, financial matters, marketing, pricing, trade secrets, products, services, policies, and procedures.
- b) “Personally Identifiable information (PII)” - information pertaining to any person or entity as defined within the Illinois Personal Information Protection Act, 2005.
- c) “University data” – information classified as Legally/Contractually Restricted by University policy.
- d) “Assessment Techniques” – information related to the execution of the vulnerability assessment process, including but not limited to techniques, programs and programming, procedures, utilities, and equipment.
- e) “Assessment Report” – information derived from the assessment process describing the Client’s environment, including but not limited to the description of systems, infrastructure, processes, physical conditions, safeguards, vulnerabilities, exposures and remedial measures.

2. Scope of Confidentiality Obligations. ISS/C, Client and other designated recipients have a duty to protect that Confidential Information which is disclosed or discovered in connection with or as a result of the vulnerability assessment process.

3. Security Measures for Confidential Information. ISS/C and Client will implement and maintain University-approved or commercially reasonable security measures to:

- a) ensure the security and confidentiality of Confidential Information, and
- b) protect against anticipated threats or hazards to the security or integrity of Confidential Information, and
- c) protect against unauthorized access to or acquisition of Confidential Information.

4. Access to and Use of Confidential Information. ISS/C and Client agree to restrict the access to and use of Confidential Information, limited to those employees, agents, or contractors who have a need to know the Confidential Information for purposes of



conducting the vulnerability assessment. All recipients of Confidential Information have an obligation to preserve and maintain the confidentiality and integrity of the Confidential Information.

5. Compliance. Vulnerability assessment activities may result in the discovery of a breach of security as defined by Federal statutes, State regulations or University policy. Where a breach is discovered and action is required for compliance, ISS/C and Client will cooperate fully with each other in efforts to promptly comply with the requirements of the regulatory agencies and University.

6. Retention of Confidential Information. Confidential Information will be retained in accordance with University data retention policies.

ISS/C and Client have caused this Agreement to be executed by authorized persons, effective the date of this Agreement.

_____ Information and Systems Security/Compliance
Type or print name of Client

By: _____
Signature

By: _____
Signature

Telephone _____

Telephone _____

Address _____

Address _____



Appendix 1 - Sample Network Vulnerability Assessment

Conducted by:

Information Systems Security and Compliance (aka "ISS/C")
Jeff Holland
Northwestern University
IP scan originated from: 192.168.127.128

Conducted for:

School of Egyptology (aka "Client")
Northwestern University
Evanston, IL

Date Conducted:

3/16/07

Focus of Assessment:

A network-based assessment of the devices noted below. There were no Google hacking, password cracking, firewall analysis, social engineering or policy reviews conducted (per the agreement with the Client).

Server1: Apache Web Appliance
Hostname: apache_appliance
IP: 192.168.127.129

Server2: Solaris Web/App Server
Hostname: unknown
IP: 192.168.127.130

Compliance Requirements (i.e. HIPAA, etc):

None



Executive Summary

The following report details the findings from the security assessment performed by ISS/C for the Client. The assessment included the following activities as outlined in the Vulnerability Assessment Profiles section of the Assessment Program document.

- Vulnerability Assessment



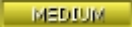

Positive Findings

The following are some positive findings from the assessment, outlining what security controls already in place are helping to secure your environment.

- There were relatively few security vulnerabilities, with only one being “High”. The “High” vulnerability (remote Telnet vulnerability on Server 2), while significant and require immediate attention, is easily fixed by applying the proper patch as noted in the recommendations.
- The Client technical personnel were responsive and helpful during and after the assessment regarding questions and the discussion of the results of the scan.

Deficiencies Noted

The following findings were noted during the assessment.

- **Server 1:**
 -  There were Cross Site Tracing vulnerabilities on 192.168.127.129 for ports 80 and 443. These should be fixed within 4 weeks.
 -  There were “Low” vulnerabilities and should be fixed within 24 weeks
- **Server 2:**
 -  There were Cross Site Tracing vulnerabilities on 192.168.127.129 for ports 80 and 443. These should be fixed within 4 weeks.
 -  There was a Telnet remote access vulnerability on port 23 that was a “High” vulnerability. This should be fixed within 1 week.

Overall Summary:



The assessment uncovered several deficiencies (one of which is of High criticality) in the security of the network that requires attention, but overall reflects the relatively secure nature of the network. In terms of a numerical score, based upon the experience of ISS/C, the Client would receive a score of 8 out of 10 (10 being the highest) in terms of security.



Findings and Recommendations

The following findings and recommendations are made per the output from the Nessus scan. Note that each device below (servers, in this case) has a synopsis and a solution for the issue. Any additional recommendations beyond what any scanning tools supply are included as necessary.

Note that the assessment agreement between the Client and ISS/C, the Client is responsible for fixing the issues themselves and following up with ISS/C in a timely manner when they have been addressed. ISS/C will be available for consultation on any of the recommendations as defined in the agreement.

For the findings, note the following:

- “Information found” maps to “Low” vulnerabilities
- “Warning found” maps to “Medium” vulnerabilities
- “Vulnerability found” maps to “High” vulnerabilities
- There is no mapping within Nessus for “Critical” vulnerabilities. These are mapped in a manual process as outlined in the Vulnerability Assessment Program document.
- “Banners” refer to information that is advertised by a computer process or service and allows a person to software tool to query the information. Knowing this information can help ascertain which vulnerabilities a host might be subject to. Also, note that these banners are also subject to falsification, so relying on them solely is not advised.
- “Concern or Vulnerability” refers to the deficiency found during the assessment. If the item is of “High” criticality, it is a vulnerability. If it of “Low” or “Medium” criticality, it is a concern.

Server 1

Information found on port https (443/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.



See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
```

```
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
```

```
RewriteRule .* - [F]
```

Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers. An attacker may use this flaw to trick your legitimate Web users to give him their credentials.

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
```

```
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
```

```
RewriteRule .* - [F]
```

Server 2



Information found on port https (443/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
RewriteRule .* - [F]
```

Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)



Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Vulnerability found on port telnet (23/tcp)

Synopsis :

It is possible to log into the remote system using telnet without supplying any credentials

Description :

The remote version of telnet does not sanitize the user-supplied 'USER' environment variable. By supplying a specially malformed USER environment variable, an attacker may force the remote telnet server to believe that the user has already authenticated.

For instance, the following command :

```
telnet -l '-fbin' 192.168.127.130
```

Will result in obtaining a shell with the privileges of the 'bin' user.

Solution :

Install patches 120068-02 (sparc) or 120069-02 (i386) which are available from Sun.

Filter incoming to this port or disable the telnet service and use SSH instead, or use inetadm to mitigate this problem (see the link below).

See also :

<http://lists.sans.org/pipermail/list/2007-February/025935.html>
<http://isc.sans.org/diary.html?storyid=2220>

Risk factor :



Critical / CVSS Base Score : 10
 (AV:R/AC:L/Au:NR/C:C/I:C/A:C/B:N)

CVE : [CVE-2007-0882](#)
 BID : [22512](#)
 Nessus ID : [24323](#)

Network Profile

IP address test was conducted from

192.168.127.128	
-----------------	--

IP ranges to be tested and details of these ranges

192.168.127.129	Apache Web Server Appliance
192.168.127.130	Solaris Web Server (Solaris 10)

Domain information and configurations

--

Zone Transfer Highlights

n/a

SERVER LIST

IP Address	Domain Name(s)	Operating System
192.168.127.129		Linux (rpath)
192.168.127.130		Solaris 10



Server 1 Information

IP Address	Domain Name
192.168.127.129	

Service	(Port/Protocol)
o norton-av-for-gateways-web-interface	(8003/tcp)
o terabase	(4000/tcp)
o ssh	(22/tcp)
o https	(443/tcp) (Security notes found)
o nfs	(2049/tcp)
o shoutcast	(8004/tcp)
o sunrpc	(111/tcp)
o http	(80/tcp) (Security notes found)
o ftp	(21/tcp)
o fcp-udp	(810/tcp)
o wpages	(776/tcp)

BANNER(S):

Port	Protocol	Banner
443	TCP	TRACE /Nessus240472754.html HTTP/1.1 Connection: Close Host: apache_appliance Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8
80	TCP	TRACE /Nessus240472754.html HTTP/1.1 Connection: Close Host: apache_appliance Pragma: no-cache User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0) Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */* Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8



CONCERNS AND VULNERABILITIES:
Concern or Vulnerability

Information found on port https (443/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)
RewriteRule .* - [F]
```

Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution



Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on  
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)  
RewriteRule .* - [F]
```



Server 2 Information

IP Address	Domain Name
192.168.127.130	

Service	(Port/Protocol)
o smtp	(25/tcp) (Security notes found)
o sometimes-rpc21	(32779/tcp)
o ssh	(22/tcp) (Security notes found)
o sometimes-rpc15	(32776/tcp)
o complex-link	(5001/tcp) (Security notes found)
o sometimes-rpc9	(32773/tcp)
o submission	(587/tcp) (Security notes found)
o smc-http	(6788/tcp) (Security notes found)
o finger	(79/tcp) (Security notes found)
o sometimes-rpc23	(32780/tcp)
o font-service	(7100/tcp)
o telnet	(23/tcp) (Security hole found)
o sometimes-rpc17	(32777/tcp)
o lockd	(4045/tcp)
o dtspcd	(6112/tcp)
o filenet-rmi	(32771/tcp)
o x11	(6000/tcp) (Security notes found)
o login	(513/tcp)
o sunrpc	(111/tcp) (Security notes found)
o smc-https	(6789/tcp) (Security notes found)
o sometimes-rpc19	(32778/tcp)
o ftp	(21/tcp) (Security notes found)
o filenet-pa	(32772/tcp)
o shell	(514/tcp)
o unknown	(32795/udp) (Security warnings)
o unknown	(32794/udp) (Security warnings)
o general/udp	(Security notes found)
o general/tcp	(Security notes found)

BANNER(S):

Port	Protocol	Banner
25	TCP	An SMTP server is running on this port Here is its banner : 220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:44:45 -0700 (PDT) Nessus ID : 10330
587	TCP	An SMTP server is running on this port Here is its banner : 220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:45:05 -0700 (PDT) Nessus ID : 10330
23	TCP	Remote telnet banner: login:



		Nessus ID : 10281
21	TCP	An FTP server is running on this port. Here is its banner : 220 unknown FTP server ready. Nessus ID : 10330

CONCERNS AND VULNERABILITIES:

Concern or Vulnerability

Information found on port https (443/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description : The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution

Add the following lines for each virtual host in your configuration file :

RewriteEngine on

RewriteCond %{REQUEST_METHOD} ^(TRACE | TRACK)

RewriteRule .* - [F]

Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when



used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2

(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

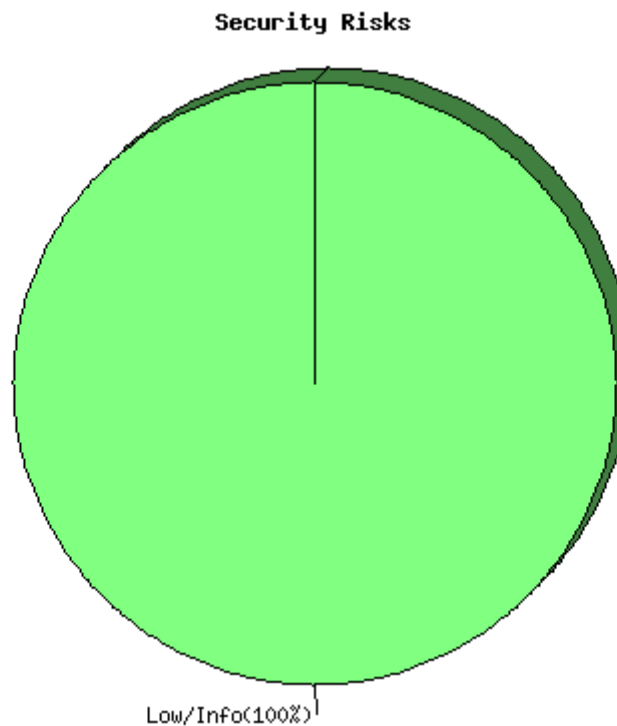
```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Appendix – Tools Outputs

Nessus Output

192.168.127.129

Repartition of the level of the security problems:



[\[Back to the index\]](#)

List of open ports :

- *norton-av-for-gateways-web-interface (8003/tcp)*
- *terabase (4000/tcp)*
- *ssh (22/tcp)*
- [https \(443/tcp\)](#) (Security notes found)
- *nfs (2049/tcp)*
- *shoutcast (8004/tcp)*
- *sunrpc (111/tcp)*
- [http \(80/tcp\)](#) (Security notes found)
- *ftp (21/tcp)*
- *fcpx-udp (810/tcp)*



- o *wpages (776/tcp)*

[\[back to the list of ports \]](#)

Information found on port https (443/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.

See also :

<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)
RewriteRule .* - [F]
```

Plugin output :



The server response from a TRACE request is :

```
TRACE /Nessus240472754.html HTTP/1.1
Connection: Close
Host: apache_appliance
Pragma: no-cache
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*
Accept-Language: en
Accept-Charset: iso-8859-1,*,utf-8
```

CVE : [CVE-2004-2320](#)
BID : [9506](#), [9561](#), [11604](#)
Other references : OSVDB:877
Nessus ID : [11213](#)

[\[back to the list of ports \]](#)

Information found on port http (80/tcp)

Synopsis :

Debugging functions are enabled on the remote HTTP server.

Description :

The remote webserver supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods which are used to debug web server connections.

It has been shown that servers supporting this method are subject to cross-site-scripting attacks, dubbed XST for "Cross-Site-Tracing", when used in conjunction with various weaknesses in browsers.

An attacker may use this flaw to trick your legitimate web users to give him their credentials.

Solution :

Disable these methods.

See also :



<http://www.kb.cert.org/vuls/id/867593>

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:N)

Solution :

Add the following lines for each virtual host in your configuration file :

```
RewriteEngine on  
RewriteCond %{REQUEST_METHOD} ^(TRACE|TRACK)  
RewriteRule .* - [F]
```

Plugin output :

The server response from a TRACE request is :

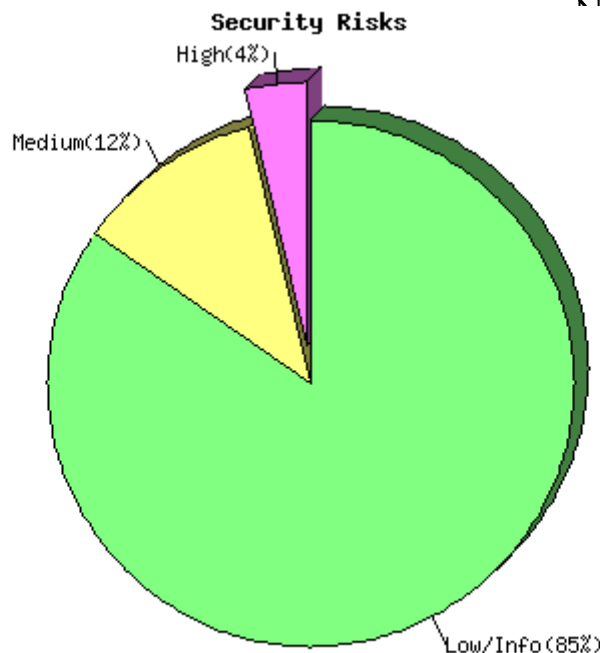
```
TRACE /Nessus240472754.html HTTP/1.1  
Connection: Close  
Host: apache_appliance  
Pragma: no-cache  
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)  
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, image/png, */*  
Accept-Language: en  
Accept-Charset: iso-8859-1,*,utf-8
```

CVE : [CVE-2004-2320](#)
BID : [9506](#), [9561](#), [11604](#)
Other references : OSVDB:877
Nessus ID : [11213](#)

This file was generated by [Nessus](#), the open-sourced security scanner.

192.168.127.130

Repartition of the level of the security problems:



[\[Back to the index\]](#)

List of open ports :

- [smtp \(25/tcp\)](#) (Security notes found)
- [sometimes-rpc21 \(32779/tcp\)](#)
- [ssh \(22/tcp\)](#) (Security notes found)
- [sometimes-rpc15 \(32776/tcp\)](#)
- [complex-link \(5001/tcp\)](#) (Security notes found)
- [sometimes-rpc9 \(32773/tcp\)](#)
- [submission \(587/tcp\)](#) (Security notes found)
- [smc-http \(6788/tcp\)](#) (Security notes found)
- [finger \(79/tcp\)](#) (Security notes found)
- [sometimes-rpc23 \(32780/tcp\)](#)
- [font-service \(7100/tcp\)](#)
- [telnet \(2003/tcp\)](#) (Security hole found)
- [sometimes-rpc17 \(32777/tcp\)](#)
- [lockd \(4045/tcp\)](#)
- [dtspcd \(6112/tcp\)](#)
- [filenet-rmi \(32771/tcp\)](#)
- [x11 \(6000/tcp\)](#) (Security notes found)
- [login \(513/tcp\)](#)
- [sunrpc \(111/tcp\)](#) (Security notes found)
- [smc-https \(6789/tcp\)](#) (Security notes found)
- [sometimes-rpc19 \(32778/tcp\)](#)



- [ftp \(21/tcp\)](#) (*Security notes found*)
- [filenet-pa \(32772/tcp\)](#)
- [shell \(514/tcp\)](#)
- [unknown \(32795/udp\)](#) (*Security warnings found*)
- [unknown \(32794/udp\)](#) (*Security warnings found*)
- [general/udp](#) (*Security notes found*)
- [general/tcp](#) (*Security notes found*)

[\[back to the list of ports \]](#)

Information found on port smtp (25/tcp)

An SMTP server is running on this port

Here is its banner :

220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:44:45 -
0700 (PDT)

Nessus ID : [10330](#)

[\[back to the list of ports \]](#)

Information found on port smtp (25/tcp)

Synopsis :

An SMTP server is listening on the remote port.

Description :

The remote host is running a mail (SMTP) server on this port.

Since SMTP servers are the targets of spammers, it is recommended you
disable it if you do not use it.

Solution :

Disable this service if you do not use it, or filter incoming traffic
to this port.

Risk factor :

None

Plugin output :

Remote SMTP server banner :

220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:44:45 -
0700 (PDT)

Nessus ID : [10263](#)

[\[back to the list of ports \]](#)



Information found on port ssh (22/tcp)

An ssh server is running on this port
Nessus ID : [10330](#)

[\[back to the list of ports \]](#)

Information found on port ssh (22/tcp)

Remote SSH version : SSH-2.0-Sun_SSH_1.1

Nessus ID : [10267](#)

[\[back to the list of ports \]](#)

Information found on port ssh (22/tcp)

The remote SSH daemon supports the following versions of the
SSH protocol :

- . 1.99
- . 2.0

Nessus ID : [10881](#)

[\[back to the list of ports \]](#)

Information found on port complex-link (5001/tcp)

A JAVA-LISTENER server is running on this port
Nessus ID : [17975](#)

[\[back to the list of ports \]](#)

Information found on port submission (587/tcp)

An SMTP server is running on this port
Here is its banner :
220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:45:05 -
0700 (PDT)
Nessus ID : [10330](#)

[\[back to the list of ports \]](#)

Information found on port submission (587/tcp)

Synopsis :



An SMTP server is listening on the remote port.

Description :

The remote host is running a mail (SMTP) server on this port.
Since SMTP servers are the targets of spammers, it is recommended you disable it if you do not use it.

Solution :

Disable this service if you do not use it, or filter incoming traffic to this port.

Risk factor :

None

Plugin output :

Remote SMTP server banner :

220 unknown ESMTP Sendmail 8.13.7+Sun/8.13.7; Thu, 15 Mar 2007 07:45:05 - 0700 (PDT)

Nessus ID : [10263](#)

[\[back to the list of ports \]](#)

Information found on port smc-http (6788/tcp)

A web server is running on this port

Nessus ID : [10330](#)

[\[back to the list of ports \]](#)

Information found on port smc-http (6788/tcp)

The remote web server type is :

Apache-Coyote/1.1

and the 'ServerTokens' directive is ProductOnly

Apache does not permit to hide the server type.

Nessus ID : [10107](#)

[\[back to the list of ports \]](#)

Information found on port smc-http (6788/tcp)

Synopsis :

Some information about the remote HTTP configuration can be



extracted.

Description :

This test gives some information about the remote HTTP protocol - the version used, whether HTTP Keep-Alive and HTTP pipelining are enabled, etc...

This test is informational only and does not denote any security problem

Solution :

None.

Risk factor :

None / CVSS Base Score : 0
(AV:R/AC:L/Au:NR/C:N/A:N/I:N/B:N)

Plugin output :

Protocol version : HTTP/1.1
SSL : no
Pipelining : yes
Keep-Alive : no
Options allowed : (Not implemented)
Headers :

Location: <http://192.168.127.130/console/faces/jsp/login/BeginLogin.jsp>
Content-Length: 0
Date: Thu, 15 Mar 2007 14:47:36 GMT
Server: Apache-Coyote/1.1

Nessus ID : [24260](#)

[\[back to the list of ports \]](#)

Information found on port finger (79/tcp)

A finger server seems to be running on this port
Nessus ID : [10330](#)

[\[back to the list of ports \]](#)

Vulnerability found on port telnet (23/tcp)



Synopsis :

It is possible to log into the remote system using telnet without supplying any credentials

Description :

The remote version of telnet does not sanitize the user-supplied 'USER' environment variable. By supplying a specially malformed USER environment variable, an attacker may force the remote telnet server to believe that the user has already authenticated.

For instance, the following command :

```
telnet -l '-fbin' 192.168.127.130
```

Will result in obtaining a shell with the privileges of the 'bin' user.

Solution :

Install patches 120068-02 (sparc) or 120069-02 (i386) which are available from Sun.

Filter incoming to this port or disable the telnet service and use SSH instead, or use inetadm to mitigate this problem (see the link below).

See also :

<http://lists.sans.org/pipermail/list/2007-February/025935.html>
<http://isc.sans.org/diary.html?storyid=2220>

Risk factor :

Critical / CVSS Base Score : 10
(AV:R/AC:L/Au:NR/C:C/I:C/A:C/B:N)

Plugin output :

It was possible to log into the remote host as 'bin' :
uid=2(bin) gid=2(bin)

The file /etc/passwd contains :



```
cat /etc/passwd
root:x:0:0:Super-User:/:usr/bin/tcsh
daemon:x:1:1:/:
bin:x:2:2:usr/bin:
sys:x:3:3:/:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
smmsp:x:25:25:SendMail Message Submission Program:/:
listen:x:37:4:Network Admin:/usr/net/nls:
gdm:x:50:50:GDM Reserved UID:/:
webservd:x:80:80:WebServer Reserved UID:/:
nobody:x:60001:60001:NFS Anonymous Access User:/:
noaccess:x:60002:60002:No Access User:/:
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/:
$
CVE : CVE-2007-0882
BID : 22512
Nessus ID : 24323
```

[\[back to the list of ports \]](#)

Warning found on port telnet (23/tcp)

Synopsis :

A telnet server is listening on the remote port

Description :

The remote host is running a telnet server.
Using telnet is not recommended as logins, passwords and commands are transferred in clear text.

An attacker may eavesdrop on a telnet session and obtain the credentials of other users.

Solution :

Disable this service and use SSH instead

Risk factor :

Medium / CVSS Base Score : 4
(AV:R/AC:L/Au:NR/C:P/A:N/I:N/B:C)



Plugin output:

Remote telnet banner:

login:

Nessus ID : [10281](#)

[\[back to the list of ports \]](#)

Information found on port telnet (23/tcp)

A telnet server seems to be running on this port

Nessus ID : [10330](#)

[\[back to the list of ports \]](#)

Information found on port x11 (6000/tcp)

Synopsis :

An X11 server is listening on the remote host

Description :

The remote host is running an X11 server. X11 is a client-server protocol which can be used to display graphical applications running on a given host on a remote client.

Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Solution :

Restrict access to this port. If the X11 client/server facility is not used, disable TCP entirely.

Risk factor :

Low / CVSS Base Score : 2
(AV:R/AC:H/Au:R/C:P/A:N/I:N/B:C)

Plugin output :

X11 Version : 11.0

Nessus ID : [10407](#)



Information found on port sunrpc (111/tcp)

The RPC portmapper is running on this port.

An attacker may use it to enumerate your list of RPC services. We recommend you filter traffic going to this port.

Risk factor : Low

CVE : [CVE-1999-0632](#), [CVE-1999-0189](#)

BID : [205](#)

Nessus ID : [10223](#)

[\[back to the list of ports \]](#)

Information found on port smc-https (6789/tcp)

An unknown server is running on top of SSL/TLS on this port. You should change find_service preferences to look for SSL based services and restart your scan.

** Because of Nessus architecture, it is now too late
** to properly identify this service.

Nessus ID : [11153](#)

[\[back to the list of ports \]](#)

Information found on port ftp (21/tcp)

An FTP server is running on this port.

Here is its banner :

220 unknown FTP server ready.

Nessus ID : [10330](#)

[\[back to the list of ports \]](#)

Information found on port ftp (21/tcp)

Synopsis :

An FTP server is listening on this port

Description :



It is possible to obtain the banner of the remote FTP server by connecting to the remote port.

Risk factor :

None

Plugin output :

The remote FTP banner is :
220 unknown FTP server ready.
Nessus ID : [10092](#)

[\[back to the list of ports \]](#)

Warning found on port unknown (32795/udp)

The rusersd RPC service is running. It provides attacker interesting information such as how often the system is being used, the names of the users, and more.

It is usually not a good idea to leave this service open.

Risk factor : Low

CVE : [CVE-1999-0626](#)

Nessus ID : [10228](#)

[\[back to the list of ports \]](#)

Information found on port unknown (32795/udp)

Using rusers, we could determine that the following users are logged in :

- root (console) from :0
- root (pts/3) from :0.0
- root (pts/4) from :0.0

Solution : disable this service.

Risk factor : Low

CVE : [CVE-1999-0626](#)

Nessus ID : [11058](#)

[\[back to the list of ports \]](#)

Warning found on port unknown (32794/udp)



The rstatd RPC service is running. It provides an attacker interesting information such as :

- the CPU usage
- the system uptime
- its network usage
- and more

Letting this service run is not recommended.

Risk factor : Low

CVE : [CVE-1999-0624](#)

Nessus ID : [10227](#)

Information found on port general/udp

For your information, here is the traceroute from 192.168.127.128 to 192.168.127.130 :

```
192.168.127.130 :  
192.168.127.128  
192.168.127.130
```

Nessus ID : [10287](#)

Information found on port general/tcp

The remote host is running one of these operating systems :

Sun Solaris 10

Sun Solaris 9

Nessus ID : [11936](#)

[\[back to the list of ports \]](#)

Information found on port general/tcp

Information about this scan :

Nessus version : 3.1.2

Plugin feed version : 200702200055

Type of plugin feed : Release

Scanner IP : 192.168.127.128

Port scanner(s) : nessus_tcp_scanner

Port range : default

Thorough tests : no

Experimental tests : no

Paranoia level : 1

Report Verbosity : 1

Safe checks : yes

Information Technology
Information Security Systems and Compliance



NORTHWESTERN
UNIVERSITY

Max hosts : 1
Max checks : 4
Scan Start Date : 2007/3/15 9:44
Scan duration : 261 sec
Nessus ID : [19506](#)



Vulnerability Exploitation / Penetration Testing

HOST: 192.168.127.130 (Solaris web/app server)

Nessus found a security hole in the Telnet daemon on 192.168.127.130. Per the notes in the aforementioned Nessus output, an unauthenticated telnet session was established for the user "bin" remotely (see screenshot below):

A terminal window titled "root@jholland-ubuntu1: ~/nessus_report2/nessus_report2" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal output shows a telnet session to 192.168.127.130. The user "bin" is established without authentication. The user runs "id" and "exit", and the connection is closed by the foreign host.

```
root@jholland-ubuntu1:~/nessus_report2/nessus_report2# telnet -l '-fbin' 192.168.127.130
Trying 192.168.127.130...
Connected to 192.168.127.130.
Escape character is '^]'.
Last login: Thu Mar 15 07:48:44 from 192.168.127.128
Sun Microsystems Inc. SunOS 5.10 Generic January 2005
$ id
uid=2(bin) gid=2(bin)
$ exit
Connection closed by foreign host.
root@jholland-ubuntu1:~/nessus_report2/nessus_report2#
```



Google Hacking

Search string	Result
Client declined this service	



Firewall Analysis Template

fingerprinting

This test is to determine the success of various packet response fingerprinting methods through the firewall.

Method	Result
Client declined this service	

stealth

This determines the viability of SYN stealth scanning through the firewall for enumeration.

Result

Client declined this service

source port control

This test measures the use of scanning with specific source ports through the firewall for enumeration.

Protocol	Source Port	Result
UDP	53	Client declined this service
UDP	161	
TCP	53	
TCP	69	

ICMP Responses

This test is to measure the firewall's response to various types of ICMP packets.

type	type description	response	RTT
Client declined this service			

Protocol

This test is to discover the firewall's ability to screen packets of various protocols.

Protocol	Result
Client declined this service	



Social Engineering Target Template

TargetDefinition

Name	E-mail	Telephone	Description
Client declined this service			

Social Engineering Telephone Attack Template

Attack Scenario	Client declined this service
Telephone #	
Person	
Description	
Results	

Social Engineering E-mail Attack Template

Attack Scenario	Client declined this service
Email	
Person	
Description	
Results	

Personally Identifiable Information (PII)

Info Found / Location	Client declined this service
Info Found / Location	
Info Found / Location	
Info Found / Location	
Info Found / Location	



Password Cracking Template

ProtectedFile

File name	Client declined this service
File type	
Crack time	
User name	
Password	

EncodedPasswordFile

IP Address	Client declined this service
Service Port	
Service Type	
Protocol	
File name	
File type	
Crack time	
Login Names	
Passwords	

ProtectedOnlineService

IP Address	Client declined this service
Service Port	
Service Type	
Protocol	
Login Names	
Passwords	



Security Policy Review

Tasks to perform for a thorough Security Policy review

- 1. Measure the security policy points against the actual state of the Internet presence.
- 2. *Approval from Management* -- Look for any sign (e.g. signature) that reveals that the policy is approved by management. Without this approval the policy is useless because staff is not required to meet the rules outlined within. From a formal point of view you could stop investigating the policy if it is not approved by management. However, testing should continue to determine how effective the security measures are on the actual state of the internet presence.
- 3. Ensure that documentation is kept, either electronically or otherwise, that the policy has been read and accepted by people before they are able to gain any access to the computer systems.
- 4. Identify incident handling procedures, to ensure that breaches are handled by the correct individual(s) and that they are reported in an appropriate manner.
- 5. *Inbound connections* -- Check out any risks mentioned on behalf of the Internet inbound connections (internet->DMZ, internet -> internal net) and measures which may be required to be implemented to reduce or eliminate those risks. These risks could be allowed on incoming connections, typically SMTP, POP3, HTTP, HTTPS, FTP, VPNs and the corresponding measures as authentication schemes, encryption and ACL. Specifically, rules that deny any stateful access to the internal net are often not met by the implementation.
- 6. *Outbound connections* -- Outbound connections could be between internal net and DMZ, as well as between internal net and the Internet. Look for any outbound rules that do not correspond to the implementation. Outbound connections could be used to inject malicious code or reveal internal specifics.
- 7. *Security measures* -- Rules that require the implementation of security measures should be met. Those could be the use of AVS, IDS, firewalls, DMZs, routers and their proper configuration/implementation according to the outlined risks to be met.
- 8. Measure the security policy points against the actual state of non-Internet connections.
- 9. *Modems* -- There should be a rule indicating that the use of modems that are not specially secured is forbidden or at least only allowed if the modems are disconnected when not in use, and configured to disallow dial-in. Check whether a corresponding rule exists and whether the implementation follows the requirements.
- 10. *Fax machines* -- There should be a rule indicating that the use of fax machines which can allow access from the outside to the memory of the machines is forbidden or at least only allowed if the machines are powered down when not in use. Check whether a corresponding rule exists and whether the implementation follows the requirements.
- 11. Measure the security policy against containment measures and social engineering tests based on the organization's employees' misuse of the Internet according to business justification and best security practices.