Information Technology

Information and Systems Security/Compliance

Information Security Vulnerability Assessment Program

Version: 1.0

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
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Version</th>
<th>Modified By</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/28/07</td>
<td>1.0</td>
<td>D. Kovarik</td>
<td>Initial publication</td>
</tr>
</tbody>
</table>

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
Table of Contents

Revisions ............................................................................................................................. 2
Contacts ............................................................................................................................. 2
Overview ............................................................................................................................. 4
Focus of Vulnerability Assessment Program ................................................................. 5
Required Elements .......................................................................................................... 5
Vulnerability Assessment Methodology ........................................................................... 6
Resources/References ..................................................................................................... 9
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 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 know 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 documented request by, and an agreement with, the Client for a Vulnerability Assessment, policy assessment, etc. This will include identification of which assessment profiles the Client requires (see Vulnerability Assessment Profiles section, page 11).
- 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 Non Disclosure Agreement (NDA) (see page 18) signed by ISS/C and Client Management.

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 can 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, and are detailed in the Vulnerability Assessment and Remediation Agreement (see page 13):

• A written request and agreement between ISS/C and the Client receiving the Assessment detailing what will be required of the Client, what will be provided by ISS/C, when the Assessment will take place and when the resulting findings report will be made available to the Client.

Client Requests should include, at a minimum:

  o What Client personnel are the key contacts before, during and after Assessment?
  o Why the Client is requesting the Assessment (e.g. compliance testing, assessment of networks handling sensitive data, etc)?
  o What are the goals and expectations of the Client after receiving the Assessment and resulting report?
  o What resources will be assessed (IP addresses, and hostnames if available)?
  o What resources shall not be assessed (IP addresses, and hostnames required)?

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

  o What IP address range will be used to originate Assessment activities
  o Dates and times the Assessment activities may be carried out
  o A signed document that identifies and accepts the risk that is inherent to Vulnerability Assessment activities and describes the limitation of liability of personnel involved in the Assessment


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 senior management sign-off on Assessment plan
4. Coordinate kick-off meeting to discuss Assessment activities
   - ISS/C and the Client review, agree to and sign the Assessment Agreement (see page 13).

- 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.

Paraphrasing the SANS article at [http://www.coresecurity.com/files/attachments/SANS_Penetration_Testing.pdf](http://www.coresecurity.com/files/attachments/SANS_Penetration_Testing.pdf) (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
  o Sample Policies - http://www.sans.org/resources/policies/
  o Misc Resouces - 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


[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.

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.
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.

Assessments may be conducted to:

- 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 a “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:

________________________________________________________________________
<table>
<thead>
<tr>
<th>NUIT Senior Management</th>
<th>Client Senior Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: __________________</td>
<td>Name: __________________</td>
</tr>
<tr>
<td>Title: _________________</td>
<td>Title: _________________</td>
</tr>
<tr>
<td>Date: __________________</td>
<td>Date: __________________</td>
</tr>
</tbody>
</table>

| 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.

<table>
<thead>
<tr>
<th>Type or print name of Client</th>
<th>Information and Systems Security/Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>By: ________________________</td>
<td>By: ________________________</td>
</tr>
<tr>
<td>Signature</td>
<td>Signature</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Print or Type Name</th>
<th>Print or Type Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Title</td>
</tr>
<tr>
<td>Telephone</td>
<td>Telephone</td>
</tr>
<tr>
<td>Address</td>
<td>Address</td>
</tr>
</tbody>
</table>
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 positives 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 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 TRAC... track 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.
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:

```apache
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:


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

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain Name(s)</th>
<th>Operating System</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.127.129</td>
<td>Apache Web Server Appliance</td>
<td>Linux (rpath)</td>
</tr>
<tr>
<td>192.168.127.130</td>
<td>Solaris Web Server (Solaris 10)</td>
<td>Solaris 10</td>
</tr>
</tbody>
</table>

Zone Transfer Highlights

n/a
# Server 1 Information

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Domain Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.127.129</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Service</th>
<th>(Port/Protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td>onorton-av-for-gateways-web-interface</td>
<td>(8003/tcp)</td>
</tr>
<tr>
<td>oterabase</td>
<td>(4000/tcp)</td>
</tr>
<tr>
<td>ossh</td>
<td>(22/tcp)</td>
</tr>
<tr>
<td>ohttps</td>
<td>(443/tcp) (Security notes found)</td>
</tr>
<tr>
<td>onfs</td>
<td>(2049/tcp)</td>
</tr>
<tr>
<td>oshoutcast</td>
<td>(8004/tcp)</td>
</tr>
<tr>
<td>osunrpc</td>
<td>(111/tcp)</td>
</tr>
<tr>
<td>ohttp</td>
<td>(80/tcp) (Security notes found)</td>
</tr>
<tr>
<td>oftp</td>
<td>(21/tcp)</td>
</tr>
<tr>
<td>ofcp-udp</td>
<td>(810/tcp)</td>
</tr>
<tr>
<td>owpages</td>
<td>(776/tcp)</td>
</tr>
</tbody>
</table>

## BANNER(S):

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>TCP</td>
<td>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, <em>/</em> Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8</td>
</tr>
<tr>
<td>80</td>
<td>TCP</td>
<td>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, <em>/</em> Accept-Language: en Accept-Charset: iso-8859-1,*,utf-8</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Service</th>
<th>(Port/Protocol)</th>
</tr>
</thead>
<tbody>
<tr>
<td>o smtp</td>
<td>(25/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o sometimes-rpc 21</td>
<td>(32779/tcp)</td>
</tr>
<tr>
<td>o ssh</td>
<td>(22/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o sometimes-rpc 15</td>
<td>(32776/tcp)</td>
</tr>
<tr>
<td>o commplex-link</td>
<td>(5001/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o sometimes-rpc 9</td>
<td>(32773/tcp)</td>
</tr>
<tr>
<td>o submission</td>
<td>(587/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o smc-http</td>
<td>(6788/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o finger</td>
<td>(79/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o sometimes-rpc 23</td>
<td>(32780/tcp)</td>
</tr>
<tr>
<td>o font-service</td>
<td>(7100/tcp)</td>
</tr>
<tr>
<td>o telnet</td>
<td>(23/tcp) (Security hole found)</td>
</tr>
<tr>
<td>o sometimes-rpc 17</td>
<td>(32777/tcp)</td>
</tr>
<tr>
<td>o lockd</td>
<td>(4045/tcp)</td>
</tr>
<tr>
<td>o dtspcd</td>
<td>(6112/tcp)</td>
</tr>
<tr>
<td>o filenet-rmi</td>
<td>(32771/tcp)</td>
</tr>
<tr>
<td>o x11</td>
<td>(6000/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o login</td>
<td>(513/tcp)</td>
</tr>
<tr>
<td>o sunrpc</td>
<td>(111/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o smc-https</td>
<td>(6789/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o sometimes-rpc 19</td>
<td>(32778/tcp)</td>
</tr>
<tr>
<td>o ftp</td>
<td>(21/tcp) (Security notes found)</td>
</tr>
<tr>
<td>o filenet-pa</td>
<td>(32772/tcp)</td>
</tr>
<tr>
<td>o shell</td>
<td>(514/tcp)</td>
</tr>
<tr>
<td>o unknown</td>
<td>(32795/udp) (Security warnings)</td>
</tr>
<tr>
<td>o unknown</td>
<td>(32794/udp) (Security warnings)</td>
</tr>
<tr>
<td>o general/udp</td>
<td>(Security notes found)</td>
</tr>
<tr>
<td>o general/tcp</td>
<td>(Security notes found)</td>
</tr>
</tbody>
</table>

### BANNER(S):

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Banner</th>
</tr>
</thead>
<tbody>
<tr>
<td>25</td>
<td>TCP</td>
<td>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</td>
</tr>
<tr>
<td>587</td>
<td>TCP</td>
<td>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</td>
</tr>
<tr>
<td>23</td>
<td>TCP</td>
<td>Remote telnet banner: login:</td>
</tr>
</tbody>
</table>
An FTP server is running on this port. Here is its banner:
220 unknown FTP server ready.

**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 web server 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:N/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 web server 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:

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)
- fcp-udp (810/tcp)
o wpages (776/tcp)

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

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:
Risk factor:

Low / CVSS Base Score: 2

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:
List of open ports:

- **smtp (25/tcp)** (Security notes found)
- **sometimes-rpc21 (32779/tcp)**
- **ssh (22/tcp)** (Security notes found)
- **sometimes-rpc15 (32776/tcp)**
- **commplex-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)**
- **dtspecd (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)**
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

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
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 commplex-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

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

A web server is running on this port
Nessus ID: 10330

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

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

Synopsis:

Some information about the remote HTTP configuration can be

[ back to the list of ports ]
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

Information found on port finger (79/tcp)

A finger server seems to be running on this port
Nessus ID : 10330

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://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:
uuucp: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:6001:6001:NFS Anonymous Access User:/
nocroot:x:6002:6002:No Access User:/
nobody4:x:65534:65534:SunOS 4.x NFS Anonymous Access User:/
$
CVE : CVE-2007-0882
BID : 22512
Nessus ID : 24323

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:N/RC:P/A:N/I:N/B:C)
Plugin output:

Remote telnet banner:
login:
Nessus ID : 10281

Information found on port telnet (23/tcp)

A telnet server seems to be running on this port
Nessus ID : 10330

Information found on port x11 (6000/tcp)

Synopsis :

A X11 server is listening on the remote host

Description :

The remote host is running a 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

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

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

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

Warning found on port unknown (32795/udp)
The rusersd RPC service is running. It provides an attacker interesting information such as how often the system is being used, the names of the users, and more.

It usually not a good idea to leave this service open.
Risk factor: Low
CVE: CVE-1999-0626
Nessus ID: 10228

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

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:
192.168.127.128
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

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
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):
### Google Hacking

<table>
<thead>
<tr>
<th>Search string</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client declined this service</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Firewall Analysis Template

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

<table>
<thead>
<tr>
<th>Method</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client declined this service</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client declined this service</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Source Port</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>UDP</td>
<td>53</td>
<td>Client declined this service</td>
</tr>
<tr>
<td>UDP</td>
<td>161</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>TCP</td>
<td>69</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>type</th>
<th>type description</th>
<th>response</th>
<th>RTT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client declined this service</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client declined this service</td>
<td></td>
</tr>
</tbody>
</table>


### Social Engineering Target Template

**Target Definition**

<table>
<thead>
<tr>
<th>Name</th>
<th>E-mail</th>
<th>Telephone</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client declined this service</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Social Engineering Telephone Attack Template

<table>
<thead>
<tr>
<th>Attack Scenario</th>
<th>Client declined this service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telephone #</td>
<td></td>
</tr>
<tr>
<td>Person</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Results</td>
<td></td>
</tr>
</tbody>
</table>

### Social Engineering E-mail Attack Template

<table>
<thead>
<tr>
<th>Attack Scenario</th>
<th>Client declined this service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td></td>
</tr>
<tr>
<td>Person</td>
<td></td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>Results</td>
<td></td>
</tr>
</tbody>
</table>

### Personally Identifiable Information (PII)

<table>
<thead>
<tr>
<th>Info Found / Location</th>
<th>Client declined this service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Info Found / Location</td>
<td></td>
</tr>
<tr>
<td>Info Found / Location</td>
<td></td>
</tr>
<tr>
<td>Info Found / Location</td>
<td></td>
</tr>
<tr>
<td>Info Found / Location</td>
<td></td>
</tr>
<tr>
<td>Info Found / Location</td>
<td></td>
</tr>
</tbody>
</table>
**Password Cracking Template**

### Protected File

<table>
<thead>
<tr>
<th><strong>File name</strong></th>
<th><strong>Client declined this service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File type</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Crack time</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Encoded Password File

<table>
<thead>
<tr>
<th><strong>IP Address</strong></th>
<th><strong>Client declined this service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Port</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Service Type</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td></td>
</tr>
<tr>
<td><strong>File name</strong></td>
<td></td>
</tr>
<tr>
<td><strong>File type</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Crack time</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Login Names</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Passwords</strong></td>
<td></td>
</tr>
</tbody>
</table>

### Protected Online Service

<table>
<thead>
<tr>
<th><strong>IP Address</strong></th>
<th><strong>Client declined this service</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Port</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Service Type</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Login Names</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Passwords</strong></td>
<td></td>
</tr>
</tbody>
</table>
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.