

**FEDERAL TRADE COMMISSION
OFFICE OF INSPECTOR GENERAL**



AUDIT REPORT

GISRA TECHNICAL EVALUATION REPORT



OFFICE OF
INSPECTOR GENERAL

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

September 16, 2002

Chairman Muris:

The Office of Inspector General (OIG) recently completed its review of information security pursuant to requirements contained in the Government Information Security Reform Act (GISRA). This is the second annual evaluation completed by the OIG. Our first report, issued in September 2001, focused on the management (policies) and operational aspects (procedures) of security controls at the FTC. This year, the OIG performed a technical assessment of the FTC's Information Technology (IT) environment, to include network infrastructure (routers, hubs and switches), desk top and server systems (PCs, e-mail and database servers) and select application systems.

The review team performed its scans from inside the agency by hooking up to the network through a port located in the OIG. The team did not perform an external penetration test, i.e., we did not try to "break in" to the FTC's computer system from outside the agency. Rather, the review team focused on mapping the internal network and equipment on the network to search for vulnerabilities that would enable individuals provided with network access to move beyond their authorizations and access sensitive systems.

The internal scan identified both strengths and weaknesses in the agency's information security program. On the positive side, the review team was unsuccessful in accessing information stored on the hard drives of FTC employees. The review team found that the remote management account on each desktop to be protected by a strong password. We also found network servers to be configured securely.

On the negative side, the OIG found vulnerabilities that permitted the review team to obtain unauthorized access to sensitive resources and information. Although access was possible, no sensitive files or data were downloaded by the review team. If any disgruntled employee, student, or contract employee with malicious intent, achieved the same level of access, they could have read, altered or deleted any data file stored on any one of the agency's data servers, to include such information as premerger filings and consumer complaints, employee e-mails or Commission minutes from nonpublic meetings. The attached OIG Technical Evaluation Report (AR 02-053) details these various vulnerabilities.

The OIG, in performing its work, used readily-available software tools, many of them freely downloaded from the Internet, to scan the network and identify linked computers. The scans found that many of the PCs or computers were configured to share files with anyone who knew where to look. The scans also revealed that many of the computers required no passwords for access or were "protected" by easily crackable passwords such as "administrator." As mentioned earlier, such rudimentary security oversights were not found on desktop computers where one might expect security lapses to occur. Rather, these were identified on Network servers and routers that are managed by IT specialists and provide access to all of the agency's sensitive information.

Such vulnerabilities were generally of the common "housekeeping" variety (as opposed to architectural or systemic vulnerabilities) and can be easily corrected with little or no additional resources. Many occur because security components of operating software are often left set on the lowest default level to ease installation and administration. The initial password is then not changed or deleted.

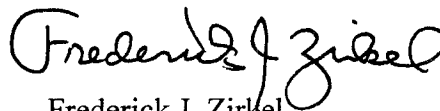
ITM staff working with OIG evaluators have already taken steps to address many of the vulnerabilities identified in the attached evaluation report.

The OIG understands that the majority of FTC users are unlikely to possess the technical computer knowledge to achieve the level of access obtained by the OIG. But the OIG believes that there exists a fairly significant population of individuals working at the agency with the requisite skills to achieve the same results as OIG evaluators. Many of these individuals are students or contractors who do not undergo any background check.

The review was conducted from May 15, 2002 to August 26, 2002. The review followed NIST guidance for information systems, OMB information security circulars and best practices used in the industry.

The OIG wishes to thank ITM management for the cooperation and assistance it provided during the period of our review.

Respectfully submitted,



Frederick J. Zirkel
Inspector General

**Federal Trade Commission
Enterprise Network**

Vulnerability Analysis

PREPARED BY:



SeNet International Corporation

e-Security—we make it practical.

TABLE OF CONTENTS

	<u>Page</u>
1. Introduction.....	1
2. Internal Vulnerability Tests.....	1
2.1 Enumeration.....	1
2.2 Scans.....	2
2.3 Penetration Planning.....	4
2.4 Penetration Testing.....	4
3. Overview of Findings.....	6
4. Findings , Implications and Recommendations.....	8

APPENDICES

Vulnerabilities Summary Matrix.....	I
Oracle Database Vulnerabilities.....	II

1 Introduction

The Government Information Security Reform Act (Security Act) directs Offices of Inspector General to perform an annual independent evaluation of the information security program and practices of the agency. For the FY 2002 review, the OIG performed a network based scan of the FTC local area network (LAN) to identify weakly protected devices including servers, hosts and network gear. The OIG also sought to identify other vulnerabilities that would enable individuals provided with network access (agency employees, contractors, consultants, students and other government employees) to gain unauthorized access to sensitive FTC databases. Scan results are presented below.

2 Internal Vulnerability Tests

Internal vulnerability tests were performed by connecting directly into the FTC headquarters LAN, as any employee with an FTC email account or any other desktop application could do, and conducting network-based scans (as opposed to host-based scans). No network login rights and/or application access privileges were provided to the test team for the purpose of these tests. Throughout the tests, the team took steps to protect any sensitive information collected and prevent accidental disruption to the operation of systems and applications.

The tests were conducted during two periods. The first period was 15 May 2002 through 30 May 2002. This initial test focused on the Oracle database systems (see letter to CIO, dated May 31, 2002, regarding oracle database vulnerabilities at Appendix II). The second test period was 10 July 2002 through 20 July 2002. It covered network devices (hubs, switches, routers) desktop systems (Windows NT and Windows 2000) and servers (Unix and Windows). The latter tests also revisited the Oracle databases to confirm that previously found vulnerabilities had been corrected.

2.1 Enumeration

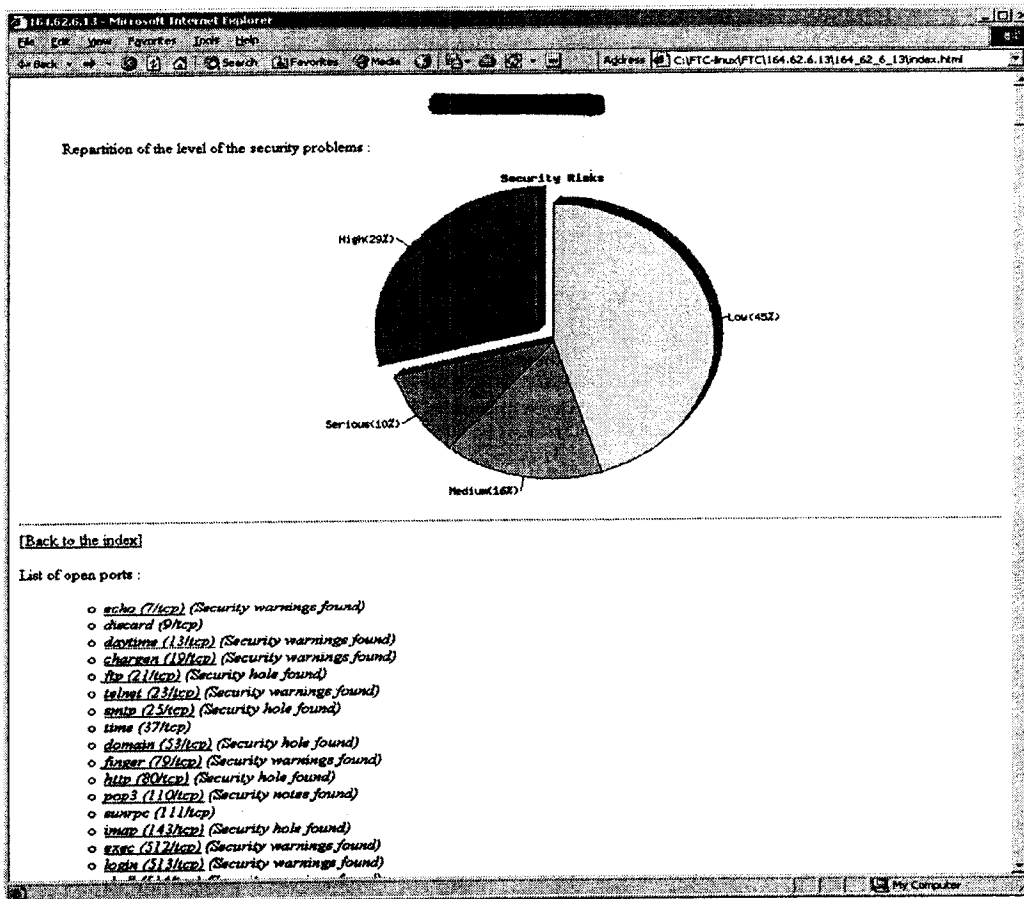
The purpose of this first step was to map the systems or identify all active hosts on the FTC network, including their IP addresses and services running on them, along with possible vulnerabilities. This automated process is facilitated by using scanning tools that are freely and widely available on the Internet.

To identify all active hosts on the FTC network we performed a ping scan on the entire FTC allocated IP address-range [REDACTED]. The result was a list of all hosts that replied to the ping requests. Below is a sample section of that list. As names are not hidden, such a list will provide an inside attacker with a good idea about the function of each listed system.

```
Host gwmigrate2 [REDACTED] appears to be up
Host fp01.trade.ftc.gov ([REDACTED]) appears to be up
Host webmail.trade.ftc.gov ([REDACTED]) appears to be up
Host dcmail2.trade.ftc.gov ([REDACTED]) appears to be up
Host fp02.trade.ftc.gov ([REDACTED]) appears to be up
Host dcmail4.trade.ftc.gov ([REDACTED]) appears to be up
Host cd1.trade.ftc.gov ([REDACTED]) appears to be up
Host interorg.trade.ftc.gov ([REDACTED]) appears to be up
Host dcmail.trade.ftc.gov ([REDACTED]) appears to be up
Host apps4.trade.ftc.gov ([REDACTED]) appears to be up
```

2.2 Scans

In the second step, the OIG ran port and vulnerability scanners (nmap and nessus, respectively which are freely available on the internet) to collect information on open ports and running services. These tests were performed on selected servers that were identified as the most “interesting,” e.g., servers where sensitive agency information may be stored, such as email servers and/or Unix database servers housing sensitive data. These servers were identified based on the name and, occasionally, on the IP address of the lists. Below is an example of scan result that clearly shows listed open ports and potential vulnerabilities found on the host:



To find all available shared drives and user accounts on the Windows network we ran NTInfoScan (NTIS) on the entire FTC IP range. The sample result of that scan is displayed below:

NTInfoScan
Results
for

by {David Litchfield}

NetBIOS

```

Share Information
Share Name :IPC$
Share Type :Default Pipe Share
Comment :Remote IPC
WARNING - Null session can be established to \\[REDACTED]\IPC$
Share Name :D$
Share Type :Default Disk Share
Comment :Default share

Share Name :ADMIN$
Share Type :Default Disk Share
Comment :Remote Admin

Share Name :C$
Share Type :Default Disk Share
Comment :Default share
Account Information
Account Name :Administrator
The Administrator account is an ADMINISTRATOR, and the password was
changed 387 days ago. This account has been used 176 times to logon.
The default Administrator account has not been renamed. Consider renaming
this account
and removing most of its rights. Use a different account as the admin
account.

Comment :Built-in account for administering the computer/domain
User Comment :
Full name :

Account Name :Guest
The Guest account is a GUEST, and the password was
changed 0 days ago. This account has been used 0 times to logon.

Comment :Built-in account for guest access to the
computer/domain
User Comment :
Full name :

Account Name :SMSCliSvcAcct&
The SMSCliSvcAcct& account is an ADMINISTRATOR, and the password was
changed 387 days ago. This account has been used 64 times to logon.

Comment :DO NOT MODIFY. Systems Management Server Internal
Account
User Comment :
Full name :SMSCliSvcAcct&

Account Name :SMSCliToknAcct&
The SMSCliToknAcct& account is a GUEST, and the password was
changed 0 days ago. This account has been used 62 times to logon.

Comment :DO NOT MODIFY. Systems Management Server Internal
Account
User Comment :
Full name :SMSCliToknAcct&

```

In addition to shares, NTIS also provides information such as user accounts local to each system. It also flags accounts with no and/or easily guessable passwords.

2.3 Penetration Planning

After the enumeration and scan phases, the OIG audit team had collected a substantial amount of useful information. The collected data was reviewed for the most “promising” vulnerabilities. Three vulnerabilities were noted:

1. Port scan on selected hosts showed two Cisco switches or routers ([REDACTED], [REDACTED]) that run vulnerable administrator web servers.
2. Four Windows servers have blank Administrator passwords. These servers’ IP addresses are [REDACTED], [REDACTED], [REDACTED] and [REDACTED]. Because of the blank passwords, these four servers were selected as targets for penetration.
3. The FTP server on [REDACTED] allows anonymous access to multiple directories including /.www. That server was selected as the OIG’s primary target.

2.4 Penetration Testing

The OIG attempted to exploit the vulnerabilities identified above. Using a web browser, we connected to Cisco web admin at <http://nnn.nnn.nnn.nnn//level/16/exec/show/config/cr> and collected running configuration files from both vulnerable switches. Analyzing these configuration files we found that a global access password (hauptwache) is exposed in one of these switches. Below is the fragment with exposed password:

```
ip default-gateway [REDACTED]
snmp-server engineID local 00000009020000027E658AC0
snmp-server community Fireball6Pa RO
snmp-server community Fireball1%Pa RW
snmp-server community FTCPenn6Pa% RW
snmp-server community public view vdefault RO
snmp-server chassis-id 0x12
snmp-server host [REDACTED] trap public
!
line con 0
  transport input none
  stopbits 1
line vty 0 4
  password [REDACTED]
  login
line vty 5 15
  password [REDACTED]
  login
```

The OIG also noted that SNMP community strings used on that router are global too. At that point, the team stopped the network penetration attempt, since we essentially gained full control of all Cisco equipment.

We connected to all Windows servers without an Administrator password assigned. On each of these servers we ran the LSADump utility. After analyzing results of LSA dumps we created

a file containing three passwords established by FTC IT staff (9Service19, hebrews6:12 and BigDummyValue).

Based on the results of the NTInfoScan, the OIG compiled a list of all administrators on the FTC network. Finally, we ran a script that attempted to connect to one of the backup domain controller (BDC) servers with every user "id" from the list with all three passwords. As a result of that step, we found an administrator account on the FTC Windows network. That account (harris) allowed us to gain full-*unlimited* control over all major Windows servers.

Using the just-discovered Domain Administrator account, we collected all user names and encrypted passwords from the primary domain controller (PDC) and one of the BDCs. An attacker could probably decrypt most of these passwords in a matter of hours if not minutes. While the audit team did seek to identify administrator passwords, we did not decrypt any user passwords used by staff to log on to the network or other applications. All FTC users can continue to use their current passwords.

With the Domain Administrator account, we connected to several Windows servers and workstations looking for additional information that would allow us to gain access to one of the UNIX servers. We found several very old backup scripts on one server (██████████). These scripts refer to several UNIX accounts, with passwords in clear text. Below is an example of one of these scripts:

```
@Echo Off
@Rem ST-Oraurr.CMD passwd_file passwd
@Rem 3:49 PM 11/15/94, ██████████
@Rem 10:45AM 06/23/95, IMS - Add Ideas
@Rem 7:55 AM 6/26/95, IMS - oraurr only
c:
cd c:\ftcprocs
@echo Processing/Updating ██████████
Echo *-----*
-----* >>c:\ftcprocs\graywolf.log
TM >>c:\ftcprocs\graywolf.log
DOSTM >>c:\ftcprocs\graywolf.log
Echo *-----* >>c:\ftcprocs\graywolf.log

Call UPD-Passwd graywolf ██████████
:exit
Echo *-----*
-----* >>c:\ftcprocs\graywolf.log
TM >>c:\ftcprocs\graywolf.log
DOSTM >>c:\ftcprocs\graywolf.log
Echo *-----* >>c:\ftcprocs\graywolf.log
```

Using the Unix account found above, we connected to the Unix server at ██████████. We then ran "ls -Ra" from the root directory and stored the directory listing in a file. That allowed us to analyze directories and find data files or scripts with world read rights. One location of such scripts is /app1/crons/. That directory holds scripts with oracle user name and password exposed to everyone who has access to graywolf.

We also collected a list of all user directories in a file. After we checked these accounts (about 450) with the finger utility, we found that all were valid and that most users never logged in to this server.

Browsing the various directories on this system we were able to find several configuration files for the Oracle database export utility where a SYSTEM account and password information were specified in plain-text. These files were stored in /sw/oracle/hsiang directory. An example of one such file is shown below:

```
userid=██████████g
file=/sw/oracle/██████████/G8select/G8select_exp_pipe
OWNER=(PMN, DOCSADM, FTC)
recordlength=8192
statistics=none
consistent=y
log=/sw/oracle/██████████/G8select/G8select_export.log
compress=y

pwd
/sw/oracle/██████████/G8select
```

The Oracle SYSTEM account and password, identified above gave us essentially full access to the Oracle database. Furthermore, **this level of access actually allows modifying the database operation and its content. Such systems at FTC include CIS, Oscar and Premerger.**

Note: No attempts were made to gain root access on any Solaris server (e.g., graywolf, timberwolf, wolfgang, etc.) as we understood these to be production servers. Whether secure or not, we were able to gain complete access from nonproduction equipment. Most of the local vulnerabilities that allow gaining root rights are usually based on various buffer overflow techniques. These attacks could make a server unstable or even cause it to reboot. Therefore, we limited ourselves to the safest possible ways to gain access. Such restraint is unlikely in an actual attack..

Finally, as a follow up to earlier reported vulnerabilities to management, the OIG audit team connected to the Oracle database with the SYSTEM account using sqlplus, ran the ftscanner.sql script against all Oracle schemas, and recorded information on Oracle users, groups, and their privileges. This was done as a verification test to confirm that Oracle-related vulnerabilities identified in the first testing period were corrected by the IT staff. We were able to confirm that the previously-identified vulnerabilities were corrected. (See Attachment II.)

3 Overview of Findings

Network scans were performed against the entire network. This included network devices, servers, desktop systems, storage devices, and printers. As a result of these scans, the OIG identified vulnerabilities that would enable persons with some understanding of network hardware and a direct connection to the FTC headquarters network to establish unlimited access to any system with minimal effort. Many consultants, contractors, other government employees, students and FTC staff possess both of these. Provided below are select examples of vulnerabilities enabling such access:

3.1 Windows Servers at IP Addresses [REDACTED],

These machines have an Administrator account with no password. Anyone with LAN access can connect to available shares and manipulate any files (read, write, change, delete). This vulnerability would allow a disgruntled employee to execute any program as an administrator on these machines, including hacking utilities such as sniffers, keystroke loggers, Trojans or any other executable program.

This vulnerability also allows an intruder to collect a list of potential passwords. There is a well-known bug in Windows OS, resulting from certain passwords being kept in the special memory in clear text. For example, the following fragment of memory dump collected from a host with IP address [REDACTED] shows several passwords are used by Domain Administrators to access network or/and configuration servers and services:

```
_SC_SNMPTTRAP
39 00 53 00 65 00 72 00 76 00 69 00 63 00 65 00  9.s.e.r.v.i.c.e.
31 00 39 00                                     1.9.
_SC_testdcmail POA
68 00 65 00 62 00 72 00 65 00 77 00 73 00 36 00  h.e.b.r.e.w.s.6.
3A 00 31 00 32 00                               :.1.2.
```

3.2 Cisco Switch (IP Address [REDACTED])

Some of the switches which form the backbone of the FTC Local Area Network essentially allow anyone with LAN access to execute commands via the built in WEB server. For example, entering [http://\[REDACTED\]/exec/show/config/cr](http://[REDACTED]/exec/show/config/cr) retrieves the switch's configuration file which contains the following section:

```
ip default-gateway [REDACTED]
snmp-server engineID local 00000009020000027E658AC0
snmp-server community Fireball6Pa RO
snmp-server community Fireball1%Pa RW
snmp-server community FTCPenn6Pa% RW
snmp-server community public view v1default RO
snmp-server chassis-id 0x12
snmp-server host [REDACTED] trap public
!
line con 0
transport input none
stopbits 1
line vty 0 4
password [REDACTED]
login
line vty 5 15
password [REDACTED]
login
```

One could potentially shut down an interface or modify other operational parameters on this switch. The clear-text password in the above example provides a convenient jumping-board to other network-devices on the FTC network.

All Cisco switches and routers were found to be accessed with the same password, and used the same SNMP community strings. While making it easier for administrators to manage the systems, it prevents tracing configuration changes to the person who made them and makes it much easier for an intruder to gain access (only one successful guess is required, not many). The password [REDACTED] exposed in that configuration file applies to *all* other routers and switches.

3.3 FTP server on [REDACTED]

This server allows anonymous read access to directory `/.www` essentially permitting anyone with LAN access to read, and in some directories, write to files. The significance of this is that since this system holds FTC's Intranet and Sentinel web sites, an unauthorized person can potentially modify these web-sites' contents and/or appearance. In addition, several configuration files with web administrators' usernames and encrypted passwords were readable. For example, the content of the file named `administrators.pwd` found in the directory `/.www/consumer/_vti_pvt` is displayed below:

```
# -FrontPage-
```



Running John the Ripper, a widely available Unix password cracker, revealed two of the four passwords above in a matter of seconds. Again, having these usernames and passwords would allow an attacker to change FTC intranet and Sentinel web sites at will.

4 Findings, Implications and Recommendations


Information Security has many interrelated aspects; information can be categorized in many ways. To aid the reader in understanding these findings, implications and recommendations, they have been grouped in the "Vulnerability Summary Matrix" that follows this section according to the Information Security category to which they most closely apply. Within each category, they are listed in descending order of Risk.

The "Findings" section of the matrix describes the discovered security-related item that requires attention, based on Federal regulations and industry best practices. "Implication" expands on the nature of the Finding, describing in more detail the potential threat to the security of the network, and the possible impact on operations. "Recommendation" describes proposed countermeasures.

Vulnerabilities Summary Matrix

The following matrices provide technical details on vulnerabilities found by the external penetration tests and the internal scans.

<i>Finding</i>	<i>Implication</i>	<i>Recommendation</i>
<p>1. Cisco Router/Switch at IP Address [REDACTED] has vulnerable administrative web server running.</p>	<p>An attacker can run commands with administrative (enable) privilege with no authentication. This allows an attacker to view and modify the configuration of the switch. Access to the configuration file allows the attacker to discover the access passwords and SNMP communities.</p> <p>Severity -- HIGH</p>	<p>Disable the administrative web server. Upgrade to current version of IOS, as there are other security issues with older IOS versions.</p>
<p>2. Cisco Router/Switch at IP Address [REDACTED] has vulnerable administrative web server running.</p>	<p>An attacker can run commands with administrative (enable) privilege with no authentication. This allows an attacker to view and modify the configuration of the switch. Access to the configuration file allows the attacker to discover the access</p>	<p>Disable the administrative web server. Upgrade to current version of IOS, as there are other security issues with older IOS versions.</p>

	<p>passwords and SNMP communities.</p> <p>Severity -- HIGH</p>	
<p>3. Various switches and routers have identical access password.</p>	<p>If identical passwords are used on all devices, an attacker that gains access to one device, can easily access all other devices.</p> <p>Severity -- HIGH</p>	<p>Set strong passwords on all network devices (>8 characters, uppercase, lowercase, numerals & special characters). Deploy AAA Server (tacacs, Radius, etc) or ensure that unique passwords are on each device. This is especially important with external devices, as external devices are at a greater risk of attack.</p>
<p>4. The following Windows servers have blank password Administrator account:</p> <p></p>	<p>An attacker can run commands with administrative privilege with no authentication.</p> <p>This allows an attacker to remotely or locally login to these servers. Add, copy or delete any files, change registry, add, modify and/or remove any applications.</p> <p>Severity - High</p>	<p>Set strong passwords (>8 characters, uppercase, lowercase, numerals & special characters) on all servers and workstations.</p>
<p>5. Various windows servers have Administrator password more than 100 days old. In some cases it's older than 500 days.</p>	<p>An enterprise security policy generally requires that passwords be changed every 60-90 days.</p>	<p>Passwords that are not changed periodically are more likely to be found by brute-force attacks, or abused by terminated employees. Administrative accounts are particularly attractive targets for abuse because of their unrestricted nature.</p>

	<p>Severity -- MEDIUM</p>	<p>All accounts, especially administrative accounts should be changed every 60-90 days. Any account used by a departing employee should be disabled, or have a password change before that employee's termination.</p>
<p>6. All Windows 2000 Servers allow "NULL" netbios sessions.</p>	<p>Allowing anonymous "null" sessions allows an attacker to collect extremely valuable information on the systems configuration: i.e. usernames, shares, security and auditing policies.</p> <p>Severity -- MEDIUM</p>	<p>The system security policy settings should disable null sessions. Especially on any system that is internet accessible.</p>
<p>7. FTP server on [redacted] has following directories as world-writable: /www/rftfm/NetTracker/... /pub/atr/admin/</p>	<p>An attacker can add, change and/or delete files from that directory tree</p> <p>Severity -- MEDIUM</p>	<p>Revoke world write rights for that directory tree.</p>
<p>8. FTP server on [redacted] allows anonymous access to /www directory and all subdirectories.</p>	<p>An attacker can collect valuable information on web master user names and passwords, all intranet and extranet web sites code.</p> <p>Severity - HIGH</p>	<p>Disable FTP anonymous access to /www directory tree.</p>
<p>9. The BIND server, on various Unix servers is not</p>	<p>The older versions of BIND software are vulnerable to</p>	<p>Upgrade to very latest version of BIND or disable that service if it is not used.</p>

<p>the latest version.</p>	<p>several attacks that can allow an attacker to gain root on this system. Severity - HIGH</p>	
<p>10. The IMAP server on various Unix servers seems to be vulnerable to various buffer overflow attacks.</p>	<p>An attacker can get access to a shell on this host. Severity - HIGH</p>	<p>Upgrade to the latest version of IMAP server or disable if it's not in use.</p>
<p>11. The remote Oracle tnslsnr has no password assigned on [REDACTED].</p>	<p>An attacker may use this fact to shut it down arbitrarily, thus preventing legitimate users from using it properly. Severity - MEDIUM</p>	<p>use the lsnrctl SET PASSWORD command to assign a password to, the tnslsnr.</p>
<p>12. The finger service is running on most of Unix servers.</p>	<p>The 'finger' service provides useful information to attackers, like usernames, home directories and last time login. Severity - MEDIUM</p>	<p>Disable finger service.</p>
<p>13. IIS server on hosts exhq1n2 and netbackup have support for .htr file</p>	<p>The IIS handler for .htr files has a well-known vulnerability, resolved with MS patch Q285985. An attacker can</p>	<p>Follow instructions in MS security bulletin MS00-018 to resolve this vulnerability. (http://www.microsoft.com/technet/security/bulletin/MS02-018.asp)</p>

<p>type</p>	<p>execute commands with SYSTEM privilege on a vulnerable IIS web server.</p> <p>Severity -- HIGH</p>	<p>Ensure that the system has MS patch Q285985 installed. Disable support for the .httr ISAPI filter.</p>
<p>14. IIS servers on [REDACTED] numerous vulnerabilities.</p>	<p>An attacker can execute arbitrary commands on the server with Administrator Privileges.</p> <p>Severity -- HIGH</p>	<p>Disable IIS if it is not used. Apply latest service pack and hot fixes. Uninstall sample applications for IIS.</p>
<p>15. Possible Backdoors are found on [REDACTED] /msadc/FireDaemon.exe //FireDaemon.exe /C/FireDaemon.exe /D/FireDaemon.exe</p>	<p>Backdoor is an application that allows an attacker to connect to the server without authentication.</p> <p>Severity - Unknown</p>	<p>Remove if found to be introduced backdoor.</p>
<p>16. Multiple vulnerabilities exist on [REDACTED]</p>	<p>An attacker can gain root access to the server</p> <p>Severity - HIGH</p>	<p>Apply latest Service Pack and hot fixes. Remove server from network if it is not used.</p>
<p>17. FTP server on host lcs05 allows anonymous access to documents marked "Restricted Confidential"</p>	<p>An attacker can collect confidential information.</p> <p>Severity – Unknown</p>	<p>Remove anonymous access to confidential information.</p>

<p>18. Various world readable files exist in multiple user directories on host [REDACTED] that contain Oracle username and password.</p>	<p>An attacker can collect Oracle user names and passwords and gain access to FTC highly confidential information stored in Oracle databases. Severity - HIGH</p>	<p>Change permissions for all script files with Oracle user names and password. Change passwords.</p>
<p>19. Several *.pf world readable files with clear text usernames and passwords exist in directory /sw/oracle/hsiang on host [REDACTED]</p>	<p>An attacker can collect several Oracle administrative accounts username and passwords. Severity - HIGH</p>	<p>Remove Oracle administrators account information from these files. Change permissions for files with Oracle user names and password. Change passwords.</p>
<p>20. Internet Information Server 4.0 on [REDACTED]</p>	<p>The http://[REDACTED]/iissamples/iissamples/query.asp page is the default sample search page for Index Server on IIS4. From here an attacker can perform searches for files of a certain type using "#filename=*.exe" or "#filename=*.asp". Severity - LOW</p>	<p>Ensure that Index Server has been configured not to return results for searches such as these.</p>
<p>21. Internet Information Server 4.0 on [REDACTED]</p>	<p>An attacker can launch password attacks against the local machine or proxied attacks against other machines on the</p>	<p>Remove that script if not used.</p>

	<p>network. Through http://[redacted]/isadmpwd/aexp2.htr.</p> <p>Severity - Medium</p>	
<p>22. FrontPage Server Extensions 97 package on [redacted]</p>	<p>Fpcount.exe has been found in the /_vti_bin/ directory. If, when the link above is followed, fifteen digits are displayed this version of fpcount.exe is from the FrontPage Server Extensions 97 package and it contains a buffer overrun that allows remote execution of arbitrary code.</p> <p>Severity - LOW</p>	<p>This should be deleted until a copy of the later version of FrontPage can be obtained.</p>
<p>23. Internet Information Server 5 on [redacted]</p>	<p>Newdsn.exe can be used by an attacker to create files anywhere on your disk if they have the NTFS correct file permissions to do so. Newdsn.exe can also be used to overwrite the DSNs on existing on-line databases making the information contained in the database inaccessible.</p> <p>Severity - Medium</p>	<p>This file, getdrvrs.exe, dsinform.exe and mkilog.exe should be deleted or renamed unless there is a strong reason not to do so. In that case, ensure that only Administrators may access them.</p>

<p>24. ISS servers on [redacted] have numerous vulnerabilities</p>	<p>An attacker can execute arbitrary commands on the server with Administrator Privileges.</p> <p>Severity -- HIGH</p>	<p>Disable IIS if it is not used. Apply latest service pack and hot fixes. Uninstall sample applications for IIS.</p>
<p>25. ISS server on [redacted]</p>	<p>The dll <code>_vti_bin/_vti_aut/dwssr.dll</code> seems to be present. This file is subject to a buffer overflow which allows anyone to execute arbitrary commands on the server and/or disable it</p> <p>Severity -- HIGH</p>	<p>delete <code>_vti_bin/_vti_aut/dwssr.dll</code></p>
<p>26. New Atlanta's ServletExec 4.1 is a servlet Engine for IIS server on [redacted]</p>	<p>An attacker can crash ISS by making an overly long request for a .jsp file.</p> <p>Severity -- HIGH</p>	<p>Download latest patch from ftp://ftp.newatlanta.com/public/4_1/patches/</p>
<p>27. FTP server on [redacted] has multiple vulnerabilities</p>	<p>An attacker can browse and possibly change any files on that server</p> <p>Severity -- HIGH</p>	<p>Update your FTP server to the latest version available.</p>

<p>28. ISS servers on [REDACTED] have multiple vulnerabilities</p>	<p>An attacker can execute arbitrary commands on the server with Administrator Privileges. Severity -- HIGH</p>	<p>Disable IIS if it is not used. Apply latest service pack and hot fixes. Uninstall sample applications for IIS.</p>
<p>29. server [REDACTED] has vulnerability on port 139</p>	<p>The hotfix for the 'Malformed request to index server' problem has not been applied. This vulnerability can allow an attacker to execute arbitrary code on the remote host. Severity -- Serious</p>	<p>See http://www.microsoft.com/technet/security/bulletin/ms01-025.asp</p>
<p>30. FTP server on [REDACTED] has multiple vulnerabilities</p>	<p>An attacker may use this problem to execute arbitrary commands on this host. Severity -- HIGH</p>	<p>Upgrade your ftp server software to the latest version or disable service if not needed.</p>
<p>31. Multiple vulnerabilities found on SMTP, IMAP, BIND servers running on [REDACTED]</p>	<p>An attacker may use this problem to execute arbitrary commands on this host. Severity -- HIGH</p>	<p>Upgrade your ftp server software to the latest version or disable service if not needed.</p>



OFFICE OF
INSPECTOR GENERAL

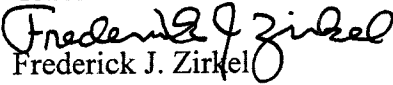
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

APPENDIX II

May 31, 2002

MEMORANDUM

TO: Stephen Warren
Chief Information Officer

FROM: 
Frederick J. Zirkel
Inspector General

SUBJECT: Oracle Database Vulnerabilities

As you know, the Government Information Security Reform Act of 2000 (Security Act) directs agency Inspectors General to perform annual independent evaluations of agency security programs and to review a subset of agency systems. While ITM participation for the second review will begin on or shortly after July 1, 2002, select OIG audit activities, including the internal scan of sensitive FTC systems, have begun.

Specifically, on May 21, 2002, the audit team performed a scan of systems housing Oracle databases. These systems were chosen by the OIG because many of the agency's most sensitive databases are Oracle based. Scan results indicate that significant vulnerabilities exist.

This initial scan focused on identifying default accounts and account-passwords (passwords) which could be exploited (primarily) by unauthorized internal users (agency employees, consultants, students and contractor staff). The review team conducted tests against three systems -- Timberwolf, Graywolf and Wolfgang, which operate the following six Oracle "instances:" CIS, PUBL, G, DW, TEST and DEVL. The OIG scan revealed that each of the six instances had a number of original password pairs still installed. As you may know, the Oracle software installs "out of the box" with over 50 default password pairs. Any disgruntled individual working at the FTC with network access and some knowledge of Oracle could not only read, but rewrite, destroy, or create new records in sensitive FTC databases, including OSCAR, HSR, and CIS. It is, therefore, critical that these default passwords, which are frequently known to installers and users of Oracle, be immediately reset once the product is installed.

The OIG met with the FTC Computer Security Officer on May 22, 2002, to present the results of our scan. Subsequent to this meeting, the OIG was informed by the Security Officer that all default passwords were removed and new, more secure passwords installed.

I will continue to keep you informed of vulnerabilities as they are discovered throughout the course of this review. We commend ITM staff for quick action taken to eliminate these vulnerabilities.

Attachment

cc: Rosemarie Straight
Don Clark
Lois Greisman
Marian Bruno