OFFICE OF INSPECTOR GENERAL
CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG Letter Report Regarding Limited Network Security Assessment Testing

OIG Report Number 02-23
April 10, 2002

GSA Contract No. GS-23F-8127H
Purchase Order No. CNSIG-02-G-0002

FOR OFFICIAL USE ONLY

This letter report contains information about Corporation computer security practices and vulnerabilities. All recipients of this report should take care to prevent the unauthorized disclosure of the report or its contents. Requests for release of this report or its contents must be referred to the Inspector General.

CORPORATION
FOR NATIONAL
SERVICE

Office of Inspector General
Corporation for National and Community Service

Audit Report 02-23

OIG Letter Report Regarding Limited Network Security Assessment Testing

Introduction

OIG engaged KPMG LLP to conduct limited follow up penetration testing on selected servers of the local area network at the Corporation's headquarters in an effort to replicate the results of testing conducted in August 2001 in connection with OIG's evaluation of the Corporation's information security practices and its compliance with the Government Information Security Reform Act (GISRA).

During the August testing, KPMG's evaluators identified some indications that malicious software, specifically Net Spy and Trojan Cow, might be present on four of the Corporation's servers. The Corporation's information technology personnel reviewed these results, concluded that they were "false-positive", and determined that no further action was necessary at that time.

In connection with the annual audit of the Corporation's Financial Statements for fiscal year 2001 and in consultation with the Corporation's staff, OIG decided to retest the affected servers in April 2002 to determine whether any indications of malicious software were still present. The evaluators concluded that neither Net Spy nor Trojan Cow software were present on the servers. KPMG and Corporation information technology personnel agreed that the August indicators were indeed "false-positive" results.

Under GISRA's requirements and implementing guidance from the Office of Management and Budget (OMB), the Corporation and OIG will conduct additional evaluations of the Corporation's information security program during the fourth quarter of fiscal year 2002.

Because this report concerns Corporation computer security practices and vulnerabilities, its distribution is limited to OIG and Corporation management and CIO personnel who have a need to know the information in order to perform their official duties. It is also available upon request to OMB and the United States Congress. Due to the security matters discussed, however, this report is exempt from release to the general public.

KPMG

2001 M Street, N.W.
Washington, DC 20036

April 10, 2002

Inspector General
Corporation for National and Community Service
Washington, DC 20525

At your request, KPMG LLP (KPMG) on April 10, 2002 performed limited penetration testing on four (4) specific servers located on the local area network at the Corporation for National and Community Service headquarters.

Background

This testing was done as a follow-up to penetration testing KPMG had previously performed in August 2001 as part of the evaluation of the Corporation's compliance with the Government Information Security Reform Act (GISRA). During the August testing the preliminary results indicated the possible presence of malicious software on four (4) of the Corporation's servers. The type of vulnerability identified by the testing could permit an unauthorized person with malicious intent to cause significant harm to the Corporation's systems. Subsequent investigation by the Corporation's information technology (IT) staff concluded that the results were a "false-positive", and that no further action was necessary. Normally, KPMG would have re-performed the testing or taken other steps to independently verify the conclusions of the Corporation's staff. However, in this case, for a variety of reasons, that could not be done at the time. Subsequently, KPMG recommended that the severity of preliminary findings was such that it would be prudent to re-test the servers in question and to verify the Corporation's conclusions.

Results in Brief

On April 10th KPMG with the assistance of the Corporation's staff, re-scanned the servers in question, and performed other procedures in an attempt to replicate the August results. During part one of the testing, KPMG did not find any signs of the malicious Net Spy Trojan software on any of the four servers. During part two of the testing, KPMG was able to replicate the symptoms that originally indicated the possibility of the malicious Trojan Cow software. However, subsequent procedures done in cooperation with the Corporation's IT staff were mutually agreed to disprove the presence of Trojan software. And, it was mutually concluded that the original indications were, in fact, a "false-positive". At that point all objectives for the testing had been met.

The Appendix to this report provides the technical details of the testing steps that were performed. Much of the relevant information about testing results is presented in the form of screen captures that were taken during the process.

We conducted our procedures in accordance auditing standards generally accepted in the United States of America and the standards applicable to performance audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

Distribution

As required by the Government Corporation Control Act, this report is intended solely for the information and use of the Corporation for National and Community Service and its Inspector General, and is not intended to be and should not be used by anyone other than these specified parties.

Felipe Alonso
Partner, KPMG LLP

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
LIMITED NETWORK SECURITY ASSESSMENT

Purpose: To describe the methodology used and test results from the limited penetration testing performed on four servers at the Corporation for National and Community Service on April 10, 2002.

Summary

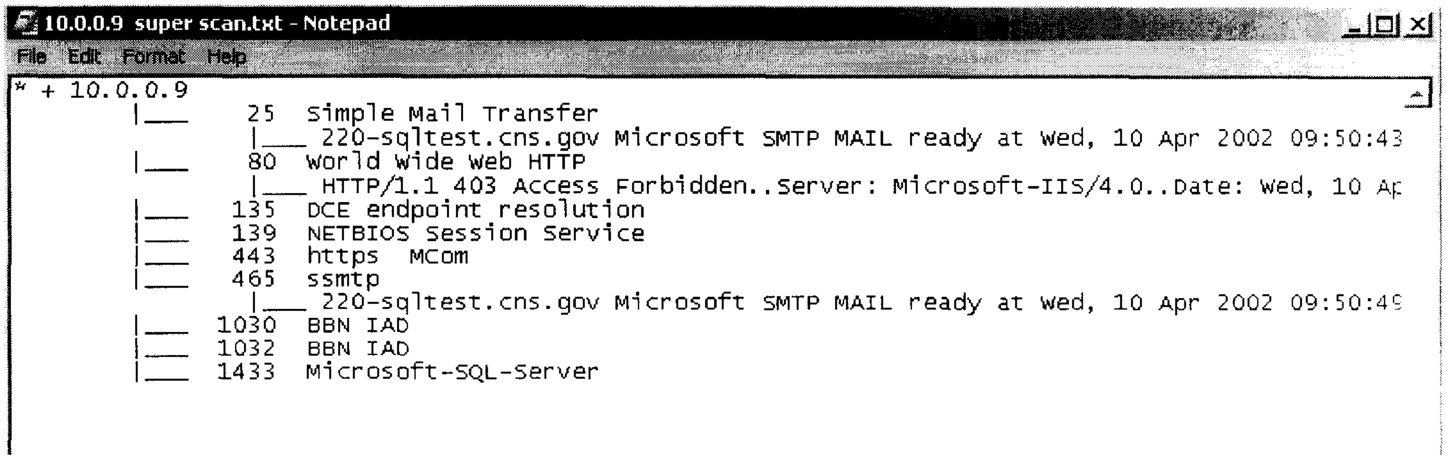
Screen-capture shots in the following sections show the step-by-step methodology KPMG used during the network security assessment. They also show the results of each test step. Because this was a "focused" assessment (a follow up examination), KPMG only scanned four servers with "Super Scan and FSCAN" scanners. KPMG was verifying whether or not Net Spy or Trojan Cow trojans were listening on ports 1033/tcp and 2001/tcp on any of following servers:

- sqltest.cns.gov
- internetmanager.cns.gov
- exchange.cns.gov
- acs.cns.gov

KPMG verified that Net Spy was not present on the four servers. More detail on this is provided in subsequent section of this appendix. KPMG did find Port 2001 was open on the ACS server. However, it was concluded that the Access Control Server that is running Cisco Secure Access Control Server software is using that port.

Test Steps:

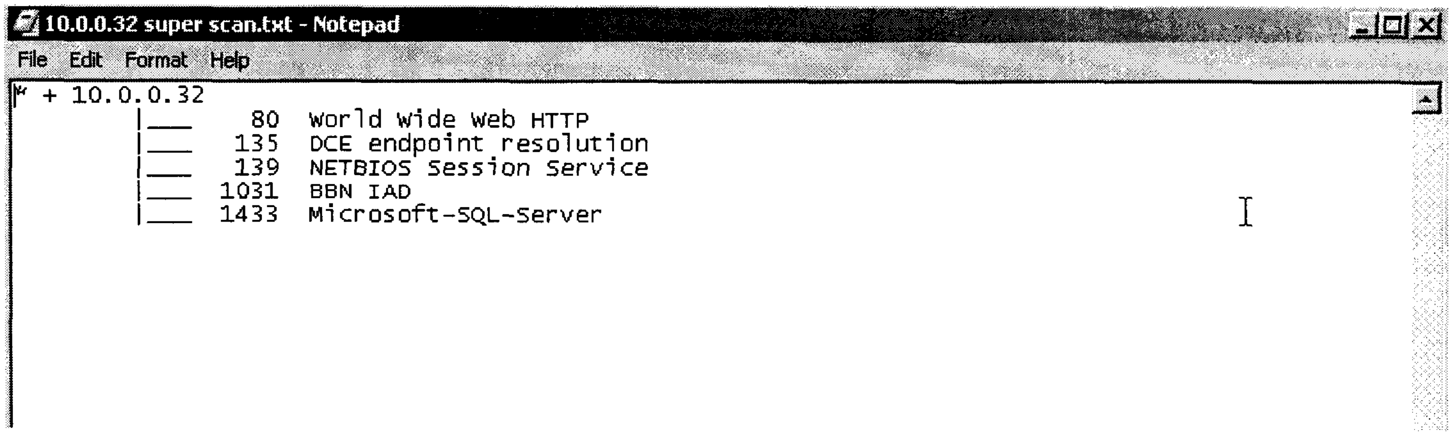
Step 1. KPMG performed a "port scan" using the SuperScan tool and found 10.0.0.9 to be running a mailserver, webserver, NETBIOS connections, SSL, and MSsql server, as shown in figure 1.
[Note: The KPMG tester's ip address was 10.0.6.13]



```
* + 10.0.0.9
        |___     25  Simple Mail Transfer
                  |___ 220-sqltest.cns.gov Microsoft SMTP MAIL ready at Wed, 10 Apr 2002 09:50:43
        |___     80  World Wide Web HTTP
                  |___ HTTP/1.1 403 Access Forbidden..Server: Microsoft-IIS/4.0..Date: Wed, 10 Ap
        |___    135  DCE endpoint resolution
        |___    139  NETBIOS Session Service
        |___    443  https  MCom
        |___    465  ssmtp
                  |___ 220-sqltest.cns.gov Microsoft SMTP MAIL ready at Wed, 10 Apr 2002 09:50:49
        |___   1030  BBN IAD
        |___   1032  BBN IAD
        |___   1433  Microsoft-SQL-Server
```

Figure 1.

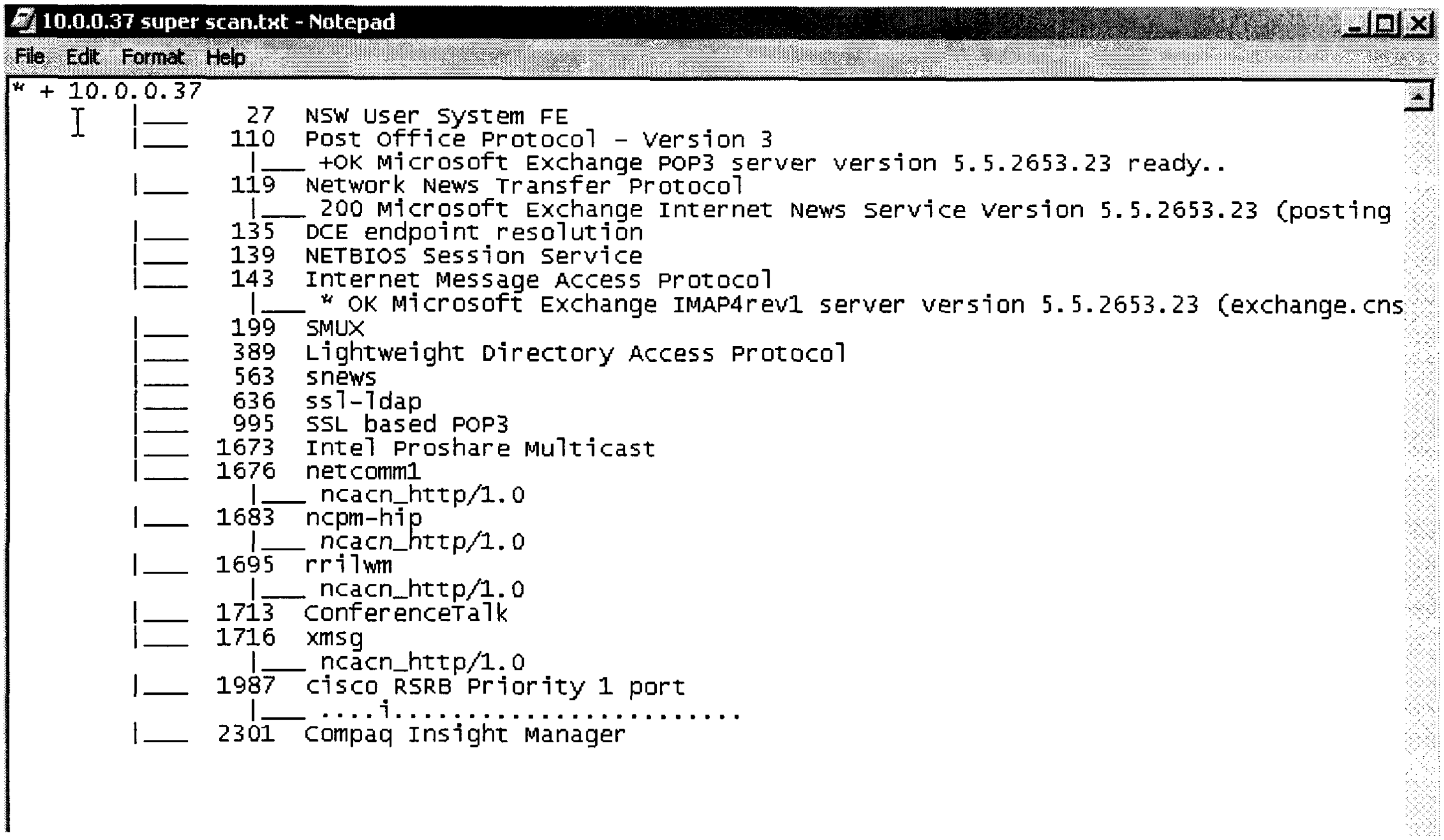
Step 2. KPMG performed a "port scan" using the SuperScan tool and found 10.0.0.32 to be running a webserver, NETBIOS connections, and a MSsql server, as shown in figure 2.



```
* + 10.0.0.32
          |___     80  World Wide Web HTTP
          |___    135  DCE endpoint resolution
          |___    139  NETBIOS Session Service
          |___   1031  BBN IAD
          |___   1433  Microsoft-SQL-Server
```

Figure 2.

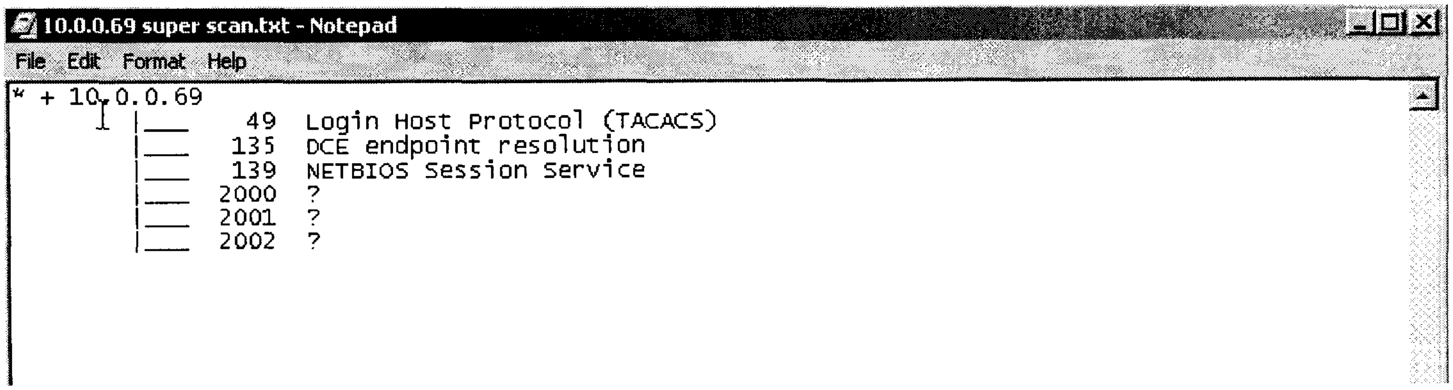
Step 3. KPMG performed a "port scan" using the SuperScan tool and found 10.0.0.37 to be using various ports, none of which contained any Trojans. All ports that are open appear to be normal or open as a result of using third-party software, as shown in figure 3.



```
* + 10.0.0.37
          |___     27  NSW User System FE
          |___    110  Post Office Protocol - Version 3
                       |___ +OK Microsoft Exchange POP3 server version 5.5.2653.23 ready..
          |___    119  Network News Transfer Protocol
                       |___ 200 Microsoft Exchange Internet News Service Version 5.5.2653.23 (posting
          |___    135  DCE endpoint resolution
          |___    139  NETBIOS Session Service
          |___    143  Internet Message Access Protocol
                       |___ * OK Microsoft Exchange IMAP4rev1 server version 5.5.2653.23 (exchange.cns
          |___    199  SMUX
          |___    389  Lightweight Directory Access Protocol
          |___    563  snews
          |___    636  ssl-ldap
          |___    995  SSL based POP3
          |___   1673  Intel Proshare Multicast
          |___   1676  netcomm1
                       |___ ncacn_http/1.0
          |___   1683  ncpm-hip
                       |___ ncacn_http/1.0
          |___   1695  rrilwm
                       |___ ncacn_http/1.0
          |___   1713  ConferenceTalk
          |___   1716  xmsg
                       |___ ncacn_http/1.0
          |___   1987  cisco RSRB Priority 1 port
                       |___ ....i........................
          |___   2301  Compaq Insight Manager
```

Figure 3.

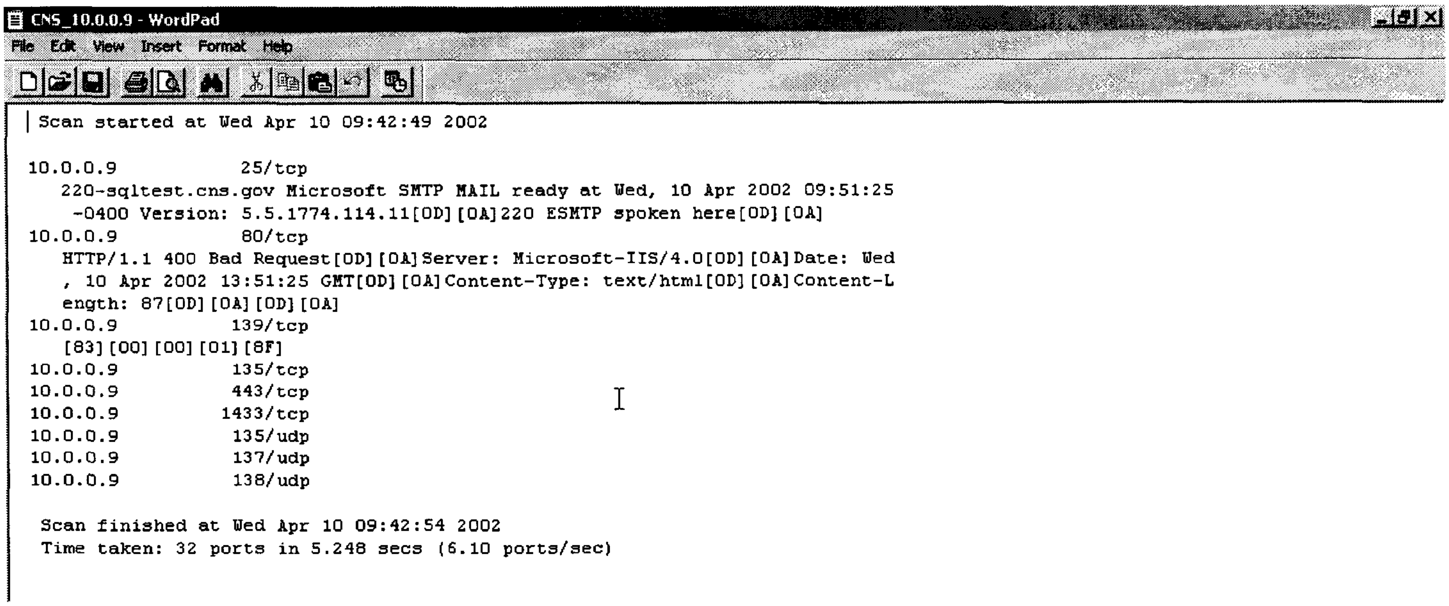
Step 4. KPMG performed a "port scan" using the SuperScan tool and found 10.0.0.69 was running Netbios connections. In addition, it appears that port 2000, 2001, and 2002 are listening, as shown in figure 4.



```
+ 10.0.0.69
      |___    49  Login Host Protocol (TACACS)
      |___   135  DCE endpoint resolution
      |___   139  NETBIOS Session Service
      |___  2000  ?
      |___  2001  ?
      |___  2002  ?
```

Figure 4.

Step 5. Because scanning tools sometimes give differing results, the above scans were repeated with a second tool. KPMG performed a "port scan" on 10.0.0.9 using the Fscan and obtained results similar to the SuperScan results, as shown in figure 5.



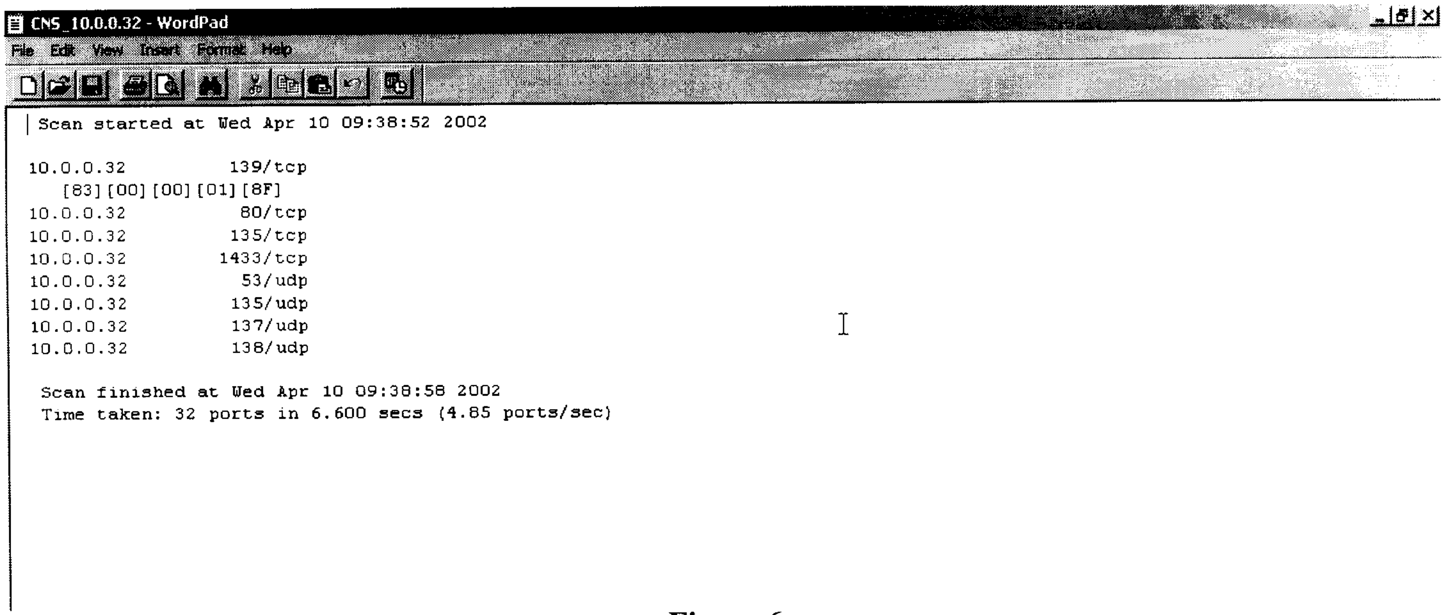
```
Scan started at Wed Apr 10 09:42:49 2002

10.0.0.9          25/tcp
   220-sqltest.cns.gov Microsoft SMTP MAIL ready at Wed, 10 Apr 2002 09:51:25
    -0400 Version: 5.5.1774.114.11[OD][OA]220 ESMTP spoken here[OD][OA]
10.0.0.9          80/tcp
   HTTP/1.1 400 Bad Request[OD][OA]Server: Microsoft-IIS/4.0[OD][OA]Date: Wed
   , 10 Apr 2002 13:51:25 GMT[OD][OA]Content-Type: text/html[OD][OA]Content-L
   ength: 87[OD][OA][OD][OA]
10.0.0.9         139/tcp
   [83][00][00][01][8F]
10.0.0.9         135/tcp
10.0.0.9         443/tcp
10.0.0.9        1433/tcp
10.0.0.9         135/udp
10.0.0.9         137/udp
10.0.0.9         138/udp

 Scan finished at Wed Apr 10 09:42:54 2002
 Time taken: 32 ports in 5.248 secs (6.10 ports/sec)
```

Figure 5.

Step 6. KPMG performed a "port scan" using the Fscan on 10.0.0.32 and obtained results similar to the SuperScan results, as shown in figure 6.



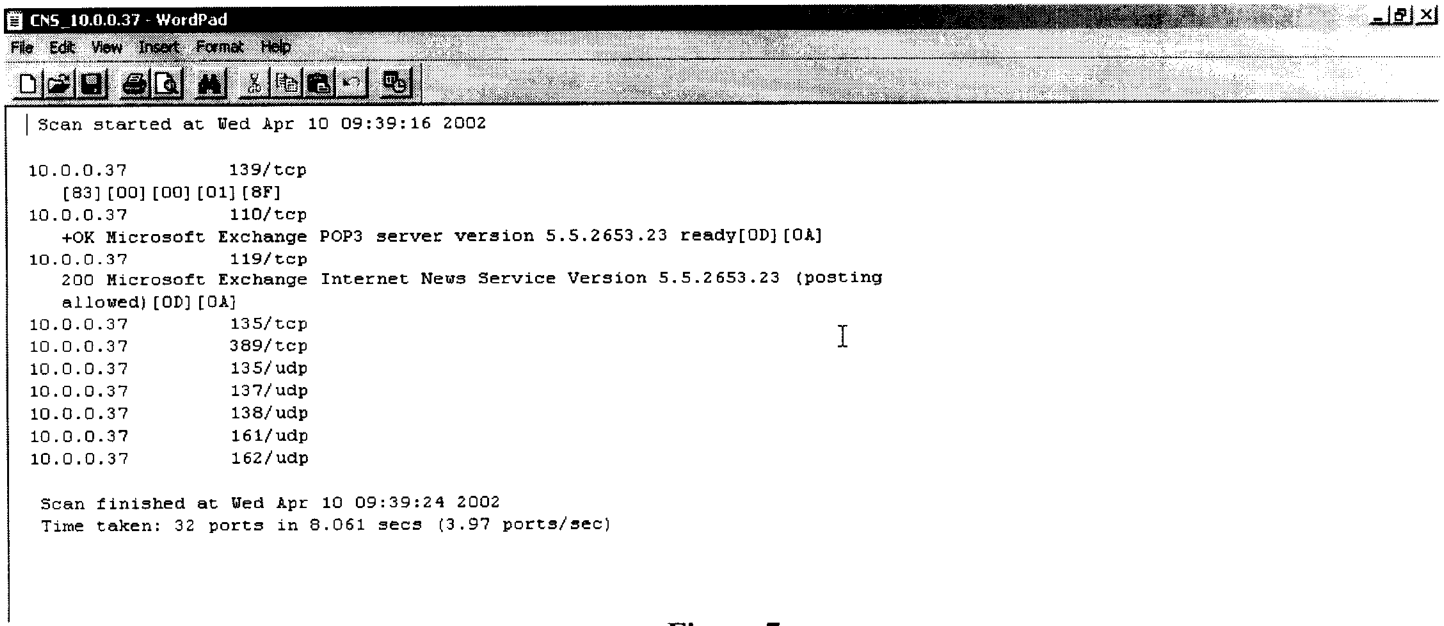
```
Scan started at Wed Apr 10 09:38:52 2002

10.0.0.32         139/tcp
   [83][00][00][01][8F]
10.0.0.32          80/tcp
10.0.0.32         135/tcp
10.0.0.32        1433/tcp
10.0.0.32          53/udp
10.0.0.32         135/udp
10.0.0.32         137/udp
10.0.0.32         138/udp

 Scan finished at Wed Apr 10 09:38:58 2002
 Time taken: 32 ports in 6.600 secs (4.85 ports/sec)
```

Figure 6.

Step 7: KPMG performed a "port scan" using the Fscan on 10.0.0.37 and obtained results similar to the SuperScan results, as shown in figure 7.



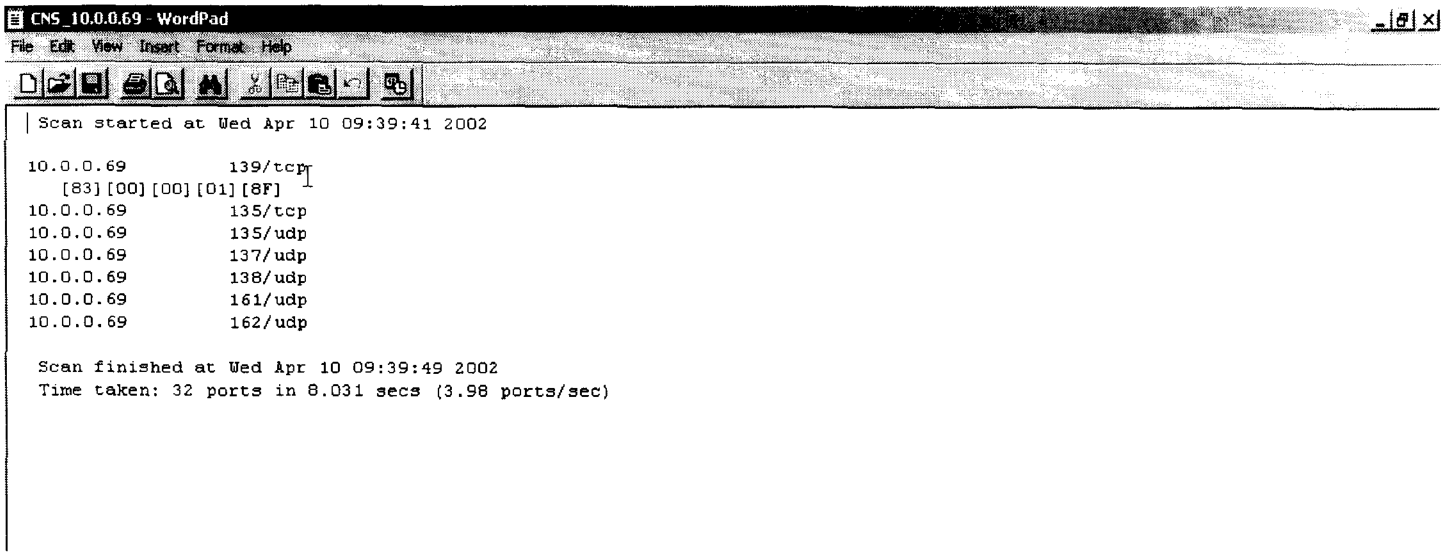
```
Scan started at Wed Apr 10 09:39:16 2002

10.0.0.37         139/tcp
   [83][00][00][01][8F]
10.0.0.37         110/tcp
   +OK Microsoft Exchange POP3 server version 5.5.2653.23 ready[0D][0A]
10.0.0.37         119/tcp
   200 Microsoft Exchange Internet News Service Version 5.5.2653.23 (posting
   allowed)[0D][0A]
10.0.0.37         135/tcp
10.0.0.37         389/tcp
10.0.0.37         135/udp
10.0.0.37         137/udp
10.0.0.37         138/udp
10.0.0.37         161/udp
10.0.0.37         162/udp

 Scan finished at Wed Apr 10 09:39:24 2002
 Time taken: 32 ports in 8.061 secs (3.97 ports/sec)
```

Figure 7.

Step 8: KPMG performed a "port scan" using the Fscan on 10.0.0.69 and obtained results similar to the SuperScan results, as shown in figure 8.



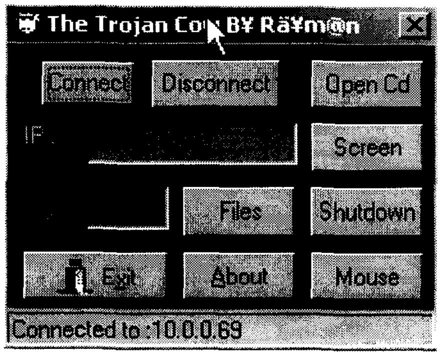
```
Scan started at Wed Apr 10 09:39:41 2002

10.0.0.69         139/tcp
   [83][00][00][01][8F]
10.0.0.69         135/tcp
10.0.0.69         135/udp
10.0.0.69         137/udp
10.0.0.69         138/udp
10.0.0.69         161/udp
10.0.0.69         162/udp

 Scan finished at Wed Apr 10 09:39:49 2002
 Time taken: 32 ports in 8.031 secs (3.98 ports/sec)
```

Figure 8.

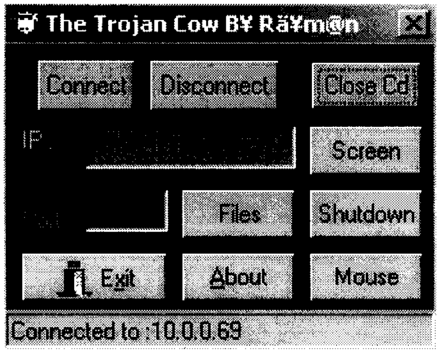
Step 9: KPMG found port 2001 open, as had been the case during the August testing. Following the testing procedure used in the prior testing, the Trojan Cow client was run, and again appeared to make a connection, as shown in figure 9.



Connected to :10.0.0.69

Figure 9.

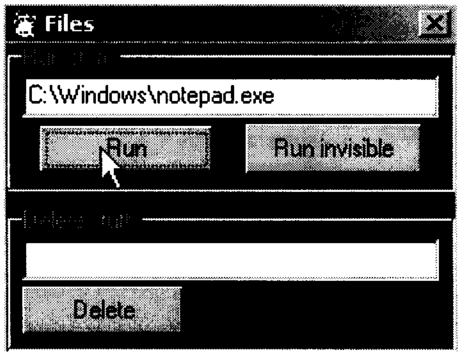
Step 10: As a method of testing whether the Trojan Cow client actually had connected to the server, an attempt was made to use two of the trojan's functions. However, KPMG was unable to open the CD tray using the Trojan Cow client, as shown in figure 10.



Connected to :10.0.0.69

Figure 10.

Step 11: And, KPMG was unable to start a process running on the server. An attempt was made to startup notepad.exe on 10.0.0.69, but was unable to do so, as shown in figure 11.



C:\Windows\notepad.exe

Figure 11.

After checking in the above manner, it was concluded that the Trojan Cow client was not really making a connection to the server, and that the indications of a connection were a "false-positive". The Corporation's IT staff provided the information that the Cisco Secure Access Control Server software was currently running on 10.0.0.69, and, the most logical conclusion was that it was the ACS software that was using port 2001.

Step 12: Subsequent to the testing done at CNCS, KPMG independently verified through vendor documentation that the ACS software does use ports 2000, 2001, and 2002 as default settings. Information regarding the Cisco Secure ACS and ports associated with the software can be found at:

http://www.cisco.com/pcgi-bin/Support/PSP/psp_view.pl?p=Software:Cisco_Secure_ACS_NT.