Security Analysis:

My_Company Internet Services Linux Server Farm

Michael James Gauthier, A+, CCDA, CCNA, MCSE+I, N+
Systems Engineer
My_Company Internet Services
November 19th, 2000

SANS Network Security Conference 2000
Monterey, CA
Securing Unix Practical Assignment
Report Introduction

Introduction

This paper is dedicated to the high-risk security issues associated with My_Company Internet Services Linux based servers. It hopes to provide a complete reference of known misconfigurations, software bugs, and physical security holes as of the time of its writing. The current practical assignment for GCUX is such an assessment of a single server, however, because the writer is responsible for the security of My_Company's servers, it was his choice to use real, mission-critical servers. Furthermore, due to the deep inter-relationship of the servers, and generally similar installations, the writer decided to evaluate all of the servers as a single autonomous body.

Background

My_Company Internet Services is an ISP serving the eastern “Some State” area from southern “Some State” to northern “Some State”. Having grown from serving a single city to serving one-third of a state, the company has scaled their servers and added servers and services on an "as needed" basis. Until recently, an outside consulting firm preformed all administrative tasks on the servers. The writer was hired approximately four months ago in an effort to reduce, and if possible, eliminate the need for outside consultants.

Currently, My_Company maintains five Linux based Internet servers. NameServer01 serves as primary DNS server, Radius server, and TFTP server. OriginalServer serves as user web and FTP server, POP3 server, secondary DNS server, commercial static web server. MailServer01 serves as SMTP server. NewWebServer serves as commercial e-commerce web server and FTP server. LogServer01 serves as central log server and administration server.

How we will proceed

This document will be broken down into three main components followed by an appendix. Each of the main discussions will center on a category of security, network based, host based, and physical security. The sections will all conclude with a plan of action including justification for the specific sequencing. The order chosen was order of importance based on My_Company's business goals and general usage of the systems. Network usage, being nearly the only usage the servers receive, will be discussed first, followed by a host-based assessment. Host usage is second, due to the fact that only paying customers have, or should have, anything other than read-only access. Physical security is last, not because it is unimportant, but because it has been the writer’s observation that few people know the physical location of the servers, especially in comparison to the number of people with network access. (i.e. the entire world)
Network Based Security

Architecture

The current network architecture is depicted in PIC1.

Currently the only non-server based firewalling being done is on Router 1 and Router 3 which are dropping the private ip address range and ip multicast. It can therefore be assumed that traffic from anywhere on the Internet can reach the servers. It should also be noted that the routers are set to drop source-routed packets. It is a requirement of the ISP to provide virtually unrestricted Internet access to customers, however unrestricted access to the servers is not in the least way a requirement. Thus, the terminal servers would need to be moved from the server segment to avoid imposing server firewalling on customer Internet connections.

Scan with nmap and nessus

The results of a full nmap scan can be found in appendix A. At first glance the results seem fairly respectable, hardly any unneeded services running. We notice TELNET running on OriginalServer and NewWebServer, which management is aware of. The DAYTIME service is available for no known reason. The use of NFS is apparent and the export list is somewhat alarming.

NameServer01 is not running any other unnecessary services. OriginalServer is running MAILSTATS on port 2525 TCP to report mail throughput. However SMTP is a false positive, it is being redirected to MailServer01. NewWebServer is running SMTP, DOMAIN, and MYSQL for no known reason. POP3
is being redirected to OriginalServer. MailServer01 is running DOMAIN; POP3 and TELNET are incorrect, the ports appear mis-configured. It is also running MAILSTATS on port 2525 TCP to report mail throughput.

Nessus found that all BIND versions were out of date and contained known security flaws, NAMED 8.1.2. The FTP servers were also found to have known security problems, PROFTPD 1.2pre10. The SSH daemon also was flagged as a serious security problem, SSHD 1.2.25. Finger.cgi was found on OriginalServer, which allows the world to do finger lookups from our server. The BIND servers allowed recursive queries with no restrictions. This allows anyone to use our DNS servers rather than just our customers. The final serious security flag was a false positive; the search.cgi script was not located on the server; the port was sent a redirect, which the scanner flagged as a return.

A UDP scan was not conducted on any hosts except LogServer01 ports 1-25000. The reason is the time sensitivity of this report. The UDP scan mentioned above took over seven hours do to an apparent configuration, limiting the ICMP error message rate. (Suggested in RFC 1812 section 4.3.2.8 and documented in the NMAP man page) As the person(s) conducting scans should be present at all times, full UDP scans are simply out of the question in this scenario.

Policy

It is currently the policy of My_Company Internet Services to allow users TELNET access to change their email account password. No users on the servers are authorized to have or use shell accounts. The purpose of the TELNET daemon is for customers to change the password for their POP3 account, thus their shell is /usr/bin/passwd. See appendix A for sample /etc/passwd file. It is also My_Company policy to allow users 4MB of web space accessible via ftp. This web space allows cgi scripts to be executed on My_Company equipment without any prior sanitizations from My_Company. The use of NFS has also been approved by My_Company to transfer mail from the mail server, MailServer01, to the POP3 server, OriginalServer. As well as to transfer radius logs from NameServer01 to LogServer01.

Recommended Plan of Action

The first recommended action is the removal of the finger.cgi. This is a quick and easy fix to a problem no one knew existed. In quick succession, the DAYTIME service should be removed from xinetd.conf. Both of these actions require negligible time to accomplish, in fact it probably took longer to write this paragraph than it will to remove these two vulnerabilities.

Next BIND, PROFTPD, and SSHD should be upgraded. This order was chosen because BIND poses the largest security threat due to the number of servers it is running on and the number of people that are aware of its existence. BIND should also be configured to allow recursive queries only from My_Company and other customer IP addresses. SSHD is considered lesser of the three because no one has a shell account and thus it receives less use and less advertisement. Finally the use of ipchains firewalling should be considered. Defense in depth
(http://www.infowar.com/iwftp/infowar/vol0302.txt heading 10³) is the best policy and every layer that a hacker needs to break down is that much more noise they will make.

Finally management should be aware of the many dangers of the use of NFS in this architecture. The decision not to implement a firewall rule set of ACL's on the Cisco router interface connected to the server farm switch should be thoroughly reconsidered, and in the writers view, reversed. Without difficulty, the terminal servers could be relocated to another segment, and ACL’s could be implemented on the Cisco router port connected to the server’s segment. Also, the purpose of the TELNET daemen should be considered as well as its use. The cost of keeping up to date on security patches for it should be weighed against the value it provides customers. Finally, the need for MYSQL, DOMAIN, and SMTP to be open on an interface other than loopback, on their respected non-commercial servers, (i.e. SMTP on servers other than the SMTP server) should be evaluated.
Host Based Security

Double Check Policies

It is currently My_Company’s policy that no user, save for corporate partners, have shell access. Thus, the host-based section of this document will focus on ensuring that this is in fact the case. We will also make certain that host based access is secured in a reasonable fashion. The majority of this section will then focus on configuration of the network services that each server offers.

We will do a quick check of passwd file, results in Appendix B, to ensure that no unauthorized user has shell access. All shell accounts check out with management, and, as a policy, shell access is restricted to SSH. We will also ensure that SSHD is restricted to authorized IP addresses, results in Appendix B, to thus limit the locations a user can gain access from. As an ISP, we can ensure that we control the majority of the address space that we allow to connect. Any that we cannot, are generally directly connected to us in the form of our partners or upstream provider. Finally, TELNETD was found running on NewWebServer with no access restrictions. This creates a large hole in the server farm’s security as a whole, due to the fact that the root password is transferred in the clear (http://www.sans.org/infosecFAQ/DSL.htm list 2 number 11) if a user su's to root.

Passwords

Currently all shell accounts are created with properly secure (http://www.ja.net/CERT/Behlers/UNIX-password-security.html section “Picking Good Passwords”) random, 8 character combinations. There is, however, no policy for changing passwords. Also, customer passwords are, as a rule, “bad” passwords, which never require changing. These situations will not change, as management has dictated them for customer ease of use and partner interaction.

Server configuration

The HTTP server, Apache, was found to be incorrectly configured on many password protected sites. The .htpasswd file was found beneath the document root (http://www.apache.org/docs/mod/mod_auth.html#authuserfile section AuthUserFile) and was named .htpasswd. Apache was also configured to relay its version information. OriginalServer was found to allow cgi exec in all home directories public_html folders, which are writable by the customers. And none of the FTP servers included an AllowFilter limiting accepted characters (http://www.proftpd.net/security.html section Securing PROFTPD) to protect against buffer-overflow attacks. Also, no quota system is in place for the home directories. Sendmail was found to respond to the HELP command, displaying its version number, even though the banner had been altered. NAMED also divulged its version number, and had no restriction on zone transfers for primary or secondary servers. NAMED also allowed recursive queries from any IP address on every
server upon which it was running. Also TFTP was running on NameServer01 with no host-based restrictions in place.

A list of SUID and SGID programs was created for each server using the find command, results in Appendix B. This list should be carefully examined and all unnecessary programs removed, or, have the SUID or SGID bit removed.

**Backups and Restoration**

Currently NewWebServer is backed up successfully and expediently on an internal tape drive every night. A full backup is performed using the dump program initiated from a cron job. MailServer01, NameServer01, OriginalServer, and LogServer01 are backed up on an internal tape drive in LogServer01. A full backup is performed nightly by a cron job that starts dump. The backup starts at five minutes past twelve and finishes at approximately three o'clock am. Unfortunately, the tape runs out of space before the full file system on each server is finished. Currently, none of the /usr partitions, MailServer01:/usr/local and /data, and LogServer01:/ and /var get backed up, and NameServer01:/var is not fully backed up. A restore procedure is in place, and was tested during the time the security audit took place, when the RADIUS user database became corrupted and a restore from backup was required. The restore was successful and completed in a timely manner; thankfully, it was contained on the part of NameServer01:/var that had been backed up.

**Logging**

A single copy of log information is kept on each server, rotated monthly and kept indefinitely. LogServer01 is the central log server for routers and terminal servers, but does not receive log information from the other servers. Currently, there is no mechanism to verify the integrity of log files, or binary and system files for that matter. Other than the backups, which go back no longer than three weeks at any one time, there is only a single copy of log information being stored.

**LSOF Results**

The results of the NMAP scan were verified, and UDP information expanded upon, by running LSOF on each server; results in Appendix B. For the most part, the NMAP results were echoed, and a snapshot view of typical server traffic was taken. One bright red flag did appear however; LogServer01 is listening for the TCP SHELL service, a. k. a. RSH. The reason this did not appear on the NMAP scan results was because XINETD implemented host based security and the machine that conducted the scan was excluded from the service. Any of the R programs are tremendously dangerous ([http://www.linuxsecurity.com/advisories/caldera_advisory-308.html](http://www.linuxsecurity.com/advisories/caldera_advisory-308.html) section 1. sub-section I8) and implements virtually no security.
**Recommended Plan of Action**

First and foremost, the TELNET daemon should be removed from NewWebServer and no user with a valid shell should be allowed to connect to OriginalServer. The SHELL service should be removed from LogServer01. A central directory should be created on the web servers where all .htpasswd files should then be kept. This directory should be owned by root and readable by world, but should not be under any HTTPD document root or symlink. The TFTPD server should have host-based security implemented, thus restricting accepted clients. An AllowFilter should then be setup on all PROFTP daemons to protect against known and unknown buffer overflow problems. A quota system should also be researched, and, if possible, implemented to protect against DoS attacks. When the BIND daemon is upgraded, it should be configured to divulge erroneous version information, and zone transfers should be restricted to the proper servers. When the Sendmail daemon is upgraded, it should be set to disallow the HELP command, and thus no longer allow its version number to be easily checked.

The sshd_config file should be examined to ensure that all AllowHosts entries are current and correct. If at all possible, a policy should be set requiring all partners to change passwords on a regular basis, along with the root password. Management is currently aware of the backup problem, and a new, larger capacity and higher transfer rate backup library is currently being purchased. In light of the fact that no firewalling is being done, the security of network backups is quite definitely in question and should be reviewed. Another case for ACL’s on the Cisco router should be made to ensure the integrity of the backups being done. Management should also evaluate the safety of allowing cgi's to be executed in user FTP home folders, but ultimately, this is a business decision. The viability of running the web server chrooted could be considered. A system such as TRIPWIRE should be evaluated to ensure the integrity of system binaries. Sending log messages to LogServer01 should be considered to ensure the integrity, and allow for the comparison of log data. And, finally, as stated above, the list of SUID and SGID files should be examined and all unnecessary executable should be removed, or have their permissions reset.
Physical Security

Data Center Access

Currently, the servers all reside in the same data center in side-by-side rail-mount cabinets. This room does not have a false ceiling, or a raised floor. All walls are cement block and run from ceiling to floor. There are two steel doors into the room, one of which does not allow outside entrance unless first opened from within. The only entrance to the room is by key card or a physical key. The physical key lock is only for emergencies that cause the key card system to fail, thus only two people pose a physical key. All in all, physical access to the room is well controlled. Unfortunately, both doors are hinged on the outside and the pins appear as though they can be easily removed. It should be noted that the room has both battery and generator backup, and that the temperature and humidity is controlled.

Server Access

Moving along to the inside of the data center, the racks the servers are stored in have neither sides and doors, nor tops and bottoms. The servers themselves have key lock front panels to hinder the removal of their covers and hard drives, however, the keys are hanging in the locks. Also, power to the machines could, accidentally, or without difficulty, be interrupted. Backup tapes are all kept on a single shelf in a cardboard box in the server room, no offsite backups are taken, nor is there any policy to do so. On a positive note, none of the servers are ever left with the console logged in, unless under the supervision of an administrator in the room.

Boot-up Security

None of the systems implement a BIOS password, nor do they have floppy boot-up disabled. The servers also allow boot-up via the CDROM drive. Worse yet, none of the servers implements a LILO prompt password, thus allowing anyone with physical access to replace init with the shell of their choice; including root privileges. ([http://www.securityportal.com/cover/coverstory20000828.html](http://www.securityportal.com/cover/coverstory20000828.html)) The systems do, surprisingly, use sulogin to require the root password for entrance into single user mode. No encryption is being used on any of the servers to store sensitive data. It should be understood that anyone who can gain physical access, and possesses minor Unix proficiencies, could easily and quickly compromise, destroy, read, or copy all information contained on the servers.

Recommendations

During the next planned reboot of the servers, a LILO prompt password should be installed. At the same time, the floppy and CDROM boot-up should be disabled, and a BIOS password installed. The root, LILO, and BIOS passwords should all
be unique. It would be within acceptable limits to write these passwords on a sheet and store that sheet in a fire safe in the data center, restricting access to the fire safe to three people at most. The keys for the servers should be removed and put in a separate fire safe, possibly with the backup tapes. The investment in full lockable server cabinets with cabinet independent battery backups should be considered, to ensure uninterrupted power flow to the servers. It would also be advisable for management to explore the cost of encrypting any data that could cause sufficient embarrassment or financial loss, if compromised. The door hinge pins should be welded in place or special secure hinges installed. In an effort to provide defense in depth, no security measure should be discounted on the bases of another security measure. All security plans and actions should be taken in an effort to sever all possible avenues of attack on multiple levels.
Bibliography

1 RFC 1812 section 4.3.2.8: Recommendation to limit the rate of ICMP error messages
2 NMAP man page section sU: States that UDP scans can be laboriously slow
3 http://www.infowar.com/iwftp/infowar/vol0302.txt heading 10: A wonderful definition of defense in depth
4 http://www.sans.org/infosecFAQ/DSL.htm list 2 number 11: Confirmstelnet transmissions are in the clear and confirms the security hazard this presents
5 http://www.ja.net/CERT/Belgers/UNIX-password-security.html section “Picking Good Passwords”: Presents a concise definition of a good Unix password
6 http://www.apache.org/docs/mod/mod_auth.html#authuserfile section AuthUserFile: Clearly documents the danger where a .htpasswd file should not be placed
7 http://www.proftpd.net/security.html section “Securing PROFTPD”: Clearly documents the advantages of using the AllowFilter directive
8 http://www.linuxsecurity.com/advisories/caldera_advisory-308.html section 1 subsection I: Documents one of the many problems with the “r” programs
9 http://www.securityportal.com/cover/coverstory20000828.html: A simply guide to gaining root with physical access
**Appendix A.**

**NMAP TCP Scan of All server IP's except LogServer01**

```
# nmap (V. 2.54BETA7) scan initiated Sun Oct 29 16:59:43 2000 as: nmap -sT -sR -o -I -v -oN /root/nmap1029.hr -oG /root/nmap1029.grep -iL /root/ipaddrlist -p 1-65535
Interesting ports on NameServer01.fdlMy_Company.com (10.0.0.11):
(The 65511 ports scanned but not shown below are in state: closed)
```

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>744/tcp</td>
<td>open</td>
<td>flexlm (mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>762/tcp</td>
<td>open</td>
<td>quotad (rstatd V1-13)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>4657/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>5808/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>14067/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>18473/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>21988/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>26477/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>29355/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32695/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>36401/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>37242/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>37818/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>42680/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>42971/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>48579/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>54844/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>64353/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=3772347 (Good luck!)

Sequence numbers: 39C72293 3959877E 3A26F986 39EEB5AF 3980F3DD 3957AB3D
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ns1.My_Company.com (192.168.0.21):
(The 65510 ports scanned but not shown below are in state: closed)

```
<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>744/tcp</td>
<td>open</td>
<td>flexlm (mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>762/tcp</td>
<td>open</td>
<td>quotad (rstatd V1-13)</td>
<td></td>
</tr>
<tr>
<td>1066/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
</tbody>
</table>
```
4238/tcp filtered unknown
6355/tcp filtered unknown
8744/tcp filtered unknown
9994/tcp filtered unknown
10062/tcp filtered unknown
22628/tcp filtered unknown
28106/tcp filtered unknown
28967/tcp filtered unknown
31559/tcp filtered unknown
35689/tcp filtered unknown
42069/tcp filtered unknown
57060/tcp filtered unknown
61551/tcp filtered unknown
63708/tcp filtered unknown
64747/tcp filtered unknown
64886/tcp filtered unknown

TCP Sequence Prediction: Class=random positive increments
Difficulty=2313548 (Good luck!)

Sequence numbers: 3C501551 3BED67F6 3B79B251 3B8EF622 3B647F34 3B9ABCFC
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on  (172.16.192.101):
(The 65511 ports scanned but not shown below are in state: closed)
<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>744/tcp</td>
<td>open</td>
<td>flexlm (mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>762/tcp</td>
<td>open</td>
<td>quotad (rstatd V1-13)</td>
<td></td>
</tr>
<tr>
<td>1320/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2844/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8045/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>11513/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>12462/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>12508/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>13039/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>29481/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>31833/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32898/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>46628/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>47137/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>52437/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>56225/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>59556/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>60112/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=4085452 (Good luck!)

Sequence numbers: 3D811FFC 3E4B0D5A 3DC2C6EF 3E305133 3DDE82B8 3DEB013D
Remote operating system guess: Linux kernel 2.2.13
Interesting ports on ns1.fdlMy_Company.com (10.0.0.21):
(The 65511 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>744/tcp</td>
<td>open</td>
<td>flexlm (mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>762/tcp</td>
<td>open</td>
<td>quotad (rstatd V1-13)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>3643/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>4848/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>5179/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>7860/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8366/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>11429/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>13319/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>20615/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>20674/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>24357/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>27189/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>27257/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>38613/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>56481/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>64637/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>65481/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=1088585 (Good luck!)

Sequence numbers: 400F583E 3FEFA0BB 400837F7 404BF7E6 40173741 3FFB4570
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on smtp.someothernet.My_Company.com (10.0.0.38):
(The 65511 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>744/tcp</td>
<td>open</td>
<td>flexlm (mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>762/tcp</td>
<td>open</td>
<td>quotad (rstatd V1-13)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>6330/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>6840/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8270/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>14912/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>17321/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>18857/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>37278/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>39644/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>40828/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>42053/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>45047/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>45179/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>45928/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>
49212/tcp filtered unknown
54529/tcp filtered unknown
60206/tcp filtered unknown
63408/tcp filtered unknown

TCP Sequence Prediction: Class=random positive increments
Difficulty=2072882 (Good luck!)

Sequence numbers: 41A074E8 41F95AD9 41D00B14 41D7824 41AD83B0
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ns1.consultant.net (192.168.0.10):
(The 65510 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>744/tcp</td>
<td>open</td>
<td>flexlm (mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>762/tcp</td>
<td>open</td>
<td>quotad (rstatd V1-13)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>5697/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>6052/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8206/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>10045/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>16644/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>30263/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>33069/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>40025/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>40667/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>46529/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>48690/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>51506/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>52662/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>53350/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>56446/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>60184/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>64822/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=3375685 (Good luck!)

Sequence numbers: 44BAB631 44A927F6 452128F2 452BA93B 456409A0 44DC6510
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ray.atw.earthreach.com (192.168.0.41):
(The 65511 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>13/tcp</td>
<td>open</td>
<td>daytime</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>744/tcp</td>
<td>open</td>
<td>flexlm (mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>762/tcp</td>
<td>open</td>
<td>quotad (rstatd V1-13)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
</tbody>
</table>


© SANS Institute 2000 - 2002
As part of GIAC practical repository.
Author retains full rights.
TCP Sequence Prediction: Class=random positive increments
Difficulty=4275223 (Good luck!)

Sequence numbers: 46CD2528 4768C311 46A2B108 46D43B0E 47117A1F 46F0B598
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on OriginalServer.fd1MyCompany.com (10.0.0.15):
(The 65506 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>672/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>5257/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>9824/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>10715/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>25334/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>26352/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>28516/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>28902/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>31309/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>35904/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>5913/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>39905/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>46266/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>57048/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>61123/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>61789/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>62886/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>
Difficulty=2631179 (Good luck!)

Sequence numbers: 49466A08 49107D7A 498D950F 498D80BB 49422964 497DE8E1
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ns2.My_Company.com (192.168.0.22):
(The 65507 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>12431/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>14380/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>15271/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>17319/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>17444/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>26898/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>28644/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>34383/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>37398/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>51276/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>52381/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>52789/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>56820/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>60985/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>63864/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>64473/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=2699440 (Good luck!)

Sequence numbers: 4B8D4FD2 4BD24885 4B53C003 4B92EB71 4B19E407 4B28CFB1
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on fdl.fdlMy_Company.com (172.7.38.130):
(The 65506 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>491/tcp</td>
<td>filtered</td>
<td>go-login</td>
<td></td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>State</td>
<td>Service (RPC)</td>
<td>Owner</td>
</tr>
<tr>
<td>--------</td>
<td>----------</td>
<td>--------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2338/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8417/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8459/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>16883/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>20690/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>21568/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>21600/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>22181/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>27178/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>33648/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>37782/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>41789/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>47775/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>55224/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>57916/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>64243/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=3048601 (Good luck!)
Sequence numbers: 4D96867F 4E39A714 4E071ADB 4DC51C77 4D60A693 4D7F27A8
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on (172.16.192.100):
(The 65506 ports scanned but not shown below are in state: closed)
<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop=3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>4418/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>14758/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>21398/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>23285/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>24126/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>26146/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>26993/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>30977/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>31880/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32916/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>43525/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>51950/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>52727/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>54566/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>58274/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>60187/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>65062/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>
TCP Sequence Prediction: Class=random positive increments
Difficulty=3392832 (Good luck!)

Sequence numbers: 504DCDFC 4FFAF71F 4FFC728E 4FD81C9B 502661CD 4F8AAP5D
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ns2.fdlMy_Company.com (10.0.0.22):
(The 65507 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>570/tcp</td>
<td>filtered</td>
<td>meter</td>
<td></td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2546/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8973/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>11717/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>19367/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>19607/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>26625/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>34968/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>35961/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>38258/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>46327/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>52130/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>52649/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>54262/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>62223/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>63625/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=972755 (Good luck!)

Sequence numbers: 5355F25F 5350CA55 532834C7 52CFF381 52EB0ED9 52F5CEB3
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on virtual.fdlMy_Company.com (10.0.0.24):
(The 65507 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>709/tcp</td>
<td>filtered</td>
<td>entrustmanager</td>
<td></td>
</tr>
</tbody>
</table>
TCP Sequence Prediction: Class=random positive increments
Difficulty=4514296 (Good luck!)

Sequence numbers: 54F5DC27 54EA7327 558C1E63 55966974 5509F80C 5515A1B7
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ftp.martin-design.net (10.0.0.32):
(The 65507 ports scanned but not shown below are in state: closed)

Port       State       Service (RPC)           Owner
21/tcp     open        ftp
22/tcp     open        ssh
23/tcp     open        telnet
25/tcp     open        smtp
53/tcp     open        domain
80/tcp     open        http
110/tcp    open        pop-3
111/tcp    open        sunrpc (rpcbind V2)
745/tcp    open        (mountd V1-2)
1265/tcp   filtered    unknown
1720/tcp   filtered    unknown
2049/tcp   open        nfs (nfs V2)
2525/tcp   open        unknown
3352/tcp   filtered    unknown
4015/tcp   filtered    unknown
40002/tcp  filtered    unknown
41485/tcp  filtered    unknown
414968/tcp filtered    unknown
20293/tcp  filtered    unknown
21242/tcp  filtered    unknown
27060/tcp  filtered    unknown
30462/tcp  filtered    unknown
39760/tcp  filtered    unknown
41037/tcp  filtered    unknown
56968/tcp  filtered    unknown
60873/tcp  filtered    unknown
63983/tcp  filtered    unknown
TCP Sequence Prediction: Class=random positive increments
Difficulty=2554166 (Good luck!)

Sequence numbers: 57BFC30F 57CBC18C 5772B8F5 577E2A19 57E904C4 57B3346A

Remote operating system guess: Linux kernel 2.2.13

Interesting ports on peter.atw.earthreach.com (192.168.0.42):
(The 65509 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>443/tcp</td>
<td>filtered</td>
<td>https</td>
<td></td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>3853/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>10779/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>16606/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>19160/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>28689/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>30052/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>42511/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>44171/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>49241/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>50361/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>51960/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>54606/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>62970/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=1355428 (Good luck!)

Sequence numbers: 59A47829 59A51EAC 59BB78CB 59A560A2 59E5C8CA 5A017E3C

Remote operating system guess: Linux kernel 2.2.13

Interesting ports on mars.someothernet.net (10.0.0.40):
(The 65506 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>754/tcp</td>
<td>filtered</td>
<td>krb_prop</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>
2049/tcp   open   nfs (nfs V2)
2525/tcp   open   unknown
2529/tcp   filtered unknown
10071/tcp  filtered unknown
20375/tcp  filtered unknown
20671/tcp  filtered unknown
22134/tcp  filtered unknown
30327/tcp  filtered unknown
30823/tcp  filtered unknown
33867/tcp  filtered unknown
34813/tcp  filtered unknown
39974/tcp  filtered unknown
40655/tcp  filtered unknown
45045/tcp  filtered unknown
55733/tcp  filtered unknown
57926/tcp  filtered unknown
61224/tcp  filtered unknown
64521/tcp  filtered unknown

TCP Sequence Prediction: Class=random positive increments
                  Difficulty=2291979 (Good luck!)

Sequence numbers: 5C0561D9 5C3B6AF9 5BF97EEA 5B7B4FB0 5B8C
                  EE50 5BCB6BD3
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ns2.consultant.net (192.168.0.9):
(The 65506 ports scanned but not shown below are in state: closed)
<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td>Owner</td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td>unknown</td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td>unknown</td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td>unknown</td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td>unknown</td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td>unknown</td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td>Owner</td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td>Owner</td>
</tr>
<tr>
<td>745/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td>Owner</td>
</tr>
<tr>
<td>1592/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td>Owner</td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>4147/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>4746/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>10497/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>10545/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>18185/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>22549/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>24134/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>27049/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>34911/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>38191/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>39296/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>48628/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>51218/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>60043/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>61914/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
<tr>
<td>63693/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td>Owner</td>
</tr>
</tbody>
</table>
TCP Sequence Prediction: Class=random positive increments
Difficulty=2429957 (Good luck!)

Sequence numbers: 5E109785 5E607A38 5E51F81D 5DEE9360 5D70D542 5DB4A80B
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on NewWebServer.My_Company.com (192.168.0.43):
(The 65509 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>143/tcp</td>
<td>filtered</td>
<td>news</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
<td></td>
</tr>
<tr>
<td>7076/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>7852/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>16336/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>23199/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>29079/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>31794/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32593/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>33914/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>42606/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>45899/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>46849/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>46924/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>57574/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>62944/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>63691/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=4610397 (Good luck!)

Sequence numbers: 5FCA9D9C 6045BE8B7 60965241 605C6DDF 6095D46B 5FA0AE95
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ftp.adci.com (192.168.0.44):
(The 65508 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2032/tcp</td>
<td>filtered</td>
<td>blackboard</td>
<td></td>
</tr>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
<td></td>
</tr>
</tbody>
</table>
3457/tcp filtered vat-control
3657/tcp filtered unknown
4819/tcp filtered unknown
10205/tcp filtered unknown
29036/tcp filtered unknown
33704/tcp filtered unknown
34971/tcp filtered unknown
42440/tcp filtered unknown
43824/tcp filtered unknown
47215/tcp filtered unknown
47941/tcp filtered unknown
54238/tcp filtered unknown
57671/tcp filtered unknown
59692/tcp filtered unknown
63190/tcp filtered unknown
64371/tcp filtered unknown

TCP Sequence Prediction: Class=random positive increments
Difficulty=2722859 (Good luck!)

Sequence numbers: 61D5686E 626B0FB2 624D7EAF 62AE64FD 6252C828 622074F8
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on ftp.somemapcom.com (192.168.0.50):
(The 65510 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
<td></td>
</tr>
<tr>
<td>3569/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8114/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8189/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8856/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>27141/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>30067/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>31354/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32016/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>40250/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>40855/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>41756/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>45338/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>50739/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>53833/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>60125/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=4625970 (Good luck!)

Sequence numbers: 64628DA3 64EBC1F9 6410650F 6472AA14 64368858 642B030E
Remote operating system guess: Linux kernel 2.2.13
Interesting ports on ftp.anothercustomer.com (192.168.0.52):
(The 65509 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>21/tcp</td>
<td>open</td>
<td>ftp</td>
<td></td>
</tr>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>40/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>domain</td>
<td></td>
</tr>
<tr>
<td>80/tcp</td>
<td>open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>443/tcp</td>
<td>open</td>
<td>https</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>3306/tcp</td>
<td>open</td>
<td>mysql</td>
<td></td>
</tr>
<tr>
<td>4193/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>4340/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>5651/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>18151/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>18360/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>31726/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32134/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32834/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>36751/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>39880/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>40480/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>46687/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>53918/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>56620/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>56969/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=1482270 (Good luck!)
Sequence numbers: 6630D3D9 6651B053 66AA3E03 66CAB184 6703EDDF 66E6D2A2
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on MailServer01.My_Company.com (192.168.0.12):
(The 65509 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>733/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2970/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>3467/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>4065/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>5804/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>6056/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>8085/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>17180/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>
TCP Sequence Prediction: Class=random positive increments
Difficulty=2229463 (Good luck!)

Sequence numbers: 69ECFAF2 697EC258 69B5B5FC 69D80D93 695CE9B3 699A27C7
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on MailServer01.fdMy_Company.com (10.0.0.12):
(The 65508 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
<tr>
<td>23/tcp</td>
<td>open</td>
<td>telnet</td>
<td></td>
</tr>
<tr>
<td>25/tcp</td>
<td>open</td>
<td>smtp</td>
<td></td>
</tr>
<tr>
<td>53/tcp</td>
<td>open</td>
<td>pop-3</td>
<td></td>
</tr>
<tr>
<td>110/tcp</td>
<td>open</td>
<td>sunrpc (rpcbind V2)</td>
<td></td>
</tr>
<tr>
<td>111/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>733/tcp</td>
<td>open</td>
<td>(mountd V1-2)</td>
<td></td>
</tr>
<tr>
<td>1621/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>1720/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>1732/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>2049/tcp</td>
<td>open</td>
<td>nfs (nfs V2)</td>
<td></td>
</tr>
<tr>
<td>2525/tcp</td>
<td>open</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>15126/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>18801/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>22893/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>31019/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>32897/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>36406/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>39558/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>39682/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>49224/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>49270/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>54428/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>55864/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>63149/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>63770/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
<tr>
<td>64832/tcp</td>
<td>filtered</td>
<td>unknown</td>
<td></td>
</tr>
</tbody>
</table>

TCP Sequence Prediction: Class=random positive increments
Difficulty=3510694 (Good luck!)

Sequence numbers: 6C1DBCAB 6C041C15 6B77D6F2 6B66238D 6BCCE475 6BC8CA33
Remote operating system guess: Linux kernel 2.2.13

Interesting ports on (192.168.0.23):
(The 65508 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>22/tcp</td>
<td>open</td>
<td>ssh</td>
<td></td>
</tr>
</tbody>
</table>
NMAP TCP Scan of LogServer01

# nmap (V. 2.54BETA7) scan initiated Tue Oct 31 08:03:48 2000 as: nmap
#  -sT -0 -sR -v -oN /root/nmap.1030.hr -oG nmap1030.grep -p 1-65535
10.0.0.14
Interesting ports on LogServer01.fdlMy_Company.com (10.0.0.14):
(The 65532 ports scanned but not shown below are in state: filtered)
Port       State       Service (RPC)
80/tcp     open        http
123/tcp    closed      ntp
443/tcp    open        https

TCP Sequence Prediction: Class=random positive increments
Difficulty=1697333 (Good luck!)

Sequence numbers: 41102D99 410CE2DC9 4108F170 4125CB1D 411FE30E 40D3F73B
Remote OS guesses: Linux 2.1.122 - 2.2.16, Linux kernel 2.2.13, Linux 2.2.14

# Nmap run completed at Tue Oct 31 09:42:28 2000 -- 1 IP address (1
host up) scanned in 5920 seconds
**NMAP UDP Scan of LogServer01**

# nmap (V. 2.54BETA7) scan initiated Tue Oct 31 09:47:26 2000 as: nmap
-sU -O -sR -v -oN /root/nmapU1030.hr -oG nmapU1030.grep -p 1-25000
10.0.0.14
Warning: OS detection will be MUCH less reliable because we did not
find at least 1 open and 1 closed TCP port
Interesting ports on LogServer01.fdlMy_Company.com (10.0.0.14):
(The 24994 ports scanned but not shown below are in state: closed)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Service (RPC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>111/udp</td>
<td>open</td>
<td>sunrpc</td>
</tr>
<tr>
<td>123/udp</td>
<td>open</td>
<td>ntp</td>
</tr>
<tr>
<td>138/udp</td>
<td>open</td>
<td>netbios-dgm</td>
</tr>
<tr>
<td>514/udp</td>
<td>open</td>
<td>syslog</td>
</tr>
<tr>
<td>748/udp</td>
<td>open</td>
<td>ris-cm</td>
</tr>
<tr>
<td>800/udp</td>
<td>open</td>
<td>mdbs_daemon</td>
</tr>
</tbody>
</table>

Remote OS guesses: 3com Office Connect Router 810, Cobalt Linux 4.0
(Fargo) Kernel 2.0.34C52_SK on MIPS or TEAMInternet Series 100
WebSense, Linux 2.2.5 - 2.2.13 SMP, Linux kernel 2.2.13

# Nmap run completed at Tue Oct 31 16:53:31 2000 -- 1 IP address (1
host up) scanned in 25565 seconds

**NESSUS Scan of All Servers except LogServer01**

Nessus Scan Report
------------------

**SUMMARY**

- Number of hosts which were alive during the test : 4
- Number of security holes found : 6
- Number of security warnings found : 30
- Number of security notes found : 28

**TESTED HOSTS**

10.0.0.15 (Security holes found)
192.168.0.43 (Security holes found)
10.0.0.11 (Security holes found)
10.0.0.12 (Security holes found)

**DETAILS**

+ 10.0.0.15 :
  . List of open ports :
    o ftp (21/tcp) (Security hole found)
    o ssh (22/tcp) (Security warnings found)
    o telnet (23/tcp) (Security warnings found)
Vulnerability found on port ftp (21/tcp):

The remote ProFTPD server is running a 1.2.0preN version.

All the 1.2.0preN versions contain several security flaws that allow an attacker to execute arbitrary code on this host.

Solution: upgrade to the 1.2.0rcN series (http://www.proftpd.net)
Risk factor: High
CVE: CVE-2000-0574

Information found on port ftp (21/tcp)

Remote FTP server banner:
proftpd 1.2.0pre3 server ready.

Warning found on port ssh (22/tcp)

You are running a version of SSH which is older than (or as old as) version 1.2.27. If this version was compiled against the RSAREF library, then it is very likely to be vulnerable to a buffer overflow which may be exploited by a cracker to gain root on your system.

To determine if you compiled ssh against the RSAREF library, type 'ssh -V' on the remote host.

Risk factor: High
Solution: Use ssh 2.x, or do not compile ssh against the RSAREF library
CVE: CVE-1999-0834

Warning found on port ssh (22/tcp)
You are running a version of SSH which is older than (or as old as) version 1.2.27.

If you compiled ssh with kerberos support, then an attacker may eavesdrop your users kerberos tickets, as sshd will set the environment variable KRB5CCNAME to 'none', so kerberos tickets will be stored in the current working directory of the user, as 'none'.

If you have nfs/smb shared disks, then an attacker may eavesdrop the kerberos tickets of your users using this flaw.

** If you are not using kerberos, then ignore this warning.

Risk factor : Serious
Solution : use ssh 1.2.28 or newer
CVE : CAN-2000-0575

. Information found on port ssh (22/tcp)

Remote SSH version :
ssh-1.5-1.2.25

. Warning found on port telnet (23/tcp)

The Telnet service is running.
This service is dangerous in the sense that it is not ciphered - that is, everyone can sniff the data that passes between the telnet client and the telnet server. This includes logins and passwords.

You should disable this service and use OpenSSH instead. (www.openssh.com)

Solution : Comment out the 'telnet' line in /etc/inetd.conf.

Risk factor : Low
CVE : CAN-1999-0619

. Information found on port telnet (23/tcp)

Remote telnet banner :
Welcome to:

. Warning found on port smtp (25/tcp)
The remote SMTP server allows the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.

Risk factor : Low/Medium

Solution : configure your SMTP server so that it can't be used as a relay any more.
CVE : CAN-1999-0512

. Information found on port smtp (25/tcp)

Remote SMTP server banner :
MailServer01.My_Company.com ESMTP Eunice Internet Mail 1.01: Mon, 30 Oct 2000 18:50:02 -0600
214-This is Sendmail version 8.9.3214-Topics:
214- HELO EHLO MAIL RCPT DATA
214- RSET NOOP QUIT HELP VRFY
214- EXPN VERB ETRN DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation send email to
214- sendmail-bugs@sendmail.org.
214-For local information send email to Postmaster at your site.
214 End of HELP info

. Vulnerability found on port domain (53/tcp) :

The remote BIND server, according to its version number, is vulnerable to several attacks that can allow an attacker to gain root on this system.

Solution : upgrade to bind 8.2.2-P3
Risk factor : High
CVE : CVE-1999-0833

. Warning found on port domain (53/tcp)

The remote name server allows recursive queries to be performed
by the host running nessusd.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

Solution: Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursive' in the 'options' section of your named.conf

If you are using another name server, consult its documentation.

Risk factor:
Serious

- Information found on port domain (53/tcp)

  The remote bind version is:
  8.1.2

- Warning found on port www (80/tcp)

  The 'finger' cgi is installed. It is usually not a good idea to have such a service installed, since it usually gives more troubles than anything else.

  Double check that you really want to have this service installed.

  Solution: remove it from /cgi-bin.

  Risk factor: Serious
  CVE: CAN-1999-0197

- Information found on port www (80/tcp)

  The remote web server type is:
  Apache/1.3.11 (Unix)

  We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult

- Information found on port pop3 (110/tcp)

  The remote POP server banner is:
+OK POP3 Goes the Weasel 2.0b4 at OriginalServer.My_Company.com starting.

. Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution: Contact your vendor for a patch
Risk factor: Low

. Information found on port general/tcp

Nmap found that this host is running Linux kernel 2.2.13

. Information found on port general/udp

For your information, here is the traceroute to 10.0.0.15:
192.168.0.1
10.0.0.15

. Warning found on port unknown (2049/tcp)

Here is the export list of 10.0.0.15:
/home MailServer01.fdlMy_Company.com,
CVE: CVE-1999-0554

. Warning found on port unknown (2049/udp)

The nfsd RPC service is running. There is a bug in older versions of this service that allow an intruder to execute arbitrary commands on your system.

Make sure that you have the latest version of nfsd

Risk factor: High
CVE: CAN-1999-0832

. Warning found on port general/icmp
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentications protocols.

Solution: filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

Risk factor: Low
CVE: CAN-1999-0524

+ 192.168.0.43:
. List of open ports:
  o ftp (21/tcp) (Security hole found)
  o ssh (22/tcp) (Security warnings found)
  o telnet (23/tcp) (Security notes found)
  o smtp (25/tcp) (Security notes found)
  o domain (53/tcp) (Security hole found)
  o www (80/tcp) (Security notes found)
  o pop3 (110/tcp) (Security notes found)
  o unknown (443/tcp)
  o general/tcp (Security notes found)
  o general/udp (Security notes found)
  o general/icmp (Security warnings found)
  o daytime (13/udp) (Security warnings found)

. Vulnerability found on port ftp (21/tcp):

The remote ProFTPD server is running a 1.2.0preN version.

All the 1.2.0preN versions contain several security flaws that allow an attacker to execute arbitrary code on this host.

Solution: upgrade to the 1.2.0rcN series (http://www.proftpd.net)
Risk factor: High
CVE: CVE-2000-0574

. Information found on port ftp (21/tcp)

Remote FTP server banner:
  proftpd 1.2.0pre10 server ready.

. Warning found on port ssh (22/tcp)

You are running a version of SSH which is
older than (or as old as) version 1.2.27. If this version was compiled against the RSAREF library, then it is very likely to be vulnerable to a buffer overflow which may be exploited by a cracker to gain root on your system.

To determine if you compiled ssh against the RSAREF library, type 'ssh -V' on the remote host.

Risk factor : High
Solution : Use ssh 2.x, or do not compile ssh against the RSAREF library
CVE : CVE-1999-0834

Warning found on port ssh (22/tcp)

You are running a version of SSH which is older than (or as old as) version 1.2.27.

If you compiled ssh with kerberos support, then an attacker may eavesdrop your users kerberos tickets, as sshd will set the environment variable KRB5CCNAME to 'none', so kerberos tickets will be stored in the current working directory of the user, as 'none'.

If you have nfs/smb shared disks, then an attacker may eavesdrop the kerberos tickets of your users using this flaw.

** If you are not using kerberos, then ignore this warning.

Risk factor : Serious
Solution : use ssh 1.2.28 or newer
CVE : CAN-2000-0575

Information found on port ssh (22/tcp)

Remote SSH version:
ssh-1.5-1.2.27

Information found on port telnet (23/tcp)

Remote telnet banner:
yü'

Information found on port smtp (25/tcp)
Remote SMTP server banner:
214-This is Sendmail version 8.9.3214-Topics:
214-HELO EHLO MAIL RCPT DATA
214-RSET NOOP QUIT HELP VRFY
214-EXPN VERB ETRN DSN
214-For more info use "HELP <topic>".
214-To report bugs in the implementation send email to
214- sendmail-bugs@sendmail.org.
214-For local information send email to Postmaster at your site.
214 End of HELP info

. Vulnerability found on port domain (53/tcp) :

The remote BIND server, according to its version number, is vulnerable to several attacks that can allow an attacker to gain root on this system.

Solution : upgrade to bind 8.2.2-P3
Risk factor : High
CVE : CVE-1999-0833

. Warning found on port domain (53/tcp)

The remote name server allows recursive queries to be performed by the host running nessusd.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

Solution : Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it).
If you are using bind 8, you can do this by using the instruction 'allow-recursive' in the 'options' section of your named.conf.

If you are using another name server, consult its documentation.

Risk factor:
Serious

Information found on port domain (53/tcp)

The remote bind version is:
8.2.1

Information found on port www (80/tcp)

The remote web server type is:
Apache/1.3.11 (Unix) mod_perl/1.21

We recommend that you configure your web server to return bogus versions, so that it makes the cracker job more difficult.

Information found on port pop3 (110/tcp)

The remote POP server banner is:
+OK POP3 Goes the Weasel 2.0b4 at OriginalServer.My_Company.com starting.

Information found on port general/tcp

Nmap found that this host is running Linux kernel 2.2.13

Information found on port general/udp

For your information, here is the traceroute to 192.168.0.43:
192.168.0.1
192.168.0.43

Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentications protocols.

Solution: filter out the icmp timestamp
requests (13), and the outgoing icmp timestamp replies (14).

Risk factor: Low
CVE: CAN-1999-0524

. Warning found on port daytime (13/udp)

The daytime service is running. The date format issued by this service may sometimes help an attacker to guess the operating system type.

In addition to that, when the UDP version of daytime is running, an attacker may link it to the echo port using spoofing, thus creating a possible denial of service.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

+ 10.0.0.11 :

. List of open ports:
  o daytime (13/tcp) (Security warnings found)
  o ssh (22/tcp) (Security warnings found)
  o domain (53/tcp) (Security hole found)
  o sunrpc (111/tcp)
  o general/tcp (Security notes found)
  o general/udp (Security notes found)
  o unknown (2049/tcp) (Security warnings found)
  o unknown (757/udp) (Security warnings found)
  o unknown (2049/udp) (Security warnings found)
  o general/icmp (Security warnings found)
  o daytime (13/udp) (Security warnings found)

. Warning found on port daytime (13/tcp)

The daytime service is running. The date format issued by this service may sometimes help an attacker to guess the operating system type.

In addition to that, when the UDP version of daytime is running, an attacker may link it to the echo port using spoofing, thus creating a possible denial of service.

Solution: disable this service in /etc/inetd.conf.

Risk factor: Low
CVE: CVE-1999-0103

. Warning found on port ssh (22/tcp)
You are running a version of SSH which is older than (or as old as) version 1.2.27. If this version was compiled against the RSAREF library, then it is very likely to be vulnerable to a buffer overflow which may be exploited by a cracker to gain root on your system.

To determine if you compiled ssh against the RSAREF library, type 'ssh -V' on the remote host.

Risk factor : High
Solution : Use ssh 2.x, or do not compile ssh against the RSAREF library
CVE : CVE-1999-0834

. Warning found on port ssh (22/tcp)

You are running a version of SSH which is older than (or as old as) version 1.2.27.

If you compiled ssh with kerberos support, then an attacker may eavesdrop your users kerberos tickets, as sshd will set the environment variable KRB5CCNAME to 'none', so kerberos tickets will be stored in the current working directory of the user, as 'none'.

If you have nfs/smb shared disks, then an attacker may eavesdrop the kerberos tickets of your users using this flaw.

** If you are not using kerberos, then ignore this warning.

Risk factor : Serious
Solution : use ssh 1.2.28 or newer
CVE : CAN-2000-0575

. Information found on port ssh (22/tcp)

Remote SSH version :
ssh-1.5-1.2.25

. Vulnerability found on port domain (53/tcp) :
The remote BIND server, according to its version number, is vulnerable to several attacks that can allow an attacker to gain root on this system.

Solution: upgrade to bind 8.2.2-P3
Risk factor: High
CVE: CVE-1999-0833

Warning found on port domain (53/tcp)

The remote name server allows recursive queries to be performed by the host running nessusd.

If this is your internal nameserver, then forget this warning.

If you are probing a remote nameserver, then it allows anyone to use it to resolve third parties names (such as www.nessus.org). This allows hackers to do cache poisoning attacks against this nameserver.

Solution: Restrict recursive queries to the hosts that should use this nameserver (such as those of the LAN connected to it). If you are using bind 8, you can do this by using the instruction 'allow-recursive' in the 'options' section of your named.conf

If you are using another name server, consult its documentation.

Risk factor: Serious

Information found on port domain (53/tcp)

The remote bind version is:
8.1.2

Information found on port general/tcp

Nmap found that this host is running Linux kernel 2.2.13

Information found on port general/udp

For your information, here is the traceroute to 10.0.0.11:
192.168.0.1
10.0.0.11

Warning found on port unknown (2049/tcp)
Here is the export list of 10.0.0.11:
/var/log/radacct LogServer01.fd1My_Company.com,

CVE : CVE-1999-0554

. Warning found on port unknown (757/udp)

The rstatd RPC service is running.
It provides an attacker interesting informations such as :
- the CPU usage
- the system uptime
- its network usage
- and more

It usually not a good idea to let this service open

Risk factor : Low
CVE : CAN-1999-0624

. Warning found on port unknown (2049/udp)

The nfsd RPC service is running.
There is a bug in older versions of this service that allow an intruder to execute arbitrary commands on your system.

Make sure that you have the latest version of nfsd

Risk factor : High
CVE : CAN-1999-0832

. Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentications protocols.

Solution : filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524
. Warning found on port daytime (13/udp)

The daytime service is running.
The date format issued by this service
may sometimes help an attacker to guess
the operating system type.

In addition to that, when the UDP version of
daytime is running, an attacker may link it
to the echo port using spoofing, thus creating
a possible denial of service.

Solution : disable this service in /etc/inetd.conf.

Risk factor : Low
CVE : CVE-1999-0103

+ 10.0.0.12 :
. List of open ports :
 o ssh (22/tcp) (Security warnings found)
 o telnet (23/tcp) (Security notes found)
 o smtp (25/tcp) (Security warnings found)
 o domain (53/tcp) (Security hole found)
 o pop3 (110/tcp)
 o sunrpc (111/tcp)
 o general/tcp (Security notes found)
 o general/udp (Security notes found)
 o unknown (2049/tcp) (Security warnings found)
 o unknown (2049/udp) (Security warnings found)
 o general/icmp (Security warnings found)

. Warning found on port ssh (22/tcp)

You are running a version of SSH which is
older than (or as old as) version 1.2.27.
If this version was compiled against the
RSAREF library, then it is very likely to
be vulnerable to a buffer overflow which
may be exploited by a cracker to gain
root on your system.

To determine if you compiled ssh against
the RSAREF library, type 'ssh -V' on the
remote host.

Risk factor : High
Solution : Use ssh 2.x, or do not compile ssh
against the RSAREF library
CVE : CVE-1999-0834

. Warning found on port ssh (22/tcp)
You are running a version of SSH which is older than (or as old as) version 1.2.27.

If you compiled ssh with kerberos support, then an attacker may eavesdrop your users kerberos tickets, as sshd will set the environment variable KRB5CCNAME to 'none', so kerberos tickets will be stored in the current working directory of the user, as 'none'.

If you have nfs/smb shared disks, then an attacker may eavesdrop the kerberos tickets of your users using this flaw.

** If you are not using kerberos, then ignore this warning.

Risk factor: Serious
Solution: use ssh 1.2.28 or newer
CVE: CAN-2000-0575

. Information found on port ssh (22/tcp)

Remote SSH version:
ssh-1.5-1.2.27

. Information found on port telnet (23/tcp)

Remote telnet banner:
y)

. Warning found on port smtp (25/tcp)

The remote SMTP server allows the relaying. This means that it allows spammers to use your mail server to send their mails to the world, thus wasting your network bandwidth.

Risk factor: Low/Medium
Solution: configure your SMTP server so that it can't be used as a relay

   any more.
CVE: CAN-1999-0512

. Information found on port smtp (25/tcp)

Remote SMTP server banner:
MailServer01.My_Company.com ESMTP Eunice Internet Mail 1.01: Mon, 30 Oct 2000
18:48:14 -0600
214-This is Sendmail version 8.9.3214-TOPICS:
214- HELO EHLO MAIL RCPT DATA
214- RSET NOOP QUIT HELP VRFY
214- EXPN VERB ETRN DSN
214- For more info use "HELP <topic>".
214- To report bugs in the implementation send email to
214- sendmail-bugs@sendmail.org.
214- For local information send email to Postmaster at your site.
214 End of HELP info

. Vulnerability found on port domain (53/tcp) :

    The remote BIND server, according to its
    version number, is vulnerable to several
    attacks that can allow an attacker to gain
    root on this system.

    Solution: upgrade to bind 8.2.2-P3
    Risk factor: High
    CVE: CVE-1999-0833

. Information found on port domain (53/tcp)

    The remote bind version is:
    8.2.1

. Information found on port general/tcp

    Nmap found that this host is running Linux kernel 2.2.13

. Information found on port general/udp

    For your information, here is the traceroute to 10.0.0.12:
    192.168.0.1
    10.0.0.12

. Warning found on port unknown (2049/tcp)
Here is the export list of 10.0.0.12:
/var/spool/mail ns2.My_Company.com,
/var/spool/mail OriginalServer.fdMy_Company.com,

CVE : CVE-1999-0554

. Warning found on port unknown (2049/udp)

The nfsd RPC service is running.
There is a bug in older versions of this service that allow an intruder to execute arbitrary commands on your system.

Make sure that you have the latest version of nfsd

Risk factor : High
CVE : CAN-1999-0832

. Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentications protocols.

Solution : filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

Risk factor : Low
CVE : CAN-1999-0524

NESSUS Scan of LogServer01
-----------------------------------------
This file was generated by the Nessus Security Scanner

Nessus Scan Report
------------------

SUMMARY
- Number of hosts which were alive during the test : 1
- Number of security holes found : 1
Number of security warnings found : 3
Number of security notes found : 2

TESTED HOSTS

10.0.0.14 (Security holes found)

DETAILS

+ 10.0.0.14 :
  . List of open ports :
    o general/udp (Security notes found)
    o unknown (748/udp) (Security warnings found)
    o www (80/tcp) (Security hole found)
    o general/tcp (Security warnings found)
    o general/icmp (Security warnings found)
  . Information found on port general/udp

    For your information, here is the traceroute to 10.0.0.14 :
    192.168.0.1
    10.0.0.14
  . Warning found on port unknown (748/udp)

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

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

    It usually not a good idea to let this service open

    Risk factor : Low
    CVE : CAN-1999-0624

  . Vulnerability found on port www (80/tcp) :

    It is possible to read arbitrary files on the remote server by requesting :

    GET /cgi-bin/search.cgi?letter=\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..\..<\n\n© SANS Institute 2000 - 2002
As part of GIAC practical repository.
Author retains full rights.
An attacker may use this flaw to read arbitrary files on this server.

Solution: remove this CGI from /cgi-bin
Bugtraq ID: 921
Risk factor: High
CVE: CAN-2000-0054

. Information found on port www (80/tcp)

The remote web server type is:
Stronghold/2.4 Apache/1.3.0 C2NetEU/2407 (Unix)

We recommend that you configure your web server to return
bogus versions, so that it makes the cracker job more difficult.

. Warning found on port general/tcp

The remote host uses non-random IP IDs, that is, it is possible to predict the next value of the ip_id field of the ip packets sent by this host.

An attacker may use this feature to determine if the remote host sent a packet in reply to another request. This may be used for portscanning and other things.

Solution: Contact your vendor for a patch
Risk factor: Low

. Warning found on port general/icmp

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.

This may help him to defeat all your time based authentications protocols.

Solution: filter out the icmp timestamp requests (13), and the outgoing icmp timestamp replies (14).

Risk factor: Low
CVE: CAN-1999-0524
This file was generated by the Nessus Security Scanner

Sample passwd for User Telnet Access
User:x:101:100:User Name:/home/A/user:/usr/bin/passwd
Appendix B.

**PASSWD Shell Accounts**

```
#!/bin/bash
#script to get valid shells in passwd, MJG 10/30/2000
SERVERLIST=$(cat /root/serverlist)
For SERVER in $SERVERLIST; do
    /usr/local/bin/ssh -n -o 'BatchMode Yes' $SERVER \
        /bin/cat /etc/passwd \
        | /usr/bin/grep -v \
        /bin/false \
        | /dev/null \
        | /etc/ftponly \
        | elm -s "Passwd shells for $SERVER" sysadmin
done

LogServer01
root:x:0:0:root:/root:/bin/bash
anotherroot:x:0:0:Anotherroot:/anotherroot:/bin/zsh
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
gbl:x:100:100:Gordon B Lastname:/home/gbl:/bin/zsh
admin01:x:1823:100:Keith:/home/admin01:/bin/sh

NewWebServer
root:x:0:0:root:/root:/bin/bash
anotherroot:x:0:0:Anotherroot:/anotherroot:/bin/zsh
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
webadmin01:x:527:100:Webadmin01:/home/webadmin01:/usr/local/bin/bash
webadmin012:x:525:100:Webadmin01 as Julie:/home/webadmin01:/usr/local/bin/bash
admin01:x:530:100:System Mailer:/home/admin01:/bin/bash
admin012:x:525:100:North Pole? Sugar Pole!/home/admin01:/bin/zsh
klapp:x:551:100:Alan Klapp:/home/klapp:/bin/zsh
mgauth:x:566:100:Mikel:/home/mgauth:/bin/zsh
route43:x:579:501:Caldera OpenLinux User:/home/route43:/bin/bash
dougs:x:585:502:Caldera OpenLinux User:/home/dougs:/bin/bash

OriginalServer
root:x:0:0:root:/root:/bin/bash
anotherroot:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
gbl:x:100:100:Gordon B Lastname:/home/A/gbl:/bin/zsh
admin01:x:1823:100:Keith Lastname,,:/home/B/admin01:/bin/bash
jbd:x:6358:100:Jack Lastname:/home/B/jbd:/bin/zsh

MailServer01
root:x:0:0:root:/root:/bin/bash
```
anotherroot:x:0:0:root:/anotherroot:/bin/zsh
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
slist:x:18:18:SmartList:/home/slist:/bin/zsh
gbl:x:100:100:Beowulf:/home/gbl:/bin/zsh

NameServer01
root:x:0:0:root:/root:/bin/zsh
anotherroot:x:0:0:Anotherroot:/root:/bin/zsh
addradius:x:0:0:Add new RADIUS user:/radius:/bin/sh
csync:x:5:0:sync:/bin/sync
shutdown:x:6:11:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
gbl:x:100:100:Gordon B Lastname:/home/gbl:/bin/bash

**SSH_CONFIG File**

```bash
#!/bin/bash
# script to get sshd_config file, MJG 10/30/2000
SERVERLIST=$(cat /root/serverlist)
For SERVER in $SERVERLIST; do
   /usr/local/bin/ssh -n -o 'BatchMode Yes' $SERVER \
   /bin/cat /etc/sshd_config \
   | elm -s "sshd_config for $SERVER" sysadmin
done

# This is ssh server systemwide configuration file. NameServer01

Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode no
X11Forwarding yes
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
AllowHosts 10.100.11.95 172.22.202.35 10.0.0.14 10.0.0.211
172.32.108.211 127.0.0.1
```

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes

# This is ssh server systemwide configuration file. OriginalServer

Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode no
X11Forwarding yes
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
AllowHosts 172.22.202.35 10.0.0.14 10.0.0.211 10.0.0.11 192.168.0.43
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes

# This is ssh server systemwide configuration file. NewWebServer

Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 2048
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin nopwd
IgnoreRhosts no
StrictModes yes
QuietMode no
X11Forwarding no
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility Local3
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
UseLogin no
AllowHosts *.consultant.net LogServer01.fd1My_Company.com *.execpc.com
#ForcedEmptyPasswdChange yes
SilentDeny no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts *.our.com friend.other.com
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes

# This is ssh server systemwide configuration file. LogServer01

Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 768
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin yes
IgnoreRhosts no
StrictModes yes
QuietMode no
X11Forwarding yes
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility DAEMON
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords yes
UseLogin no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
AllowHosts 172.22.202.35 10.0.0.211 10.0.0.11 10.0.0.12 10.0.0.13
10.0.0.15 10.0.0.240 172.32.108.211 10.0.0.244 0.0.2.17 127.10.196.171
127.200.163.110 127.10.205.50
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes

# This is ssh server systemwide configuration file. MailServer01

Port 22
ListenAddress 0.0.0.0
HostKey /etc/ssh_host_key
RandomSeed /etc/ssh_random_seed
ServerKeyBits 2048
LoginGraceTime 600
KeyRegenerationInterval 3600
PermitRootLogin no
IgnoreRhosts no
StrictModes yes
QuietMode no
X11Forwarding no
X11DisplayOffset 10
FascistLogging no
PrintMotd yes
KeepAlive yes
SyslogFacility Local3
RhostsAuthentication no
RhostsRSAAuthentication yes
RSAAuthentication yes
PasswordAuthentication yes
PermitEmptyPasswords no
UseLogin no
AllowSHosts *.consultant.net 10.0.0.14 10.0.0.11
AllowHosts 172.22.202.35 10.0.0.14 10.0.0.211 10.0.0.11
#ForcedEmptyPasswdChange yes
SilentDeny no
# CheckMail no
# PidFile /u/zappa/.ssh/pid
# AllowHosts *.our.com friend.other.com
# DenyHosts lowsecurity.theirs.com *.evil.org evil.org
# Umask 022
# SilentDeny yes

SUID and SGID Files Owned by root
#!/bin/bash
#script to get valid shells in passwd, MJG 10/30/2000
SERVERLIST=$(cat /root/serverlist)
For SERVER in $SERVERLIST; do
  /usr/local/bin/ssh -n -o 'BatchMode Yes' $SERVER \
  /usr/bin/find / -perm +6000 \
  | elm -s "suid and sgid for $SERVER" sysadmin
done

NameServer01
/var/spool/fax/outgoing/locks
/usr/local/bin/ssh1
/usr/local/src/perl5.004_04/lib/auto
/usr/local/src/perl5.004_04/lib/auto/Text
/usr/local/src/perl5.004_04/lib/auto/Text/ParseWords
/usr/local/src/perl5.004_04/.config
/usr/local/src/ipchains/ipchains-1.3.9
/usr/local/src/ipchains/ipchains-1.3.9/libipfwc
/usr/local/src/ipchains/ipchains-scripts-1.1.2
/usr/lib/dosemu/0.66.7.0/bin/dos
/usr/lib/majordomo/wrapper
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/write
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/wall
/usr/bin/at
/usr/bin/man
/usr/bin/passwd
/usr/bin/chage
/usr/bin/expiry
/usr/bin/gpasswd
/usr/bin/crontab
/usr/bin/suidperl
/usr/bin/sperl5.00403
/usr/bin/screen
/usr/bin/quota
/usr/bin/minicom
/usr/bin/rcp
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/xmonisdn
/usr/bin/smbmount
/usr/bin/smbunmount
/usr/bin/elm
/usr/bin/mutt
/usr/bin/lockfile
/usr/bin/procmail
/usr/bin/sperl5.00404
/usr/bin/su
/usr/bin/suexec
/usr/bin/suexec
/usr/bin/suexec
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/write
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/wall
/usr/bin/at
/usr/bin/man
/usr/bin/passwd
/usr/bin/sperl5.00403
/usr/bin/chage
/usr/bin/expiry
/usr/bin/gpasswd
/usr/bin/crontab
/usr/bin/quota
/usr/bin/screen
/usr/bin/elm
/usr/bin/minicom
/usr/bin/mutt
/usr/bin/rpc
/usr/bin/rlogin
/usr/bin/rsh
/usr/bin/lockfile
/usr/bin/procmail
/usr/local/bin/ssh1
/usr/local/src/proftpd-1.2.0pre3
/usr/local/src/proftpd-1.2.0pre3/contrib
/usr/local/src/proftpd-1.2.0pre3/contrib/libcap
/usr/local/src/proftpd-1.2.0pre3/doc
/usr/local/src/proftpd-1.2.0pre3/include
/usr/local/src/proftpd-1.2.0pre3/lib
/usr/local/src/proftpd-1.2.0pre3/modules
/usr/local/src/proftpd-1.2.0pre3/sample-configurations
/usr/local/src/proftpd-1.2.0pre3/src
/usr/local/src/qpopper3.0/popper/popauth
/usr/sbin/lpc
/usr/sbin/sendmail
/usr/sbin/traceroute
/usr/X11R6/bin/cardinfo
/home/A/ftp/pub
/bin/su
/bin/login
/bin/mount
/bin/umount
/bin/mail
/bin/ping
/sbin/cardctl
/sbin/dump
/sbin/restore
/sbin/rmt

NewWebServer
/usr/local/apache/bin/suexec
/usr/local/apache/htdocs/oldpeter/home/delliott/perl/perl5.004_04
/usr/local/apache/htdocs/oldpeter/home/delliott/perl/perl5.004_04/Porting
/usr/local/apache/htdocs/oldpeter/home/delliott/perl/perl5.004_04/cygwin
/usr/local/apache/htdocs/oldpeter/home/delliott/perl/perl5.004_04/eg
/usr/local/apache/htdocs/oldpeter/home/delliott/perl/perl5.004_04/eg/cgi
/var/spool/fax/outgoing/locks
/bin/mail
/bin/ping
/bin/su
/bin/login
/sbin/dump
/sbin/restore
/sbin/rmt

MailServer01
/usr/bin/wall
/usr/bin/procmail
/usr/bin/lockfile
/usr/bin/write
/usr/bin/sudo
/usr/bin/elm
/usr/bin/passwd
/usr/bin/sperl5.00502
/usr/bin/rsh
/usr/sbin/sendmail
/usr/sbin/traceroute
/usr/libexec/pt_chown
/usr/adm/su
/var/spool/fax/outgoing/locks
/home/slist/.bin/multigram
/home/slist/.bin/choplist
/home/slist/.bin/idhash
/home/slist/.bin/senddigest
/home/slist/.bin/flist
/bin/mail
/bin/ping
/bin/su
/bin/login
/sbin/dump
/sbin/restore
/sbin/rmt
/data/old/bin/su
/data/old/bin/login
/data/old/bin/mount
/data/old/bin/umount
/data/old/bin/mail
/data/old/bin/ping
/data/old/home/ftp/pub
/data/old/sbin/cardctl
/data/old/sbin/rmt
/data/old/sbin/dump
/data/old/sbin/restore
/data/old/sbin/rmt
/data/old/usr/local/bin/ssh1
/data/old/usr/lib/majordomo/wrapper
/data/old/usr/src/linux-2.0.37/drivers/sound
/data/old/usr/src/linux-2.0.37/drivers/sound/lowlevel
/data/old/usr/bin/chfn
/data/old/usr/bin/chsh
/data/old/usr/bin/newgrp
/data/old/usr/bin/write
/data/old/usr/bin/lpq
/data/old/usr/bin/lpr
/data/old/usr/bin/lprm
/data/old/usr/bin/wall
/data/old/usr/bin/at
/data/old/usr/bin/man
/data/old/usr/bin/passwd
/data/old/usr/bin/suidperl
/data/old/usr/bin/sperl5.00403
/data/old/usr/bin/chage
/data/old/usr/bin/expiry
/data/old/usr/bin/gpasswd
/data/old/usr/bin/crontab
/data/old/usr/bin/quota
/data/old/usr/bin/screen
/data/old/usr/bin/elm
/data/old/usr/bin/mutt
/data/old/usr/bin/minicom
/data/old/usr/bin/rcp
/data/old/usr/bin/rlogin
/data/old/usr/bin/rsh
/data/old/usr/bin/lockfile
/data/old/usr/bin/procmail
/data/old/usr/bin/smbmount
/data/old/usr/bin/smbumount
/data/old/usr/bin/1pc
/data/old/usr/bin/sendmail
/data/old/usr/bin/traceroute
/data/old/usr/X11R6/bin/cardinfo
/data/old/usr/libexec/sendmail/mail.local
/data/old/usr/libexec/sendmail/sendmail
/data/old/var/spool/fax/outgoing/locks
/nfs/home/A/ftp/pub

LogServer01
/var/spool/fax/outgoing/locks
/usr/local/bin/ssh1
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/write
/usr/bin/lpq
/usr/bin/lpr
/usr/bin/lprm
/usr/bin/wall
/usr/bin/at
/usr/bin/man
/usr/bin/passwd
/usr/bin/sperl5.00403
/usr/bin/chage
/usr/bin/expiry
/usr/bin/gpasswd
/usr/bin/crontab
/usr/bin/quota
/usr/bin/screen
/usr/bin/zgv
/usr/bin/elm
/usr/bin/minicom
/usr/bin/mutt
LSOF –i of all Servers

#!/bin/bash
#script to get valid shells in passwd, MJG 10/30/2000
SERVERLIST=$(cat /root/serverlist)
For SERVER in $SERVER
    do
        /usr/local/bin/ssh -n -o 'BatchMode Yes' $SERVER \
        /usr/sbin/lsof -I \
        | elm -s "Passwd shells for $SERVER" sysadmin
    done

NameServer01
<table>
<thead>
<tr>
<th>COMMAND</th>
<th>PID</th>
<th>USER</th>
<th>FD</th>
<th>TYPE</th>
<th>DEVICE</th>
<th>SIZE</th>
<th>NODE</th>
<th>NAME</th>
</tr>
</thead>
<tbody>
<tr>
<td>rpc.portm</td>
<td>90</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>DEVICE</td>
<td>SIZE</td>
<td>NODE</td>
<td>NAME</td>
</tr>
<tr>
<td>rpc.portm</td>
<td>90</td>
<td>root</td>
<td>4u</td>
<td>inet</td>
<td>DEVICE</td>
<td>SIZE</td>
<td>NODE</td>
<td>NAME</td>
</tr>
<tr>
<td>syslogd</td>
<td>98</td>
<td>root</td>
<td>1u</td>
<td>inet</td>
<td>40</td>
<td>UDP</td>
<td></td>
<td>syslog</td>
</tr>
<tr>
<td>xntpd</td>
<td>128</td>
<td>root</td>
<td>5u</td>
<td>inet</td>
<td>83</td>
<td>UDP</td>
<td></td>
<td>ntp</td>
</tr>
<tr>
<td>xntpd</td>
<td>128</td>
<td>root</td>
<td>6u</td>
<td>inet</td>
<td>85</td>
<td>UDP</td>
<td></td>
<td>localhost:ntp</td>
</tr>
<tr>
<td>xinetd</td>
<td>185</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>134</td>
<td>UDP</td>
<td></td>
<td>daytime</td>
</tr>
<tr>
<td>xinetd</td>
<td>185</td>
<td>root</td>
<td>5u</td>
<td>inet</td>
<td>171</td>
<td>UDP</td>
<td></td>
<td>daytime</td>
</tr>
<tr>
<td>sshd</td>
<td>197</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>222</td>
<td>TCP</td>
<td></td>
<td>ssh</td>
</tr>
<tr>
<td>radiusd</td>
<td>1594</td>
<td>root</td>
<td>4u</td>
<td>inet</td>
<td>7057926</td>
<td>UDP</td>
<td></td>
<td>radacct</td>
</tr>
<tr>
<td>Service</td>
<td>PID</td>
<td>User</td>
<td>Type</td>
<td>Port</td>
<td>Protocol</td>
<td>Destinations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-----</td>
<td>--------</td>
<td>------</td>
<td>----------</td>
<td>----------</td>
<td>-------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>radiusd</td>
<td>1594</td>
<td>root</td>
<td></td>
<td>7057927</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>radiusd</td>
<td>2958</td>
<td>root</td>
<td></td>
<td>7057926</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>radiusd</td>
<td>2958</td>
<td>root</td>
<td></td>
<td>7057927</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>radiusd</td>
<td>2958</td>
<td>root</td>
<td></td>
<td>7057928</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>sshd</td>
<td>16734</td>
<td>root</td>
<td></td>
<td>7465536</td>
<td>TCP</td>
<td>NameServer01.fdlMy_Company.com:ssh (ESTABLISHED)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>21860</td>
<td>root</td>
<td></td>
<td>7057926</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>21860</td>
<td>root</td>
<td></td>
<td>7057927</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>21860</td>
<td>root</td>
<td></td>
<td>7057928</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>21860</td>
<td>root</td>
<td></td>
<td>7057929</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23463</td>
<td>root</td>
<td></td>
<td>7057926</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23463</td>
<td>root</td>
<td></td>
<td>7057927</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23463</td>
<td>root</td>
<td></td>
<td>7057928</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23463</td>
<td>root</td>
<td></td>
<td>7057929</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23817</td>
<td>root</td>
<td></td>
<td>7057926</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23817</td>
<td>root</td>
<td></td>
<td>7057927</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23817</td>
<td>root</td>
<td></td>
<td>7057928</td>
<td>UDP</td>
<td>*:radacct</td>
<td></td>
<td></td>
</tr>
<tr>
<td>named</td>
<td>23817</td>
<td>root</td>
<td></td>
<td>7057929</td>
<td>UDP</td>
<td>*:radius</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
radiusd   23817 root    7u  inet 7057929       UDP *:2465
radiusd   32516 root    4u  inet 7057926       UDP *:radacct
radiusd   32516 root    5u  inet 7057927       UDP *:radius
radiusd   32516 root    6u  inet 7057928       UDP *:2464
radiusd   32516 root    7u  inet 7057929       UDP *:2465

OriginalServer
COMMAND     PID USER   FD   TYPE   DEVICE SIZE NODE NAME
rpc.portm   92 root    3u  inet       48       UDP *:sunrpc
rpc.portm   92 root    4u  inet       49 TCP *:sunrpc (LISTEN)
syslogd    100 root    1u  inet       54  UDP *:syslog
xntpd       129 root    4u  inet       88  UDP *:ntp
xntpd       129 root    5u  inet       89  UDP localhost:ntp
xntpd       129 root    6u  inet       90  UDP
OriginalServer.fdlMy_Company.com:ntp
rpc.mount   141 root    4u  inet       104      UDP *:742
rpc.mount   141 root    5u  inet       109      TCP *:745 (LISTEN)
rpc.nfsd    143 root    4u  inet       120      UDP *:2049
rpc.nfsd    143 root    5u  inet       123      TCP *:2049 (LISTEN)
sshd        199 root    3u  inet       265 TCP *:sshd (LISTEN)
httpd       240 root  142u  inet       779 TCP *:www (LISTEN)
proftpd     242 root    0u  inet      784 TCP *:ftp (LISTEN)
proftpd     2075 root    0u  inet 59278157       TCP OriginalServer.fdlMy_Company.com:ftp->209.83.4.215:1297 (CLOSE)
proftpd     2075 root    1u  inet 59278157       TCP OriginalServer.fdlMy_Company.com:ftp->209.83.4.215:1297 (CLOSE)
proftpd    5533 root    0u  inet 60264399       TCP
OriginalServer.fdlMy_Company.com:ftp->ppp-
012.max1.cli.dyn.My_Company.com:1754 (ESTABLISHED)
proftpd    5533 root    1u  inet 60264399       TCP
OriginalServer.fdlMy_Company.com:ftp->ppp-
012.max1.cli.dyn.My_Company.com:1754 (ESTABLISHED)
proftpd    5533 root    10u inet 60264459        TCP
OriginalServer.fdlMy_Company.com:ftp-data->ppp-
012.max1.cli.dyn.My_Company.com:1756 (ESTABLISHED)
proftpd    5533 root   11u  inet 60264459       TCP
OriginalServer.fdlMy_Company.com:ftp->ppp-
012.max1.cli.dyn.My_Company.com:1756 (ESTABLISHED)

named    6543 root    3u  inet 78210568       UDP *:2850
named    6543 root    20u inet 55812111       UDP localhost:domain
named    6543 root    21u inet 55812112       TCP localhost:domain
(named)  (LISTEN)
named    6543 root    22u inet 55812113       UDP
OriginalServer.fdlMy_Company.com:domain
named    6543 root    23u inet 55812114       TCP
OriginalServer.fdlMy_Company.com:domain (LISTEN)
named    6543 root    24u inet 55812115       UDP
ns2.My_Company.com:domain
named    6543 root    25u inet 55812116       TCP
ns2.My_Company.com:domain (LISTEN)
named    6543 root    26u inet 55812117       UDP
OriginalServer.My_Company.com:domain
named    6543 root    27u inet 55812118       TCP
OriginalServer.My_Company.com:domain (LISTEN)
named    6543 root    28u inet 55812119       UDP
172.16.192.100:domain
named    6543 root    29u inet 55812120       TCP
172.16.192.100:domain (LISTEN)
named    6543 root    30u inet 55812121       UDP
ns2.fdlMy_Company.com:domain
named    6543 root    31u inet 55812122       TCP
ns2.fdlMy_Company.com:domain (LISTEN)
named    6543 root    32u inet 55812123       UDP
virtual.fdlMy_Company.com:domain
named    6543 root    33u inet 55812124       TCP
virtual.fdlMy_Company.com:domain (LISTEN)
named    6543 root    34u inet 55812125       UDP ftp.martin-
design.net:domain
named    6543 root    35u inet 55812126       TCP ftp.martin-
design.net:domain (LISTEN)
named    6543 root    36u inet 55812127       UDP
peter.atw.earthreach.com:domain
named    6543 root    37u inet 55812128       TCP
peter.atw.earthreach.com:domain (LISTEN)
named    6543 root    38u inet 55812129       UDP
mars.someothernet.net:domain
named    6543 root    39u inet 55812130       TCP
mars.someothernet.net:domain (LISTEN)
named    6543 root    40u inet 55812131       UDP
ns2.consultant.net:domain
named    6543 root    41u inet 55812132       TCP
ns2.consultant.net:domain (LISTEN)
proftpd    6768 root    0u  inet 57753695       TCP
virtual.fd1My_Company.com:ftp->127.200.221.98:1032 (ESTABLISHED)
proftpd    6768 root    1u  inet 57753695       TCP
virtual.fd1My_Company.com:ftp->127.200.221.98:1032 (ESTABLISHED)
proftpd    6768 root   11u  inet 57757801       TCP
virtual.fd1My_Company.com:1436->127.200.221.98:1039 (ESTABLISHED)
proftpd    6768 root   12u  inet 57757801       TCP
virtual.fd1My_Company.com:1436->127.200.221.98:1039 (ESTABLISHED)
proftpd    8021 root    0u  inet 3600583       TCP
proftpd    8021 root    1u  inet 3600583       TCP
proftpd    8021 root   10u  inet 3600633       TCP
proftpd    8021 root   11u  inet 3600633       TCP
proftpd    9795 root    0u  inet 69774888       TCP
proftpd    9795 root    1u  inet 69774888       TCP
proftpd    9795 root   10u  inet 69777012       TCP
proftpd    9795 root   11u  inet 69777012       TCP
proftpd   10608 root    0u  inet 47362328       TCP
proftpd   10608 root    1u  inet 47362328       TCP
proftpd   10608 root   11u  inet 47365697       TCP
proftpd   10608 root   12u  inet 47365697       TCP
xinetd    11091 root    3u  inet 48962714       TCP *:telnet (LISTEN)
xinetd    11091 root    6u  inet 48962715       TCP *:pop3 (LISTEN)
xinetd    11091 root    7u  inet 48962716       TCP *:mailstats (LISTEN)
xinetd    11091 root    8u  inet 48962717       TCP *:smtp (LISTEN)
xinetd    11091 root    9u  inet 48962717       TCP *:smtp (LISTEN)
xinetd    11091 root   10u  inet 78166812       TCP
OriginalServer.fd1My_Company.com:2181 (CLOSE)
xinetd    11091 root   11u  inet 78166819       TCP
OriginalServer.fd1My_Company.com:2186->MailServer01.fd1My_Company.com:smtp (ESTABLISHED)
proftpd 13977 root 0u inet 3637312 TCP
proftpd 13977 root 1u inet 3637312 TCP
proftpd 13977 root 10u inet 3637411 TCP
proftpd 13977 root 11u inet 3637411 TCP
sshd 14343 root 5u inet 78183584 TCP
OriginalServer.fd1My_Company.com:ssh->LogServer01.fd1My_Company.com:1021 (ESTABLISHED)
proftpd 15747 root 0u inet 35145553 TCP
proftpd 15747 root 1u inet 35145553 TCP
proftpd 15747 root 10u inet 35148425 TCP
proftpd 15747 root 11u inet 35148425 TCP
xinetd 16131 root 3u inet 48962714 TCP ::telnet (LISTEN)
xinetd 16131 root 6u inet 48962715 TCP ::pop3 (LISTEN)
xinetd 16131 root 7u inet 48962716 TCP ::mailstats (LISTEN)
xinetd 16131 root 8u inet 48962717 TCP ::smtp (LISTEN)
proftpd 16517 root 0u inet 32992292 TCP
proftpd 16517 root 1u inet 32992292 TCP
proftpd 16517 root 10u inet 32995363 TCP
proftpd 16517 root 11u inet 32995363 TCP
xinetd 19418 root 3u inet 48962714 TCP ::telnet (LISTEN)
xinetd 19418 root 6u inet 48962715 TCP ::pop3 (LISTEN)
xinetd 19418 root 7u inet 48962716 TCP ::mailstats (LISTEN)
xinetd 19418 root 8u inet 48962717 TCP ::smtp (LISTEN)
xinetd 19418 root 9u inet 62443606 TCP
xinetd 19418 root 10u inet 62443611 TCP
OriginalServer.fd1My_Company.com:4611 (CLOSE)
xinetd 19418 root 11u inet 62443620 TCP
OriginalServer.fd1My_Company.com:4613->MailServer01.fd1My_Company.com:smtp (ESTABLISHED)
xinetd    19420 root    3u  inet  48962714 TCP :telnet (LISTEN)
xinetd    19420 root    6u  inet  48962715 TCP :pop3 (LISTEN)
xinetd    19420 root    7u  inet  48962716 TCP :mailstats (LISTEN)
xinetd    19420 root    8u  inet  48962717 TCP :smtp (LISTEN)
xinetd    19420 root    9u  inet  62443606 TCP
xinetd    19420 root   10u  inet  62443611 TCP
>xMailServer01.fdlMy_Company.com:smtp (ESTABLISHED)
proftpd   19860 root    0u  inet  23879782 TCP
proftpd   19860 root    1u  inet  23879782 TCP
proftpd   19860 root   10u  inet  23880373 TCP
proftpd   19860 root    11u  inet  23880373 TCP
proftpd   19884 root    0u  inet  76693542 TCP
proftpd   19884 root    1u  inet  76693542 TCP
proftpd   19884 root   10u  inet  76693813 TCP
proftpd   19884 root    11u  inet  76693813 TCP
popper    20150 root    0u  inet  78218989 TCP
popper    20150 root    1u  inet  78218989 TCP
popper    20150 root    2u  inet  78218989 TCP
proftpd   20256 root    0u  inet  45478115 TCP
OriginalServer.fdlMy_Company.com:ftp->cbrg1346.capecod.net:49192 (ESTABLISHED)
proftpd   20256 root    1u  inet  45478115 TCP
OriginalServer.fdlMy_Company.com:ftp->cbrg1346.capecod.net:49192 (ESTABLISHED)
proftpd   20256 root   10u  inet  45479720 TCP
proftpd  20256 root   11u  inet  45479720    TCP
(ESTABLISHED)
httpd  20283 root  3u  inet  78225037    TCP
(ESTABLISHED)
httpd  20283 root 142u  inet   779    TCP *:www (LISTEN)
popper  20404 root  0u  inet  78220540    TCP
OriginalServer.fdlMy_Company.com:pop3->ppp-
094.max1.rpn.dyn.My_Company.com:1076 (ESTABLISHED)
popper  20404 root   1u  inet  78220540    TCP
OriginalServer.fdlMy_Company.com:pop3->ppp-
094.max1.rpn.dyn.My_Company.com:1076 (ESTABLISHED)
popper  20404 root   2u  inet  78220540    TCP
OriginalServer.fdlMy_Company.com:pop3->ppp-
094.max1.rpn.dyn.My_Company.com:1076 (ESTABLISHED)
xinetd  20495 root   3u  inet  48962714    TCP *:telnet (LISTEN)
xinetd  20495 root   6u  inet  48962715    TCP *:pop3 (LISTEN)
xinetd  20495 root   7u  inet  48962716    TCP *:mailstats
(ESTABLISHED)
xinetd  20495 root   8u  inet  48962717    TCP *:smtp (LISTEN)
xinetd  20495 root   9u  inet  78221050    TCP
OriginalServer.fdlMy_Company.com:smtp->ppp-
021.max1.cli.dyn.My_Company.com:4202 (ESTABLISHED)
xinetd  20496 root   3u  inet  48962714    TCP *:telnet (LISTEN)
xinetd  20496 root   6u  inet  48962715    TCP *:pop3 (LISTEN)
xinetd  20496 root   7u  inet  48962716    TCP *:mailstats
(ESTABLISHED)
xinetd  20496 root   8u  inet  48962717    TCP *:smtp (LISTEN)
xinetd  20496 root   9u  inet  78221050    TCP
OriginalServer.fdlMy_Company.com:smtp->ppp-
021.max1.cli.dyn.My_Company.com:4202 (ESTABLISHED)
xinetd  20496 root   10u  inet  78221051   TCP
OriginalServer.fdlMy_Company.com:2889 (CLOSE)
xinetd  20496 root   11u  inet  78221052   TCP
OriginalServer.fdlMy_Company.com:2890-
>MailServer01.fdlMy_Company.com:smtp (ESTABLISHED)
xinetd  20496 root   3u  inet  48962714    TCP *:telnet (LISTEN)
xinetd  20496 root   6u  inet  48962715    TCP *:pop3 (LISTEN)
xinetd  20496 root   7u  inet  48962716    TCP *:mailstats
(ESTABLISHED)
xinetd  20496 root   8u  inet  48962717    TCP *:smtp (LISTEN)
xinetd  20496 root   9u  inet  78221050    TCP
OriginalServer.fdlMy_Company.com:smtp->ppp-
021.max1.cli.dyn.My_Company.com:4202 (ESTABLISHED)
xinetd  20496 root   10u  inet  78221051   TCP
OriginalServer.fdlMy_Company.com:2889 (CLOSE)
xinetd  20496 root   11u  inet  78221052   TCP
OriginalServer.fdlMy_Company.com:2890-
>MailServer01.fdlMy_Company.com:smtp (ESTABLISHED)
httpd  20664 root  3u  inet  78225139    TCP
(ESTABLISHED)
httpd  20664 root 142u  inet   779    TCP *:www (LISTEN)
httpd  20665 root  3u  inet  78224886    TCP
(ESTABLISHED)
httpd  20665 root 142u  inet   779    TCP *:www (LISTEN)
httpd  20689 root  3u  inet  78225052    TCP
(ESTABLISHED)
httpd  20689 root 142u  inet   779    TCP *:www (LISTEN)
httpd  20692 root  3u  inet  78225134    TCP
(ESTABLISHED)
<table>
<thead>
<tr>
<th>Service</th>
<th>PID</th>
<th>Username</th>
<th>Type</th>
<th>Source IP</th>
<th>Protocol</th>
<th>Destination IP</th>
<th>State</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Protocol Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>20692</td>
<td>root</td>
<td>142u</td>
<td>inet</td>
<td>TCP</td>
<td>*:www (LISTEN)</td>
<td>LISTEN</td>
<td>779</td>
<td></td>
<td></td>
</tr>
<tr>
<td>httpd</td>
<td>20693</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>TCP</td>
<td>virtual.fdlMy_Company.com:www</td>
<td></td>
<td>78225118</td>
<td>stclemens.cpe.dsl.enteract.com:20980</td>
<td>TCP</td>
</tr>
<tr>
<td>httpd</td>
<td>20698</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>TCP</td>
<td>virtual.fdlMy_Company.com:www</td>
<td>ESTABLISHED</td>
<td></td>
<td>ppp-008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>httpd</td>
<td>20693</td>
<td>root</td>
<td>142u</td>
<td>inet</td>
<td>TCP</td>
<td>*:www (LISTEN)</td>
<td>LISTEN</td>
<td>779</td>
<td></td>
<td></td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>TCP</td>
<td>48962717</td>
<td>LISTEN</td>
<td>7822534</td>
<td>ppp-008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>6u</td>
<td>inet</td>
<td>TCP</td>
<td>48962717</td>
<td>LISTEN</td>
<td></td>
<td>virtual.fdlMy_Company.com:www</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>7u</td>
<td>inet</td>
<td>TCP</td>
<td>48962716</td>
<td>LISTEN</td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>8u</td>
<td>inet</td>
<td>TCP</td>
<td>48962717</td>
<td>SMTP</td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>9u</td>
<td>inet</td>
<td>TCP</td>
<td>78226228</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>10u</td>
<td>inet</td>
<td>TCP</td>
<td>7822629</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>11u</td>
<td>inet</td>
<td>TCP</td>
<td>7822895</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>12u</td>
<td>inet</td>
<td>TCP</td>
<td>47426420</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>11u</td>
<td>inet</td>
<td>TCP</td>
<td>47426420</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>12u</td>
<td>inet</td>
<td>TCP</td>
<td>47426420</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>9u</td>
<td>inet</td>
<td>TCP</td>
<td>7822628</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>TCP</td>
<td>48962714</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>6u</td>
<td>inet</td>
<td>TCP</td>
<td>48962715</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>7u</td>
<td>inet</td>
<td>TCP</td>
<td>48962716</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>8u</td>
<td>inet</td>
<td>TCP</td>
<td>48962717</td>
<td>SMTP</td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>9u</td>
<td>inet</td>
<td>TCP</td>
<td>7822628</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>10u</td>
<td>inet</td>
<td>TCP</td>
<td>7822629</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>11u</td>
<td>inet</td>
<td>TCP</td>
<td>7822895</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>12u</td>
<td>inet</td>
<td>TCP</td>
<td>47426420</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>11u</td>
<td>inet</td>
<td>TCP</td>
<td>47426420</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>12u</td>
<td>inet</td>
<td>TCP</td>
<td>47426420</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>9u</td>
<td>inet</td>
<td>TCP</td>
<td>7822628</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>TCP</td>
<td>48962714</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>6u</td>
<td>inet</td>
<td>TCP</td>
<td>48962715</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>7u</td>
<td>inet</td>
<td>TCP</td>
<td>48962716</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>8u</td>
<td>inet</td>
<td>TCP</td>
<td>48962717</td>
<td>SMTP</td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>9u</td>
<td>inet</td>
<td>TCP</td>
<td>7822628</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>10u</td>
<td>inet</td>
<td>TCP</td>
<td>7822629</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>11u</td>
<td>inet</td>
<td>TCP</td>
<td>7822895</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>12u</td>
<td>inet</td>
<td>TCP</td>
<td>47426420</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>9u</td>
<td>inet</td>
<td>TCP</td>
<td>7822628</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>3u</td>
<td>inet</td>
<td>TCP</td>
<td>48962714</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>6u</td>
<td>inet</td>
<td>TCP</td>
<td>48962715</td>
<td></td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>7u</td>
<td>inet</td>
<td>TCP</td>
<td>48962716</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>8u</td>
<td>inet</td>
<td>TCP</td>
<td>48962717</td>
<td>SMTP</td>
<td></td>
<td>&gt;ppp 008.max1.rpn.dyn.My_Company.com:1027</td>
<td>TCP</td>
</tr>
<tr>
<td>xinetd</td>
<td>20769</td>
<td>root</td>
<td>9u</td>
<td>inet</td>
<td>TCP</td>
<td>7822628</td>
<td></td>
<td></td>
<td>OriginalServer.fdlMy_Company.com:smtp</td>
<td>TCP</td>
</tr>
</tbody>
</table>
popper    20859 root    0u  inet 78223085       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
012.max3.ply.dyn.My_Company.com:1031 (ESTABLISHED)
popper    20859 root    1u  inet 78223085       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
012.max3.ply.dyn.My_Company.com:1031 (ESTABLISHED)
popper    20859 root    2u  inet 78223085       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
012.max3.ply.dyn.My_Company.com:1031 (ESTABLISHED)
httpd     20860 root    3u  inet 78224893       TCP
(ESTABLISHED)
httpd     20860 root    142u  inet 779       TCP *:www (LISTEN)
proftpd   20866 root    0u  inet 47426796       TCP
(ESTABLISHED)
proftpd   20866 root    1u  inet 47426796       TCP
(ESTABLISHED)
proftpd   20866 root    11u  inet 47427172       TCP
virtual.fd1My_Company.com:3728->wildone.My_Company.com:1133
(ESTABLISHED)
proftpd   20866 root    12u  inet 47427172       TCP
virtual.fd1My_Company.com:3728->wildone.My_Company.com:1133
(ESTABLISHED)
popper    20941 root    0u  inet 78223540       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
015.max1.rpn.dyn.My_Company.com:1028 (ESTABLISHED)
popper    20941 root    1u  inet 78223540       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
015.max1.rpn.dyn.My_Company.com:1028 (ESTABLISHED)
popper    20941 root    2u  inet 78223540       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
015.max1.rpn.dyn.My_Company.com:1028 (ESTABLISHED)
popper    21084 root    0u  inet 78224300       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
013.max3.ply.dyn.My_Company.com:1041 (ESTABLISHED)
popper    21084 root    1u  inet 78224300       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
013.max3.ply.dyn.My_Company.com:1041 (ESTABLISHED)
popper    21084 root    2u  inet 78224300       TCP
OriginalServer.fd1My_Company.com:pop3->ppp-
013.max3.ply.dyn.My_Company.com:1041 (ESTABLISHED)
popper    21112 root    0u  inet 78224527       TCP
OriginalServer.fd1My_Company.com:pop3->208.161.99.110:1481
(ESTABLISHED)
popper    21112 root    1u  inet 78224527       TCP
OriginalServer.fd1My_Company.com:pop3->208.161.99.110:1481
(ESTABLISHED)
popper    21112 root    2u  inet 78224527       TCP
OriginalServer.fd1My_Company.com:pop3->208.161.99.110:1481
(ESTABLISHED)
httpd     21152 root    3u  inet 78225047       TCP
(ESTABLISHED)
httpd     21152 root    142u  inet 779       TCP *:www (LISTEN)
httpd     21154 root    3u  inet 78225042       TCP
(ESTABLISHED)
httpd     21154 root   142u inet 779 TCP *:www (LISTEN)
httpd     21155 root    3u  inet 78225152       TCP
virtual.fdMy_Company.com:www->fltg3-ppp10.fltg.net:1118 (ESTABLISHED)
httpd     21155 root   142u inet 779 TCP *:www (LISTEN)
popper    21160 root    0u  inet 78224900       TCP
popper    21160 root    1u  inet 78224900       TCP
popper    21160 root    2u  inet 78224900       TCP
popper    21175 root    0u  inet 78225003       TCP
OriginalServer.fdMy_Company.com:pop3->216.183.229.24:2589 (ESTABLISHED)
popper    21175 root    1u  inet 78225003       TCP
OriginalServer.fdMy_Company.com:pop3->216.183.229.24:2589 (ESTABLISHED)
popper    21175 root    2u  inet 78225003       TCP
OriginalServer.fdMy_Company.com:pop3->216.183.229.24:2589 (ESTABLISHED)
popper    21175 root    3u  inet 78225127       UDP *:3190
httpd     21182 root   142u inet 779 TCP *:www (LISTEN)
popper    21184 root    0u  inet 78225061       TCP
popper    21184 root    1u  inet 78225061       TCP
popper    21184 root    2u  inet 78225061       TCP
httpd     21186 root    3u  inet 78225133       TCP
virtual.fdMy_Company.com:www->stclemens.cpe.dsl.enteract.com:25810
(ESTABLISHED)
httpd     21186 root   142u inet 779 TCP *:www (LISTEN)
httpd     21187 root    3u  inet 78225147       TCP
(ESTABLISHED)
httpd     21187 root   142u inet 779 TCP *:www (LISTEN)
popper    21194 root    0u  inet 78225112       TCP
OriginalServer.fdMy_Company.com:pop3->ppp-017.max1.ply.dyn.My_Company.com:1873 (ESTABLISHED)
popper    21194 root    1u  inet 78225112       TCP
OriginalServer.fdMy_Company.com:pop3->ppp-017.max1.ply.dyn.My_Company.com:1873 (ESTABLISHED)
popper    21194 root    2u  inet 78225112       TCP
OriginalServer.fdMy_Company.com:pop3->ppp-017.max1.ply.dyn.My_Company.com:1873 (ESTABLISHED)
httpd     21198 root   142u inet 779 TCP *:www (LISTEN)
httpd     21200 root   142u inet 779 TCP *:www (LISTEN)
httpd     21201 root   142u inet 779 TCP *:www (LISTEN)
sshd     21208 root    5u  inet 78225184   TCP
LogServer01.fdMy_Company.com:ssh-
>LogServer01.fdMy_Company.com:1022 (ESTABLISHED)
httpd     21213 root  142u  inet 779 (LISTEN)
 proftpd  21221 root  0u  inet 40850438   TCP
 virtual.fdMy_Company.com:ftp->209.176.213.125:1727 (CLOSE_WAIT)
 proftpd  21221 root  1u  inet 40850438   TCP
 virtual.fdMy_Company.com:ftp->209.176.213.125:1727 (CLOSE_WAIT)
 proftpd  21221 root  10u inet 40858866   TCP
 proftpd  21221 root  11u inet 40858866   TCP
 proftpd  22253 root  0u inet 49198932   TCP
 virtual.fdMy_Company.com:ftp->AC86AB2B.ipt.aol.com:1025 (CLOSE_WAIT)
 proftpd  22523 root  1u inet 49198932   TCP
 virtual.fdMy_Company.com:ftp->AC86AB2B.ipt.aol.com:1025 (CLOSE_WAIT)
 proftpd  22523 root  10u inet 49199226   TCP
 virtual.fdMy_Company.com:ftp-data->AC86AB2B.ipt.aol.com:1029 (ESTABLISHED)
 proftpd  22523 root  11u inet 49199226   TCP
 virtual.fdMy_Company.com:ftp-data->AC86AB2B.ipt.aol.com:1029 (ESTABLISHED)
 proftpd  22990 root  0u inet 29331079   TCP
 proftpd  22990 root  1u inet 29331079   TCP
 proftpd  22990 root  11u inet 29334432   TCP
 proftpd  22990 root  12u inet 29334432   TCP
 proftpd  26064 root  0u inet 23918446   TCP
 proftpd  26064 root  1u inet 23918446   TCP
 proftpd  26064 root  10u inet 23918625   TCP
 proftpd  26064 root  11u inet 23918625   TCP
 proftpd  27043 root  0u inet 62293229   TCP
 virtual.fdMy_Company.com:ftp->127.200.221.102:1199 (CLOSE)
 proftpd  27043 root  1u inet 62293229   TCP
 virtual.fdMy_Company.com:ftp->127.200.221.102:1199 (CLOSE)
 proftpd  27043 root  11u inet 62308613   TCP
 virtual.fdMy_Company.com:3684->127.200.221.102:1493 (ESTABLISHED)
 proftpd  27043 root  12u inet 62308613   TCP
 virtual.fdMy_Company.com:3684->127.200.221.102:1493 (ESTABLISHED)
 proftpd  28334 root  0u inet 3724747    TCP
<table>
<thead>
<tr>
<th>Process</th>
<th>PID</th>
<th>User</th>
<th>FD</th>
<th>Type</th>
<th>Device</th>
<th>Size</th>
<th>Node</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>sshd</td>
<td>28492</td>
<td>root</td>
<td>5u</td>
<td>inet</td>
<td>77912492</td>
<td>TCP</td>
<td></td>
<td>OriginalServer.fd1My_Company.com:ssh-206.98.28.34:4800 (CLOSE_WAIT)</td>
</tr>
<tr>
<td>sshd</td>
<td>28492</td>
<td>root</td>
<td>10u</td>
<td>inet</td>
<td>77912492</td>
<td>TCP</td>
<td></td>
<td>OriginalServer.fd1My_Company.com:ssh-206.98.28.34:3187 (ESTABLISHED)</td>
</tr>
<tr>
<td>proftpd</td>
<td>29855</td>
<td>root</td>
<td>0u</td>
<td>inet</td>
<td>62506129</td>
<td>TCP</td>
<td></td>
<td>virtual.fd1My_Company.com:ftp-206.98.28.34:4800 (CLOSE_WAIT)</td>
</tr>
<tr>
<td>proftpd</td>
<td>29855</td>
<td>root</td>
<td>11u</td>
<td>inet</td>
<td>62506129</td>
<td>TCP</td>
<td></td>
<td>virtual.fd1My_Company.com:ftp-data-206.98.28.34:3187 (ESTABLISHED)</td>
</tr>
<tr>
<td>proftpd</td>
<td>31937</td>
<td>root</td>
<td>0u</td>
<td>inet</td>
<td>59261873</td>
<td>TCP</td>
<td></td>
<td>OriginalServer.fd1My_Company.com:ftp-209.83.4.215:1236 (CLOSE)</td>
</tr>
<tr>
<td>proftpd</td>
<td>31937</td>
<td>root</td>
<td>10u</td>
<td>inet</td>
<td>59261873</td>
<td>TCP</td>
<td></td>
<td>OriginalServer.fd1My_Company.com:ftp-data-209.83.4.215:1236 (CLOSE)</td>
</tr>
</tbody>
</table>

NewWebServer

**COMMAND** PID USER FD TYPE DEVICE SIZE NODE NAME
sshd  115 root  3u  IPv4  97  TCP *:ssh (LISTEN)
xntpd      122   root    4u  IPv4     119       UDP *:ntp
xntpd      122   root    5u  IPv4     120       UDP localhost:ntp
xntpd      122   root    6u  IPv4     121       UDP
NewWebServer.My_Company.com:ntp
xntpd      122   root    7u  IPv4     122       UDP ftp.adci.com:ntp
xntpd      122   root    8u  IPv4     123       UDP
ftp.somemapcom.com:ntp
xinetd    145   root    3u  IPv4     158       TCP *:pop3 (LISTEN)
xinetd    145   root    5u  IPv4     159       UDP *:discard
xinetd    145   root    6u  IPv4     160       TCP *:telnet (LISTEN)
xinetd    145   root    7u  IPv4     161       UDP *:daytime
xinetd    145   root    8u  IPv4     162       UDP *:time
mysqld    156   root    3u  IPv4     166       TCP *:3306 (LISTEN)
mysqld    158   root    3u  IPv4     166       TCP *:3306 (LISTEN)
mysqld    159   root    3u  IPv4     166       TCP *:3306 (LISTEN)
sendmail  162   root    4u  IPv4     190       TCP *:smtp (LISTEN)
httpd      167   root   99u  IPv4     760       TCP *:www (LISTEN)
httpsd     10569   root   15u  IPv4     832       TCP *:443 (LISTEN)
httpsd     10570   root   15u  IPv4     832       TCP *:443 (LISTEN)
httpsd     10571   root   15u  IPv4     832       TCP *:443 (LISTEN)
httpsd     10572   root   15u  IPv4     832       TCP *:443 (LISTEN)
httpsd     10891   root   15u  IPv4     832       TCP *:443 (LISTEN)
httpsd     10893   root   15u  IPv4     832       TCP *:443 (LISTEN)
httpsd     10894   root   15u  IPv4     832       TCP *:443 (LISTEN)
httpd  11550   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11551   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11552   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11553   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11554   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11556   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11558   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11570   root   99u  IPv4    760       TCP  *:www (LISTEN)
httpd  11571   root   99u  IPv4    760       TCP  *:www (LISTEN)
sshd   11676   root    5u  IPv4    5186247     TCP *:ssh (LISTEN)
httpsd  20754   root   15u  IPv4    832       TCP  *:443 (LISTEN)
httpsd  20757   root   15u  IPv4    832       TCP  *:443 (LISTEN)
MAILSERVER01
COMMAND     PID USER   FD   TYPE DEVICE SIZE NODE NAME
sshd        116 root    3u  IPv4       99       TCP  *:ssh (LISTEN)
xntpd       123 root    4u  IPv4    130       TCP *:ntpd
xntpd       123 root    5u  IPv4    131       TCP  localhost:ntpd
xntpd       123 root    6u  IPv4    132       UDP
MAILSERVER01.fdlMy_Company.com:ntp
xinetd      152 root    7u  IPv4    133       UDP
MAILSERVER01.fdlMy_Company.com:ntp
xinetd      152 root    8u  IPv4    134       UDP  192.168.0.23:ntp
rpc.portm   127 root    3u  IPv4    127       TCP  *:sunrpc
rpc.portm   127 root    4u  IPv4    128       TCP  *:sunrpc (LISTEN)
rpc.mount   129 root    4u  IPv4    145       UDP  *:730
rpc.mount   129 root    5u  IPv4    150       TCP  *:733 (LISTEN)
rpc.nfsd    132 root    4u  IPv4    163       UDP  *:2049
rpc.nfsd    132 root    5u  IPv4    166       TCP  *:2049 (LISTEN)
xinetd      152 root    3u  IPv4    218       TCP  *:mailstats (LISTEN)
xinetd      152 root    4u  IPv4    219       TCP  *:pop3 (LISTEN)
xinetd      152 root    5u  IPv4    220       UDP  *:discard
xinetd      152 root    6u  IPv4    221       TCP  *:telnet (LISTEN)
xinetd      152 root    7u  IPv4    222       UDP  *:daytime
xinetd      152 root    8u  IPv4    223       UDP  *:time
sendmail    952 root   11u  IPv4    30143618     TCP
MAILSERVER01.fdlMy_Company.com:3199->196.3.64.6:smtp (SYN_SENT)
sendmail   2121 root   11u  IPv4    30147197     TCP
MAILSERVER01.fdlMy_Company.com:3414->63.214.2.93:smtp (SYN_SENT)
sendmail   2799 root   11u  IPv4    30139237     TCP
MAILSERVER01.fdlMy_Company.com:2941->204.176.182.122:smtp (SYN_SENT)
sendmail   3886 root   11u  IPv4    30147551     TCP
MAILSERVER01.fdlMy_Company.com:3442->206.10.25.251:smtp (SYN_SENT)
sendmail   4750 root   11u  IPv4    30151222     TCP
MAILSERVER01.fdlMy_Company.com:3663->200.127.0.3:smtp (SYN_SENT)
sendmail   4750 root   13u  IPv4    30150027     TCP
MAILSERVER01.fdlMy_Company.com:3591->c.mx.execpc.com:smtp (ESTABLISHED)
sendmail   4750 root   14u  IPv4    30150027     TCP
MAILSERVER01.fdlMy_Company.com:3591->c.mx.execpc.com:smtp (ESTABLISHED)
sendmail   5051 root    1u  IPv4    30063796     TCP
sendmail  5051  root    3u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
sendmail  5051  root    5u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
sendmail  5055  root    1u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
sendmail  5055  root    3u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
sendmail  5055  root    5u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
sendmail  5055  root    1u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
Sendmail  5055  root    3u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
Sendmail  5055  root    5u  IPv4  30063796  TCP
MailServer01.My_Company.com:smtfp->ppp-
013.max1.rpn.dyn.My_Company.com:1133 (ESTABLISHED)
Sendmail  5296  root   11u  IPv4  30149100  TCP
MailServer01.My_Company.com:3525->199.201.120.1:smtp (SYN_SENT)
Sendmail  6576  root   11u  IPv4  30138498  TCP
MailServer01.My_Company.com:2904->co.ozaukee.wi.us:smtp (CLOSE_WAIT)
Sendmail  6576  root   12u  IPv4  30138498  TCP
MailServer01.My_Company.com:2904->co.ozaukee.wi.us:smtp (CLOSE_WAIT)
Sendmail  6576  root   13u  IPv4  30138568  TCP
MailServer01.My_Company.com:2908->196.3.64.6:smtp (SYN_SENT)
Sendmail  6850  root   11u  IPv4  30142201  TCP
MailServer01.My_Company.com:3089->172.173.224.16:smtp (SYN_SENT)
Sendmail  7794  root   1u  IPv4  30082497  TCP
MailServer01.My_Company.com:smtfp->ppp-
049.max1.rpn.dyn.My_Company.com:1100 (ESTABLISHED)
Sendmail  7794  root   3u  IPv4  30082497  TCP
MailServer01.My_Company.com:smtfp->ppp-
049.max1.rpn.dyn.My_Company.com:1100 (ESTABLISHED)
Sendmail  7794  root   5u  IPv4  30082497  TCP
MailServer01.My_Company.com:smtfp->ppp-
049.max1.rpn.dyn.My_Company.com:1100 (ESTABLISHED)
Sendmail  7810  root   1u  IPv4  30082497  TCP
MailServer01.My_Company.com:smtfp->ppp-
049.max1.rpn.dyn.My_Company.com:1100 (ESTABLISHED)
Sendmail  7810  root   3u  IPv4  30082497  TCP
MailServer01.My_Company.com:smtfp->ppp-
049.max1.rpn.dyn.My_Company.com:1100 (ESTABLISHED)
Sendmail  7810  root   5u  IPv4  30082497  TCP
MailServer01.My_Company.com:smtfp->ppp-
049.max1.rpn.dyn.My_Company.com:1100 (ESTABLISHED)
Sendmail  8163  root   11u  IPv4  30138014  TCP
MailServer01.My_Company.com:2874->co.ozaukee.wi.us:smtp (CLOSE_WAIT)
Sendmail  8163  root   12u  IPv4  30138014  TCP
MailServer01.My_Company.com:2874->co.ozaukee.wi.us:smtp (CLOSE_WAIT)
Sendmail  8163  root   13u  IPv4  30135333  TCP
MailServer01.My_Company.com:2703->mta-v14.mail.yahoo.com:smtp
(CLOSE_WAIT)
Sendmail  8163  root   14u  IPv4  30135333  TCP
MailServer01.My_Company.com:2703->mta-v14.mail.yahoo.com:smtp
(CLOSE_WAIT)
Sendmail  8163  root   15u  IPv4  30138055  TCP
sendmail  9565 root  3u  IPv4 30143298     TCP
MailServer01.My_Company.com:3177->mta-v14.mail.yahoo.com:smtp
(SYN_SENT)

sendmail  9794 root  11u IPv4 30140336    TCP
MailServer01.My_Company.com:2993->futuresite.register.com:smtp
(SYN_SENT)

sendmail  9855 root  3u  IPv4 30140214     TCP
MailServer01.My_Company.com:2988->mta-v12.mail.yahoo.com:smtp
(SYN_SENT)

sendmail  10616 root  3u  IPv4 30145110     TCP
MailServer01.My_Company.com:3289->mx-b-rwc.mail.home.com:smtp
(SYN_SENT)

sendmail  10766 root  3u  IPv4 30149786     TCP
MailServer01.My_Company.com:3576->mta-v11.mail.yahoo.com:smtp
(SYN_SENT)

sendmail  11035 root  3u  IPv4 30148164     TCP
MailServer01.My_Company.com:3488->mta-v12.mail.yahoo.com:smtp
(SYN_SENT)

sendmail  11173 root  11u IPv4 30149480     TCP
MailServer01.My_Company.com:3555->mta-v12.mail.yahoo.com:smtp
(SYN_SENT)

sendmail  11211 root  1u  IPv4 30105389     TCP

sendmail  11211 root  3u  IPv4 30105389     TCP

sendmail  12042 root  3u  IPv4 30144174     TCP

sendmail  12800 root  11u IPv4 30145969     TCP

sendmail  13153 root  3u  IPv4 30143563     TCP
MailServer01.My_Company.com:smtp->leusps01.landsend.com:smtp (SYN_SENT)

sendmail  13157 root  3u  IPv4 30147823     TCP
MailServer01.My_Company.com:smtp->mta-v11.mail.yahoo.com:smtp (SYN_SENT)

sendmail  13311 root  3u  IPv4 30149461     TCP
MailServer01.My_Company.com:smtp->mta-v12.mail.yahoo.com:smtp (SYN_SENT)
sendmail  13395 root    3u  IPv4 30149739       TCP
MailServer01.My_Company.com:3573->mta-v12.mail.yahoo.com:smtp
(SYN_SENT)
sendmail  14254 root    3u  IPv4 30141716       TCP
MailServer01.My_Company.com:3053->mta-v11.mail.yahoo.com:smtp
(SYN_SENT)
sendmail  14358 root    11u IPv4 30150017       TCP
MailServer01.My_Company.com:3590->isc.freei.net:smtp (ESTABLISHED)
sendmail  14358 root    12u IPv4 30150017       TCP
MailServer01.My_Company.com:3590->isc.freei.net:smtp (ESTABLISHED)
sendmail  14358 root    13u IPv4 30150763       TCP
MailServer01.My_Company.com:3641->ntfvt.d.fvt.com:smtp (SYN_SENT)
sendmail  14512 root    3u  IPv4 30143447       TCP
MailServer01.My_Company.com:3186->mta-v12.mail.yahoo.com:smtp
(SYN_SENT)
sendmail  14620 root    11u IPv4 30145158       TCP
MailServer01.My_Company.com:3294->mxpool01.netaddress.usa.net:smtp
(CLOSE_WAIT)
sendmail  14620 root    12u IPv4 30145158       TCP
MailServer01.My_Company.com:3294->mxpool01.netaddress.usa.net:smtp
(CLOSE_WAIT)
sendmail  14620 root    13u IPv4 30145228       TCP
MailServer01.My_Company.com:3299->mta-v9.mail.yahoo.com:smtp (SYN_SENT)
sendmail  14716 root    11u IPv4 30143184       TCP
MailServer01.My_Company.com:3168->mail.peshtigotimes.com:smtp
(SYN_SENT)
sendmail  15187 root    3u  IPv4 30146249       TCP
MailServer01.My_Company.com:3360->mta-v9.mail.yahoo.com:smtp (SYN_SENT)
sendmail  15303 root    3u  IPv4 30146294       TCP
MailServer01.My_Company.com:3364->mta-v9.mail.yahoo.com:smtp (SYN_SENT)
sendmail  15574 root    3u  IPv4 30148009       TCP
MailServer01.My_Company.com:3478->mx-f-rwc.mail.home.com:smtp
(SYN_SENT)
sendmail  15574 root    13u IPv4 30147838       TCP
MailServer01.My_Company.com:3468->red1.netwurx.net:smtp (ESTABLISHED)
sendmail  15574 root    14u IPv4 30147838       TCP
MailServer01.My_Company.com:3468->red1.netwurx.net:smtp (ESTABLISHED)
sendmail  15574 root    15u IPv4 30147962       TCP
MailServer01.My_Company.com:3475->mail.nconnect.net:smtp (ESTABLISHED)
sendmail  15574 root    16u IPv4 30147962       TCP
MailServer01.My_Company.com:3475->mail.nconnect.net:smtp (ESTABLISHED)
sendmail  15579 root    1u  IPv4 30134171       TCP
sendmail  15579 root    3u  IPv4 30134171       TCP
sendmail  15579 root    5u  IPv4 30134171       TCP
sendmail  15602 root    3u  IPv4 30147714       TCP
MailServer01.My_Company.com:3456->mta-v14.mail.yahoo.com:smtp
(SYN_SENT)
sendmail  15609 root    1u  IPv4 30134171       TCP
sendmail  15609 root    3u  IPv4 30134171       TCP
sendmail  15609 root    5u  IPv4 30134171       TCP
sendmail  15652 root    3u  IPv4 30148210       TCP
MailServer01.My_Company.com:3493->mta-v13.mail.yahoo.com:smtp (SYN_SENT)
sendmail  15693 root    3u  IPv4 30148388       TCP
MailServer01.My_Company.com:3499->mta-v14.mail.yahoo.com:smtp (SYN_SENT)
sendmail  15742 root    3u  IPv4 30148758       TCP
MailServer01.My_Company.com:3523->mta-v5.mail.yahoo.com:smtp (ESTABLISHED)
sendmail  15931 root    3u  IPv4 30150235       TCP
MailServer01.My_Company.com:3604->mta-v14.mail.yahoo.com:smtp (SYN_SENT)
sendmail  16237 root    3u  IPv4 30138042       TCP
MailServer01.My_Company.com:2876->mta-v14.mail.yahoo.com:smtp (SYN_SENT)
sendmail  16476 root    11u IPv4 30148546       TCP
sendmail  16482 root    3u  IPv4 30139995       TCP
MailServer01.My_Company.com:2972->mta-v13.mail.yahoo.com:smtp (SYN_SENT)
sendmail  16486 root    3u  IPv4 30145029       TCP
MailServer01.My_Company.com:3282->mta-v9.mail.yahoo.com:smtp (SYN_SENT)
sendmail  16591 root    1u  IPv4 30140765       TCP
MailServer01.My_Company.com:smtp->m28.boston.juno.com:57950 (ESTABLISHED)
sendmail  16591 root    3u  IPv4 30140765       TCP
MailServer01.My_Company.com:smtp->m28.boston.juno.com:57950 (ESTABLISHED)
sendmail  16591 root    5u  IPv4 30140765       TCP
MailServer01.My_Company.com:smtp->m28.boston.juno.com:57950 (ESTABLISHED)
sendmail  16609 root    3u  IPv4 30141195       TCP
MailServer01.My_Company.com:3019->mta-v13.mail.yahoo.com:smtp (SYN_SENT)
sendmail  16668 root    1u  IPv4 30141542       TCP
sendmail  16668 root    3u  IPv4 30141542       TCP
sendmail  16668 root    5u  IPv4 30141542       TCP
sendmail  16738 root    1u  IPv4 30141996       TCP
sendmail 16738 root 3u IPv4 30141996 TCP
sendmail 16738 root 5u IPv4 30141996 TCP
sendmail 16739 root 1u IPv4 30141996 TCP
sendmail 16739 root 3u IPv4 30141996 TCP
sendmail 16739 root 5u IPv4 30141996 TCP
sendmail 16897 root 6u IPv4 30144728 TCP
sendmail 16897 root 13u IPv4 30144292 TCP
sendmail 16897 root 14u IPv4 30144292 TCP
sendmail 16897 root 15u IPv4 30144332 TCP
sendmail 16897 root 16u IPv4 30144332 TCP
sendmail 16897 root 17u IPv4 30144332 TCP
sendmail 17678 root 6u IPv4 30141542 TCP
MailServer01.My_Company.com:smtp->mta.excite.com:smtp (ESTABLISHED)
sendmail 17678 root 8u IPv4 30141542 TCP
MailServer01.My_Company.com:smtp->mta.excite.com:smtp (ESTABLISHED)
sendmail 17678 root 9u IPv4 30141542 TCP
MailServer01.My_Company.com:smtp->mta.excite.com:smtp (ESTABLISHED)
sendmail 17678 root 10u IPv4 30141542 TCP
MailServer01.My_Company.com:smtp->mta.excite.com:smtp (ESTABLISHED)
sendmail 17809 root 1u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 3u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 5u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 7u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 9u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 11u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 13u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 15u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 17u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 19u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 21u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 23u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)
sendmail 17809 root 25u IPv4 30148716 TCP
MailServer01.My_Company.com:smtp->smtp1.mailbits.com:16547 (ESTABLISHED)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.
sendmail 17826 root 14u IPv4 30149165 TCP
MailServer01.My_Company.com:3532->mta.excite.com:smtp (ESTABLISHED)
sendmail 17826 root 15u IPv4 30149184 TCP
MailServer01.My_Company.com:3535->red1.netwurx.net:smtp (ESTABLISHED)
sendmail 17826 root 16u IPv4 30149184 TCP
MailServer01.My_Company.com:3535->red1.netwurx.net:smtp (ESTABLISHED)
sendmail 17828 root 3u IPv4 30149156 TCP
MailServer01.My_Company.com:3530->mta-v12.mail.yahoo.com:smtp (SYN_SENT)
sendmail 17872 root 3u IPv4 30149707 TCP
MailServer01.My_Company.com:3571->mta-v13.mail.yahoo.com:smtp (SYN_SENT)
sendmail 17897 root 11u IPv4 30145340 TCP
sendmail 18068 root 1u  IPv4 30150620  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1780
(ESTABLISHED)
sendmail 18068 root 3u  IPv4 30150620  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1780
(ESTABLISHED)
sendmail 18068 root 5u  IPv4 30150620  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1780
(ESTABLISHED)
sendmail 18080 root 1u  IPv4 30150605  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1764
(ESTABLISHED)
sendmail 18080 root 3u  IPv4 30150605  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1764
(ESTABLISHED)
sendmail 18080 root 5u  IPv4 30150605  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1764
(ESTABLISHED)
sendmail 18081 root 1u  IPv4 30150696  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1779
(ESTABLISHED)
sendmail 18081 root 3u  IPv4 30150696  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1779
(ESTABLISHED)
sendmail 18081 root 5u  IPv4 30150696  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1779
(ESTABLISHED)
sendmail 18084 root 3u  IPv4 30150721  TCP
MailServer01.My_Company.com:smtp->c012-h018.c012.sfo.cp.net:61933
(ESTABLISHED)
sendmail 18084 root 5u  IPv4 30150721  TCP
MailServer01.My_Company.com:smtp->c012-h018.c012.sfo.cp.net:61933
(ESTABLISHED)
sendmail 18084 root 6u  IPv4 30150728  TCP
MailServer01.My_Company.com:smtp->c012-h018.c012.sfo.cp.net:auth
(SYN_SENT)
sendmail 18090 root 1u  IPv4 30150774  TCP
MailServer01.fd1My_Company.com:smtp->OriginaServer.fd1My_Company.com:3851
(ESTABLISHED)
sendmail 18090 root 3u  IPv4 30150774  TCP
MailServer01.fd1My_Company.com:smtp->OriginaServer.fd1My_Company.com:3851
(ESTABLISHED)
sendmail 18090 root 5u  IPv4 30150774  TCP
MailServer01.fd1My_Company.com:smtp->OriginaServer.fd1My_Company.com:3851
(ESTABLISHED)
sendmail 18095 root 1u  IPv4 30150774  TCP
MailServer01.fd1My_Company.com:smtp->OriginaServer.fd1My_Company.com:3851
(ESTABLISHED)
sendmail 18095 root 3u  IPv4 30150774  TCP
MailServer01.fd1My_Company.com:smtp->OriginaServer.fd1My_Company.com:3851
(ESTABLISHED)
sendmail 18095 root 5u  IPv4 30150774  TCP
MailServer01.fd1My_Company.com:smtp->OriginaServer.fd1My_Company.com:3851
(ESTABLISHED)
sendmail 18096 root 1u  IPv4 30150696  TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1779
(ESTABLISHED)
sendmail  18096 root    3u  IPv4 30150696       TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1779
(ESTABLISHED)

sendmail  18096 root    5u  IPv4 30150696       TCP
MailServer01.My_Company.com:smtp->web902.mail.yahoo.com:1779
(ESTABLISHED)

sendmail  18101 root    1u  IPv4 30150835       TCP

sendmail  18101 root    3u  IPv4 30150835       TCP

sendmail  18101 root    5u  IPv4 30150835       TCP

sendmail  18110 root    1u  IPv4 30150835       TCP

sendmail  18110 root    3u  IPv4 30150835       TCP

sendmail  18110 root    5u  IPv4 30150835       TCP

sendmail  18125 root    3u  IPv4 30150971       TCP
MailServer01.My_Company.com:smtp->mail.sriw.be:1508 (ESTABLISHED)

sendmail  18125 root    5u  IPv4 30150971       TCP
MailServer01.My_Company.com:smtp->mail.sriw.be:1508 (ESTABLISHED)

sendmail  18125 root    6u  IPv4 30151208       UDP

sendmail  18137 root    1u  IPv4 30151044       TCP
MailServer01.My_Company.com:smtp->imo-d10.mx.aol.com:44742
(ESTABLISHED)

sendmail  18137 root    3u  IPv4 30151044       TCP
MailServer01.My_Company.com:smtp->imo-d10.mx.aol.com:44742
(ESTABLISHED)

sendmail  18137 root    5u  IPv4 30151044       TCP
MailServer01.My_Company.com:smtp->imo-d10.mx.aol.com:44742
(ESTABLISHED)

sendmail  18150 root    3u  IPv4 30151113       TCP
MailServer01.My_Company.com:smtp->outmta006.topica.com:65415
(ESTABLISHED)

sendmail  18150 root    5u  IPv4 30151113       TCP
MailServer01.My_Company.com:smtp->outmta006.topica.com:65415
(ESTABLISHED)

sendmail  18150 root    6u  IPv4 30151121       TCP
MailServer01.My_Company.com:smtp->outmta006.topica.com:auth (SYN_SENT)

sendmail  18153 root    1u  IPv4 30151142       TCP
MailServer01.My_Company.com:smtp->serak.svc.tds.net:43196 (ESTABLISHED)

sendmail  18153 root    3u  IPv4 30151142       TCP
MailServer01.My_Company.com:smtp->serak.svc.tds.net:43196 (ESTABLISHED)

sendmail  18153 root    5u  IPv4 30151142       TCP
MailServer01.My_Company.com:smtp->serak.svc.tds.net:43196 (ESTABLISHED)

sendmail  18170 root    3u  IPv4 30151250       TCP
MailServer01.My_Company.com:smtp->LogServer01.fdlMy_Company.com:4526
(ESTABLISHED)
sendmail 18170 root 5u  IPv4 30151250  TCP
MailServer01.My_Company.com:smtp->LogServer01.fd1My_Company.com:4526
(ESTABLISHED)

sendmail 18170 root 6u  IPv4 30151256  TCP
MailServer01.My_Company.com:3664->LogServer01.fd1My_Company.com:auth
(SYN_SENT)

sshd 18173 root 5u  IPv4 30151267  TCP
(ESTABLISHED)

sendmail 18174 root 3u  IPv4 30151271  TCP
MailServer01.My_Company.com:smtp->LogServer01.fd1My_Company.com:4527
(ESTABLISHED)

sendmail 18174 root 5u  IPv4 30151271  TCP
MailServer01.My_Company.com:smtp->LogServer01.fd1My_Company.com:4527
(ESTABLISHED)

sendmail 18175 root 1u  IPv4 30151044  TCP
MailServer01.My_Company.com:smtp->imo-d10.mx.aol.com:44742
(ESTABLISHED)

sendmail 18175 root 3u  IPv4 30151044  TCP
MailServer01.My_Company.com:smtp->imo-d10.mx.aol.com:44742
(ESTABLISHED)

sendmail 18175 root 5u  IPv4 30151044  TCP
MailServer01.My_Company.com:smtp->imo-d10.mx.aol.com:44742
(ESTABLISHED)

sendmail 18176 root 3u  IPv4 30151286  TCP
MailServer01.My_Company.com:smtp->imo-d02.mx.aol.com:59216
(ESTABLISHED)

sendmail 18176 root 5u  IPv4 30151286  TCP
MailServer01.My_Company.com:smtp->imo-d02.mx.aol.com:59216
(ESTABLISHED)

sendmail 18176 root 6u  IPv4 30151292  TCP
MailServer01.My_Company.com:3666->imo-d02.mx.aol.com:auth (SYN_SENT)

sendmail 19585 root 11u  IPv4 30147096  TCP

sendmail 21250 root 3u  IPv4 24653214  TCP *:smtp (LISTEN)

sendmail 21499 root 11u  IPv4 30144533  TCP
MailServer01.My_Company.com:3244->isc.freei.net:smtp (ESTABLISHED)

sendmail 21499 root 12u  IPv4 30144533  TCP
MailServer01.My_Company.com:3244->isc.freei.net:smtp (ESTABLISHED)

sendmail 21499 root 13u  IPv4 30144723  TCP
MailServer01.My_Company.com:3253->futuresite.register.com:smtp
(SYN_SENT)

sendmail 23970 root 11u  IPv4 30141502  TCP
MailServer01.My_Company.com:3038->216.102.246.27:smtp (SYN_SENT)

named 27647 root 3u  IPv4 28371188  UDP *:2118

named 27647 root 20u  IPv4 28371180  UDP localhost:domain

(named (LISTEN)

named 27647 root 21u  IPv4 28371181  TCP localhost:domain

named 27647 root 22u  IPv4 28371182  UDP

MailServer01.My_Company.com:domain

named 27647 root 23u  IPv4 28371183  TCP
MailServer01.My_Company.com:domain (LISTEN)

named 27647 root 24u  IPv4 28371184  UDP

MailServer01.fd1My_Company.com:domain
named     27647 root   25u  IPv4 28371185       TCP
MailServer01.fdlMy_Company.com:domain (LISTEN)
named     27647 root   26u  IPv4 28371186       UDP 192.168.0.23:domain
named     27647 root   27u  IPv4 28371187       TCP 192.168.0.23:domain
(LISTEN)
sendmail  27952 root    1u  IPv4 30004839       TCP
MailServer01.My_Company.com:smtp->ppp-
062.max1.rpn.dyn.My_Company.com:1180 (ESTABLISHED)
sendmail  27952 root    3u  IPv4 30004839       TCP
MailServer01.My_Company.com:smtp->ppp-
062.max1.rpn.dyn.My_Company.com:1180 (ESTABLISHED)
sendmail  27952 root    5u  IPv4 30004839       TCP
MailServer01.My_Company.com:smtp->ppp-
062.max1.rpn.dyn.My_Company.com:1180 (ESTABLISHED)
sendmail  28028 root    1u  IPv4 30004839       TCP
MailServer01.My_Company.com:smtp->ppp-
062.max1.rpn.dyn.My_Company.com:1180 (ESTABLISHED)
sendmail  28028 root    3u  IPv4 30004839       TCP
MailServer01.My_Company.com:smtp->ppp-
062.max1.rpn.dyn.My_Company.com:1180 (ESTABLISHED)
sendmail  28028 root    5u  IPv4 30004839       TCP
MailServer01.My_Company.com:smtp->ppp-
062.max1.rpn.dyn.My_Company.com:1180 (ESTABLISHED)
sendmail  30661 root    1u  IPv4 30019583       TCP
MailServer01.My_Company.com:smtp->ppp-
076.max1.rpn.dyn.My_Company.com:1189 (ESTABLISHED)
sendmail  30661 root    3u  IPv4 30019583       TCP
MailServer01.My_Company.com:smtp->ppp-
076.max1.rpn.dyn.My_Company.com:1189 (ESTABLISHED)
sendmail  30661 root    5u  IPv4 30019583       TCP
MailServer01.My_Company.com:smtp->ppp-
076.max1.rpn.dyn.My_Company.com:1189 (ESTABLISHED)
sendmail  30661 root    11u IPv4 30143170       TCP
MailServer01.My_Company.com:smtp->ppp-
076.max1.rpn.dyn.My_Company.com:1189 (ESTABLISHED)
sendmail  30715 root   11u IPv4 30143170       TCP
MailServer01.My_Company.com:smtp->ppp-
076.max1.rpn.dyn.My_Company.com:1189 (ESTABLISHED)
sendmail  30823 root    1u  IPv4 30020454       TCP
MailServer01.fdlMy_Company.com:smtp->
>OriginalServer.fdlMy_Company.com:2186 (ESTABLISHED)
sendmail  30823 root    3u  IPv4 30020454       TCP
sendmail 30833 root 3u IPv4 30020454 TCP
MailServer01.fdlMy_Company.com:smtp-
>OriginalServer.fdlMy_Company.com:2186 (ESTABLISHED)
sendmail 30833 root 5u IPv4 30020454 TCP
MailServer01.fdlMy_Company.com:smtp-
>OriginalServer.fdlMy_Company.com:2186 (ESTABLISHED)
sendmail 31528 root 11u IPv4 25180766 TCP
MailServer01.My_Company.com:2707->jax-mail101.firstunion.com:smtp (ESTABLISHED)
sendmail 31576 root 1u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)
sendmail 31576 root 3u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)
sendmail 31576 root 5u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)
sendmail 31576 root 3u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)
sendmail 31576 root 5u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)
sendmail 31576 root 3u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)
sendmail 31576 root 5u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)
sendmail 31576 root 3u IPv4 30025189 TCP
MailServer01.My_Company.com:smtp->6.47.228.206.in-addr.arpa:3316 (ESTABLISHED)

LogServer01
COMMAND PID USER FD TYPE DEVICE SIZE NODE NAME
rpc.portm 91 root 3u inet 34 UDP *:sunrpc
rpc.portm 91 root 4u inet 35 TCP *:sunrpc (LISTEN)
syslogd 96 root 1u inet 39 UDP *:syslog
xntpd 127 root 4u inet 77 UDP *:ntp
xntpd 127 root 5u inet 78 UDP localhost:ntp
xntpd 127 root 6u inet 79 UDP
LogServer01.fdlMy_Company.com:ntp
rpc.rstat 144 root 3u inet 96 UDP *:748
rpc.rstat 144 root 4u inet 105 TCP *:753 (LISTEN)
ssh 3198 root 3u inet 13903047 TCP
LogServer01.fdlMy_Company.com:1021->OriginalServer.fdlMy_Company.com:ssh (ESTABLISHED)
httpsd 3396 root 15u inet 91978 TCP *:ssl1 (LISTEN)
httpsd 3396 root 16u inet 91979 TCP *:www (LISTEN)
httpsd 3397 root 15u inet 91978 TCP *:ssl1 (LISTEN)
httpsd    3397 root  16u  inet  91979    TCP *:www (LISTEN)
httpsd    4169 root  15u  inet  91978    TCP *:ssl (LISTEN)
httpsd    4169 root  16u  inet  91979    TCP *:www (LISTEN)
httpsd    6282 root  15u  inet  91978    TCP *:ssl (LISTEN)
httpsd    6282 root  16u  inet  91979    TCP *:www (LISTEN)
httpsd    11309 root  15u  inet  91978    TCP *:ssl (LISTEN)
httpsd    11309 root  16u  inet  91979    TCP *:www (LISTEN)
httpsd    11933 root  15u  inet  91978    TCP *:ssl (LISTEN)
httpsd    11933 root  16u  inet  91979    TCP *:www (LISTEN)
xinetd    14468 root  3u  inet  1921754  TCP *:shell (LISTEN)
httpsd    15658 root  15u  inet  91978    TCP *:ssl (LISTEN)
httpsd    15658 root  16u  inet  91979    TCP *:www (LISTEN)
httpsd    15659 root  15u  inet  91978    TCP *:ssl (LISTEN)
httpsd    15659 root  16u  inet  91979    TCP *:www (LISTEN)
sshd      24104 root  7u  inet  13842206  TCP LogServer01.fdlMy_Company.com:ssh-
          >OriginalServer.fdlMy_Company.com:1022 (ESTABLISHED)
sshd      24880 root  3u  inet  3846147    TCP *:ssh (LISTEN)
sshd      27489 root  7u  inet  13859703  TCP LogServer01.fdlMy_Company.com:ssh-
          >OriginalServer.fdlMy_Company.com:1021 (ESTABLISHED)
httpsd    31565 root  15u  inet  91978    TCP *:ssl (LISTEN)
httpsd    31565 root  16u  inet  91979    TCP *:www (LISTEN)
# Upcoming Training

<table>
<thead>
<tr>
<th>Training Type</th>
<th>Location</th>
<th>Dates</th>
<th>Delivery</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANSFIRE 2020, DC</td>
<td></td>
<td>Jun 13, 2020 - Jun 20, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>