Global Information Assurance Certification Paper

Security Assessment
of
McClure Industries, Inc.

August 2000

SecureDogHosting
5501 Cherokee Avenue
1st Floor
Alexandria, VA 22312
703.256.2869

Table of Contents

Executive Summary

The purpose of this assessment is to examine the corporate Information Technology (IT) security practices of McClure Industries, Inc. and compare them to industry best practices. Practices that are found to be noncompliant with industry best practices will be identified. SecureDogHosting will make recommendations to bring security practices within acceptable limits of industry best practices. Some of the more common vulnerabilities are found within the configuration of the operating system, third-party software, administrative practices, and security policies.

McClure Industries is not compliant with all industry best practices; the results of the assessment are summarized below.

Policies: No policies are in place for McClure Industries. Policies are the backbone of a solid IT security stance. Without comprehensive policies in place it is difficult to plan for potential disasters including loss of power, loss of network connectivity, denial of service attacks, or natural disaster. A lack of complete and tested policies and plans for responding to such potential disasters is a serious threat to McClure Industries ability to continue IT operations.

Configuration Vulnerabilities: McClure Industries currently deploys servers in a default state. This means that servers are not configured for their specific roles within the corporate infrastructure and not hardened for additional security. Most default server installations, with few exceptions, are not "secure by default". Deploying servers or other infrastructure items without first securing them for their specific roles creates a high risk of vulnerability that is not normally acceptable.

Administrative Practices: Many key policies are not in place for the administration of McClure Industries infrastructure. This includes not having plans or policies in place for passwords (aging, length, etc.), user account handling, regular backup policies, or incident handling. Without these types of specific policies being in place and known by system administrators a serious risk exists for improperly configured users, passwords, backups, etc. and creates a high level of vulnerability to the infrastructure as a whole.

Access to the network perimeter is acceptable, with a firewall and a "deny by default" rule set in place. No external dial in (modem) connections are permitted. System administrators are aware of security issues and are knowledgeable of security practices as a whole. Additional training and personnel may benefit the IT staff to assist in correcting current security issues.

Introduction

The purpose of this assessment is to examine the corporate Information Technology (IT) security practices of McClure Industries, Inc. and compare them to industry best practices. Practices that are found to be noncompliant with industry best practices will be identified. SecureDogHosting will make recommendations to bring security practices within acceptable limits of industry best practices.

Conduct of the Assessment

SecureDogHosting visited the McClure Industries, Inc. facility in Washington DC during August 1-4, 2000. During the visit a Linux server was analyzed and interviews were held with key IT personnel.

Overview of Existing Infrastructure

Network

The network is run on 100BaseT. The network primarily consists of numerous hubs plugged into a single switch. Internet connectivity is gained through a Cisco router and a Watchguard firewall. No remote dial in connections are provided.

Systems

The assessed system that this document discusses was an Intel based Linux server running RedHat 6.1. The primary role assigned to the assessed machine is that of a web server.

Most server nodes at McClure Industries are RedHat Linux based and used for serving web content, database applications, and electronic mail services.

Physical

Physical security is adequate for the expected threat level of McClure Industries. All access is controlled via electronic cipher-locks. The data center is located behind an additional electronic cipher-lock to ensure controlled access.

Threat Level

The threat level of McClure Industries is low for most types of computer crime. McClure Industries, its line of business, and its network do not represent the typical target of computer-based crime. McClure Industries may still become a target even though it doesn't match the typical target profile by disgruntled employees, competitive companies, or disaster.

Risk Assessment

Based on the interviews of McClure Industries' employees, assessment of a deployed system, and physical inspection of the data center, deviations from best practices exist. Each deviation carries with it an associated risk. It should be noted that this review has only examined a deployed system, the policies, procedures, and practices of the IT environment and therefore, does not completely address all possible threats and vulnerabilities to corporate information. The risks presented below are arranged in order of criticality.

Risk is derived from a combination of a system vulnerability and the existence of a threat that can exploit the vulnerability. The overall risk of each vulnerability is ranked on a scale from one to ten and defined as Low Risk, Medium Risk, or High Risk. These terms are defined as:

- **Low Risk (1-4)** - The vulnerability poses a small level of risk to the confidentiality, integrity, and/or availability of McClure Industries' data or IT systems, and/or it is unlikely to occur. Action to remove the vulnerability should be taken if the small reduction in risk outweighs the cost.

- **Medium Risk (5-7)** - The vulnerability poses a significant level of risk to the confidentiality, integrity, and/or availability of McClure Industries information or IT systems. There is a real possibility that this may occur. Action to remove the vulnerability is advised.

- **High Risk (8-10)** - The vulnerability poses a real danger to the confidentiality, integrity, and/or availability, of McClure Industries' data or IT systems. Action should be taken immediately to remove this vulnerability.

Policies and Plans

No infrastructure related policies or plans currently exist for McClure Industries. The lack of complete and tested plans for responding to IT related events is a serious threat to the company's ability to continue IT operations. All recommended policies and plans should be tested frequently to ensure their accuracy and effectiveness. Listed below are some of the specific plans that do not exist, their respective risk level and SecureDogHosting's recommendations.

Incident Response Plan

McClure Industries does not have an incident response plan. An incident is defined as a breach in security, whether the breach occurs externally or from within the organization. The presence of an incident response plan will assist in the identification and containment of an incident. Without a plan in place containment may occur slowly and evidence may be lost or corrupted prior to areas of authority being properly assigned.

RISK LEVEL: 9 (High)

Recommendation: Create an incident response plan for McClure Industries. Should an incident occur steps and procedures will be available to an assigned incident response team. This will assist with the proper handling of data, containment procedures, recovery procedures, and how best to proceed with possible prosecution.

For more information regarding incident response procedures see the Reference section of this document.

Disaster Recovery Plan

McClure Industries does not have a disaster recovery plan. A disaster is defined as an event that considerably effects the IT posture of the company. This can include the loss of a system, loss of power, natural disaster, or any other event that may result in a diminished IT posture. The presence of a disaster recovery plan will lend structure to the overall IT posture and provide steps that should be taken in the event of a disaster.

RISK LEVEL: 9 (High)

Recommendation: Create a disaster recovery plan for McClure Industries. In the even of a disaster steps and procedures will be available to the recovery team members. This plan will assist in defining disaster criticality, assigning areas of responsibility to recovery team members, and reducing down time in the event of a disaster.

The disaster recovery plan should include areas of responsibility for disaster recovery team members, how usable hardware can be redistributed, the priority of services that must be re-established, a time-line of recovery events, and how to deal with the public (press, law enforcement authorities, etc.).

Backup Policy

McClure Industries does not have a backup policy. A backup policy is designed to assist system administrators on what to backup, how often to backup, and how backups are handled and stored. Having a backup policy in place will assist in ensuring that all necessary data is backed up in an accurate and timely fashion, are retained for a sufficient amount of time, and are accessible in a timely manner.

Backups are occurring at McClure Industries, however there is no policy in place to define the procedures on how backups are to be handled.

RISK LEVEL: 8 (High)

Recommendation: Create an effective backup policy for McClure Industries. Having accurate backups is a critical factor for every IT department. The backup policy should at a minimum contain steps and procedures on:

- what data is backed up
- how often data is backed up
- the type of backup (full, differential, etc.)
- how the backups are scheduled and verified
- how the backup media is handled and labeled
- how the backup media is stored
- how long the backup media is retained
- how backup media is rotated and expired
- how backup data is recovered

See the Reference section of this document for additional information.

System and Configuration Vulnerabilities

System and configuration vulnerabilities focuses on how systems are deployed within the assessed IT infrastructure. Correct system configuration is vital when considering the impact it has on the security stance of your company. There are many scripts and tools to assist an experienced system administrator with configuration issues. Some of the available tools will assist with the actual configuration of a system while others can test for configuration vulnerabilities on a particular system.

The items below list some of the most critical, from a vulnerability aspect, configuration issues present within McClure Industries. Also included will be an associated risk level and SecureDogHosting's recommendation.

Lack of Shadowed Passwords

Currently shadowed passwords are not being employed on the assessed servers at McClure Industries. Though there can be circumstances where shadowed passwords can not be employed there is no reason for shadow passwords not being employed at McClure Industries. The lack of shadowed passwords greatly increases the risk of brute force password cracking by such utilities as *crack*.

RISK LEVEL: 9 (High)

Recommendation: Employ shadowed passwords immediately. While there are some circumstances where shadowed passwords cannot be deployed, this is not true at McClure Industries. The Shadow Suite, which is freely available and included in most Linux distributions, also includes additional functionality that should be considered for deployment as well, including:

- utilities for adding, modifying, and deleting user accounts and groups
- password aging and expiration
- account expiration and locking
- shadowed group passwords

Refer to Appendix A for a current snap shot of the */etc/passwd* file and a listing of the */etc* file system on the McClure Industries machine. The snap shots illustrate the lack of shadowed passwords (and groups).

Not Configured by Role

The server that was assessed was not configured for its role within the enterprise. Running unnecessary services, having unnecessary user accounts, and the availability of unnecessary run levels greatly increases the possibility of vulnerable positions for a given machine. Only accounts, services, and run levels that are needed should be available for a machine's designated role. To increase the overall security and availability of a machine its role should be as singular in purpose as possible. For example, running sendmail on a web server is not necessary to serve web pages. Running sendmail on a web server does however create an additional service that may be vulnerable to compromise or a denial of service attack.

The machine assessed was to be strictly used as a web server, so additional processes, such as sendmail, ntalk, and talk are not required. Other services such as ftp may not be required depending on how data is transferred.

Too many accounts on the assessed machine are also still present. Accounts that no longer have a role on a given machine should be deleted or disabled. This will assist in account control and user accountability. It also decreases the probability of incorrectly configured users and excessive system permissions.

Run levels that are not needed for a specific role should also be removed. Only the bare set of run levels imaginable for a given role should be permitted.

Removing or disabling the above listed accounts, run levels, processes, and services not only creates a machine with less potential for vulnerability but also increases an administrator's ability to determine a potential compromise.

RISK LEVEL: 8 (High)

Recommendation: Decide what given machines will be responsible for serving (http, terminal, mail, etc.) and configure them to optimize their given role while decreasing the vulnerabilities associated with additional services. A server that is responsible for only serving mail requests does not need to have non-related additional services running such as telnet (replace this with SSH), or web services running. Disable or remove unnecessary services and related accounts from the server. Unnecessary run levels can also be removed.

To verify only required services are running perform a "ps -aux" to see what processes are running. Continue to remove processes, run levels, and accounts until only the minimal services run on a given system to perform its role.

Refer to Appendix B to view snap shots of excessive run levels, *inetd.conf*, and excessive processes for the role of the assessed machine.

Third-Party Software

The assessed machine at McClure Industries contains various forms of third-party software. Third-party software is defined as software that is not part of the operating system. Third-party software is not needed for the system to run but is normally needed to perform its assigned functions (e.g. web serving).

The assessed machine includes Apache, a well known and commonly deployed web server; Sendmail, also a well known piece of software that is commonly deployed for mail services; and Bind, which is a well known name server. Additional third-party software is also installed, but this assessment will primarily focus on Apache, Sendmail, and Bind.

Apache (www.apache.org) is the most widely deployed web server on the Internet and due to the role of the assessed machine a web server is required. Apache is very good about listing security problems, their respective patches, and links to CERT advisories in relation to Apache. However, running any public application, such as a web server does provide an avenue for potential attacks. Typical attacks on web servers are CGI script attacks and denial of service attacks.

Sendmail (www.sendmail.org) is the most widely deployed mail server on the Internet. Sendmail is also very good at citing current known security holes and information on them at their web site. Due to the role of the assessed machine Sendmail should be disabled or removed. Continuing to run Sendmail creates an additional avenue for potential attack. Sendmail is frequently being scrutinized for security and deployed properly can run in a very secure fashion. Typical Sendmail attacks are buffer-overflows and denial of service attacks.

Bind (http://www.isc.org/products/BIND/) is the mostly widely deployed name server on the Internet. ISC (the organization that is responsible for Bind) has a link on their web page to known vulnerabilities and associated patches. However, due to the role of the assessed machine Bind is not needed and should be disable or removed. As with Sendmail, continuing to run unnecessary

services provides an additional avenue for attack. Typical Bind attacks are buffer-overflows and denial of service attacks.

RISK LEVEL: 8 (High)

Recommendation: Remove unneeded third-party software (see "Not Configured by Role") and review upgrade to the most recent Apache distribution (1.3.12 as of this writing). Other web servers are also available on the market if Apache's performance or security stance do not meet McClure Industries needs.

Additional information can be found in the Reference section of this report.

Intrusion Detection and Vulnerability Scanning

McClure Industries does not currently have an intrusion detection system in place nor does it scan its infrastructure for vulnerabilities. Vulnerability scanning and intrusion detection play a vital role in maintaining a secure infrastructure. Without the ability to determine if a machine has been compromised it may stay in production for an extended period of time in a compromised state. Initial vulnerability scanning can be conducted prior to machines being put into production. Intrusion detection will aid in the ability to identify potential attacks or suspicious activity on the network.

RISK LEVEL: 7 (Medium)

Recommendation: Deploy an intrusion detection system and implement vulnerability scanning. Intrusion detections systems and vulnerability scanning software can be obtained free of cost (See Appendix C for a list of options). Also implement procedures and schedules when intrusion detection and vulnerability scanning should be conducted. Formal training in the areas of intrusion detection and vulnerability scanning may also greatly benefit McClure Industries' system administrators.

Physical Environment

The physical security of McClure Industries' IT department and data center are reasonable considering their expected threat level. Programmable crypto-locks are in place with sections having different door codes.

All systems are connected to commercial grade uninterruptible power supplies in the event of power surges or a power outage.

McClure Industries does not currently have in place an automated fire suppression system. Halon fire extinguishers are distributed throughout the data center but the data center is not manned during non-work hours. A fire during non-work hours could potentially destroy the entire data center.

RISK LEVEL: 6 (Medium)

Recommendation: Though programmable locks are currently being deployed they may not sophisticated enough. Consider more sophisticated locks that can be installed so that locks remain in the locked position during power outages and accesses can be logged for later review.

SecureDogHosting also recommends investing in a commercial grade fire suppression system in the event that a fire occurs during non-work hours. Though the chance of fire may be unlikely the result could be devastating and bring all IT functions to a stop.

Training

While most of the IT staff that was interviewed is very knowledgeable of general IT practices they have not been formally trained in IT security. IT security is difficult and dangerous to learn on the job. Training will assist administrators by giving them a more complete background on which to draw data.

RISK LEVEL: 5 (Medium)

Recommendation: Set up a formal training program to which McClure Industries can send its system administrators. An annual training budget line can be incorporated into the traditional IT budget to assist with cost control. SecureDogHosting recommends sending your key administrators to at least one training event per year to keep them current.

An example of a formal training event cost matrix is included in this document.

Conclusion

Security is a vital part of an IT infrastructure and should be considered an integral part of all business decisions. This assessment was an important first step in creating a more secure IT environment for McClure Industries.

McClure Industries is recommended to invest additional resources to increase its current level of security. Using this report as a guide will assist McClure Industries in adhering to common industry best practices.

The security policies that have been recommended in this document will create the foundation that McClure Industries' corporate security stance will be built. SecureDogHosting is available for additional assistance or periodic re-assessments if deemed necessary.

Prioritized List of Security Vulnerabilities and Issues

Though discussed throughout the report the following list displays security vulnerabilities and issues by level of risk.

- No Incident Response Policy
- No Disaster Recovery Policy
- No Backup Policy
- Lack of Shadowed Passwords
- Server Not Configured by Role
- Vulnerability of Third-Party Software
- No Intrusion Detection System or Vulnerability Scanning
- Lack of Fire Suppression System
- No formal training

Prioritized List of Recommended Courses of Action

Though outlined throughout the report the following list addresses recommended fixes for the most critical findings.

- Write and test an Incident Response Policy
- Write and test a Disaster Recovery Policy
- Write and test a Backup Policy
- Convert current password systems to shadowed passwords
- Reconfigure machines for only required accounts, services, run levels, and processes
- Remove third-party software that is not needed and upgrade the current version of Apache to 1.3.12 (as of this writing)
- Evaluate and deploy an Intrusion Detection System and implement policies for Vulnerability Scanning
- Purchase a commercial grade unattended fire suppression system
- Send system administrators to training courses

Cost Estimates Based on Recommended Courses of Action

- **Write and test an Incident Response Policy**

This task will be personnel based and will primarily involve research and writing.

Labor Category	Rate	Time	Total
Technical Writer	$60.00	40 hrs.	$2400
System Admin	$88.00	40 hrs.	$3520
CIO	$120.00	10 hrs.	$1200

Total Cost: $ 7120

- **Write and test a Disaster Recovery Policy**

This task will be personnel based and will primarily involve research and writing.

Labor Category	Rate	Time	Total
Technical Writer	$60.00	40 hrs.	$2400
System Admin	$88.00	40 hrs.	$3520
CIO	$120.00	10 hrs.	$1200

Total Cost: $ 7120

- **Write and test a Backup Policy**

This task will be personnel based and will primarily involve research, writing, and configuration.

Labor Category	Rate	Time	Total
Technical Writer	$60.00	40 hrs.	$2400
System Admin	$88.00	40 hrs.	$3520
CIO	$120.00	10 hrs.	$1200

Total Cost: $ 7120

- **Convert current password systems to shadowed passwords**

This task will be personnel based and will primarily involve configuration and testing.

Labor Category	Rate	Time	Total
System Admin	$88.00	10 hrs.	$880

Total Cost: $ 880

- **Reconfigure machines for only required accounts, services, run levels, and processes**

This task will be personnel based and will primarily involve configuration and testing.

Labor Category	Rate	Time	Total
System Admin	$88.00	30 hrs.	$2640

Total Cost: $ 2640

- **Remove third-party software that is not needed and upgrade the current version of Apache to 1.3.12 (as of this writing)**

This task will be personnel based and will primarily involve configuration and testing.

Labor Category	Rate	Time	Total
System Admin	$88.00	30 hrs.	$2640

Total Cost: $ 2640

- **Evaluate and deploy an Intrusion Detection System and implement policies for Vulnerability Scanning**

This task will be personnel based and will primarily involve research, configuration, and testing.

Labor Category	Rate	Time	Total
System Admin	$88.00	160 hrs.	$14080
CIO	$120.00	20 hrs.	$2400

Total Cost: $16,480

- **Purchase a commercial grade unattended fire suppression system**

This task will be personnel and equipment based and will primarily involve research, installation, and testing.

Labor Category	Rate	Time	Total
System Admin	$88.00	80 hrs.	$7040
CIO	$120.00	80 hrs.	$9600
Suppression Sys.	$130,000	00 hrs.	$130,000

Total Cost: $146,640

- **Send system administrators to training courses**

Direct Costs	Total
Formal Training (SANS UNIX Track 6)	$2795
Hotel Stay (6 days @ $172.00)	$1032
Meals (6 days @ $48.00 (per diem rate)	$288
Rental Car (6 days @ $45.00)	$270

Total Cost: $ 4385

Approximate Total Cost to Implement All Recommendations: $ 195,025

Appendixes

Appendix A

Snap shot of /etc/passwd: (too many accounts and no shadow passwd)

```
[root@machine /root]# cat /etc/passwd |less
root:mSeuQKrEOa4LI:0:0:root:/root:/bin/bash
bin:*:1:1:bin:/bin:
daemon:*:2:2:daemon:/sbin:
adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd:
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:
news:*:9:13:news:/var/spool/news:
uucp:*:10:14:uucp:/var/spool/uucp:
operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games:
gopher:*:13:30:gopher:/usr/lib/gopher-data:
ftp:*:14:50:FTP User:/home/ftp:
nobody:*:99:99:Nobody:/:
xfs:!!:100:101:X Font Server:/etc/X11/fs:/bin/false
postgres:!!:40:233:PostgreSQL Server:/var/lib/pgsql:/bin/bash
machine:$1$anKnniJT$B3x4PhaeF68S/AZb/OXAq0:500:500:Default
Account:/home/machine:/bin/bash
industry:$1$WYAY75q6$/21EJ3T4kTt8HX5ToNRau0:501:501::/home/industry:/bi
n/bash
```

Snap shot of /etc: (lack of shadow passwords and shadow groups)

```
...
-rw-r--r--   1 root     root          449 May 30 11:18 group
...
-rw-r--r--   1 root     root           66 Jul 29 11:53 issue
-rw-r--r--   1 root     root           65 Jul 29 11:53 issue.net
...
-rw-r--r--   1 root     root            0 Jul  6  1995 motd
...
-rw-r--r--   1 root     root          803 May 30 11:18 passwd
...
-rw-r--r--   1 root     root           55 Feb 25 02:26 shells
```

Appendix B

Snap shot of rc3.d: (not configured for server role; too many services)

```
[root@machine rc3.d]# ls /etc/rc.d/rc3.d/
K05innd       K34yppasswdd  K84ypserv   S25netfs     S55sshd     S90xfs
K10pulse      K35smb        S05kudzu    S30syslog    S60lpd      S99linuxconf
K20nfs        K45named      S10network  S40atd       S75keytable S99local
K20rstatd     K50snmpd      S11portmap  S40crond     S80sendmail
K20rusersd    K55routed     S16apmd     S45pcmcia    S85gpm
K20rwhod      K60mars-nwe   S20random   S50inet      S85httpd
[root@machine rc3.d]#
```

Snap shot of /etc/inetd.conf: (not customized for server role; too many services)

```
[root@machine /root]# cat /etc/inetd.conf |less
#
# inetd.conf    This file describes the services that will be available
#               through the INETD TCP/IP super server.  To re-configure
#               the running INETD process, edit this file, then send the
#               INETD process a SIGHUP signal.
#
# Version:      @(#)/etc/inetd.conf     3.10    05/27/93
#
# Authors:      Original taken from BSD UNIX 4.3/TAHOE.
#               Fred N. van Kempen, <waltje@uwalt.nl.mugnet.org>
#
# Modified for Debian Linux by Ian A. Murdock <imurdock@shell.portal.com>
#
# Modified for RHS Linux by Marc Ewing <marc@redhat.com>
#
# <service_name> <sock_type> <proto> <flags> <user> <server_path> <args>
#
# Echo, discard, daytime, and chargen are used primarily for testing.
#
# To re-read this file after changes, just do a 'killall -HUP inetd'
#
#echo   stream  tcp     nowait  root    internal
#echo   dgram   udp     wait    root    internal
#discard        stream  tcp     nowait  root    internal
```

```
#discard        dgram   udp     wait    root    internal
#daytime        stream  tcp     nowait  root    internal
#daytime        dgram   udp     wait    root    internal
#chargen        stream  tcp     nowait  root    internal
#chargen        dgram   udp     wait    root    internal
#time   stream  tcp     nowait  root    internal
#time   dgram   udp     wait    root    internal
#
# These are standard services.
#
ftp     stream  tcp     nowait  root    /usr/sbin/tcpd  in.ftpd -l -a
telnet  stream  tcp     nowait  root    /usr/sbin/tcpd  in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
shell   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rshd
login   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rlogind
#exec   stream  tcp     nowait  root    /usr/sbin/tcpd  in.rexecd
#comsat dgram   udp     wait    root    /usr/sbin/tcpd  in.comsat
talk    dgram   udp     wait    nobody.tty      /usr/sbin/tcpd  in.talkd
ntalk   dgram   udp     wait    nobody.tty      /usr/sbin/tcpd  in.ntalkd
#dtalk  stream  tcp     wait    nobody.tty      /usr/sbin/tcpd  in.dtalkd
#
# Pop and imap mail services et al
#
#pop-2  stream  tcp     nowait  root    /usr/sbin/tcpd ipop2d
#pop-3  stream  tcp     nowait  root    /usr/sbin/tcpd ipop3d
#imap   stream  tcp     nowait  root    /usr/sbin/tcpd imapd
#
# The Internet UUCP service.
#
#uucp   stream  tcp     nowait  uucp    /usr/sbin/tcpd  /usr/lib/uucp/uucico     -l
#
# Tftp service is provided primarily for booting.  Most sites
# run this only on machines acting as "boot servers." Do not uncomment
# this unless you *need* it.
#
#tftp   dgram   udp     wait    root    /usr/sbin/tcpd  in.tftpd
#bootps dgram   udp     wait    root    /usr/sbin/tcpd  bootpd
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers."  Many sites choose to disable
```

```
# some or all of these services to improve security.
#
finger  stream  tcp     nowait  nobody  /usr/sbin/tcpd  in.fingerd
#cfinger stream tcp     nowait  root    /usr/sbin/tcpd  in.cfingerd
#systat stream  tcp     nowait  guest   /usr/sbin/tcpd  /bin/ps -auwwx
#netstat        stream  tcp     nowait  guest   /usr/sbin/tcpd  /bin/netstat    -f in
et
#
# Authentication
#
auth    stream  tcp     wait    root    /usr/sbin/in.identd in.identd -e -o
#
# End of inetd.conf
linuxconf stream tcp wait root /bin/linuxconf linuxconf --http
#swat       stream  tcp     nowait.400      root /usr/sbin/swat swat
```

Snap shot of /etc/rc.d: (not customized for server role; too many run levels)

```
[root@machine /root]# ls -al /etc/rc.d/
total 33
drwxr-xr-x  10 root     root         1024 Mar 10 08:08 .
drwxr-xr-x  31 root     root         3072 Jul 30 11:18 ..
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 init.d
-rwxr-xr-x   1 root     root         2889 Nov  8  1999 rc
-rwxr-xr-x   1 root     root          933 Sep 30  1999 rc.local
-r-xr-x---   1 news     news         2964 Aug 30  1999 rc.news
-rwxr-xr-x   1 root     root        13049 Nov 30  1999 rc.sysinit
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 rc0.d
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 rc1.d
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 rc2.d
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 rc3.d
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 rc4.d
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 rc5.d
drwxr-xr-x   2 root     root         1024 Mar 16 10:47 rc6.d
[root@machine /root]#
```

Running processes: (not customized for server role; too many processes)

```
[root@machine /root]# ps -aux
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME
COMMAND
root         1  0.0  0.1  1104  368 ?        S    Jul29   0:04 init [3]
root         2  0.0  0.0     0    0 ?        SW   Jul29   0:00 [kflushd]
root         3  0.0  0.0     0    0 ?        SW   Jul29   0:00 [kupdate]
root         4  0.0  0.0     0    0 ?        SW   Jul29   0:00 [kpiod]
root         5  0.0  0.0     0    0 ?        SW   Jul29   0:00 [kswapd]
root         6  0.0  0.0     0    0 ?        SW<  Jul29   0:00 [mdrecoveryd]
bin        320  0.0  0.1  1196  396 ?        S    Jul29   0:00 portmap
root       336  0.0  0.1  1088  464 ?        S    Jul29   0:00 /usr/sbin/apmd -p
root       389  0.0  0.2  1152  560 ?        S    Jul29   0:00 syslogd -m 0
root       400  0.0  0.2  1412  752 ?        S    Jul29   0:00 klogd
daemon     416  0.0  0.1  1128  484 ?        S    Jul29   0:00 /usr/sbin/atd
root       432  0.0  0.2  1304  600 ?        S    Jul29   0:00 crond
root       452  0.0  0.1  1124  484 ?        S    Jul29   0:00 inetd
root       479  0.0  0.1  1176  500 ?        S    Jul29   0:00 lpd
root       508  0.0  0.4  2104 1108 ?        S    Jul29   0:00 sendmail: accepti
root       525  0.0  0.1  1144  476 ?        S    Jul29   0:00 gpm -t ps/2
root       541  0.0  0.5  2560 1316 ?        S    Jul29   0:00 httpd
xfs        568  0.0  0.3  1880  964 ?        S    Jul29   0:00 xfs -droppriv -da
root       607  0.0  0.1  1076  384 tty1     S    Jul29   0:00 /sbin/mingetty tt
root       608  0.0  0.1  1076  384 tty2     S    Jul29   0:00 /sbin/mingetty tt
root       609  0.0  0.1  1076  384 tty3     S    Jul29   0:00 /sbin/mingetty tt
root       610  0.0  0.1  1076  384 tty4     S    Jul29   0:00 /sbin/mingetty tt
root       611  0.0  0.1  1076  384 tty5     S    Jul29   0:00 /sbin/mingetty tt
root       612  0.0  0.1  1076  384 tty6     S    Jul29   0:00 /sbin/mingetty tt
nobody    1001  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1002  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1003  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1004  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1005  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1006  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1007  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1008  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1009  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
nobody    1010  0.0  0.5  2748 1428 ?        S    04:02   0:00 httpd
root      1444  0.0  0.3  1704  876 ?        S    11:24   0:00 in.telnetd
root      1445  0.0  0.4  2292 1200 pts/0    S    11:24   0:00 login -- machine
machine   1446  0.0  0.3  1724  956 pts/0    S    11:25   0:00 -bash
```

```
root     1457  0.0  0.4  2060 1060 pts/0    S    11:25   0:00 su
root     1459  0.0  0.3  1752  992 pts/0    S    11:25   0:00 bash
root     1484  0.0  0.3  2676  964 pts/0    R    11:35   0:00 ps -aux
root     1485  0.0  0.3  1752  992 pts/0    R    11:35   0:00 bash
```

Appendix C

Intrusion Detection Systems

Internet Security Systems (www.iss.net)
Snort (www.snort.org)

System Vulnerability and Integrity Tools

COPS (ftp://coast.cs.purdue.edu/pub/tools/unix/cops)
Tiger (ftp://net.tamu.edu/ftp/security/TAMU)
Tripwire (ftp://coast.cs.purdue.edu/pub/tools/unix/Tripwire)
SATAN (ftp://ftp.porcupine.org/pub/security)
Nessus (www.nessus.org)

Sample Nessus Scan Results:

Number of hosts which were alive during the test : 1
Number of security holes found : 0
Number of security warnings found : 0
Number of security notes found : 1

List of the tested hosts :

- 10.0.0.333 (Security notes found)

[Back to the top]

10.0.0.333 :

List of open ports :

- general/udp (Security notes found)

[back to the list of ports]

Information found on port general/udp

For your information, here is the traceroute to 216.88.27.43 :
10.0.0.1
10.0.0.333

This file was generated by Nessus, the open-sourced security scanner.

References

Albitz, Paul and Liu Cricket, DNS and BIND, Cambridge: O'Reilly & Associates, Inc., 1998.

Costales, Bryan and Allman Eric. sendmail. Cambridge: O'Reilly & Associates, Inc., 1997.

"IDM - Apache: The Definitive Guide, 2nd Edition: Chapter 13 Security." Chapater Excerpt From: Apache: The Definitive Guide, 2nd Edition. <http://idm.internet.com/articles/200005/apachndex.html> (1 August 2000).

"Internet Software Consortium - BIND." ISC BIND. <http://www.isc.org/products/BIND/> (1 August 2000).

Preston, W. Curtis. Unix Backup & Recovery. Cambridge: O'Reilly & Associates, Inc., 1999.

"rfc2196." Site Security Handbook. <ftp://ftp.isi.edu/in-notes/rfc2196.txt> (1 August 2000).

"Sendmail Home Page." Welcome to Sendmail. <http://www.sendmail.org> (1 August 2000).

"The Apache Software Foundation." The Apache Software Foundation. < http://www.apache.org/ > (1 August 2000).

Last Updated: May 28th, 2017

Upcoming Training

SANS London July 2017	**London, United Kingdom**	**Jul 03, 2017 - Jul 08, 2017**	**Live Event**
SANSFIRE 2017	**Washington, DC**	**Jul 22, 2017 - Jul 29, 2017**	**Live Event**
SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**