



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Securing Linux/Unix (Security 506)"  
at <http://www.giac.org/registration/gcux>

**Network Security Assessment  
Performed for Singing Beagle Productions  
By Melete Security Association**

22 November, 2000

Joseph Purvis,  
Principal Security Engineer

© SANS Institute 2000 - 2002. Author retains full rights.

## **Executive Summary:**

At the request of the customer, Singing Beagle Productions ("SB" or "the customer" hereafter), an internal audit was conducted of a single server, identified by the customer as their single most critical information asset and single greatest point of exposure to external network traffic. This was done as a proof-of-concept audit, meant to determine whether further auditing of corporate resources would be required.

The host known as "kumo.singingbeagle.org" (172.16.2.1) was examined thoroughly by a security engineer, Joseph Purvis, on 17 through 20 November, 2000. Thorough network scans and assessments were performed from the same network segment as the host (to assess actual security), and scans were performed through the firewall to assess the security of the firewall protection. The engineer also performed a host-based assessment to examine the operating system's configuration and overall security, and conducted interviews with key systems administration personnel to assess policies and procedures governing the day-to-day administration of the host.

When initially installed, some steps appear to have been taken to secure the host for public access, however such steps were insufficient even at the time; since no little to no ongoing maintenance has been provided for the host since then, the once "not-quite-secure" configuration has slipped entirely to a dangerously insecure configuration. Although the risk of compromise is mitigated by the firewalling and network address translation provided, the services available through the firewall would provide a determined attacker with a basic toolkit sufficient to compromise the server and gain access to the internal network.

**In the short term, therefore, it is the recommendation of the engineer and Melete that the host be replaced as soon as possible;** preferably, the host should be immediately decommissioned and rebuilt from scratch or replaced with a different server which has been thoroughly hardened by trained professionals. If the host cannot be decommissioned due to the criticality of applications running on it, a replacement host should be built as soon as possible, and the current host should be secured as best as time and resources will allow.

In the longer term, while the security knowledge of staff is deemed more than sufficient in general, Unix-specific security training should be provided for any staff responsible for maintaining the host. In addition, the development of clear policies and procedures for providing maintenance, upgrades, and monitoring of the host must be developed as soon as possible, and staff members must be given clear-cut lists of tasks and responsibilities to guarantee that necessary maintenance is performed in a timely and accurate manner. A set of configuration and deployment guidelines, written with security as a foremost goal, must be developed as soon as possible to govern the deployment of future hosts: some good guides for getting started with this are provided in Appendix A.

As for the possibility of further auditing, the engineer and Melete certainly would recommend it, whether conducted internally by the customer or by Melete. The problems uncovered here are sufficient to warrant investigation of the entire enterprise to examine larger issues of policy and procedure as well as examining other hosts:

many issues of policy have not been focused on as significantly here because the scope of the investigation was directed solely at a single host.

The rest of this document will provide a more in-depth discussion of each of these points, including tools and methods used to gather data; an analysis of the vulnerabilities discovered, organized by category and priority/risk level; conclusions drawn from the data received, and specific recommendations for improving the security of the system, including a rough costs estimate for implementing such recommendations.

© SANS Institute 2000 - 2002, Author retains full rights

## Detailed Findings and Analysis

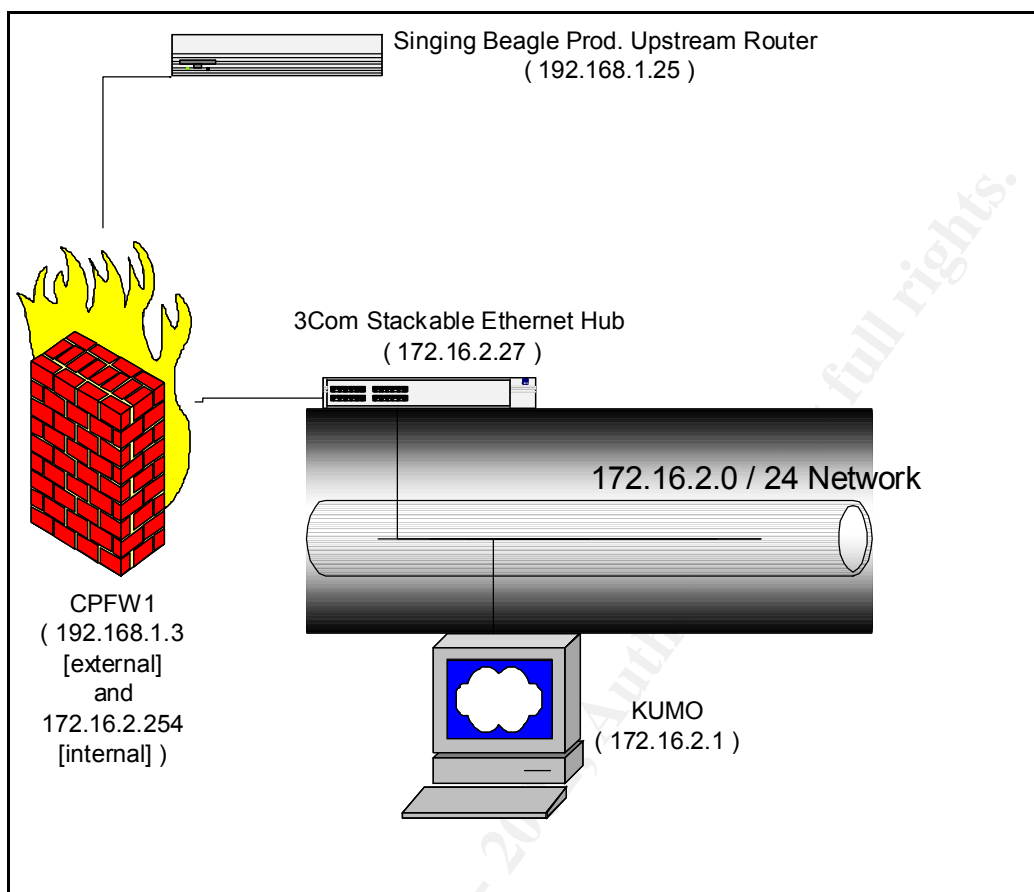
Background: With the recent shift in internal staffing and a significant turnover of staff to a competitor, the management team at Singing Beagle Productions requested Melete Security Association to conduct an audit to define the company's current information security posture, and determine whether it required shoring up in any areas.

In order to determine initial areas requiring further focus, a single server was identified for a "proof of concept" audit: the server "kumo.singingbeagle.org" (172.16.2.1) was identified as the company's single greatest information security asset and the single point of greatest exposure to external network traffic on the company's network.

The host chosen, a Sun Ultra/1 running Solaris version 2.6, serves as the primary webserver for the company, including a support center for tracking trouble tickets regarding the company's products, an information distribution center for releasing new information about company products, and an FTP server to offer patches and upgrades for products sold and resold by the firm. The server sits on a DMZ (172.16.2.0 / 24) with several other corporate servers, including the company email server and an internal webserver; connectivity to the outside world is offered through a Check Point firewall in front of the network, performing Network Address Translation (NAT) to statically-defined external addresses. This means that customers connecting to the webserver do so through the firewall, but talk directly to the webserver: only the source and destination addresses of packets are altered in the course of a network transaction--no content is changed or scanned.

The following diagram is offered to illustrate the placement of the host assessed relative to the network on which it is installed.

© SANS Institute 2000 - 2002



**Conventions:** Within this document, a number of typographical conventions have been employed to ensure differentiation of instructions and clarity of meaning. Instructions provided in *regular-weight monospaced font* are commands to be performed on a Unix host, or listings of files on a Unix host; in large blocks or scripts such instructions will be interspersed with annotations from the engineer, provided in *italic monospaced font*.

In addition, to ensure the safety of the Singing Beagle Productions network and the hosts mentioned herein, certain steps have been taken to sanitize the data presented. In particular, certain network numbers have been replaced: while the internal network (172.16.2.0 / 24) remains the same, the initial three octets of external network addresses have been edited as if the host actually were on the 192.168.X.X network. Thus, a host which might actually possess the address 1.2.3.4 would be noted herein as 192.168.3.4. In addition, usernames and GECOS entries have been replaced with sanitized values to protect the identity of users, although the UIDs and GIDs have not been cleaned, to allow the customer to back trace information presented to the actual files resident on the hosts in question.

Endnotes have been employed throughout, and can be found before the appendices at the end of the document; any questions regarding the information offered herein or the presentation thereof may be referred by email to [auditor@melete.org](mailto:auditor@melete.org).

### **Auditing Methodology:**

## I. General Methodology

Inspection of the host was conducted in three phases. Phase one consisted of network port sweeps and vulnerability scans, performed using a variety of publicly-available tools to assess which network services were running on the host, how much information could be gained from those services, and what vulnerabilities the daemons themselves or the services they offer might present to the host. This portion of the assessment was carried out from a laptop installed on the same network segment as the target host, in order to examine the security of the host itself. A scan of the host through the firewall, performed from the external network segment, was also conducted, to assess what services the firewall would allow through to the host.

The second phase of the assessment was host-based: the engineer was granted an unprivileged account and the root password to the host, which he used to login to the host from the internal network segment. Once logged in, the engineer accessed the root account and performed a thorough assessment of the host's configuration, including operating system version and patch level, daemons running and their configuration, and a limited assessment of the webserver running on the host. This was done both to examine the general security of the host's configuration and to verify that the host's setup matched its profile on the network: no ports were open from the network that did not appear open from the host, configuration files matched the actual behavior of the daemons they governed and so forth, as disjuncts between the two profiles might present evidence that a system compromise had occurred.

Finally, once the inspections of the host itself had concluded, the engineer conducted an inspection of the host's environment, including network layout, physical security measures, and interviews with systems administration personnel responsible for the server, to examine policies and procedures.

## II. Tools Employed

### a. Phase One: Network Security

Tools employed during this phase were publicly-available, open-source security scanners run from a Linux platform. A list of websites for downloading and obtaining more information about these tools is provided in Appendix B.

- i. Nmap: nmap is a port scanner, used for obtaining a list of open ports on a target system. Scans performed obtained complete lists of open TCP and UDP ports (i.e. covering the complete range of port numbers from 1 to 65535), and connected to the RPC portmapper server and Ident daemon on the host to gather additional information about any open ports discovered. Additional plugins were utilized which obtained banners<sup>1</sup> from well-known services, reporting the banners for FTP, HTTP, SMTP, SSH and SunRPC services. In addition to standard full-connect TCP scanning (completing the SYN-SYN/ACK-ACK handshake and then tearing down the connection with FIN packets), a "half-open" TCP scan was performed (sending a SYN, receiving a SYN/ACK on an open port, and tearing down

the connection immediately with a RST), both to ensure that the lists of open ports were the same and for later correlation against system logs to examine how much activity was successfully logged.

- ii. Nessus: To quote the website of the Nessus project, "The 'Nessus' Project aims to provide to the internet community a free, powerful, up-to-date and easy to use remote security scanner." Utilizing a built-in database of several hundred (543 at last count) known vulnerabilities, it performs a series of scans and attacks against the target host to see which attacks succeed, producing at the end a report of attacks to which the host is vulnerable. Since the target host is a production server identified as a critical asset, the most dangerous attacks, designed to verify the vulnerability of the host to a variety of denial of service attacks, were disabled to prevent loss of service.
- iii. SAINT: Like Nessus, SAINT (System Administrator's Integrated Network Tool, according to its creators) is a network-based vulnerability scanner, descended from the popular SATAN network scanning tool. Although its database of known vulnerabilities is smaller than that of Nessus, it is broader, and covers specific, high-risk vulnerabilities (such as the SANS "Top Ten Internet Security Vulnerabilities") that can pose grave risk to a host. In addition, the reports generated by SAINT can be easier to comprehend, and the practice of running multiple vulnerability scanners can serve as a cross-check for vulnerabilities identified, as well as providing additional sources of information.
- iv. Whisker and Malice: Since the customer identified the server in question as offering web services as part of its function, a pair of webserver vulnerability scanners were utilized to check for obvious risks. Whisker, written by rain forest puppy [sic], is a Perl-based scanner that employs a database of known webserver holes to scan a host, focusing on CGI vulnerabilities, and offers command-line switches to avoid Intrusion Detection Systems<sup>ii</sup>; Malice, authored by Natas, is similarly Perl-based but utilizes a larger database of both CGI and webserver configuration vulnerabilities.

b. Phase Two: Host Security

Assessing the security of a host from the "inside" (i.e. by directly logging in to it) poses a significant challenge to the responsible assessor. In order to obtain a clear picture of the operating environment of the host, the auditor must treat the host like a crime scene and disturb it as little as possible while observing and examining it: changes to the host will make it difficult to impossible to clearly define the state of the host's security, since it will be unclear what effect the auditor's changes have made to the host. Any changes which are made to the host's environment (and some, such as log entries, are inevitable), must be carefully noted, for liability's sake, if nothing else. Proceeding with that in mind, all login sessions on the host were performed utilizing the "script" program, which spawns a subshell and logs all



data printed to the screen during that shell session to a text file. This meant that any commands issued by the auditor could be allowed to print their output directly to the screen instead of being redirected to a file to be pushed back to the auditor's machine later, following the same principle of creating as little new data on the host as possible. In addition, the tools and programs used in this phase of the assessment were only those which existed on the host prior to examination: no new data was transferred to the host during the assessment. The list of commands below is truncated to include the most significant commands issued: a complete log of all sessions on the host can be found in Appendix C, "Raw Data".

- i. ``ps -elf``: Lists all running processes on the host
- ii. ``uname -a``: Prints the OS version and physical architecture of the machine
- iii. ``eeprom security-mode``: Reports the current settings for the password-protection feature of the Sparc hardware PROM.
- iv. ``last``: Prints a list of all the users who logged into the machine through remote login utilities such as ssh, telnet or rsh, on the physical console or through ftp
- v. ``netstat -a``: Reports the list of network ports in "listening" state (i.e. a daemon has bound to that port to offer a network service) and the list of established network connections, including TCP and UDP connections as well as local Unix domain sockets.
- vi. ``rpcinfo -p``: Lists information about RPC (Remote Procedure Call) daemons running and the ports to which they are bound.
- vii. ``showrev -a``: Prints out basic information about the host, including OS version, architecture version, and a list of patches to the OS installed, if any.
- viii. ``dmesg``: Prints the list of output produced by the system's last boot; performed principally to look for reported errors or misconfigurations.
- ix. ``pkginfo``: Prints out the list of software packages installed using Solaris' built-in software package system. This would not catch any software installed by hand-compiling it, such as the Apache webserver, but would catch software such as Check Point's firewall software, or the OpenWindows suite of graphical interface software.
- x. A large number of files were opened and their contents printed using the ``cat`` utility; these included a significant portion of the boot scripts and configuration files in `/etc`, as well as various other configuration and log files scattered throughout the filesystem.

c. Phase III: Environmental and Systemic Inspection

The "tools" used for this portion of the assessment were far more abstract. An inspection of the server room in which the host resides was carried out, followed by interviews with the administrators identified by the customer as responsible for the upkeep on the server. Although legal constraints prevent the inclusion of a verbatim transcript of these interviews, the list below

should serve as a guide to what was inspected; a checklist, completed by the auditor during the interview, provides the data examined for each point.

- i. Physical Security:
  1. Does the server reside in a server room with a generally clean (uncluttered, organized) and stable, climate-controlled environment, with temperature and humidity kept at constant, controlled levels?
  2. Is access to the server room limited to a known number of people, and controlled through the use of a cipher-lock or badge reader at all access points?
  3. Is there a computer-safe fire suppression system in place such as Halon-2 or similar systems?
  4. Is the server stored securely in a rack and not stacked on a shelf underneath other units?
  5. Is the server's CPU kept in a locked cabinet to control access to removable media drives?
- ii. Systems Administrators: What is the overall level of Unix knowledge among those responsible for the administration of the server? What is their level of security knowledge? What are their specific responsibilities with regards to the host, and are those personally-developed or handed to them from company policy and standard procedure?
- iii. Host Knowledge: Are the administrators able to list the services which should be/are running on the box without logging in to look? Is there a document stating the host's function made available and kept up to date? Is there an installation and configuration history document kept by the systems administrators to record changes to the host? What is the administrator's general impression of the security level and overall configuration of the host?

### **Analysis of Vulnerability:**

#### **I. Operating System Vulnerabilities**

- a. Unnecessary Software Installed: When building and installing a host which will act as a server, it is important to define the list of functions that host will perform, and then install only the software required to perform those functions. Installing additional software only offers attackers greater opportunity for mischief, and leads to greater administrative workload trying to keep all software on the server patched up to date, as the list of things to patch is proportionally longer. The simplest solution is to start from the basic set of packages, defined as the "Core Utilities", and install other packages on top of that as they are needed (some packages can and should be removed from Core Utilities as well on servers requiring higher levels of security, such as firewalls).

The list of packages installed on Kumo is extensive, and includes a number of software packages which are unnecessary. If the host is to stay in service as it is for any length of time, Melete would strongly recommend the removal of the following groups of packages post-haste if

they are not performing integral functions on the server:

[It is important to note that this is only a partial list, which includes many packages with known vulnerabilities. The customer is strongly urged to review the list of packages installed manually (using the "pkginfo" command) and uninstall any which do not meet the list of approved functions for the server. An entry followed by an asterisk (\*) denotes a group of packages which match that expression.]

NSCPNav (Netscape Navigator)	SUNWdt* (CDE packages)
SUNWeu* (European locales for CDE)	SUNWi*of and SUNWi*rf (X11 fonts)
SUNWjv* (Java packages)	SUNWol* (OpenLook packages)
SUNWpcelx, SUNWpcm*, SUNWpcser (PCMCIA drivers)	SUNWplow* (OpenWindows Locales)
SUNWpm* (Power Management)	SUNWtltk* (ToolTalk)
SUNWxw* (X-Windows packages)	SUNWypr and SUNWypu (NIS packages)

- b. **Operating System Version:** Although running the very latest version of an operating system can pose as many or more problems as a well-supported, slightly older revision, it is important to develop a policy for reviewing new releases and gradually moving older servers up to them or replacing them with units running newer versions. Newer versions of an OS can provide new security and auditing tools, fixes for problems in previous releases, and so forth; Melete recommends in general that customers stay no more than one major revision behind their software vendor, to avoid being caught by end-of-lifecycle problems and forced into premature upgrades.

While Solaris 2.6 continues to be supported by Sun, two major revisions of Solaris (7 and 8) have since been released and are in production in many facilities. Kumo continues to run version 2.6, and given the nonexistent list of patches installed (cf. "Security Patches" section below), is likely running an early version as well. The customer is strongly encouraged either to look at replacing Kumo with a new server running a fully-patched version of Solaris 7 or to schedule a time to upgrade Kumo at least to version 7; in addition, steps should be taken to begin reviewing Solaris 8 to see if it will meet the customer's needs, and testing it in a lab to make sure it will function as the customer requires.

## II. Configuration Vulnerabilities

- a. **Sparc PROM Access Control:** The Sparc platform for Solaris offers a command-line interactive PROM, used to configure hardware and select boot devices. The PROM offers three security levels, 'full', in which a password is required to be typed on the console in order to boot, reboot or reconfigure the machine through the PROM; 'command', in which the system will boot and reboot without prompting for the password, but will require the password for booting off of alternate media or using the

interactive PROM environment; and 'none', in which no password is required for any action. 'Command' mode is the recommended setting, which allows hosts to reboot unattended in emergencies, but keeps an attacker with console access from booting the system off of alternate media.

Currently, the PROM security mode is set to 'none', which means a determined attacker can boot the system off of alternate media, alter hardware settings and boot devices, and even render the host useless by changing the PROM password to an unknown setting and rebooting the machine. Since the PROM password and security mode can be set while the machine is booted (using the 'eeprom' command), this poses a significant risk to the system. The customer is urged to determine a PROM password for the system, set the password and security-mode, and consider disabling the 'eeprom' command on the host by removing or altering the permissions on it.

- b. ToolTalk Database Server (rpc.ttdbserver): The ToolTalk database server, activated by default on Solaris, contains a known buffer overflow for which exploits have been widely distributed. On any secure system, it is generally an unwise idea to run any sort of RPC service at all; this service should be patched regardless, and either deactivated or very carefully monitored and firewalled.

This service was found running on Kumo, and has a widely-known and recently-publicized exploit. The customer is strongly urged to apply the latest patch cluster for Solaris, or, if a single fix is needed, to apply the appropriate Sun patch to fix the exploit (105802), available from <http://sunsolve.sun.com>. To disable the service entirely, edit the /etc/inetd.conf file, and insert a # at the beginning of the line which begins "100083/1 tli rpc/tcp", then restart the inetd server by obtaining its PID ("ps -elf | grep inetd") and issuing a "kill -HUP <PID>" as root.

- c. Direct Root Login: Many Unix systems offer the ability for users to login to the system directly as root from the network. Although Solaris does not offer this feature by default, it can be activated; Melete strongly recommends that it be left deactivated, and that users be actively prevented from logging in over the network, being forced instead to login as an unprivileged user and use a utility such as the built-in 'su' program to access the root account. Allowing direct root logins over the network allows an attacker a single point on which to concentrate her efforts: she need only break or guess the password for the root account, and she has gained access to the system, without needing to guess the username or the password of any unprivileged accounts. From a practical standpoint as well, forcing users to login with their own account first lends a measure of change control and auditing to the system, since any disastrous change can likely be back-traced to the user who executed 'su' last, simply by

reading the system logs.

Although Kumo has been configured not to allow direct root logins over ssh, root is still allowed to connect to the system through ftp, which would enable an attacker with the root password to alter files on the system, upload new files, and so forth. The customer is strongly urged to create an /etc/ftpusers file: any account names placed in this file will be prevented from logging in via FTP. It should contain "root", plus the names of any disabled or non-interactive accounts on the system, such as bin, dev, lp, and so forth.

- d. TCP Wrappers: The TCP Wrappers package, authored by Wietse Venema, provides an additional layer of auditing and sanity checking for software such as telnet or ftp (TCP-based connection software). It offers granular access controls by IP address, and significant audit trails of what IPs connected to a server when and with what service, offering systems administrators a greater degree of security, especially when running services such as a public FTP server. This software is not installed by default on Solaris, but must be compiled on a secure system and distributed to servers, which must then have the /etc/inetd.conf file modified to use it.

This package was not installed on Kumo, and definitely should be. Without it, administrators have no way to block out known wrongdoers, and a significantly reduced degree of auditing of FTP and login sessions. To install, download the software (URL is given in Appendix B) to a secure, non-production server, and compile it. Copy the resulting binaries to the production server, and then edit the /etc/inet/inetd.conf file to use the new "tcpd" server instead of any services, so a line that originally read

```
ftp stream tcp nowait root /usr/sbin/in.ftpd in.ftpd  
-l -a
```

would now read

```
ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l  
-a
```

- e. Logging of Failed Logins: Although by default, Solaris' syslog configuration will log failed logins, the log to which it should write this information (/var/adm/loginlog) is not created by default, and so it will throw away information about failed logins with creating an audit trail. Creating such an audit trail is an integral part of a responsible system security policy, since without it, an attacker can attempt to break logins and passwords by brute-force without the systems administrators being aware of his activities.

The necessary logfile for auditing failed logins on Solaris did not exist on Kumo, and the customer is strongly advised to create it and set it up in the log rotation scheme as soon as possible. To create the file, execute the following commands as root:

```
/bin/touch /var/adm/loginlog
```

```
/bin/chown root:sys /var/adm/loginlog
/bin/chmod 0600 /var/adm/loginlog
```

- f. **Log Review:** The most valuable tool an administrator has in keeping her system secure is the system logs, which inform her of what connections were made, which users logged in, and so forth. It is vital to the security of a server that these logs be reviewed by hand periodically to search for anomalies; there is a wide variety of software available such as swatch or logcheck (URLs for both are in Appendix B) which will gather up logs and help sort out information before mailing the rest to systems admins for review.

Although webserver logs from Kumo are being parsed daily by a script and mailed to administrators, the system logs are not. This means that no one is examining who logs in to the system, what FTP sessions are conducted, and so forth. The customer is strongly urged to install one of the suggested log-checking packages such as swatch or logcheck and configure it to email its output to a systems administrator daily.

- g. **Central Log Host:** One of the first actions an intruder will take upon successfully breaking into a system is to erase the logs, removing traces of the attack and the intruder's actions. One of the easiest ways to prevent this is to have the syslog daemon log additional copies of system log entries to another host on the network, which has been highly secured beforehand to prevent tampering, or to a lineprinter or similar device. In the event of a log anomaly, there is now a tamper-proof copy of system logs which will aid systems administrators in identifying the intruder and cleaning up the system.

No external logging was being performed on Kumo, which would leave systems administrators with much less information to work with in the case of a security incident. The customer is strongly encouraged to deploy either a network-based centralized log host, or else configure and attach a line-printer or similar device to Kumo for storing logs, and configure syslog to copy system log entries to it as appropriate.

### III. Risks from Third-Party Software

- a. **FTP Server Version:** Some effort appears to have been put into installing and configuring a copy of the Washington University FTP Server (wu-ftpd), which offers a significantly greater degree of control over FTP sessions, including locking off anonymous and guest sessions into chroot-ed jails, and automatically altering file permissions on uploaded files to prevent mischief. The version of the wu-ftpd server on Kumo, however, is version 2.4.1, which is many revisions behind the current version, 2.6.1. Versions prior to 2.6.1, in particular the 2.4.x series, contained numerous buffer overflow and string-format attacks which would give an attacker a root shell on the system or allow her to overwrite files on the disk; these attacks are well-known, and exploits to take advantage of them are widely distributed. The customer is strongly

encouraged, if further FTP service on this host serves their purpose, to upgrade the FTP server as soon as possible to the latest version, and keep track of development of the wu-ftpd server, to ensure that new versions are tested soon after they are released and installed on Kumo as soon as is practically possible.

- b. Apache Server Version: Apache has had a generally good history from a security standpoint: a significant number of the previous releases of Apache have been issued to fix stability problems rather than actively exploitable security holes. Nonetheless, for a production webserver, stability can be as big an issue as security, and just as important (if not more so) a reason to perform regular upgrades.

The version of Apache currently running on Kumo is XXXX, which is significantly behind the current stable version, 1.3.14. Moreover, version 1.3.14 was released to fix actively-exploitable security holes in the immediately-prior release (1.3.13), to which the version on Kumo is presently vulnerable. Melete recommends that the webserver on Kumo be upgraded to the latest stable version of Apache as soon as possible, to prevent attacks being perpetrated against the server.

- c. Vulnerable CGI Scripts: One of the most prevalent vulnerabilities to which web servers are prone is badly coded CGI scripting, which can open enormous holes in a site's security easily, even through heavy firewalling.

Although no formal code review was conducted, four separate security scanners run against Kumo produced no vulnerable CGI scripts. Melete would recommend that the customer perform an internal code audit of the CGI scripts on Kumo to ensure good programming practices have been followed.

- d. SSH Server: Kumo employs Secure Shell (SSH) exclusively for remote administrative access, which is a good step and much to be commended. However, there are two flaws with the current SSH setup which put the system at risk, both of which are relatively simple fixes.

First, the version of SSH running on Kumo is the "commercial" ([www.ssh.com](http://www.ssh.com)) version, rev. 1.2.21: this is significantly behind the current release, 1.2.30. Several of the intervening releases of SSH have been issued to fix known, exploitable security holes; the customer is strongly advised to upgrade to the latest version as soon as possible. Secondly, the server is currently configured to recognize and accept the use of .shosts files as an authentication method, which is significantly less secure than the use of RSA-style public/private keypairs. In the same spirit as deactivating .rhosts authentication on the host, .shosts should in a truly secure configuration be deactivated completely in favor of RSA keypairs (change the options "Rhosts Authentication" and "RhostsRSA Authentication" to "no" and "RSAAuthentication" to "yes" in the /etc/sshd\_config file).

#### IV. Administrative Practices

- a. Lack of Specific Administration: At the moment, no administrator is specifically tasked with maintenance on Kumo: the task falls to a group of individuals "as they get time". This poses a significant risk, paired with the lack of specific policy surrounding Kumo. Without specific policy dictating the actions administrators are responsible for performing and who is responsible for performing them, it is simply too easy for more clearly-defined priorities to overrule the periodic maintenance and upkeep of this system.

To remedy this, a specific list of responsibilities for Kumo and the periodic dates on which they need to be performed (first of the month, once per week, &c.) must be generated. This information must then be doled out to the appropriate administrative personnel so that an individual or (preferably) an individual with several backups and cross-checks is responsible for each item on the list.

#### V. Security Patches and so forth

- a. No System Patches: Following the release of a version of Solaris, Sun will periodically distribute additional system patches which are meant to fix security vulnerabilities and correct program errors to improve the functionality of the system. These patches are distributed through <http://sunsolve.sun.com>, and are freely available to all. Especially given that many patches fix well-known security holes with widely-distributed exploits, keeping a system up to the latest patch revision level is part of the scope of any reasonable security program. This involves developing a policy that mandates keeping hosts up-to-date, and a set of procedures that dictate who is responsible for keeping track of new patches as they are released, and how those new patches will be downloaded, installed and tested on a non-production system, and then rolled out to a production environment in a timely and responsible fashion.

Kumo has no software patches installed, meaning the system was installed as is from the distribution media and put out on the network. This is highly dangerous: many of the other vulnerabilities to which Kumo is vulnerable would be solved if the appropriate patches were installed. Systems administrators should schedule downtime on Kumo as soon as possible, download the latest patch cluster for Solaris 2.6, and install it in single user mode.

#### VI. Data Handling

- a. Insecure Data Handling: Given the sensitivity of the data stored on system backup tapes, it is absolutely imperative that backups be made using a strong encryption system with limited key access. Many commercial backup solutions will provide this with minimal reduction in performance, and the security of the resulting backups is well worth it. Especially when performing offsite backups, or in situations where backup tapes must be stored in insecure areas (i.e. not in a locked cabinet), utilization of encryption is a vital part of an enterprise backup scheme.



Kumo's backups are currently being written out without encryption, which would allow any attacker who obtained a system backup tape to read it, giving him access to sensitive company data and opportunities for system access through cracking passwords and obtaining valid usernames. As the customer develops their backup procedures and policies, encryption of backups must be an integral part of that design.

- b. Insecure Media Handling: In addition to encryption of data stored on backup media, it is imperative that other avenues and channels of information outflow be carefully and rigorously controlled and sanitized. Hard drives sent to manufacturers for repair, system drives and tapes re-used in new machines and systems re-purposed or re-leased must all be carefully scrutinized by administrators and returned to a sterile state.

Backup tapes from Kumo are routinely used in other systems through the Singing Beagle Productions enterprise, and on two occasions, disks from Kumo have been re-purposed into other systems without being purged, following upgrades. Singing Beagle Productions is urged to develop a secure media handling policy that mandates the erasure of all media being re-purposed or re-used, and the manual sanitization of all leased or re-purposed systems coming in or out of the enterprise.

- c. File Integrity Checking: Given the prevalence of "rootkits" which will replace system binaries and libraries with booby-trapped or trojaned copies, it is absolutely vital that a baseline file integrity check be performed with software such as Tripwire, and that regular checks of the filesystem be performed against this baseline, to ensure no system files have been tampered with.

At present, no such file integrity software is in use on Kumo; it should be a priority to implement such a system as soon as possible. Since no baseline was taken of Kumo prior to putting it into production, any current filesystem baseline must be considered no more than marginally trusted, however at least a current baseline would ensure that no files have changed from this point forward.

## VII. Data Encryption

- a. Login and System Remote Access: Despite their apparent usefulness for remote systems administration, remote access services such as telnet and the "r-commands" (rlogin, rsh, and rexec) suffer from the flaw of passing usernames, passwords, and all data during transactions in the clear over intervening networks. The Secure Shell (SSH) suite of software offers a drop-in replacement for all of these commands, and pipes all session data over an encrypted tunnel between client and server. In addition, stronger authentication mechanisms are provided for offering passwordless access or integration with one-time password schemes such as S/Key and OPIE.

Kumo employs SSH exclusively, without offering telnet or r-services (all of which have been disabled to prevent bypassing SSH). Aside from

software upgrades (cf. "Risks from Third-Party Software", above), no further recommendations need be made here.

- b. Secure Data on Insecure Protocols: The webserver on Kumo serves, among other functions, as a point for tracking customer information and trouble tickets, any or all of which could be considered sensitive data. While this data is protected with a reasonably well-designed password scheme, all usernames, passwords and transferred data pass in cleartext over the Internet between client and server.

Given the sensitivity of the data stored on the server and the client's expressed desire to run a tightly-secured system, it is Melete's recommendation that the existing Apache server be replaced with a server capable of running SSL (Secure Sockets Layer) transactions. The Apache + mod\_ssl project distributes a freeware Apache version with SSL plugins; commercial variants from Covalent and C2 are also recommended, as is the Netscape iPlanet server.

### VIII. Appropriate Access Restrictions

- a. Physical Access: Despite all attempts to secure the console against malicious intrusions, the simple fact remains that a determined, skilled intruder with enough time and access to the physical console of a machine can gain access to the data on the disks, almost no matter what preventative measures are taken. To prevent this, it is imperative to store the CPU of the system in a secure facility: in a server room which offers badge-controlled access or cipherlocks, and preferably locked racks or cabinets inside for storing the CPU itself.

The physical access surrounding the console for Kumo was entirely unacceptable. Although inside an office with both access points controlled by cipherlocks, the door to the server room is right next to an entrance point, which would make it easy for an intruder to slip in after an employee. The door to the server room is unlocked and remains constantly open; there are no physical locks on the racks or the console itself to prevent physical tampering. All of this needs to be corrected as soon as possible: given the constant throughput of visitors, office staff and building workers, the protection of the physical console cannot be guaranteed, putting the entire system in jeopardy.

- b. Electronic Access: Just as restricting the physical console of a server to a known set of trusted users increases the security of the system, so, too, does taking the same measures to protect access to the root account.

- A. Legacy Accounts: One important step in retaining control of the root account on a system is user account lifecycle maintenance: removing old and legacy logins, locking unused user accounts and so forth. Kumo displayed a number of accounts from former employees which were not disabled, potentially leaving doors into the system for attacks both from disgruntled employees and from clever attackers breaking unwatched system accounts. The

removal of these accounts will greatly increase the security of the system, along with an immediate change of the root password to ensure former admins will not be able to gain access.

- B. Granular Admin Restrictions: Not all administrators have the same level of knowledge, or require the same level of access, and by the same token, neither do all users. At the moment, the permissions on the `/sbin/su` file on Kumo are set to the default, which allows anyone on the system to access the root account if she knows the password. A first step towards reducing access to this would be to add known administrative accounts to an admin group such as "wheel", and change the permissions on the file to remove universal access. To do this, edit the `/etc/group` file and add known admin account names to the line which begins "wheel", separated by commas, then execute the following commands as root, which will restrict access appropriately:

```
/bin/chown root:wheel /sbin/su
/bin/chmod 4750 /sbin/su
```

[Note that if you later install the SUNWsutl package, which contains statically-linked binaries of system commands, you will need to perform the same restriction on `/sbin/su.static`.]

IX. Backup policies, disaster preparedness, &c.

- a. No Backup Procedures: In order to protect both against malicious actions by intruders and hardware failures that could render a system unusable, it is essential for an organization to develop a firm backup policy and set of accompanying procedures that dictate how backups will be performed and when. This task must be handed to a systems administrator or group of administrators whose explicit responsibility it will be not only to perform the backups regularly, but to test the quality of the backups by attempting partial and full restores from backup tapes on a regular basis.

While there is a local tape drive on Kumo and associated scripts for performing backups, it is not the explicit responsibility of any administrator to perform this task; rather, it is performed "whenever significant change is made to the host", according to the administrators interviewed. In addition, there is no testing of backups, periodic or otherwise. These could leave the host in a disastrously vulnerable state should a hard drive fail or an intruder wipe the disks to prevent discovery. Melete's strong recommendation is that the customer perform an immediate review of backup policy and procedure, and begin implementing a sound backup strategy as soon as possible.

- b. No Hardware Failure Provisions: Especially for systems defined as high-profile or mission-critical to a company, it is vital to have spare hardware onsite, preferably kept in warm standby (e.g. a spare host with daily-synchronized disks, ready to be substituted should the live host fail for any reason). This includes not just spare hard drives and memory

DIMMs, but also a spare system and potentially may extend to spare network hardware.

While spare hard drives could likely be scrounged from the lab in which Kumo is installed, such a procedure would be time-consuming, and would risk installing a piece of equipment with unknown filesystems on it and a potential for rapid failure. It is imperative that the customer purchase sufficient spare hardware for Kumo that a total systems failure could be sustained and the system would be back online rapidly. Should this prove difficult to budget for in the short term, there are companies such as Comdisco which will keep a copy of system backups and bring a copy of your host online within a short time should a failure occur.

X. Other issues

- a. **Firewalling:** The importance of good firewalling cannot overshadow the importance of host-based security; a good firewall, however, can help supplement a site's security significantly.

After scanning Kumo through the site firewall (a Check Point Firewall-1 implementation), no unfiltered ports were discovered. This means the firewall is stateful, and is successfully checking each inbound connection against the state table to ensure that attackers may not bypass the firewall rulebase. The rulebase, however, includes a number of open ports which are not secure and should not be required for production service on Kumo. Open ports are listed below: ports surrounded with brackets ([]) should definitely be closed, and ports surrounded with parentheses () should be reviewed and closed if they are not required for the services Kumo provides.

Port	Service Name
21	FTP
22	SSH
(25)	(SMTP)
80	HTTP
[111]	[SunRPC / Portmapper]
[139]	[NetBIOS]
[6000]	[X-Windows]
[6112]	[DTSPC]
[7100]	[Font-service]
[32772]	[RPC]
[32773]	[RPC]
(33285)	[Unknown]
(33313)	(Unknown)

b.

**Prioritized Risks:**

Two lists of prioritized risks have been presented here: the first is the list which should be followed if Kumo is to be maintained online in its present state for any length

of time; the second is the list of errors to ensure are avoided should the customer opt to build a replacement server for Kumo. Obviously, building a secure replacement should start from a well-written and tested secure configuration document: good starting points are the Solaris Security FAQ, the "Hardening Solaris for Firewall-1" document online by Lance Spitzner, and of course the SANS [Step-by-Step Guide to Securing Solaris](#). Items below have been annotated where needed; unannotated items are believed to be self-explanatory.

#### List 1: Risks in Current Configuration

1. No System Patches: Given the sheer number of security issues and stability fixes these provide, scheduling time to install the latest complete patch cluster from Sun must be the customer's first priority.
2. RPC ToolTalk Server: Apply the patch for this vulnerability and (preferably) disable the service entirely.
3. FTP and Apache Version Upgrades: Since these are public services offered through the firewall with known security exploits, these must be the next point of attack on the part of the customer. While upgrading Apache, the customer would be well-advised to install a webserver with SSL capabilities, either the freeware Apache+mod\_ssl package or a similar commercial package. While upgrading the FTP software, the creation and stocking of an `/etc/ftpusers` file should be considered mandatory.
4. Legacy Accounts: Several of these are former systems administrators, who may have backdoors in the system. Locking off their accounts and renaming their home directories should be a sufficient step to keep them out until a new, clean system can be installed.
5. SSH Version: This is only marginally lower on the list, and should be considered a high priority, especially since upgrading to the latest version will require little more than compiling a new binary and installing it: the configuration files have not changed between 1.2.21 and 1.2.30.
6. TCP Wrappers: Especially given that the system is a public FTP server, installing TCP wrappers will be an important step to controlling access to resources and generating good logs of FTP sessions. As a bonus, SSH can be compiled with the TCP Wrapper libraries, allowing admins to control access to SSH as well through the same interface.
7. Log Review and Configuring Centralized Logging: These two go hand in hand--logs are currently not being reviewed, and will be much easier to review on a regular basis when they are concatenated to a single secure point, which will, in turn, ensure that the logs remain tamper-proof.
8. Filesystem Integrity Checking: Under any newly-implemented server, the use of filesystem integrity checking would be an absolute imperative early on in the implementation, then frequently and regularly thereafter. Since Kumo has already existed for some time without such software, any integrity checking software will only ensure that no changes are made from this point forward, which will provide some degree of security but is not quite as high on the list of priorities.

9. Physical Security: Since the outside perimeter of the office is at least partially secured, this will likely not prove a first avenue of attack on Kumo. Nonetheless, this issue needs to be dealt with in short order; this should include the configuration of secure console settings such as the PROM password and security mode.
10. Unnecessary Software Installed: Although not currently posing active remote security risks, the list of software currently installed includes a number of packages with known local root exploits, which could hand control of the box over to a malicious trusted user. The customer would be well-advised to review the list of installed software as soon as possible, and test removing packages during maintenance windows until only required packages are installed.
11. Backup Procedures and Policies: A full backup of the system should be taken as soon as possible, and another one when the system has been more significantly secured. Singing Beagle Productions needs to institute a firm backup plan, as discussed above, and ensure that system backups are being carried out on a regular basis.
12. Granular Administration: Given the small number of actual administrators, this is not a high priority, but should definitely be an item on the list to complete. Administration of any server by more than one administrator is much easier when there are good records of what changed on a host and who changed it: mandating these log entries through the use of software such as sudo will improve the situation considerably.
13. Hardware Failure Preparedness / Disaster Preparedness
14. Specific Systems Administration Procedures and Policies; Determination of Responsibility for Enforcing Policy and Procedure

List 2: Risks to Avoid for Replacement Units:

1. OS Version: Any new implementation of this server configuration should definitely employ at least Solaris version 7, and version 8 should be considered (although it is not a requirement).
2. Unnecessary Software Installed: As stated above, beginning with a minimal configuration and adding onto it anything further which is required will ultimately result in a far more secure server than starting from too much software and paring things down.
3. No Software Patches: Immediately following a successful installation, the latest patch cluster from Sun must be installed for the host to be considered production-ready.
4. FTP/Apache/SSH Software Versions: Obviously, any new server installed should use the latest versions of this software; with the recent demise of the RSA Patent, Melete can find no reason not to recommend that any new Apache version installed be SSL-capable, even if such functionality is not immediately implemented.
5. TCP Wrappers

6. Centralized Logging and Log Review
7. Granular Administration Setup
8. Backups and Filesystem Integrity Checks: Immediately following the final configuration of the server but prior to putting it into production (preferably while not connected to any network), a "gold" backup must be performed on the new host. This backup should be retained through the life of the host and tested thoroughly: no matter what may occur to the rest of the backups or the host itself, this backup will provide a safe fallback to the initial implementation baseline. Hand in hand with this is a baseline using Tripwire or similar software: performing this baseline prior to connecting the host to a network will provide an absolute standard against which future filesystem checks can be verified to be sure no changes have been made.
9. Physical Security
10. Disaster Preparedness / Hardware Failure Preparedness
11. Specific Systems Administration Procedures and Policies; Determination of Responsibility for Enforcing Policy and Procedure

### Costs Estimate

It is vital to remember that the following are purely estimates, and should be considered neither actual estimates or price quotes for services rendered by Melete nor anything more than conjecture.

Complete Repairs to Existing System:

\$200 x 16 hours = \$3200	Engineer billable time for repairs
\$150 x 8 hours = \$1200	Tech Writer billable time: document new system as installed and repaired
\$150 x 40 hours = \$6000	Tech Writer billable time: generate policy and procedure documents for new system
\$10400	Total tangible expense for system repairs
2.5 - 3 hours	Total required system downtime for repairs, subdividable into smaller chunks: 1-1.5 hours - Install latest patch cluster 1-1.5 hours - Perform system level-0 "gold" backup and perform Tripwire integrity check .05 hours - Install latest Apache version <sup>iii</sup> .05 hours - Install latest wu-ftpd version <sup>iv</sup> .05 hours - Install latest SSH daemon <sup>v</sup> .05 hours - Install TCP Wrappers <sup>vi</sup>

Develop and Implement New System:

\$200 x 24 hours = \$4800	Engineer billable time for implementation
---------------------------	---

\$150 x 4 hours = \$600	Tech Writer billable time: document new system as installed <sup>vii</sup>
\$150 x 40 hours = \$6000	Tech Writer billable time: generate policy and procedure documents for new system
\$11400	Total tangible expense for system repairs

© SANS Institute 2000 - 2002, Author retains full rights.



## Appendices

---

### Appendix A: Suggested References in Print

1. Practical Unix and Internet Security (Garfinkel, Spafford. c. 1995 by O'Reilly and Associates, Inc., ISBN 1565921488)  
Although becoming somewhat dated, this is still one of the canonical guides to Unix security, and is worth every system administrator and security engineer's time.
2. Unix Systems Administration Handbook (Nemeth, & al. c. 2000 by Prentice Hall, ISBN 0130206016)  
Now in its third printing, this multi-platform guide to the world of systems administration offers, among other things, fantastic chapters on general system security, developing good systems administration policies and procedures, and maintaining good political relations as systems administrators dealing with the rest of the world.
3. Solaris Security: Step by Step (Pomeranz, & al. Published by the SANS Institute, [www.sans.org](http://www.sans.org))  
Written by the consensus of a large group of Solaris administrators and gurus, this is not only an excellent guide to creating a secure baseline Solaris install, but an excellent starting point for adapting to other Unix flavors.
4. Linux System Security: The Administrator's Guide to Open Source Security Tools (Mann, Mitchell. c. 1999 by Prentice Hall, ISBN 0130158070)  
A recent work, this serves as a good guide to implementing tools such as SSH and Tripwire, as well as tips for secure NFS implementations, general system security, and advanced topics such as varieties of the cryptographic filesystem and using ipchains for firewalling. Although Linux-focused, many of the tools quoted here will be readily adaptable to other platforms with little trouble; the guide is worth purchasing for the chapter on SSH alone (although it does not cover OpenSSH).
5. Hacking Exposed (Scambray, McClure, Kurtz. c. 2000 by Osborne/McGraw-Hill, ISBN 0072127481)  
Now in its second edition, this is a terrific guide to getting inside the mind of the average system intruder, which will in turn guide administrators towards finding the holes in their own networks. This is a good guide for more advanced, security-focused administrators, since it focuses less on simply probing the local network for vulnerabilities, and more on the skills of profiling networks and penetrating systems.
6. Essential System Administration (Frisch, Loukides (editor). c. 1995, O'Reilly and Associates, Inc., ISBN 1565921275)  
A bit due for a second edition, this is the other "bible" for systems administrators: an excellent guide to Unix in general.
7. Building Internet Firewalls (Zwicky, Cooper, Chapman. c. 2000, O'Reilly and Associates, Inc., ISBN 1565928717)  
Once the hosts are all secured, the next step is to work on firewalling to protect the entries and exits on the network, and take some of the load of

repelling intruders off of the servers. This is an excellent guide to firewalls, especially in it's new edition. Check out also the older Firewalls and Internet Security: Repelling the Wily Hacker (Cheswick, Bellovin, c. 1994 Addison Wesley Longman, Inc., ISBN 0201633574) and the newer Building Linux and OpenBSD Firewalls (Sonnenreich, Yates. c. 1999 Wiley, John and Sons, Inc., ISBN 0471353663), both excellent guides to furthering one's firewall education.

8. Network Intrusion Detection: An Analyst's Handbook (Northcutt, Novak, McLachlan. c. 2000, New Riders Publishing, ISBN 0735710082)

For the advanced security-minded administrator, the next step is to begin watching the network proactively for attack, and there is no better guide to digging into that than this book. Can't be recommended highly enough.

---

#### Appendix B: Online Resources and Tools

URLs for further security information

- <http://www.securityfocus.com> : Home to the Bugtraq vulnerability discussion list and database, this has become one of the places to visit for security news, vulnerability information, tools, product guides and articles on Internet security and related topics.
- <http://www.sans.org> : Systems Administration and Network Security (SANS) Institute hosts periodic conferences throughout the U.S. and internationally, offering education and discussion of varied Internet security topics.
- <http://www.cerias.purdue.edu> : Although perhaps not as loudly thriving as their predecessor, COAST, the Center for Education and Research in Information Assurance and Security (CERIAS) continues to offer an excellent FTP archive of security tools and a wide variety of whitepapers, research projects, and interesting discussion on various topics within Internet security.
- <http://www.cert.org> : Somewhat overshadowed by Bugtraq these days because of their more conservative timeline for releasing security alerts, the CERT Coordination Center is nonetheless doing some excellent work concatenating cross-platform security vulnerabilities, educating administrators about trends in vulnerabilities, and encouraging the free flow of information about security and the threat from network attackers.

URLs for Unix Security and Systems Administration Tools:

- <http://www.apache.org> : Home of development on the Apache webserver; be sure also to visit [www.modssl.org](http://www.modssl.org) and [www.openssl.org](http://www.openssl.org) for information on building free, SSL-enabled Apache implementations.
- <http://www.wu-ftpd.org> : Site for development of the Washington University FTP daemon (wu-ftpd).
- <http://www.psonic.com/abacus/logcheck> : Site to visit for information about logcheck, a freeware log parser. Logcheck will parse through system logs, collect any information that does not match a set of known acceptable information, and mail the output to a systems administrator for review, thus significantly easing the job of periodic log review. An excellent tool.

- <http://www.stanford.edu/~atkins/swatch> : Swatch is the opposite of logcheck, although the two perform similar functions. Rather than discarding known goodness, swatch parses logs looking for predefined triggers, and sends alerts when it finds them. More flexible than logwatch, Swatch is capable of taking a number of different actions based on the triggers it finds and the configuration it has been given.
- <http://www.insecure.org/nmap> : Site for Nmap, the freeware Network Mapper written by Fyodor. A Swiss Army Knife of network scanning, nmap has plugins for TCP and UDP scanning, OS fingerprinting and detection, and further plugins from other authors offer version and vulnerability checking to boot.
- <http://www.nessus.org> : Site for the Nessus security scanner, used in this assessment (see discussion under "Tools" section of "Methodology").
- <http://www.wwdsi.com> : Home of the SAINT vulnerability scanner, also used in this assessment
- <http://packetstorm.securify.com> : Spanning the bridge between the "white hat" world of security professionals and the "black hat" world of intruders, PacketStorm offers a significant collection of "hacker tools", including the Malice and Whisker tools used in this assessment. The collection also includes a number of actual system exploits, useful for examination and comparison during a forensic examination.
- <http://freshmeat.net> : An excellent site for open-source (and some non-open-source) code of all kinds, Freshmeat offers a vast library of software, with a significant focus on Linux.
- <ftp://ftp.porcupine.org/pub/security> : Site to download Wietse Venema's TCP Wrappers program, mentioned several times in this document.
- <http://www.enteract.com/~lspitz> : Site of Lance Spitzner, a consultant and engineer for Sun Microsystems. Lance's pages contain a terrific collection of whitepapers on system security and checklists and hardening documents for Solaris and Linux.
- <http://www.sunworld.com/sunworldonline/common/security-faq.html> : The Solaris Security FAQ, while somewhat dated in places, is an excellent resource for shoring up the security of Solaris servers.

---

### Appendix C: Raw Data Gathered

[ Additional Note about Data Sanitation: In order to facilitate the processing of certain large collections of usernames, some usernames from accounts no longer present but verified as once having existed have been replaced as well. The logins on the system have been checked: no logins appeared in any system logs which had no corresponding entries at some point in the system configuration (which would indicate an intrusion). ]

```
# nmap (V. 2.54BETA4) scan initiated Fri Nov 17 17:31:02 2000 as:
/usr/local/bin/nmap -sS -O -p 1-65535 -vv -oN nmap-synOS.log 172.16.2.1
Interesting ports on (172.16.2.1):
```

.....  
(The 65523 ports scanned but not shown below are in state: closed)

Port	State	Service
21/tcp	open	ftp
22/tcp	open	ssh
25/tcp	open	smtp
80/tcp	open	http
111/tcp	open	sunrpc
6000/tcp	open	X11
6112/tcp	open	dtspc
7100/tcp	open	font-service
32772/tcp	open	sometimes-rpc7
32773/tcp	open	sometimes-rpc9
33285/tcp	open	unknown
33313/tcp	open	unknown

TCP Sequence Prediction: Class=random positive increments  
Difficulty=39423 (Worthy challenge)

Sequence numbers: A89A690A A89AAB3E A89AE1D9 A89BA327 A89D77EB A89E9B59

Remote operating system guess: Solaris 2.6 - 2.7

OS Fingerprint:

TSeq (Class=RI%gcd=1%SI=99FF)

T1 (Resp=Y%DF=Y%W=2297%ACK=S++%Flags=AS%Ops=NNTNWME)

T2 (Resp=N)

T3 (Resp=N)

T4 (Resp=Y%DF=Y%W=0%ACK=0%Flags=R%Ops=)

T5 (Resp=Y%DF=Y%W=0%ACK=S++%Flags=AR%Ops=)

T6 (Resp=Y%DF=Y%W=0%ACK=0%Flags=R%Ops=)

T7 (Resp=Y%DF=Y%W=0%ACK=S%Flags=AR%Ops=)

PU (Resp=Y%DF=Y%TOS=0%IPLen=70%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)

# Nmap run completed at Fri Nov 17 17:31:41 2000 -- 1 IP address (1 host up)  
scanned in 38 seconds

# nmap (V. 2.54BETA4) scan initiated Fri Nov 17 17:32:43 2000 as:  
/usr/local/bin/nmap -sT -sR -I -p 1-65535 -vv -oN nmap-connectRPCIdent.log  
172.16.2.1

Interesting ports on (172.16.2.1):

(The 65523 ports scanned but not shown below are in state: closed)

Port	State	Service (RPC)	Owner
21/tcp	open	ftp	
22/tcp	open	ssh	
25/tcp	open	smtp	
80/tcp	open	http	
111/tcp	open	sunrpc (rpcbind V2-4)	
6000/tcp	open	X11	
6112/tcp	open	dtspc	
7100/tcp	open	font-service	
32772/tcp	open	sometimes-rpc7 (tttdserverd V1)	
32773/tcp	open	sometimes-rpc9	
33285/tcp	open	(ttsession V1-4)	
33313/tcp	open	(kcms_server V1)	

# Nmap run completed at Fri Nov 17 17:33:05 2000 -- 1 IP address (1 host up)  
scanned in 21 seconds

```

.....
# nmap (V. 2.54BETA4) scan initiated Fri Nov 17 17:34:12 2000 as:
/usr/local/bin/nmap -sT -sV -FV -oN nmap-version.log 172.16.2.1
Interesting ports on (172.16.2.1):
(The 23 ports scanned but not shown below are in state: closed)
Port      State      Service      Protocol      Version
21/tcp    open       ftp          FTP           wu-2.4.2-academ[BETA-
16](1)
22/tcp    open       ssh          SSH           1.5-1.2.21
25/tcp    open       smtp         SMTP
80/tcp    open       http         HTTP          Apache/1.2.6
mod_perl/1.10
111/tcp   open       sunrpc       RPC
# Nmap run completed at Fri Nov 17 17:34:29 2000 -- 1 IP address (1 host up)
scanned in 17 seconds

# nmap (V. 2.54BETA4) scan initiated Wed Nov 22 10:44:58 2000 as: nmap -sA -p
1-65535 -vv -oN nmap-ACK.log 192.168.56.129
All 65535 scanned ports on (192.168.56.129) are: filtered
# Nmap run completed at Wed Nov 22 11:39:22 2000 -- 1 IP address (1 host up)
scanned in 3264 seconds

# nmap (V. 2.54BETA4) scan initiated Wed Nov 22 11:47:17 2000 as:
/usr/local/bin/nmap -sT -p 1-65535 -oN nmap-TCPthroughfire.log -vv
kumo.singingbeagle.org
Interesting ports on (192.168.56.129):
(The 65522 ports scanned but not shown below are in state: closed)
Port      State      Service
21/tcp    open       ftp
22/tcp    open       ssh
25/tcp    open       smtp
80/tcp    open       http
111/tcp   open       sunrpc
139/tcp   filtered  netbios-ssn
6000/tcp  open       X11
6112/tcp  open       dtspc
7100/tcp  open       font-service
32772/tcp open       sometimes-rpc7
32773/tcp open       sometimes-rpc9
33285/tcp open       unknown
33313/tcp open       unknown

# Nmap run completed at Wed Nov 22 11:56:21 2000 -- 1 IP address (1 host up)
scanned in 543 seconds

```

Nessus Scan Report

---

SUMMARY

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

.....  
TESTED HOSTS

172.16.2.1 (Security warnings found)

DETAILS

- + 172.16.2.1 :
  - . List of open ports :
    - o unknown (32772/tcp) (Security warnings found)
  - . Warning found on port unknown (32772/tcp)

The tooltalk RPC service is running.  
A possible implementation fault in the  
ToolTalk object database server may allow a  
cracker to execute arbitrary commands as  
root.

\*\* This warning may be a false  
positive since the presence  
of the bug was not tested \*\*

Solution : Disable this service.  
See also : CERT Advisory CA-98.11

Risk factor : High  
CVE : CVE-1999-0003

*Engineer's Note: Owing to the difficulties converting HTML into a Word doc, I have condensed the SAINT output page into plain text below, word-for-word. The EXPN and VRFY commands showed as activated, but in fact were not: the host runs SMAP from the Firewall Toolkit, which will respond positively to any EXPN or VRFY request whether the user account in question actually exists or not (thus giving out no information).*

Results - 172.16.2.1

General Host Information

Host type: Solaris 2.6 - 2.7  
Subnet 172.16.2  
Scanning level: heavyplus  
Last scan: Fri Nov 17 18:04:42 2000

Network Services:

FTP server  
SMTP server  
SSH server  
WWW server  
X Windows server  
XDM (X login) server  
1/UDP server  
6112/TCP server  
7100/TCP server  
sunrpc server

.....  
Vulnerable Services:

Sendmail command EXPN is enabled  
Sendmail command VRFY is enabled  
SSH-1.2.21\n is vulnerable

[ Top 10 ] tooltalk version may be vulnerable to a buffer overflow (CVE 1999-0003)

*Engineer's Note: This is the output from running the Whisker tool against 172.16.2.1. I also ran "Malice", which ran for a minute and a half, then returned that the site's security was such that it could find nothing wrong.*

-- whisker / v1.4.0+SSL / rain forest puppy / www.wiretrip.net --  
- Loaded script database of 2124 lines

= - - - - = - - - - =

= Host: 172.16.2.1

= Server: Apache/1.2.6 mod\_perl/1.10

+ 404 File Not Found: GET /cfdocs/  
+ 404 File Not Found: GET /scripts/  
+ 404 File Not Found: GET /cfcache.map  
+ 404 File Not Found: GET /cfide/Administrator/startstop.html  
+ 404 File Not Found: GET /cfappman/index.cfm  
+ 403 Forbidden: GET /cgi-bin/  
+ 403 Forbidden: GET /cgi-bin/dbmlparser.exe  
+ 404 File Not Found: HEAD /\_vti\_inf.html  
+ 404 File Not Found: HEAD /\_vti\_pvt/  
+ 403 Forbidden: HEAD /cgi-bin/webdist.cgi  
+ 403 Forbidden: HEAD /cgi-bin/handler  
+ 403 Forbidden: HEAD /cgi-bin/wrap  
+ 403 Forbidden: HEAD /cgi-bin/pfdisplay.cgi  
+ 403 Forbidden: HEAD /cgi-bin/MachineInfo  
+ 404 File Not Found: HEAD /mall\_log\_files/order.log  
+ 404 File Not Found: HEAD /PDG\_Cart/  
+ 404 File Not Found: HEAD /quikstore.cfg  
+ 404 File Not Found: HEAD /orders/  
+ 404 File Not Found: HEAD /Admin\_files/order.log  
+ 404 File Not Found: HEAD /WebShop/  
+ 404 File Not Found: HEAD /pw/storemgr.pw  
+ 404 File Not Found: HEAD /bigconf.cgi  
+ 404 File Not Found: HEAD /icat  
+ 403 Forbidden: HEAD /cgi-bin/icat  
+ 404 File Not Found: HEAD /cgi-local/  
+ 404 File Not Found: HEAD /htbin/  
+ 404 File Not Found: HEAD /cgibin/  
+ 404 File Not Found: HEAD /cgis/  
+ 404 File Not Found: HEAD /cgi/  
+ 404 File Not Found: HEAD /cgi-csc/  
+ 404 File Not Found: HEAD /bin/  
+ 404 File Not Found: HEAD /apps/  
+ 403 Forbidden: HEAD /cgi-bin/flexform.cgi  
+ 403 Forbidden: HEAD /cgi-bin/flexform  
+ 403 Forbidden: HEAD /cgi-bin/LWGate  
+ 403 Forbidden: HEAD /cgi-bin/lwgate  
+ 403 Forbidden: HEAD /cgi-bin/LWGate.cgi  
+ 403 Forbidden: HEAD /cgi-bin/lwgate.cgi  
+ 404 File Not Found: HEAD /cgi-win/  
+ 403 Forbidden: HEAD /cgi-bin/pu3.pl

.....

```
+ 403 Forbidden: HEAD /cgi-bin/meta.pl
+ 403 Forbidden: HEAD /cgi-bin/day5datacopier.cgi
+ 403 Forbidden: HEAD /cgi-bin/webutils.pl
+ 403 Forbidden: HEAD /cgi-bin/tigvote.cgi
+ 403 Forbidden: HEAD /cgi-bin/tpgnrock
+ 403 Forbidden: HEAD /cgi-bin/webwho.pl
+ 403 Forbidden: HEAD /cgi-bin/form.cgi
+ 403 Forbidden: HEAD /cgi-bin/message.cgi
+ 403 Forbidden: HEAD /cgi-bin/.cobalt/siteUserMod/siteUserMod.cgi
+ 403 Forbidden: HEAD /cgi-bin/.fhp
+ 403 Forbidden: HEAD /cgi-bin/htsearch
+ 403 Forbidden: HEAD /cgi-bin/plusmail
+ 404 File Not Found: HEAD /manage/cgi/cgiproc
+ 403 Forbidden: HEAD /cgi-bin/ultraboard.cgi
+ 403 Forbidden: HEAD /cgi-bin/ultraboard.pl
+ 403 Forbidden: HEAD /cgi-bin/perlshop.cgi
+ 403 Forbidden: HEAD /cgi-bin/download.cgi
+ 403 Forbidden: HEAD /cgi-bin/bnbform.cgi
+ 403 Forbidden: HEAD /cgi-bin/bnbform
+ 403 Forbidden: HEAD /cgi-bin/cgi-lib.pl
+ 403 Forbidden: HEAD /cgi-bin/post_query
+ 403 Forbidden: HEAD /cgi-bin/upload.pl
+ 403 Forbidden: HEAD /cgi-bin/rwwwshell.pl
+ 403 Forbidden: HEAD /cgi-bin/nlog-smb.pl
+ 403 Forbidden: HEAD /cgi-bin/nlog-smb.cgi
+ 403 Forbidden: HEAD /cgi-bin/wwwboard/
+ 404 File Not Found: HEAD /wwwboard/
+ 403 Forbidden: HEAD /cgi-bin/wwwboard.pl
+ 403 Forbidden: HEAD /cgi-bin/wwwboard/wwwboard.pl
+ 403 Forbidden: HEAD /cgi-bin/wwwboard.cgi
+ 403 Forbidden: HEAD /cgi-bin/wwwboard/wwwboard.cgi
+ 404 File Not Found: HEAD /logs/
+ 404 File Not Found: HEAD /database/
+ 404 File Not Found: HEAD /databases/
+ 403 Forbidden: HEAD /cgi-bin/cachemgr.cgi
+ 404 File Not Found: HEAD /.htaccess
+ 403 Forbidden: HEAD /cgi-bin/.htaccess
+ 404 File Not Found: HEAD /docs/
+ 403 Forbidden: HEAD /~root/
+ 403 Forbidden: HEAD /cgi-bin/htgrep.cgi
+ 403 Forbidden: HEAD /cgi-bin/htgrep
+ 404 File Not Found: HEAD /ws_ftp.ini
+ 403 Forbidden: HEAD /cgi-bin/ws_ftp.ini
+ 404 File Not Found: HEAD /WS_FTP.ini
+ 403 Forbidden: HEAD /cgi-bin/WS_FTP.ini
+ 403 Forbidden: HEAD /cgi-bin/ax-admin.cgi
+ 403 Forbidden: HEAD /cgi-bin/axs.cgi
+ 403 Forbidden: HEAD /cgi-bin/responder.cgi
+ 403 Forbidden: HEAD /cgi-bin/w3-sql
+ 404 File Not Found: HEAD /search97.vts
+ 404 File Not Found: HEAD /search.vts
+ 404 File Not Found: HEAD /search97cgi/s97.cgi
+ 403 Forbidden: HEAD /cgi-bin/unlg1.1
+ 403 Forbidden: HEAD /cgi-bin/unlg1.2
+ 403 Forbidden: HEAD /cgi-bin/gH.cgi
+ 403 Forbidden: HEAD /cgi-bin/test-cgi
+ 403 Forbidden: HEAD /cgi-bin/campas
```



.....

```
+ 403 Forbidden: HEAD /cgi-bin/www-sql
+ 403 Forbidden: HEAD /cgi-bin/w3-msql
+ 403 Forbidden: HEAD /cgi-bin/view-source
+ 403 Forbidden: HEAD /cgi-bin/add_ftp.cgi
+ 403 Forbidden: HEAD /cgi-bin/cgiwrap
+ 403 Forbidden: HEAD /cgi-bin/guestbook.cgi
+ 403 Forbidden: HEAD /cgi-bin/guestbook.pl
+ 403 Forbidden: HEAD /cgi-bin/edit.pl
+ 403 Forbidden: HEAD /cgi-bin/webbbs.cgi
+ 403 Forbidden: HEAD /cgi-bin/whois_raw.cgi
+ 404 File Not Found: HEAD /webcart/
+ 404 File Not Found: HEAD /webcart-lite/
+ 403 Forbidden: HEAD /cgi-bin/AnyBoard.cgi
+ 403 Forbidden: HEAD /cgi-bin/admin.php
+ 403 Forbidden: HEAD /cgi-bin/code.php
+ 403 Forbidden: HEAD /cgi-bin/dumpenv.pl
+ 403 Forbidden: HEAD /cgi-bin/admin.php3
+ 403 Forbidden: HEAD /cgi-bin/code.php3
+ 403 Forbidden: HEAD /cgi-bin/login.cgi
+ 403 Forbidden: HEAD /cgi-bin/login.pl
+ 404 File Not Found: HEAD /reviews/newpro.cgi
+ 404 File Not Found: HEAD /piranha/secure/passwd.php3
+ 403 Forbidden: HEAD /cgi-bin/sojourn.cgi
+ 403 Forbidden: HEAD /cgi-bin/dfire.cgi
+ 403 Forbidden: HEAD /cgi-bin/spin_client.cgi
+ 403 Forbidden: HEAD /cgi-bin/Count.cgi
+ 403 Forbidden: HEAD /cgi-bin/stats.prf
+ 403 Forbidden: HEAD /cgi-bin/statsconfig
+ 404 File Not Found: HEAD /srchadm
+ 403 Forbidden: HEAD /cgi-bin/count.cgi
+ 404 File Not Found: HEAD /users/scripts/submit.cgi
+ 403 Forbidden: HEAD /cgi-bin/nph-test-cgi
+ 403 Forbidden: HEAD /cgi-bin/webgais
+ 403 Forbidden: HEAD /cgi-bin/websendmail
+ 403 Forbidden: HEAD /cgi-bin/bb-hist.sh
+ 404 File Not Found: HEAD /bb-dnbd/
+ 403 Forbidden: HEAD /cgi-bin/faxsurvey
+ 403 Forbidden: HEAD /cgi-bin/htmlscript
+ 403 Forbidden: HEAD /cgi-bin/aglimpse
+ 403 Forbidden: HEAD /cgi-bin/glimpse
+ 403 Forbidden: HEAD /cgi-bin/man.sh
+ 403 Forbidden: HEAD /cgi-bin/architext_query.pl
+ 403 Forbidden: HEAD /cgi-bin/architext_query.cgi
+ 403 Forbidden: HEAD /cgi-bin/excite
+ 403 Forbidden: HEAD /cgi-bin/getdoc.cgi
+ 403 Forbidden: HEAD /cgi-bin/webplus
+ 403 Forbidden: HEAD /cgi-bin/bizdb1-search.cgi
+ 403 Forbidden: HEAD /cgi-bin/cart.pl
+ 403 Forbidden: HEAD /cgi-bin/filemail.pl
+ 403 Forbidden: HEAD /cgi-bin/filemail
+ 403 Forbidden: HEAD /cgi-bin/php.cgi
+ 403 Forbidden: HEAD /cgi-bin/jj
+ 403 Forbidden: HEAD /cgi-bin/info2www
+ 403 Forbidden: HEAD /cgi-bin/nph-publish
+ 403 Forbidden: HEAD /cgi-bin/ax.cgi
+ 404 File Not Found: HEAD /session/admnlogin
+ 403 Forbidden: HEAD /cgi-bin/rpm_query
```

.....

- + 403 Forbidden: HEAD /cgi-bin/AnyForm2
- + 403 Forbidden: HEAD /cgi-bin/AnyForm
- + 403 Forbidden: HEAD /cgi-bin/textcounter.pl
- + 403 Forbidden: HEAD /cgi-bin/wwwthreads/
- + 404 File Not Found: HEAD /wwwthreads/
- + 403 Forbidden: HEAD /cgi-bin/wwwthreads/w3tvars.pm
- + 403 Forbidden: HEAD /cgi-bin/wwwthreads/3tvars.pm
- + 403 Forbidden: HEAD /cgi-bin/classified.cgi
- + 403 Forbidden: HEAD /cgi-bin/classifieds.cgi
- + 403 Forbidden: HEAD /cgi-bin/classifieds
- + 404 File Not Found: HEAD /ss.cfg
- + 404 File Not Found: HEAD /ncl\_items.html
- + 403 Forbidden: HEAD /cgi-bin/survey.cgi
- + 403 Forbidden: HEAD /cgi-bin/survey
- + 404 File Not Found: HEAD /test/test.cgi
- + 403 Forbidden: HEAD /cgi-bin/search.cgi
- + 403 Forbidden: HEAD /cgi-bin/c\_download.cgi
- + 403 Forbidden: HEAD /cgi-bin/ntitar.pl
- + 403 Forbidden: HEAD /cgi-bin/enter.cgi
- + 403 Forbidden: HEAD /cgi-bin/dig.cgi
- + 403 Forbidden: HEAD /cgi-bin/tidfinder.cgi
- + 403 Forbidden: HEAD /cgi-bin/tablebuild.pl
- + 403 Forbidden: HEAD /cgi-bin/displayTC.pl
- + 403 Forbidden: HEAD /cgi-bin/dasp/fm\_shell.asp
- + 403 Forbidden: HEAD /cgi-bin/printenv
- + 403 Forbidden: HEAD /cgi-bin/environ.cgi
- + 403 Forbidden: HEAD /cgi-bin/session/adminlogin
- + 403 Forbidden: HEAD /cgi-bin/finger
- + 403 Forbidden: HEAD /cgi-bin/finger.pl
- + 403 Forbidden: HEAD /cgi-bin/finger.cgi
- + 403 Forbidden: HEAD /cgi-bin/maillist.pl
- + 403 Forbidden: HEAD /cgi-bin/maillist.cgi
- + 403 Forbidden: HEAD /cgi-bin/sh
- + 403 Forbidden: HEAD /cgi-bin/bash
- + 403 Forbidden: HEAD /cgi-bin/ash
- + 403 Forbidden: HEAD /cgi-bin/tcsh
- + 403 Forbidden: HEAD /cgi-bin/ksh
- + 403 Forbidden: HEAD /cgi-bin/csh
- + 403 Forbidden: HEAD /cgi-bin/rksh
- + 403 Forbidden: HEAD /cgi-bin/rsh
- + 403 Forbidden: HEAD /cgi-bin/zsh
- + 403 Forbidden: HEAD /cgi-bin/perl
- + 403 Forbidden: HEAD /cgi-bin/test-cgi.tcl
- + 404 File Not Found: HEAD /php/
- + 404 File Not Found: HEAD /mlog.phtml
- + 403 Forbidden: HEAD /cgi-bin/mlog.phtml
- + 404 File Not Found: HEAD /mylog.phtml
- + 403 Forbidden: HEAD /cgi-bin/mylog.phtml
- + 404 File Not Found: HEAD /HyperStat/stat\_what.log
- + 404 File Not Found: HEAD /Stats/
- + 404 File Not Found: HEAD /WebTrend/
- + 404 File Not Found: HEAD /analog/
- + 404 File Not Found: HEAD /cache-stats/
- + 404 File Not Found: HEAD /easylog/easylog.html
- + 404 File Not Found: HEAD /hit\_tracker/
- + 404 File Not Found: HEAD /hitmatic/
- + 404 File Not Found: HEAD /hitmatic/analyse.cgi

.....

```
+ 404 File Not Found: HEAD /hyperstat/stat_what.log
+ 404 File Not Found: HEAD /log/
+ 404 File Not Found: HEAD /logfile/
+ 404 File Not Found: HEAD /logfiles/
+ 404 File Not Found: HEAD /logger/
+ 404 File Not Found: HEAD /logging/
+ 404 File Not Found: HEAD /logs/access_log
+ 404 File Not Found: HEAD /ministats/admin.cgi
+ 404 File Not Found: HEAD /scripts/weblog
+ 404 File Not Found: HEAD /server_stats/
+ 404 File Not Found: HEAD /stat/
+ 404 File Not Found: HEAD /statistics/
+ 404 File Not Found: HEAD /stats/
+ 404 File Not Found: HEAD /super_stats/access_logs
+ 404 File Not Found: HEAD /trafficlog/
+ 404 File Not Found: HEAD /ustats/
+ 404 File Not Found: HEAD /w3perl/admin
+ 404 File Not Found: HEAD /webaccess/access-options.txt
+ 404 File Not Found: HEAD /weblog/
+ 404 File Not Found: HEAD /weblogs/
+ 404 File Not Found: HEAD /webstats/
+ 404 File Not Found: HEAD /wstats/
+ 404 File Not Found: HEAD /wusage/
+ 404 File Not Found: HEAD /wwwlog/
+ 404 File Not Found: HEAD /wwwstats/
+ 404 File Not Found: HEAD /access-log
+ 404 File Not Found: HEAD /access.log
+ 404 File Not Found: HEAD /awebvisit.stat
+ 404 File Not Found: HEAD /dan_o.dat
+ 404 File Not Found: HEAD /hits.txt
+ 404 File Not Found: HEAD /log.htm
+ 404 File Not Found: HEAD /log.html
+ 404 File Not Found: HEAD /log.txt
+ 404 File Not Found: HEAD /logfile
+ 404 File Not Found: HEAD /logfile.htm
+ 404 File Not Found: HEAD /logfile.html
+ 404 File Not Found: HEAD /logfile.txt
+ 404 File Not Found: HEAD /logger.html
+ 404 File Not Found: HEAD /stat.htm
+ 404 File Not Found: HEAD /stats.htm
+ 404 File Not Found: HEAD /stats.html
+ 404 File Not Found: HEAD /stats.txt
+ 404 File Not Found: HEAD /webaccess.htm
+ 404 File Not Found: HEAD /wwwstats.html
+ 403 Forbidden: HEAD /cgi-bin/log/
+ 403 Forbidden: HEAD /cgi-bin/log/nether-log.pl?checkit
+ 403 Forbidden: HEAD /cgi-bin/logs/
+ 403 Forbidden: HEAD /cgi-bin/stat/
+ 403 Forbidden: HEAD /cgi-bin/stats.pl
+ 403 Forbidden: HEAD /cgi-bin/stats/
+ 403 Forbidden: HEAD /cgi-bin/clickcount.pl?view=test
+ 403 Forbidden: HEAD /cgi-bin/cstat.pl
+ 403 Forbidden: HEAD /cgi-bin/ex-logger.pl
+ 403 Forbidden: HEAD /cgi-bin/hitview.cgi
+ 403 Forbidden: HEAD /cgi-bin/log-reader.cgi
+ 403 Forbidden: HEAD /cgi-bin/logit.cgi
+ 403 Forbidden: HEAD /cgi-bin/logs.pl
```

.....  
+ 403 Forbidden: HEAD /cgi-bin/lookwho.cgi  
+ 403 Forbidden: HEAD /cgi-bin/mini\_logger.cgi  
+ 403 Forbidden: HEAD /cgi-bin/ratlog.cgi  
+ 403 Forbidden: HEAD /cgi-bin/robadmin.cgi  
+ 403 Forbidden: HEAD /cgi-bin/show.pl  
+ 403 Forbidden: HEAD /cgi-bin/stats-bin-p/reports/index.html  
+ 403 Forbidden: HEAD /cgi-bin/statview.pl  
+ 403 Forbidden: HEAD /cgi-bin/viewlogs.pl  
+ 403 Forbidden: HEAD /cgi-bin/wwwstats.pl  
+ 404 File Not Found: HEAD /admin/  
+ 404 File Not Found: HEAD /Admin\_files/  
+ 404 File Not Found: HEAD /DMR/  
+ 404 File Not Found: HEAD /StoreDB/  
+ 404 File Not Found: HEAD /Web\_store/  
+ 404 File Not Found: HEAD /access/  
+ 404 File Not Found: HEAD /account/  
+ 404 File Not Found: HEAD /accounting/  
+ 404 File Not Found: HEAD /administrator/  
+ 404 File Not Found: HEAD /app/  
+ 404 File Not Found: HEAD /archive/  
+ 404 File Not Found: HEAD /asp/  
+ 404 File Not Found: HEAD /atc/  
+ 404 File Not Found: HEAD /backup/  
+ 404 File Not Found: HEAD /bak/  
+ 404 File Not Found: HEAD /beta/  
+ 404 File Not Found: HEAD /buy/  
+ 404 File Not Found: HEAD /buynow/  
+ 404 File Not Found: HEAD /c/  
+ 404 File Not Found: HEAD /cart/  
+ 404 File Not Found: HEAD /ccard/  
+ 404 File Not Found: HEAD /config/  
+ 404 File Not Found: HEAD /counter/  
+ 404 File Not Found: HEAD /credit/  
+ 404 File Not Found: HEAD /customers/  
+ 404 File Not Found: HEAD /dat/  
+ 404 File Not Found: HEAD /data/  
+ 404 File Not Found: HEAD /db/  
+ 404 File Not Found: HEAD /dbase/  
+ 404 File Not Found: HEAD /doc-html/  
+ 404 File Not Found: HEAD /down/  
+ 404 File Not Found: HEAD /download/  
+ 404 File Not Found: HEAD /downloads/  
+ 404 File Not Found: HEAD /employees/  
+ 404 File Not Found: HEAD /exe/  
+ 404 File Not Found: HEAD /file/  
+ 404 File Not Found: HEAD /files/  
+ 404 File Not Found: HEAD /forum/  
+ 404 File Not Found: HEAD /fpadmin/  
+ 404 File Not Found: HEAD /ftp/  
+ 404 File Not Found: HEAD /guestbook/  
+ 404 File Not Found: HEAD /guests/  
+ 404 File Not Found: HEAD /home/  
+ 404 File Not Found: HEAD /htdocs/  
+ 404 File Not Found: HEAD /html/  
+ 404 File Not Found: HEAD /ibill/  
+ 404 File Not Found: HEAD /idea/  
+ 404 File Not Found: HEAD /ideas/

.....  
+ 404 File Not Found: HEAD /incoming/  
+ 404 File Not Found: HEAD /info/  
+ 404 File Not Found: HEAD /install/  
+ 404 File Not Found: HEAD /intranet/  
+ 404 File Not Found: HEAD /jave/  
+ 404 File Not Found: HEAD /jdbc/  
+ 404 File Not Found: HEAD /lib/  
+ 404 File Not Found: HEAD /library/  
+ 404 File Not Found: HEAD /login/  
+ 404 File Not Found: HEAD /mail/  
+ 404 File Not Found: HEAD /mall\_log\_files/  
+ 404 File Not Found: HEAD /manual/  
+ 404 File Not Found: HEAD /marketing/  
+ 404 File Not Found: HEAD /mysql/  
+ 404 File Not Found: HEAD /new/  
+ 404 File Not Found: HEAD /odbc/  
+ 404 File Not Found: HEAD /old/  
+ 404 File Not Found: HEAD /oracle/  
+ 404 File Not Found: HEAD /order/  
+ 404 File Not Found: HEAD /outgoing/  
+ 404 File Not Found: HEAD /pages/  
+ 404 File Not Found: HEAD /passwords/  
+ 404 File Not Found: HEAD /perl/  
+ 404 File Not Found: HEAD /private/  
+ 404 File Not Found: HEAD /pub/  
+ 404 File Not Found: HEAD /public/  
+ 404 File Not Found: HEAD /purchase/  
+ 404 File Not Found: HEAD /purchases/  
+ 404 File Not Found: HEAD /pw/  
+ 404 File Not Found: HEAD /register/  
+ 404 File Not Found: HEAD /registered/  
+ 404 File Not Found: HEAD /reseller/  
+ 404 File Not Found: HEAD /retail/  
+ 404 File Not Found: HEAD /root/  
+ 404 File Not Found: HEAD /sales/  
+ 404 File Not Found: HEAD /search/  
+ 404 File Not Found: HEAD /sell/  
+ 404 File Not Found: HEAD /setup/  
+ 404 File Not Found: HEAD /shop/  
+ 404 File Not Found: HEAD /shopper/  
+ 404 File Not Found: HEAD /site/iissamples/  
+ 404 File Not Found: HEAD /software/  
+ 404 File Not Found: HEAD /source/  
+ 404 File Not Found: HEAD /sql/  
+ 404 File Not Found: HEAD /store/  
+ 404 File Not Found: HEAD /support/  
+ 404 File Not Found: HEAD /temp/  
+ 404 File Not Found: HEAD /test/  
+ 404 File Not Found: HEAD /test-cgi/  
+ 404 File Not Found: HEAD /tmp/  
+ 200 OK: HEAD /tools/  
+ 404 File Not Found: HEAD /tree/  
+ 404 File Not Found: HEAD /updates/  
+ 404 File Not Found: HEAD /usage/  
+ 404 File Not Found: HEAD /user/  
+ 404 File Not Found: HEAD /users/  
+ 404 File Not Found: HEAD /web/

.....

```
+ 404 File Not Found: HEAD /web800fo/
+ 404 File Not Found: HEAD /webadmin/
+ 404 File Not Found: HEAD /webboard/
+ 404 File Not Found: HEAD /webdata/
+ 404 File Not Found: HEAD /website/
+ 404 File Not Found: HEAD /www/
+ 404 File Not Found: HEAD /www-sql/
+ 404 File Not Found: HEAD /wwwjoin/
+ 404 File Not Found: HEAD /import/
+ 404 File Not Found: HEAD /zipfiles/
+ 404 File Not Found: HEAD /password.htm
+ 403 Forbidden: HEAD /cgi-bin/password.htm
+ 404 File Not Found: HEAD /password.html
+ 403 Forbidden: HEAD /cgi-bin/password.html
+ 404 File Not Found: HEAD /password.dat
+ 403 Forbidden: HEAD /cgi-bin/password.dat
+ 404 File Not Found: HEAD /password.data
+ 403 Forbidden: HEAD /cgi-bin/password.data
+ 404 File Not Found: HEAD /password.txt
+ 403 Forbidden: HEAD /cgi-bin/password.txt
+ 404 File Not Found: HEAD /password.asp
+ 403 Forbidden: HEAD /cgi-bin/password.asp
+ 404 File Not Found: HEAD /password.dbf
+ 403 Forbidden: HEAD /cgi-bin/password.dbf
+ 404 File Not Found: HEAD /password.ini
+ 403 Forbidden: HEAD /cgi-bin/password.ini
+ 404 File Not Found: HEAD /password.db
+ 403 Forbidden: HEAD /cgi-bin/password.db
+ 404 File Not Found: HEAD /password.cfg
+ 403 Forbidden: HEAD /cgi-bin/password.cfg
+ 404 File Not Found: HEAD /password.exe
+ 403 Forbidden: HEAD /cgi-bin/password.exe
+ 404 File Not Found: HEAD /password.htx
+ 403 Forbidden: HEAD /cgi-bin/password.htx
+ 404 File Not Found: HEAD /password.lst
+ 403 Forbidden: HEAD /cgi-bin/password.lst
+ 404 File Not Found: HEAD /password.cgi
+ 403 Forbidden: HEAD /cgi-bin/password.cgi
+ 404 File Not Found: HEAD /password.pl
+ 403 Forbidden: HEAD /cgi-bin/password.pl
+ 404 File Not Found: HEAD /password.php3
+ 403 Forbidden: HEAD /cgi-bin/password.php3
+ 404 File Not Found: HEAD /passwords.htm
+ 403 Forbidden: HEAD /cgi-bin/passwords.htm
+ 404 File Not Found: HEAD /passwords.html
+ 403 Forbidden: HEAD /cgi-bin/passwords.html
+ 404 File Not Found: HEAD /passwords.dat
+ 403 Forbidden: HEAD /cgi-bin/passwords.dat
+ 404 File Not Found: HEAD /passwords.data
+ 403 Forbidden: HEAD /cgi-bin/passwords.data
+ 404 File Not Found: HEAD /passwords.txt
+ 403 Forbidden: HEAD /cgi-bin/passwords.txt
+ 404 File Not Found: HEAD /passwords.asp
+ 403 Forbidden: HEAD /cgi-bin/passwords.asp
+ 404 File Not Found: HEAD /passwords.dbf
+ 403 Forbidden: HEAD /cgi-bin/passwords.dbf
+ 404 File Not Found: HEAD /passwords.ini
```

.....  
+ 403 Forbidden: HEAD /cgi-bin/passwords.ini  
+ 404 File Not Found: HEAD /passwords.db  
+ 403 Forbidden: HEAD /cgi-bin/passwords.db  
+ 404 File Not Found: HEAD /passwords.cfg  
+ 403 Forbidden: HEAD /cgi-bin/passwords.cfg  
+ 404 File Not Found: HEAD /passwords.exe  
+ 403 Forbidden: HEAD /cgi-bin/passwords.exe  
+ 404 File Not Found: HEAD /passwords.htx  
+ 403 Forbidden: HEAD /cgi-bin/passwords.htx  
+ 404 File Not Found: HEAD /passwords.lst  
+ 403 Forbidden: HEAD /cgi-bin/passwords.lst  
+ 404 File Not Found: HEAD /passwords.cgi  
+ 403 Forbidden: HEAD /cgi-bin/passwords.cgi  
+ 404 File Not Found: HEAD /passwords.pl  
+ 403 Forbidden: HEAD /cgi-bin/passwords.pl  
+ 404 File Not Found: HEAD /passwords.php3  
+ 403 Forbidden: HEAD /cgi-bin/passwords.php3  
+ 404 File Not Found: HEAD /pass.htm  
+ 403 Forbidden: HEAD /cgi-bin/pass.htm  
+ 404 File Not Found: HEAD /pass.html  
+ 403 Forbidden: HEAD /cgi-bin/pass.html  
+ 404 File Not Found: HEAD /pass.dat  
+ 403 Forbidden: HEAD /cgi-bin/pass.dat  
+ 404 File Not Found: HEAD /pass.data  
+ 403 Forbidden: HEAD /cgi-bin/pass.data  
+ 404 File Not Found: HEAD /pass.txt  
+ 403 Forbidden: HEAD /cgi-bin/pass.txt  
+ 404 File Not Found: HEAD /pass.asp  
+ 403 Forbidden: HEAD /cgi-bin/pass.asp  
+ 404 File Not Found: HEAD /pass.dbf  
+ 403 Forbidden: HEAD /cgi-bin/pass.dbf  
+ 404 File Not Found: HEAD /pass.ini  
+ 403 Forbidden: HEAD /cgi-bin/pass.ini  
+ 404 File Not Found: HEAD /pass.db  
+ 403 Forbidden: HEAD /cgi-bin/pass.db  
+ 404 File Not Found: HEAD /pass.cfg  
+ 403 Forbidden: HEAD /cgi-bin/pass.cfg  
+ 404 File Not Found: HEAD /pass.exe  
+ 403 Forbidden: HEAD /cgi-bin/pass.exe  
+ 404 File Not Found: HEAD /pass.htx  
+ 403 Forbidden: HEAD /cgi-bin/pass.htx  
+ 404 File Not Found: HEAD /pass.lst  
+ 403 Forbidden: HEAD /cgi-bin/pass.lst  
+ 404 File Not Found: HEAD /pass.cgi  
+ 403 Forbidden: HEAD /cgi-bin/pass.cgi  
+ 404 File Not Found: HEAD /pass.pl  
+ 403 Forbidden: HEAD /cgi-bin/pass.pl  
+ 404 File Not Found: HEAD /pass.php3  
+ 403 Forbidden: HEAD /cgi-bin/pass.php3  
+ 404 File Not Found: HEAD /users.htm  
+ 403 Forbidden: HEAD /cgi-bin/users.htm  
+ 404 File Not Found: HEAD /users.html  
+ 403 Forbidden: HEAD /cgi-bin/users.html  
+ 404 File Not Found: HEAD /users.dat  
+ 403 Forbidden: HEAD /cgi-bin/users.dat  
+ 404 File Not Found: HEAD /users.data  
+ 403 Forbidden: HEAD /cgi-bin/users.data

.....

- + 404 File Not Found: HEAD /users.txt
- + 403 Forbidden: HEAD /cgi-bin/users.txt
- + 404 File Not Found: HEAD /users.asp
- + 403 Forbidden: HEAD /cgi-bin/users.asp
- + 404 File Not Found: HEAD /users.dbf
- + 403 Forbidden: HEAD /cgi-bin/users.dbf
- + 404 File Not Found: HEAD /users.ini
- + 403 Forbidden: HEAD /cgi-bin/users.ini
- + 404 File Not Found: HEAD /users.db
- + 403 Forbidden: HEAD /cgi-bin/users.db
- + 404 File Not Found: HEAD /users.cfg
- + 403 Forbidden: HEAD /cgi-bin/users.cfg
- + 404 File Not Found: HEAD /users.exe
- + 403 Forbidden: HEAD /cgi-bin/users.exe
- + 404 File Not Found: HEAD /users.htx
- + 403 Forbidden: HEAD /cgi-bin/users.htx
- + 404 File Not Found: HEAD /users.lst
- + 403 Forbidden: HEAD /cgi-bin/users.lst
- + 404 File Not Found: HEAD /users.cgi
- + 403 Forbidden: HEAD /cgi-bin/users.cgi
- + 404 File Not Found: HEAD /users.pl
- + 403 Forbidden: HEAD /cgi-bin/users.pl
- + 404 File Not Found: HEAD /users.php3
- + 403 Forbidden: HEAD /cgi-bin/users.php3
- + 404 File Not Found: HEAD /clients.htm
- + 403 Forbidden: HEAD /cgi-bin/clients.htm
- + 404 File Not Found: HEAD /clients.html
- + 403 Forbidden: HEAD /cgi-bin/clients.html
- + 404 File Not Found: HEAD /clients.dat
- + 403 Forbidden: HEAD /cgi-bin/clients.dat
- + 404 File Not Found: HEAD /clients.data
- + 403 Forbidden: HEAD /cgi-bin/clients.data
- + 404 File Not Found: HEAD /clients.txt
- + 403 Forbidden: HEAD /cgi-bin/clients.txt
- + 404 File Not Found: HEAD /clients.asp
- + 403 Forbidden: HEAD /cgi-bin/clients.asp
- + 404 File Not Found: HEAD /clients.dbf
- + 403 Forbidden: HEAD /cgi-bin/clients.dbf
- + 404 File Not Found: HEAD /clients.ini
- + 403 Forbidden: HEAD /cgi-bin/clients.ini
- + 404 File Not Found: HEAD /clients.db
- + 403 Forbidden: HEAD /cgi-bin/clients.db
- + 404 File Not Found: HEAD /clients.cfg
- + 403 Forbidden: HEAD /cgi-bin/clients.cfg
- + 404 File Not Found: HEAD /clients.exe
- + 403 Forbidden: HEAD /cgi-bin/clients.exe
- + 404 File Not Found: HEAD /clients.htx
- + 403 Forbidden: HEAD /cgi-bin/clients.htx
- + 404 File Not Found: HEAD /clients.lst
- + 403 Forbidden: HEAD /cgi-bin/clients.lst
- + 404 File Not Found: HEAD /clients.cgi
- + 403 Forbidden: HEAD /cgi-bin/clients.cgi
- + 404 File Not Found: HEAD /clients.pl
- + 403 Forbidden: HEAD /cgi-bin/clients.pl
- + 404 File Not Found: HEAD /clients.php3
- + 403 Forbidden: HEAD /cgi-bin/clients.php3
- + 404 File Not Found: HEAD /login.htm



.....

- + 403 Forbidden: HEAD /cgi-bin/login.htm
- + 404 File Not Found: HEAD /login.html
- + 403 Forbidden: HEAD /cgi-bin/login.html
- + 404 File Not Found: HEAD /login.dat
- + 403 Forbidden: HEAD /cgi-bin/login.dat
- + 404 File Not Found: HEAD /login.data
- + 403 Forbidden: HEAD /cgi-bin/login.data
- + 404 File Not Found: HEAD /login.txt
- + 403 Forbidden: HEAD /cgi-bin/login.txt
- + 404 File Not Found: HEAD /login.asp
- + 403 Forbidden: HEAD /cgi-bin/login.asp
- + 404 File Not Found: HEAD /login.dbf
- + 403 Forbidden: HEAD /cgi-bin/login.dbf
- + 404 File Not Found: HEAD /login.ini
- + 403 Forbidden: HEAD /cgi-bin/login.ini
- + 404 File Not Found: HEAD /login.db
- + 403 Forbidden: HEAD /cgi-bin/login.db
- + 404 File Not Found: HEAD /login.cfg
- + 403 Forbidden: HEAD /cgi-bin/login.cfg
- + 404 File Not Found: HEAD /login.exe
- + 403 Forbidden: HEAD /cgi-bin/login.exe
- + 404 File Not Found: HEAD /login.htx
- + 403 Forbidden: HEAD /cgi-bin/login.htx
- + 404 File Not Found: HEAD /login.lst
- + 403 Forbidden: HEAD /cgi-bin/login.lst
- + 404 File Not Found: HEAD /login.cgi
- + 404 File Not Found: HEAD /login.pl
- + 404 File Not Found: HEAD /login.php3
- + 403 Forbidden: HEAD /cgi-bin/login.php3
- + 404 File Not Found: HEAD /admin.htm
- + 403 Forbidden: HEAD /cgi-bin/admin.htm
- + 404 File Not Found: HEAD /admin.html
- + 403 Forbidden: HEAD /cgi-bin/admin.html
- + 404 File Not Found: HEAD /admin.dat
- + 403 Forbidden: HEAD /cgi-bin/admin.dat
- + 404 File Not Found: HEAD /admin.data
- + 403 Forbidden: HEAD /cgi-bin/admin.data
- + 404 File Not Found: HEAD /admin.txt
- + 403 Forbidden: HEAD /cgi-bin/admin.txt
- + 404 File Not Found: HEAD /admin.asp
- + 403 Forbidden: HEAD /cgi-bin/admin.asp
- + 404 File Not Found: HEAD /admin.dbf
- + 403 Forbidden: HEAD /cgi-bin/admin.dbf
- + 404 File Not Found: HEAD /admin.ini
- + 403 Forbidden: HEAD /cgi-bin/admin.ini
- + 404 File Not Found: HEAD /admin.db
- + 403 Forbidden: HEAD /cgi-bin/admin.db
- + 404 File Not Found: HEAD /admin.cfg
- + 403 Forbidden: HEAD /cgi-bin/admin.cfg
- + 404 File Not Found: HEAD /admin.exe
- + 403 Forbidden: HEAD /cgi-bin/admin.exe
- + 404 File Not Found: HEAD /admin.htx
- + 403 Forbidden: HEAD /cgi-bin/admin.htx
- + 404 File Not Found: HEAD /admin.lst
- + 403 Forbidden: HEAD /cgi-bin/admin.lst
- + 404 File Not Found: HEAD /admin.cgi
- + 403 Forbidden: HEAD /cgi-bin/admin.cgi

```
.....
+ 404 File Not Found: HEAD /admin.pl
+ 403 Forbidden: HEAD /cgi-bin/admin.pl
+ 404 File Not Found: HEAD /admin.php3
+ 404 File Not Found: HEAD /store.htm
+ 403 Forbidden: HEAD /cgi-bin/store.htm
+ 404 File Not Found: HEAD /store.html
+ 403 Forbidden: HEAD /cgi-bin/store.html
+ 404 File Not Found: HEAD /store.dat
+ 403 Forbidden: HEAD /cgi-bin/store.dat
+ 404 File Not Found: HEAD /store.data
+ 403 Forbidden: HEAD /cgi-bin/store.data
+ 404 File Not Found: HEAD /store.txt
+ 403 Forbidden: HEAD /cgi-bin/store.txt
+ 404 File Not Found: HEAD /store.asp
+ 403 Forbidden: HEAD /cgi-bin/store.asp
+ 404 File Not Found: HEAD /store.dbf
+ 403 Forbidden: HEAD /cgi-bin/store.dbf
+ 404 File Not Found: HEAD /store.ini
+ 403 Forbidden: HEAD /cgi-bin/store.ini
+ 404 File Not Found: HEAD /store.db
+ 403 Forbidden: HEAD /cgi-bin/store.db
+ 404 File Not Found: HEAD /store.cfg
+ 403 Forbidden: HEAD /cgi-bin/store.cfg
+ 404 File Not Found: HEAD /store.exe
+ 403 Forbidden: HEAD /cgi-bin/store.exe
+ 404 File Not Found: HEAD /store.htx
+ 403 Forbidden: HEAD /cgi-bin/store.htx
+ 404 File Not Found: HEAD /store.lst
+ 403 Forbidden: HEAD /cgi-bin/store.lst
+ 404 File Not Found: HEAD /store.cgi
+ 403 Forbidden: HEAD /cgi-bin/store.cgi
+ 404 File Not Found: HEAD /store.pl
+ 403 Forbidden: HEAD /cgi-bin/store.pl
+ 404 File Not Found: HEAD /store.php3
+ 403 Forbidden: HEAD /cgi-bin/store.php3
+ 404 File Not Found: HEAD /passwd
+ 403 Forbidden: HEAD /cgi-bin/passwd
+ 404 File Not Found: HEAD /passwd.txt
+ 403 Forbidden: HEAD /cgi-bin/passwd.txt
+ 404 File Not Found: HEAD /password
+ 403 Forbidden: HEAD /cgi-bin/password
+ 404 File Not Found: HEAD /status/
```

*Engineer's Note: The remainder of the data are the script outputs from logging into the machine to perform a host-based assessment. Unless you're really curious, there's not much down there of particular note.*

```
jpurvis@172.16.2.1's password:
Last login: Fri Nov 17 15:22:47 2000 from cerberus.XXX.XXX
Sun Microsystems Inc. SunOS 5.6 Generic August 1997
Sun Microsystems Inc. SunOS 5.6 Generic August 1997
kumo$
uname -a
kumo$ kumo$ uname -a
SunOS kumo 5.6 Generic sun4u sparc SUNW,Ultra-1
kumo$ su -
Password:
```

```

.....
Sun Microsystems Inc.   SunOS 5.6           Generic August 1997
You have mail.
# /usr/sbin/arp -a
Net to Media Table
Device   IP Address                Mask           Flags   Phys Addr
-----
le0      kuko-dmz                  255.255.255.255      08:00:20:9a:25:78
le0      172.16.2.47              255.255.255.255      00:10:a4:ed:86:f4
le0      kumo                      255.255.255.255      SP      08:00:20:7c:50:84
le0      BASE-ADDRESS.MCAST.NET 240.0.0.0           SM      01:00:5e:00:00:00

# /usr/sbin/auditconfig -chkconf
auditconfig: auditon(2) failed.
auditconfig: error = Invalid argument(22)

# /usr/sbin/auditconfig -getcond
auditconfig: auditon(2) failed.
auditconfig: error = Invalid argument(22)

# /usr/sbin/auditconfig -getpolicy
auditconfig: auditon(2) failed.
auditconfig: error = Invalid argument(22)

# df
/                (/dev/dsk/c0t0d0s0 ): 108886 blocks   44142 files
/usr             (/dev/dsk/c0t0d0s6 ): 209144 blocks   252689 files
/proc           (/proc              ): 0 blocks       916 files
/dev/fd         (fd                 ): 0 blocks       0 files
/var            (/dev/dsk/c0t0d0s1 ): 522956 blocks   146224 files
/opt            (/dev/dsk/c0t0d0s5 ): 666556 blocks   384353 files
/ftp02         (/dev/dsk/c0t1d0s6 ): 425766 blocks   489123 files
/ftp01         (/dev/dsk/c0t1d0s7 ): 122018 blocks   489071 files
/data          (/dev/dsk/c0t2d0s7 ): 600688 blocks   483972 files
/tmp           (swap               ): 541232 blocks   9598 files

# eeprom security-mode
security-mode=none

# env
HOME=/
HZ=
LOGNAME=root
PATH=/usr/local/bin:/bin:/usr/bin:/usr/sbin:/usr/ucb:/etc
SHELL=/sbin/sh
TERM=xterm-color
TZ=US/Pacific

# ifconfig -a
lo0: flags=849<UP,LOOPBACK,RUNNING,MULTICAST> mtu 8232
    inet 127.0.0.1 netmask ff000000
le0: flags=863<UP,BROADCAST,NOTRAILERS,RUNNING,MULTICAST> mtu 1500
    inet 172.16.2.1 netmask ffffffff broadcast 172.16.2.255
    ether 8:0:20:7c:50:84

# last
jpurvis pts/3          172.16.2.47      Fri Nov 17 15:43  still logged in
jpurvis pts/3          cerberus.XXX.XXX Fri Nov 17 15:22 - 15:24  (00:01)

```

```

-----
X41      ftp      cerberus.XXX.XXX Tue Nov 14 15:52 - 15:54 (00:02)
X41      ftp      cerberus.XXX.XXX Tue Nov 14 15:48 - 15:51 (00:03)
X41      ftp      thorn.brooks.X41 Tue Nov 14 15:46 - 15:48 (00:02)
X41      ftp      cerberus.XXX.XXX Tue Nov 14 15:31 - 15:32 (00:01)
jpurvis  pts/3      cerberus.XXX.XXX Tue Nov 14 15:19 - 16:47 (01:28)
internal ftp      fw.XXXXXXXXXXXXX.c Tue Oct 24 15:22 - 15:24 (00:02)
internal ftp      fw.XXXXXXXXXXXXX.c Tue Oct 24 15:21 - 15:22 (00:01)
internal ftp      cerberus.XXX.XXX Tue Oct 24 13:00 - 13:01 (00:00)
internal ftp      cerberus.XXX.XXX Tue Oct 24 12:36 - 12:57 (00:21)
internal ftp      cerberus.XXX.XXX Tue Oct 24 12:35 - 12:35 (00:00)
jpurvis  pts/3      cerberus.XXX.XXX Tue Oct 24 12:25 - 14:47 (02:21)
root     console   :0           Tue Oct 24 12:07  still logged in
root     console   :0           Fri Aug 18 09:25 - 09:33 (00:08)
root     console   :0           Fri Aug 18 09:12 - 09:13 (00:00)
root     console   :0           Mon Jul 10 15:09 - 15:12 (00:02)
XXXXXX40 pts/1      cerberus.XXX.XXX Sat May 6 15:59 - 16:01 (00:02)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri May 5 12:51 - 16:09 (03:18)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri May 5 12:48 - 12:50 (00:02)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri May 5 12:05 - 12:05 (00:00)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri May 5 10:51 - 11:12 (00:20)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri May 5 10:09 - 10:18 (00:09)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri May 5 10:07 - 10:09 (00:01)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri May 5 10:01 - 10:06 (00:04)
root     console   Fri May 5 09:21 - 10:00 (00:38)
root     console   :0           Fri May 5 09:20 - 09:21 (00:00)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri Apr 28 15:46 - 15:58 (00:11)
reboot   system boot Tue Apr 25 21:44
root     console   :0           Tue Apr 25 16:54 - 16:57 (00:03)
XXXXXX40 pts/1      cerberus.XXX.XXX Thu Apr 20 09:53 - 09:57 (00:03)
XXXXXX40 pts/1      cerberus.XXX.XXX Mon Mar 27 15:14 - 15:39 (00:25)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri Mar 24 12:21 - 12:24 (00:03)
XXXXXX40 pts/1      cerberus.XXX.XXX Thu Mar 23 14:21 - 16:45 (02:23)
XXXXXX40 pts/2      cerberus.XXX.XXX Wed Mar 22 11:06 - 12:51 (01:45)
XXXXXX40 pts/1      cerberus.XXX.XXX Wed Mar 22 10:46 - 12:51 (02:04)
XXXXXX40 pts/1      cerberus.XXX.XXX Tue Mar 21 10:46 - 13:32 (02:46)
XXXXXX40 pts/2      cerberus.XXX.XXX Mon Mar 20 12:36 - 14:06 (01:30)
XXXXXX40 pts/1      cerberus.XXX.XXX Mon Mar 20 10:30 - 13:45 (03:14)
XXXXXX40 pts/2      cerberus.XXX.XXX Fri Mar 10 11:32 - 11:49 (00:17)
XXXXXX40 pts/2      cerberus.XXX.XXX Fri Mar 10 11:19 - 11:20 (00:00)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri Mar 10 11:05 - 12:50 (01:45)
XXXXXX40 pts/2      cerberus.XXX.XXX Fri Mar 10 10:53 - 11:09 (00:16)
XXXXXX40 pts/1      cerberus.XXX.XXX Fri Mar 10 10:51 - 11:04 (00:12)
XXXXXX40 pts/1      cerberus.XXX.XXX Wed Mar 8 10:36 - 13:37 (03:01)
XXXXXX40 pts/2      cerberus.XXX.XXX Tue Mar 7 14:13 - 14:27 (00:13)
XXXXXX40 pts/1      cerberus.XXX.XXX Tue Mar 7 14:11 - 14:28 (00:16)
XXXXXX40 pts/1      cerberus.XXX.XXX Tue Feb 22 14:27 - 14:29 (00:01)
reboot   system boot Sun Feb 20 16:51
reboot   system boot Sun Feb 20 16:16
XXXXXX40 pts/4      cerberus.XXX.XXX Fri Feb 18 09:36 - 09:58 (00:21)
XXXXXX40 pts/4      cerberus.XXX.XXX Wed Feb 16 14:28 - 15:08 (00:40)
XXXXXX40 pts/4      kuko-dmz      Wed Feb 16 11:46 - 11:48 (00:01)
XXXXXX40 pts/4      kuko-dmz      Wed Feb 16 11:39 - 11:43 (00:03)
XXXXXX40 pts/4      cerberus.XXX.XXX Mon Jan 24 11:30 - 11:33 (00:02)
XXXXXX40 pts/4      cerberus.XXX.XXX Mon Jan 24 11:25 - 11:30 (00:04)
XXXXXXXX6 ftp      cerberus.XXX.XXX Sat Jan 23 15:35 - 15:36 (00:00)
XXXXXXXX6 pts/1      cerberus.XXX.XXX Fri Jan 22 15:56 - 16:38 (00:41)
XXXXXXXX6 ftp      cerberus.XXX.XXX Fri Jan 22 10:09 - 10:11 (00:02)

```

XXXXXXX6	pts/1	cerberus.XXX.XXX	Fri	Jan	22	08:24	-	08:32	(00:08)
XXXXX31	ftp	cerberus.XXX.XXX	Thu	Jan	21	13:54	-	14:05	(00:10)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Tue	Jan	19	20:37	-	20:41	(00:03)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Tue	Jan	19	20:37	-	20:41	(00:03)
XXXXX31	ftp	cerberus.XXX.XXX	Tue	Jan	19	14:35	-	14:51	(00:15)
XXXXX31	ftp	cerberus.XXX.XXX	Tue	Jan	19	11:10	-	11:13	(00:02)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:46	-	00:47	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:45	-	00:46	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:41	-	00:42	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:41	-	00:41	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:37	-	00:38	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:37	-	00:37	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:36	-	00:37	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:33	-	00:33	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:30	-	00:32	(00:02)
testacct	pts/2	cerberus.XXX.XXX	Tue	Jan	19	00:26	-	00:30	(00:03)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Tue	Jan	19	00:15	-	00:47	(00:31)
XXXXXXX6	ftp	cerberus.XXX.XXX	Sun	Jan	17	20:33	-	20:33	(00:00)
XXXXXXX6	ftp	192.168.84.164	Sun	Jan	17	20:32	-	20:32	(00:00)
XXXXXXX6	pts/2	cerberus.XXX.XXX	Sun	Jan	17	12:32	-	12:34	(00:02)
testacct	pts/2	cerberus.XXX.XXX	Sun	Jan	17	12:30	-	12:30	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Sun	Jan	17	11:35	-	11:36	(00:00)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Sun	Jan	17	11:34	-	13:46	(02:11)
testacct	pts/2	cerberus.XXX.XXX	Sun	Jan	17	00:49	-	00:49	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Sun	Jan	17	00:47	-	00:47	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Sun	Jan	17	00:41	-	00:41	(00:00)
testacct	pts/2	cerberus.XXX.XXX	Sun	Jan	17	00:37	-	00:40	(00:03)
testacct	pts/2	cerberus.XXX.XXX	Sun	Jan	17	00:15	-	00:16	(00:01)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Sun	Jan	17	00:14	-	00:53	(00:39)
XXXXXXX6	ftp	cerberus.XXX.XXX	Fri	Jan	15	11:42	-	11:42	(00:00)
XXXXXXX6	ftp	192.168.84.164	Fri	Jan	15	11:42	-	11:42	(00:00)
XXXXXXX6	pts/2	cerberus.XXX.XXX	Fri	Jan	15	10:57	-	11:40	(00:42)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Fri	Jan	15	10:57	-	11:40	(00:43)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Fri	Jan	15	10:47	-	10:55	(00:08)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Fri	Jan	15	10:24	-	10:47	(00:23)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Wed	Jan	13	22:45	-	22:45	(00:00)
XXXXXXX6	ftp	cerberus.XXX.XXX	Tue	Jan	12	12:28	-	12:29	(00:00)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Tue	Jan	12	12:28	-	12:28	(00:00)
XXXXXXX6	ftp	192.168.84.164	Tue	Jan	12	12:27	-	12:27	(00:00)
XXXXXXX6	ftp	192.168.84.164	Tue	Jan	12	12:25	-	12:26	(00:00)
XXXXXXX6	pts/1	cerberus.XXX.XXX	Tue	Jan	12	11:44	-	11:52	(00:07)
XXXXXXX6	ftp	cerberus.XXX.XXX	Tue	Jan	12	11:44	-	11:45	(00:01)
XXXXXXX6	ftp	cerberus.XXX.XXX	Tue	Jan	12	11:37	-	11:38	(00:00)
XXXXXXX6	ftp	cerberus.XXX.XXX	Tue	Jan	12	09:53	-	09:55	(00:02)
XXXXXXX6	ftp	cerberus.XXX.XXX	Tue	Jan	12	09:52	-	09:53	(00:00)
XXXXXXX6	pts/5	cerberus.XXX.XXX	Tue	Jan	12	09:49	-	12:27	(02:38)
XXXXXXX6	ftp	192.168.84.165	Mon	Jan	11	16:03	-	16:03	(00:00)
XXXXXXX6	ftp	192.168.84.164	Mon	Jan	11	16:02	-	16:02	(00:00)
XXXXXXX6	pts/7	cerberus.XXX.XXX	Mon	Jan	11	15:51	-	16:00	(00:09)
XXXXXXX6	ftp	192.168.84.165	Mon	Jan	11	15:45	-	15:45	(00:00)
XXXXXXX6	ftp	192.168.84.165	Mon	Jan	11	15:45	-	15:45	(00:00)
XXXXXXX6	ftp	192.168.84.164	Mon	Jan	11	15:45	-	15:45	(00:00)
XXXXXXX6	ftp	192.168.84.195	Mon	Jan	11	15:05	-	15:05	(00:00)
XXXXXXX6	ftp	192.168.84.164	Mon	Jan	11	15:03	-	15:03	(00:00)
XXXXXXX6	pts/6	cerberus.XXX.XXX	Mon	Jan	11	14:14	-	16:26	(02:11)
XXXXXXX6	ftp	cerberus.XXX.XXX	Mon	Jan	11	14:06	-	14:06	(00:00)
XXXXXXX6	ftp	cerberus.XXX.XXX	Mon	Jan	11	12:06	-	12:23	(00:16)

```

-----
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Jan 11 12:04 - 12:06 (00:01)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Mon Jan 11 11:56 - 16:39 (04:42)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Jan 11 10:09 - 10:25 (00:15)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Mon Jan 11 09:55 - 10:01 (00:05)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Jan 11 09:48 - 10:08 (00:19)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Jan 11 09:12 - 09:13 (00:00)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Mon Jan 11 08:41 - 09:47 (01:05)
XXXXXXXX12 pts/5 cerberus.XXX.XXX Fri Jan 8 14:18 - 14:23 (00:05)
XXXXXXXX6 ftp 192.168.84.164 Fri Jan 8 14:04 - 14:05 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri Jan 8 13:35 - 13:43 (00:07)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Fri Jan 8 13:10 - 13:35 (00:24)
XXXXXXXX12 pts/5 cerberus.XXX.XXX Fri Jan 8 12:27 - 12:32 (00:04)
XXXXXXXX12 pts/5 cerberus.XXX.XXX Fri Jan 8 12:27 - 12:27 (00:00)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Fri Jan 8 12:24 - 12:27 (00:02)
asdfXXX1 ftp cerberus.XXX.XXX Thu Jan 7 09:58 - 10:07 (00:09)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Thu Jan 7 09:24 - 09:35 (00:11)
asdfXXX1 ftp cerberus.XXX.XXX Wed Jan 6 16:41 - 16:44 (00:02)
asdfXXX1 ftp cerberus.XXX.XXX Wed Jan 6 16:02 - 16:03 (00:01)
XXXXX31 ftp cerberus.XXX.XXX Wed Jan 6 11:31 - 11:44 (00:13)
asdfXXX1 pts/5 cerberus.XXX.XXX Wed Jan 6 08:25 - 08:27 (00:02)
asdfXXX1 ftp cerberus.XXX.XXX Tue Jan 5 14:06 - 14:11 (00:05)
XXXXX31 ftp 192.168.173.3 Tue Jan 5 08:28 - 08:54 (00:26)
XXXXX31 ftp 192.168.173.3 Tue Jan 5 08:18 - 08:27 (00:08)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Tue Jan 5 00:39 - 00:46 (00:07)
XXXXXXXX6 ftp cerberus.XXX.XXX Tue Jan 5 00:37 - 00:46 (00:08)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Mon Jan 4 22:06 - 22:10 (00:03)
XXXXXXXX6 ftp 10k.singingbeagl Mon Jan 4 15:41 - 15:41 (00:00)
XXXXXXXX6 ftp 10k.singingbeagl Mon Jan 4 15:40 - 15:40 (00:00)
XXXXXXXX6 ftp 10k.singingbeagl Mon Jan 4 15:23 - 15:23 (00:00)
XXXXXXXX6 ftp kuki-dmz Mon Jan 4 15:22 - 15:22 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Jan 4 15:03 - 15:03 (00:00)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Mon Jan 4 14:02 - 16:41 (02:39)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Mon Jan 4 10:39 - 12:54 (02:14)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Mon Jan 4 10:19 - 12:53 (02:33)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Thu Dec 24 13:43 - 13:45 (00:01)
XXXXXXXX6 ftp 192.168.84.164 Thu Dec 24 13:37 - 13:37 (00:00)
XXXXXXXX6 ftp 192.168.84.164 Thu Dec 24 13:29 - 13:29 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Dec 24 13:29 - 13:29 (00:00)
XXXXXXXX6 ftp 192.168.84.164 Thu Dec 24 13:25 - 13:25 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Dec 24 13:24 - 13:24 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Dec 24 13:24 - 13:24 (00:00)
XXXXXXXX6 ftp 192.168.84.164 Thu Dec 24 11:39 - 11:40 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Dec 24 11:37 - 11:38 (00:00)
XXXXXXXX6 ftp 192.168.84.196 Thu Dec 24 09:25 - 09:25 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Dec 24 09:07 - 09:07 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Dec 24 09:05 - 09:07 (00:01)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Wed Dec 23 09:58 - 11:07 (01:08)
asdfXXX1 ftp cerberus.XXX.XXX Wed Dec 23 09:29 - 09:45 (00:16)
XXXXXXXX6 ftp cerberus.XXX.XXX Tue Dec 22 15:06 - 15:06 (00:00)
XXXXXXXX6 ftp kuki-dmz Tue Dec 22 15:04 - 15:05 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Tue Dec 22 14:55 - 14:55 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Tue Dec 22 13:11 - 13:11 (00:00)
XXXXXXXX6 ftp kuki-dmz Tue Dec 22 13:09 - 13:09 (00:00)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Tue Dec 22 12:28 - 12:30 (00:02)
asdfXXX1 pts/4 cerberus.XXX.XXX Mon Dec 21 08:00 - 08:00 (00:00)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Sat Dec 19 08:33 - 08:46 (00:13)
XXXXXXXX5 pts/4 cerberus.XXX.XXX Fri Dec 18 14:05 - 14:12 (00:07)

```

```

-----
asdfXXX1  ftp          cerberus.XXX.XXX Fri Dec 18 13:00 - 13:21 (00:21)
asdfXXX1  ftp          cerberus.XXX.XXX Fri Dec 18 12:50 - 12:56 (00:05)
asdfXXX1  ftp          cerberus.XXX.XXX Fri Dec 18 12:42 - 12:48 (00:05)
asdfXXX1  pts/4       cerberus.XXX.XXX Fri Dec 18 12:41 - 13:38 (00:57)
asdfXXX1  pts/4       cerberus.XXX.XXX Fri Dec 18 07:50 - 08:09 (00:19)
asdfXXX1  pts/4       cerberus.XXX.XXX Fri Dec 18 07:16 - 07:18 (00:01)
asdfXXX1  ftp          cerberus.XXX.XXX Thu Dec 17 13:46 - 14:02 (00:15)
asdfXXX1  pts/4       cerberus.XXX.XXX Thu Dec 17 12:59 - 15:03 (02:03)
XXXXXXXX6  pts/4       192.168.84.163   Thu Dec 17 11:07 - 11:08 (00:00)
XXXXXX31  ftp          XXXXX31.XXX.XXX Tue Dec 15 15:57 - 15:59 (00:02)
XXXXXX31  ftp          cerberus.XXX.XXX Tue Dec 15 15:55 - 15:55 (00:00)
XXXXXX31  ftp          XXXXX31.XXX.XXX Tue Dec 15 15:46 - 15:55 (00:08)
XXXXXX31  ftp          cerberus.XXX.XXX Tue Dec 15 15:29 - 15:37 (00:07)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Tue Dec 15 15:27 - 17:51 (02:24)
XXXXXXXX6  ftp          cerberus.XXX.XXX Tue Dec 15 15:26 - 15:29 (00:02)
XXXXXXXX4  pts/4       cerberus.XXX.XXX Mon Dec 14 16:35 - 17:00 (00:24)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Sun Dec 13 17:36 - 17:44 (00:07)
XXXXXXXX4  pts/4       cerberus.XXX.XXX Sat Dec 12 12:33 - 13:35 (01:01)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Thu Dec 10 23:18 - 01:18 (02:00)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Thu Dec 10 17:05 - 17:06 (00:01)
XXXXXXXX6  pts/5       cerberus.XXX.XXX Thu Dec 10 16:11 - 16:12 (00:01)
XXXXXXXX4  pts/4       cerberus.XXX.XXX Thu Dec 10 14:21 - 17:02 (02:41)
XXXXXXXX4  pts/4       cerberus.XXX.XXX Thu Dec 10 11:46 - 12:19 (00:32)
XXXXXXXX5  pts/4       cerberus.XXX.XXX Wed Dec  9 13:11 - 13:21 (00:09)
XXXXXXXX5  pts/4       cerberus.XXX.XXX Wed Dec  9 11:32 - 12:27 (00:54)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Wed Dec  9 09:47 - 09:48 (00:01)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Wed Dec  9 09:32 - 09:33 (00:01)
XXXXXXXX5  pts/4       cerberus.XXX.XXX Wed Dec  9 07:56 - 08:21 (00:25)
root      ftp          10k.singingbeagl Wed Dec  9 00:23 - 00:23 (00:00)
root      ftp          10k.singingbeagl Wed Dec  9 00:10 - 00:10 (00:00)
root      ftp          10k.singingbeagl Wed Dec  9 00:10 - 00:10 (00:00)
root      ftp          10k.singingbeagl Wed Dec  9 00:02 - 00:03 (00:00)
root      ftp          10k.singingbeagl Wed Dec  9 00:00 - 00:01 (00:00)
root      ftp          10k.singingbeagl Tue Dec  8 23:56 - 23:57 (00:00)
root      ftp          10k.singingbeagl Tue Dec  8 23:53 - 23:53 (00:00)
root      ftp          cerberus.XXX.XXX Tue Dec  8 23:47 - 23:47 (00:00)
root      ftp          cerberus.XXX.XXX Tue Dec  8 23:43 - 23:44 (00:00)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Tue Dec  8 23:15 - 00:58 (01:42)
XXXXXXXX5  pts/4       cerberus.XXX.XXX Tue Dec  8 21:04 - 21:17 (00:12)
XXXXXXXX6  pts/4       cerberus.XXX.XXX Thu Dec  3 10:28 - 10:29 (00:00)
XXXXXXXX6  ftp          192.168.84.195   Thu Dec  3 08:23 - 08:23 (00:00)
XXXXXXXX6  ftp          cerberus.XXX.XXX Thu Dec  3 08:22 - 08:23 (00:00)
XXXXXXXX6  ftp          192.168.84.195   Thu Dec  3 08:17 - 08:17 (00:00)
XXXXXXXX6  ftp          cerberus.XXX.XXX Thu Dec  3 08:16 - 08:16 (00:00)
root      console     :0                 Tue Dec  1 09:46 - 11:37 (42+01:50)
root      console     :0                 Mon Nov 30 16:05 - 16:16 (00:11)
reboot    system boot                                     Mon Nov 30 15:26
reboot    system boot                                     Mon Nov 30 15:22
reboot    system boot                                     Mon Nov 30 15:18
reboot    system boot                                     Mon Nov 30 15:10
XXXXXXXX5  pts/6       cerberus.XXX.XXX Mon Nov 30 13:29 - 13:29 (00:00)
XXXXXXXX6  pts/6       cerberus.XXX.XXX Sat Nov 28 12:12 - 12:12 (00:00)
XXXXXXXX6  ftp          172.16.1.100     Wed Nov 25 23:07 - 23:07 (00:00)
XXXXXXXX6  ftp          cerberus.XXX.XXX Wed Nov 25 23:06 - 23:07 (00:00)
asdfXXX1  pts/6       cerberus.XXX.XXX Tue Nov 24 14:08 - 14:09 (00:00)
XXXXXXXX6  ftp          172.16.1.253     Tue Nov 24 13:08 - 13:08 (00:00)
XXXXXXXX6  ftp          cerberus.XXX.XXX Tue Nov 24 10:50 - 10:50 (00:00)

```

```

-----
XXXXXXXX6 ftp kuki-dmz Tue Nov 24 10:48 - 10:48 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Tue Nov 24 10:20 - 12:22 (02:01)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Nov 23 17:09 - 17:09 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Nov 23 09:57 - 09:57 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Nov 23 00:01 - 00:05 (00:03)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sun Nov 22 23:17 - 23:20 (00:02)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Nov 21 00:33 - 02:45 (02:12)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Fri Nov 20 06:45 - 06:47 (00:01)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Thu Nov 19 21:11 - 21:13 (00:01)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Tue Nov 17 22:45 - 22:47 (00:01)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Nov 14 23:24 - 00:11 (00:47)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Nov 14 02:34 - 02:37 (00:02)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Nov 14 01:49 - 01:50 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Nov 14 00:38 - 00:42 (00:04)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Nov 14 00:27 - 00:33 (00:06)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri Nov 13 09:29 - 09:43 (00:13)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri Nov 13 09:28 - 09:29 (00:01)
XXXXX31 ftp 192.168.170.227 Thu Nov 12 11:05 - 11:07 (00:01)
XXXXX31 ftp 192.168.170.227 Thu Nov 12 11:04 - 11:05 (00:00)
XXXXX31 ftp 192.168.170.227 Thu Nov 12 11:00 - 11:02 (00:02)
XXXXX31 ftp 192.168.170.227 Thu Nov 12 11:00 - 11:02 (00:02)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Thu Nov 12 00:03 - 00:04 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Nov 11 15:24 - 15:56 (00:31)
XXXXXXXX6 ftp seki Wed Nov 11 14:59 - 15:00 (00:01)
XXXXXXXX6 ftp seki Wed Nov 11 14:58 - 14:59 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Nov 11 10:27 - 10:39 (00:12)
XXXXXXXX4 pts/6 cerberus.XXX.XXX Tue Nov 10 11:18 - 11:47 (00:28)
XXXXXXXX5 pts/6 cerberus.XXX.XXX Mon Nov 9 08:29 - 08:33 (00:04)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Nov 7 11:05 - 11:07 (00:02)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Fri Nov 6 09:34 - 09:36 (00:01)
XXXXXXXX6 ftp kuki-dmz Thu Nov 5 17:50 - 17:50 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Nov 5 17:49 - 17:49 (00:00)
XXXXXXXX6 pts/8 cerberus.XXX.XXX Thu Nov 5 12:02 - 13:55 (01:52)
XXXXXXXX5 pts/7 cerberus.XXX.XXX Thu Nov 5 11:38 - 12:17 (00:38)
XXXXXXXX5 pts/6 cerberus.XXX.XXX Thu Nov 5 10:31 - 12:42 (02:11)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Thu Nov 5 09:24 - 10:09 (00:45)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Nov 4 17:47 - 17:58 (00:11)
XXXXXXXX6 pts/7 cerberus.XXX.XXX Wed Nov 4 16:41 - 16:49 (00:08)
XXXXXXXX5 pts/6 cerberus.XXX.XXX Wed Nov 4 16:39 - 16:50 (00:11)
XXXXXXXX5 pts/6 cerberus.XXX.XXX Wed Nov 4 11:59 - 12:01 (00:01)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Nov 4 00:39 - 01:47 (01:07)
XXXXXXXX6 ftp kuki-dmz Mon Nov 2 11:02 - 11:02 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Nov 2 11:00 - 11:01 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Nov 2 09:29 - 10:24 (00:55)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Oct 28 20:13 - 20:18 (00:04)
XXXXX31 pts/6 XXXXX31.XXX.XXX Wed Oct 28 14:40 - 14:40 (00:00)
XXXXX31 pts/6 cerberus.XXX.XXX Wed Oct 28 14:39 - 14:39 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 26 19:20 - 19:27 (00:06)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Fri Oct 23 12:37 - 13:03 (00:25)
XXXXXXXX4 pts/6 cerberus.XXX.XXX Fri Oct 23 08:19 - 10:31 (02:11)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Oct 21 20:08 - 20:10 (00:01)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Tue Oct 20 09:30 - 09:50 (00:19)
XXXXXXXX6 pts/6 seki Mon Oct 19 17:04 - 17:05 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 19 16:22 - 16:22 (00:00)
XXXXX31 ftp gatekeeper.ce9.u Mon Oct 19 14:05 - 14:32 (00:27)
XXXXX31 ftp gatekeeper.ce9.u Mon Oct 19 13:43 - 13:57 (00:13)
XXXXXXXX4 pts/6 cerberus.XXX.XXX Mon Oct 19 12:41 - 12:43 (00:01)

```



```

-----
XXXXX31 ftp gatekeeper.ce9.u Mon Oct 19 11:43 - 12:04 (00:20)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 19 09:24 - 12:21 (02:57)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sat Oct 17 00:39 - 00:42 (00:03)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Oct 14 10:53 - 10:53 (00:00)
XXXXXXXX4 pts/6 cerberus.XXX.XXX Tue Oct 13 12:32 - 14:41 (02:09)
XXXXX31 ftp 208.202.157.62 Tue Oct 13 09:59 - 10:18 (00:19)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Tue Oct 13 00:49 - 00:51 (00:02)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 12 22:19 - 22:19 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 12 22:11 - 22:18 (00:06)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 12 21:57 - 22:10 (00:13)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 12 21:57 - 22:10 (00:13)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Sun Oct 11 03:10 - 03:27 (00:16)
XXXXX31 ftp we-192-168-2-117 Thu Oct 8 19:15 - 19:21 (00:05)
XXXXX31 ftp we-192-168-2-117 Wed Oct 7 18:25 - 18:26 (00:00)
XXXXX31 ftp we-192-168-2-117 Wed Oct 7 12:21 - 12:24 (00:03)
XXXXXXXX6 ftp cerberus.XXX.XXX Wed Oct 7 11:37 - 11:37 (00:00)
XXXXXXXX6 ftp kuki-dmz Wed Oct 7 11:36 - 11:36 (00:00)
XXXXX31 ftp cerberus.XXX.XXX Tue Oct 6 14:34 - 14:36 (00:02)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 09:20 - 09:38 (00:18)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 09:15 - 09:20 (00:04)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 09:13 - 09:14 (00:01)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 09:10 - 09:12 (00:02)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 09:09 - 09:10 (00:01)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 09:03 - 09:08 (00:05)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 09:01 - 09:03 (00:01)
asdfXXX1 ftp cerberus.XXX.XXX Tue Oct 6 07:51 - 08:06 (00:15)
asdfXXX1 pts/6 cerberus.XXX.XXX Tue Oct 6 07:32 - 09:38 (02:05)
XXXXXXXX6 pts/7 cerberus.XXX.XXX Mon Oct 5 01:18 - 03:31 (02:12)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Oct 5 01:17 - 01:17 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Oct 5 01:15 - 03:32 (02:17)
XXXXX31 ftp cerberus.XXX.XXX Sat Oct 3 13:03 - 13:48 (00:45)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Fri Oct 2 22:45 - 22:54 (00:09)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Thu Oct 1 23:33 - 23:48 (00:14)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Tue Sep 29 19:39 - 19:55 (00:16)
ftp ftp ns.texlab.XXX.XX Tue Sep 29 07:31 - 09:25 (01:54)
XXXXX31 ftp 192.168.148.2 Mon Sep 28 14:25 - 14:37 (00:12)
XXXXX31 ftp 192.168.148.2 Mon Sep 28 14:14 - 14:17 (00:02)
XXXXX31 ftp 192.168.148.2 Mon Sep 28 14:11 - 14:11 (00:00)
XXXXX31 ftp 192.168.37.68 Fri Sep 25 18:48 - 18:50 (00:01)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Fri Sep 25 00:47 - 01:35 (00:48)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Fri Sep 25 00:34 - 00:42 (00:07)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri Sep 25 00:31 - 00:31 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri Sep 25 00:22 - 00:22 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri Sep 25 00:03 - 00:12 (00:08)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Sep 24 23:20 - 23:31 (00:10)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Thu Sep 24 23:09 - 00:42 (01:33)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Sep 24 17:13 - 17:13 (00:00)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Thu Sep 24 17:04 - 17:41 (00:36)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Thu Sep 24 16:39 - 17:47 (01:08)
XXXXX31 ftp cerberus.XXX.XXX Thu Sep 24 10:18 - 10:20 (00:01)
ftp ftp ns.texlab.XXX.XX Wed Sep 23 20:56 - 21:07 (00:10)
ftp ftp ns.texlab.XXX.XX Wed Sep 23 20:53 - 20:56 (00:02)
ftp ftp ns.texlab.XXX.XX Wed Sep 23 20:52 - 20:53 (00:01)
ftp ftp ns.texlab.XXX.XX Wed Sep 23 20:35 - 20:37 (00:02)
ftp ftp ns.texlab.XXX.XX Wed Sep 23 19:28 - 19:31 (00:02)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Mon Sep 21 11:02 - 11:10 (00:07)
XXXXXXXX4 pts/5 cerberus.XXX.XXX Mon Sep 21 10:48 - 13:13 (02:24)

```

```

-----
ftp      ftp      cerberus.XXX.XXX Thu Sep 17 09:07 - 09:07 (00:00)
XXXXXXXX4 pts/5    cerberus.XXX.XXX Mon Sep 21 10:48 - 13:13 (02:24)
XXXXXXXX6 pts/5    cerberus.XXX.XXX Sun Sep 20 01:40 - 02:10 (00:30)
XXXXXX31 ftp      192.168.37.70   Fri Sep 18 15:35 - 15:35 (00:00)
XXXXXX31 ftp      192.168.37.68   Fri Sep 18 13:27 - 13:27 (00:00)
XXXXXX31 ftp      192.168.37.68   Fri Sep 18 12:46 - 12:49 (00:02)
XXXXXX31 ftp      192.168.120.21  Fri Sep 18 11:16 - 11:21 (00:04)
XXXXXX31 ftp      cerberus.XXX.XXX Fri Sep 18 08:09 - 09:48 (01:38)
XXXXXX31 ftp      cerberus.XXX.XXX Fri Sep 18 01:57 - 02:06 (00:08)
XXXXXXXX4 ftp      cerberus.XXX.XXX Fri Sep 18 01:55 - 01:57 (00:01)
XXXXXX31 ftp      cerberus.XXX.XXX Fri Sep 18 00:26 - 01:55 (01:29)
XXXXXX31 ftp      192.168.37.68   Thu Sep 17 11:34 - 11:35 (00:00)
XXXXXX31 ftp      192.168.37.68   Thu Sep 17 11:13 - 11:29 (00:15)
XXXXXX31 ftp      cerberus.XXX.XXX Thu Sep 17 09:39 - 09:42 (00:02)
XXXXXX31 ftp      cerberus.XXX.XXX Thu Sep 17 09:37 - 09:37 (00:00)
XXXXXX31 ftp      cerberus.XXX.XXX Thu Sep 17 09:36 - 09:36 (00:00)
XXXXXX31 ftp      cerberus.XXX.XXX Thu Sep 17 09:28 - 09:29 (00:00)
XXXXXXXX6 pts/5    cerberus.XXX.XXX Thu Sep 17 09:11 - 13:40 (04:28)
XXXXXXXX6 ftp      cerberus.XXX.XXX Thu Sep 17 09:07 - 09:07 (00:00)
XXXXXXXX4 ftp      cerberus.XXX.XXX Wed Sep 16 21:53 - 21:54 (00:01)
spear21  ftp      cerberus.XXX.XXX Wed Sep 16 21:50 - 21:52 (00:02)
XXXXXXXX4 pts/5    cerberus.XXX.XXX Wed Sep 16 21:48 - 21:54 (00:06)
spear21  pts/5    cerberus.XXX.XXX Wed Sep 16 21:48 - 21:48 (00:00)
spear21  pts/5    cerberus.XXX.XXX Wed Sep 16 21:38 - 21:38 (00:00)
spear21  pts/5    cerberus.XXX.XXX Wed Sep 16 21:37 - 21:37 (00:00)
spear21  ftp      cerberus.XXX.XXX Wed Sep 16 10:43 - 10:44 (00:00)
spear21  ftp      cerberus.XXX.XXX Wed Sep 16 10:28 - 10:43 (00:15)
spear21  ftp      cerberus.XXX.XXX Wed Sep 16 10:27 - 10:28 (00:00)
spear21  ftp      cerberus.XXX.XXX Wed Sep 16 10:18 - 10:19 (00:00)
spear21  ftp      cerberus.XXX.XXX Wed Sep 16 10:15 - 10:17 (00:01)
spear21  ftp      cerberus.XXX.XXX Wed Sep 16 10:10 - 10:14 (00:03)
ftp      ftp      192.168.51.254  Tue Sep 15 12:50 - 13:07 (00:16)
XXXXXXXX6 pts/5    cerberus.XXX.XXX Tue Sep 15 12:42 - 12:45 (00:02)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Sep 15 12:40 - 12:45 (00:05)
ftp      ftp      cerberus.XXX.XXX Tue Sep 15 11:41 - 11:41 (00:00)
ftp      ftp      cerberus.XXX.XXX Tue Sep 15 11:41 - 11:41 (00:00)
XXXXXXXX6 ftp      kuko-dmz        Fri Sep 11 10:15 - 10:15 (00:00)
XXXXXXXX6 ftp      cerberus.XXX.XXX Fri Sep 11 10:12 - 10:13 (00:00)
XXXXXXXX6 pts/6    cerberus.XXX.XXX Thu Sep 10 09:57 - 09:57 (00:00)
spear21  ftp      cerberus.XXX.XXX Thu Sep 10 09:56 - 09:57 (00:00)
spear21  pts/5    cerberus.XXX.XXX Thu Sep 10 09:55 - 09:55 (00:00)
spear21  pts/5    cerberus.XXX.XXX Thu Sep 10 09:52 - 09:52 (00:00)
spear21  pts/5    cerberus.XXX.XXX Thu Sep 10 09:50 - 09:50 (00:00)
XXXXXXXX4 pts/5    cerberus.XXX.XXX Wed Sep 9 11:22 - 11:31 (00:09)
XXXXXXXX6 pts/3    cerberus.XXX.XXX Tue Sep 8 17:38 - 17:53 (00:15)
XXXXXXXX6 pts/3    cerberus.XXX.XXX Tue Sep 8 17:37 - 17:37 (00:00)
root     console  :0              Tue Sep 8 16:44 - 13:31 (82+21:46)
asdfXXX1 pts/1    cerberus.XXX.XXX Tue Sep 8 06:56 - 06:56 (00:00)
XXXXXXXX6 pts/1    cerberus.XXX.XXX Mon Sep 7 22:53 - 22:53 (00:00)
spear21  ftp      cerberus.XXX.XXX Thu Sep 3 13:34 - 13:35 (00:01)
spear21  pts/1    cerberus.XXX.XXX Thu Sep 3 13:33 - 13:33 (00:00)
spear21  pts/1    cerberus.XXX.XXX Thu Sep 3 13:32 - 13:32 (00:00)
XXXXXXXX6 ftp      cerberus.XXX.XXX Thu Sep 3 10:02 - 10:02 (00:00)
XXXXXXXX6 pts/1    cerberus.XXX.XXX Thu Sep 3 10:01 - 13:04 (03:03)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Sep 1 21:44 - 21:44 (00:00)
XXXXXXXX6 pts/3    cerberus.XXX.XXX Tue Sep 1 21:24 - 22:09 (00:45)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Sep 1 21:24 - 21:24 (00:00)

```

```

-----
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Tue Sep 1 21:19 - 22:09 (00:50)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Tue Sep 1 21:16 - 22:09 (00:53)
XXXXXXXXX6 ftp cerberus.XXX.XXX Tue Sep 1 21:16 - 21:16 (00:00)
XXXXXXXXX11 pts/1 cerberus.XXX.XXX Tue Sep 1 20:21 - 20:23 (00:02)
XXXXXXXXX11 ftp cerberus.XXX.XXX Tue Sep 1 20:12 - 20:24 (00:11)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Tue Sep 1 19:56 - 20:10 (00:14)
asdfXXX1 pts/1 cerberus.XXX.XXX Tue Sep 1 07:31 - 08:01 (00:29)
XXXXXXXXX11 ftp cerberus.XXX.XXX Mon Aug 31 17:00 - 17:01 (00:00)
XXXXXXXXX11 ftp cerberus.XXX.XXX Mon Aug 31 16:04 - 16:23 (00:18)
XXXXXXXXX11 pts/2 cerberus.XXX.XXX Mon Aug 31 15:13 - 15:42 (00:28)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Mon Aug 31 14:38 - 16:54 (02:15)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Sun Aug 30 02:09 - 02:13 (00:03)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Sat Aug 29 08:52 - 09:21 (00:29)
spear21 ftp 192.168.235.252 Fri Aug 28 13:31 - 13:31 (00:00)
spear21 ftp 192.168.235.252 Fri Aug 28 11:19 - 11:25 (00:05)
spear21 ftp cerberus.XXX.XXX Fri Aug 28 10:12 - 10:15 (00:03)
ftp ftp unogate.unocal.c Thu Aug 27 11:14 - 11:14 (00:00)
ftp ftp unogate.unocal.c Wed Aug 26 13:51 - 14:17 (00:26)
ftp ftp unogate.unocal.c Wed Aug 26 09:51 - 09:55 (00:03)
XXXXXXXXX6 ftp cerberus.XXX.XXX Wed Aug 26 09:37 - 09:38 (00:01)
asdfXXX1 pts/1 cerberus.XXX.XXX Tue Aug 25 11:21 - 11:21 (00:00)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Mon Aug 24 00:41 - 00:44 (00:02)
spear21 ftp seki Fri Aug 21 10:00 - 10:08 (00:07)
XXXXXXXXX6 ftp 192.168.84.130 Thu Aug 20 14:34 - 14:36 (00:02)
XXXXXXXXX6 ftp 192.168.84.130 Thu Aug 20 14:32 - 14:32 (00:00)
XXXXXXXXX6 ftp seki Thu Aug 20 14:21 - 14:22 (00:00)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Thu Aug 20 14:20 - 16:50 (02:29)
XXXXXXXXX6 ftp cerberus.XXX.XXX Thu Aug 20 14:04 - 14:05 (00:00)
XXXXXXXXX6 ftp 192.168.84.130 Thu Aug 20 13:06 - 13:06 (00:00)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Thu Aug 20 13:02 - 16:40 (03:37)
XXXXXXXXX6 ftp 192.168.84.130 Thu Aug 20 13:00 - 13:02 (00:01)
XXXXXXXXX6 ftp 192.168.84.130 Wed Aug 19 16:38 - 16:38 (00:00)
XXXXXXXXX6 ftp 192.168.84.130 Wed Aug 19 16:37 - 16:37 (00:00)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Wed Aug 19 16:11 - 17:35 (01:23)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Aug 19 16:06 - 17:34 (01:28)
XXXXXXXXX6 ftp seki Tue Aug 18 16:35 - 16:35 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Tue Aug 18 16:34 - 16:35 (00:00)
XXXXXXXXX6 ftp kuko-dmz Tue Aug 18 15:19 - 15:19 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Tue Aug 18 15:18 - 15:18 (00:00)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Tue Aug 18 15:18 - 16:38 (01:20)
XXXXXXXXX6 ftp 192.168.84.130 Tue Aug 18 15:17 - 15:18 (00:00)
XXXXXXXXX6 ftp 192.168.84.130 Tue Aug 18 15:09 - 15:10 (00:00)
XXXXXXXXX6 pts/1 192.168.84.130 Tue Aug 18 15:04 - 15:12 (00:08)
XXXXXXXXX6 ftp 192.168.84.130 Tue Aug 18 15:03 - 15:07 (00:03)
ftp ftp 192.168.84.130 Tue Aug 18 15:02 - 15:03 (00:01)
XXXXXXXXX6 pts/1 192.168.84.130 Tue Aug 18 11:48 - 11:49 (00:00)
XXXXXXXXX6 ftp 192.168.84.130 Tue Aug 18 11:19 - 11:20 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Tue Aug 18 11:09 - 11:10 (00:00)
spear21 ftp cerberus.XXX.XXX Tue Aug 18 10:15 - 10:22 (00:06)
spear21 ftp cerberus.XXX.XXX Tue Aug 18 10:15 - 10:15 (00:00)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Tue Aug 18 10:12 - 10:22 (00:09)
XXXXXXXXX4 pts/1 cerberus.XXX.XXX Tue Aug 18 10:09 - 10:34 (00:25)
XXXXXXXXX4 ftp cerberus.XXX.XXX Tue Aug 18 10:07 - 10:15 (00:07)
spear21 ftp cerberus.XXX.XXX Tue Aug 18 10:06 - 10:07 (00:01)
spear21 ftp cerberus.XXX.XXX Tue Aug 18 08:46 - 09:06 (00:20)
XXXXXXXXX4 pts/1 cerberus.XXX.XXX Tue Aug 18 08:45 - 09:12 (00:26)
XXXXXXXXX4 pts/1 cerberus.XXX.XXX Mon Aug 17 11:05 - 11:27 (00:21)

```

```

-----
XXXXXXXXX6 pts/1      192.168.51.254    Thu Aug 13 16:32 - 16:38 (00:06)
spear21    ftp      cerberus.XXX.XXX Thu Aug 13 11:01 - 11:02 (00:01)
spear21    ftp      cerberus.XXX.XXX Thu Aug 13 10:50 - 10:57 (00:07)
XXXXXXXXX6 pts/1      cerberus.XXX.XXX Wed Aug 12 00:22 - 00:57 (00:34)
XXXXXXXXX6 pts/1      cerberus.XXX.XXX Fri Aug  7 16:13 - 18:24 (02:11)
XXXXXXXXX6 ftp      cerberus.XXX.XXX Fri Aug  7 16:12 - 16:13 (00:00)
XXXXXXXXX6 pts/1      cerberus.XXX.XXX Fri Aug  7 15:57 - 15:58 (00:00)
XXXXXXXXX6 ftp      cerberus.XXX.XXX Fri Aug  7 15:57 - 15:57 (00:00)
XXXXXXXXX6 ftp      cerberus.XXX.XXX Fri Aug  7 15:54 - 15:56 (00:01)
root       console  :0              Fri Aug  7 13:05 - 14:42 (01:37)
spear21    ftp      192.168.51.76   Fri Aug  7 10:44 - 11:01 (00:16)
spear21    ftp      cerberus.XXX.XXX Fri Aug  7 07:49 - 08:34 (00:44)
XXXXXXXXX4 ftp      cerberus.XXX.XXX Fri Aug  7 07:48 - 07:49 (00:00)
spear21    ftp      192.168.119.171 Thu Aug  6 16:05 - 16:22 (00:17)
ftp        ftp      192.168.119.171 Thu Aug  6 15:39 - 15:40 (00:01)
spear21    ftp      192.168.51.76   Thu Aug  6 14:56 - 14:58 (00:02)
spear21    ftp      192.168.119.171 Thu Aug  6 14:50 - 14:56 (00:05)
spear21    ftp      192.168.119.171 Thu Aug  6 14:41 - 14:42 (00:01)
spear21    ftp      192.168.119.171 Thu Aug  6 14:33 - 14:40 (00:06)
ftp        ftp      192.168.119.171 Thu Aug  6 14:33 - 14:33 (00:00)
spear21    ftp      192.168.192.157 Thu Aug  6 10:47 - 10:50 (00:02)
spear21    ftp      192.168.192.157 Thu Aug  6 09:48 - 09:51 (00:03)
XXXXXXXX11 pts/0      cerberus.XXX.XXX Thu Aug  6 08:30 - 08:33 (00:03)
XXXXXXXXX6 pts/2      cerberus.XXX.XXX Wed Aug  5 22:24 - 22:58 (00:34)
XXXXXXXXX6 pts/0      cerberus.XXX.XXX Wed Aug  5 22:19 - 00:30 (02:10)
spear21    ftp      192.168.192.148 Wed Aug  5 11:45 - 11:46 (00:01)
spear21    ftp      192.168.192.148 Wed Aug  5 11:37 - 11:39 (00:01)
asdfXXX1  ftp      cerberus.XXX.XXX Wed Aug  5 07:13 - 07:18 (00:05)
spear21    ftp      192.168.192.145 Tue Aug  4 10:01 - 10:03 (00:02)
spear21    ftp      cerberus.XXX.XXX Mon Aug  3 15:05 - 15:07 (00:01)
spear21    ftp      cerberus.XXX.XXX Mon Aug  3 15:05 - 15:05 (00:00)
XXXXXXXXX4 pts/2      cerberus.XXX.XXX Thu Jul 30 15:19 - 17:28 (02:09)
XXXXXXXXX4 pts/0      cerberus.XXX.XXX Thu Jul 30 13:37 - 15:47 (02:10)
XXXXXXXXX4 pts/0      cerberus.XXX.XXX Thu Jul 30 10:45 - 13:16 (02:31)
XXXXXXXXX4 pts/0      cerberus.XXX.XXX Thu Jul 30 09:09 - 10:34 (01:24)
asdfXXX1  ftp      cerberus.XXX.XXX Thu Jul 30 08:04 - 08:12 (00:07)
asdfXXX1  ftp      cerberus.XXX.XXX Thu Jul 30 08:00 - 08:02 (00:02)
asdfXXX1  ftp      cerberus.XXX.XXX Thu Jul 30 07:56 - 07:59 (00:03)
asdfXXX1  ftp      cerberus.XXX.XXX Thu Jul 30 07:52 - 07:52 (00:00)
XXXXXXXXX4 ftp      cerberus.XXX.XXX Wed Jul 29 17:47 - 17:48 (00:01)
XXXXXXXXX4 ftp      cerberus.XXX.XXX Wed Jul 29 17:27 - 17:28 (00:01)
XXXXXXXXX4 pts/4      cerberus.XXX.XXX Wed Jul 29 16:31 - 18:31 (01:59)
XXXXXXXXX4 pts/3      cerberus.XXX.XXX Wed Jul 29 16:09 - 18:31 (02:21)
XXXXXXXXX4 pts/2      cerberus.XXX.XXX Wed Jul 29 14:38 - 17:29 (02:51)
XXXXXXXXX4 pts/0      cerberus.XXX.XXX Wed Jul 29 13:14 - 17:21 (04:07)
XXXXXXXXX4 pts/0      cerberus.XXX.XXX Wed Jul 29 12:49 - 12:59 (00:09)
XXXXXXXXX2 pts/0      cerberus.XXX.XXX Wed Jul 29 10:50 - 10:50 (00:00)
XXXXXXXXX4 ftp      cobalt.fooar.as Wed Jul 29 10:44 - 10:44 (00:00)
spear21    ftp      pna-169.kla-ten- Wed Jul 29 10:32 - 10:32 (00:00)
XXXXXXXXX4 pts/0      cerberus.XXX.XXX Tue Jul 28 18:15 - 18:32 (00:17)
XXXXXXXXX4 pts/0      cerberus.XXX.XXX Tue Jul 28 14:24 - 16:41 (02:17)
XXXXXXXXX6 ftp      pna-169.kla-ten- Tue Jul 28 11:13 - 11:20 (00:07)
XXXXXXXXX4 pts/2      cerberus.XXX.XXX Tue Jul 28 10:32 - 14:34 (04:01)
spear21    ftp      cerberus.XXX.XXX Tue Jul 28 09:12 - 09:20 (00:08)
ftp        ftp      cerberus.XXX.XXX Tue Jul 28 09:11 - 09:12 (00:00)
ftp        ftp      cerberus.XXX.XXX Tue Jul 28 09:11 - 09:11 (00:00)
ftp        ftp      cerberus.XXX.XXX Tue Jul 28 09:10 - 09:11 (00:00)

```

```

-----
XXXXXXXX4 pts/0      cerberus.XXX.XXX Tue Jul 28 08:41 - 10:52 (02:10)
XXXXXXXX6 ftp          cerberus.XXX.XXX Mon Jul 27 12:00 - 12:00 (00:00)
root      console      :0              Mon Jul 27 11:57 - 11:58 (00:00)
XXXXXXXX6 pts/0      cerberus.XXX.XXX Mon Jul 27 11:51 - 14:11 (02:20)
reboot    system boot              Mon Jul 27 11:49
root      console      :0              Mon Jul 27 11:07 - 11:48 (00:40)
XXXXXXXX6 pts/2      cerberus.XXX.XXX Mon Jul 27 10:31 - down (01:17)
asdfXXX1 pts/1      cerberus.XXX.XXX Mon Jul 27 10:13 - 11:06 (00:53)
reboot    system boot              Sun Jul 26 13:24
XXXXXXXX4 pts/5      cerberus.XXX.XXX Sat Jul 25 16:44 - 16:47 (00:03)
XXXXXXXX4 pts/5      cerberus.XXX.XXX Fri Jul 24 16:45 - 17:03 (00:17)
XXXXXXXX4 pts/6      cerberus.XXX.XXX Thu Jul 23 16:19 - 16:20 (00:00)
XXXXXXXX4 ftp          gateway.bar.foo Thu Jul 23 16:03 - 16:04 (00:01)
spear21  ftp          cerberus.XXX.XXX Thu Jul 23 15:56 - 16:03 (00:07)
spear21  ftp          cerberus.XXX.XXX Thu Jul 23 15:49 - 15:55 (00:06)
XXXXXXXX4 pts/5      cerberus.XXX.XXX Thu Jul 23 15:24 - 17:51 (02:26)
asdfXXX1 pts/5      cerberus.XXX.XXX Thu Jul 23 13:33 - 13:33 (00:00)
asdfXXX1 pts/5      cerberus.XXX.XXX Thu Jul 23 12:51 - 13:29 (00:37)
asdfXXX1 pts/5      cerberus.XXX.XXX Thu Jul 23 10:51 - 11:25 (00:34)
asdfXXX1 pts/5      cerberus.XXX.XXX Thu Jul 23 09:22 - 10:32 (01:10)
XXXXXXXX6 pts/5      cerberus.XXX.XXX Tue Jul 21 15:06 - 16:29 (01:22)
spear21  ftp          foo0-249.bar-baz Tue Jul 21 09:27 - 10:07 (00:39)
spear21  ftp          foo0-249.bar-baz Mon Jul 20 14:09 - 14:14 (00:05)
spear21  ftp          cerberus.XXX.XXX Mon Jul 20 13:59 - 14:09 (00:10)
spear21  ftp          cerberus.XXX.XXX Mon Jul 20 10:59 - 11:01 (00:01)
spear21  ftp          cerberus.XXX.XXX Mon Jul 20 10:31 - 10:59 (00:27)
XXXXXXXX5 pts/5      cerberus.XXX.XXX Mon Jul 20 10:02 - 10:14 (00:11)
XXXXXXXX5 pts/5      cerberus.XXX.XXX Mon Jul 20 10:02 - 10:02 (00:00)
spear21  ftp          cerberus.XXX.XXX Mon Jul 20 09:28 - 09:30 (00:01)
spear21  ftp          cerberus.XXX.XXX Mon Jul 20 09:25 - 09:25 (00:00)
XXXXXXXX5 pts/5      cerberus.XXX.XXX Mon Jul 20 09:15 - 09:37 (00:22)
XXXXXXXX5 pts/5      cerberus.XXX.XXX Mon Jul 20 09:03 - 09:14 (00:11)
XXXXXXXX4 pts/5      cerberus.XXX.XXX Fri Jul 17 13:13 - 14:01 (00:48)
ftp      ftp          foo0-119.bar-baz Fri Jul 17 11:02 - 11:05 (00:02)
XXXXXXXX6 ftp          mailman.XXX.XXX Fri Jul 17 10:48 - 11:02 (00:14)
ftp      ftp          mailman.XXX.XXX Fri Jul 17 10:47 - 10:48 (00:00)
XXXXXXXX4 pts/5      cerberus.XXX.XXX Fri Jul 17 06:50 - 06:55 (00:05)
XXXXXXXX2 ftp          cerberus.XXX.XXX Thu Jul 16 21:10 - 21:33 (00:23)
XXXXXXXX4 ftp          mailman.XXX.XXX Thu Jul 16 17:10 - 17:13 (00:03)
XXXXXXXX4 pts/5      cerberus.XXX.XXX Thu Jul 16 17:09 - 17:24 (00:15)
XXXXXXXX6 pts/9      cerberus.XXX.XXX Thu Jul 16 15:57 - down (9+21:27)
XXXXXXXX4 pts/8      cerberus.XXX.XXX Thu Jul 16 15:56 - 17:24 (01:28)
XXXXXXXX6 pts/7      cerberus.XXX.XXX Thu Jul 16 15:45 - 16:56 (01:11)
XXXXXXXX6 pts/8      cerberus.XXX.XXX Thu Jul 16 15:25 - 15:35 (00:10)
XXXXXXXX4 pts/6      cerberus.XXX.XXX Thu Jul 16 15:03 - 17:51 (02:47)
XXXXXXXX4 ftp          cerberus.XXX.XXX Thu Jul 16 15:01 - 15:02 (00:01)
XXXXXXXX4 pts/7      cerberus.XXX.XXX Thu Jul 16 13:30 - 15:41 (02:11)
XXXXXXXX4 pts/6      cerberus.XXX.XXX Thu Jul 16 12:13 - 14:23 (02:10)
XXXXXXXX4 pts/5      cerberus.XXX.XXX Thu Jul 16 11:25 - 17:02 (05:37)
XXXXXXXX6 ftp          10k.singingbeagl Thu Jul 16 11:10 - 11:10 (00:00)
XXXXXXXX6 ftp          cerberus.XXX.XXX Thu Jul 16 11:09 - 11:09 (00:00)
XXXXXXXX6 pts/6      cerberus.XXX.XXX Thu Jul 16 10:25 - 11:19 (00:54)
XXXXXXXX6 pts/5      cerberus.XXX.XXX Thu Jul 16 10:14 - 11:20 (01:05)
XXXXXXXX2 ftp          cerberus.XXX.XXX Wed Jul 15 17:18 - 17:32 (00:13)
XXXXXXXX4 pts/7      cerberus.XXX.XXX Wed Jul 15 17:16 - 17:18 (00:01)
XXXXXXXX2 pts/6      cerberus.XXX.XXX Wed Jul 15 17:12 - 17:18 (00:06)
XXXXXXXX2 ftp          cerberus.XXX.XXX Wed Jul 15 17:11 - 17:12 (00:00)

```

```

-----
XXXXXXXX4  ftp          gateway.pub.foob Wed Jul 15 17:06 - 17:06 (00:00)
XXXXXXXX2  pts/7          cerberus.XXX.XXX Wed Jul 15 16:56 - 17:08 (00:11)
XXXXXXXX2  ftp           cerberus.XXX.XXX Wed Jul 15 16:50 - 16:54 (00:03)
XXXXXXXX4  pts/6          cerberus.XXX.XXX Wed Jul 15 16:35 - 17:05 (00:29)
XXXXXXXX4  pts/5          cerberus.XXX.XXX Wed Jul 15 14:30 - 17:18 (02:47)
XXXXXXXX6  pts/5          cerberus.XXX.XXX Wed Jul 15 14:24 - 14:25 (00:00)
ftp        ftp           pix3-112.kla-ten Wed Jul 15 14:20 - 14:23 (00:03)
XXXXXXXX6  pts/5          cerberus.XXX.XXX Wed Jul 15 14:19 - 14:19 (00:00)
XXXXXXXX6  ftp           cerberus.XXX.XXX Wed Jul 15 14:17 - 14:18 (00:00)
ftp        ftp           pix3-112.kla-ten Wed Jul 15 11:29 - 13:18 (01:49)
XXXXXXXX6  ftp           cerberus.XXX.XXX Wed Jul 15 11:27 - 11:27 (00:00)
XXXXXXXX6  ftp           cerberus.XXX.XXX Wed Jul 15 11:20 - 11:25 (00:05)
ftp        ftp           cerberus.XXX.XXX Wed Jul 15 11:19 - 11:20 (00:00)
XXXXXXXX6  pts/5          cerberus.XXX.XXX Wed Jul 15 11:10 - 11:28 (00:18)
spear21   ftp           cerberus.XXX.XXX Wed Jul 15 10:59 - 11:16 (00:17)
asdfXXX2  ftp           cerberus.XXX.XXX Wed Jul 15 06:55 - 06:59 (00:03)
XXXXXXXX2  ftp           cerberus.XXX.XXX Tue Jul 14 19:07 - 19:07 (00:00)
XXXXXXXX4  ftp           gateway.pub.gett Tue Jul 14 16:50 - 16:50 (00:00)
XXXXXXXX4  pts/5          cerberus.XXX.XXX Tue Jul 14 16:22 - 17:10 (00:48)
XXXXXXXX4  pts/5          cerberus.XXX.XXX Tue Jul 14 15:07 - 15:32 (00:25)
XXXXXXXX4  pts/5          cerberus.XXX.XXX Tue Jul 14 13:33 - 14:40 (01:07)
spear21   ftp           cerberus.XXX.XXX Mon Jul 13 17:19 - 17:26 (00:07)
spear21   ftp           cerberus.XXX.XXX Mon Jul 13 17:12 - 17:13 (00:00)
spear21   ftp           cerberus.XXX.XXX Mon Jul 13 17:11 - 17:12 (00:00)
XXXXXXXX6  pts/6          kuko-dmz          Mon Jul 13 16:52 - 18:52 (02:00)
XXXXXXXX6  pts/5          kuko-dmz          Mon Jul 13 15:19 - 16:53 (01:33)
root      console       :0                Mon Jul 13 12:47 - down (13+00:37)
spear21   ftp           cerberus.XXX.XXX Fri Jul 10 15:28 - 15:34 (00:06)
ftp        ftp           cerberus.XXX.XXX Fri Jul 10 15:27 - 15:28 (00:00)
jjXXXXXX3 pts/3          cerberus.XXX.XXX Fri Jul 10 14:08 - 14:10 (00:02)
XXXXXXXX4  ftp           209.60.58.129    Fri Jul 10 12:05 - 12:11 (00:05)
XXXXXXXX4  pts/1          cerberus.XXX.XXX Fri Jul 10 11:17 - 14:16 (02:58)
jjXXXXXX3 pts/1          cerberus.XXX.XXX Fri Jul 10 11:17 - 11:17 (00:00)
jjXXXXXX3 pts/1          cerberus.XXX.XXX Fri Jul 10 11:15 - 11:15 (00:00)
jjXXXXXX3 ftp           cerberus.XXX.XXX Fri Jul 10 11:15 - 11:15 (00:00)
jjXXXXXX3 ftp           cerberus.XXX.XXX Fri Jul 10 11:10 - 11:10 (00:00)
jjXXXXXX3 ftp           cerberus.XXX.XXX Fri Jul 10 10:32 - 10:33 (00:00)
jjXXXXXX3 ftp           cerberus.XXX.XXX Fri Jul 10 10:02 - 10:02 (00:00)
jjXXXXXX3 pts/1          cerberus.XXX.XXX Fri Jul 10 09:59 - 10:38 (00:39)
jjXXXXXX3 pts/1          cerberus.XXX.XXX Fri Jul 10 08:14 - 08:45 (00:30)
spear21   ftp           cerberus.XXX.XXX Thu Jul 9 16:50 - 16:54 (00:03)
XXXXXXXX4  ftp           cerberus.XXX.XXX Thu Jul 9 15:46 - 15:54 (00:08)
XXXXXXXX4  ftp           cerberus.XXX.XXX Thu Jul 9 15:39 - 15:44 (00:05)
XXXXXXXX4  pts/1          cerberus.XXX.XXX Thu Jul 9 15:37 - 15:46 (00:09)
XXXXXXXX4  ftp           cerberus.XXX.XXX Thu Jul 9 15:24 - 15:28 (00:04)
XXXXXXXX4  ftp           192.168.58.5     Thu Jul 9 15:19 - 15:23 (00:04)
jjXXXXXX3 pts/3          cerberus.XXX.XXX Thu Jul 9 12:21 - 12:21 (00:00)
XXXXXXXX4  ftp           192.168.58.5     Thu Jul 9 11:07 - 11:13 (00:05)
XXXXXXXX4  pts/3          cerberus.XXX.XXX Thu Jul 9 11:07 - 11:17 (00:09)
jjXXXXXX3 pts/1          cerberus.XXX.XXX Thu Jul 9 10:47 - 13:25 (02:38)
jjXXXXXX3 console       :0                Thu Jul 9 10:35 - 10:39 (00:04)
jjXXXXXX3 console       :0                Thu Jul 9 10:33 - 10:34 (00:01)
jjXXXXXX3 pts/5          localhost         Thu Jul 9 10:31 - 10:31 (00:00)
root      console       :0                Thu Jul 9 10:24 - 10:32 (00:08)
spear21   ftp           cerberus.XXX.XXX Thu Jul 9 09:51 - 09:52 (00:01)
spear21   ftp           cerberus.XXX.XXX Thu Jul 9 09:50 - 09:50 (00:00)
spear21   ftp           cerberus.XXX.XXX Thu Jul 9 09:42 - 09:45 (00:02)

```

```

.....
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 14:35 - 14:42 (00:06)
XXXXXXXX2 pts/1 cerberus.XXX.XXX Wed Jul 8 14:31 - 14:34 (00:03)
XXXXXXXX4 ftp 192.168.58.5 Wed Jul 8 14:27 - 14:28 (00:01)
XXXXXXXX4 pts/1 cerberus.XXX.XXX Wed Jul 8 14:25 - 14:30 (00:04)
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 14:24 - 14:25 (00:00)
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 14:01 - 14:04 (00:02)
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 13:34 - 13:38 (00:04)
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 13:27 - 13:31 (00:03)
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 13:21 - 13:24 (00:03)
XXXXXXXX9 ftp cerberus.XXX.XXX Wed Jul 8 13:19 - 13:20 (00:00)
XXXXXXXX4 ftp 192.168.58.5 Wed Jul 8 13:11 - 13:19 (00:07)
XXXXXXXX2 pts/3 cerberus.XXX.XXX Wed Jul 8 13:11 - 15:39 (02:28)
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 13:07 - 13:09 (00:01)
XXXXXXXX4 pts/1 cerberus.XXX.XXX Wed Jul 8 12:57 - 14:17 (01:19)
XXXXXXXX2 pts/1 cerberus.XXX.XXX Wed Jul 8 10:43 - 11:05 (00:22)
XXXXXXXX2 ftp cerberus.XXX.XXX Wed Jul 8 10:38 - 10:42 (00:04)
spear21 ftp cerberus.XXX.XXX Mon Jul 6 10:36 - 10:36 (00:00)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 14:38 - 14:52 (00:13)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 14:33 - 14:38 (00:05)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 14:05 - 14:33 (00:27)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:57 - 13:59 (00:01)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:38 - 13:53 (00:15)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:31 - 13:33 (00:02)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:30 - 13:31 (00:01)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:26 - 13:29 (00:02)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:22 - 13:26 (00:04)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:18 - 13:20 (00:02)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 13:12 - 13:16 (00:04)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 12:52 - 13:07 (00:15)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 12:45 - 12:47 (00:02)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 12:41 - 12:43 (00:01)
XXXXXXXX9 ftp cerberus.XXX.XXX Thu Jul 2 12:24 - 12:34 (00:09)
XXXXXXXX9 pts/4 cerberus.XXX.XXX Thu Jul 2 12:10 - 14:40 (02:30)
XXXXXXXX2 pts/3 cerberus.XXX.XXX Thu Jul 2 11:58 - 14:00 (02:02)
spear21 pts/3 cerberus.XXX.XXX Thu Jul 2 11:57 - 11:57 (00:00)
XXXXXXXX2 pts/3 cerberus.XXX.XXX Thu Jul 2 11:57 - 11:57 (00:00)
spear21 pts/4 cerberus.XXX.XXX Thu Jul 2 11:41 - 11:41 (00:00)
spear21 pts/4 cerberus.XXX.XXX Thu Jul 2 11:41 - 11:41 (00:00)
spear21 pts/3 cerberus.XXX.XXX Thu Jul 2 11:39 - 11:39 (00:00)
spear21 pts/3 cerberus.XXX.XXX Thu Jul 2 11:36 - 11:36 (00:00)
spear21 pts/3 cerberus.XXX.XXX Thu Jul 2 11:32 - 11:32 (00:00)
spear21 pts/3 cerberus.XXX.XXX Thu Jul 2 11:31 - 11:31 (00:00)
XXXXXXXX4 pts/1 cerberus.XXX.XXX Thu Jul 2 11:23 - 14:18 (02:54)
asdfXXX3 ftp cerberus.XXX.XXX Wed Jul 1 10:37 - 10:51 (00:14)
asdfXXX3 ftp cerberus.XXX.XXX Wed Jul 1 10:26 - 10:30 (00:04)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Jul 1 09:35 - 09:35 (00:00)
spear21 ftp foo0-249.bar-baz Wed Jul 1 09:33 - 09:37 (00:03)
asdfXXX3 ftp cerberus.XXX.XXX Wed Jul 1 09:31 - 09:33 (00:02)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Jul 1 09:31 - 09:33 (00:01)
spear21 ftp pix0-81.kla-tenc Tue Jun 30 15:17 - 15:20 (00:03)
XXXXXXXX4 pts/1 cerberus.XXX.XXX Tue Jun 30 15:09 - 15:12 (00:02)
XXXXXXXX4 ftp cerberus.XXX.XXX Tue Jun 30 15:07 - 15:09 (00:01)
spear21 ftp foo0-249.bar-baz Tue Jun 30 14:30 - 14:36 (00:05)
XXXXXXXX4 pts/3 cerberus.XXX.XXX Tue Jun 30 14:28 - 14:28 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Tue Jun 30 14:27 - 14:29 (00:01)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Tue Jun 30 14:26 - 14:29 (00:03)
spear21 ftp foo0-249.bar-baz Tue Jun 30 14:20 - 14:27 (00:06)

```

```

-----
spear21 ftp foo0-249.bar-baz Tue Jun 30 14:16 - 14:17 (00:00)
XXXXXXX6 pts/1 cerberus.XXX.XXX Tue Jun 30 14:14 - 14:16 (00:01)
spear21 ftp foo0-249.bar-baz Tue Jun 30 14:11 - 14:12 (00:00)
spear21 ftp foo0-249.bar-baz Tue Jun 30 14:08 - 14:09 (00:01)
XXXXXXX4 ftp cerberus.XXX.XXX Tue Jun 30 14:08 - 14:08 (00:00)
XXXXXXX4 pts/1 cerberus.XXX.XXX Tue Jun 30 14:06 - 14:11 (00:05)
XXXXXXX6 ftp cerberus.XXX.XXX Tue Jun 30 09:59 - 10:00 (00:00)
XXXXXXX6 ftp seki Tue Jun 30 09:59 - 09:59 (00:00)
XXXXXXX6 ftp seki Tue Jun 30 09:58 - 09:58 (00:00)
XXXXXXX6 pts/1 cerberus.XXX.XXX Tue Jun 30 09:57 - 09:59 (00:02)
XXXXXXX6 ftp cerberus.XXX.XXX Mon Jun 29 15:54 - 15:54 (00:00)
XXXXXXX6 ftp seki Mon Jun 29 15:53 - 15:53 (00:00)
XXXXXXX6 pts/1 cerberus.XXX.XXX Mon Jun 29 15:50 - 15:54 (00:03)
ftp ftp 192.168.220.249 Mon Jun 29 11:16 - 11:26 (00:10)
XXXXXXX4 pts/1 cerberus.XXX.XXX Sun Jun 28 16:15 - 16:22 (00:07)
XXXXXXX4 ftp 192.168.249.130 Sun Jun 28 16:14 - 16:20 (00:06)
XXXXXXX4 ftp 192.168.249.130 Sun Jun 28 16:09 - 16:12 (00:02)
XXXXXXX4 pts/1 mailman.XXX.XXX Sun Jun 28 16:07 - 16:12 (00:04)
XXXXXXX4 ftp mailman.XXX.XXX Sun Jun 28 16:06 - 16:07 (00:00)
XXXXXXX4 pts/1 cerberus.XXX.XXX Sat Jun 27 12:01 - 12:24 (00:23)
spear21 ftp cerberus.XXX.XXX Wed Jun 24 15:34 - 15:35 (00:00)
XXX33 ftp pix3-130.foo-bar Wed Jun 24 11:16 - 11:17 (00:00)
XXXXXXX6 pts/1 cerberus.XXX.XXX Wed Jun 24 11:15 - 11:17 (00:01)
XXX33 ftp cerberus.XXX.XXX Wed Jun 24 11:15 - 11:16 (00:01)
XXX33 ftp seki Wed Jun 24 11:10 - 11:10 (00:00)
XXX33 ftp seki Wed Jun 24 10:54 - 11:10 (00:15)
XXX33 ftp seki Wed Jun 24 10:24 - 10:25 (00:01)
XXX33 ftp cerberus.XXX.XXX Wed Jun 24 10:06 - 10:06 (00:00)
XXX33 ftp cerberus.XXX.XXX Wed Jun 24 10:06 - 10:06 (00:00)
XXX33 ftp seki Tue Jun 23 16:47 - 16:47 (00:00)
XXXXXXX6 pts/3 cerberus.XXX.XXX Tue Jun 23 14:38 - 15:21 (00:42)
ftp ftp foo0-249.bar-baz Tue Jun 23 14:28 - 14:32 (00:03)
XXX33 ftp foo0-249.bar-baz Tue Jun 23 14:27 - 14:28 (00:00)
XXX33 ftp seki Tue Jun 23 14:24 - 14:27 (00:02)
XXX33 ftp seki Tue Jun 23 14:24 - 14:24 (00:00)
XXXXXXX6 pts/1 cerberus.XXX.XXX Tue Jun 23 14:08 - 15:20 (01:12)
XXX33 ftp seki Tue Jun 23 13:33 - 13:40 (00:07)
XXX33 ftp seki Tue Jun 23 13:24 - 13:26 (00:02)
XXXXXXX4 pts/3 mailman.XXX.XXX Tue Jun 23 12:40 - 12:42 (00:01)
XXXXXXX4 ftp 192.168.112.2 Tue Jun 23 12:39 - 12:42 (00:02)
XXXXXXX4 ftp 192.168.112.2 Tue Jun 23 12:36 - 12:36 (00:00)
spear21 ftp 192.168.112.2 Tue Jun 23 11:06 - 11:19 (00:12)
XXXXXXX4 pts/3 mailman.XXX.XXX Tue Jun 23 11:00 - 11:19 (00:19)
XXXXXXX4 pts/1 cerberus.XXX.XXX Tue Jun 23 10:51 - 13:14 (02:22)
XXX33 ftp seki Mon Jun 22 17:56 - 17:58 (00:02)
XXX33 ftp pix1-112.foo-bar Mon Jun 22 15:35 - 15:38 (00:03)
XXX33 ftp pix1-112.foo-bar Mon Jun 22 15:34 - 15:35 (00:00)
XXX33 ftp pix1-112.foo-bar Mon Jun 22 15:34 - 15:34 (00:00)
XXX33 ftp foo0-249.bar-baz Mon Jun 22 15:31 - 15:34 (00:03)
XXX33 ftp seki Mon Jun 22 15:14 - 15:15 (00:00)
XXX33 ftp cerberus.XXX.XXX Mon Jun 22 15:12 - 15:14 (00:01)
XXXXXXX6 pts/1 cerberus.XXX.XXX Mon Jun 22 14:57 - 15:27 (00:29)
XXX33 ftp seki Mon Jun 22 14:42 - 14:43 (00:01)
spear21 ftp seki Mon Jun 22 14:42 - 14:42 (00:00)
XXX33 ftp seki Mon Jun 22 14:37 - 14:38 (00:01)
spear21 ftp seki Mon Jun 22 14:25 - 14:26 (00:00)
XXX33 ftp cerberus.XXX.XXX Mon Jun 22 13:43 - 14:25 (00:42)

```



```

-----
spear21 ftp cerberus.XXX.XXX Mon Jun 22 13:42 - 13:42 (00:00)
XXX33 ftp seki Mon Jun 22 13:26 - 13:27 (00:00)
spear21 ftp seki Mon Jun 22 13:25 - 13:26 (00:00)
XXX33 ftp seki Mon Jun 22 13:24 - 13:25 (00:00)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Mon Jun 22 12:22 - 13:38 (01:16)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Jun 22 12:14 - 12:20 (00:05)
XXXXXXXX6 pts/3 cerberus.XXX.XXX Mon Jun 22 12:13 - 13:38 (01:25)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Mon Jun 22 11:43 - 13:53 (02:10)
ftp ftp pix2-201.foo-bar Fri Jun 19 14:38 - 14:39 (00:00)
ftp ftp cerberus.XXX.XXX Fri Jun 19 14:37 - 14:38 (00:01)
ftp ftp cerberus.XXX.XXX Fri Jun 19 14:30 - 14:30 (00:00)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Fri Jun 19 14:29 - 15:12 (00:42)
ftp ftp pix1-46.foo-bar Fri Jun 19 14:28 - 14:30 (00:02)
ftp ftp pix1-218.foo-bar Wed Jun 17 17:48 - 17:48 (00:00)
XXX33 ftp 192.168.115.11 Wed Jun 17 11:11 - 11:42 (00:31)
XXX33 ftp cerberus.XXX.XXX Wed Jun 17 10:22 - 10:47 (00:24)
XXX33 ftp 192.168.115.11 Wed Jun 17 09:03 - 09:33 (00:30)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Tue Jun 16 18:52 - 18:52 (00:00)
ftp ftp pix3-67.foo-bar Tue Jun 16 18:42 - 18:48 (00:06)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Tue Jun 16 18:40 - 18:51 (00:11)
XXXXXXXX6 ftp cerberus.XXX.XXX Tue Jun 16 18:39 - 18:40 (00:00)
spear21 ftp cerberus.XXX.XXX Tue Jun 16 18:39 - 18:39 (00:00)
spear21 ftp pix3-67.foo-bar Tue Jun 16 10:38 - 10:41 (00:02)
XXXXXXXX6 pts/1 mailman.XXX.XXX Tue Jun 16 10:35 - 10:37 (00:02)
spear21 ftp seki Tue Jun 16 10:33 - 10:36 (00:02)
XXX33 ftp seki Tue Jun 16 10:23 - 10:23 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Tue Jun 16 09:24 - 09:25 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon Jun 15 16:55 - 16:55 (00:00)
asdfXXX1 ftp cerberus.XXX.XXX Mon Jun 15 14:52 - 15:08 (00:15)
XXX33 ftp cerberus.XXX.XXX Mon Jun 15 10:35 - 10:35 (00:00)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Mon Jun 15 10:34 - 12:44 (02:10)
XXX33 ftp 192.168.115.11 Mon Jun 15 08:59 - 09:05 (00:06)
XXXXXXXX6 pts/3 cerberus.XXX.XXX Thu Jun 11 01:39 - 01:49 (00:09)
XXXXXXXX6 pts/3 cerberus.XXX.XXX Thu Jun 11 01:38 - 01:39 (00:01)
XXXXXXXX6 ftp seki Thu Jun 11 00:46 - 00:46 (00:00)
XXXXXXXX6 ftp seki Thu Jun 11 00:45 - 00:45 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu Jun 11 00:43 - 00:44 (00:00)
XXXXXXXX6 pts/4 cerberus.XXX.XXX Thu Jun 11 00:37 - 01:49 (01:11)
XXXXXXXX6 pts/3 cerberus.XXX.XXX Thu Jun 11 00:37 - 01:37 (01:00)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Thu Jun 11 00:18 - 02:38 (02:20)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Jun 10 23:41 - 23:45 (00:03)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Jun 10 23:38 - 23:41 (00:03)
XXXXXXXX4 ftp cerberus.XXX.XXX Wed Jun 10 16:18 - 16:34 (00:15)
XXXXXXXX4 pts/1 cerberus.XXX.XXX Wed Jun 10 16:10 - 16:35 (00:24)
XXXXXXXX4 ftp cerberus.XXX.XXX Wed Jun 10 16:10 - 16:16 (00:05)
XXXXXXXX6 pts/1 mailman.XXX.XXX Wed Jun 10 15:21 - 15:23 (00:01)
XXX33 ftp seki Wed Jun 10 15:19 - 15:20 (00:01)
XXXXXXXX6 pts/1 mailman.XXX.XXX Wed Jun 10 13:44 - 13:46 (00:02)
XXX33 ftp yadayada1.nashua Wed Jun 10 08:11 - 08:13 (00:02)
XXX33 ftp foobar.bazquux.a Wed Jun 10 07:40 - 07:42 (00:01)
XXX33 ftp cerberus.XXX.XXX Tue Jun 9 17:46 - 17:46 (00:00)
XXX33 ftp seki Tue Jun 9 17:43 - 17:43 (00:00)
XXX33 ftp seki Tue Jun 9 15:56 - 15:56 (00:00)
XXX33 ftp seki Tue Jun 9 15:53 - 15:54 (00:00)
asdfXXX1 ftp cerberus.XXX.XXX Tue Jun 9 07:45 - 07:48 (00:02)
XXX33 ftp seki Mon Jun 8 18:59 - 18:59 (00:00)
XXX33 ftp seki Mon Jun 8 18:38 - 18:38 (00:00)

```

XXX33	ftp	seki	Mon Jun 8 18:12 - 18:13	(00:00)
XXX33	ftp	seki	Mon Jun 8 18:11 - 18:12	(00:00)
XXX33	ftp	seki	Mon Jun 8 18:10 - 18:10	(00:00)
XXX33	ftp	seki	Mon Jun 8 18:09 - 18:10	(00:00)
XXXXXXXX6	pts/1	kuko-dmz	Mon Jun 8 17:21 - 17:22	(00:00)
XXXXXXXX6	pts/1	kuko-dmz	Mon Jun 8 17:07 - 17:09	(00:01)
XXXXXXXX6	pts/1	kuko-dmz	Mon Jun 8 16:56 - 16:57	(00:00)
XXX33	ftp	dargghasd.nashua	Mon Jun 8 15:47 - 16:02	(00:15)
XXX33	ftp	seki	Mon Jun 8 15:44 - 15:45	(00:00)
XXX33	ftp	seki	Mon Jun 8 14:45 - 14:46	(00:00)
XXX33	ftp	seki	Mon Jun 8 14:38 - 14:38	(00:00)
XXXXXXXX6	ftp	seki	Mon Jun 8 14:02 - 14:03	(00:00)
XXX33	ftp	seki	Mon Jun 8 13:36 - 13:37	(00:00)
XXX33	ftp	dargghasd.nashua	Mon Jun 8 13:35 - 13:36	(00:01)
XXX33	ftp	seki	Mon Jun 8 13:04 - 13:04	(00:00)
XXX33	ftp	seki	Mon Jun 8 12:54 - 12:55	(00:00)
XXX33	ftp	dargghasd.nashua	Mon Jun 8 12:39 - 12:40	(00:00)
XXX33	ftp	seki	Mon Jun 8 10:57 - 10:58	(00:00)
XXX33	ftp	dargghasd.nashua	Mon Jun 8 10:57 - 10:57	(00:00)
XXX33	ftp	mailman.XXX.XXX	Mon Jun 8 10:51 - 10:51	(00:00)
XXXXXXXX6	pts/1	mailman.XXX.XXX	Mon Jun 8 10:47 - 10:51	(00:03)
spear21	ftp	localhost	Fri Jun 5 19:39 - 19:39	(00:00)
spear21	ftp	localhost	Fri Jun 5 19:38 - 19:39	(00:00)
spear21	ftp	localhost	Fri Jun 5 19:36 - 19:37	(00:00)
XXXXXXXX6	pts/1	mailman.XXX.XXX	Fri Jun 5 19:19 - 19:40	(00:21)
spear21	ftp	seki	Fri Jun 5 18:11 - 18:11	(00:00)
XXXXXXXX6	ftp	seki	Fri Jun 5 17:29 - 17:32	(00:02)
dfXX12	ftp	meihost.goaway.y	Fri Jun 5 10:26 - 10:32	(00:05)
dfXX12	ftp	cerberus.XXX.XXX	Fri Jun 5 09:42 - 09:54	(00:11)
XXXXXXXX4	pts/1	cerberus.XXX.XXX	Fri Jun 5 09:35 - 09:54	(00:19)
dfXX12	ftp	cerberus.XXX.XXX	Fri Jun 5 09:33 - 09:34	(00:00)
asdfXXX1	ftp	cerberus.XXX.XXX	Fri Jun 5 08:04 - 08:05	(00:00)
XXXXXXXX6	pts/1	cerberus.XXX.XXX	Fri Jun 5 01:30 - 02:34	(01:04)
spear21	ftp	cerberus.XXX.XXX	Thu Jun 4 15:01 - 15:02	(00:00)
dfXX12	ftp	cerberus.XXX.XXX	Thu Jun 4 14:57 - 14:57	(00:00)
XXXXXXXX6	pts/3	cerberus.XXX.XXX	Thu Jun 4 14:56 - 15:02	(00:06)
XXXXXXXX6	pts/1	cerberus.XXX.XXX	Thu Jun 4 14:49 - 14:57	(00:07)
fdXXXXX4	ftp	cerberus.XXX.XXX	Thu Jun 4 14:43 - 14:44	(00:00)
XXXXXXXX6	pts/4	cerberus.XXX.XXX	Thu Jun 4 14:40 - 14:54	(00:13)
XXXXXXXX6	pts/4	cerberus.XXX.XXX	Thu Jun 4 14:23 - 14:40	(00:16)
XXXXXXXX6	pts/1	cerberus.XXX.XXX	Thu Jun 4 14:19 - 14:41	(00:21)
spear21	ftp	cerberus.XXX.XXX	Thu Jun 4 11:46 - 11:51	(00:04)
XXXXXXXX6	pts/1	cerberus.XXX.XXX	Thu Jun 4 00:23 - 00:43	(00:19)
XXXXXXXX6	pts/1	cerberus.XXX.XXX	Thu Jun 4 00:12 - 00:23	(00:11)
XXXXXXXX6	pts/3	cerberus.XXX.XXX	Tue Jun 2 23:11 - 23:14	(00:02)
XXXXXXXX6	pts/1	cerberus.XXX.XXX	Tue Jun 2 23:09 - 23:12	(00:02)
spear21	ftp	cerberus.XXX.XXX	Mon Jun 1 16:33 - 16:33	(00:00)
XXXXXXXX6	pts/1	cerberus.XXX.XXX	Mon Jun 1 08:55 - 09:41	(00:46)
XXXXXXXX4	ftp	seki	Fri May 29 10:08 - 10:11	(00:02)
XXXXXXXX4	ftp	seki	Fri May 29 10:08 - 10:08	(00:00)
XXXXXXXX4	ftp	seki	Fri May 29 10:07 - 10:08	(00:00)
XXXXXXXX4	ftp	seki	Fri May 29 10:05 - 10:05	(00:00)
XXXXXXXX6	ftp	seki	Tue May 26 11:34 - 11:34	(00:00)
XXXXXXXX6	ftp	cerberus.XXX.XXX	Tue May 26 11:33 - 11:34	(00:00)
XXXXXXXX6	pts/4	cerberus.XXX.XXX	Tue May 26 10:07 - 13:59	(03:52)
XXXXXXXX6	pts/3	cerberus.XXX.XXX	Tue May 26 10:06 - 14:02	(03:55)
XXXXXXXX6	ftp	cerberus.XXX.XXX	Tue May 26 09:27 - 09:27	(00:00)

```

-----
XXXXXXXX6 pts/1 cerberus.XXX.XXX Tue May 26 09:25 - 13:19 (03:53)
spear21 ftp cerberus.XXX.XXX Mon May 25 10:53 - 10:56 (00:02)
spear21 pts/1 cerberus.XXX.XXX Mon May 25 10:53 - 10:53 (00:00)
XXXXXXXX4 pts/1 cerberus.XXX.XXX Mon May 25 10:49 - 10:53 (00:04)
XXXXXXXX6 ftp seki Fri May 22 09:17 - 09:18 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri May 22 09:04 - 09:07 (00:02)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu May 21 19:04 - 19:04 (00:00)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Thu May 21 19:03 - 19:04 (00:00)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Thu May 21 18:50 - 19:03 (00:13)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Tue May 19 23:41 - 00:04 (00:22)
XXXXXXXX6 ftp pix2-22.foo-barc Tue May 19 08:59 - 09:01 (00:02)
XXXXXXXX6 ftp cerberus.XXX.XXX Mon May 18 23:17 - 23:20 (00:02)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Mon May 18 23:16 - 23:18 (00:01)
XXXXXXXX6 ftp cerberus.XXX.XXX Fri May 15 17:55 - 18:00 (00:05)
spear21 ftp seki Fri May 15 16:41 - 16:42 (00:00)
spear21 ftp seki Fri May 15 16:38 - 16:39 (00:01)
spear21 ftp seki Fri May 15 16:36 - 16:37 (00:01)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Fri May 15 15:16 - 15:16 (00:00)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Fri May 15 13:57 - 14:44 (00:47)
XXXXXXXX6 pts/3 cerberus.XXX.XXX Fri May 15 03:16 - 04:06 (00:49)
XXXXXXXX6 pts/2 cerberus.XXX.XXX Fri May 15 01:16 - 03:16 (02:00)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Thu May 14 23:52 - 03:25 (03:32)
XXXXXXXX6 ftp cerberus.XXX.XXX Thu May 14 23:52 - 23:52 (00:00)
asdfXXX1 ftp cerberus.XXX.XXX Thu May 14 16:06 - 16:22 (00:15)
asdfXXX1 ftp cerberus.XXX.XXX Thu May 14 15:23 - 15:43 (00:20)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Thu May 14 15:03 - 17:29 (02:26)
XXXXXXXX6 pts/1 cerberus.XXX.XXX Wed May 13 16:17 - 16:19 (00:01)
XXXXXXXX5 pts/1 cerberus.XXX.XXX Wed May 13 14:30 - 15:34 (01:03)
XXXXXXXX5 ftp cerberus.XXX.XXX Wed May 13 12:45 - 12:46 (00:00)
XXXXXXXX5 pts/1 cerberus.XXX.XXX Wed May 13 12:33 - 12:49 (00:15)
asdfXXX1 ftp cerberus.XXX.XXX Tue May 12 12:36 - 12:36 (00:00)
asdfXXX1 ftp cerberus.XXX.XXX Mon May 11 09:44 - 10:00 (00:15)
spear21 ftp cerberus.XXX.XXX Mon May 11 09:08 - 09:08 (00:00)
ftp ftp cerberus.XXX.XXX Mon May 11 09:05 - 09:08 (00:02)
spear21 ftp 192.168.9.157 Fri May 8 14:58 - 15:06 (00:08)
asdfXXX1 ftp cerberus.XXX.XXX Fri May 8 10:01 - 10:01 (00:00)
XXXXXXXX4 pts/5 cerberus.XXX.XXX Fri May 8 09:20 - 09:27 (00:07)
XXXXX32 ftp cerberus.XXX.XXX Thu May 7 11:20 - 11:22 (00:02)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Wed May 6 21:57 - 22:28 (00:31)
XXXXX32 ftp cerberus.XXX.XXX Tue May 5 14:51 - 14:55 (00:03)
XXXXXXXX4 ftp cerberus.XXX.XXX Tue May 5 14:44 - 14:51 (00:06)
asdfXXX1 ftp cerberus.XXX.XXX Tue May 5 08:35 - 08:37 (00:02)
asdfXXX1 pts/1 cerberus.XXX.XXX Tue May 5 07:14 - 07:18 (00:03)
asdfXXX1 ftp cerberus.XXX.XXX Mon May 4 08:36 - 08:53 (00:16)
XXXXXXXX5 pts/1 cerberus.XXX.XXX Sat May 2 08:41 - 08:54 (00:12)
spear21 ftp cerberus.XXX.XXX Fri May 1 16:02 - 16:03 (00:01)
spear21 ftp cerberus.XXX.XXX Fri May 1 15:41 - 15:58 (00:16)
spear21 ftp cerberus.XXX.XXX Fri May 1 15:40 - 15:41 (00:00)
XXXXXXXX5 pts/1 cerberus.XXX.XXX Fri May 1 13:51 - 13:51 (00:00)
XXXXXXXX5 pts/6 cerberus.XXX.XXX Fri May 1 11:16 - 13:51 (02:34)
asdfXXX1 ftp cerberus.XXX.XXX Fri May 1 10:38 - 10:54 (00:15)
spear21 ftp cerberus.XXX.XXX Fri May 1 10:32 - 10:33 (00:01)
asdfXXX1 ftp cerberus.XXX.XXX Fri May 1 10:05 - 10:16 (00:10)
spear21 ftp cerberus.XXX.XXX Fri May 1 09:33 - 09:33 (00:00)
javelin ftp cerberus.XXX.XXX Fri May 1 09:17 - 09:33 (00:15)
XXXXXXXX5 ftp cerberus.XXX.XXX Fri May 1 09:13 - 09:17 (00:04)
XXXXXXXX5 pts/5 cerberus.XXX.XXX Fri May 1 08:54 - 11:16 (02:22)

```

```

-----
asdfXXX1 ftp cerberus.XXX.XXX Fri May 1 07:59 - 08:07 (00:08)
spear21 ftp cerberus.XXX.XXX Fri May 1 02:02 - 02:03 (00:00)
spear21 ftp cerberus.XXX.XXX Thu Apr 30 23:19 - 23:25 (00:05)
XXXXXXXX6 pts/6 cerberus.XXX.XXX Thu Apr 30 23:18 - 00:07 (00:48)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Thu Apr 30 22:31 - 23:35 (01:04)
XXXXXX32 ftp cerberus.XXX.XXX Thu Apr 30 10:10 - 10:12 (00:02)
XXXXXXXX5 ftp cerberus.XXX.XXX Wed Apr 29 15:09 - 15:09 (00:00)
XXXXXXXX5 pts/5 cerberus.XXX.XXX Wed Apr 29 14:49 - 17:18 (02:29)
XXXXXXXX5 ftp cerberus.XXX.XXX Wed Apr 29 10:56 - 10:56 (00:00)
XXXXXXXX5 ftp cerberus.XXX.XXX Wed Apr 29 10:05 - 10:20 (00:15)
XXXXXXXX5 ftp cerberus.XXX.XXX Wed Apr 29 09:59 - 09:59 (00:00)
XXXXXXXX5 pts/5 cerberus.XXX.XXX Wed Apr 29 09:50 - 14:22 (04:32)
XXXXXX32 ftp cerberus.XXX.XXX Wed Apr 29 09:13 - 09:14 (00:00)
ftp ftp cerberus.XXX.XXX Wed Apr 29 09:10 - 09:11 (00:00)
ftp ftp cerberus.XXX.XXX Wed Apr 29 09:08 - 09:10 (00:01)
ftp ftp cerberus.XXX.XXX Wed Apr 29 09:08 - 09:08 (00:00)
ftp ftp cerberus.XXX.XXX Wed Apr 29 09:08 - 09:08 (00:00)
ftp ftp cerberus.XXX.XXX Wed Apr 29 09:08 - 09:08 (00:00)
ftp ftp cerberus.XXX.XXX Wed Apr 29 09:07 - 09:08 (00:00)
XXXXXXXX4 ftp cerberus.XXX.XXX Tue Apr 28 14:06 - 14:18 (00:11)
XXXXXXXX4 ftp cerberus.XXX.XXX Tue Apr 28 13:42 - 13:43 (00:01)
XXXXXXXX4 ftp cerberus.XXX.XXX Tue Apr 28 13:06 - 13:42 (00:35)
XXXXXXXX4 ftp cerberus.XXX.XXX Tue Apr 28 11:18 - 11:25 (00:07)
XXXXXXXX4 ftp cerberus.XXX.XXX Tue Apr 28 11:10 - 11:18 (00:08)
XXXXXXXX6 pts/5 mailman.XXX.XXX Mon Apr 27 15:13 - 15:29 (00:15)
XXXXXXXX6 ftp seki Mon Apr 27 12:24 - 12:26 (00:02)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Mon Apr 27 12:09 - 14:26 (02:16)
asdfXXX1 ftp cerberus.XXX.XXX Mon Apr 27 08:38 - 08:38 (00:00)
asdfXXX1 ftp cerberus.XXX.XXX Mon Apr 27 08:16 - 08:17 (00:00)
XXXXXX32 ftp cerberus.XXX.XXX Mon Apr 27 08:07 - 08:09 (00:01)
asdfXXX1 ftp cerberus.XXX.XXX Mon Apr 27 07:42 - 08:07 (00:25)
asdfXXX1 pts/5 cerberus.XXX.XXX Mon Apr 27 07:40 - 08:00 (00:19)
asdfXXX1 ftp cerberus.XXX.XXX Mon Apr 27 07:05 - 07:11 (00:06)
asdfXXX1 pts/5 cerberus.XXX.XXX Mon Apr 27 06:47 - 07:15 (00:27)
asdfXXX1 pts/5 cerberus.XXX.XXX Mon Apr 27 06:44 - 06:47 (00:02)
XXXXXXXX6 ftp cerberus.XXX.XXX Sat Apr 25 01:52 - 01:52 (00:00)
XXXXXXXX6 pts/5 cerberus.XXX.XXX Sat Apr 25 01:41 - 02:09 (00:28)
root console :0 Fri Apr 24 13:46 - 09:36 (13+19:49)
asdfXXX1 pts/2 cerberus.XXX.XXX Fri Apr 24 07:58 - 07:59 (00:00)
ftp ftp cerberus.XXX.XXX Thu Apr 23 13:03 - 13:04 (00:01)
XXXXXXXX5 pts/3 cerberus.XXX.XXX Wed Apr 22 15:54 - 18:03 (02:09)
XXXXXXXX6 ftp cerberus.XXX.XXX Wed Apr 22 15:53 - 15:54 (00:00)
XXXXXXXX6 ftp cerberus.XXX.XXX Wed Apr 22 15:46 - 15:47 (00:00)
XXXXXXXX6 pts/2 cerberus.XXX.XXX Wed Apr 22 15:45 - 18:16 (02:31)
XXXXXXXX6 ftp cerberus.XXX.XXX Wed Apr 22 15:36 - 15:38 (00:01)
XXXXXXXX6 ftp cerberus.XXX.XXX Wed Apr 22 15:35 - 15:36 (00:00)
XXXXXXXX6 pts/2 cerberus.XXX.XXX Wed Apr 22 15:33 - 15:40 (00:07)
XXXXXXXX5 ftp cerberus.XXX.XXX Wed Apr 22 14:13 - 14:13 (00:00)
XXXXXXXX5 pts/4 cerberus.XXX.XXX Wed Apr 22 13:31 - 14:12 (00:41)
XXXX4 ftp cerberus.XXX.XXX Wed Apr 22 13:30 - 13:30 (00:00)
XXXX4 ftp cerberus.XXX.XXX Wed Apr 22 13:28 - 13:29 (00:00)
XXXX4 ftp cerberus.XXX.XXX Wed Apr 22 13:28 - 13:28 (00:00)
XXXX2 ftp cerberus.XXX.XXX Wed Apr 22 13:17 - 13:24 (00:06)
XXXX2 ftp cerberus.XXX.XXX Wed Apr 22 13:12 - 13:12 (00:00)
XXXX2 ftp cerberus.XXX.XXX Wed Apr 22 13:10 - 13:10 (00:00)
XXXX2 ftp cerberus.XXX.XXX Wed Apr 22 13:09 - 13:10 (00:00)
XXXX2 ftp cerberus.XXX.XXX Wed Apr 22 13:08 - 13:09 (00:00)

```

```

-----
XXXX2      ftp      cerberus.XXX.XXX Wed Apr 22 13:07 - 13:08 (00:01)
XXXXXXXX6  pts/3    cerberus.XXX.XXX Wed Apr 22 12:39 - 15:39 (02:59)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Wed Apr 22 12:16 - 14:36 (02:20)
root      console  :0              Wed Apr 22 11:09 - 11:11 (00:02)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Wed Apr 22 09:38 - 11:39 (02:01)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Wed Apr 22 09:36 - 09:37 (00:01)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Wed Apr 22 09:34 - 09:35 (00:01)
XXXXXXXX6  ftp      cerberus.XXX.XXX Tue Apr 21 23:14 - 23:15 (00:00)
XXXXXXXX6  pts/2    cerberus.XXX.XXX Tue Apr 21 22:38 - 00:18 (01:39)
XXXXXXXX6  ftp      seki            Tue Apr 21 14:10 - 14:11 (00:00)
milhaton  ftp      asdfasd.w00t.org Tue Apr 21 12:26 - 12:37 (00:11)
root      console  :0              Tue Apr 21 10:04 - 10:11 (00:07)
XXXXX32   ftp      kuko-dmz        Tue Apr 21 09:38 - 09:38 (00:00)
XXXXXXXX6  pts/2    kuko-dmz        Tue Apr 21 09:11 - 09:37 (00:26)
XXXXX32   ftp      kuko-dmz        Tue Apr 21 09:10 - 09:10 (00:00)
XXXXX32   ftp      kuko-dmz        Tue Apr 21 09:07 - 09:08 (00:00)
XXXXX32   ftp      SECURE8.foob.edu Mon Apr 20 14:49 - 14:57 (00:08)
XXXXX32   ftp      SECUREj.foob.edu Mon Apr 20 14:48 - 14:48 (00:00)
XXXXX32   ftp      SECURE4.foob.edu Mon Apr 20 14:47 - 14:47 (00:00)
XXXXX32   ftp      SECURE5.foob.edu Mon Apr 20 14:39 - 14:39 (00:00)
ftp       ftp      SECURE2.foob.edu Mon Apr 20 14:33 - 14:35 (00:01)
XXXXX32   ftp      SECURE8.foob.edu Mon Apr 20 14:32 - 14:32 (00:00)
ftp       ftp      SECUREj.foob.edu Mon Apr 20 14:24 - 14:24 (00:00)
XXXXX32   ftp      SECURE2.foob.edu Mon Apr 20 14:11 - 14:24 (00:13)
XXXXXXXX6  pts/2    cerberus.XXX.XXX Mon Apr 20 10:07 - 10:08 (00:00)
XXXXX32   ftp      cerberus.XXX.XXX Mon Apr 20 10:07 - 10:08 (00:01)
XXXXX32   ftp      cerberus.XXX.XXX Mon Apr 20 09:53 - 09:56 (00:03)
ftp       ftp      cerberus.XXX.XXX Mon Apr 20 07:05 - 07:05 (00:00)
XXXXXXXX5  ftp      cerberus.XXX.XXX Fri Apr 17 16:58 - 16:59 (00:00)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Fri Apr 17 16:53 - 17:35 (00:41)
XXXXXXXX6  ftp      cerberus.XXX.XXX Fri Apr 17 10:10 - 10:10 (00:00)
XXXXXXXX6  pts/2    cerberus.XXX.XXX Fri Apr 17 08:58 - 11:11 (02:13)
XXXXX32   ftp      cerberus.XXX.XXX Fri Apr 17 07:45 - 08:02 (00:16)
XXXXXXXX5  ftp      cerberus.XXX.XXX Thu Apr 16 20:41 - 20:42 (00:00)
XXXXXXXX4  pts/2    cerberus.XXX.XXX Thu Apr 16 15:13 - 15:19 (00:05)
XXXXXXXX4  pts/2    cerberus.XXX.XXX Thu Apr 16 11:16 - 11:45 (00:29)
ftp       ftp      cerberus.XXX.XXX Thu Apr 16 08:50 - 09:07 (00:16)
ftp       ftp      cerberus.XXX.XXX Thu Apr 16 08:50 - 08:50 (00:00)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Wed Apr 15 17:56 - 18:09 (00:12)
XXXXXXXX6  pts/2    cerberus.XXX.XXX Wed Apr 15 11:05 - 11:34 (00:29)
XXXXX32   ftp      cerberus.XXX.XXX Wed Apr 15 11:04 - 11:05 (00:00)
XXXXX32   ftp      192.168.77.226 Wed Apr 15 07:37 - 07:39 (00:02)
ftp       ftp      192.168.77.226 Wed Apr 15 07:30 - 07:37 (00:07)
asdfXXX1  pts/2    cerberus.XXX.XXX Wed Apr 15 07:20 - 07:21 (00:01)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Tue Apr 14 20:13 - 20:17 (00:03)
ftp       ftp      cerberus.XXX.XXX Tue Apr 14 15:34 - 15:34 (00:00)
ftp       ftp      cerberus.XXX.XXX Tue Apr 14 15:34 - 15:34 (00:00)
ftp       ftp      cerberus.XXX.XXX Tue Apr 14 15:33 - 15:34 (00:00)
XXXXX32   ftp      cerberus.XXX.XXX Tue Apr 14 15:30 - 15:33 (00:03)
XXXXXXXX6  pts/2    cerberus.XXX.XXX Mon Apr 13 23:11 - 23:25 (00:13)
XXXXXXXX6  pts/2    cerberus.XXX.XXX Mon Apr 13 09:51 - 12:40 (02:48)
XXXXXXXX6  pts/2    cerberus.XXX.XXX Sat Apr 11 11:34 - 12:48 (01:14)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Fri Apr 10 12:34 - 13:58 (01:24)
asdfXXX1  pts/3    cerberus.XXX.XXX Fri Apr 10 09:54 - 09:54 (00:00)
XXXXXXXX5  ftp      cerberus.XXX.XXX Fri Apr 10 09:32 - 09:32 (00:00)
XXXXXXXX5  ftp      cerberus.XXX.XXX Fri Apr 10 09:23 - 09:24 (00:00)
XXXXXXXX5  pts/2    cerberus.XXX.XXX Fri Apr 10 08:32 - 10:22 (01:50)

```

```

-----
XXXXX32  ftp          cerberus.XXX.XXX Thu Apr  9 17:43 - 17:45 (00:02)
XXXXX32  ftp          woogah.foobar.c  Thu Apr  9 17:07 - 17:43 (00:35)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Thu Apr  9 16:53 - 16:54 (00:00)
XXXXXXXX6 pts/2       10k.singingbeagl Thu Apr  9 01:42 - 04:09 (02:27)
XXXXXXXX5 ftp          cerberus.XXX.XXX Wed Apr  8 17:02 - 17:03 (00:00)
XXXXXXXX5 ftp          cerberus.XXX.XXX Wed Apr  8 16:59 - 17:00 (00:00)
XXXXXXXX5 pts/2       cerberus.XXX.XXX Wed Apr  8 15:23 - 17:04 (01:40)
XXXXXXXX5 ftp          cerberus.XXX.XXX Wed Apr  8 10:55 - 10:56 (00:00)
XXXXXXXX5 ftp          cerberus.XXX.XXX Wed Apr  8 10:13 - 10:13 (00:00)
XXXXXXXX5 pts/2       cerberus.XXX.XXX Wed Apr  8 09:28 - 11:38 (02:09)
XXXXXXXX6 ftp          cerberus.XXX.XXX Wed Apr  8 02:59 - 03:00 (00:01)
XXXXXXXX6 pts/3       cerberus.XXX.XXX Wed Apr  8 02:53 - 03:01 (00:08)
XXXXXXXX6 pts/5       cerberus.XXX.XXX Wed Apr  8 01:16 - 02:01 (00:45)
XXXXXXXX6 pts/4       cerberus.XXX.XXX Wed Apr  8 01:12 - 02:45 (01:32)
XXXXXXXX6 pts/3       cerberus.XXX.XXX Wed Apr  8 01:08 - 02:45 (01:37)
XXXXXXXX6 ftp          cerberus.XXX.XXX Wed Apr  8 00:59 - 01:00 (00:00)
XXXXXXXX6 ftp          cerberus.XXX.XXX Wed Apr  8 00:58 - 00:58 (00:00)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Wed Apr  8 00:52 - 02:53 (02:00)
XXXXXXXX4 ftp          mailman.XXX.XXX  Tue Apr  7 15:56 - 15:57 (00:01)
XXXXXXXX4 pts/6       cerberus.XXX.XXX Tue Apr  7 15:34 - 16:25 (00:51)
XXXXXXXX4 ftp          mailman.XXX.XXX  Tue Apr  7 14:15 - 14:20 (00:04)
ftp      ftp          cerberus.XXX.XXX Tue Apr  7 14:09 - 14:15 (00:05)
milhaton ftp          cerberus.XXX.XXX Tue Apr  7 13:59 - 14:00 (00:00)
root     console     :0                Tue Apr  7 13:51 - 16:54 (03:03)
XXXXXXXX4 pts/2       cerberus.XXX.XXX Tue Apr  7 12:20 - 13:12 (00:52)
XXXXXXXX4 pts/2       cerberus.XXX.XXX Tue Apr  7 11:32 - 11:32 (00:00)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Mon Apr  6 18:15 - 18:15 (00:00)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Mon Apr  6 17:34 - 18:13 (00:38)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Mon Apr  6 17:05 - 17:22 (00:17)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Sat Apr  4 18:24 - 21:06 (02:42)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Sat Apr  4 18:06 - 18:23 (00:16)
XXXXXXXX4 ftp          cerberus.XXX.XXX Fri Apr  3 10:25 - 10:26 (00:00)
XXXXXXXX4 pts/2       cerberus.XXX.XXX Fri Apr  3 10:23 - 13:02 (02:39)
ftp      ftp          cerberus.XXX.XXX Fri Apr  3 09:51 - 09:51 (00:00)
ftp      ftp          cerberus.XXX.XXX Fri Apr  3 09:51 - 09:51 (00:00)
ftp      ftp          cerberus.XXX.XXX Fri Apr  3 09:51 - 09:51 (00:00)
ftp      ftp          cerberus.XXX.XXX Fri Apr  3 09:51 - 09:51 (00:00)
ftp      ftp          cerberus.XXX.XXX Fri Apr  3 09:51 - 09:51 (00:00)
ftp      ftp          cerberus.XXX.XXX Fri Apr  3 09:50 - 09:51 (00:00)
XXXXXXXX4 pts/2       cerberus.XXX.XXX Fri Apr  3 08:58 - 09:20 (00:22)
XXXXXXXX6 pts/2       cerberus.XXX.XXX Fri Apr  3 08:42 - 08:57 (00:14)
milhaton pts/2       cerberus.XXX.XXX Fri Apr  3 08:42 - 08:42 (00:00)
XXXXXXXX5 ftp          cerberus.XXX.XXX Fri Apr  3 08:18 - 08:18 (00:00)
XXXXXXXX5 ftp          cerberus.XXX.XXX Fri Apr  3 07:42 - 07:43 (00:00)
XXXXXXXX5 ftp          cerberus.XXX.XXX Fri Apr  3 07:29 - 07:30 (00:00)
XXXXXXXX5 pts/2       cerberus.XXX.XXX Fri Apr  3 07:09 - 08:19 (01:10)
ftp      ftp          10k.singingbeagl Fri Apr  3 01:32 - 01:48 (00:16)
milhaton ftp          10k.singingbeagl Fri Apr  3 01:30 - 01:32 (00:01)
XXXXXXXX6 ftp          10k.singingbeagl Fri Apr  3 01:27 - 01:30 (00:02)
XXXXXXXX6 ftp          10k.singingbeagl Fri Apr  3 01:25 - 01:26 (00:00)
milhaton ftp          10k.singingbeagl Fri Apr  3 01:23 - 01:25 (00:01)
XXXXXXXX6 ftp          10k.singingbeagl Fri Apr  3 01:22 - 01:23 (00:00)
milhaton ftp          10k.singingbeagl Fri Apr  3 01:04 - 01:04 (00:00)
milhaton ftp          10k.singingbeagl Fri Apr  3 00:57 - 00:57 (00:00)
milhaton ftp          10k.singingbeagl Fri Apr  3 00:56 - 00:57 (00:00)
milhaton ftp          10k.singingbeagl Fri Apr  3 00:54 - 00:54 (00:00)
milhaton ftp          10k.singingbeagl Fri Apr  3 00:53 - 00:53 (00:00)

```

```

-----
XXXXXXXXX6 ftp 10k.singingbeagl Fri Apr 3 00:43 - 00:43 (00:00)
milhaton ftp 10k.singingbeagl Fri Apr 3 00:43 - 00:43 (00:00)
milhaton ftp 10k.singingbeagl Fri Apr 3 00:34 - 00:34 (00:00)
ftp ftp 10k.singingbeagl Fri Apr 3 00:26 - 00:34 (00:08)
ftp ftp 10k.singingbeagl Fri Apr 3 00:21 - 00:26 (00:04)
ftp ftp 10k.singingbeagl Fri Apr 3 00:19 - 00:21 (00:02)
ftp ftp 10k.singingbeagl Fri Apr 3 00:17 - 00:17 (00:00)
milhaton ftp 10k.singingbeagl Fri Apr 3 00:12 - 00:13 (00:01)
milhaton ftp 10k.singingbeagl Fri Apr 3 00:11 - 00:12 (00:00)
XXXXXXXXX6 ftp 10k.singingbeagl Fri Apr 3 00:10 - 00:10 (00:00)
XXXXXXXXX6 ftp 10k.singingbeagl Fri Apr 3 00:09 - 00:09 (00:00)
XXXXXX32 ftp 10k.singingbeagl Fri Apr 3 00:09 - 00:09 (00:00)
milhaton ftp 10k.singingbeagl Fri Apr 3 00:08 - 00:09 (00:00)
milhaton ftp 10k.singingbeagl Fri Apr 3 00:06 - 00:08 (00:01)
XXXXXXXXX6 ftp 10k.singingbeagl Fri Apr 3 00:01 - 00:01 (00:00)
ftp ftp 10k.singingbeagl Fri Apr 3 00:00 - 00:01 (00:00)
ftp ftp 10k.singingbeagl Thu Apr 2 23:59 - 00:00 (00:01)
XXXXXXXXX6 pts/3 cerberus.XXX.XXX Thu Apr 2 23:46 - 03:39 (03:53)
ftp ftp 10k.singingbeagl Thu Apr 2 23:38 - 23:39 (00:00)
XXXXXXXXX6 ftp 10k.singingbeagl Thu Apr 2 23:37 - 23:38 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Thu Apr 2 23:36 - 23:36 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Thu Apr 2 23:35 - 23:35 (00:00)
XXXXXXXXX6 ftp 10k.singingbeagl Thu Apr 2 23:13 - 23:14 (00:01)
XXXXXXXXX6 ftp cerberus.XXX.XXX Thu Apr 2 23:07 - 23:07 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Thu Apr 2 23:06 - 23:07 (00:00)
ftp ftp 10k.singingbeagl Thu Apr 2 22:51 - 22:51 (00:00)
ftp ftp 10k.singingbeagl Thu Apr 2 22:32 - 22:32 (00:00)
XXXXXXXXX6 pts/3 10k.singingbeagl Thu Apr 2 22:27 - 22:28 (00:00)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Thu Apr 2 22:18 - 01:51 (03:33)
XXXXXXXXX6 pts/2 10k.singingbeagl Thu Apr 2 22:14 - 22:15 (00:00)
XXXXXXXXX6 pts/2 10k.singingbeagl Thu Apr 2 22:09 - 22:14 (00:04)
XXXXXXXXX6 ftp 10k.singingbeagl Thu Apr 2 22:07 - 22:08 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Thu Apr 2 21:52 - 21:53 (00:00)
XXXXXXXXX6 ftp kuko-dmz Thu Apr 2 14:18 - 14:18 (00:00)
XXXXXXXXX6 ftp kuko-dmz Thu Apr 2 14:18 - 14:18 (00:00)
XXXXXXXXX6 pts/3 kuko-dmz Thu Apr 2 14:16 - 16:17 (02:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Thu Apr 2 13:36 - 13:36 (00:00)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Thu Apr 2 13:34 - 16:14 (02:39)
XXXXXXXXX6 pts/2 192.168.84.66 Wed Apr 1 18:50 - 18:53 (00:02)
root ftp cerberus.XXX.XXX Wed Apr 1 18:03 - 18:03 (00:00)
root ftp cerberus.XXX.XXX Wed Apr 1 18:01 - 18:01 (00:00)
root ftp cerberus.XXX.XXX Wed Apr 1 18:01 - 18:01 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Wed Apr 1 18:00 - 18:01 (00:00)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Wed Apr 1 17:59 - 18:47 (00:47)
ftp ftp cerberus.XXX.XXX Wed Apr 1 17:38 - 17:46 (00:07)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Wed Apr 1 15:14 - 15:17 (00:03)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Wed Apr 1 14:29 - 14:49 (00:20)
XXXXXXXXX6 ftp 192.168.84.66 Wed Apr 1 14:28 - 14:28 (00:00)
root console :0 Wed Apr 1 14:21 - 14:22 (00:00)
XXXXXXXXX5 pts/2 cerberus.XXX.XXX Wed Apr 1 14:00 - 14:06 (00:06)
root console :0 Wed Apr 1 10:32 - 11:47 (01:15)
XXXXXXXXX6 pts/3 cerberus.XXX.XXX Sun Mar 29 18:10 - 18:18 (00:08)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Sun Mar 29 17:16 - 20:14 (02:58)
ftp ftp cerberus.XXX.XXX Sun Mar 29 17:00 - 17:00 (00:00)
ftp ftp cerberus.XXX.XXX Sun Mar 29 16:59 - 16:59 (00:00)
XXXXXXXXX5 pts/1 cerberus.XXX.XXX Fri Mar 27 14:48 - 15:20 (00:32)
root console :0 Fri Mar 27 13:45 - 13:48 (00:02)

```

```

-----
XXXXXXXXX5 ftp cerberus.XXX.XXX Fri Mar 27 11:49 - 11:49 (00:00)
XXXXXXXXX5 pts/2 cerberus.XXX.XXX Fri Mar 27 11:38 - 11:48 (00:10)
XXXXXXXXX5 ftp cerberus.XXX.XXX Fri Mar 27 10:58 - 10:58 (00:00)
XXXXXXXXX5 ftp cerberus.XXX.XXX Fri Mar 27 10:39 - 10:40 (00:00)
XXXXXXXXX5 pts/4 cerberus.XXX.XXX Fri Mar 27 10:05 - 10:38 (00:33)
XXXXXXXXX5 ftp cerberus.XXX.XXX Fri Mar 27 09:52 - 09:52 (00:00)
XXXXXXXXX5 pts/1 cerberus.XXX.XXX Fri Mar 27 09:46 - 12:35 (02:49)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Mar 25 16:24 - 16:43 (00:19)
XXXXXXXXX6 ftp cerberus.XXX.XXX Wed Mar 25 15:36 - 15:37 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Wed Mar 25 15:33 - 15:33 (00:00)
XXXXXXXXX5 pts/5 cerberus.XXX.XXX Wed Mar 25 15:31 - 15:35 (00:03)
XXXXXXXXX5 pts/5 cerberus.XXX.XXX Wed Mar 25 15:04 - 15:22 (00:17)
XXXXXXXXX5 pts/5 cerberus.XXX.XXX Wed Mar 25 15:04 - 15:04 (00:00)
XXXXXXXXX6 pts/4 cerberus.XXX.XXX Wed Mar 25 15:00 - 16:44 (01:43)
XXXXXXXXX6 ftp cerberus.XXX.XXX Wed Mar 25 15:00 - 15:15 (00:15)
XXXXXXXXX5 pts/2 cerberus.XXX.XXX Wed Mar 25 14:45 - 15:23 (00:37)
XXXXXXXXX5 ftp cerberus.XXX.XXX Wed Mar 25 14:45 - 14:45 (00:00)
XXXXXXXXX6 pts/2 cerberus.XXX.XXX Wed Mar 25 14:21 - 14:21 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Wed Mar 25 14:21 - 14:21 (00:00)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Mar 25 13:28 - 15:40 (02:11)
XXXXXXXXX5 pts/1 cerberus.XXX.XXX Wed Mar 25 12:42 - 13:18 (00:35)
XXXXXXXXX5 ftp cerberus.XXX.XXX Wed Mar 25 12:15 - 12:16 (00:00)
XXXXXXXXX5 ftp cerberus.XXX.XXX Wed Mar 25 10:03 - 10:03 (00:00)
XXXXXXXXX5 ftp cerberus.XXX.XXX Wed Mar 25 10:01 - 10:02 (00:00)
XXXXXXXXX5 pts/1 cerberus.XXX.XXX Wed Mar 25 09:55 - 12:23 (02:28)
XXXXXXXXX5 ftp cerberus.XXX.XXX Wed Mar 25 09:54 - 09:54 (00:00)
XXXXXXXXX5 pts/4 cerberus.XXX.XXX Wed Mar 25 09:25 - 09:52 (00:27)
XXXXXXXXX6 pts/4 cerberus.XXX.XXX Tue Mar 24 18:04 - 18:05 (00:00)
root console :0 Tue Mar 24 17:38 - 09:49 (16:10)
root console :0 Mon Mar 23 18:50 - 19:03 (00:12)
root console :0 Mon Mar 23 18:47 - 18:48 (00:00)
reboot system boot Thu Mar 19 12:45
root console :0 Thu Mar 19 12:15 - 12:16 (00:01)
XXXXXXXXX5 pts/1 192.168.84.65 Thu Mar 19 11:10 - 11:13 (00:02)
XXXXXXXXX5 console Thu Mar 19 11:06 - 11:11 (00:04)
XXXXXXXXX5 console :0 Thu Mar 19 11:05 - 11:06 (00:00)
XXXXXXXXX5 console :0 Thu Mar 19 11:05 - 11:05 (00:00)
XXXXXXXXX5 console :0 Thu Mar 19 11:05 - 11:05 (00:00)
XXXXXXXXX5 console :0 Thu Mar 19 11:04 - 11:04 (00:00)
XXXXXXXXX6 pts/1 cerberus.XXX.XXX Wed Mar 11 16:26 - 17:56 (01:30)
root console :0 Wed Mar 11 14:41 - 14:51 (00:09)
root console :0 Wed Mar 11 12:37 - 12:38 (00:01)
root console :0 Wed Mar 11 12:29 - 12:34 (00:04)
root console :0 Wed Mar 11 10:38 - 10:43 (00:04)
XXXXXXXXX6 ftp cerberus.XXX.XXX Tue Mar 10 19:03 - 19:03 (00:00)
XXXXXXXXX6 ftp 192.168.84.200 Tue Mar 10 19:01 - 19:01 (00:00)
XXXXXXXXX6 ftp cerberus.XXX.XXX Tue Mar 10 18:55 - 18:55 (00:00)
XXXXXXXXX6 pts/3 cerberus.XXX.XXX Tue Mar 10 18:23 - 19:33 (01:10)
root console :0 Tue Mar 10 15:33 - 15:57 (00:23)
ftp ftp cerberus.XXX.XXX Wed Feb 25 10:21 - 10:21 (00:00)
ftp ftp cerberus.XXX.XXX Wed Feb 25 10:20 - 10:21 (00:00)
XXXXXXXXX6 pts/5 cerberus.XXX.XXX Wed Feb 25 09:59 - 12:11 (02:11)
XXXXXXXXX5 pts/7 cerberus.XXX.XXX Wed Feb 25 09:53 - 10:10 (00:16)
XXXXXXXXX6 pts/6 cerberus.XXX.XXX Wed Feb 25 09:52 - 12:02 (02:10)
XXXXXXXXX5 pts/5 cerberus.XXX.XXX Wed Feb 25 09:44 - 09:54 (00:09)
XXXXXXXXX6 pts/4 cerberus.XXX.XXX Wed Feb 25 09:34 - 11:44 (02:10)
XXXXXXXXX6 pts/3 cerberus.XXX.XXX Wed Feb 25 09:15 - 11:26 (02:10)

```



```

-----
XXXXX32  ftp      cerberus.XXX.XXX Tue Feb 24 18:07 - 18:08 (00:00)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:57 - 17:58 (00:00)
XXXXXXXX6 pts/4    cerberus.XXX.XXX Tue Feb 24 17:57 - 18:08 (00:11)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:46 - 17:48 (00:01)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 17:46 - 17:46 (00:00)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:41 - 17:43 (00:02)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:33 - 17:35 (00:01)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:32 - 17:32 (00:00)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:31 - 17:32 (00:00)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:28 - 17:31 (00:03)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:26 - 17:28 (00:01)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:25 - 17:26 (00:00)
ftp      ftp      cerberus.XXX.XXX Tue Feb 24 17:17 - 17:25 (00:07)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 17:17 - 17:17 (00:00)
XXXXXXXX6 pts/3    cerberus.XXX.XXX Tue Feb 24 17:16 - 20:01 (02:45)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 17:04 - 17:17 (00:13)
XXXXXXXX6 pts/8    cerberus.XXX.XXX Tue Feb 24 16:27 - 19:22 (02:55)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 16:26 - 16:41 (00:15)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 16:24 - 16:24 (00:00)
XXXXXXXX6 pts/7    cerberus.XXX.XXX Tue Feb 24 16:21 - 18:35 (02:13)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 16:20 - 16:20 (00:00)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 15:50 - 16:06 (00:15)
XXXXXXXX6 pts/6    cerberus.XXX.XXX Tue Feb 24 15:02 - 18:18 (03:16)
XXXXXXXX6 pts/5    cerberus.XXX.XXX Tue Feb 24 14:55 - 17:06 (02:10)
XXXXXXXX6 pts/4    cerberus.XXX.XXX Tue Feb 24 14:41 - 16:53 (02:11)
XXXXXXXX6 pts/3    cerberus.XXX.XXX Tue Feb 24 14:24 - 16:50 (02:25)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 14:20 - 14:36 (00:15)
XXXXXXXX6 pts/5    cerberus.XXX.XXX Tue Feb 24 11:25 - 13:38 (02:13)
XXXXXXXX6 pts/4    cerberus.XXX.XXX Tue Feb 24 11:09 - 13:29 (02:20)
XXXXXXXX6 ftp      cerberus.XXX.XXX Tue Feb 24 11:08 - 11:08 (00:00)
XXXXXXXX6 pts/3    cerberus.XXX.XXX Tue Feb 24 11:06 - 13:15 (02:08)
XXXXXXXX6 pts/3    cerberus.XXX.XXX Sun Feb 22 15:16 - 17:29 (02:13)
XXXXXXXX5 pts/3    cerberus.XXX.XXX Tue Feb 17 14:05 - 14:09 (00:03)
XXXXXXXX5 pts/3    cerberus.XXX.XXX Tue Feb 17 13:50 - 13:54 (00:04)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Fri Feb 13 14:29 - 14:31 (00:02)
XXXXXXXX5 ftp      cerberus.XXX.XXX Fri Feb 13 14:29 - 14:29 (00:00)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Fri Feb 13 12:07 - 14:22 (02:15)
XXXXXXXX5 pts/3    cerberus.XXX.XXX Fri Feb 13 10:45 - 13:01 (02:15)
XXXXXXXX5 ftp      cerberus.XXX.XXX Fri Feb 13 10:38 - 10:38 (00:00)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Fri Feb 13 10:34 - 10:45 (00:10)
XXXXXXXX5 ftp      cerberus.XXX.XXX Fri Feb 13 10:33 - 10:33 (00:00)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Fri Feb 13 10:11 - 10:34 (00:23)
XXXXXXXX5 pts/2    cerberus.XXX.XXX Fri Feb 13 10:00 - 10:11 (00:10)
XXXXXXXX5 pts/2    cerberus.XXX.XXX Fri Feb 13 10:00 - 10:00 (00:00)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Fri Feb 13 09:45 - 10:01 (00:15)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Fri Feb 13 09:37 - 09:45 (00:08)
XXXXXXXX5 pts/2    cerberus.XXX.XXX Fri Feb 13 09:34 - 09:35 (00:01)
XXXXXXXX5 ftp      cerberus.XXX.XXX Fri Feb 13 09:30 - 09:33 (00:03)
XXXXXXXX5 ftp      cerberus.XXX.XXX Fri Feb 13 09:16 - 09:21 (00:05)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Fri Feb 13 09:15 - 09:35 (00:19)
XXXXXXXX6 pts/2    cerberus.XXX.XXX Thu Feb 12 16:04 - 18:23 (02:18)
XXXXXXXX2 pts/1    cerberus.XXX.XXX Thu Feb 12 15:49 - 18:05 (02:16)
XXXXXXXX2 pts/1    cerberus.XXX.XXX Wed Feb 11 16:57 - 16:58 (00:00)
XXXXXXXX2 pts/1    cerberus.XXX.XXX Wed Feb 11 16:56 - 16:57 (00:01)
XXXXXXXX5 pts/2    cerberus.XXX.XXX Wed Feb 11 16:48 - 16:49 (00:01)
XXXXXXXX2 pts/1    cerberus.XXX.XXX Wed Feb 11 16:47 - 16:51 (00:03)
XXXXXXXX5 pts/1    cerberus.XXX.XXX Wed Feb 11 16:18 - 16:18 (00:00)

```

```

-----
XXXXXX2 pts/4 localhost Wed Feb 11 16:15 - 16:15 (00:00)
root console :0 Wed Feb 11 16:07 - 16:17 (00:10)
root console :0 Wed Feb 11 10:18 - 10:22 (00:04)
reboot system boot Mon Feb 9 15:19
root console :0 Mon Feb 2 09:19 - down (7+06:00)
root console :0 Mon Feb 2 09:18 - 09:18 (00:00)
root console :0 Fri Jan 30 13:38 - 14:24 (00:46)
root console :0 Fri Jan 30 13:01 - 13:31 (00:29)
root console :0 Thu Jan 29 09:08 - 10:02 (00:53)
root console :0 Wed Jan 28 16:08 - 16:24 (00:16)
reboot system boot Wed Jan 28 16:06
root console :0 Wed Jan 28 16:03 - 16:06 (00:02)
root console :0 Wed Jan 28 16:02 - 16:03 (00:01)
reboot system boot Wed Jan 28 15:56
root console :0 Wed Jan 28 15:19 - 15:56 (00:37)
root ftp 192.168.84.65 Wed Jan 28 15:13 - 15:16 (00:02)
root console :0 Tue Jan 27 18:00 - 18:03 (00:02)
reboot system boot Tue Jan 27 17:59
root ftp 192.168.84.65 Tue Jan 27 17:27 - 17:32 (00:04)
root console :0 Tue Jan 27 17:26 - 17:58 (00:32)
root console :0 Mon Jan 26 17:51 - 17:54 (00:02)
reboot system boot Mon Jan 26 17:49
root console :0 Mon Jan 26 17:31 - 17:49 (00:17)
reboot system boot Mon Jan 26 17:25

```

wtmp begins Mon Jan 26 17:25

# logins -x

```

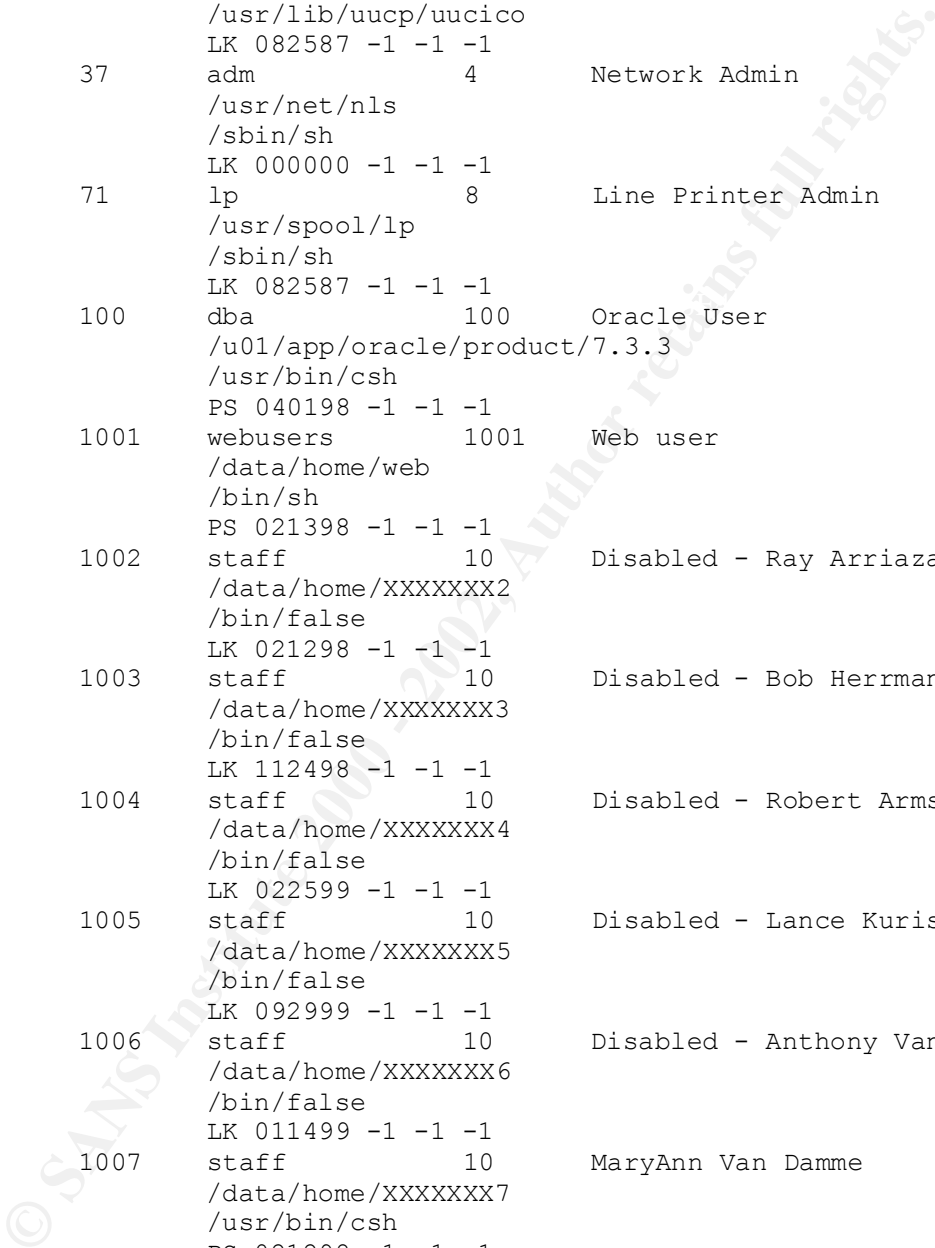
root      0      other      1      Super-User
          /
          /sbin/sh
smtp      0      PS 120699 -1 -1 -1
          root      0      Mail Daemon User
          /
          /sbin/sh
daemon   1      LK 082587 -1 -1 -1
          other      1
          /
          /sbin/sh
bin       2      LK 082587 -1 -1 -1
          bin      2
          /usr/bin
          /sbin/sh
sys       3      LK 082587 -1 -1 -1
          sys      3
          /
          /sbin/sh
adm       4      LK 082587 -1 -1 -1
          adm      4      Admin
          /var/adm
          /sbin/sh
uucp     5      LK 082587 -1 -1 -1
          uucp     5      uucp Admin
          /usr/lib/uucp
          /sbin/sh
smap     6      LK 082587 -1 -1 -1
          mail     6      SMAP Daemon User

```

```

.....
          /var/spool/smap
          /sbin/sh
          LK 082587 -1 -1 -1
nuucp      9          nuucp      9          uucp Admin
          /var/spool/uucppublic
          /usr/lib/uucp/uucico
          LK 082587 -1 -1 -1
listen    37          adm      4          Network Admin
          /usr/net/nls
          /sbin/sh
          LK 000000 -1 -1 -1
lp        71          lp      8          Line Printer Admin
          /usr/spool/lp
          /sbin/sh
          LK 082587 -1 -1 -1
oracle    100         dba      100         Oracle User
          /u01/app/oracle/product/7.3.3
          /usr/bin/csh
          PS 040198 -1 -1 -1
web       1001        webusers 1001        Web user
          /data/home/web
          /bin/sh
          PS 021398 -1 -1 -1
XXXXXXXX2 1002         staff    10          Disabled - Ray Arriaza
          /data/home/XXXXXXXX2
          /bin/false
          LK 021298 -1 -1 -1
XXXXXXXX3 1003         staff    10          Disabled - Bob Herrman
          /data/home/XXXXXXXX3
          /bin/false
          LK 112498 -1 -1 -1
XXXXXXXX4 1004         staff    10          Disabled - Robert Armstrong
          /data/home/XXXXXXXX4
          /bin/false
          LK 022599 -1 -1 -1
XXXXXXXX5 1005         staff    10          Disabled - Lance Kurisaki
          /data/home/XXXXXXXX5
          /bin/false
          LK 092999 -1 -1 -1
XXXXXXXX6 1006         staff    10          Disabled - Anthony Van Damme
          /data/home/XXXXXXXX6
          /bin/false
          LK 011499 -1 -1 -1
XXXXXXXX7 1007         staff    10          MaryAnn Van Damme
          /data/home/XXXXXXXX7
          /usr/bin/csh
          PS 021298 -1 -1 -1
XXXXXX8  1008         webusers 1001        Rocky Weber
          /data/home/asdfXXX1
          /bin/csh
          PS 110599 -1 -1 -1
XXXXXXXX9 1009         staff    10          Andre Jackson
          /data/home/XXXXXXXX9
          /usr/bin/csh
          PS 022399 -1 -1 -1
XXXXXXXX11 1011        staff    10          Disabled - Todd Allaria
          /data/home/XXXXXXXX11

```



```

.....
/bin/false
LK 080698 -1 -1 -1
XXXXXX12      1012  staff          10      Sean Bridgewater
/data/home/XXXXXX12
/usr/bin/csh
PS 010899 -1 -1 -1
XXXXXX13      1013  staff          10      Disabled - Richard Jensen
/data/home/XXXXXX13
/bin/false
LK 032399 -1 -1 -1
XXXXXX14      1014  staff          10      Disabled - Jeff Thomas
/data/home/XXXXXX14
/bin/false
LK 081399 -1 -1 -1
XXXXXX15      1015  webusers      1001    Disabled - Teresa Mulvihill
/data/home/XXXXXX15
/bin/false
LK 092199 -1 -1 -1
XXXXXX40      1016  staff          10      Mark Graves
/data/home/XXXXXX40
/usr/bin/csh
PS 042800 -1 -1 -1
ftp           30000  ftp           30000   Anonymous FTP
/ftp/home/ftp/./
/bin/false
LK 083099 -1 -1 -1
XXXXXX31      30001  ftp           30000   IP Team
/ftp01/home/XXXXXX31/./distribution
/bin/false
PS 121799 -1 -1 -1
XXXXXX32      30002  ftp           30000   Checkpoint
/ftp02/home/vendors/XXXXXX32/./incoming
/bin/false
LK 110598 -1 -1 -1
XXX33         30003  ftp           30000   Axent
/ftp02/home/vendors/XXX33/./incoming
/bin/false
LK 110598 -1 -1 -1
X34           30004  ftp           30000   KLA Tencor
/ftp02/home/customers/X34/./incoming
/bin/false
LK 022399 -1 -1 -1
XXXXX35       30005  ftp           30000   Alteon
/ftp02/home/vendors/XXXXX35/./incoming
/bin/false
PS 040699 -1 -1 -1
XXXXX36       30006  ftp           30000   Boeing
/ftp02/home/customers/XXXXX36/./outgoing
/bin/false
PS 050699 -1 -1 -1
X37           30007  ftp           30000   Apt Search
/ftp02/home/customers/X37/./outgoing
/bin/false
PS 042999 -1 -1 -1
XXXXXX38      30008  ftp           30000   Princess Cruise
/ftp02/home/customers/XXXXXX38/./incoming
/bin/false

```

```

.....
internal      30009    PS 090199 -1 -1 -1
              ftp          30000
              /ftp02/home/customers/internal/./incoming
              /dev/null
X41           30010    PS 102400 -1 -1 -1
              ftp          30000
              /ftp02/home/customers/X41/./outgoing
              /dev/null
patches      30500    PS 111400 -1 -1 -1
              ftp          30000    Support
              /ftp02/home/customers/patches/./distribution
              /bin/false
XXXXX40      30501    PS 083099 -1 -1 -1
              other        1
              /home/XXXXX40
              /bin/sh
jpurvis      30502    PS 050500 -1 -1 -1
              sysadmin      14
              /data/home/jpurvis
              /bin/ksh
nobody       60001    PS 102400 -1 -1 -1
              nobody        60001    Nobody
              /
              /sbin/sh
noaccess     60002    LK 082587 -1 -1 -1
              noaccess      60002    No Access User
              /
              /sbin/sh
nobody4      65534    LK 082587 -1 -1 -1
              nogroup       65534    SunOS 4.x Nobody
              /
              /sbin/sh
              LK 082587 -1 -1 -1

```

```

# mount
/ on /dev/dsk/c0t0d0s0 read/write/setuid/largefiles on Tue Apr 25 21:44:28
2000
/usr on /dev/dsk/c0t0d0s6 read/write/setuid/largefiles on Tue Apr 25 21:44:28
2000
/proc on /proc read/write/setuid on Tue Apr 25 21:44:28 2000
/dev/fd on fd read/write/setuid on Tue Apr 25 21:44:28 2000
/var on /dev/dsk/c0t0d0s1 read/write/setuid/largefiles on Tue Apr 25 21:44:28
2000
/opt on /dev/dsk/c0t0d0s5 setuid/read/write/largefiles on Tue Apr 25 21:44:29
2000
/ftp02 on /dev/dsk/c0t1d0s6 setuid/read/write/largefiles on Tue Apr 25
21:44:29 2000
/ftp01 on /dev/dsk/c0t1d0s7 setuid/read/write/largefiles on Tue Apr 25
21:44:29 2000
/data on /dev/dsk/c0t2d0s7 setuid/read/write/largefiles on Tue Apr 25
21:44:29 2000
/tmp on swap read/write on Tue Apr 25 21:44:29 2000

```

```
# netstat
```

```
TCP
Local Address      Remote Address    Swind Send-Q Rwind Recv-Q  State
```

```

-----
localhost.33287      localhost.32772      32768      0 32768      0
ESTABLISHED
localhost.32772      localhost.33287      32768      0 32768      0
ESTABLISHED
localhost.33290      localhost.33285      32768      0 32768      0
ESTABLISHED
localhost.33285      localhost.33290      32768      0 32768      0
ESTABLISHED
localhost.33293      localhost.33292      32768      0 32768      0
ESTABLISHED
localhost.33292      localhost.33293      32768      0 32768      0
ESTABLISHED
localhost.33296      localhost.33285      32768      0 32768      0
ESTABLISHED
localhost.33285      localhost.33296      32768      0 32768      0
ESTABLISHED
localhost.33299      localhost.33298      32768      0 32768      0
ESTABLISHED
localhost.33298      localhost.33299      32768      0 32768      0
ESTABLISHED
localhost.33302      localhost.33285      32768      0 32768      0
ESTABLISHED
localhost.33285      localhost.33302      32768      0 32768      0
ESTABLISHED
localhost.33305      localhost.33304      32768      0 32768      0
ESTABLISHED
localhost.33304      localhost.33305      32768      0 32768      0
ESTABLISHED
localhost.41708      localhost.33285      32768      0 32768      0
ESTABLISHED
localhost.33285      localhost.41708      32768      0 32768      0
ESTABLISHED
localhost.41711      localhost.41710      32768      0 32768      0
ESTABLISHED
localhost.41710      localhost.41711      32768      0 32768      0
ESTABLISHED
kumo.22              172.16.2.47.756     32120      0 8760      0
ESTABLISHED

```

Active UNIX domain sockets

Address	Type	Vnode	Conn	Local Addr	Remote Addr
6032f210	stream-ord	0	0		
6032fe10	stream-ord	60057470	0	/tmp/.X11-unix/X0	

# netstat -a

UDP

Local Address	Remote Address	State
*.sunrpc		Idle
*.*		Unbound
*.32771		Idle
*.177		Idle
*.syslog		Idle
*.*		Unbound

TCP

Local Address	Remote Address	Swind	Send-Q	Rwind	Recv-Q	State
*.*	*.*	0	0	0	0	IDLE
*.sunrpc	*.*	0	0	0	0	LISTEN
*.*	*.*	0	0	0	0	IDLE
*.smtp	*.*	0	0	0	0	LISTEN
*.fs	*.*	0	0	0	0	LISTEN
*.dtspc	*.*	0	0	0	0	LISTEN
*.32772	*.*	0	0	0	0	LISTEN
*.22	*.*	0	0	0	0	LISTEN
*.32773	*.*	0	0	0	0	LISTEN
*.80	*.*	0	0	0	0	LISTEN
*.6000	*.*	0	0	0	0	LISTEN
*.33285	*.*	0	0	0	0	LISTEN
localhost.33287	localhost.32772	32768	0	32768	0	ESTABLISHED
localhost.32772	localhost.33287	32768	0	32768	0	ESTABLISHED
localhost.33290	localhost.33285	32768	0	32768	0	ESTABLISHED
localhost.33285	localhost.33290	32768	0	32768	0	ESTABLISHED
localhost.33293	localhost.33292	32768	0	32768	0	ESTABLISHED
localhost.33292	localhost.33293	32768	0	32768	0	ESTABLISHED
localhost.33296	localhost.33285	32768	0	32768	0	ESTABLISHED
localhost.33285	localhost.33296	32768	0	32768	0	ESTABLISHED
localhost.33299	localhost.33298	32768	0	32768	0	ESTABLISHED
localhost.33298	localhost.33299	32768	0	32768	0	ESTABLISHED
localhost.33302	localhost.33285	32768	0	32768	0	ESTABLISHED
localhost.33285	localhost.33302	32768	0	32768	0	ESTABLISHED
localhost.33305	localhost.33304	32768	0	32768	0	ESTABLISHED
localhost.33304	localhost.33305	32768	0	32768	0	ESTABLISHED
*.ftp	*.*	0	0	0	0	LISTEN
*.33313	*.*	0	0	0	0	LISTEN
localhost.41708	localhost.33285	32768	0	32768	0	ESTABLISHED
localhost.33285	localhost.41708	32768	0	32768	0	ESTABLISHED
localhost.41711	localhost.41710	32768	0	32768	0	ESTABLISHED
localhost.41710	localhost.41711	32768	0	32768	0	ESTABLISHED
kumo.ftp	172.16.2.47.59512	0	0	8855	0	LISTEN
kumo.22	172.16.2.47.756	32120	0	8760	0	ESTABLISHED
*.*	*.*	0	0	0	0	IDLE

Active UNIX domain sockets

```
-----
Address Type Vnode Conn Local Addr Remote Addr
6032f210 stream-ord 0 0
6032fe10 stream-ord 60057470 0 /tmp/.X11-unix/X0
```

```
# netstat -i
```

```
Name Mtu Net/Dest Address Ipkts Ierrs Opkts Oerrs Collis
Queue
lo0 8232 loopback localhost 71164 0 71164 0 0 0
le0 1500 kumo kumo 316698 0 313156 1 619 0
```

```
# netstat -l
```

```
usage: netstat [ -adgimnprsDMv ] [-I interface] [interval] [system] [core]
```

```
# netstat -p
```

```
Net to Media Table
```

```
Device IP Address Mask Flags Phys Addr
-----
le0 kuko-dmz 255.255.255.255 08:00:20:9a:25:78
le0 172.16.2.47 255.255.255.255 00:10:a4:ed:86:f4
le0 kumo 255.255.255.255 SP 08:00:20:7c:50:84
le0 BASE-ADDRESS.MCAST.NET 240.0.0.0 SM 01:00:5e:00:00:00
```

```
# netstat -rn
```

```
Routing Table:
```

```
Destination Gateway Flags Ref Use Interface
-----
172.16.2.0 172.16.2.1 U 3 5163 le0
224.0.0.0 172.16.2.1 U 3 0 le0
default 172.16.2.254 UG 0 51268
127.0.0.1 127.0.0.1 UH 0 71131 lo0
```

```
# ps -elf
```

```
F S UID PID PPID C PRI NI ADDR SZ WCHAN STIME TTY
TIME CMD
19 T root 0 0 0 0 SY 10416f88 0 Apr 25 ?
0:00 sched
8 S root 1 0 0 41 20 60333608 165 60333800 Apr 25 ?
0:03 /etc/init -
19 S root 2 0 0 0 SY 60332f48 0 10432c34 Apr 25 ?
0:00 pageout
19 S root 3 0 0 0 SY 60332888 0 10435cdc Apr 25 ?
176:28 fsflush
8 S root 196 1 0 41 20 60331448 184 60029c78 Apr 25 ?
0:00 /usr/lib/saf/sac -t 300
8 S root 172 1 0 41 20 603306c8 281 600a4d46 Apr 25 ?
0:01 /usr/sbin/vold
8 S root 9967 1 0 61 20 60331b08 192 600a5a16 Aug 18 console
0:00 /usr/lib/saf/ttymon -g -h -p kumo c
8 S root 107 1 0 41 20 604761d0 236 600a5016 Apr 25 ?
0:01 /usr/sbin/rpcbind
8 S root 157 1 0 41 20 60476f50 299 60477148 Apr 25 ?
0:32 /usr/sbin/nscd
8 S smap 163 1 0 41 20 60330008 188 60330200 Apr 25 ?
0:00 /usr/local/etc/smapd
8 S root 151 1 0 51 20 60477610 189 60029eb8 Apr 25 ?
0:12 /usr/sbin/cron
```



```

.....
 8 S      root    137      1  0  41 20 60476890      400 60476f38   Apr 25 ?
0:03 /usr/sbin/syslogd -n -z 14
 8 S      root    109      1  0  89 20 60330d88      248 600a5066   Apr 25 ?
0:00 /usr/sbin/keyserv
 8 S      root    134      1  0  41 20 603321c8      218 600a4ed6   Apr 25 ?
0:00 /usr/sbin/inetd -s
 8 S      root   3368  3323  0  40 20 6060a8a0      622 600a41b6   Oct 24 pts/2
0:00 [ sdt_shel ]
 8 S      root    170      1  0  40 20 60475450      112 600a4e36   Apr 25 ?
0:00 /usr/lib/utmpd
 8 S      root   3385      1  0  40 20 605a8898      504 600a42a6   Oct 24 pts/2
0:26 /usr/dt/bin/ttssession
 8 S      root   3408  3405  0  40 20 60609b20      849 60354d38   Oct 24 pts/2
0:00 dtfile -noview
 8 S      root   3394      1  0  79 20 60660f68      200 60660fd8   Oct 24 ?
0:00 /bin/ksh /usr/dt/bin/sdtvolcheck -d
 8 S      root    183      1  0  51 20 605a9618      212 600a508e   Apr 25 ?
2:19 /usr/local/sbin/sshd
 8 S      root    189      1  0  51 20 605a8f58      724 600a4936   Apr 25 ?
0:00 /usr/dt/bin/dtlogin -daemon
 8 S      root   3404  3385  0  47 20 6065f468      113 6065f4d8   Oct 24 pts/2
0:00 /bin/sh -c dtfile -noview
 8 S      root    193      1  0  40 20 605a7b18      370 605a7d10   Apr 25 ?
0:01 /usr/local/etc/httpd/bin/httpd -f /
 8 S      root    200    196  0  41 20 605a7458      193 605a7650   Apr 25 ?
0:00 /usr/lib/saf/ttymon
 8 S      root  25931   183  4  41 20 6085edc8      222 604bec2e 15:43:11 ?
0:02 /usr/local/sbin/sshd
 8 S      root   3333  3323  0  40 20 60661628      245 600a4666   Oct 24 ?
0:00 /usr/openwin/bin/fbconsole
 8 S      root   3386  3371  0  50 20 6065eda8      772 600a4706   Oct 24 pts/2
0:12 /usr/dt/bin/dtssession
 8 S      root   9972      1  0  40 20 604746d0      245 600a4346   Aug 18 ?
0:00 /usr/openwin/bin/fbconsole -d :0
 8 S      web  17661   193  0  41 20 60609460      377 6072bdec   Nov 07 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S      root   3371  3368  0  43 20 605a81d8        36 605a8248   Oct 24 pts/2
0:00 [ sh ]
 8 S      root   9969   189  0  40 20 60474d90     2062 600a41de   Aug 18 ?
0:57 /usr/openwin/bin/Xsun :0 -nobanner
 8 R      root  25940  25934  0  78 20 6060a1e0        36          15:43:32 pts/3
0:00 -sh
 8 S      root   3392  3386  0  40 20 606086e0      865 600a4616   Oct 24 ?
0:01 dtwm
 8 S      root   9970   189  0  64 20 60608da0      736 60608e10   Aug 18 ?
0:00 /usr/dt/bin/dtlogin -daemon
 8 S      web  18600   193  0  41 20 6085a040      374 604bf03e   Nov 08 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S      web  17675   193  0  41 20 60861648      377 601b7e8c   Nov 07 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S      root   3403  3394  0  69 20 60608020      102 60029138   Oct 24 ?
0:00 /bin/cat /tmp/.removable/notify0
 8 S      root   3405  3404  0  50 20 6060b620      854 600a5796   Oct 24 pts/2
0:05 dtfile -noview
 8 S      root   3370      1  0  40 20 60475b10      246 600a4206   Oct 24 ?
0:00 /usr/dt/bin/dsdm

```

```

.....
 8 S    root  3323  9970  0  40 20 605a6018    202 605a6088   Oct 24 ?
0:00 /bin/ksh /usr/dt/bin/Xsession
 8 S    root  3620   134  0  51 20 606601e8    348 604bffdde   May 05 ?
0:00 /usr/dt/bin/rpc.ttdbserverd
 8 S    web   18597   193  0  41 20 6085bb40    376 601bb20c    Nov 08 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S    web   18598   193  0  41 20 606608a8    377 601ba76c    Nov 08 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S    web   19195   193  0  41 20 6085c8c0    375 6072bf2c    Nov 09 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S    root  3337     1  0  40 10 60474010    503 600a42f6    Oct 24 ?
0:00 /usr/openwin/bin/speckeydsd
 8 S    root  8744  3386  0  51 20 6085c200    335 604bedbe    Oct 27 ?
0:00 /usr/dt/bin/dtexec -open 0 -ttproci
 8 S    web   18601   193  0  41 20 6065e6e8    375 6072be8c    Nov 08 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S    web   17677   193  0  41 20 6060af60    377 601ba6cc    Nov 07 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S    web   18599   193  0  41 20 605a66d8    376 600b43ac    Nov 08 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S    web   17676   193  0  41 20 608608c8    375 601ba4ec    Nov 07 ?
0:00 /usr/local/etc/httpd/bin/httpd -f /
 8 S    jpurvis 25934 25931  0  51 20 6065fb28    199 6065fb98 15:43:12 pts/3
0:00 -ksh
 8 S    nobody 17669   134  0  40 20 6085cf80    344 600a495e    Nov 07 ?
0:00 fs
 8 S    root  8745  8744  0  80 30 60860f88    629 600a42ce    Oct 27 ?
0:00 /usr/dt/bin/dtscreen -mode blank
 8 O    root  25963 25940  1  78 20 6085a700    106                15:43:49 pts/3
0:00 ps -elf

```

```

# rpcinfo -p
  program vers proto  port  service
    100000   4  tcp   111   rpcbind
    100000   3  tcp   111   rpcbind
    100000   2  tcp   111   rpcbind
    100000   4  udp   111   rpcbind
    100000   3  udp   111   rpcbind
    100000   2  udp   111   rpcbind
    100083   1  tcp   32772
1342177279   4  tcp   33285
1342177279   1  tcp   33285
1342177279   3  tcp   33285
1342177279   2  tcp   33285
    100221   1  tcp   33313

```

```

# showrev -a
Hostname: kumo
Hostid: 807c5084
Release: 5.6
Kernel architecture: sun4u
Application architecture: sparc
Hardware provider: Sun_Microsystems
Domain:
Kernel version: SunOS 5.6 Generic August 1997

```

```

OpenWindows version:

```

.....  
OpenWindows Version 3.6 7 July 1997  
No patches are installed

# dmesg

```
Nov 17 15:46
cpu0: SUNW,UltraSPARC (upaid 0 impl 0x10 ver 0x22 clock 143 MHz)
SunOS Release 5.6 Version Generic [UNIX(R) System V Release 4.0]
Copyright (c) 1983-1997, Sun Microsystems, Inc.
mem = 65536K (0x4000000)
avail mem = 60874752
Ethernet address = 8:0:20:7c:50:84
root nexus = Sun Ultra 1 SBus (UltraSPARC 143MHz)
sbus0 at root: UPA 0x1f 0x0 ...
espdma0 at sbus0: SBus0 slot 0xe offset 0x8400000
esp0:   esp-options=0x46

esp0 at espdma0: SBus0 slot 0xe offset 0x8800000 Onboard device sparc9 ipl 4
sd0 at esp0: target 0 lun 0
sd0 is /sbus@1f,0/espdma@e,8400000/esp@e,8800000/sd@0,0
    <SUN2.1G cyl 2733 alt 2 hd 19 sec 80>
sd1 at esp0: target 1 lun 0
sd1 is /sbus@1f,0/espdma@e,8400000/esp@e,8800000/sd@1,0
    <SUN2.1G cyl 2733 alt 2 hd 19 sec 80>
sd2 at esp0: target 2 lun 0
sd2 is /sbus@1f,0/espdma@e,8400000/esp@e,8800000/sd@2,0
    <SUN2.1G cyl 2733 alt 2 hd 19 sec 80>
sd6 at esp0: target 6 lun 0
sd6 is /sbus@1f,0/espdma@e,8400000/esp@e,8800000/sd@6,0
root on /sbus@1f,0/espdma@e,8400000/esp@e,8800000/sd@0,0:a fstype ufs
zs0 at sbus0: SBus0 slot 0xf offset 0x1100000 Onboard device sparc9 ipl 12
zs0 is /sbus@1f,0/zs@f,1100000
zs1 at sbus0: SBus0 slot 0xf offset 0x1000000 Onboard device sparc9 ipl 12
zs1 is /sbus@1f,0/zs@f,1000000
keyboard is </sbus@1f,0/zs@f,1000000> major <29> minor <2>
mouse is </sbus@1f,0/zs@f,1000000:b> major <29> minor <3>
stdin is </sbus@1f,0/zs@f,1000000> major <29> minor <2>
cgsix0 at sbus0: SBus0 slot 0x2 offset 0x0 SBus level 5 sparc9 ipl 9
cgsix0 is /sbus@1f,0/cgsix@2,0
cgsix0: screen 1152x900, double buffered, 4M mappable, rev 11
stdout is </sbus@1f,0/cgsix@2,0> major <39> minor <0>
ledma0 at sbus0: SBus0 slot 0xe offset 0x8400010
le0 at ledma0: SBus0 slot 0xe offset 0x8c00000 Onboard device sparc9 ipl 6
le0 is /sbus@1f,0/ledma@e,8400010/le@e,8c00000
dump on /dev/dsk/c0t0d0s3 size 262176K

# cat /.dtprofile
#####
###
###   .dtprofile
###
###   user personal environment variables
###
###   Common Desktop Environment (CDE)
###
###   (c) Copyright 1993-1997 Sun Microsystems, Inc.
###   (c) Copyright 1993,1994 Hewlett-Packard Company
```

```

.....
### (c) Copyright 1993,1994 International Business Machines Corp.
### (c) Copyright 1993,1994 Novell, Inc.
###
###
### @(#)dtprofile.src 1.10 97/05/20
###
#####

#####
###
### Your $HOME/.dtprofile is read each time you login to the Common Desktop
### Environment (CDE) and is the place to set or override desktop
### environment variables for your session. Environment variables set in
### $HOME/.dtprofile are made available to all applications on the desktop.
### The desktop will accept either sh or ksh syntax for the commands in
### $HOME/.dtprofile.
###
#####

#####
###
### Random stdout and stderr output from the desktop Session Mgr can be
### directed into user's $HOME/.dt/sessionlogs directory. By default this
### output is not recorded. Instead it is sent off to /dev/null (Unix's
### "nothing" device).
###
### If this random dtsession output is wanted (usually only wanted for
### debugging purposes), commenting out following "dtstart_sessionlogfile"
### lines will send output to your $HOME/.dt/sessionlogs directory.
###
### Alternatively, can change "/dev/null" to "/dev/console" to see this
### debugging output on your console device. Can start a console via the
### Workspace programs menu or via Application Mgr's Desktop Tools
### "Terminal Console" icon.
###
#####

echo "This session log file is currently disabled." >
$dtstart_sessionlogfile
echo "To enable logging, edit $HOME/.dtprofile and" >>
$dtstart_sessionlogfile
echo "remove dtstart_sessionlogfile=/dev/null line." >>
$dtstart_sessionlogfile

export dtstart_sessionlogfile="/dev/null"

#####
###
### By default, the desktop will read your standard $HOME/.profile
### or $HOME/.login files. This can be changed commenting out the
### DTSOURCEPROFILE variable assignment at the end of this file. The
### desktop reads .profile if your $SHELL is "sh" or "ksh", or .login
### if your $SHELL is "csh".
###
###

```

```

.....
### The desktop reads the .dtprofile and .profile/.login with a simulated
### terminal via the sdt_shell program. The sdt_shell program will create
### a controlling terminal. Shell output will be logged to the location
### $HOME/.dt/startlog. Any shell requested input will receive an end
### of file character (Control-D).
###
### This being the case .profile/.login should avoid requiring interaction
### with the user at login time. Any messages printed in these scripts will
### not be seen when you log in and any prompts such as by the "read"
### command will return an end-of-file to the calling script.
###
### With minor editing, it is possible to adapt your .profile or .login
### for use both with and without the desktop. Group user interaction
### statements not appropriate for your desktop session into one section
### and enclose them with an "if" statement that checks for absence of
### of the "DT" environment variable. When the desktop reads your .profile
### or .login file, it will set "DT" to a non-empty value for which your
### .profile or .login can test.
###
### example for sh/ksh
###
###   if [ ! "$DT" ]; then
###       #
###       # commands and environment variables not appropriate for desktop
###       #
###       echo "Please enter some data:"
###       read data
###       ...
###   fi
###
###   #
###   # environment variables common to both desktop and non-desktop
###   #
###   PATH=$HOME/bin:$PATH
###   MYVAR=value
###   export MYVAR
###   ...
###
### example for csh
###
###   if ( ! ${?DT} ) then
###       #
###       # commands and environment variables not appropriate for desktop
###       #
###       echo "Please enter some data:"
###       read data
###       ...
###   endif
###
###   #
###   # environment variables common to both desktop and non-desktop
###   #
###   setenv PATH $HOME/bin:$PATH
###   setenv MYVAR value
###   ...
###

```

```

.....
### Errors in .dtprofile/.profile/.login are logged to
"$HOME/.dt/startlog".
### If after you login, an environment they should have set and exported is
### not present and this $HOME/.dtprofile file has set
"DTSOURCEPROFILE=true"
### check $HOME/.dt/startlog for possible .profile/.login script error
### output.
###
#####
#

DTSOURCEPROFILE=true

# cat /.login
# @(#)local.login 1.3      93/09/15 SMI
stty -istrip
# setenv TERM `tset -Q -`

# cat /.profile
#
# @(#)local.profile 1.4 93/09/15 SMI
#
umask 077
stty istrip
PATH=/usr/local/bin:/bin:/usr/bin:/usr/sbin:/usr/ucb:/etc
export PATH

# cat /data/home/XXXXXXX3/.login
# @(#)local.login 1.3      93/09/15 SMI
stty -istrip
# setenv TERM `tset -Q -`

# cat /data/home/XXXXXXX3/.profile
#
# @(#)local.profile 1.4 93/09/15 SMI
#
umask 077
stty istrip
PATH=/usr/local/bin:/bin:/usr/bin:/usr/sbin:/usr/ucb:/etc:/usr/ccs/bin:.
export PATH

# cat /data/home/asdfXXX1/.login
# @(#)local.login 1.3      93/09/15 SMI
stty -istrip
# setenv TERM `tset -Q -`

# cat /data/home/XXXXX32/etc/group
root::0:root
other::1:
bin::2:root,bin,daemon
sys::3:root,bin,sys,adm
adm::4:root,adm,daemon
uucp::5:root,uucp
mail::6:root
tty::7:root,tty,adm

```

```
.....
lp::8:root,lp,adm
nuucp::9:root,nuucp
staff::10:
daemon::12:root,daemon
sysadmin::14:
nobody::60001:
noaccess::60002:
nogroup::65534:
ftp::30000:ftp

# cat /data/home/XXXXXXX6/.shosts
192.168.61.1 web

# cat /data/home/XXXXXXX6/.ssh/known_hosts
10k.singingbeagle.org 1024 35
13275539567091527588162470426171709799610233092456282301373614356489649559710
12653031973148159741706911884959800068697838408228703820421995213272487394016
57639292324064169301351140585872853726824839454640532691121109099121079152017
71689659816915734421099030536665696189467530573954070311977616428938167747306
1
192.168.84.195 1024 33
11226761931868747481172188323518658035661510728164666273670787081661444319325
63853108882750922901251689820872249117553369338435329092332605158650688917550
27911294398973110003804389482972101255636164438754729601998207508108306392719
69055295735792246473767774899150400932673874139029428993902222164739079163002
7

# cat /data/home/XXXXXXX6/known_hosts
cerberus.XXX.XXX 1024 37
16049639826343881599260485653817118975869289396617828645422116435577238205785
24285632625966897455097670315147440269448490890580530337928659197287510663586
16836435756132997784202782590816898826231940937236516948083914830936077358965
33275068086292444041014866736824431344172345407998736782406099248366129863856
1
192.168.51.4 1024 35
13814241458381655568889947654187511158316561369223591386874313407420796591583
40597973658790894250809851845213432350954516451201964390830596847211963039753
19349617538485322905708025316201970527949937318008184539189771438050744433833
58828385220870261708735985757718491880747764394797878816344368489156382964260
7
192.168.84.66 1024 35
13275539567091527588162470426171709799610233092456282301373614356489649559710
12653031973148159741706911884959800068697838408228703820421995213272487394016
57639292324064169301351140585872853726824839454640532691121109099121079152017
71689659816915734421099030536665696189467530573954070311977616428938167747306
1
192.168.51.10 1024 35
15011973138211389394779543443025172023679944987373675280742638073395215160732
15497608469626624419054926352540356245793698646510263523595258959768192040856
06850860608038132123081045142485328565437104540500423190789500968026760774024
78897106068023746394850660380682096857213156780438066609217588841075450771599
3

# cat /etc/cron.d/at.deny
daemon
bin
smtp
```

```

.....
nuucp
listen
nobody
noaccess

# cat /etc/cron.d/cron.deny
daemon
bin
smtp
nuucp
listen
nobody
noaccess

# cat /etc/default/inetinit
# @(#)inetinit.dfl 1.2 97/05/08
#
# TCP_STRONG_ISS sets the TCP initial sequence number generation parameters.
# Set TCP_STRONG_ISS to be:
#     0 = Old-fashioned sequential initial sequence number generation.
#     1 = Improved sequential generation, with random variance in
increment.
#     2 = RFC 1948 sequence number generation, unique-per-connection-ID.
#
TCP_STRONG_ISS=1

# cat /etc/default/init
# @(#)init.dfl 1.2 92/11/26
#
# This file is /etc/default/init. /etc/TIMEZONE is a symlink to this file.
# This file looks like a shell script, but it is not. To maintain
# compatibility with old versions of /etc/TIMEZONE, some shell constructs
# (i.e., export commands) are allowed in this file, but are ignored.
#
# Lines of this file should be of the form VAR=value, where VAR is one of
# TZ, LANG, or any of the LC_* environment variables.
#
TZ=US/Pacific

# cat /etc/default/kbd
#pragma ident "@(#)kbd.dfl 1.2 96/06/07 SMI"
#
# Copyright 1996, Sun Microsystems, Inc.
# All Rights Reserved.
#
# /etc/default/kbd
#
# kbd default settings processed via kbd(1).
#
# KEYBOARD_ABORT affects the default behavior of the keyboard abort
# sequence, see kbd(1) for details. The default value is "enable".
# The optional value is "disable". Any other value is ignored.
#
# KEYCLICK affects the default keyclick behavior. Possible values are
# 'on' and 'off'. Any other value is ignored. The default behavior is
# to leave the current keyclick setting unchanged.
#

```



```

.....
# Uncomment the following lines to change the default values.
#
#KEYBOARD_ABORT=enable
#KEYCLICK=off

# cat /etc/default/login
#ident "@(#)login.dfl 1.8      96/10/18 SMI" /* SVr4.0 1.1.1.1 */

# Set the TZ environment variable of the shell.
#
#TIMEZONE=EST5EDT

# ULIMIT sets the file size limit for the login.  Units are disk blocks.
# The default of zero means no limit.
#
#ULIMIT=0

# If CONSOLE is set, root can only login on that device.
# Comment this line out to allow remote login by root.
#
CONSOLE=/dev/console

# PASSREQ determines if login requires a password.
#
PASSREQ=YES

# ALTSHELL determines if the SHELL environment variable should be set
#
ALTSHELL=YES

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:

# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin

# TIMEOUT sets the number of seconds (between 0 and 900) to wait before
# abandoning a login session.
#
#TIMEOUT=300

# UMASK sets the initial shell file creation mode mask.  See umask(1).
#
#UMASK=022

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all root logins at level LOG_NOTICE and multiple failed login
# attempts at LOG_CRIT.
#
SYSLOG=YES

# cat /etc/default/passwd
#ident "@(#)passwd.dfl 1.3      92/07/14 SMI"
MAXWEEKS=
MINWEEKS=

```

```

.....
PASSLENGTH=6

# cat /etc/default/su
#ident "@(#)su.dfl 1.6 93/08/14 SMI" /* SVr4.0 1.2 */

# SULONG determines the location of the file used to log all su attempts
#
SULONG=/var/adm/sulog

# CONSOLE determines whether attempts to su to root should be logged
# to the named device
#
#CONSOLE=/dev/console

# PATH sets the initial shell PATH variable
#
#PATH=/usr/bin:

# SUPATH sets the initial shell PATH variable for root
#
#SUPATH=/usr/sbin:/usr/bin

# SYSLOG determines whether the syslog(3) LOG_AUTH facility should be used
# to log all su attempts. LOG_NOTICE messages are generated for su's to
# root, LOG_INFO messages are generated for su's to other users, and LOG_CRIT
# messages are generated for failed su attempts.
#
SYSLOG=YES

# cat /etc/defaultrouter
#192.168.84.158
172.16.2.254

# cat /etc/dfs/dfstab

# Place share(1M) commands here for automatic execution
# on entering init state 3.
#
# Issue the command '/etc/init.d/nfs.server start' to run the NFS
# daemon processes and the share commands, after adding the very
# first entry to this file.
#
# share [-F fstype] [ -o options] [-d "<text>"] <pathname> [resource]
# .e.g,
# share -F nfs -o rw=engineering -d "home dirs" /export/home2

# cat /etc/ftpaccess
loginfails 2

guestgroup ftponly

noretrieve /etc/passwd /etc/group core

class local real,guest,anonymous *.domain 0.0.0.0
class remote real,guest,anonymous *

limit local 100 Any /etc/msgs/msg.toomany

```

```

.....
limit    remote  100 Any                               /etc/msgs/msg.toomany

readme   README*   login
readme   README*   cwd=*

message  /welcome.msg      login
message  .message     cwd=*

compress      no          local remote
tar           no          local remote

# allow use of private file for SITE GROUP and SITE GPASS?
private       yes

# passwd-check <none|trivial|rfc822> [<enforce|warn>]
passwd-check  rfc822  warn

log commands  anonymous,guest
log transfers anonymous,guest,real inbound,outbound

shutdown /etc/msgs/shutmsg

# all the following default to "yes" for everybody
delete        no          anonymous          # delete permission?
overwrite     no          anonymous          # overwrite permission?
rename        no          anonymous          # rename permission?
chmod         no          real,guest,anonymous # chmod permission?
umask         no          real,guest,anonymous # umask permission?

# specify the upload directory information
upload /ftp/home/ftp *          no
upload /ftp/home/ftp /incoming yes      ftp      ftp  0666 dirs
upload /ftp/home/ftp /bin      no
upload /ftp/home/ftp /etc      no

# directory aliases... [note, the ":" is not required]
alias  inc:    /incoming

# cdpath
cdpath /incoming
cdpath /pub
cdpath /

# path-filter...
path-filter anonymous /etc/pathmsg ^[-A-Za-z0-9_\.]*$ ^\  ^-
path-filter  guest   /etc/pathmsg ^[-A-Za-z0-9_\.]*$ ^\  ^-

# specify which group of users will be treated as "guests".
guestgroup ftponly

email XXXXXX15@singingbeagle.org

# cat /etc/ftphosts
# Example host access file
#
# Everything after a '#' is treated as comment,
# empty lines are ignored

```

```

.....
# cat /etc/group
root::0:root,XXXXX40
other::1:jpurvis
bin::2:root,bin,daemon
sys::3:root,bin,sys,adm
adm::4:root,adm,daemon
uucp::5:root,uucp
mail::6:root
tty::7:root,tty,adm
lp::8:root,lp,adm
nuucp::9:root,nuucp
staff::10:XXXXX8,XXXXXX11,jpurvis
daemon::12:root,daemon
sysadmin::14:
nobody::60001:
noaccess::60002:
nogroup::65534:
webusers::1001:web,XXXXXXXX5,XXXXX8,XXXXXXXX6,XXXXXX15
ftp::30000:ftp
ftponly::30001:ftp,XXXXX32,XXXXX31,XXX33,X34,XXXX35,XXXX36,X37,XXXXXX38,patches
dba::100:

# cat /etc/inet/hosts
#
# Internet host table
#
127.0.0.1        localhost
#192.168.84.129 kumo kumo.singingbeagle.org loghost
172.16.2.1      kumo kumo.singingbeagle.org loghost
#
#192.168.84.65  toomi
172.16.1.30     10k.singingbeagle.org
#192.168.84.66 10k.singingbeagle.org

#192.168.84.67 enchi-in
172.16.1.0      seki-int
#192.168.84.94 seki-int
#
172.16.2.254    kuko-dmz
#192.168.84.158 kuko-dmz
#
192.168.84.193 seki
192.168.84.194 enchi-out
192.168.84.200 prowler

# cat /etc/inet/inetd.conf
#
#ident "@(#)inetd.conf 1.27 96/09/24 SMI" /* SVr4.0 1.5 */
#
#
# Configuration file for inetd(1M). See inetd.conf(4).
#
# To re-configure the running inetd process, edit this file, then
# send the inetd process a SIGHUP.
#

```

```

.....
# Syntax for socket-based Internet services:
# <service_name> <socket_type> <proto> <flags> <user> <server_pathname>
<args>
#
# Syntax for TLI-based Internet services:
#
# <service_name> tli <proto> <flags> <user> <server_pathname> <args>
#
# Ftp and telnet are standard Internet services.
#
ftp      stream  tcp      nowait  root    /usr/sbin/in.ftpd      in.ftpd -l -a
#telnet  stream  tcp      nowait  root    /usr/sbin/in.telnetd   in.telnetd
smtp     stream  tcp      nowait  root    /usr/local/etc/smmap    smap
#
# Tnamed serves the obsolete IEN-116 name server protocol.
#
##name   dgram    udp      wait    root    /usr/sbin/in.tnamed    in.tnamed
#
# Shell, login, exec, comsat and talk are BSD protocols.
#
##shell  stream  tcp      nowait  root    /usr/sbin/in.rshd      in.rshd
##login  stream  tcp      nowait  root    /usr/sbin/in.rlogind   in.rlogind
##exec   stream  tcp      nowait  root    /usr/sbin/in.rexecd    in.rexecd
##comsat      dgram    udp      wait    root    /usr/sbin/in.comsat    in.comsat
##talk   dgram    udp      wait    root    /usr/sbin/in.talkd     in.talkd
#
# Must run as root (to read /etc/shadow); "-n" turns off logging in
utmp/wtmp.
#
##uucp   stream  tcp      nowait  root    /usr/sbin/in.uucpd     in.uucpd
#
# Tftp service is provided primarily for booting.  Most sites run this
# only on machines acting as "boot servers."
#
#tftp    dgram    udp      wait    root    /usr/sbin/in.tftpd     in.tftpd -s
/tftpboot
#
# 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/in.fingerd   in.fingerd
#systat  stream  tcp      nowait  root    /usr/bin/ps             ps -ef
#netstat  stream  tcp      nowait  root    /usr/bin/netstat       netstat -f inet
#
# Time service is used for clock synchronization.
#
##time   stream  tcp      nowait  root    internal
##time   dgram    udp      wait    root    internal
#
# Echo, discard, daytime, and chargen are used primarily for testing.
#
##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
#
#
# RPC services syntax:
# <rpc_prog>/<vers> <endpoint-type> rpc/<proto> <flags> <user> \
# <pathname> <args>
#
# <endpoint-type> can be either "tli" or "stream" or "dgram".
# For "stream" and "dgram" assume that the endpoint is a socket descriptor.
# <proto> can be either a nettype or a netid or a "*". The value is
# first treated as a nettype. If it is not a valid nettype then it is
# treated as a netid. The "*" is a short-hand way of saying all the
# transports supported by this system, ie. it equates to the "visible"
# nettype. The syntax for <proto> is:
#      *|<nettype|netid>|<nettype|netid>{[,<nettype|netid>]}
# For example:
# dummy/1      tli      rpc/circuit_v,udp    wait    root    /tmp/test_svc
test_svc
#
# Solstice system and network administration class agent server
##100232/10    tli      rpc/udp wait root /usr/sbin/sadmind   sadmind
#
# Rquotad supports UFS disk quotas for NFS clients
#
##rquotad/1   tli      rpc/datagram_v  wait root /usr/lib/nfs/rquotad
rquotad
#
# The rusers service gives out user information. Sites concerned
# with security may choose to disable it.
#
##rusersd/2-3  tli      rpc/datagram_v,circuit_v    wait root
/usr/lib/netsvc/rusers/rpc.rusersd   rpc.rusersd
#
# The spray server is used primarily for testing.
#
##sprayd/1     tli      rpc/datagram_v  wait root
/usr/lib/netsvc/spray/rpc.sprayd     rpc.sprayd
#
# The rwall server allows others to post messages to users on this machine.
#
##walld/1      tli      rpc/datagram_v  wait root
/usr/lib/netsvc/rwall/rpc.rwalld     rpc.rwalld
#
# Rstatd is used by programs such as perfmeter.
#
##rstatd/2-4   tli      rpc/datagram_v  wait root
/usr/lib/netsvc/rstat/rpc.rstatd     rpc.rstatd
#
# The rexd server provides only minimal authentication and is often not run
#
#rexd/1        tli      rpc/tcp wait root /usr/sbin/rpc.rexd   rpc.rexd
#

```

```

.....
# rpc.cmsd is a data base daemon which manages calendar data backed
# by files in /var/spool/calendar
#
#
# Sun ToolTalk Database Server
#
#
# UFS-aware service daemon
#
#ufsd/1 tli      rpc/*  wait   root   /usr/lib/fs/ufs/ufsd  ufsd -p
#
# Sun KCMS Profile Server
#
100221/1          tli      rpc/tcp wait   root /usr/openwin/bin/kcms_server
kcms_server
#
# Sun Font Server
#
fs                stream  tcp    wait  nobody /usr/openwin/lib/fs.auto  fs
#
# CacheFS Daemon
#
##100235/1 tli rpc/tcp wait root /usr/lib/fs/cachefs/cachefsd cachefsd
#
# Kerbd Daemon
#
##kerbd/4          tli      rpc/ticlts  wait   root   /usr/sbin/kerbd
kerbd
#
# Print Protocol Adaptor - BSD listener
#
##printer          stream  tcp    nowait  root   /usr/lib/print/in.lpd
in.lpd
dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd
##xaudio  stream tcp  wait  root /usr/openwin/bin/Xaserver Xaserver -noauth
-inetd
##100068/2-5 dgram rpc/udp wait root /usr/dt/bin/rpc.cmsd rpc.cmsd
100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd
/usr/dt/bin/rpc.ttdbserverd

# cat /etc/inet/netmasks
#
# The netmasks file associates Internet Protocol (IP) address
# masks with IP network numbers.
#
#      network-number  netmask
#
# The term network-number refers to a number obtained from the Internet
Network
# Information Center.  Currently this number is restricted to being a class
# A, B, or C network number.  In the future we should be able to support
# arbitrary network numbers per the Classless Internet Domain Routing
# guidelines.
#
# Both the network-number and the netmasks are specified in
# "decimal dot" notation, e.g:
#

```

```

.....
#           128.32.0.0 255.255.255.0
#
#192.168.84.0 255.255.255.224
172.16.2.0    255.255.255.0

# cat /etc/mail/aliases
#ident "@(#)aliases 1.13 92/07/14 SMI" /* SVr4.0 1.1 */

##
# Aliases can have any mix of upper and lower case on the left-hand side,
# but the right-hand side should be proper case (usually lower)
#
# >>>>>>>>> The program "newaliases" will need to be run after
# >> NOTE >> this file is updated for any changes to
# >>>>>>>>> show through to sendmail.
#
# @(#)aliases 1.8 86/07/16 SMI
##

# Following alias is required by the mail protocol, RFC 822
# Set it to the address of a HUMAN who deals with this system's mail
problems.
Postmaster: root

# Alias for mailer daemon; returned messages from our MAILER-DAEMON
# should be routed to our local Postmaster.
MAILER-DAEMON: postmaster

# Aliases to handle mail to programs or files, eg news or vacation
# decode: "|/usr/bin/uudecode"
nobody: /dev/null

# Sample aliases:

# Alias for distribution list, members specified here:
#staff:wnj,mosher,sam,ecc,mckusick,sklower,olson,rwh@ernie

# Alias for distribution list, members specified elsewhere:
#keyboards: :include:/usr/jfarrell/keyboards.list

# Alias for a person, so they can receive mail by several names:
#epa:eric

# cat /etc/mnttab
/dev/dsk/c0t0d0s0 / ufs rw,suid,dev=800000,largefiles
956724268
/dev/dsk/c0t0d0s6 /usr ufs rw,suid,dev=800006,largefiles
956724268
/proc /proc proc rw,suid,dev=2900000 956724268
fd /dev/fd fd rw,suid,dev=29c0000 956724268
/dev/dsk/c0t0d0s1 /var ufs rw,suid,dev=800001,largefiles
956724268
/dev/dsk/c0t0d0s5 /opt ufs suid,rw,largefiles,dev=800005
956724269
/dev/dsk/c0t1d0s6 /ftp02 ufs suid,rw,largefiles,dev=80000e
956724269

```



```

.....
/dev/dsk/c0t1d0s7      /ftp01  ufs      suid,rw,largefiles,dev=80000f
956724269
/dev/dsk/c0t2d0s7      /data   ufs      suid,rw,largefiles,dev=800017
956724269
swap    /tmp     tmpfs    dev=1    956724269
kumo:vold(pid172)     /vol    nfs      ignore,noquota,dev=2b00001
956724295

# cat /etc/motd
Sun Microsystems Inc.  SunOS 5.6      Generic August 1997

# cat /etc/nsswitch.conf
#
# /etc/nsswitch.files:
#
# An example file that could be copied over to /etc/nsswitch.conf; it
# does not use any naming service.
#
# "hosts:" and "services:" in this file are used only if the
# /etc/netconfig file has a "-" for nametoaddr_libs of "inet" transports.

passwd:    files
group:     files
hosts:     files dns
networks:  files
protocols: files
rpc:       files
ethers:    files
netmasks:  files
bootparams: files
publickey: files
# At present there isn't a 'files' backend for netgroup; the system will
# figure it out pretty quickly, and won't use netgroups at all.
netgroup:  files
automount: files
aliases:   files
services:  files
sendmailvars: files

# cat /etc/pam.conf
#ident "@(#)pam.conf 1.19      95/11/30 SMI"
#
# PAM configuration
#
# Authentication management
#
login    auth required    /usr/lib/security/pam_unix.so.1
login    auth required    /usr/lib/security/pam_dial_auth.so.1
#
rlogin   auth sufficient  /usr/lib/security/pam_rhosts_auth.so.1
rlogin   auth required    /usr/lib/security/pam_unix.so.1
#
dtlogin  auth required    /usr/lib/security/pam_unix.so.1
#
rsh      auth required    /usr/lib/security/pam_rhosts_auth.so.1
other    auth required    /usr/lib/security/pam_unix.so.1
#

```

```

.....
# Account management
#
login    account required    /usr/lib/security/pam_unix.so.1
dtlogin  account required    /usr/lib/security/pam_unix.so.1
#
other    account required    /usr/lib/security/pam_unix.so.1
#
# Session management
#
other    session required    /usr/lib/security/pam_unix.so.1
#
# Password management
#
other    password required    /usr/lib/security/pam_unix.so.1

# cat /etc/passwd
root::0:1:Super-User:/:/sbin/sh
daemon:x:1:1:/:
bin:x:2:2:./usr/bin:
sys:x:3:3:./:
adm:x:4:4:Admin:/var/adm:
lp:x:71:8:Line Printer Admin:/usr/spool/lp:
smap:x:6:6:SMAP Daemon User:/var/spool/smap:
smtp:x:0:0:Mail Daemon User:./:
uucp:x:5:5:uucp Admin:/usr/lib/uucp:
nuucp:x:9:9:uucp Admin:/var/spool/uucppublic:/usr/lib/uucp/uucico
listen:x:37:4:Network Admin:/usr/net/nls:
nobody:x:60001:60001:Nobody:./:
noaccess:x:60002:60002:No Access User:./:
nobody4:x:65534:65534:SunOS 4.x Nobody:./:
oracle:x:100:100:Oracle User:/u01/app/oracle/product/7.3.3:/usr/bin/csh
web:x:1001:1001:Web user:/data/home/web:/bin/sh
XXXXXXXX2:x:1002:10:Disabled - XXXX:/data/home/XXXXXXXX2:/bin/false
XXXXXXXX3:x:1003:10:Disabled - XXXX:/data/home/XXXXXXXX3:/bin/false
XXXXXXXX4:x:1004:10:Disabled - XXXX:/data/home/XXXXXXXX4:/bin/false
XXXXXXXX5:x:1005:10:Disabled - XXXX:/data/home/XXXXXXXX5:/bin/false
XXXXXXXX6:x:1006:10:Disabled - XXXX:/data/home/XXXXXXXX6:/bin/false
XXXXXXXX7:x:1007:10:XXXX:/data/home/XXXXXXXX7:/usr/bin/csh
XXXXXXXX8:x:1008:1001:XXXX:/data/home/asdfXXX1:/bin/csh
XXXXXXXX9:x:1009:10:XXXX:/data/home/XXXXXXXX9:/usr/bin/csh
XXXXXXXX11:x:1011:10:Disabled - XXXX:/data/home/XXXXXXXX11:/bin/false
XXXXXXXX12:x:1012:10:XXXX:/data/home/XXXXXXXX12:/usr/bin/csh
XXXXXXXX13:x:1013:10:Disabled - XXXX:/data/home/XXXXXXXX13:/bin/false
XXXXXXXX14:x:1014:10:Disabled - XXXX:/data/home/XXXXXXXX14:/bin/false
ftp:x:30000:30000:Anonymous FTP:/ftp/home/ftp/./:/bin/false
XXXXXXXX31:x:30001:30000:XXXX:/ftp01/home/XXXXXXXX31/./distribution:/bin/false
XXXXXXXX32:x:30002:30000:XXXX:/ftp02/home/vendors/XXXXXXXX32/./incoming:/bin/false
XXX33:x:30003:30000:XXXX:/ftp02/home/vendors/XXX33/./incoming:/bin/false
X34:x:30004:30000:XXXX:/ftp02/home/customers/X34/./incoming:/bin/false
XXXXXXXX35:x:30005:30000:Alteon:/ftp02/home/vendors/XXXXXXXX35/./incoming:/bin/false
XXXXXXXX36:x:30006:30000:Boeing:/ftp02/home/customers/XXXXXXXX36/./outgoing:/bin/false
e
X37:x:30007:30000:XXXX:/ftp02/home/customers/X37/./outgoing:/bin/false
XXXXXXXX38:x:30008:30000:XXXX:/ftp02/home/customers/XXXXXXXX38/./incoming:/bin/false
patches:x:30500:30000:Support:/ftp02/home/customers/patches/./distribution:/bin/false

```

```
.....
XXXXXX15:x:1015:1001:Disabled - XXXX:/data/home/XXXXXX15:/bin/false
XXXXX40:x:1016:10:XXXX:/data/home/XXXXX40:/usr/bin/csh
XXXXX40:x:30501:1:::/home/XXXXX40:/bin/sh
jpurvis:x:30502:14:::/data/home/jpurvis:/bin/ksh
internal:x:30009:30000::/ftp02/home/customers/internal/./incoming:/dev/null
X41:x:30010:30000::/ftp02/home/customers/X41/./outgoing:/dev/null
```

```
# cat /etc/resolv.conf
domain XXX.XXX
nameserver 192.168.62.2
nameserver 192.168.62.11
```

```
# cat /etc/rpc
#ident "@(#)rpc          1.11      95/07/14 SMI"      /* SVr4.0 1.2 */
#
#      rpc
#
rpcbind          100000   portmap sunrpc rpcbind
rstatd          100001   rstat rup perfmeter
rusersd         100002   rusers
nfs             100003   nfsprog
ypserv          100004   ypprog
mountd          100005   mount showmount
ypbind          100007
walld           100008   rwall shutdown
yppasswd        100009   yppasswd
etherstatd      100010   etherstat
rquotad         100011   rquotaproq quota rquota
sprayd          100012   spray
3270_mapper     100013
rje_mapper      100014
selection_svc   100015   selnsvc
database_svc    100016
rex             100017   rex
alis            100018
sched           100019
llockmgr        100020
nlockmgr        100021
x25.inr         100022
statmon         100023
status          100024
ypupdated       100028   ypupdate
keyserver       100029   keyserver
bootparam       100026
sunlink_mapper  100033
tfsd            100037
nsd             100038
nsemntd         100039
showfh          100043   showfh
ioadmd          100055   rpc.ioadmd
NETlicense      100062
sunisamd        100065
debug_svc       100066   dbsrv
bugtraqd        100071
kerbd           100078
event           100101   na.event      # SunNet Manager
logger          100102   na.logger     # SunNet Manager
```

```

-----
sync          100104  na.sync
hostperf     100107  na.hostperf
activity     100109  na.activity      # SunNet Manager
hostmem      100112  na.hostmem
sample       100113  na.sample
x25          100114  na.x25
ping         100115  na.ping
rpcnfs       100116  na.rpcnfs
hostif       100117  na.hostif
etherif      100118  na.etherif
iproutes     100120  na.iproutes
layers       100121  na.layers
snmp         100122  na.snmp snmp-cmc snmp-synoptics snmp-unisys snmp-utk
traffic      100123  na.traffic
nfs_acl      100227
sadmind      100232
nisd         100300  rpc.nisd
nispasswd    100303  rpc.nispasswd
ufsd         100233  ufsd
pcnfsd       150001

```

```

# cat /etc/shadow
root:HYG9nQWtJnEDw:10931::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
smmap:NP:6445::::::
smtp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
listen:*LK*::::::
nobody:NP:6445::::::
noaccess:NP:6445::::::
nobody4:NP:6445::::::
oracle:9HYdoknN7Qm6M:10317::::::
web:1kvYWejMEpt9E:10270::::::
XXXXXXXX2:*LK*:10269::::::
XXXXXXXX3:*LK*:10554::::::
XXXXXXXX4:*LK*:10647::::::
XXXXXXXX5:*LK*:10863::::::
XXXXXXXX6:*LK*:10605::::::
XXXXXXXX7:hGM12lHd6Xrec:10269::::::
XXXXXXXX8:mklNkXczA7QvE:10900::::::
XXXXXXXX9:CSsbIoaAtdPNs:10645::::::
XXXXXXXX11:*LK*:10444::::::
XXXXXXXX12:FmCFTMIy.6KB.:10599::::::
XXXXXXXX13:*LK*:10673::::::
ftp:NP:10833::::::
XXXXX31:u7eqNokeHteUg:10942::::::
XXXXX32:*LK*:10535::::::
XXX33:*LK*:10535::::::
X34:*LK*:10645::::::
XXXX35:ySrf71BYBST0c:10687::::::
XXXX36:tJIpQM2WK4NIM:10717::::::
X37:gQaPh02A7ppOc:10710::::::

```

```

.....
patches:u7eqNokeHteUg:10833:.....:
XXXXXX14:*LK*:10816:.....:
XXXXXX38:rYY19HbnWuFh.:10835:.....:
XXXXXX15:*LK*:10855:.....:
XXXXXX40:elASNDmu5tRcM:11075:.....:
XXXXXX40:8mqEBt/uy0Fzs:11082:.....:
jpurvis:/wLYcqbd7VG2:11254:.....:
internal:L5W9mxQPNe5.k:11254:.....:
X41:8KgpAGkUgfkQA:11275:.....:

# cat /etc/skel/.profile
#     This is the default standard profile provided to a user.
#     They are expected to edit it to meet their own needs.

MAIL=/usr/mail/${LOGNAME:?}

# cat /etc/skel/local.profile
#
# @(#)local.profile 1.4 93/09/15 SMI
#
stty istrip
PATH=/usr/bin:/usr/ucb:/etc:.
export PATH

#
# If possible, start the windows system
#
if [ `tty` = "/dev/console" ] ; then
    if [ "$TERM" = "sun" -o "$TERM" = "AT386" ] ; then

        if [ ${OPENWINHOME:-""} = "" ] ; then
            OPENWINHOME=/usr/openwin
            export OPENWINHOME
        fi

        echo ""
        echo "Starting OpenWindows in 5 seconds (type Control-C to
interrupt)"

        sleep 5
        echo ""
        ${OPENWINHOME}/bin/openwin

        clear          # get rid of annoying cursor rectangle
        exit           # logout after leaving windows system

    fi

fi

# cat /etc/ssh_config
# This is ssh client systemwide configuration file.  This file provides
# defaults for users, and the values can be changed in per-user configuration
# files or on the command line.

# Configuration data is parsed as follows:
# 1. command line options
# 2. user-specific file

```

.....  
# 3. system-wide file  
# Any configuration value is only changed the first time it is set.  
# Thus, host-specific definitions should be at the beginning of the  
# configuration file, and defaults at the end.

# Site-wide defaults for various options

# Host \*  
# ForwardAgent yes  
# ForwardX11 yes  
# RhostsAuthentication yes  
# RhostsRSAAuthentication yes  
# RSAAuthentication yes  
# TISAuthentication no  
# PasswordAuthentication yes  
# FallBackToRsh yes  
# UseRsh no  
# BatchMode no  
# StrictHostKeyChecking no  
# IdentityFile ~/.ssh/identity  
# Port 22  
# Cipher idea  
# EscapeChar ~

# cat /etc/sshd\_config  
# This is ssh server systemwide configuration file.

Port 22  
ListenAddress 0.0.0.0  
HostKey /etc/ssh\_host\_key  
RandomSeed /etc/ssh\_random\_seed  
ServerKeyBits 768  
LoginGraceTime 600  
KeyRegenerationInterval 3600  
PermitRootLogin no  
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  
# PidFile /u/zappa/.ssh/pid  
# AllowHosts \*.our.com friend.other.com  
# DenyHosts lowsecurity.theirs.com \*.evil.org evil.org  
# Umask 022  
# SilentDeny on  
  
# cat /etc/syslog.conf

```

.....
#ident "@(#)syslog.conf 1.4 96/10/11 SMI" /* SunOS 5.0 */
#
# Copyright (c) 1991-1993, by Sun Microsystems, Inc.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words. Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice /dev/console
*.err;kern.debug;mail.crit /var/adm/messages

# added for wu-ftpd & sshd
daemon.info /var/adm/messages

*.alert;kern.err;daemon.err operator
*.alert root

*.emerg *

# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
auth.notice ifdef(`LOGHOST', /var/log/authlog, @loghost)

mail.debug ifdef(`LOGHOST', /var/log/syslog, @loghost)

#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef(`LOGHOST', ,
user.err /dev/console
user.err /var/adm/messages
user.alert `root, operator'
user.emerg *
)

# cat /ftp01/home/XXXXX31/etc/group
root::0:root
other::1:
bin::2:root,bin,daemon
sys::3:root,bin,sys,adm
adm::4:root,adm,daemon
uucp::5:root,uucp
mail::6:root
tty::7:root,tty,adm
lp::8:root,lp,adm
nuucp::9:root,nuucp
staff::10:
daemon::12:root,daemon
sysadmin::14:
nobody::60001:
noaccess::60002:
nogroup::65534:
ftp::30000:ftp

```

```

.....
Script started on Fri Nov 17 18:17:20 2000
1000 [18:17:20 -!R!- kumo] ssh jpurvis@172.16.2.1
jpurvis@172.16.2.1's password:
Last login: Fri Nov 17 15:43:12 2000 from 172.16.2.47
Sun Microsystems Inc.   SunOS 5.6       Generic August 1997
Sun Microsystems Inc.   SunOS 5.6       Generic August 1997
kumo$ su -
Password:
Sun Microsystems Inc.   SunOS 5.6       Generic August 1997
You have mail.
# showrev -p
No patches are installed
# pkginfo
application FSFgzp           gzip
application NSCPnav         Netscape Navigator (export)
system SUNWab2m             Solaris Documentation Server Lookup
system SUNWaccr             System Accounting, (Root)
system SUNWaccu             System Accounting, (Usr)
system SUNWadmap            System administration applications
system SUNWadmc             System administration core libraries
system SUNWadmfw            System & Network Administration Framework
system SUNWadmr             System & Network Administration Root
system SUNWapppr            PPP/IP Asynchronous PPP daemon configuration files
system SUNWapppu            PPP/IP Asynchronous PPP daemon and PPP login
service
system SUNWarc              Archive Libraries
system SUNWast              Automated Security Enhancement Tools
system SUNWatfsr            AutoFS, (Root)
system SUNWatfsu            AutoFS, (Usr)
system SUNWaudio            Audio applications
system SUNWaudmo            Audio demo programs
system SUNWbcp              SunOS 4.x Binary Compatibility
system SUNWbnur             Networking UUCP Utilities, (Root)
system SUNWbnuu             Networking UUCP Utilities, (Usr)
system SUNWbtool            CCS tools bundled with SunOS
system SUNWcar              Core Architecture, (Root)
system SUNWcg6              GX (cg6) Device Driver
system SUNWcg6h             GX (cg6) Header Files
ALE SUNWciui8              Chinese/PRC iconv modules for UTF-8
system SUNWcpr              Suspend, Resume package
system SUNWcsd              Core Solaris Devices
system SUNWcsr              Core Solaris, (Root)
system SUNWcsu              Core Solaris, (Usr)
system SUNWdfb              Dumb Frame Buffer Device Drivers
system SUNWdfbh             Dumb Frame Buffer Header Files
system SUNWdhcsr            BOOTP/DHCP Server Services, (Root)
system SUNWdhcsu            BOOTP/DHCP Server Services, (Usr)
system SUNWdial             Buttons/Dials (bd) Streams Module
application SUNWdialh       Buttons/Dials (bd) Header Files
system SUNWdoc              Documentation Tools
system SUNWdtab             CDE DTBUILDER
system SUNWdtbas            CDE application basic runtime environment
system SUNWdtcor            Solaris Desktop /usr/dt filesystem anchor
system SUNWdtDEM            CDE DEMOS
system SUNWdtDMN            CDE daemons
system SUNWdtDST            CDE Desktop Applications
system SUNWdtDTE            Solaris Desktop Login Environment

```



system	SUNWdthe	CDE HELP RUNTIME
system	SUNWdthed	CDE HELP DEVELOPER ENVIRONMENT
system	SUNWdthev	CDE HELP VOLUMES
system	SUNWdthj	HotJava Browser for Solaris
system	SUNWdticn	CDE icons
system	SUNWdtim	Solaris CDE Image Viewer
system	SUNWdtinc	CDE Includes
system	SUNWdtlog	System boot for Desktop Login
system	SUNWdtma	CDE man pages
system	SUNWdtmad	CDE developer man pages
system	SUNWdtrme	CDE Release Documentation
system	SUNWdtwm	CDE DESKTOP WINDOW MANAGER
system	SUNWenise	Base Partial Locales
system	SUNWesu	Extended System Utilities
system	SUNWeudba	UTF-8 L10N for CDE Base
system	SUNWeudbd	UTF-8 L10N for CDE Dtbuilder
system	SUNWeudda	UTF-8 L10N For CDE Desktop Applications
system	SUNWeudhr	UTF-8 L10N For CDE Help Runtime
system	SUNWeudhs	UTF-8 L10N For CDE Help Runtime
system	SUNWeudis	UTF-8 L10N For CDE Icons
system	SUNWeudiv	UTF-8 L10N For Desktop Imagetool
system	SUNWeudlg	UTF-8 L10N For CDE Desktop Login
system	SUNWeudmg	UTF-8 L10N For Desktop Window Manager
system	SUNWeuise	European Partial Locales
system	SUNWEuluf	UTF-8 L10N For Language Environment User Files
system	SUNWEuodf	UTF-8 Core OPENLOOK Desktop Files
system	SUNWeuxwe	UTF-8 X Window Environment
system	SUNWfac	Framed Access Command Environment
system	SUNWfns	Federated Naming System
system	SUNWfnsx5	FNS Support For X.500 Directory Context
system	SUNWhea	SunOS Header Files
ALE	SUNWhiu8	Chinese/Taiwan iconv modules for UTF-8
system	SUNWhmd	SunSwift SBus Adapter Drivers
system	SUNWhmdu	SunSwift SBus Adapter Headers
system	SUNWi1of	ISO-8859-1 (Latin-1) Optional Fonts
system	SUNWi2of	X11 ISO-8859-2 optional fonts
system	SUNWi2rf	X11 ISO-8859-2 required fonts
system	SUNWi4of	X11 ISO-8859-4 optional fonts
system	SUNWi4rf	X11 ISO-8859-4 required fonts
system	SUNWi5of	X11 ISO-8859-5 optional fonts
system	SUNWi5rf	X11 ISO-8859-5 required fonts
system	SUNWi7of	X11 ISO-8859-7 optional fonts
system	SUNWi7rf	X11 ISO-8859-7 required fonts
system	SUNWi9of	X11 ISO-8859-9 optional fonts
system	SUNWi9rf	X11 ISO-8859-9 required fonts
system	SUNWinst	Install Software
system	SUNWipc	Interprocess Communications
system	SUNWislcc	XSH4 conversion for Eastern European locales
system	SUNWisolc	XSH4 conversion for ISO Latin character sets
system	SUNWjju8	Japanese iconv modules for UTF-8
system	SUNWjvdm	JavaVM demo programs
system	SUNWjvdev	JavaVM developers packages, includes javac, javah, and javap
system	SUNWjvjit	Java JIT compiler
system	SUNWjvman	JavaVM man pages
system	SUNWjvrt	JavaVM run time environment
application	SUNWkcspf	KCMS Optional Profiles

application	SUNWkcspg	KCMS Programmers Environment
application	SUNWkcsrt	KCMS Runtime Environment
system	SUNWkey	Keyboard configuration tables
ALE	SUNWkiu8	Korean UTF-8 iconv modules for UTF-8
system	SUNWkvm	Core Architecture, (Kvm)
system	SUNWleo	ZX System Software (Device Driver)
application	SUNWleoo	ZX XGL support
system	SUNWleor	ZX System Software (Root)
application	SUNWleow	ZX Window System Support
system	SUNWlibC	SPARCompilers Bundled libC
system	SUNWlibCf	SunSoft WorkShop Bundled libC (cfront version)
system	SUNWlibm	Sun WorkShop Bundled libm
system	SUNWlibms	Sun WorkShop Bundled shared libm
system	SUNWloc	System Localization
system	SUNWlpmsg	LP Alerts
system	SUNWluxal	Sun Enterprise Network Array social Device Driver
system	SUNWluxdv	Sun Enterprise Network Array sf Device Driver
system	SUNWluxop	Sun Enterprise Network Array firmware and
utilities		
system	SUNWman	On-Line Manual Pages
system	SUNWmfdev	Motif UIL Compiler
system	SUNWmfman	CDE Motif Manuals
system	SUNWmfrun	Motif RunTime Kit
system	SUNWmibii	Solstice Enterprise Agent SNMP daemon
system	SUNWnisr	Network Information System, (Root)
system	SUNWnisu	Network Information System, (Usr)
system	SUNWntpr	NTP, (Root)
system	SUNWntpu	NTP, (Usr)
system	SUNWoladd	OPEN LOOK Alternate Desktop Demos
system	SUNWolaud	OPEN LOOK Audio applications
system	SUNWolbk	OpenWindows online handbooks
system	SUNWoldcv	OPEN LOOK document and help viewer applications
system	SUNWoldem	OPEN LOOK demo programs
system	SUNWoldim	OPEN LOOK demo images
system	SUNWoldst	OPEN LOOK deskset tools
system	SUNWoldte	OPEN LOOK Desktop Environment
system	SUNWolimt	OPEN LOOK imagetool
system	SUNWolinc	OPEN LOOK include files
system	SUNWolman	OPEN LOOK toolkit/desktop users man pages
system	SUNWolrte	OPEN LOOK toolkits runtime environment
system	SUNWolslb	OPEN LOOK toolkit/desktop static/lint libraries
system	SUNWolsrc	OPEN LOOK sample source
system	SUNWos86u	Platform Support, OS Functionality (Usr)
system	SUNWosdem	OS demo source
system	SUNWowbcp	OpenWindows binary compatibility
system	SUNWowrqd	OpenWindows required core package
system	SUNWpcelx	3COM EtherLink III PCMCIA Ethernet Driver
system	SUNWpcmcia	PCMCIA Card Services, (Root)
system	SUNWpcmcu	PCMCIA Card Services, (Usr)
system	SUNWpcmem	PCMCIA memory card driver
system	SUNWpcr	SunSoft Print - Client, (root)
system	SUNWpcser	PCMCIA serial card driver
system	SUNWpcu	SunSoft Print - Client, (usr)
application	SUNWpexcl	PEX Runtime Client Library
application	SUNWpexh	PEX Client Developer Files
application	SUNWpexsv	PEX Runtime Server Extension
system	SUNWpldte	Eastern European locale support

system	SUNWploc	Partial Locales
system	SUNWploc1	Supplementary Partial Locales
system	SUNWplow	OpenWindows enabling for Partial Locales
system	SUNWplow1	OpenWindows enabling for Supplementary Partial Locales
system	SUNWpmowm	Power Management OW Utilities Man Pages
system	SUNWpmowr	Power Management OW Utilities, (Root)
system	SUNWpmowu	Power Management OW Utilities, (Usr)
system	SUNWpmr	Power Management config file and rc script
system	SUNWpmu	Power Management binaries
system	SUNWpppk	PPP/IP and IPdialup Device Drivers
system	SUNWpsdpr	PCMCIA ATA card driver
system	SUNWpsf	PostScript filters - (Usr)
system	SUNWpsr	SunSoft Print - LP Server, (root)
system	SUNWpsu	SunSoft Print - LP Server, (usr)
system	SUNWrdm	On-Line Open Issues ReadMe
system	SUNWrtvc	SunVideo Device Driver
application	SUNWrtvc1	SunVideo XIL library support
application	SUNWrtvcu	SunVideo Runtime Support Software
system	SUNWsaacom	Solstice Enterprise Agent files for root file
system	SUNWsadmi	Solstice Enterprise Agent Desktop Management Interface
system	SUNWsadml	Solstice Launcher.
system	SUNWsasnm	Solstice Enterprise Agent Simple Network Management Protocol
system	SUNWscbcp	SPARCCompilers Binary Compatibility Libraries
system	SUNWscplp	SunSoft Print - Source Compatibility, (Usr)
system	SUNWscpr	Source Compatibility, (Root)
system	SUNWscpu	Source Compatibility, (Usr)
system	SUNWses	SCSI Enclosure Services Device Driver
system	SUNWsolnm	Solaris Naming Enabler
system	SUNWspl	Spell Checking Engine - Base Release (English)
system	SUNWsprot	Solaris Bundled tools
system	SUNWsr	Source Compatibility Archive Libraries
system	SUNWsrregu	Solaris User Registration
system	SUNWsrh	Source Compatibility Header Files
system	SUNWssadv	SPARCstorage Array Drivers
system	SUNWssaop	SPARCstorage Array Utility
system	SUNWsutl	Static Utilities
system	SUNWswmt	Patch Utilities
application	SUNWsx	SX Shareable Library
application	SUNWsxow	SX Window System Support
application	SUNWsxogl	SX XGL Support
application	SUNWtcxow	TCX Window System Support
application	SUNWtcxu	TCX XGL Support
system	SUNWter	Terminal Information
system	SUNWtltk	ToolTalk runtime
system	SUNWtltkd	ToolTalk developer support
system	SUNWtltkm	ToolTalk manual pages
system	SUNWtnfc	TNF Core Components
system	SUNWtnfd	TNF Developer Components
system	SUNWtoo	Programming Tools
system	SUNWuiu8	Iconv modules for UTF-8 Locale
system	SUNWuium	Iconv Man Pages for UTF-8 Locale
system	SUNWulcf	UTF-8 Locale Environment Common Files
system	SUNWuxlcf	UTF-8 X Locale Environment Common Files

```

-----
system      SUNWvolg      Volume Management Graphical User Interface
system      SUNWvolr      Volume Management, (Root)
system      SUNWvolu      Volume Management, (Usr)
system      SUNWxcu4      XCU4 Utilities
system      SUNWxcu4t     XCU4 make and sccs utilities
application SUNWxgldg     XGL Generic Loadable Libraries
application SUNWxgler  XGL English Localization
application SUNWxglft  XGL Stroke Fonts
application SUNWxglh   XGL Include Files
application SUNWxglrt  XGL Runtime Environment
system      SUNWxil8n     X Window System I18N Common Package
application SUNWxilcg   CG14 XIL Support
application SUNWxildh   XIL Loadable Pipeline Libraries
application SUNWxilh    XIL API Header Files
application SUNWxilmn   XIL man pages and demos
application SUNWxilow   XIL Deskset Loadable Pipeline Libraries
application SUNWxilr1   XIL Runtime Environment
application SUNWxilvl   VIS/XIL Support
system      SUNWxim       X Window System X Input Method Server Package
system      SUNWxwacx     AccessX client program
system      SUNWxwcft     X Window System common (not required) fonts
system      SUNWxwdem     X Window System demo programs
system      SUNWxwdim     X Window System demo images
system      SUNWxwdv      X Windows System Window Drivers
system      SUNWxwdxnm    DPS motif library
system      SUNWxwfa      X Window System Font Administrator
system      SUNWxwfnt     X Window System platform required fonts
system      SUNWxwfs      Font server
system      SUNWxwhl      X Window System & Graphics Header links in
/usr/include
system      SUNWxwice     ICE components
system      SUNWxwinc     X Window System include files
system      SUNWxwman     X Window System online user man pages
system      SUNWxwmod     OpenWindows kernel modules
system      SUNWxwoft     X Window System optional fonts
system      SUNWxwopt     nonessential MIT core clients and server
extensions
system      SUNWxwplt     X Window System platform software
system      SUNWxwpmn     X Window System online programmers man pages
system      SUNWxwpsr     Sun4u-platform specific X server auxiliary filter
modules
system      SUNWxwrt1     X Window System & Graphics Runtime Library Links
in /usr/lib
system      SUNWxwslb     X Window System static/lint libraries
system      SUNWxwsrc     X Window System sample source
system      SUNWypr       NIS Server for Solaris (root)
system      SUNWypu       NIS Server for Solaris (usr)
utility     md5sum        md5sum 1.00 SPARC Solaris 2.6
# ls -l /var/log/syslog
-rw-r--r--  1 root   other           6054 Nov 17 05:00 /var/log/syslog
# ls -l /var/adm/messages
-rw-r--r--  1 root   other           7809 Nov 17 16:44 /var/adm/messages
# ls -l /var/adm
total 6436
drwxrwxr-x  5 adm     adm             512 Jan 26 1998 acct
-rw-----  1 uucp    bin              0 Jan 26 1998 aculog
drwx-----  2 root    other           512 May  5 2000 backup

```

```

-----
-rw-r--r-- 1 root root 4096 Apr 2 1998 ftp.pids-all
-rw-r--r-- 1 root root 4096 Nov 17 16:31 ftp.pids-remote
drwxr-xr-x 2 root other 512 Dec 1 1999 fw
-r--r--r-- 1 root root 854084 Nov 17 16:44 lastlog
drwxrwxr-x 2 adm adm 512 Jan 26 1998 log
-rw-r--r-- 1 root other 7809 Nov 17 16:44 messages
-rw-r--r-- 1 root other 2638 Nov 7 14:58 messages.0
-rw-r--r-- 1 root other 525 Nov 4 23:50 messages.1
-rw-r--r-- 1 root other 2911 Oct 24 15:25 messages.2
-rw-r--r-- 1 root other 0 Oct 15 03:10 messages.3
-rw-r--r-- 1 root other 0 Oct 8 03:10 messages.4
-rw-r--r-- 1 root other 0 Oct 1 03:10 messages.5
-rw----- 1 root other 1601 Dec 30 1999 nohup.out
drwxrwxr-x 2 adm adm 512 Jan 26 1998 passwd
drwxrwxr-x 2 adm sys 512 Jan 26 1998 sa
-rw-rw-rw- 1 bin bin 0 Jan 26 1998 spellhist
-rw----- 1 root root 17135 Nov 17 16:45 sulog
-rw-r--r-- 1 root bin 432 Nov 17 16:44 utmp
-rw-r--r-- 1 root bin 4464 Nov 17 16:44 utmpx
-rw-rw-rw- 1 root root 3904 Apr 25 2000 vold.log
-rw-rw-r-- 1 adm adm 218016 Nov 17 16:44 wtmp
-rw-rw-r-- 1 adm adm 2252088 Nov 17 16:44 wtmpx
-rw-rw---- 1 root other 694845 Nov 14 15:57 xferlog
# exit
kumo$ exit
Connection to 172.16.2.1 closed.
1001 [18:21:24 -!R!- kumo]#
Script done on Fri Nov 17 18:21:25 2000

```

## End Notes

<sup>i</sup> The "banner" on a service is the initial greeting string put out by the daemon when a client connects to it, either as a greeting message or in response to a client's request for the server's version information. Banners frequently include the name and version number of the software used, and may also include the architecture of the system they are employed upon, the current date and time according to the system, and so forth. Such information is of great use to an intruder, since it provides clues to what attacks will work against a host.

<sup>ii</sup> These switches were not utilized here, as no intrusion detection was in place on the internal network, and using them slows down the scan significantly.

<sup>iii</sup> Only includes stopping the old daemon and starting new, not compiling and testing new version

<sup>iv</sup> Only includes stopping the old daemon and starting new, not compiling and testing new version

<sup>v</sup> Only includes stopping the old daemon and starting new, not compiling and testing new version

<sup>vi</sup> Only includes stopping the old daemon and starting new, not compiling and testing new version

<sup>vii</sup> Time here has been reduced, since any competent tech writer will take less time to document a clean, secure new installation he/she can document as the installation proceeds than learn a currently-configured one and document it after the fact.

# Upcoming Training

Click Here to  
**{Get CERTIFIED!}**



<b>SANS 2019</b>	<b>Orlando, FL</b>	<b>Apr 01, 2019 - Apr 08, 2019</b>	<b>Live Event</b>
<b>SANSFIRE 2019</b>	<b>Washington, DC</b>	<b>Jun 15, 2019 - Jun 22, 2019</b>	<b>Live Event</b>
<b>Community SANS New York SEC506</b>	<b>New York, NY</b>	<b>Jul 15, 2019 - Jul 20, 2019</b>	<b>Community SANS</b>
<b>SANS Network Security 2019</b>	<b>Las Vegas, NV</b>	<b>Sep 09, 2019 - Sep 16, 2019</b>	<b>Live Event</b>