

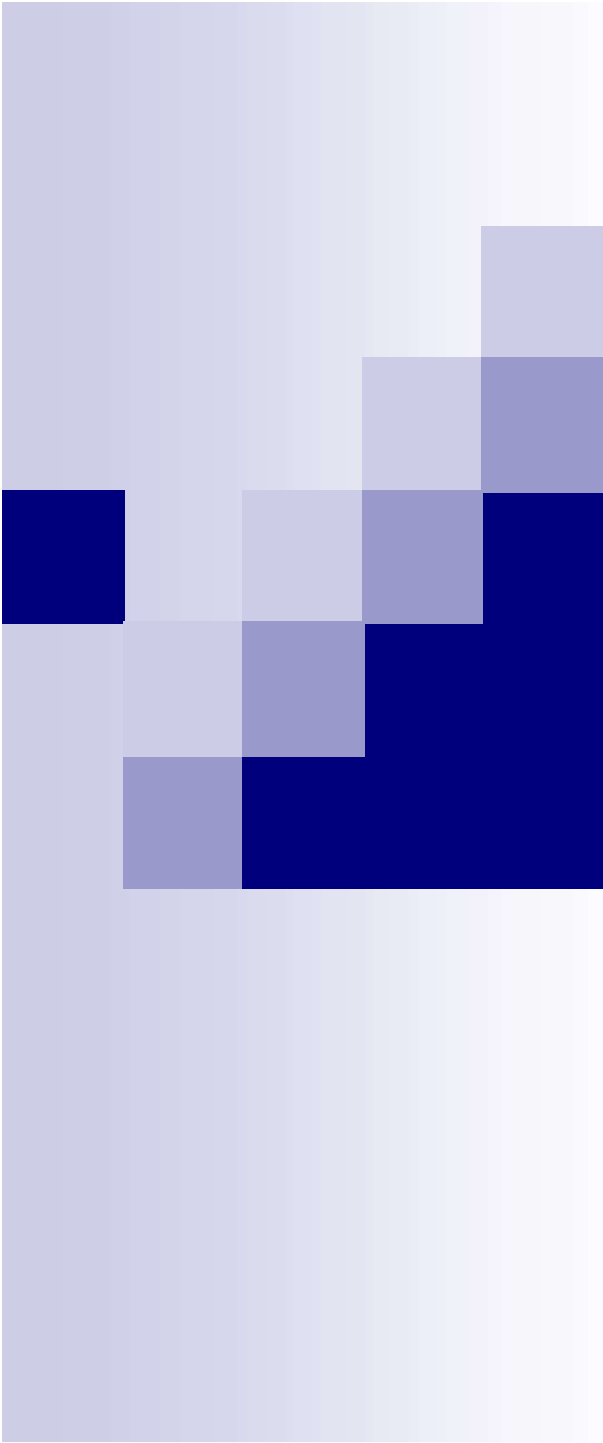


UNIX/Linux Auditing

Baccam Consulting, LLC
tanya@securityaudits.org

Training Events – www.securityaudits.org/events.html

***CISSP Course being offered April 25-April 29, 2016



Copyright © 2005-2016, Baccam Consulting, LLC. All rights reserved. The entire contents of this publication are the property of Baccam Consulting, LLC. User may not copy, reproduce, distribute, display, modify or create derivative works based up on all or any portion of this publication in any medium whether printed, electronic or otherwise, without the express written consent of Baccam Consulting, LLC.



Overall Agenda

- **Background**
 - Users/Groups
 - Permissions
 - Passwords
 - Patching
 - Auditing/Logging
-



UNIX “Philosophies”

- Do one thing and do one thing well
 - Originally built with the developer in mind
 - Everything is treated as a file
-



Logical File System (1)

- /etc
 - The “brains”
 - Contains the administrative files, including the configuration files for different services.
 - Users, passwords, messages, and tab files
 - Similar to the Windows registry
- /bin
 - Contains binary files, or executable files
 - At times the bin directory is also linked to other directories such as /usr/bin
 - Today executables are stored in multiple locations
- /sbin
 - Contains binaries including system binaries, daemons, and administrative programs
- /home
 - Usually the location of user home directories



Logical File System (2)

- /root
 - Often the home directory for root's files
 - Different than the "root directory"
 - /usr
 - Contains the files that are used by multiple users of the system, including some administrative tools
 - Home directories can be placed here too
 - /var
 - Contains variables or rapidly changing data
 - logfiles
 - spools, such as the mailqueue
 - /proc
 - Contains information about processes
-



Logical File System (3)

- /lib
 - Contains the shared libraries
- /dev
 - Contains the device files
 - monitors, disk drives, CD-ROMs, printers, memory
 - Should only be writable by root
- /mnt
 - Reserved for mounting removable file systems
- /boot
 - Contains most of the files involved in constructing or running the bootstrap
- /tmp
 - Contains temporary files



Overall Agenda

- Background
 - **Users/Groups**
 - Permissions
 - Passwords
 - Patching
 - Auditing/Logging
-



User Key Principles

Principle of Least Privilege

Separation of Duties


Rotation of Duties



/etc/passwd

- Lists users on the system
 - Contains 7 fields separated by a “:”
 - Name – the username
 - Password – password field
 - Should have an “x”
 - UserID – user’s identification
 - Watch out for accounts with a UID of “0”
 - Look for duplicate IDs
 - PrincipleGroup – user’s group ID (GID)
 - Gecos – stores the user’s full name
 - HomeDirectory – user’s home directory
 - Shell – user’s default shell
-

Sample /etc/passwd



The image shows a terminal window titled "tanya@linux:~ - Shell - Konsole". The terminal displays the output of the command "cat /etc/passwd". The output lists system and user accounts with their respective UID, GID, name, description, home directory, and shell. The accounts listed are root, bin, daemon, lp, mail, news, uucp, games, man, at, wwwrun, ftp, postfix, sshd, ntp, nobody, and tanya.

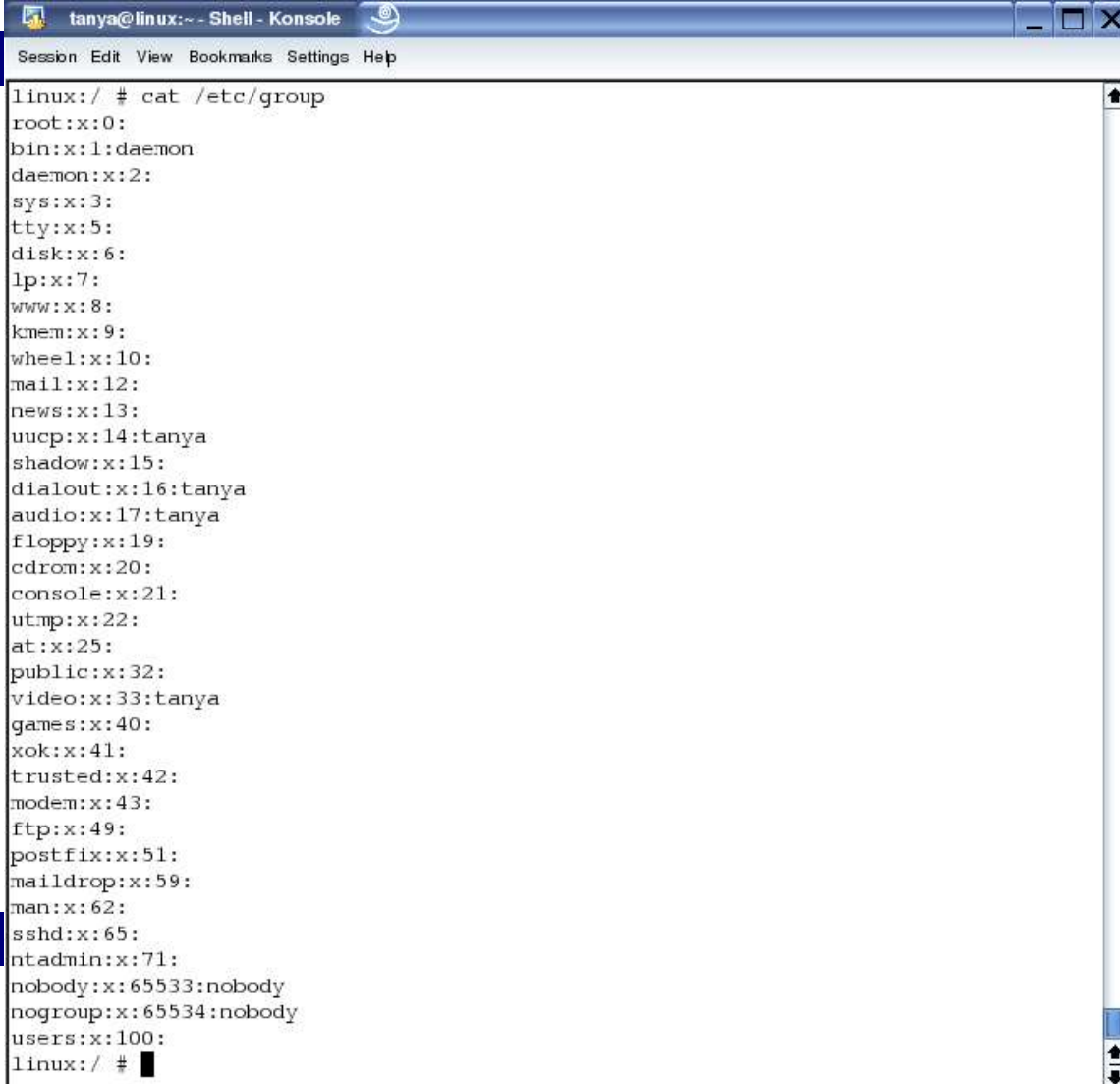
```
linux:/ # cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/bash
daemon:x:2:2:Daemon:/sbin:/bin/bash
lp:x:4:7:Printing daemon:/var/spool/lpd:/bin/bash
mail:x:8:12:Mailer daemon:/var/spool/clientmqueue:/bin/false
news:x:9:13:News system:/etc/news:/bin/bash
uucp:x:10:14:Unix-to-Unix CoPy system:/etc/uucp:/bin/bash
games:x:12:100:Games account:/var/games:/bin/bash
man:x:13:62:Manual pages viewer:/var/cache/man:/bin/bash
at:x:25:25:Batch jobs daemon:/var/spool/atjobs:/bin/bash
wwwrun:x:30:8:WWW daemon apache:/var/lib/wwwrun:/bin/false
ftp:x:40:49:FTP account:/srv/ftp:/bin/bash
postfix:x:51:51:Postfix Daemon:/var/spool/postfix:/bin/false
sshd:x:71:65:SSH daemon:/var/lib/sshd:/bin/false
ntp:x:74:65534:NTP daemon:/var/lib/ntp:/bin/false
nobody:x:65534:65533:nobody:/var/lib/nobody:/bin/bash
tanya:x:500:100:tanya:/home/tanya:/bin/bash
linux:/ # █
```



/etc/group

- Lists groups on the system
- Each line in the file names a group
- The primary group that a user belongs to is listed in the /etc/passwd file
- Contains 4 fields separated by a “:”
 - Group name – gives the group name
 - Encrypted password – gives the group password
 - Group ID – group identification number
 - List of comma-separated users who are in the group
- Commands: groups, id, chage -l

Sample /etc/group

A terminal window titled 'tanya@linux:~ - Shell - Konsole' showing the output of the command 'cat /etc/group'. The output lists system and user groups with their respective IDs and names. The window has a menu bar with 'Session Edit View Bookmarks Settings Help' and a scrollbar on the right side.

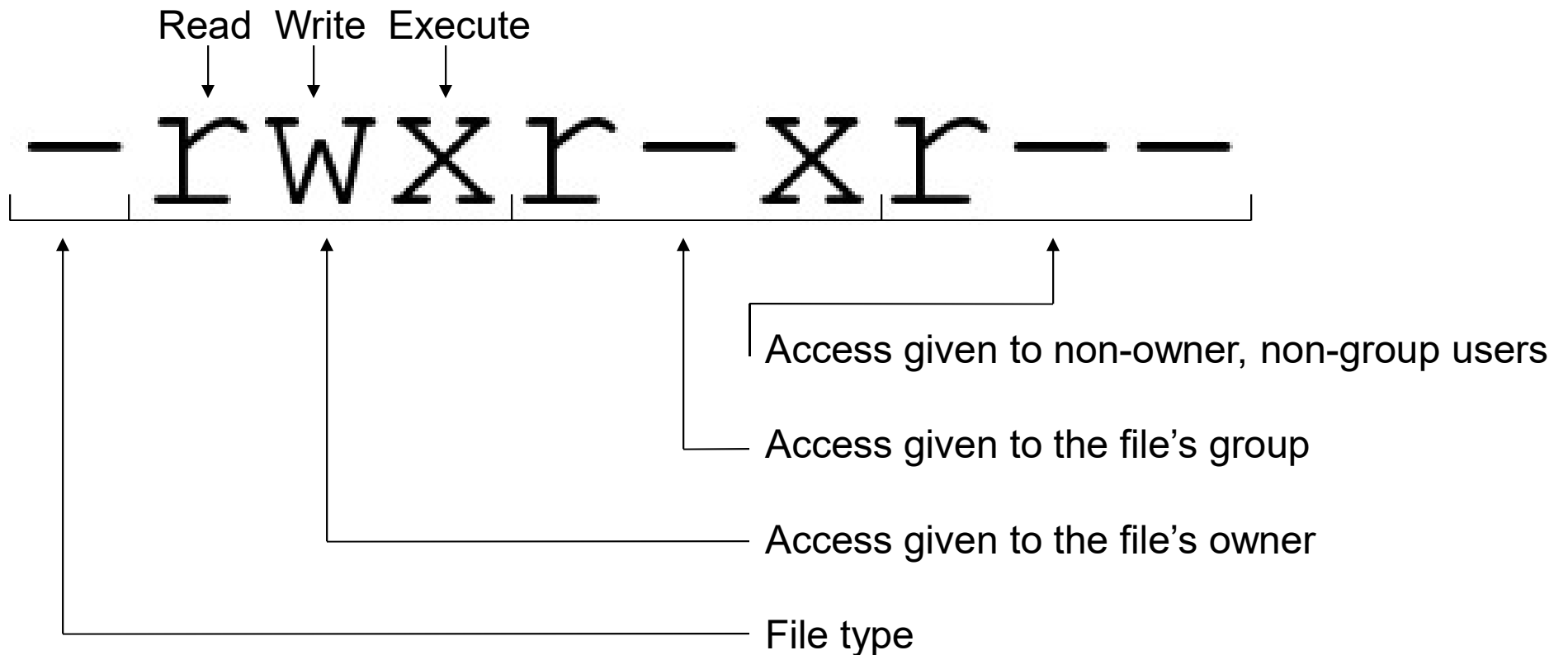
```
linux:/ # cat /etc/group
root:x:0:
bin:x:1:daemon
daemon:x:2:
sys:x:3:
tty:x:5:
disk:x:6:
lp:x:7:
www:x:8:
kmem:x:9:
wheel:x:10:
mail:x:12:
news:x:13:
uucp:x:14:tanya
shadow:x:15:
dialout:x:16:tanya
audio:x:17:tanya
floppy:x:19:
cdrom:x:20:
console:x:21:
uucp:x:22:
at:x:25:
public:x:32:
video:x:33:tanya
games:x:40:
xok:x:41:
trusted:x:42:
modem:x:43:
ftp:x:49:
postfix:x:51:
maildrop:x:59:
man:x:62:
sshd:x:65:
ntadmin:x:71:
nobody:x:65533:nobody
nogroup:x:65534:nobody
users:x:100:
linux:/ #
```



Overall Agenda

- Background
 - Users/Groups
 - **Permissions**
 - Passwords
 - Patching
 - Auditing/Logging
-

Permissions





Directory Permissions

- r = List the contents of the directory
 - List the file names
- w = create, delete, rename files in the directory
- x = can 'cd' into the directory, access contents, not list contents
 - List information from the inode – information about the files
 - Need access to the inode to be able to read/write files in the directory
- Permissions do not grant users the right to run certain *programs*, they grant the right to use certain *system calls*
 - Ex. 'cat'/'more' – written using read() system call, so read permission is necessary

File Resultant Permissions

Directory Permissions

	-	r	x	wX
-	None	None	None	Delete file
r	None	None	Read data	Delete file Read data
w	None	None	Add/Delete data	Delete file Add/Delete data
rw	None	None	Update data	Delete file Update data
x	Can't execute	Can't execute	Execute	Delete file Execute

File Permissions

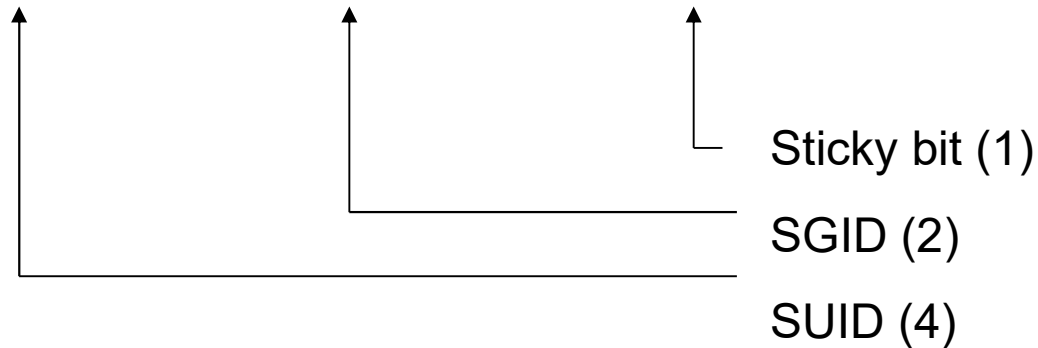


Permissions – Octal Equivalents

- Permissions can also be specified in 3 or 4 digit octal values
 - Read (r) = 4
 - Write (w) = 2
 - Exec (x) = 1
 - Examples
 - -rwxrw-r-- = 764
 - -r-xr----- = 540
-

“Special” Permissions Illustration

`-rwsrwsrwt`



■ Examples

- `drwxrwxrwt = 1777`
- `-rwsr-xr-x = 4755`



Overall Agenda

- Background
 - Users/Groups
 - Permissions
 - **Passwords**
 - Patching
 - Auditing/Logging
-



Passphrase Policy Recommendations

- Maximum Password Age: 60 days
 - Minimum Password Age: 1 day
 - Minimum Password Length: 15 characters
 - Password History Length: 24 prior passwords
 - Password Complexity
 - Lockout Observation Window: 10 minutes
 - Lockout Duration: 5 minutes
 - Lockout Threshold: 5 failed attempts
-



/etc/shadow

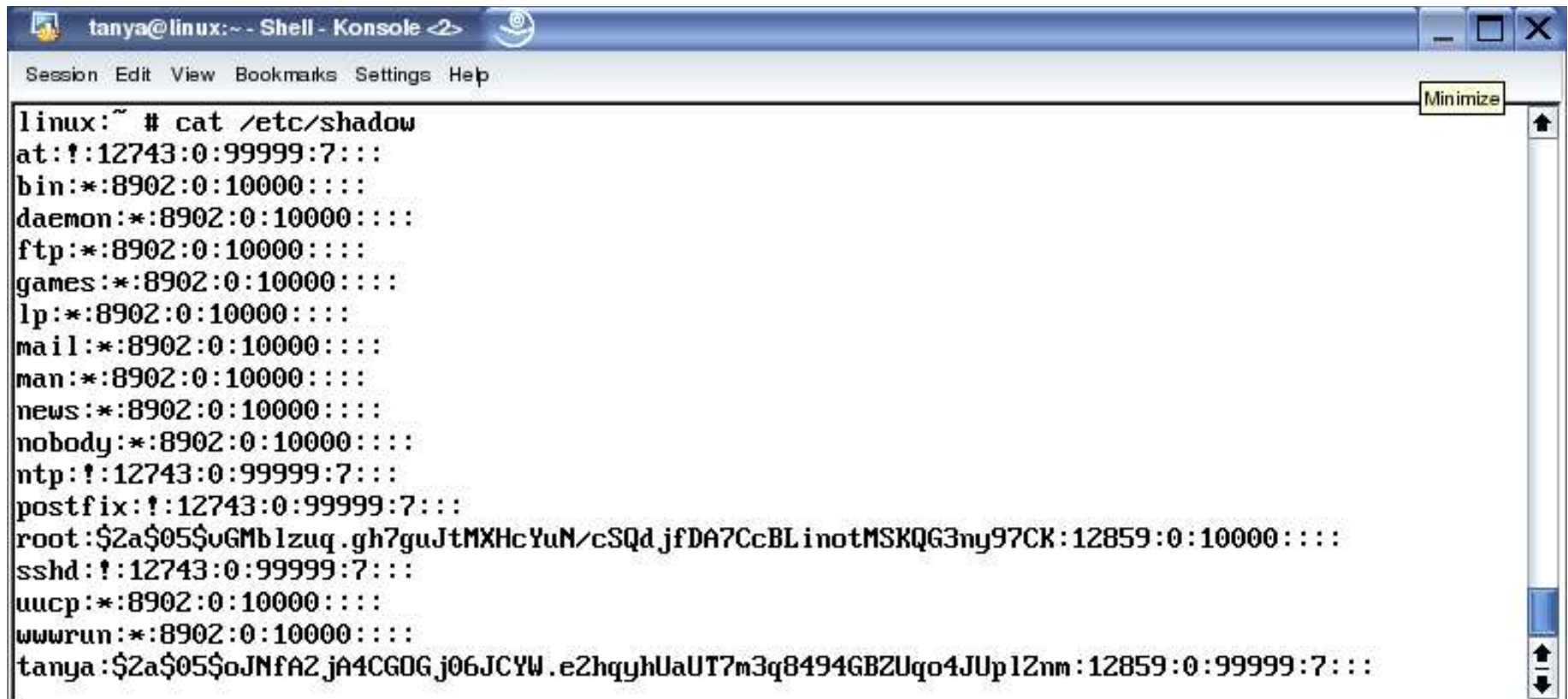
- Stores the encrypted passwords, as well as other information about passwords
 - Don't use /etc/passwd to store encrypted passwords!
- Permissions on the /etc/shadow file should not allow normal users to read the file
 - 640 should apply to the file where the owner is root and the group is shadow, or similar



/etc/shadow Fields

- Contains 9 fields separated by a “:”
 - Username or User ID
 - Password in its encrypted format
 - All accounts should have a password, be locked out or removed
 - Fields starting with “!” or “*” means account is locked out
 - Number of days since Jan 1, 1970 that the password was last changed.
 - “=DATE(1970,1,1)-DATE(2005,6,30)” = 12,964
 - “=DATE(1970,1,1)+12964” = 6/30/2005
 - Minimum number of required days between password changes
 - Maximum number of days that a password is valid for
 - Number of days before expiring that the user starts to receive a warning message
 - Number of inactive days allowed for the user
 - Date after which the account can no longer be used
 - Number of days since January 1, 1970
 - Flag – not currently used

Sample /etc/shadow

A screenshot of a Linux terminal window titled "tanya@linux:~ - Shell - Konsole". The terminal shows the command "cat /etc/shadow" and its output, which is the contents of the /etc/shadow file. The output lists system users and the root user with their password hashes and expiration dates. The root user's password hash is "\$2a\$05\$uGmb1zuq.gh7guJtMXHcYuN/cSQd.jfDA7CcBLi notMSKQG3ny97CK:12859:0:10000::::". The terminal window has a menu bar with "Session Edit View Bookmarks Settings Help" and a "Minimize" button. A vertical scrollbar is visible on the right side of the terminal window.

```
linux:~ # cat /etc/shadow
at:!:12743:0:99999:7:::
bin:!:8902:0:10000::::
daemon:!:8902:0:10000::::
ftp:!:8902:0:10000::::
games:!:8902:0:10000::::
lp:!:8902:0:10000::::
mail:!:8902:0:10000::::
man:!:8902:0:10000::::
news:!:8902:0:10000::::
nobody:!:8902:0:10000::::
ntp:!:12743:0:99999:7:::
postfix:!:12743:0:99999:7:::
root:$2a$05$uGmb1zuq.gh7guJtMXHcYuN/cSQd.jfDA7CcBLi notMSKQG3ny97CK:12859:0:10000::::
sshd:!:12743:0:99999:7:::
uucp:!:8902:0:10000::::
wwwrun:!:8902:0:10000::::
tanya:$2a$05$oJNfAZ.jA4CGOG.j06JCYW.e2hqyhUaUT7m3q8494GBZUqo4JUpl2nm:12859:0:99999:7:::
```



PAM

- Pluggable Authentication Modules
 - Many modules exist
- Library and API that applications can use to authenticate users
- Can be used by many authentication systems
 - /etc/passwd, /etc/shadow, NIS, NIS+, LDAP, Kerberos, etc.
- Important files
 - PAM applications configured in /etc/pam.d or in /etc/pam.conf
 - Library modules normally stored in the directory /lib/security or /usr/lib/security
 - Configuration files are located in the directory /etc/security



Overall Agenda

- Background
 - Users/Groups
 - Permissions
 - Passwords
 - **Patching**
 - Auditing/Logging
-



Centralized Patch Management

- Patches can be “pushed” out after they’ve been tested
 - Multiple groups can exist
- Patches should be prioritized



Patching UNIX

- Easy way for admin to manage source
 - Keep app source code on system and recompile when needed
 - Located at /usr/src or /usr/local/src
- Automated patch management tools do exist
 - autorpm, yast on-line update, apt-get, pkginfo, cron
- RCS, CVS, SCCS
 - Revision control systems
 - CVS allows anonymous client connections so used can “check out” the latest revisions
- You need to know what’s installed in order to keep a system patched!



Auditor Patching Tips

- Who submits changes?
- Who approves changes?
- Is there a patch management system?
- How are changes backed out if necessary?
- How are changes assigned to be completed?
- How is change integrity verified?
- How are changes tested?
- How are changes moved to the production environment?
- What's the emergency process?
 - *** Sample a few changes, as well as recent vulnerabilities.



Overall Agenda

- Background
 - Users/Groups
 - Permissions
 - Passwords
 - Patching
 - **Auditing/Logging**
-



Typical UNIX Logs

- /var/log – typical log directory
 - /var/run/utmp
 - Currently logged in users
 - Ephemeral in nature
 - Binary file
 - Log must be created
 - Contains: Username, terminal, login time, remote host
 - Commands: finger, who, w, users
 - wtmp
 - Login-logout history
 - Binary file
 - Contains: Username, terminal, login time, logout time, remote host
 - Commands: finger, who, last
-



Typical UNIX Logs

- **btmpt**
 - Bad login attempts
 - Binary file
 - Log must be created
 - Commands: lastb
 - **messages**
 - Messages from the syslog facility
 - **secure**
 - Access and authentication
 - **/var/adm/sulog**
 - Logs use of the su command
 - /etc/default/su identifies the location of the log
 - **aculog**
 - Dial-out modem log
-



Typical UNIX Logs

- lastlog
 - Logs each user's most recent login and possibly the last unsuccessful login
 - Command: lastlog
- loginlog
 - Bad login attempts
- /var/account/acct
 - Process-level accounting
 - Command: sa
- Extended audit capabilities are available
 - Can be specific to each Vendor and/or version of UNIX



Syslog.conf

- Syslog provides for log centralization
- Main configuration file for syslog
 - # lines are ignored
 - Each entry has the following
 - Facility
 - auth, authpriv, cron, daemon, kern, lpr, mail, mark, news, syslog, user, uucp, local0 through local7
 - Specifies the subsystem that produced the message
 - Priority
 - debug, info, notice, warning/warn, err/error, crit, alert, emerg/panic (same as emerg)
 - Defines the severity of the message
 - Action
 - Lists the log file location



Example syslog.conf

```
#!/usr/sbin/rsyslogd 2>>/dev/null
#; Critical system failures that management needs to see
*.err;*.crit;*.emerg                                /var/log/critical.log

#; Do not log auth/authpriv messages here; rather log them to
#; a separate file for processing by security staff.
auth,authpriv.none                                  /var/log/messages
auth,authpriv.debug                                  /var/log/auth.log
cron.info                                            /var/log/cron.log
news,kern,lpr,daemon,ftp,mail.info                 /var/log/daemon.log

#; For more critical errors tell root. Ignore user messages.
*.err;user.none                                     root
```



Logrotate

- Logs need to be managed
 - Allows automatic rotation, compression, removal, and mailing of log files
 - Each log file may be handled daily, weekly, monthly, or when it grows too large
 - Normally, logrotate runs as a cron job
-



Auditor Log Tips

- Logs should be reviewed on a daily basis or according to policy
 - Unsuccessful user login attempts
 - Superuser access
 - System modifications
 - Review what is being logged
 - Centralized logging should be occurring
 - Integrity checking tools should be used
-



Thank you!

Tanya Baccam, CPA, CISA, CISM, GPPA, GCIH, CITP, CISSP, Oracle DBA

Baccam Consulting, LLC

tanya@securityaudits.org

Training Opportunities – www.securityaudits.org/events.html

972.294.4193



Courses Coming Up

CISSP Prep

April 25-29, 2016

Auditing Active Directory and Windows

May 16-18, 2016

Auditing Oracle Databases

May 31-June 2, 2016

Auditing Web Applications

July 2016

See www.securityaudits.org/events.html to register
