IT-ADVENTURES

MAKING IT FUN

File Permissions and Network Tools

Module 5

Module 5 Agenda

- Users and Passwords
- Hash Functions
- Managing Users
- File Permissions
- Network tools

Users and Passwords

Users and Passwords

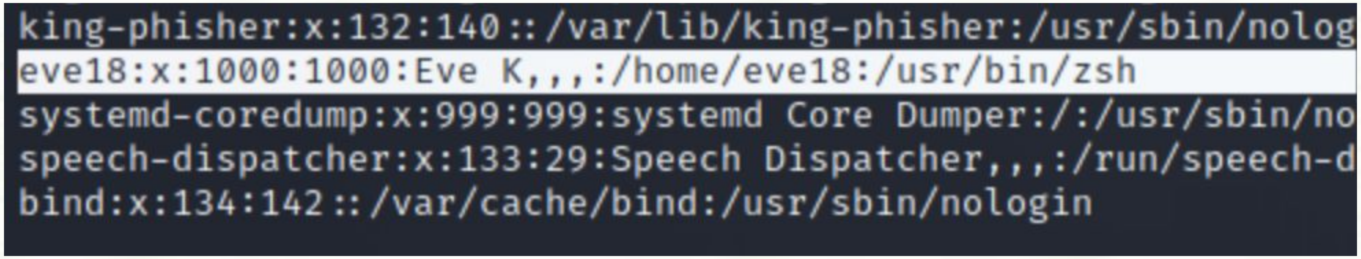
Main Components of User Account:

- username
- group
- UID (User ID)
- GID (Group ID)
- password
- home directory
- shell

Users and Passwords

Example from **/etc/passwd** File:

- Recall that this file contains a list of all users on a machine.
- In the image below, we see user eve18.
- The “x” refers to the location of the password in the **/etc/shadow** file.
- The 1000s refer to the UID/GID respectively.
- The words “Eve K” occupy the comments field.

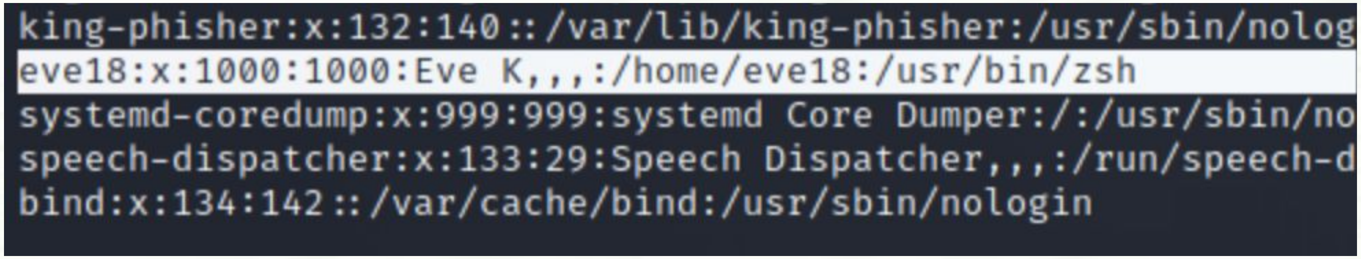


```
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nolog
eve18:x:1000:1000:Eve K,,,:/home/eve18:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/no
speech-dispatcher:x:133:29:Speech Dispatcher,,,:/run/speech-d
bind:x:134:142::/var/cache/bind:/usr/sbin/nologin
```

Users and Passwords

Example from **/etc/passwd** File (cont.):

- The path of the user’s home directory is listed as **/home/eve18** which is where this user “lands” when they log in and open a terminal window
- The **/usr/bin/zsh** path is the location of the shell, which does a lot of background work.



```
king-phisher:x:132:140::/var/lib/king-phisher:/usr/sbin/nolog
eve18:x:1000:1000:Eve K,,,:/home/eve18:/usr/bin/zsh
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/no
speech-dispatcher:x:133:29:Speech Dispatcher,,,:/run/speech-d
bind:x:134:142::/var/cache/bind:/usr/sbin/nologin
```

Users and Passwords

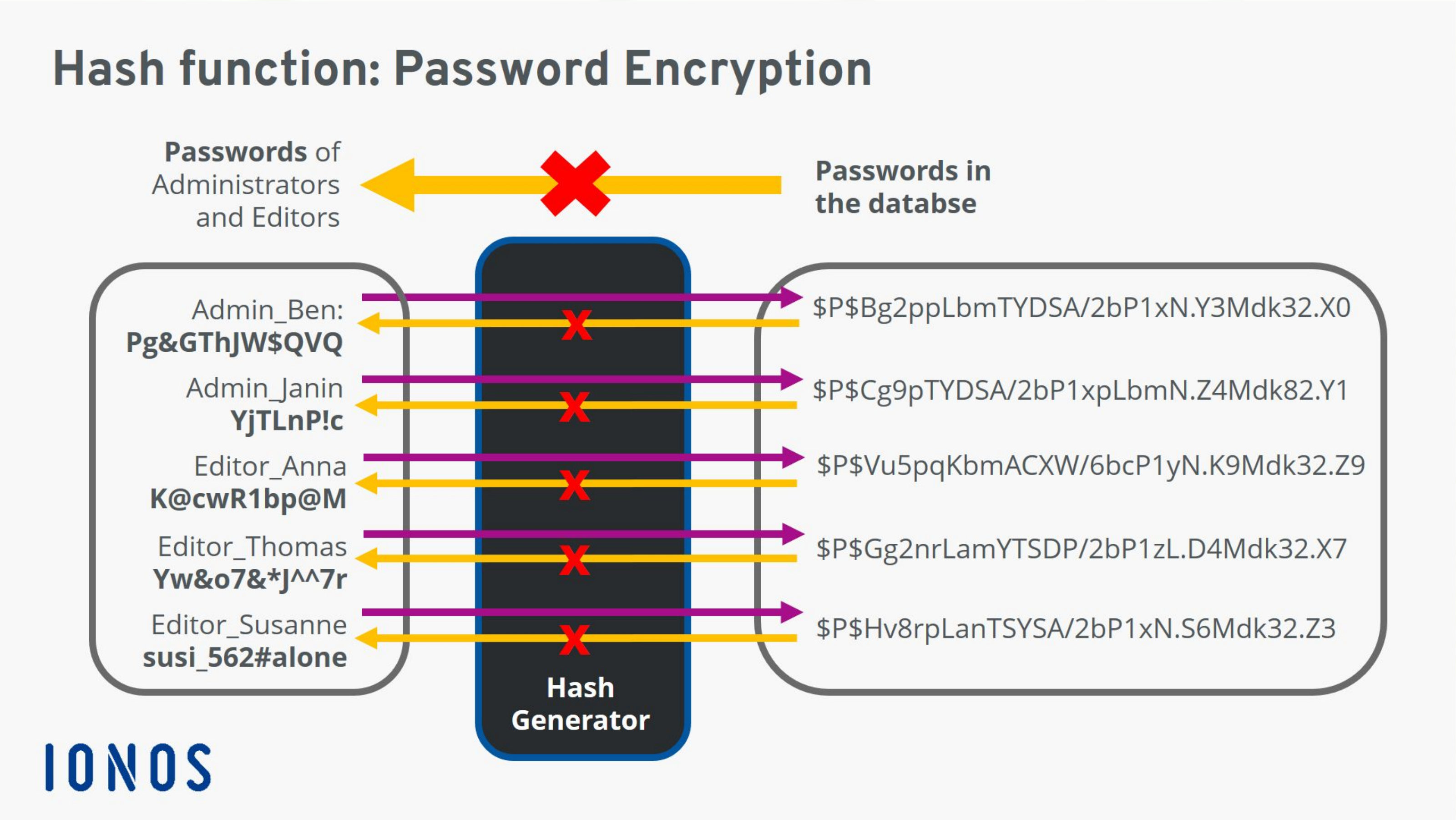
- As you may know, passwords are everywhere now days.
- Passwords are used to login into your computer, phone, email, schools accounts, bank accounts, and websites.
- Passwords are an easy way for sites to prove your identity.
- Retailers normally save users' passwords using hash functions.

Hash Functions

Hash Functions

- Hash Functions:
  - Hash functions are used by retailers to help users' passwords classified.
  - These functions convert passwords into a random output of values called hash values.
- Hash Values:
  - Hash Values are the randomly encrypted code of passwords.
  - No two passwords create the same hash value
  - They are irreversible (can not be translated into the original password).

Hash Functions



Hash function: Password Encryption
Passwords of Administrators and Editors
Passwords in the databse
Admin_Ben:
Pg&GThJW$QVQ
Admin_Janin
YjTLnP!c
Editor_Anna
K@cwR1bp@M
Editor_Thomas
Yw&o7&*J^^7r
Editor_Susanne
susi_562#alone
Hash Generator
PBg2ppLbmTYDSA/2bP1xN.Y3Mdk32.X0
PCg9pTYDSA/2bP1xpLbmN.Z4Mdk82.Y1
PVu5pqKbmACXW/6bcP1yN.K9Mdk32.Z9
PGg2nrLamYTSDP/2bP1zL.D4Mdk32.X7
PHv8rpLanTSYSA/2bP1xN.S6Mdk32.Z3
IONOS

“Hash Function: Password Encryption .” *IONOS Digital Guide*, 14 Oct. 2020, www.ionos.com/digitalguide/server/security/hash-function/.

Hash Functions

- Password Files:
    - Usernames and hash values are stored in password files. (Ex: /etc/shadow)
    - Although hash functions are meant to secure your users passwords, they are not perfect.
    - When entering in a password, the hash functions converts it. Then compares it to the hash values stored for that specific username.
    - Hackers can steal the passwords files and use programs to crack the hash functions.
    - However, there are ways to help insecure your password is more secure.

Hash Functions

- <u>Strong Passwords</u>
  - It is critical to create passwords that humans **and** computers can not crack.
  - Do not share your password with <u>anyone.</u>
  - Store your passwords in a secure spot (not on device).
  - Do not share personal information online or on the phone.
  - Watch out for phishing links.
  - Be careful using public devices or networks.

Hash Functions

- Strong Passwords
  - Create long passwords with a variety of characters and symbols.
  - Do not use common passwords or add common knowledge about yourself in passwords.

Password Creation:

West Valley Bank - Your Friendly N...
www.westvalleybank.com/account_maker/passcode
WEST VALLEY BANK
Welcome New User!
Please create a password for your user account.
Password
Confirm Password
Submit
Where dollars make cents!

https://youtu.be/wHY2WQsmMzM

Managing Users

Managing Users

Important Files to Remember:

- **/etc/passwd**

  Repository of users and user information.

- **/etc/shadow**

  Stores user’s password hashes and other password details.

- **/etc/group**

  Lists every group within the system.

- **/etc/gshadow**

  Stores group password hashes.

Managing Users

Commands:

- Create a new user use **sudo adduser <mikey>**, you will be asked to provide a password and other user info. (mikey is just an example and can be substituted)
- Switch from one user to another use **su - <mikey>** ; use **exit** to go back to your own account.
- To change a user's password, use command **passwd** while existing as that user in the terminal.
- To render a user's password useless simply use **sudo passwd -l <user>**.
    - *This is necessary when an employee leaves a company and all of their accounts need to be disabled.

Managing Users

Commands:

- To delete a user account use **sudo userdel -r user7** ; don’t worry about the error message.
- You have probably noticed that most of these commands require sudo or root privileges to run. This is because creating and deleting user accounts is a significant “power” that not every user should have.

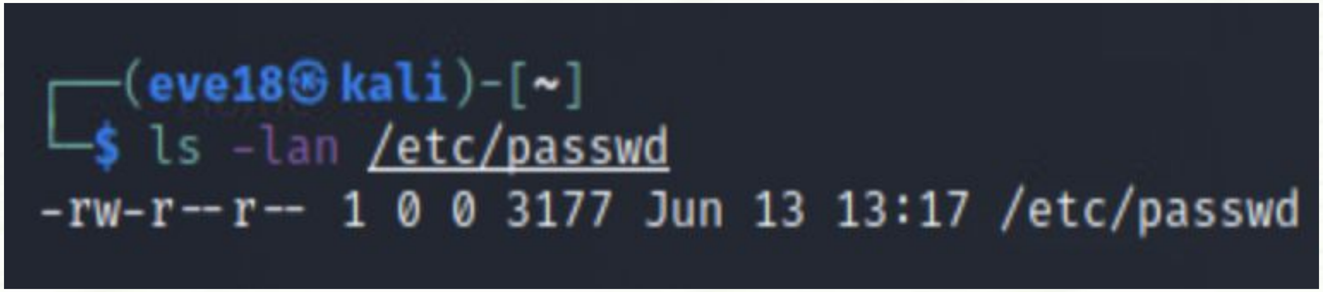
*Make sure to update your commands cheat sheet.

File Permissions

File Permissions

- Every file on your VM has a set of rules that control who is allowed to read, edit or run the file.
- The way we can view these permissions is with the command **ls -lan <filepath>**, where “ls” simply means list all contents and “-lan” are a set of flags that format the output.
- This is the output of the famous /etc/passwd file:

  Let’s analyze it on the next slide...

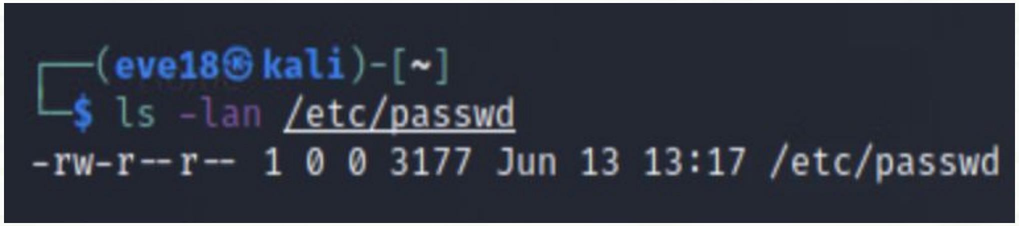


```
┌──(eve18㉿kali)-[~]
└─$ ls -lan /etc/passwd
-rw-r--r-- 1 0 0 3177 Jun 13 13:17 /etc/passwd
```

File Permissions

Based on the /etc/passwd file permissions:

- The very first character "-" shows that this is indeed a file. A "d" or "l" in its place would signify a directory or a symbolic link respectively.
- The next nine characters are split into three parts. Where the first third [rw-] are the user permissions, the middle three are group permissions [r--] and the final third are world permissions.
- The lone number "1" isn't exactly important, but it is there to represent the number of hard links.
- Next are the UID and GID. Both "0" in this instance.



```
┌──(eve18㉿kali)-[~]
└─$ ls -lan /etc/passwd
-rw-r--r-- 1 0 0 3177 Jun 13 13:17 /etc/passwd
```

File Permissions

Based on the /etc/passwd file permissions:

- The number “3177” represents the file size in bytes.
- The last date of modification is “Jun 13” at 13:17.
- And finally the object name is at the very end which in this case ends up being the file path itself.

Let’s go back to the user, group, world permissions.

- We can see that the user can only read and write the file but not execute it. The group and the world can only read the file but cannot edit or run it.
- Write privileges are denoted by a “w” and execute privileges are denoted by an “x”. Read privileges are denoted by “r”.

File Permissions

Changing Permissions:

- Many times we require additional functionality to carry out our job. When this is the case we need to modify existing file permissions.
- Before we show you how to modify permissions, y'all need to know the "weight" every permission has.

Read[r]: 4	Write[w]: 2	Execute[x]: 1

- Notice that these are powers of 2.
- If we set file2's permissions to "757" using **chmod 757 file2**, we are essentially granting the user and the world, full rwx privileges, while the group only r-x privileges.

File Permissions

Still fuzzy on where the numbers come from?

- Seven comes from 4+2+1 or rwx, each of those read, write, execute permissions has a “weight”.

- **chmod** comes from “change mode”.
- Use either **ls -l <file>** or **ls -lan <file>** to view a file’s current permissions.

Don’t worry you will try out a lot of permission-setting commands in the activity!

Network Tools

Network Tools

- ***ping***
  - Sends ICMP echo-request packets to network hosts (servers, routers, etc)
  - Helps us “poke” a certain point in our network to see if it is active/running
  - ctrl + c to stop sending packets
- ***dig***
  - Maps domain names to IP addresses and vice versa
  - DNS lookup utility, parse output with flags

Network Tools

- ***whois***
  - Returns information about a domain such as current owner, admin and other contact info
- ***traceroute***
  - Used to trace the network packet paths, from its source to its destination
- ***netstat***
  - Helps us know what ports and services are open on a machine which is especially useful when trying to attack the machine

Network Tools

- *Wireshark*
  - An application used to monitor network traffic. Not a command.
- ***tcpdump***
  - Alternative to Wireshark but not as powerful.

To Do

- ❑ Complete Activity One
- ❑ Complete Activity Two
- ❑ Complete Module 5 Check your Knowledge! Worksheet

End of Module 5!

What questions do you have?

Next Module Topic:

DNS and Firewall!

Questions?

Contact IT-Adventures support staff!

email:

ita@iastate.edu

Your school's IP-Range can be found at:

http://www.it-adventures.org/ip-ranges/