THE GenCyber® EXPERIENCE

BASIC CHALLENGE #2

CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

FLORIDA
CYBER RANGE

CREDITS

FUNDED BY A GRANT FROM

Acknowledgment

This lesson was funded by a GenCyber Grant administered by the National Security Agency and the National Science Foundation and awarded to the Center for Cybersecurity at the University of West Florida, Pensacola, FL, USA.

Authors

Emily Miller, B.S. Cybersecurity candidate (2025), UWF Hal Marcus College of Science and Engineering
Guy Garrett, M.S., M.B.A., Associate Director, Technology & Training, Center for Cybersecurity, GenCyber PI

Questions/Comments

Email ggarrett@uwf.edu

OBJECTIVES

1. Demonstrate the ability to apply critical thinking.
2. Explain Boolean conditional statements.
3. Given a scenario, perform a system’s validation test on a website.
4. Identify cybersecurity flaws in system design and execution.

NICE Cybersecurity Workforce Framework Connections (NIST SP 800-181 rev. 1)

T0511 Perform developmental testing on systems under development
K0004 Knowledge of cybersecurity and privacy principles
K0091 Knowledge of systems testing and evaluation methods
K0250 Knowledge of test and evaluation processes for learners
S0015 Skill in conducting test events
A0026 Ability to analyze test data

RESOURCES

1. Computer with Internet access
2. Google Chrome browser (recommended)
3. Email account.
4. Hack This Site account.

*Note: If you want to use this lesson in your school, please engage your system's IT team. Most schools block access to websites like this and require special permissions to allow access in a classroom.

Source: hackthissite.org

THE GenCyber EXPERIENCE

THE 6 GENCYBER CONCEPTS

Confidentiality

The property that information is not disclosed to individuals, devices, or processes unless they have been authorized to access the information.

Integrity

The property that an information system, or a component of a system has not been modified or destroyed in an unauthorized manner.

Availability

The property that information or information systems should be accessible and usable upon demand.

Defense in Depth

A comprehensive strategy including multiple layers of security within a system so that if one layer fails, another layer of security is in place to prevent the unauthorized access/disclosure.

Think Like the Adversary

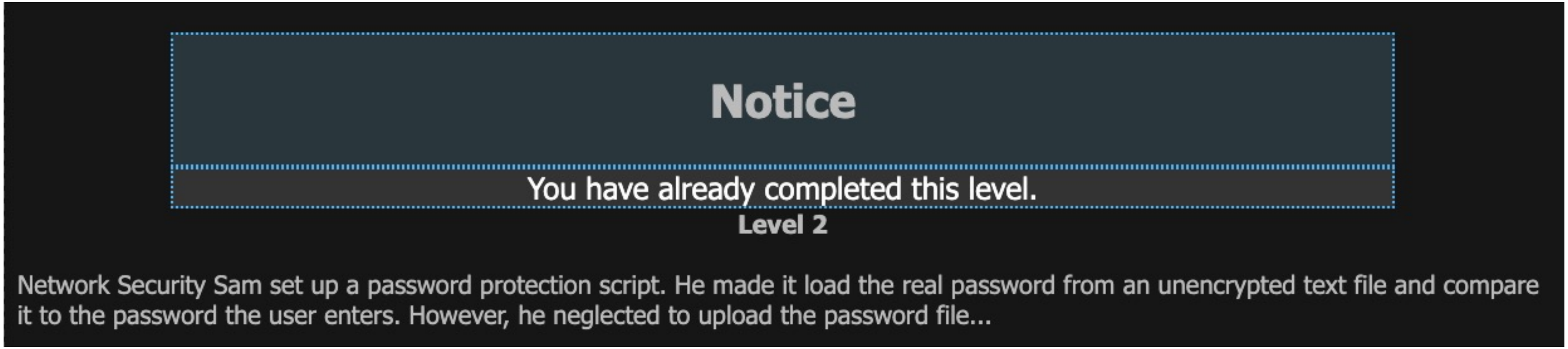
The strategy of putting yourself inside the mind of a potential attacker that allows you to anticipate attack strategies and defend your systems accordingly.

A → B

Keep It Simple

The strategy of designing information and security systems to be configured and operated as simply as possible.

BASIC CHALLENGE #2



Notice

You have already completed this level.

Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

Source: hackthissite.org

What is the challenge?

How do you frame the problem?

THE GenCyber EXPERIENCE

BASIC CHALLENGE #2 - BREAKDOWN

What did Sam do?

Confidentiality

1. **Set up password protection?**
2. Used a script?
3. Compares the user's input to the actual password.
4. Actual password is in an unencrypted text file.

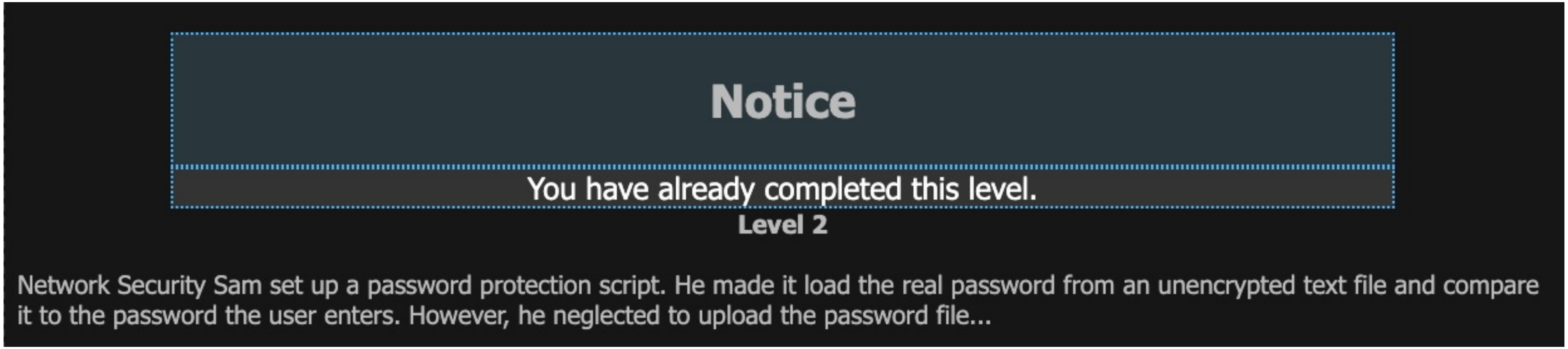
~~Defense in Depth~~

What did Sam forget to do?

1. Upload the password file.

Is there any other potential problem(s) with Sam's plan?

BASIC CHALLENGE #2 - BREAKDOWN



Notice

You have already completed this level.

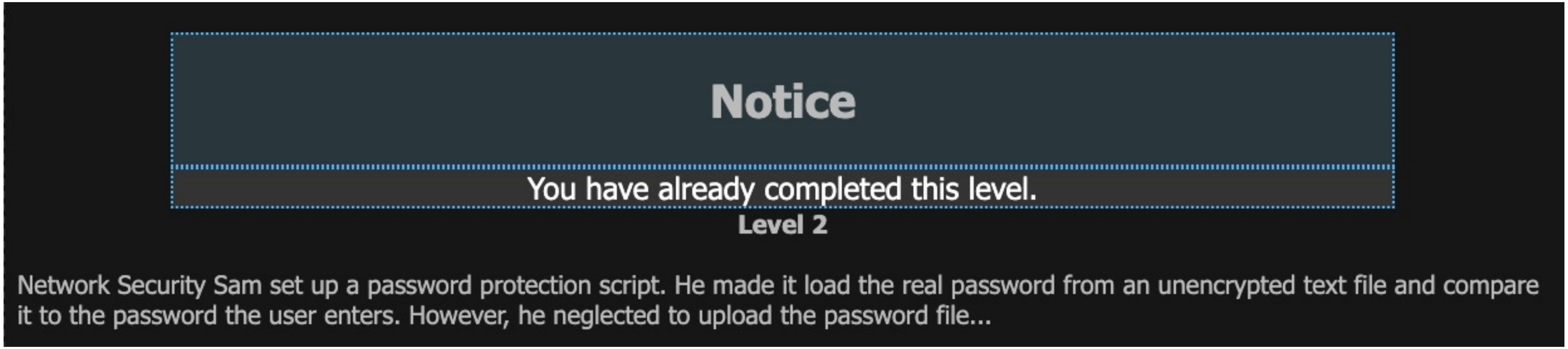
Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

Source: hackthissite.org

What happens when someone enters a password, activates the script and there is no password file for the script to use?

BASIC CHALLENGE #2 - BREAKDOWN



Notice

You have already completed this level.

Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

Source: hackthissite.org

What is the challenge?

Find the password when there is no password file

HOW DOES PASSWORD VALIDATION WORK?

Compare & Contrast

- Look for similarities and differences
- English essay example – Write a 500-word essay and compare and contrast books versus computers.

Logic

- True or False
- If the user input matches what the system expects, then you have a “true” condition.
- If the user input does not match what the system expects, then you have a “false” condition.

THE GenCyber EXPERIENCE

EXAMPLE MATCHING & LOGIC

- Uniforms identify teammates and opponents.
- Players compare/contrast uniform colors, patterns, etc… to determine friend vs. foe.
- In this case the yellow team has the ball.
- If yellow (true), then pass.
- If green (false) then keep

Source: Welcome to all and thank you for your visit!/Pixabay

THE GenCyber EXPERIENCE

YOUR TURN

Can you think of some other examples where people make decisions using logic?

Source: Benjamin Balazs/Pixabay

USING LOGIC IN PASSWORD VALIDATION

Logic Statements - If, then

- A true condition will permit access to the system.
- A false condition will deny access to the system.
- **If** the user input equals (true) the expected input, **then** permit.
- **If** the user input does not equal (false) the expected input, **then** deny.

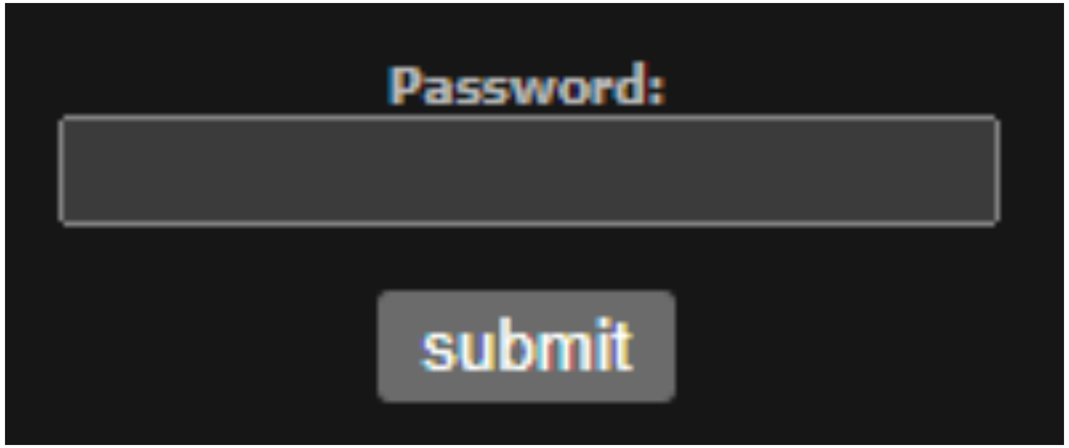
CRACKING THE CODE

```
from getpass import getpass

password = getpass(“Please enter your username: “)

if password == “1234”:
     print(“Welcome!”

else:
     print(“Login failed!”
```



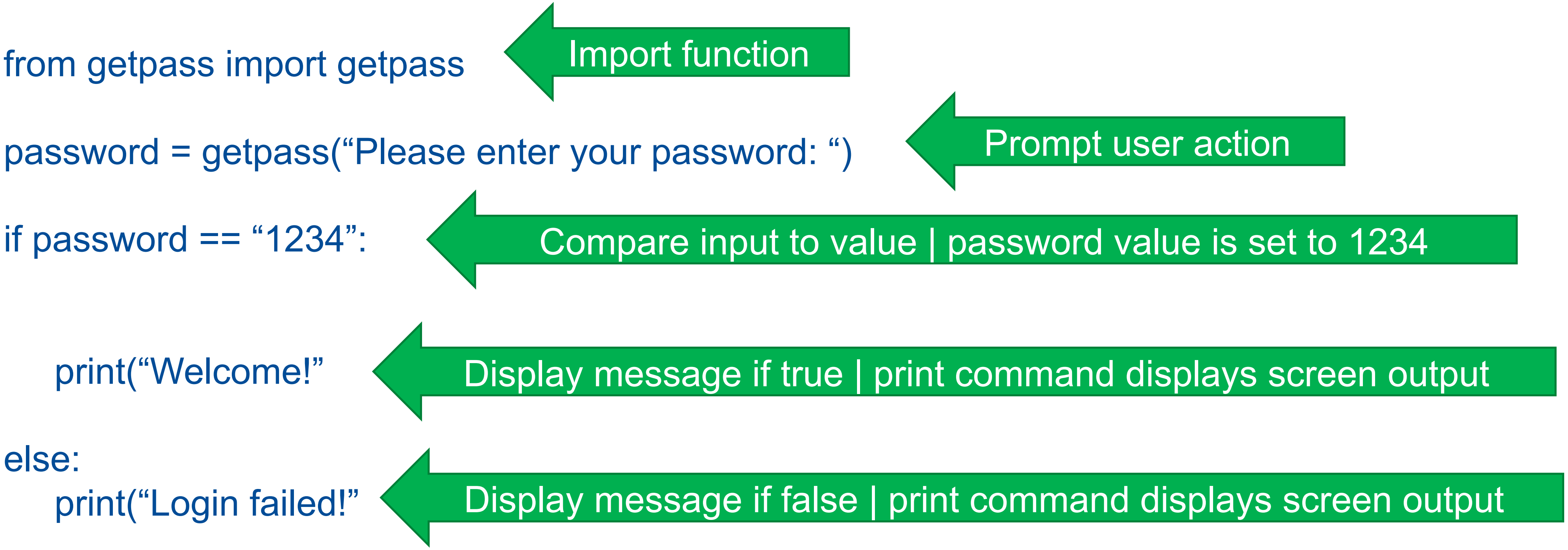
Source: hackthissite.org

function (python)

getpass.getpass(prompt=‘Password:’,stream=None)

THE GenCyber EXPERIENCE

CRACKING THE CODE



```
from getpass import getpass

password = getpass(“Please enter your password: “)

if password == “1234”:

    print(“Welcome!”

else:
    print(“Login failed!”
```

Import function

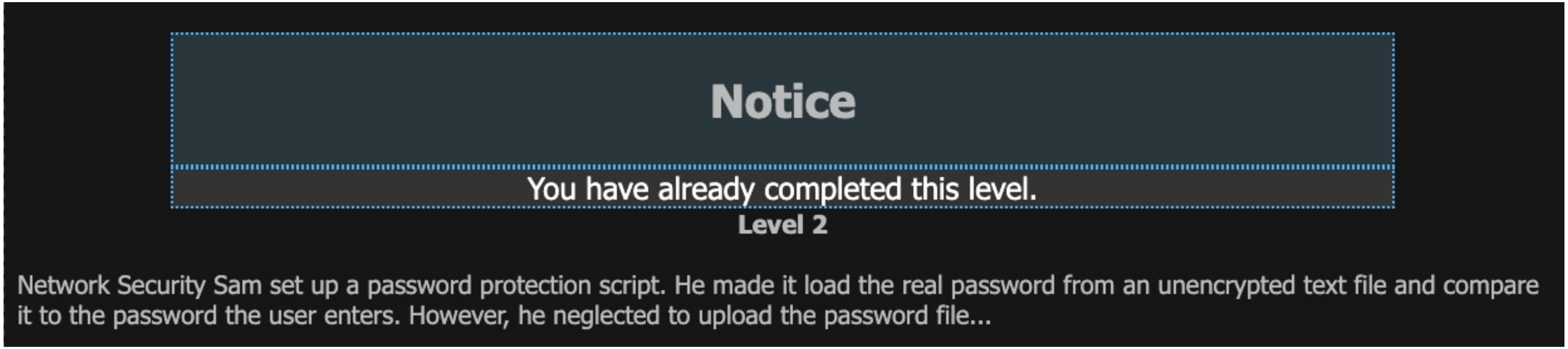
Prompt user action

Compare input to value | password value is set to 1234

Display message if true | print command displays screen output

Display message if false | print command displays screen output

WHEN LOGIC FAILS



Notice

You have already completed this level.

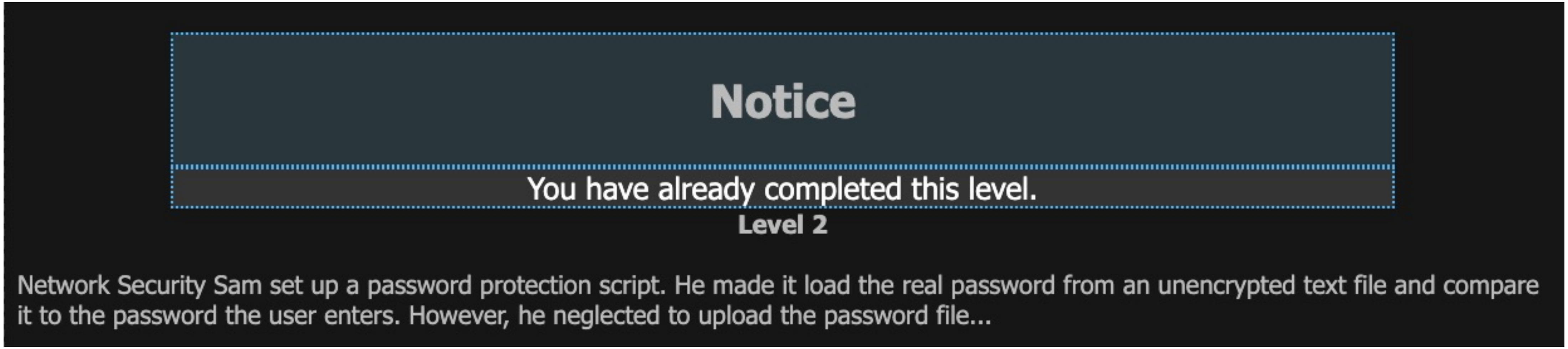
Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

Source: hackthissite.org

What happens when there is no password?

GIVE IT A TRY



Notice

You have already completed this level.

Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

Source: hackthissite.org

Return to Hack This Site and see if you know the answer.

NO SPOILERS!!!

THE GenCyber EXPERIENCE

HOT WASH

Hot Wash

Military term for a de-briefing (discussion) that immediately follows an exercise.

Purpose

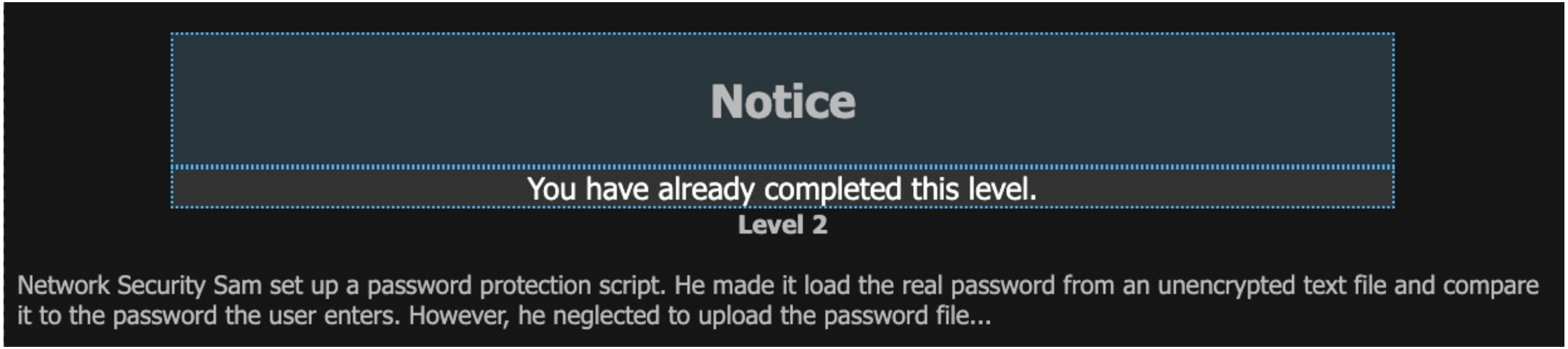
1. Evaluate performance.

2. Discuss strengths/weaknesses.

3. Identify lessons learned.

Source: Reto Gerber/Pixabay

HOT WASH



Notice

You have already completed this level.

Level 2

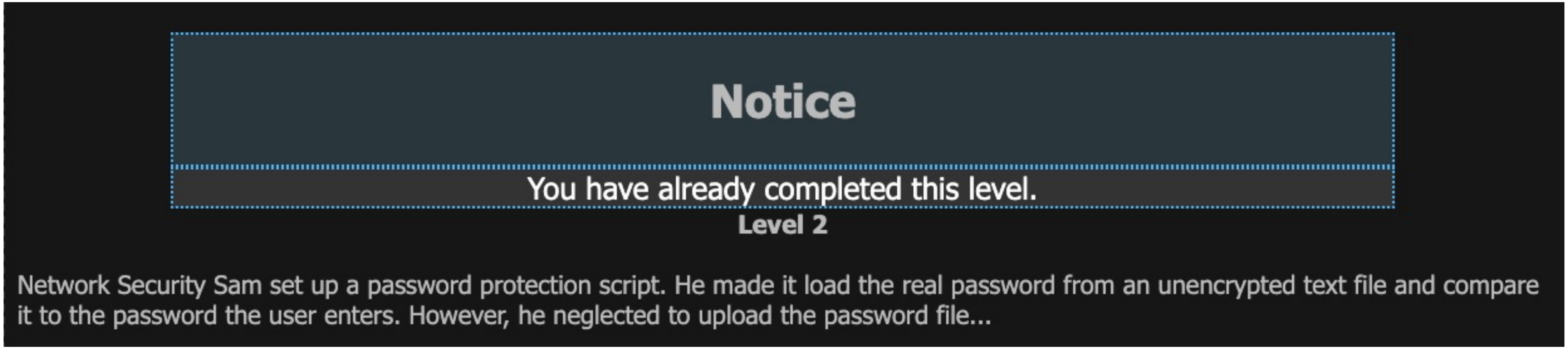
Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

Source: hackthissite.org

Was this a technical problem?

THE GenCyber EXPERIENCE

HOT WASH



Notice

You have already completed this level.

Level 2

Network Security Sam set up a password protection script. He made it load the real password from an unencrypted text file and compare it to the password the user enters. However, he neglected to upload the password file...

Source: hackthissite.org

Key Ideas

- "Enter the password" (action)
- Cyber is not always technical.

Question

What happens if there is no password?

STEP #1 THINK

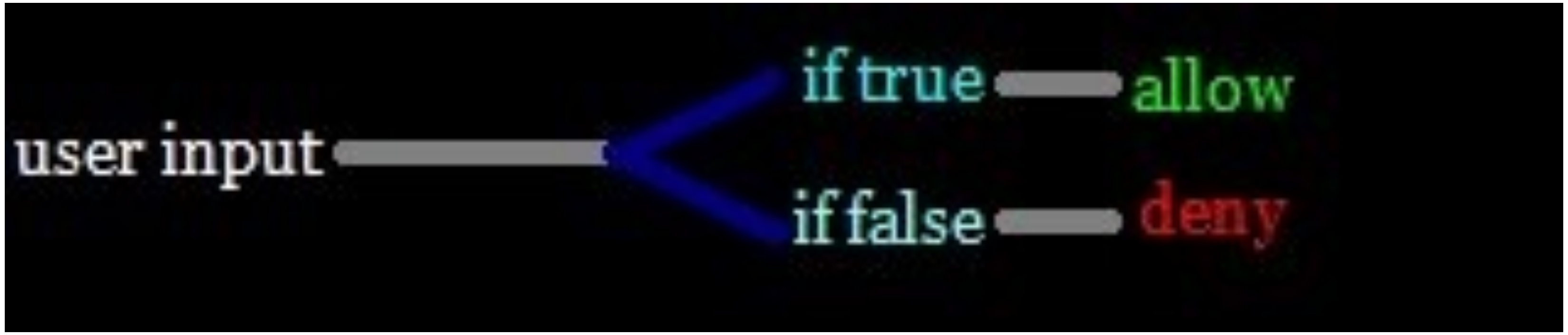
- Critical thinking is very important to cybersecurity professionals

- Not every answer will be technical, sometimes all you need is to stop and think about what was provided to you

- In the prompt it says “He made it load the real password from an unencrypted text file and compare it to the password the user enters. **<u>However, he neglected to upload the password file</u>**…”

    - The last sentence is the most important!

STEP #2 APPLYING WHAT IS IMPORTANT

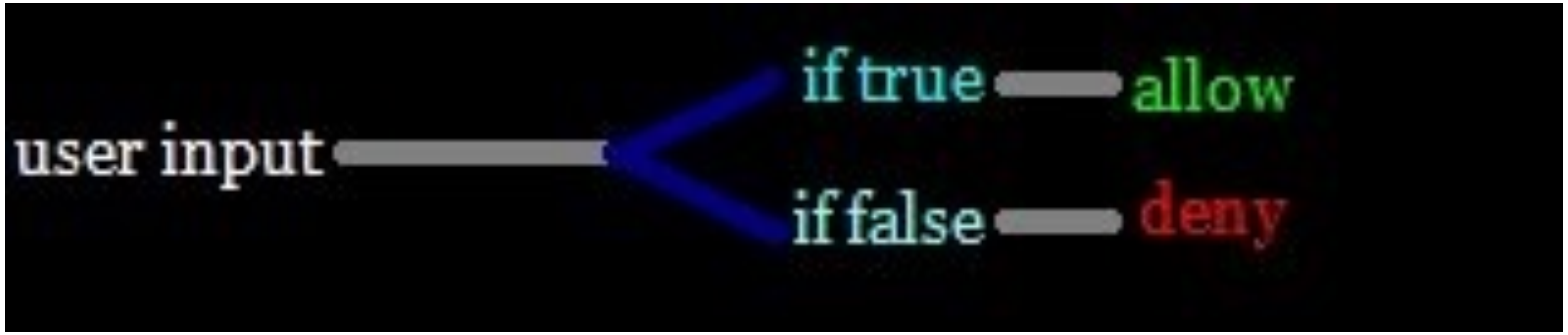


Source: hackthissite.org

- Sam did not upload a password file, what does this mean for the password?

- What happens if there is no password file for your password guess to be checked against?

STEP #2 APPLYING WHAT IS IMPORTANT



Source: hackthissite.org

A password script is meant to check for the correct password, if there is no password, what happens?

THE GenCyber EXPERIENCE

APPLY THE GENCYBER CONCEPTS

Concept	Application	Concept	Application
Confidentiality	Passwords are used to prevent unauthorized access.	Defense in Depth	Storing passwords in an unencrypted file could defeat this layer of defense.
Integrity	The missing file sets the password value to password==[enter key]. This is an improper modification.	Think Like the Adversary	You used context clues to guess the password. Knowing how passwords work helped you.
✓ Availability	The missing password file could prevent authorized users from gaining access.	A → B Keep It Simple	Many coding languages have functions which you can implement in your project.

THE GenCyber® EXPERIENCE

NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NSF

THANK YOU FOR JOINING US!

CENTER FOR CYBERSECURITY
AT THE UNIVERSITY OF WEST FLORIDA

FLORIDA
CYBER RANGE