Auditing and Remediation

Module 12

Module 12 Agenda

➢ Auditing

➢ Remediation

➢ Cyber Security Careers

Auditing

Auditing

- By definition, an audit is an inspection of an organization's systems or its individual's accounts.

- There are many different types of audits that can be performed. For example….

  - Internal audits
  - External audits
  - IRS tax audits
  - Financial audits
  - Operational audits
  - Pay audits

  - Compliance audits
  - Information Technology (IT) / cyber security audits
  - Payroll audits

Auditing

- As you may have guessed, we are going to focus on Information Technology/cyber security audits.
    - **Information Technology (IT) and cyber security audits** are performed in order to detect issues within computer systems and its software.
    - Audits help search computers for vulnerabilities that need to be patched.

*IT and cyber security audits differ from pen-tests because they are used to check what security controls are in place and if those said controls are working properly. Whereas pen-tests evaluate the entire risk level of the system.

Auditing

What is it:

- **IT/cyber security auditing** is the examination of a computer system to make sure everything is clean and up to date.
  - It is essentially a checklist to help systems evaluate if they have the proper security measures in place.

Auditing

Why:

- With the internet rapidly expanding, cyber threats/attacks are becoming increasingly prevalent
    - Auditing helps find holes within cyber security infrastructure
    - Auditing can help monitor network security
    - Audits help the user maintain updated software to protect itself

Auditing

How it works:

- IT/cyber security audits are most often conducted by third-parties.

- The computer system's encrypted data is sent to a auditing company to be evaluated.
  - It is compared to regulations and is given either a pass or fail report after completion

- The auditing company follows a security model to make sure data will not be exposed during the process.

8

Remediation

Remediation

Remediation is the process of taking some kind of action to prevent any further damage to an attacked system or to start the clean-up process after the damage has already been dealt.

What is it:

- For cyber security in particular, **remediation** is the process of stopping and treating a data breach.

- Detects and contains a breach before it grows and damages the entire system

Remediation

Why:

- Security breaches are a major threat for companies and business.
    - They can expose sensitive data concerning the company and its customers
- Failing to detect breaches can put companies at greater risk

How it works:

- Detects and evaluates the cause of the breach
- Determine how to stop the harmful activity and how to patch the damage

Remediation

Breaches:

On your own time throughout the week, find time to read this article about how breaches happen, how to detect them, and how to fix them. *This will be very helpful for the CDC*

How To Detect Data Breaches:

Article

Jobs in Cyber Security

Jobs in Cyber Security

Being a junior security auditor is actually a career that cyber security students can pursue. Watch the video below that explains the job! :)

https://youtu.be/iW7W_6stSh0

Jobs in Cyber Security

- Cyber security jobs are in high demand and offer competitive salaries
    - According to cybercademy.org
        - "3.5 million cyber security jobs are expected to open by this year"
        - "$83,000 is the national average salary for entry-level cyber security analysts"

- Cyber security offers a variety of careers

Jobs in Cyber Security

Cyber security students have a lot of options for careers. Including those listed below…

- Penetration Tester
- Incident Responder
- Cyber security Analyst
- Security Specialist
- Vulnerability Assessor

We will be discovering what cyber security career is right for you in Activity 2

Jobs in Cyber Security

Poster [Link](#)

Jobs in Cyber Security

As mentioned in the previous video, basic cyber security skills include…

- Knowledge of operating systems like Windows, Unix, and Linux
- Programming skills in C, C++, Java, PHP, and Python (you can learn more about programming by completing the Smart-IT venue of IT-Adventures)
- Elementary concepts (firewalls, access controls, malware, etc.)

Jobs in Cyber Security

Cyber security skills can be developed through…

- Online programs/certifications
- College degrees in:
  - Software Engineering
  - Computer Science
  - Computer Information Systems
  - Business Information Systems
  - Information Assurance

To Do

- ❏ Complete Module 12 Activity 1
- ❏ Complete Module 12 Activity 2
- ❏ Read the following article: link

End of Module 12!

What questions do you have?

Final Module Topic:

Physical Security & Social Engineering

Questions?

Contact IT-Adventures support staff!

email:
ita@iastate.edu