PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)

Attack and Defense: A Warmup

Cisco | Networking Academy®
Mind Wide Open™

Objectives

Part 1: Attack

Task 1: Do a detailed search on high profile cyberattacks in the recent 5 years.

Task 2: Based on your search, write an analysis of a cyberattack.

Part 2: Defense

Part 1: Background / Scenario

Governments, businesses, and individual users are increasingly the targets of cyberattacks and experts predict that these attacks are likely to increase in the future. Cybersecurity education is a top international priority as high-profile cyber-security related incidents raise the fear that attacks could threaten the global economy. The Center for Strategic and International Studies estimates that the cost of cybercrime to the global economy is more than $600 billion annually. In this lab, you will study four high profile cyberattacks and be prepared to discuss the who, what, why and how of each attack.

Required Resources

- PC or mobile device with internet access

Instructions

Part 1:

Task 1 Conduct search of high profile cyberattacks.

a. Using your favorite search engine conduct a search for each of the cyberattacks listed below. Your search will likely turn up multiple results ranging from news articles to technical articles. (Not limited to the following listed)
   - The Stuxnet Virus
   - Marriott data breach
   - United Nations data breach
   - Microsoft customer support database breach
   - Lifelabs data breach

   Note: You can use the web browser in virtual machine installed to research the hack. By using the virtual machine, you may prevent malware from being installed on your computer.

b. Also, conduct a search for Internet of Things (IoT) vulnerabilities. During your search, find an example of an IoT vulnerability for each of the IoT verticals: industry, energy systems, healthcare, and government.

c. Read the articles found from your search and share your thoughts (You shall select any one attack)

Task 2 Analysis of a cyberattack.

Write an analysis of the attack you have selected and try to answer the questions below. (Brief each answers within 20 to 50 words)

Who were the victims of the attacks?

What technologies and tools were used in the attack?

When did the attack happen within the network?

What systems were targeted?

What was the motivation of the attackers in this case? What did they hope to achieve?

What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

What is the vulnerability and who might exploit it? Explain.

Why does the vulnerability exist?

What could be done to limit the vulnerability?

Part 2: Background / Scenario

As individuals, in this field people perform a wide variety of jobs including, but not limited to, consultation, investigation, and program management services to mitigate risks from both internal and external sources. Those individuals, known as cybersecurity professionals are required to evaluate, design and implement security plans, conduct in-depth fraud investigation, perform security research and risk assessment, and propose solutions to potential security breaches.

Individuals with good security skills have a great earning potential. To be considered for one of these high paying jobs, it is very important to have the proper qualifications. Because of this, it is important to consider the industry certifications available for this career path. There are many certifications to choose from. Selecting the right certification(s) for you requires careful consideration.

Required Resources

- PC or mobile device with internet access

Instructions

Conduct search of Certifications.

1. Use your favorite search engine to conduct a search for the most popular cybersecurity-related certifications. List them below with the organization that provides the certification.

2. Pick three certifications from the list above and provide more detail about the certification requirements and knowledge gained i.e.: vendor specific or neutral, number of exams to gain certification, exam requirements, topics covered etc.

Investigate positions available within cybersecurity

Glassdoor is one of the largest job sites worldwide. Using your browser of choice, access glassdoor.com and search to find cybersecurity jobs available that were posted within the last two weeks. Adjust the search as you would like. You can search for jobs in your area or an area that you would like to live and work in. You could also use other job sites.

3. How many new job listings were posted within the last two weeks?

4. What is the salary range for the top 10 listings?

5. What are the most common qualifications required by employers?

6. What industry certifications are required by these employers?

7. Investigate online resources that allow you to legally test your hacking skills. These tools allow a novice with limited cyber security experience to sharpen their penetration testing skills. One such site is Google Gruyere (Web Application Exploits and Defenses). What kinds of challenges can you find?