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)

Lab 1: Attack and Defense: A Warmup

Cisco | Networking Academy®
Mind Wide Open™

n.kaliyamurthy@uwtsd.ac.uk

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 favourite 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**

In Jan 2010 a virus named 'Stuxnet',was discovered. It was a completely new type of virus - rather than hijacking computers or stealing information (like a traditional computer virus), it was designed to damage equipment that was controlled by computers. It was so unique, that a book was written about it called "*Countdown to zero day*". This led to a documentary being made (and shown on the BBC) called "*Zero Day*".
The main outline of the story is that in 2010, something unusual started happening at the uranium enrichment plant in Natanz, Iran.
Employees at the site started to notice that the centrifuges needed replacing at an unusually high rate. It wasn't discovered until months later that the reason for this was a piece of software, specifically designed to prevent the Iranian president from building a nuclear bomb. Computer security experts from around the world worked for months to deconstruct the code and ultimately discover what is now known to be the first 'digital weapon'. Rumoured to be created by the American Government, yet this is unconfirmed.

- **Marriott data breach**

In 2018, the Marriott hotel chain admitted that its computer system had been compromised, and hundreds of millions of customer records, including credit card and passport numbers could have been stolen by hackers. Four years earlier, the Marriott purchased another hotel chain called 'Starwood'; but didn't replace their computer systems with the Marriott's.

Before the acquisition, Starwood's security hadn't been the best (a different hacker had already gained access once before) and after the merger in September 2016, most of Starwood's corporate staff, including those managing information technology and security, were laid off.
The biggest shock of this story was not the fact that hackers were able to install a 'Remote Access Trojan (RAT) or MimiKatz malware, but it was that they were able to continue to have access to the system for four years before being detected. Another lesson to be learned from this is that much more care needs to be taken when dealing with sensitive information such as not storing the encryption key on the same server as the encrypted data. One possible reason for this attack has been suggested that it could have been the Chinese government, with the intention of creating a data-lake of information on American government employees that big data techniques can be used to analyse.

- **United Nations data breach**

One of the big threats in cyber security are 'Advanced Persistent Threats' or APTs. These are typically hacking groups or organised crime syndicates who use advanced and sophisticated techniques to gain unauthorised access to a system.
It is thought that APT actors were responsible for the U.N. cyberattack in 2019, one week after they called for an investigation into claims that Jeff Bezos' smartphone had been hacked by a Saudi Prince.
The U.N. attack affected at least 42 servers, including administrator accounts, user and password management systems, system controls and firewalls. Approximately 400GB of data is believed to have been stolen.
APT actors are most commonly linked with nation-state hackers and cyber-espionage campaigns. It is thought that the hackers gained entry using a known weakness in a Microsoft program called 'sharepoint'. It had been previously patched by Microsoft, but it appeared the U.N. hadn't updated their systems and the patch hadn't been installed.

- **Microsoft customer support database breach**

In December 2019, Microsoft's systems were breached, specifically an internal customer support database. The system consisted of a cluster of 5 servers which all mirrored each other and were used to simplify search operations in a customer support database.

It was realised that the reason these servers were able to be hacked was "misconfigured Azure security rules". Microsoft had to notify all of its affected customers, but also said that it found no malicious use for the stolen data. Yet the servers contained support records spanning 14 years - roughly 250 million entries, including email addresses, IP addresses and support case details.

One of the lessons learned was that databases should always require authentication, and that the data should always be encrypted; this one was unsecured, so anyone with a browser could access the database because no authentication was required at all, and some of the data was stored in plain text!

- **Lifelabs data breach**

Canada's largest data breach to date was a medical testing company called lifelabs. Almost half of Canada's population have had some sort of testing done with Lifelabs, it is thought to have exposed the sensitive personal information of approx. 15 million people. A civil lawsuit then followed seeking over $1b in damages. The breach included lab test results, national health card numbers, names, dates of birth, home addresses and email addresses.

It was suggested that a breach of this size may be an indication that new legislation maybe required. An investigation was carried out to determine whether the company took 'reasonable

precautions', and found they "lacked adequate security policies and procedures to protect patient data".

LifeLabs admitted that they made a payment to the hackers to retrieve the stolen data, but there can be no way to be certain that the criminals didn't make copies of the data.

The breach was caused by a "failure of adequate cyber security safety measures and controls". But since the breach, the firm has spent $50m to enhance its information security management and continues to employ outside cybersecurity teams to monitor and test their system.

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**
  North American casino by using an Internet-connected fish tank
- **Energy systems**
  In 2016, hackers left the residents of two apartment buildings in Lappeenranta, Finland in freezing cold for nearly a week by launching a DDoS attack on their environmental control systems via thermostats
- **Healthcare**
  In one instance, researchers from Check Point Research were able to find an ultrasound machine running a Windows 2000 OS which no longer receives security patches, leaving the machine vulnerable to a multitude of attacks
- **Government**
  Hackers working for the Russian government have been using printers, video decoders, and other so-called Internet-of-things devices as a beachhead to penetrate targeted computer networks, Microsoft officials warned

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

The CheckPoint research case was interesting because it was left vulnerable because everyone using the equipment was focused on it's primary use, and not being conscience of the fact that it is connected to the Internet, and therefore is also a route into the network from outside. The staff using the ultrasound machines would not have been thinking about the software running in the background, and possibly the IT staff of the hospital would have been concentrating on their office computers, and not thinking of all of the other devices which aren't immediately obvious. As more and more devices now require a connection to a network, from thermostats to smart lights, its becoming such so common to type a wifi code into a device, its easy to forget that this device needs updating as often as a computer.

The only answer is for company policies and procedures to be put in place for someone to regularly check all of the devices connected to the network, and update them and test them frequently. If everyone thinks that it is 'somebody else's job' then it never gets done.

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?

The direct victims of the attack were the hospital where the equipment was stored, but the real victims would be the patients who's personal information was stolen.

In another example - WannaCry attack that caused 20,000 appointments in the UK's NHS to be cancelled and over £150 million spent on remedying the attack.

What technologies and tools were used in the attack?

Researchers found that some of these machines were running on legacy software. Due to old and well-known security gaps in Windows 2000, the hackers were able to exploit one of these vulnerabilities and gain access to the machine's entire database of patient ultrasound images

When did the attack happen within the network?

All of the reports are from March 2019, and in Aug 2019 at the Defcon security conference it was shown how hacked ultrasound devices can be turned into acoustic weapons

https://nakedsecurity.sophos.com/2019/08/13/hacked-devices-can-be-turned-into-acoustic-weapons/

What systems were targeted?

Hospitals are regular targets of cyberattacks as patients medical data can be sold on the darkweb for a high price.

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

Usually hospitals are attacked and patient data stolen or encrypted, then the hospital would be held to ransom and only given access to their data after paying

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

In This particular case nobody as it was a research company carrying out the attack, a so-called "white-hat hacker". But if it had been a real world hacker, they could have used this easy way into the network to then cause serious damage throughout the hospital. Customer's data could have been stolen and sold, a ransom demanded for not cancelling all of the patient's appointments.

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

The vulnerability comes from the fact that the windows system running behind the ultrasound program was very outdated and hadn't had any security patches for many years. The people who would be interested in this would be looking to cause mayhem in the hospital unless a fee was paid. Or people willing to profit from selling patients personal and medical data (which apparently sells for anything from $60 to $1000.

Why does the vulnerability exist?

As time goes on, more and more weakness' are found on operating systems, usually these are 'patched' straight away – meaning that a fix for this weakness is downloaded on every device as soon as it is found. But if an operating system is left for years without having any of the recent patches applied, it becomes susceptible to attacks.

What could be done to limit the vulnerability?

This particular device was running Windows 2000, this has not been current (meaning no longer receives windows updates) for many years. The operating system should have been upgraded before Windows 2000 was made obsolete.

Part 2: Background / Scenario

Based on the lecture session, to defend any network, what is the available system? In other words. 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.

    - Certified Ethical Hacker (CEH) ...
    - CompTIA Security+ ...
    - Certified Information System Security Professional (CISSP) ...
    - Certified Information Security Manager (CISM) ...
    - Certified Information Systems Auditor (CISA) ...
    - NIST Cybersecurity Framework (NCSF) ...
    - Certified Cloud Security Professional (CCSP)
    - AWS Certified Security – Specialty Amazon

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.

AWS Certified Security

- Security Basics
- Security of AWS
- Security in AWS
- Using AWS Security Products
- Securing AWS Services
- Identity and Access Management
- Compliance
- Incident Management & Troubleshooting

Certified Ethical Hacker

- Module 01: Introduction to Ethical Hacking
- Module 02: Footprinting and Reconnaissance
- Module 03: Scanning Networks
- Module 04: Enumeration
- Module 05: Vulnerability Analysis
- Module 06: System Hacking
- Module 07: Malware Threats
- Module 08: Sniffing
- Module 09: Social Engineering
- Module 10: Denial-of-Service
- Module 11: Session Hijacking
- Module 12: Evading IDS, Firewalls, and Honeypots
- Module 13: Hacking Web Servers
- Module 14: Hacking Web Applications
- Module 15: SQL Injection
- Module 16: Hacking Wireless Networks
- Module 17: Hacking Mobile Platforms
- Module 18: IoT Hacking
- Module 19: Cloud Computing
- Module 20: Cryptography

Certified Information System Security Professional

- Module 1. Security and Risk Management
- Module 2. Asset Security
- Module 3. Security Engineering
- Module 4. Communication & Network Security
- Module 5. Identity & Access Management
- Module 6. Security Assessment & Testing

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?

432

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

   £36k - £51,855

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

   Security specialist

6. What industry certifications are required by these employers?

CompTIA Security +, CISSP and CCNA Security

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?

   Cross-site Scripting (XSS), Cross-site Forgery (XSF), Denial of Service (DoS)