Cybersecurity Presentation 1
Casey Adams

Charleston Southern University

CSCI.405

What is Cybersecurity?

- What is Cybersecurity?
- What makes us vulnerable?
- What should we be aware of when we are talking about attacks?
- How can we protect ourselves?

(Speaker Notes)

-No one can be too careful when it comes to Cybersecurity. According to the Cybersecurity Infrastructure Security Agency, (What is Cybersecurity?, 2021) "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

-Many things makes us vulnerable but mostly human error makes us vulnerable.

-We will talk about these questions throughout this presentation.

-This information we are going to talk about will center around security vulnerabilities, ways to protect yourself and your company, what to expect from attackers, and so much more. The subject of this presentation though will prove it does not matter how big your company is, what they do, or who they know. If a company is not following security procedures, providing training, and following best practices then that company could end up Heartland Payments.

Heartland Payment Systems Attack

- What was the Heartland Payment Systems Attack?
- When did the attack happen and what exactly happened?
- What effects did this attack have on Heartland as a company?

(Speaker Notes)

According to SmarterMSP.com, the Heartland Payment Systems was one of the worst hacks a company has experienced. (Chadran, 2015) " On January 20, 2009, Heartland Payment Systems announced that it had been “the victim of a security breach within its processing system in 2008.” Within days, Heartland’s stock price dropped 50 percent, sinking nearly 80 percent by early March." Attacks such as these do not just affect the value the attackers immediately steal from the company or the value they will later steal from the information they gained from the companies customers. The trust between the company and the customer is totally broken.

How the Attack Happened

- How did the attack happen?
- What did it take to pull off this attack?

(Speaker Notes)

-How the attack happened. The Cybercriminals hacked Heartland Payments by using a SQL injection.

-(Chadran, 2015) "A web form on the company's site unwittingly allowed access to Heartland's corporate network, where more extensive damage was done"

-Attackers spent many months trying to gain access by by-passing firewalls, anti-virus, and detection tools in order to install a sniffer tool.

-This attack took planning and time to pull off, but what was as important as having the knowledge to complete this attack was to have patients to successfully complete this attack. It took many months for this attack to become successful. The bad guys have no problem waiting for a "pay day" if they know it will pay off in the end.

What is a SQL injection and how is it done?

- A Sequel injection aka a SQL injection is an attack that injects malicious SQL code into an application in order to view or modify a database.
- Input code into a vulnerable input on a webpage or app.
- After the attacker executes the code, the attacker gets a response which gives the attacker knowledge of the data base.

(Speaker Notes)

What attackers do for SQL injection is input malicious code where you would input some type of information within a data input area such as where you would input a username or password. When you input any information into into a data point, attackers instead input an incomplete part of code. Once the computer pieces together the incomplete part of code to the rest of the code, the computer unknowingly executes the code for the attackers purposes.

Non SQL injection or Normal Input

- The following pictures are provided from W3schools.com. This is an example of normal input and how this input from the user interacts with the code. (Speaker Notes) Talk and explain the picture.

Username:
John Doe

Password:
myPass

Example

```
uName = getRequestString("username");
uPass = getRequestString("userpassword");

sql = 'SELECT * FROM Users WHERE Name ="' + uName + '" AND Pass ="' + uPass + '"'
```

Result

```
SELECT * FROM Users WHERE Name ="John Doe" AND Pass ="myPass"
```

SQL Injection Examples

- Within the username and password data input point we can see how it completes the code to execute so it is always “true” no matter what is input which allows the attacker to gain access.

User Name:

" or ""="

Password:

" or ""="

The code at the server will create a valid SQL statement like this:

Result

```
SELECT * FROM Users WHERE Name ="" or ""="" AND Pass ="" or ""=""
```

The SQL above is valid and will return all rows from the "Users" table, since **OR ""=""** is always TRUE.

Access to Information

- Once the attackers gained access what did they do?
- What tools did they use to gain the information they were seeking?

(Speakers Notes)

According to an article written by Grant Gross in 2015 on computerworld.com, after the successful SQL injection attack on Heartland Payments, the attackers “placed malware into the compromised networks that gave them backdoor access”. This allowed them access to the data they would end up stealing and also allow them to use a Sniffer on the network which we will talk about in our next slide.

Sniffer

- What was the next Phase of the attackers plan?
- What is a “Sniffer”?
- Why was a “Sniffer” helpful for the attackers in this case?

(Speak Notes)

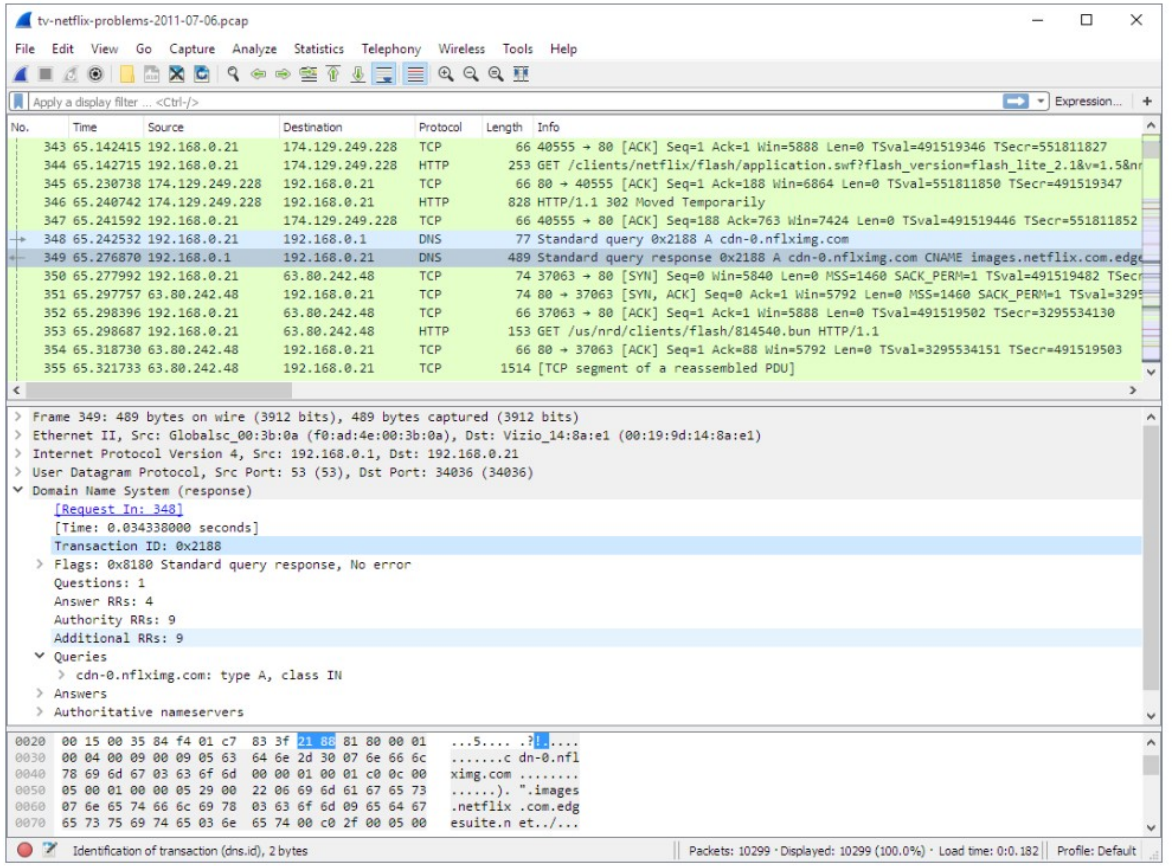
-A Sniffer has many names, one being a packet analyzer.

-Purpose is to identify and monitor network traffic.

-Once attackers were in Heartlands network a sniffer is how they could monitor network traffic packets with credit card information. Anytime any information is passed over the network it is done so in packets. Any and all information is passed this way. There are ways/rules/regulations to prevent attackers/hackers from seeing this information now but at the time of this attack, Heartland made a very costly mistake which effected the company and the customers of the company.

These attackers were committed, willing to wait and once they were inside the network they knew using a Sniffer or packet analyzer would help them get what they wanted which was money. This is not always the case though. Sometimes hackers simply do it just for the fame or just to be disrupters. Using their real names would get them caught to quickly so If they immediately put their name out in public after their first successful attack they would not be able to attack again which is why they go by nicknames or be apart of a hacking group but when it comes to the hack of Heartland Payments, we found out who exactly they are which tells us more of their intentions.

Sniffer Example



- This picture shows just some of the data that a “Sniffer” can show us. It will show us what IP address a packet came from and where it is going to, the port it is using, when it happened, many other things about the information being sent, and when it is not encrypted we can see pretty much anything.

The Cyber Criminals

- Russian citizens Vladimir Drinkman, 37, of Syktyvkar and Moscow, Russia, and Dmitriy Smilianets, 34, of Moscow.
- Worked with another famous cyber criminal named Albert Gonzalez who stole physical hardware to gain information from Heartland Payments along with stealing data from many other businesses.
- Other codefendants who were able to avoid capture before Drinkman and Smilianets were Alexandr Kalinin, Roman Kotov, and Mikhail Rytikov. These men were either from Russia or from Ukraine.

Conclusion

- This team of hackers are a very smart group of people. Each member had some type of specialty with computers and each had their role in making their attack successful.
- As discussed earlier, not only did it effect the people who had their personal information stolen, it also greatly affected the companies they had stolen from by stock prices falling, time and effort, and most importantly lost of trust by their customers. Trust is a hard thing to earn back.
- To prevent a SQL injection attack relies on the developers who create the code. According to SQL injection Prevention Cheat Sheet, depending on the language you use to write the code there are different ways to stop SQL injection by not allowing code to execute in the data input areas of company run sites.

Java – use PreparedStatement()

PHP – use parameterized queries (bindParam())

In a language such as PHP, using code such as stripcslashes($username); or mysqli_real_escape_string($con, $username); will prevent code from being written in the data input area. There are many ways to prevent SQL injection but you have to have a very good understanding of developing code. Ensuring that your developers are knowledgeable and security focused can end up saving your company a lot of money and avoid a headache in the future. Cybersecurity is one of the most important topics today for a businesses that relies on anything with an online presence.

References

- What is Cybersecurity?. (2021, February 01). https://www.cisa.gov/news-events/news/what-cybersecurity

- Chadran, Achmad. (2015, October 19). The 3 worst data breaches of all time (the lessons learned). https://smartermsp.com/3-worst-data-breaches-time-learned/

- SQL Injection, n.d. https://www.w3schools.com/sql/sql_injection.asp

- Higgins, Kelly Jackson. (2018, February 16). Russian Hackers Sentenced in Heartland Payment Systems Breach Case.https://www.darkreading.com/attacks-breaches/russian-hackers-sentenced-in- heartland-payment-systems-breach-case

- Gross, Grant. (2015, February 17). Russian extradited to U.S. for hacks tha tstole 10M credit card numbers. https://www.computerworld.com/article/2885453/russian-extradited-to-us-for-hacks-that-stole- 160m-credit-card- numbers.html#:~:text=Vladimir%20Drinkman%2C%2034%2C%20of%20Syktyykar,said%20in%20a%20press%20release.