Hands-on B1: Predicting Threats

1. **What are the most significant cyber security concerns in 2020 shifted from 2019?**

In 2019, we saw the growth of a series of complex and targeted ransomware attacks. Specific industries have suffered severely, including state and local governments and healthcare organizations. The new grim reality is that the attackers spent more time collecting information on the victims, achieved the most considerable degree of damage, and expanded the refunds scale.

1. **In your opinion, what were the top 3 most significant security issues in 2019 and why did you choose these?**

*Over 100 Million JustDial Users’ Personal Data Found Exposed On the Internet April , 2019*

More than half a billion JustDial user's information was exposed. And it includes usernames, email addresses, mobile numbers, addresses, occupations, and even photos. It is a grave privacy breach. May cause a lot of fraud. Cause significant direct economic losses to users.

*Data Breach Forces Medical Debt Collector AMCA to File for Bankruptcy Protection,* June , 2019

The exposed information included names, date of birth, address, phone, date of service, provider, balance information, and credit card or bank account. This information can directly cause significant economic losses to the victims.

*Massive Capital One breach exposes personal info of 100 million Americans* August, 2019

Many people were affected by this information leak, and there were many information contents. It includes Customer status data, e.g., credit scores, credit limits, balances, payment history, contact information. It causes significant direct economic losses to users.

**3. Which of the recent technologies are most exploited and why do you think they become the growing target?**

Chapter 9

It should be ZERO TRUST NETWORKS. Zero Trust Networks is about having the ability to “Divide and Rule” your network in order to reduce the risk of lateral movement. The key idea is to create a network segmentation by placing multiple inspection points within the network to block malicious or unauthorized lateral movement; so in the event of a breach, the threat is easily contained and isolated. The best practice is to create a very granular segmentation by defining “least privileged” access control strategy; where user/system can gain access only to the resources that they are meant to use. For example, an access to source code should be granted only to R&D team members. This way only the absolute minimum, legitimate traffic between segments is allowed, while everything else is automatically denied.

Hands-on B2: Password Cracking

1. **What is hash? How is it related to password? How is it used for password cracking?**

Hash is to map data of any length to a domain of finite length. It is to mix a string of data M and output another piece of fixed-length data H as the characteristic of this data.

The most straightforward and most time-consuming method is Brute force Attack, which is cracked through a lot of attempts and massive calculations. Another cracking way is Dictionary Attack, a preset list of frequently used or mutated password dictionaries to check one by one. It has less time complexity than brute force cracking. Still, there is a high probability that the password does not exist in the dictionary.

1. **Submit your result of hash cracking, including the original word used for the hash and the type of hash function. If one or more of those hashes cannot be cracked, please state that you did not manage and your opinion about why it was not cracked.**

The website of crackstation.net uses massive pre-computed lookup tables to crack password hashes. Maybe the hash value does not find the corresponding password in the hash table.

Other possibilities are: crackstation.net does not support this hash encryption method. Or the Hash value has been tampered with, failing to parse usually.

|  |  |  |
| --- | --- | --- |
| **Hash** | **Type** | **Result** |
| 81dc9bdb52d04dc20036dbd8313ed055 | md5 | 1234 |
| e91e6348157868de9dd8b25c81aebfb9 | md6 | security |
| b273b0604664ef525ef83046d1b79659 | unknown |  |
| 7110eda4d09e062aa5e4a390b0a572ac0d2c0220 | shal | 1234 |
| c84c50d5a767a23bda0ea5ca348fed54c6db9aab | shal | fun |

**3. Create at least 2 hash digests. You can use a tool like this: http://www.fileformat.info/tool/hash.htm. Submit your original word, corresponding hash digest, and hash function.**

|  |  |  |
| --- | --- | --- |
| Original text | MD5 | SHA-1 |
| massey | 1c34523403b86c6d23730a71c3b58720 | 1c06368eae0b0d8664c0ce6102f697dfa9961ce5 |
| NewZealand | 10628dfb1306f3da181885e4691029e4 | 94674db52ffc47736b4f47c138606668a76602e8 |
| Implementation&Management\_SystemsSecurity | b009e808a77e7b289b667c2547c068c5 | 1b329efa1aad14ce429a02144401b34dc9c74d09 |

Hands-on B3: Exploiting Web

1. **Let’s assume that someone else was already logged in. Describe what attack is attempted by the following sequence and the way the attack is executed.**

It is a Command Injection attack. The hacker uses a piece of script code to register, and the server saves this code to the database. When this user is queried, the Javascript will be executed. When hackers change the script to other offensive back-end server languages or SQL statements, it will cause significant damage to the server or database. This type of attack can be effectively avoided through double regular verification of the front and back ends.

1. **Describe what attack is attempted by the following sequence and the way the attack is executed.**

It is a typical SQL injection. Enclose other SQL statements in the get request. This statement is executed at the database level and returns all user information in the User table.

The above URL did not return any users.