LAB Manual

PART A

(PART A : TO BE REFFERED BY STUDENTS)

**Experiment No.02**

**A.1 Aim:**

To study and analyse different types of web security threats.

**A.2 Prerequisite:**

Knowledge of security attacks and security fundamentals

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Identify different type of attacks

2. Analyse security incidents.

**A.4 Theory:**

1. **Equifax Data Breach –**

Credit reporting agency Equifax aggregates financial data on more than 800 million consumers and 88 million businesses worldwide. On July 29, 2017, the company detected and blocked suspicious network activity associated with a web portal used by U.S. consumers to file disputes.

Later analysis revealed the portal’s application framework, Apache Struts, was outdated and had a severe security vulnerability. Equifax hired cybersecurity firm Mandiant to conduct a forensic analysis, which revealed a massive data breach affecting 143 million U.S. consumers.

Further investigation later increased the number to 145.5 million – or about 45% of the U.S. population.

Severe Vulnerability Overlooked

Equifax was first alerted to the Apache Struts vulnerability (CVE-2017-5638) on March 8, 2017, more than two months before the breach started, according to testimony to a U.S. House subcommittee by former Equifax CEO Richard Smith.

Equifax failed to act on the alert and apply the available patch. Seven days later, the company also performed vulnerability scans that failed to identify the flaw, said Smith. Hackers launched the attack exploiting the vulnerability about two months later, on May 13, 2017. By the time the breach was discovered in late July, hackers had accessed dozens of databases and created more than 30 backdoors into Equifax’s systems.

Answer following questions:

1. Analyze and mention the security loophole/s in above scenario.
2. Mention security measure to overcome this issue

**2. Uber Data Breach** –

57 Million Records Uber’s CEO revealed on Nov. 21, 2017, that the ride-hailing service failed to disclose a massive data breach last year. In Oct. 2016, hackers accessed a server containing personal information for more than 57 million Uber drivers and riders. They demanded a $100,000 ransom to delete their copy of the data, which Uber paid.

The attackers allegedly first accessed a private GitHub repository used by Uber’s developers. The repository contained code with login credentials for other Uber systems, which ultimately provided access to the stolen data. Uber later identified the hackers and pushed them to sign nondisclosure agreements. It also disguised the ransom payment as part of a bug bounty program, according to the New York Times. Lawsuits are now raining down on Uber from attorneys general across the U.S.

Answer following questions:

1. Identify type of security attack
2. Do you think there was security loophole/s in above scenario?
3. Mention security measure to overcome such type of issue.

**3. WannaCry Cyber Attack –**

300,000 Systems What some have called “the worse ransomware attack ever” struck in May 2017, infecting an estimated 300,000 computer systems just four days.

WannaCry was similar to many ransomware attacks, i.e. it encrypted files and demanded a Bitcoin payment to decrypt them. However, it differed in one major way: worm tactics. Once WannaCry infected a machine, it scanned the connected LANs and WANs to find and attack other vulnerable hosts. The subsequent infections occurred automatically without user interaction. This allowed WannaCry to seize entire networks and even hop to others, rapidly sparking a flash epidemic worldwide. The National Health Service in the U.K. was hit particularly hard, with at least one-third of health trusts (i.e. healthcare offices and services) disrupted and over 19,000 appointments canceled, including surgeries.

Stolen NSA Cyber Weapons

WannaCry spread via EternalBlue, an exploit for Windows Server Message Block version 1 (SMBv1), a legacy network file-sharing protocol present in every version of Windows released in the last 15 years (and maybe more). The exploit is allegedly from a cache of cyber weapons stolen from the U.S. National Security Administration (NSA) and released publicly on April 14, 2017.

Microsoft issued a patch for the vulnerability on March 14, 2017. When the attack began, every Windows system that had not been patched within eight weeks was vulnerable. EternalBlue was also used in the Petya ransomware and NotPetya malware attacks in June, and has also been observed in other attacks.

Answer following questions:

1. What is ransomware?
2. Mention security measure to overcome such type of issue.

**4. The Joker malware**

steals money from users by subscribing them to paid subscriptions without their consent. It first simulates interaction with ads without users' knowledge and then steals the victim's SMS messages including OTP to authenticate payments. Joker malware found hiding inside of seemingly legitimate applications, a new variant of the Joker Dropper and Premium Dialer spyware was discovered by Check Point’s researchers in the Google Play Store. The new, updated Joker malware can download additional malware to the device, which in turn subscribes the victim to a number of premium services without their consent.

Read more information about Joker malware on following articles:

<https://www.theweek.in/news/sci-tech/2020/07/13/What-is-the-Joker-malware-Heres-how-it-affects-apps.html>

<https://threatpost.com/joker-android-malware-dupes-its-way-back-onto-google-play/157307/>

<https://www.thequint.com/tech-and-auto/tech-news/google-removes-11-apps-from-playstore-with-joker-malware>

<https://www.phonearena.com/news/google-play-joker-android-malware-delete-these-apps_id125906>

<https://www.firstpost.com/tech/news-analysis/joker-malware-an-app-vulnerability-that-may-have-tricked-you-to-steal-your-money-7341821.html>

Answer the following questions:

1. Why Joker malware is different than other malwares?
2. List the apps which are affected by this malware as of now (current date).
3. List the precautions for such scenario, also give justification for each precaution.
4. Give thought “future of such malware”.

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no portal access available)***

|  |  |
| --- | --- |
| Roll. No. N049 | Name: Tarun Tanmay |
| Class MBATech CE, 3 Year | Batch: B3 |
| Date of Experiment: 15/7/2020 | Date of Submission: 15/7/2020 |
| Grade: | |

**B.1 Theory written by student:**

**Equifax Data Breach:**

**Do you think there was security loophole/s in above scenario?**

• The Apache Struts software in use was outdated and had a serious vulnerability

flaw (CVE-2017-5638).

• Also, the vulnerability scans performed by were faulty and did not identify the

flaw in the Apache Struts Software.

**Mention security measure to overcome such type of issue.**

• Track of Common Vulnerabilities through a reputable source such as Mandiant.

• Keep a detailed list of all the software&#39;s dependencies, libraries, and

components, by version and at the most current general release version so as to

track down the corrupted component quickly.

• Ensure the business partners factor 20 percent of their quarterly release budget

to keeping applications and their dependencies current.

**Uber Data Breach**

1)**Type of attack**: Data Breach

2) **Security Loopholes:**

* Usage of 3rd party cloud based services without considering a corporate infrastructure
* Developers failed to scan and maintain the resources from malware or breech

**3)Security Measure:**

1. All the dependencies in the GitHub used by Uber developers should be properly maintained

and scanned periodically for any malware or breach.

2. A zero-trust stance created and maintained that ensures all access to services must be

authenticated, authorized and encrypted.

3. Avoiding use of third party resources for data storage and access

Usage of 3rd party cloud based services without considering a corporate infrastructure

Developers failed to scan and maintain the resources from malware or breech

**WannaCry Cyber Attack**

1)**What is Ransomware?**

Ransomware is malicious software that infects your computer and displays messages

demanding a fee to be paid in order for your system to work again. This class of malware is a

criminal moneymaking scheme that can be installed through deceptive links in an email

message, instant message or website. It has the ability to lock a computer screen or encrypt

important, predetermined files with a password.

**Mention security measure to overcome such type of issue.**

1)Prevent the infection from spreading by separating all infected computers from each other,

shared storage, and the network.

2) From messages, evidence on the computer, and identification tools, determine which

malware strain you are dealing with.

3) Report to the authorities to support and coordinate measures to counter attack.

4) Use safe backups and program and software sources to restore your computer or outfit a

new platform.

5) Make an assessment of how the infection occurred and what you can do to put measures

into place that will prevent it from happening again

**Joker Malware**

1. Malware can be of different kinds. Joker is a TROJAN malware which is activated only

when a user interacts with it in the form of an app installation as such. The virus then

goes past the device&s security and is able to render the device useless or even steal

information

2. com.imagecompress.android, com.relax.relaxation.androidsms,

com.cheery.message.sendsms (two different instances),

com.peason.lovinglovemessage, com.contact.withme.texts, com.hmvoice.friendsms,

com.file.recovefiles, com.LPlocker.lockapps, com.remindme.alram and

com.training.memorygame.

3. Monthly check your bank account statements and verify each transaction that you’ve

made to not be a victim of Joker malware. The person should also check his messages

and notice any unusual activity like generation of an OTP without his intervention.

Install security solutions like QuickHeal or Kaspersky which continuously scan any new

downloads or installations on your device to prevent any malware from infecting the

system.

4. Malwares are man-made. If you find a solution to stop one, after a while, a few more

will pop up. The most secure device is only one which is completely isolated, i.e. doesn’t

have any connectivity. But in the real world, such a device would be deemed completely

useless. Hence, we should keep our security up-to date and keep apps update. Also, we

should be careful on which websites we store our passwords.

**B.2 Conclusion:**

**After successful completion of this experiment I am able to** 1. Identify different type of attacks

2. Analyse security incidents.