Homework Assignment 4

Graded

Student

HARRY KIM

Total Points

97 / 100 pts

Question 1

Upload your PDF document

97 / 100 pts

- ✔ **+ 10 pts** Finding security issue #1
- ✔ **+ 10 pts** Finding security issue #2
- ✔ **+ 10 pts** Finding security issue #3
- ✔ **+ 10 pts** Finding security issue #4
- ✔ **+ 10 pts** Finding security issue #5
- ✔ **+ 10 pts** Finding security issue #6
- ✔ **+ 10 pts** Finding security issue #7
- ✔ **+ 10 pts** Finding security issue #8
- ✔ **+ 10 pts** Finding security issue #9
- ✔ **+ 10 pts** Finding security issue #10
- 💬 **− 3 pts** A better mitigation for security issue 1 would be HTTPS.

  The potential consequences fail to describe or demonstrate why security issue 6 is a problem. -3

Question assigned to the following page: 1

Harry Kim
u1226472

CS 4440 Assignment 4

Security Issue 1: The Web Server uses HTTP protocols, meaning that all the communications between the clients and the Web Server are based on HTTP protocols.

Potential consequences: This is a vulnerability because it allows attackers to perform TCP Hijacking on a well known port (HTTP port 80). The connection of the clients can be hijacked which allows attackers to insert malicious data into the TCP stream and victims will believe it came from the original source when in reality they are being attacked and possibly stripped of sensitive data.

Mitigation: Use a private port or intercept packets between the source and destination IP addresses (packet sniffing) to verify that the connection has not been intercepted by an attacker.

Security Issue 2: The web page is vulnerable to XSS (Cross-Site Scripting). An attacker would be able to send malicious code in the form of a browser side script.

Potential consequences: This vulnerability can lead to the attacker stealing an EasyTax employee's session, stealing sensitive data, rewriting the webpage, and redirecting benign users to a malicious website to steal their information.

Mitigation: Encrypt or validate all user supplied input. Perform allow list input validation on user input. Use HTML sanitizer.

Security Issue 3: All the data saved to the Database Server is plain data (data is not encrypted when stored to the database). An attacker within the company would be able to access the data physically.

Potential consequences: This vulnerability would lead to unwanted theft of client data or massive leaks that include user data and/or sensitive company data that can be given or sold to the wrong hands.

Mitigation: Encrypt the data that is stored in the Database Server.

Security Issue 4: The WorkStation runs Windows XP. This version of windows is known to have many security issues as described in https://en.wikipedia.org/wiki/Criticism_of_Windows_XP.

Potential consequences: Attackers would utilize buffer overflows to allow attackers to cause a denial of service or execute malicious code. Windows XP users are also susceptible to malware

Question assigned to the following page: 1

such as viruses, trojan horses, and worms through emails. Especially since It is connected to both the Web Server and the Database Server.

Mitigation: Upgrade the operating system to the current Windows OS and regularly update.

Security Issue 5: Bob uses the Work Station for personal use such as checking emails and surfing the internet.

Potential consequences: Bob would be able to open an email or open a website that installs malware to EasyTax's systems which can be used by attackers to manipulate the data and ask for a ransome on a company-wide scale.

Mitigation: Block and ban employees from opening non-approved sites and logging in any email account that is not company related.

Security Issue 6: EasyTax configures a static IP for the Work Station and makes the Work Station directly accessible from the internet.

Potential consequences: If an attacker knows the IP address, they will use it to steal very important information such as locations and online identities.

Mitigation: Use dynamic IP.

Security Issue 7: Bob uses "123456" as the password to log into the Remote Desktop. According to https://www.security.org/how-secure-is-my-password/, a computer would be able to crack this password almost instantly.

Potential consequences: An attacker would login to the Remote Desktop to steal sensitive data or install malware onto company systems.

Mitigation: Require all passwords to include numbers and special symbols to increase the security.

Security Issue 8: Bob uses SMBv1 to allow remote file access which is a version of SMB that Microsoft does not consider safe to use. SMBv1 has a multitude of security concerns outlined in this article: https://kb.iu.edu/d/aumn#security.

Potential consequences: Using the outlined exploits, attackers would send out devastating malwares such as the WannaCry ransomware attack back in 2017.

Question assigned to the following page: 1

Harry Kim
u1226472

Mitigation: Update to the latest SMB version and frequently update.

Security Issue 9: All messages going through the Work Station's communication channel between Bob and the clients are encrypted using the DES algorithm, which is no longer considered a secure algorithm due to the relatively short 56-bit key size which makes it vulnerable to brute force attacks and cryptanalysis.

Potential consequences: An attacker would be able to crack the DES algorithm encryption by which point they would intercept private messages between Bob and the clients he is communicating with.

Mitigation: Use a different, updated, and more secure encryption system like AES to encrypt messages with sensitive data.

Security Issue 10: After Bob recovered the data from the database, he ignored the ransomware which was still running on his computer and continued with his work as if nothing happened at all.

Potential consequences: The ransomware could potentially spread to all other machines within the company and cause a company-wide catastrophe of data loss which at that point would only be recoverable via paying the ransom.

Mitigation: As soon as ransomware is detected, employees should immediately report to their company's network security team to avoid the spread of the malware, disable the malware, and to isolate and learn more about such attacks to avoid them in the future.