Advanced security assignment 2

C20452282

Ethar Boudouara

Q1

The shortage of security personnel worldwide can be attributed to serval factors:

Skill gap:

Due to rapid technologies improvements security workers must be knowledgeable in cybersecurity, data analytics, risk assessment, and threat intelligence. However, there is a shortage of people with specialised training and expertise in these fields.

Increasing demand:

As global dangers such as terrorism, cybercrime, and geopolitical tensions have increased, so has demand for security people. Organisations from all sectors, including government agencies, businesses, and private firms, are actively looking for qualified security specialists to protect their assets and information.

Retention Challenges:

Security professions can be hard, with long hours, high stress levels, and exposure to potentially hazardous circumstances. This might make it difficult to retain competent workers, since many may seek different career paths that provide a better work-life balance and job satisfaction.

Competitive Job Market:

The shortage of security staff has resulted in a highly competitive job market, making it difficult for organisations to attract and retain top talent. Furthermore, the globalisation of labour markets has made it simpler for skilled security personnel to find work abroad, worsening the shortfall in some areas.

To address the shortage of security personnel, several measures and actions can be taken

Promotion of Diversity and inclusion:

Encouraging diversity and inclusion in the security profession can help attract a wider range of talent and viewpoints. Efforts should be made to hire people from underrepresented groups and to promote inclusive work cultures that encourage innovation and collaboration.

Enhanced Recruitment Strategies :

Organisations should use innovative recruitment strategies to attract qualified candidates, such as offering competitive salaries and benefits packages, utilising social media and professional networks for talent sourcing, and collaborating with educational institutions to identify promising candidates.

Technology Adoption:

The use of sophisticated technologies such as artificial intelligence, machine learning, and automation can serve to increase the skills of security professionals while alleviating some of the staffing restrictions. These technologies have the potential to expedite security operations, improve threat detection and response capabilities, and allow workers to focus on more important activities.

A security specialist must possess knowledge of security across several platforms, fundamental computer forensics abilities, an awareness of hacking, technical acumen, and soft skills such as communication. n order to become a security expert, I will need to improve my knowledge of security across multiple platforms as well as my core computer forensics skills. These are not huge impediments, and they can be learned over time, but they are currently preventing me from becoming a security expert.

Q2 For this part I used JSHint a code analysis tool that checks that checks javascript code for potential issues

A screenshot of a black and white page

Description automatically generated

Q3

Google Hacking: Basic Operators

Basic Operators Used Alone:

+ (Plus Operator): Used to ensure that the search results contain the specified term.

For example, the search term +security vulnerabilities will provide results that have both "security" and "vulnerabilities".

- (Minus Operator): Used to eliminate certain terms from search results.

For example, cybersecurity -attacks will show results about cybersecurity that do not include the word "attacks".

Basic Operators for Combination:

" " (Quotation Marks): Used to search for a specific phrase.

For example, searching for "network security" will yield results that include the precise term "network security."

\*\*\* (Asterisk Operator)\*\*: Serves as a wildcard for any word or phrase.

For example, searching for "security tips" will provide results such as "security best practices tips" or "security awareness tips."

~: this makes the search result include synonyms of a word you’re searching for

Example: ~happy

Same result without operator if you do

“happy” OR “content” OR “pleased”

. : is used to search for specific domains

Example: google.com

OR: this lets you retrieve search results for either of the keywords searched Example: “korea” OR “South Korea”

| : is used to search for either of the two specified key words in search

Example: happy | content

“happy” | “content”

Advanced Operators Used Alone:

allintext: Looks for occurrences of all terms in the text of a webpage.

For example, allintext:security vulnerabilities will yield webpages that contain the words "security" and "vulnerabilities".

allintitle: Searches for all of the terms in a webpage's title.

For example, allintitle:cybersecurity best practices will return sites with the words "cybersecurity" and "best practices" in the title.

Advanced Operators Used in Combination

Site: Restricts the search to a certain site or domain.

For example, searching for security vulnerabilities at site:example.com will only yield results for the website "example.com".

Filetype: Limits the search to a certain file type.

For example, filetype:pdf cybersecurity guidelines will return PDF documents providing cybersecurity guidelines.

Equivalent operators in Bing:

While Bing may not have direct equivalents to all of Google's operators, it does provide similar capabilities via its own set of operators:

Basic Operators:

+ (Plus Operator): Bing does not recognise the "+" operator in search queries.

- (Minus Operator): Bing allows you to exclude specific terms by using the "-" operator.

Advanced operators:

site:: Bing, like Google, allows the "site:" operator to limit results to a certain site or domain.

Bing supports the "filetype:" operator for limiting results to specific file types.

Bing supports the "intitle:" operator, which allows you to search for specified phrases in webpage titles.

List of Ten Search Engines:

Bing

Advantage: Offers different search results and works well with Microsoft services.

Disadvantage: The index may not be as extensive as Google's.

Yahoo

Advantage: Provides a diverse selection of material, including news, email, and more.

Disadvantage: Relying on Bing search results.

DuckDuckGo

Advantage: prioritises user privacy and does not collect user data.

One disadvantage is that search results may be less thorough than those provided by Google or Bing.

Baidu

Advantage: The largest search engine in China, with results in Chinese.

Disadvantage: Limited applicability outside of Chinese-speaking regions.

Yandex

Advantage: A popular search engine in Russia that offers localised search results.

Disadvantage: Limited use outside of Russian-speaking regions.

Ask.com

Advantage: Provides a question-and-answer format for search queries.

Disadvantage: Search results may be less thorough than those from other search engines.

AOL Search

Advantage: Allows access to a variety of AOL services and content.

Disadvantage: Relying on Bing search results.

WolframAlpha

Advantage: It focuses on delivering computational responses to inquiries.

Disadvantage: Not appropriate for general web searches.

Qwant

Advantage: Values privacy and does not collect user data.

One disadvantage is that search results may be less relevant than those provided by other search engines.

Ecosia

Advantage: Uses search money to plant trees all over the world.

One disadvantage is that search results may be less thorough than those provided by Google or Bing.

Q4

SQL Injections:

Vulnerability: Without sufficient input validation, attackers can insert SQL commands into an application's database queries.

Exploit: Attackers can use SQL queries to extract, edit, or remove sensitive data from the database.

For example, an attacker injects '; DROP TABLE users; --' into a login form, forcing the database to drop the "users" table.

Cross-site scripting (XSS):

Vulnerability: A lack of input sanitization allows attackers to insert malicious scripts into web pages seen by other users.

Exploit: Attackers can run arbitrary JavaScript code in other users' sessions, resulting in session hijacking, data theft, or defacement.

An attacker injects <script>alert('XSS attack!');</script> into a forum post, which causes it to execute when other users view it.

Buffer Overflow:

Vulnerability: Poor memory management allows attackers to write outside the buffer's boundaries, resulting in data corruption or the execution of arbitrary code.

Attackers create input data that exceeds the buffer size limit, overwriting nearby memory addresses with malicious code.

Assume an attacker presents a crafted input to a susceptible application, leading it to overwrite a return address and reroute the execution flow to a shellcode payload.

Cross-site request forgery (CSRF):

Vulnerability: Without CSRF tokens or unpredictable request parameters, attackers can falsify requests on behalf of authenticated users.

Exploit: Attackers deceive victims into performing unauthorised operations on a trusted web application, such as updating account settings or conducting financial transactions.

For example, an attacker uses a weakness in a web server's file upload functionality to upload a malicious PHP script, which is subsequently executed on the server to acquire control.

Information Disclosure:

Vulnerability: Improper error handling or improper permissions allow attackers to get access to sensitive information such as system configuration details or user passwords.

Exploit: Attackers employ vulnerabilities to obtain sensitive data contained in files, folders, or system logs that are accessible to unauthenticated users.

For example, an attacker searches a website's "robots.txt" file for hidden directories or files containing sensitive information.

Man-in-the-Middle (MITM) Attack:

Vulnerability: The absence of encryption or inadequate authentication procedures allows attackers to intercept and manipulate communication between two parties.

Exploit: Attackers position themselves between the client and the server to intercept and alter data transmitted between them, potentially stealing sensitive information or introducing malware.

For example, an attacker creates a rogue Wi-Fi hotspot and intercepts unencrypted HTTP communication between a user's device and a website, allowing them to obtain login credentials.

A Denial-of-Service (DoS) attack

Vulnerability: Resource exhaustion or improper capacity management allows attackers to overrun a system or network, rendering it inaccessible to legitimate users.

Attackers overwhelm a target system or network with too much traffic, requests, or malicious packets, causing it to slow down, crash, or become unresponsive.

Attackers overwhelm a target system or network with too much traffic, requests, or malicious packets, causing it to slow down, crash, or become unresponsive.

Example: An attacker uses a botnet to perform a distributed denial-of-service (DDoS) assault against a website, flooding the server with a high volume of requests and leaving it unreachable to normal users.

LDAP Injection:

Vulnerability: Incorrect input validation enables attackers to modify LDAP queries used for user authentication and permission.

Attackers introduce malicious LDAP filter strings into input fields to bypass authentication systems or get unauthorised access to data.

An attacker creates a malicious LDAP query string that pulls all user records from the directory, including sensitive information like passwords.

XML External Entity (XXE) Injection

Vulnerability: Insecure XML processing allows attackers to use external entity references to gain access to local or remote files and execute arbitrary code.

Exploit: Attackers insert malicious XML payloads including external entity declarations, which the XML parser uses to reveal sensitive information or execute commands.

For example, an attacker sends a forged XML document that includes an external entity reference to a local file holding password hashes, allowing them to extract sensitive information.

SQL injection demo link

<https://www.codingame.com/playgrounds/154/sql-injection-demo/sql-injection>

admin

unknown' or '1'='1

cross site scripting

<https://learn.snyk.io/lessons/xss/javascript/>

A screenshot of a computer

Description automatically generated

Graphical user interface, application, website

Description automatically generated