CSC8015

SECURITY ANALYSIS REPORT

TABLE OF CONTENTS

2023-2024
MSc Computer Science
Nazli ALDOGAN
Std. No 230404296

ANSWERS FOR QUESTION 1

OS and Service Detection

YouTube video link: https://youtu.be/8ith5-hvm4c?si=r3eMQuypLVu0EaCB

1. The -sV option can be used to detect running services and make guesses on operating systems. Based on the scan -sv operation being applied to port 80 of scanme.nmap.org, *What Linux Distribution is likely to be running?*

   By running the “nmap scanme.nmap.org -sV” command, I am able to view all of the active ports and also to see what systems are running on these active ports. By looking at port 80 here, I can see that it is running the Ubuntu Linux distribution.

   In order to see only the specified port, in our case, port 80, I could also run the “nmap -sV -p80 scanme.nmap.org” command, showing me only port 80 this time. Again, I would see that it is running the Ubuntu Linux distribution.

2. Again using the -sV option to detect services, *What version of SSH is being used?*

   By running the “nmap scanme.nmap.org -sV” command, I view all the active ports and the systems running on these ports and see the SSH service is from port 22 and it uses the 6.6.1p1 version.

TELNET Analysis

YouTube video link: https://youtu.be/nqWZ_Tv3X-Q?si=r1rmSg_VBGU3YTgO

1. The Wireshark has many useful utilities. One of these, is to follow a particular data stream in its entirety. This is a TCP connection. *What is the username used in this TELNET connection?*

   By following the TCP stream, I can view the information sent between the two devices as Wireshark captures this data. I can view the username used in this TELNET connection is fake.

2. *What is the password used in the TELNET connection?*
   The password used in this TELNET connection is user.

3. What is the IP address of the server?
   The IP address of the server is 204.71.200.67.

4. *What is the exact command that is used to determine all the files in the working directory in this TELNET exchange?*
   The exact command that is used to determine all the files in the working directory in this TELNET exchange is ls -a.
   All of the files in the working directory are: . .. .cshrc .login .mailrc .profile .rhosts.

ANSWERS FOR QUESTION 2

CASE STUDY 1:

CYBERSECURITY RISK ASSESSMENT OF X BUILDING'S SENSOR NETWORK

The purpose of this report is to identify and diagnose some cybersecurity threats concerning the deployment of 1000 sensors across X Building, and to propose some possible precautionary actions. As a white hat hacker, I ensure properly conducting the security analysis by working in compliance with the following methodology: (1) identify the system properties, (2) diagnose potential threats, (3) assess possible vulnerabilities, (4) provide precautionary actions, and (5) review this assessment.

1. SYSTEM PROPERTIES

Building X has 1000 sensors deployed for capturing CO_2 and analysing how the building is utilised, wired using the KNX protocol to BACnet controllers, connected to the main building management system using the IP network present in the building. Ensuring security is vital, an attack-prone system can lead to major problems exemplified by the Johnson Controls ransomware attack on September 2023, causing 27Tb data theft with expenses exceeding $27 million.

2. POTENTIAL THREATS

Some of the potential threats this system could face include:

(1) Denial of Service (DoS) attacks such as DNS floods & Distributed Denial-of-Service (DDoS) attacks such as Ping floods, causing service disruption,
(2) Man in the Middle (MitM) attacks such as ARP spoofing, leading to unauthorised access to sensor data and its manipulation,
(3) Replay attacks facilitated by network traffic interception via sniffing, exploiting KNX or BACnet protocol vulnerabilities.

3. POSSIBLE VULNERABILITIES

To assess vulnerabilities, I propose carrying out the following penetration testing in the building:

Use Nmap to:

(a) perform *initial reconnaissance* for live-hosts & open-ports identification,
(b) conduct a *scanning* for target-host-running service identification,
(c) implement *enumeration* for extracting further details on hosts & services,
(d) attempt *exploitation* of identified vulnerabilities with collected information,
(e) perform *further reconnaissance* on the breached system for inspecting data-steal & privilege-escalation attempts.

Use Wireshark during the stages stated above ensuring to:

- Capture & analyse network traffic,
- Analyse network packets,
- Detect potential flaws, unusual behaviour, any data-exfiltration or privilege-escalation attempts.

To conclude the test, compile a report outlining discoveries, vulnerabilities, and suggested measures, alongside in-depth analysis derived from Nmap scans and Wireshark captures.

4. PRECAUTIONARY ACTIONS

The precautionary actions I offer are to:

- Enable strong encryption & authentication for communication between sensors, controllers, and the building management system by using strong cryptographic protocols,
- Guard building well physically to stop tampering,
- Update cryptographic protocols & keys frequently,
- Implement network segmentation for isolating critical systems from sensors.

5. ASSESSMENT REVIEW

This report identifies and addresses some threats; however, to comply with the specification limitations, only three were listed. Nmap and Wireshark are useful tools for testing sensor vulnerabilities, but they cannot detect physical vulnerabilities, or insider threats.

Word Count for Case Study 1: 437 words

CASE STUDY 2:

CYBERSECURITY RISK ASSESSMENT OF Y UNIVERSITY'S SENSOR SERVER

The purpose of this report is to identify and diagnose some cybersecurity threats concerning the deployment of a web server for Y University's sensor management, and to propose some possible precautionary actions. As a white hat hacker, I ensure properly conducting the security analysis by working in compliance with the following methodology: (1) identify the system properties, (2) diagnose potential threats, (3) assess possible vulnerabilities, (4) provide precautionary actions, and (5) review this assessment.

1. SYSTEM PROPERTIES

University Y has deployed a Web server for sensor management, allowing users to register new sensors and monitor the existing ones. The server is hosted as a virtual machine within the Azure infrastructure managed by the University, limiting access to machines within the local University network. Operating on an Ubuntu platform, the server utilizes Apache 2 as its web server and runs a MySQL database managed by PHP scripts for data interaction.

Guaranteeing the security of this system is of utmost importance, an attack-susceptible system can cause serious problems. An attack type this system is prone to called cross-site scripting, for instance, resulted in a £183 million fine to be paid by the British Airways in 2019.

2. POTENTIAL THREATS

Some of the potential threats this system could face include:

(1) Cross-site scripting (XSS) attack by injecting malicious payloads, resulting in attacks such as session hijacking or data theft when executed by victim,
(2) Classic SQL injection by directly injecting malicious SQL code into user-supplied input fields,
(3) Remote Code Execution (RCE) attack by injecting malicious PHP code or uploading disguised PHP files.

3. POSSIBLE VULNERABILITIES

To assess vulnerabilities, I propose carrying out the following penetration testing in the building:

(a) Use OWASP ZAP's passive and active scanner & Burp Suite's Spider and Scanner tool to identify vulnerable input fields, forms, parameters, and check for the abovementioned threats,
(b) Exploit the vulnerabilities by injecting malicious payloads, SQL queries, and PHP code and uploading disguised PHP files.

To conclude the test, compile a report outlining discoveries, vulnerabilities, and suggested measures, alongside in-depth analysis derived from OWASP ZAP and Burp Suite scans.

4. PRECAUTIONARY ACTIONS

The precautionary actions I offer are to:

- Implement strict input, file upload validation & sanitisation techniques and whitelisting approaches,
- Utilise parameterised queries or prepared statements in MySQL,
- Employ strong encryption mechanisms, multi-factor authentication, etc.

5. ASSESSMENT REVIEW

This report identifies and addresses some threats; however, to comply with the specification limitations, only three were listed. OWASP ZAP and Burp Suite are useful tools for scanning vulnerabilities, but they fall short on advanced-attack detection and may produce false positives.

Word Count for Case Study 2: 436 words

REFERENCES

1. Y. Mo and B. Sinopoli, “Secure control against replay attacks,” 2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2009, pp. 911-918, doi: 10.1109/ALLERTON.2009.5394956. keywords: {Control systems;Computer crime;Communication system control;Robust control;Steady-state;Detectors;National security;Detection algorithms;Video recording;Aerodynamics}.
2. Mirkovic, J. and Reiher, P., 2004. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, *34*(2), pp.39-53.
3. Küppers, M., Schuba, M., Neugebauer, G., Höner, T. and Hack, S., 2023, August. Security analysis of the KNX smart building protocol. In *Proceedings of the 18th International Conference on Availability, Reliability and Security* (pp. 1-7).
4. Kaur, J., Tonejc, J., Wendzel, S. and Meier, M., 2015. Securing BACnet’s pitfalls. In *ICT Systems Security and Privacy Protection: 30th IFIP TC 11 International Conference, SEC 2015, Hamburg, Germany, May 26-28, 2015, Proceedings 30* (pp. 616-629). Springer International Publishing.
5. Fatemifar, S., Arashloo, S.R., Awais, M. and Kittler, J., 2019, May. Spoofing attack detection by anomaly detection. In *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 8464-8468). IEEE.
6. Kapko, M. (2024) *Johnson Controls reports $27m hit from Ransomware attack*, *Facilities Dive*. Available at: https://www.facilitiesdive.com/news/johnson-controls-ransomware-cyber-attack/706325/.
7. Froehlich, A. (2023) *Security breach at Johnson Controls highlights smart building supply chain concerns*, *Security Info Watch*. Available at: https://www.securityinfowatch.com/cybersecurity/article/53078295/security-breach-at-johnson-controls-highlights-smart-building-supply-chain-concerns.
8. *British Airways faces record £183m fine for Data Breach* (2019) *BBC News*. Available at: https://www.bbc.com/news/business-48905907.
9. Jaipur, W. (2023) *What is the advantage and disadvantage of nmap?*, *Blog*. Available at: https://techfygeeks.wixsite.com/blog/post/what-is-the-advantage-and-disadvantage-of-nmap.
10. Network Security (2023) *What are the benefits and challenges of using wireshark for network traffic analysis?*, *Wireshark: Benefits and Challenges for Network Analysis*. Available at: https://www.linkedin.com/advice/1/what-benefits-challenges-using-wireshark-network.
11. Homola, I. (2023) *OWASP ZAP: 8 core features (pros & cons)*, *Codiga*. Available at: https://www.codiga.io/blog/owasp-zap/.
12. Network Security (2024) *What are the advantages of using BURP suite for web application penetration testing?*, *How Burp Suite Can Help You With Web Application Penetration Testing*. Available at: https://www.linkedin.com/advice/1/what-advantages-using-burp-suite-web-application-yakbe.
13. Tidmarsh, D. (2023) *Man-in-the-middle attack (MITM): Definition, types, & prevention methods*, *Cybersecurity Exchange*. Available at: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/man-in-the-middle-attack-mitm/.