Vulnerability Audit and Assessment - Baseline Analysis and Plan
Word count: 599

Table of Contents Page

Vulnerability Audit and Assessment - Baseline Analysis and Plan

1 Purpose Of Assessment

Identify potential vulnerabilities - Identifying these vulnerabilities will provide an opportunity for improving the applications security (Kritikos et al. 2019)

2 Method and evaluation

Scope

Remote analysis with automated vulnerability scanning and manual command line scanning

Objectives of the audit

Detect vulnerabilities and respond with mitigation recommendations

This Baseline analysis and plan will be created from intel gained via the reconnaissance phase of the lockheed martin cyber kill chain.

Reason for using the kill chain format

According to Hutchins et al. (2011), the kill chain becomes a model for actionable intelligence. By following the seven phases, this assessment will replicate the path taken by adversaries.

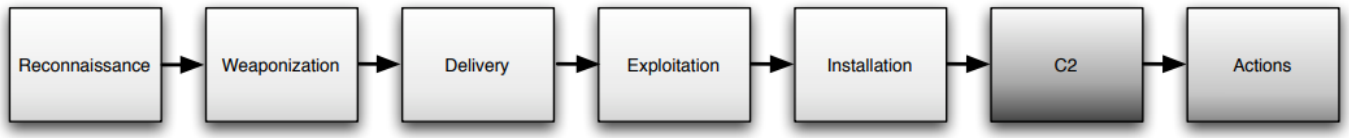

Fig1. Lockheed Martin Cyber Kill Chain.

Out of scope

- Not a penetration test
- Emphasis on network security

Stakeholder buy-in

- Yes

3 Selection of tools

Tools and Justification

The selected tools and terminal commands which have been chosen for this assessment along with a brief justification are located in Fig2 and Fig3, below.

ZAP and Nessus have been chosen as the vulnerability scanning tools due to the ability to discover vulnerable areas of an application (Kritikos et al. 2019).

Network Vulnerability Tools/Commands	Justification
OWASP ZAP	To crawl the website for web application vulnerabilities
Nessus	To discover application and system vulnerabilities
Builtwith	Gain a detailed overview of the website technology profile
whatweb	Discover the technology stack, server, languages, versions used.
Traceroute	To observe the hops (Routers/IPs) of ICMP between us and allthegear.org.uk
MTR	Test for packet loss and if a rate limit has been implemented
DIG	Check DNS information ,axfr for zone transfer configuration and MX
WHOIS	Collect Registrar and server hosting details
DNSDumpster	For linked host discovery and visual mapping to identify weak areas

Fig2. Tools and commands for allthegear.org.uk assessment

Scanning Accuracy of ZAP Proxy (Kritikos et al. 2019:16)

Vulnerability area	ZAP Proxy Full_Remote Scanning Accuracy
Cross-Site Scripting	55.69%
Insecure cookie	55.56%
Path Traversal	11.28%
SQL Injection	49.63%

Fig3. Justification for using ZAP and Nessus as a cross reference

Challenges of the Tools

According to Kritikos et al. (2019), ZAPProxy in full_remote scan mode produced a 15.65% accuracy assessment for plugins due to false negatives but has a median vulnerability coverage of 51.51%, see Fig4 below.

For this reason, Nessus will also be used for cross-referencing results.

Scanning Time And Accuracy Benchmark (Kritikos et al. 2019:15)

Tool	Operation mode	Accuracy	Time	Comments
ZAP Proxy	Full_Remote	15.65%	12 Minutes	Remote scanning with all vulnerability scanning plugins. Reached 48% progress and then the benchmark app went down. Bad accuracy is due to many false negatives.

Fig4. Example of the challenge of the tool ZAP

4 Business impacts on use of tools

Potential impacts

- Inform them that their systems could detect a DOS attack during the assessment.
- Webstore interruptions due to assessment scanning

Preparations and mitigations prior to scanning

- Could run a small scan prior to the full scan to check the effect.
- The team should backup and test all systems and files prior to the vulnerability scanning commencing (NCSC, 2021).
- The scanning should take place at a time when the store has the least visitors and with low aggression to minimize disruption.

5 Plan of vulnerability checking

Reconnaissance Phase

In the recon phase, this assessment will use a four step process as illustrated in Fig5: The findings will then be presented with most critical as a priority.

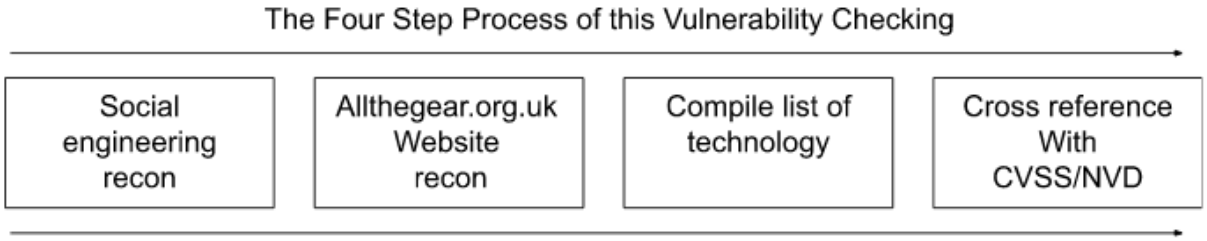

Fig5. The four step process during the reconnaissance phase

1. Social Engineering Recon For Personal Information Discovery
    A. Human assets
        - Employees/Contractors
        - Passwords
        - Usernames
        - Forms of authentication

2. Website Recon To Discover:
    A. Web assets (Website Recon)
        - Type and version of Operating System
        - Hosting provider
        - Ip address and sub-domains
        - Middleware
    B. Physical assets
        - Check for IDS/IPS (WAF) and configurations
    C. Document and analyze data of the website and its components
        - Web traffic analysis
    D. Performance monitoring
        - Latency
    E. Content analysis
        - Content of website
        - Structure of website
        - Types of media used
    F. Dependency analysis
        - Third-party
        - Libraries
        - Plugins
        - APIs

3. Compile List of Technology
    A. The Technology Profile Behind The Website
        - Frameworks and versions
        - SSL Certificates
        - Email Hosting
        - DNS
        - Servers and versions
        - Payment systems

4. Cross Reference And Compile A List With CVSS/NVD
    A. Identify known vulnerabilities and severity
        - Against website
        - Against components

Timeline

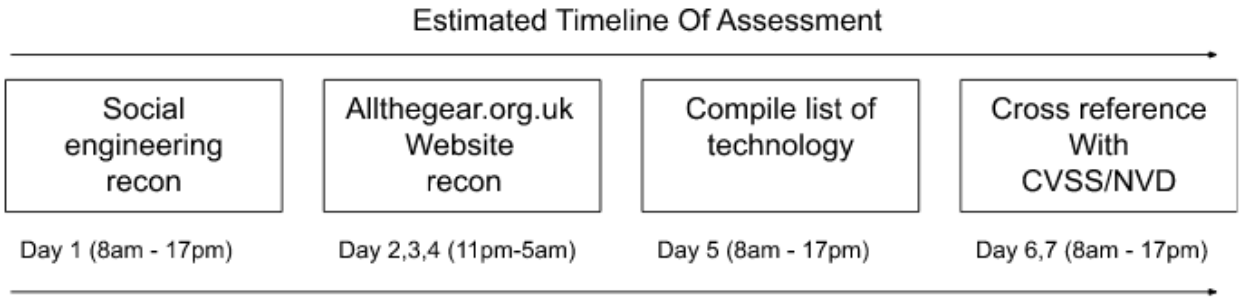

Fig6. Reconnaissance timeline and plan

6 List of Standards recommended for business

A. Standards
    - ISO27001
    - OWASP ASVS (OWASP, 2021)
    - NVD

B. Compliance
    - GDPR (Consult a DPO)
    - PCI-DSS (Consult a QSA to determine the company's specific PCI DSS compliance obligations)

7 Summary Of Limitations And Assumptions

1. Using multiple tools should reduce missed vulnerabilities
2. Due to passive scanning mode, The OWASPS ZAP results may not discover login pages.
3. False positives will need to be manually excluded
4. Limitations due to shared hosting

8 References

Hutchins, E. et al (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. Available from: http://gauss.ececs.uc.edu/Project4/Documents/kill-chain.pdf [Accessed on 10th February 2023]

Kritikos, K., Magoutis, K., Papoutsakis, M. and Ioannidis, S., 2019. A survey on vulnerability assessment tools and databases for cloud-based web applications. *Array*, *3*, p.100011

Moore, P & Householder, A (2019) Multi-Method Modeling and Analysis of the Cybersecurity Vulnerability Management Ecosystem. SEI. Available from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=550431 [Accessed on 9th February 2023]

NCSC (2021) Cyber Essentials: Requirements for IT infrastructure. Available from: https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-3-0.pdf

OWASP (2021) ASVS: Application Security Verification Standard.Available from: https://owasp.org/www-project-application-security-verification-standard/ [Accessed on 12th February 2023]