University of Essex Online

Development Team Project

by

(*Kikelomo Obayemi, Suresh Melvin Sigera, Japhet Ndhlovu)*

Proposal for Penetration Test on TEAM A's Website

1. BACKGROUND

Team A runs an e-commerce website that provides payment services and advice for commercial website operators. E-commerce solutions present a modern and convenient way to get goods and services to consumers online however there are concerns around privacy and security of information and assets (Niranjanamurthy et al., 2013). As with e-commerce businesses, Team A's website faces a variety of security risks which is discussed in the next section.

2. SECURITY CHALLENGES

2.1 Web applications

When web-based projects are created without adequate focus on security, it could lead to loss of assets, exposure of sensitive information and partial or complete disruption of services (Bach-Nutman, 2021). The most critical web application security risks according to OWASP (2021) are:

- Injection
- Broken Authentication
- Sensitive Data Exposure
- XML External Entities (XXE)
- Broken Access Control

- Security Misconfiguration
- Cross site Scripting (XXS)
- Insecure Deserialization
- Using components with Known Vulnerabilities
- Insufficient Logging and Monitoring

2.2 E-commerce Businesses

There has been a significant increase in global e-commerce sales from 2014 till date. A recent study released by Statista shows sales in 2020 was 4.28 trillion US dollars (a 28% increase from 2019) and is projected to rise to 6.388 trillion US dollars by the year 2024 (Statista, 2021).

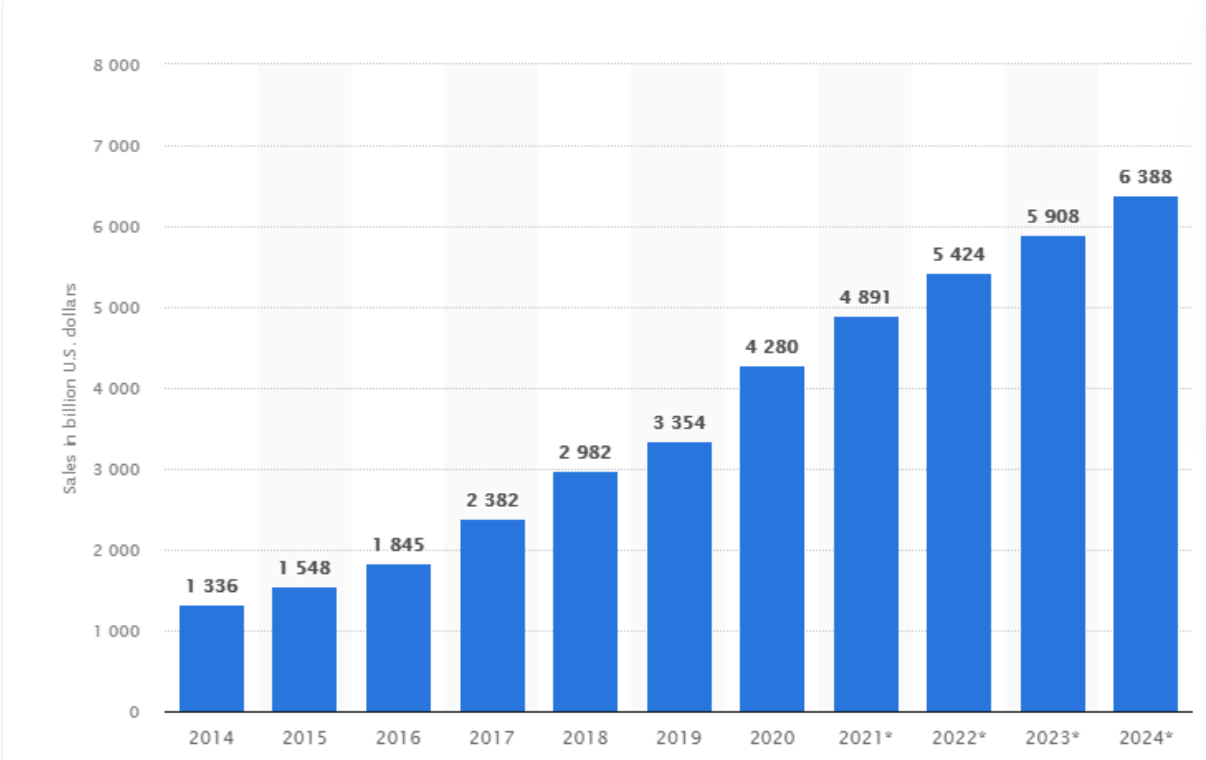


Fig 1: E-commerce sales from 2014 to 2024 (in billion US dollars) (Statista, 2021)

However, as more sales move online, cyber-attacks are also increasing making it difficult for e-commerce companies to tackle privacy and security issues (Hlova, 2021). Lukic (2020) in a GlobalTrade Magazine article states that e-commerce companies face millions of attacks per year from cyber criminals. Sift (2021), a payment fraud solutions company reported that as e-commerce traffic surged in the year 2020, the value of fraudulent purchases rose by over 69%. To minimise the impact of cyber attacks to its business and customers, e-commerce companies must be equipped to deal with a range of threats (Hightower, 2021). The first step to securing a business is **Penetration Testing** (Martin, 2017).

3. METHODOLOGY

Denis et al., (2016) defines penetration testing (also known as pen test) as

"a simulation of an attack to verify the security of a system or environment to be analysed".

The benefits of penetration testing according to Al Shebli & Behesti (2018) include:

- helping an organisation to evaluate its IT security posture against vulnerabilities and threats.
- helping to identify security weaknesses and spurring an organisation towards taking proactive steps in safeguarding its system.
- helping to evaluate the effectiveness of an organisation's IT policies and processes.
- creating awareness and closing knowledge gaps of employees.

- most importantly, helping to minimise financial and information loss which could lead to reputational damage and cause customers to lose trust in the company.

There are a number of known methodologies that could be used to conduct penetration testing. The top 5 according to Vumetric (2021) are: Open Source Secure Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP), National Institute of Standards and Technology (NIST), Penetration Testing Execution Standard (PTES) and Information Systems Security Assessment Framework (ISSAF). Our chosen methodology for the proposed pen test is the Penetration Testing Execution Standard (PTES).

3.1 Penetration Testing Execution Standard (PTES)

The PTES has been chosen because of its structured approach to pen testing. It consists of seven clearly defined stages as shown in the diagram below.

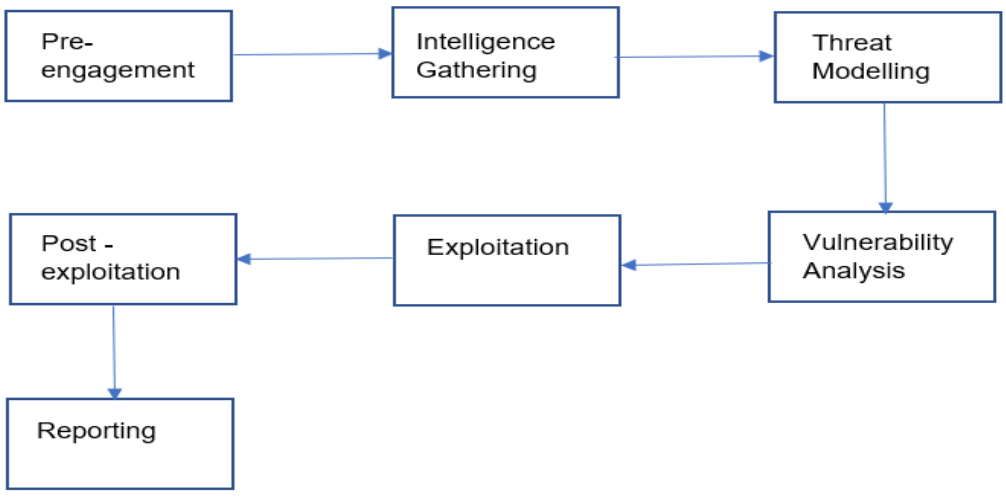


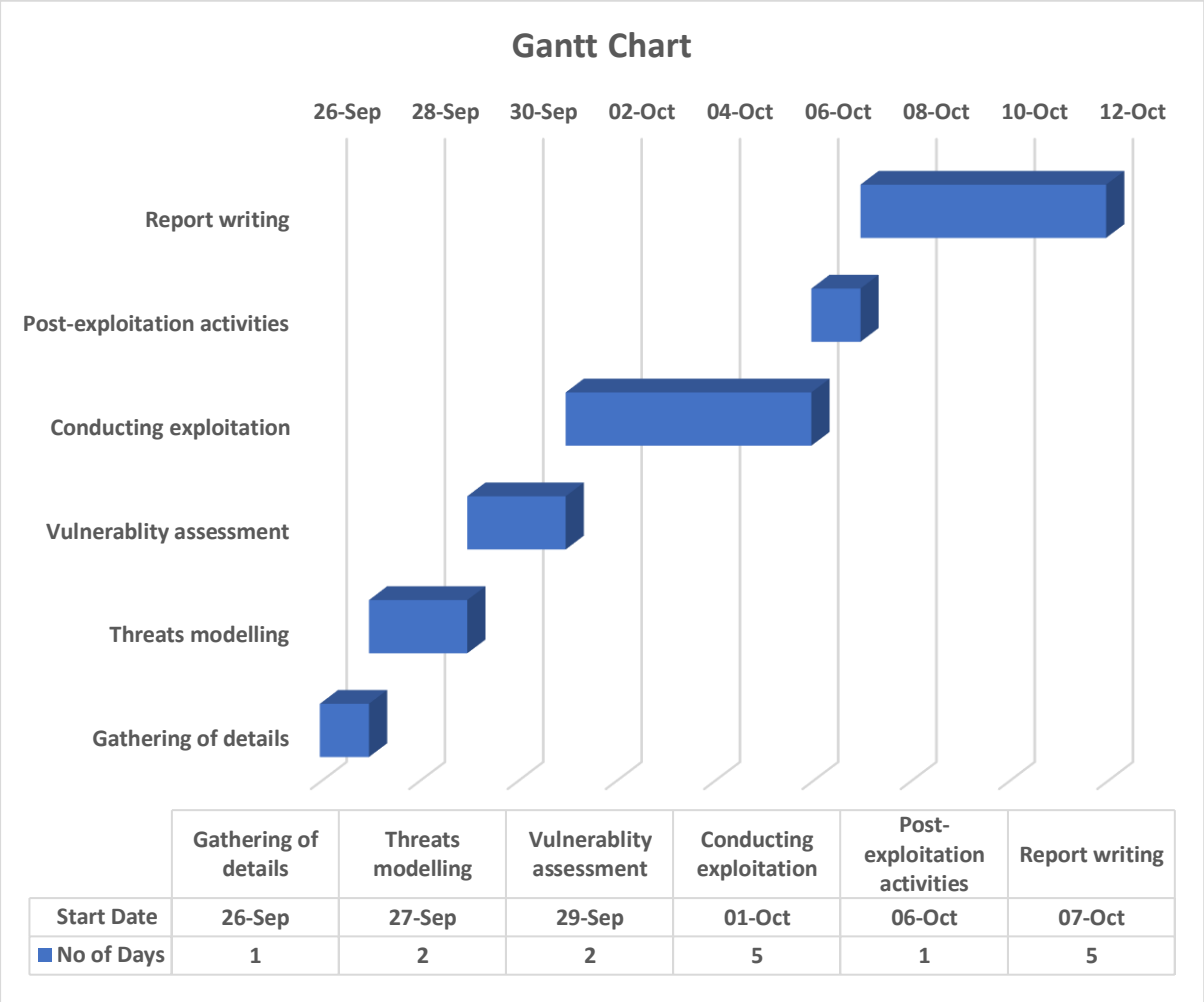
Fig 2: The seven stages of the PTES (Dinis and Serrão, 2014)

3.2 Scope of Work

Figure 2 above provides an overview of the scope of work for this pen test. The main aspects have been further outlined below:

1. Intelligence gathering: getting familiar with Team A's organisation to determine details that could be utilised.
2. Threats modelling: identification and classification of threats
3. Vulnerability assessment: determining the associated risk level of threats identified.
4. Exploitation: various attacks will be simulated on Team A's system
5. Post-Exploitation: housekeeping activities
6. Executive Report which includes:
    - Details of security vulnerabilities discovered.
    - A summary of recommendations and possible mitigations for identified risks.
    - Applicable standards and guidelines for the e-commerce industry.

3.2.1 Project Timeline



	Gathering of details	Threats modelling	Vulnerablity assessment	Conducting exploitation	Post-exploitation activities	Report writing
Start Date	26-Sep	27-Sep	29-Sep	01-Oct	06-Oct	07-Oct
No of Days	1	2	2	5	1	5

Total number of days for Project Completion: 16 days

4. TOOLS

The table below shows a list of tools that will be used for the penetration test:

Tool	Reason
Nmap	Nmap will be used for network scanning. It can help to detect available hosts on the network, services they

	are running and scan for open ports (Networkworld, 2018). Open ports can provide a pathway for attackers to access applications that are listening on those ports (LIFARS, 2020)
Metasploit	It has a framework that allows for exploitation of a wide range of vulnerabilities (Rapid7, n.d) including those already considered in Section 2.
OWASP ZAP (Zed Attack Proxy)	This will be used to discover security vulnerabilities in web applications such as the OWASP top 10.
Kali Linux	Kali linux is an advanced penetration testing tool with a suite of over 600 tools (Kali, n.d). Kali Linux has been chosen for any other security risk not initially considered but discovered during the pen test.
Others	Use of Basic Network troubleshooting commands such as ping, netstat, whois, traceroute, dig, nslookup

5. BUSINESS IMPACT

According to SearchSecurity, (n.d.), some common impacts of pen testing to the business include:

- Complications with Availability (DoS): Certain penetration activities, such as automated scanning may cause disruptions, more so on legacy systems. This could be managed via a planned schedule and prior communication to affected users (Vumetric, 2021).

- Possibility of filling the database with junk data that can be difficult to clean after penetration testing.

6. LIMITATION(S) AND ASSUMPTION(S)

6.1 Limitation

Time: penetration assessment is usually carried out within a defined period. The testing team has a specified duration to establish risks and vulnerabilities and generate results as a report. In contrast, attackers have substantial time to determine and probe more vulnerabilities. Hence, timed penetration tests gives the attacker an advantage over the tester as the attacker has more time to capitalize on the vulnerabilities (cypress data defense, n.d.).

6.2 Assumption

Team A's staff are adequately trained on social engineering activities and are unlikely to fall victim to phishing attacks therefore this test will not focus on phishing.

REFERENCES

Al Shebli, H.M.Z. and Beheshti, B.D. (2018), May. A study on penetration testing process and tools. *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 4 May* 2018 Farmingdale, NY, USA:1-7. DOI: 10.1109/LISAT.2018.8378035

Bach-Nutman, M., 2020. Understanding The Top 10 OWASP Vulnerabilities. Available from: https://arxiv.org/ftp/arxiv/papers/2012/2012.09960.pdf [Accessed 15 August 2021]

Cypress data defense (n.d.). Major Limitations of Penetration Testing You Need to Know. [online] Available at: https://www.cypressdatadefense.com/blog/limitations-of-penetration-testing/. [Accessed 18 September 2021]

Denis, M., Zena, C. and Hayajneh, T., (2016) Penetration testing: Concepts, attack methods, and defense strategies. *IEEE Long Island Systems, Applications and Technology Conference (LISAT) 29* April. 2016 Farmingdale, NY, USA:1-6. DOI:10.1109/LISAT.2016.7494156

Dinis, B. and Serrão, C. (2014). Using PTES and open-source tools as a way to conduct external footprinting security assessments for intelligence gathering. Using PTES and open-source tools as a way to conduct external footprinting security assessments for intelligence gathering, (3-4):271-279.

Hightower S.S (2021) The economic impact of data security breaches in e-commerce Available from: https://enterprise.verizon.com/resources/articles/s/economic-impact-of-data-security-breaches-in-ecommerce/ [Accessed 31 August 2021]

Hlova M. (2020) Six types of Security vulnerabilities in e-commerce and how to solve them Available from:https://www.n-ix.com/6-types-security-vulnerabilities-ecommerce-solve-them/ [Accessed 31 August 2021]

Kali (n.d) Kali. Available from: https://www.kali.org/#kali-highlights [Accessed 14 September 2021]

LIFARS (2020) Are open ports a security risk? Available from: https://lifars.com/2020/10/are-open-ports-a-security-risk/ [Accessed 14 September 2021]

Lukic D. (2020) E-commerce and Data Breaching: The Next Cyberthreat. *Global Trade Magazine* Available from: https://www.globaltrademag.com/e-commerce-and-data-breaching-the-next-cyberthreat/ [Accessed 1 Sept 2021]

Martin C. (2017) Why a Penetration Test is the First Step to Securing Your Business Available from: https://www.linkedin.com/pulse/first-step-toward-effective-info-security-cody-martin [Accessed 15 Sept 2021]

Networkworld (2018) What is Nmap? Why you need this network mapper. Available from: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html [Accessed 14 Sept 2021]

Niranjanamurthy, M., Kavyashree, N., Jagannath, S. and Chahar, D. (2013). Analysis of e-commerce and m-commerce: advantages, limitations and security issues. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(6):2360-2370.

OWASP (2021) OWASP Top 10 Available from: https://owasp.org/www-project-top-ten/ [Accessed 15 August 2021]

Rapid7 (n.d) Metasploit Framework. Available from: https://docs.rapid7.com/metasploit/msf-overview/ [Accessed 14 September 2021]

RSI Security (2018) The importance of having a web application vulnerability plan Available from: https://blog.rsisecurity.com/the-importance-of-having-a-web-application-vulnerability-management-plan/ [Accessed 31 August 2021]

SearchSecurity. (n.d.). Testing applications in production vs. non-production benefits. Available from: https://searchsecurity.techtarget.com/tip/Testing-applications-in-production-vs-non-production-benefits [Accessed 13 Sep. 2021].

Sift (2021) Exposing the Multi billion Dollar Fraud Economy *Q1 2021:Safety Index* Available from: https://pages.sift.com/rs/526-PCC-974/images/ebook-Q1-2021-Digital-Trust-Safety-Index-Exposing-Fraud-Economy.pdf [Accessed 31 August 2021]

Statista (2021) Available from: Retail e-commerce sales worldwide from 2014 to 2024 https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/ [Accessed 31 August 2021]

Vumetric (2021) Top 5 Penetration Testing Methodologies and Standards Available from: https://www.vumetric.com/blog/top-penetration-testing-methodologies/ [Accessed 12 September 2021]