Hochschule Worms

Fachbereich Informatik

Studiengang Angewandte Informatik B.Sc.

Provisorisch: Penetration Testing im Rahmen von Webanwendung

Dokumentation des Praxissemesters bei der Firma

WALLSEC

Bruno Macedo da Silva
676839
inf3645@hs-worms.de
Bebelstraße 22 Z18
67549 Worms

Betreuer	Prof. Dr. Zdravko Bozakov Peter Todorov
Bearbeitungszeitraum:	Summer Semester 2022
Abgabedatum:	xxx. XXXXXX XXXX
Sperrvermerk:	Ja/Nein

Inhaltsverzeichnis

Glossar

Confidentiality, Integrity and Availability (CIA) Beschreibt die drei wichtigsten Schutzziele der IT-Sicherheit, und zwar Vertraulichkeit, Integrität und Verfügbarkeit Wendzel (2018) .

Common Vulnerability Scoring System (CVSS) Internationale Standards für die Bewertung von Verwundbarkeiten von IT-Systemen. Es wurde im Jahr 2005 von dem National Infrastructure Advisory Councils entstanden und ist heute von dem Forum of Incident Response and Security Teams verwaltet Security Insider (2019) .

National Institute of Standards and Technology (NIST) USA-Behörden dafür zuständig, Reglungen im Bereich Informationstechnologie zu vereinheitlichen und voranzutreiben Hochschule Worms (2018) .

Open-source intelligence (OSINT) Datenerhebung und Sammlung aus offenen Quellen, wie von Online-Repositories, Nachrichten, sozialen Netzwerken, wissenschaftliche Texten unter anderen öffentlichen Quellen. In diesem Fall gibt es keine direkte Kontakte mit dem Ziel. Es kann passive Reconnaissance genannt werden Yeboah-Ofori (2018).

Rules of Engagement (ROE) Bezieht sich auf ein vertragliches Dokument, der zwischen Kunden und Tester geschlossen wird, um den Umfang und die Rahmenbedingungen des Testes festzulegen. In diesem Dokument steht under anderen folgenden Informationen: Umgang mit sensitiven Daten, Notfallkontakten, Identifikation der zu testenden Objekten und Einschränkungen des Testobjekte Triaxiom Security (2018).

Cyberangriff Angriffe, die über den Cyberspace stattfinden. Solche Angriffe zielen Unternehmen und deren Infrastrukturen, um sie zu zerstören, sie zu lähmen, sie zu

kontrollieren oder die Integrität deren Daten zu stehlen oder zu dominieren National Institute of Standards and Technology (2020).

Cybersicherheit Dieser Domäne umfasst Kenntnisse und Methode für den Schutz, für die Prävention, für die Wiederherstellung von elektronischen Kommunikationsmittel und dessen Inhalt. Es konzentriert sich in ihrer Verfügbarkeit, Integrität, Authentizität, Vertraulichkeit und Verbindlichkeit National Institute of Standards and Technology (2020).

Schwachstelle Schwäche eines Systems Wendzel (2018).

Verwundbarkeit Oder als *vulnerability* gekannt. Es beschreibt eine von Angreifer ausnutzbare Schwachstelle Wendzel (2018).

Abkürzungen

CIA Confidentiality, Integrity and Availability.

CVSS Common Vulnerability Scoring System.

FPO Fachspezifische Prüfungsordnung.

NIST National Institute of Standards and Technology.

OSINT Open-source intelligence.

ROE Rules of Engagement.

1 Einleitung

Mein Praxissemester findet im Rahmen der Fachspezifische Prüfungsordnung (FPO) 2008 für den Studiengang Angewandte Informatik B.Sc. und dessen Modulhandbuch Hochschule Worms (2018). Die Stellensuche orientierte sich auf dem Schwerpunkt Networks & Security und spezifischer auf Cybersicherheit und Penetrations Testing.

Da es sich um einen spezifischen Bereich geht, war die Suche auf wenigen Firmen eingeschränkt, wo ich meine Bewerbungsunterlagen schickte. Die Firma Wallsec GmbH in Wiesloch-Walldorf hatte eine offene Stelle für Student, die meiner Suche entspricht. Die Aufgabe in der Stellenbeschreibung ging hauptsächlich Durchführung von Penetrationstests, Source-Code-Analyse, Dokumentation, Evaluation und Entwicklung von Sicherheitsprozessen. Als Voraussetzung verlangte Wallsec zwar wenig Fachkenntnis im Bereich Sicherheit und Penetration Testing, aber wollte große Interesse von den Kandidaten für das Lernen Wallsec Security (2022).

Das Bewerbungs- bis zum Einstiegsverfahren dauert ungefähr einen Monat. Am 15ten Juli 2022 fing ich an bei Wallsec als Praktikant im Vollzeit zu arbeiten. In diesem Bericht werden wir folgenden Themen bearbeiten:

- Informationen über die Wallsec
- Konzepte von Penetration Testing
- Aufgabebereich der Tätigkeit
- Ergebnis des Praxissemesters

1.1 Wallsec

Die Firma wurde im Jahr 2020 von Peter Todorov in Walldorf-Wiesloch, Baden Württemberg, gegründet. Laut der Beschreibung der Webseite fokussierte sie auf die Planung,

Bereitstellung und Risikoanalysen von Sicherheits-Infrastrukturen von Firmen verschiedenen Größen Wallsec Security (2022). Wallsec bietet folgenden Leistungen an:

- Penetrationstests
- Schwachstellenmanagement
- Richtlinien
- Automatisierung
- DevOps und CI/CD Pipeline Sicherheit
- Beratung im Bereich Cyberabwehr

2 Anwendungsdomäne

Oft bekommen wir Nachrichten über Firmen oder Regierungen, deren Geheimnis im Netz von Angreifer veröffentlicht wurden oder deren Diensten wegen Cyberangriff unerreichbar sind. Da solche Situationen öfter als je vorgekommen sind, ist das Interesse und die Forschung in dem Bereich Cybersicherheit in den letzten zehn Jahr rasant gestiegen Openvpn (2022).

Solche Situationen verletzen die drei wichtigsten Ziele der Cybersicherheit, und zwar die Vertraulichkeit, die Integrität und die Verfügbarkeit (aus dem Englisch Confidentiality, Integrity and Availability (CIA)) . Diese Zielen bekommen in den Fachliteraturen folgenden Beschreibungen: Schutz gegen unautorisierte Informationsgewinnung; Schutz gegen unautorisierte Datenmanipulation und Zugriffsgewährleistung für authentifizierte und autorisierte Subjekten Wendzel (2018). Ein Angriff zielt Schwachstelle oder Verwundbarkeit eines Systems. Diese wird dann zu einer Bedrohung, wenn es möglich ist, dieses System auszunutzen.

2.1 Theorie über Penetration Testing

Eine heutzutage sehr verwendete Methode, um Verwundbarkeit zu finden und zu analysieren ist durch Schwachstellenanalyse und Penetrations Testing. Der National Institute of Standards and Technology (NIST) beschreibt das erste als systematische Analyse eines Systems oder Produktes in Bezug auf ihrer Sicherheit, um dessen Schwachstelle zu finden; und das zweite als Methode für die Verifizierung von binärischen Komponenten oder Anwendungen im Ganzen, um zu finden, ob dessen Verwundbarkeiten in Bezug auf ihre Daten oder Resources ausnutzbare sind National Institute of Standards and Technology (2020). Man kann auch sagen, dass es bei der Schwachstellenanalyse eine Datenerhebung stattfindet, die später in der Penetration Testing in eine autorisierte Weise ausgenutzt wirdGoel and Mehtre (2015). Das Ergebnis dieser zwei Prozessen werden später dem

Beauftragter bekanntgemacht, damit Sicherheitsmaßnahmen genommen werden können.

Der Begriff ist auch als "Red Teaming", als "Ethikal Hacking", als "Pentest" oder als "white hats (weiße Huts)" bekannt. Es umfasst spezifische Analyse von Drohungen und von Verwundbarkeiten eines Produktes und es findet im Rahmen einen Vertrag oder ROE zwischen einen Kunde und die Firma oder Person statt, die für die Tests verantwortlich sind Bishop (2007).

2.2 Phase und Methodologie eines Penetration Testing

Ein Penetration Testing findet in einer systematischen Reihenfolge mit drei Hauptphasen: Vorbereitung, Implementation und Analysis Shebli and Beheshti (2018). Während der Vorbereitung werden der Umfang, die Ziele und due Dauer definiert. Bei der Implementation wird das System oder das Produkt in ihren Aufbau erkannt, analysiert und ausgenutzt (*exploited*). In der letzten Phase werden die gefundenen Verwundbarkeiten sämtliche Lösungsvorschlägen dem Beauftragter mitgeteilt. In manche Fälle kann das getestete Objekt bezüglich seiner Sicherheit mithilfe der Common Vulnerability Scoring System (CVSS) bewertet werden. Diese Punktmechanismus stellt eine internationale anerkannte Evaluation eines Objekts dar.

Es gibt drei bekannte Methodologie, wo ein Penetration Testing stattfindet, und zwar *white box*, *black box* oder *zero-knowledge* und *grey box*. In der ersten Methodologie bekommen die Tester ausführliche Informationen über das getestet Objekt, wie Quellcode, interne Logik und Struktur. In der zweiten haben die Tester nur Open-source intelligence (OSINT) Informationen. Die dritte Variante ist eine Mischung aus den ersten zwei, in diesem Fall bekommen die Tester beschränkte Informationen über das zu testende Objekt andFarmeena Khan (2012).

2.3 Tools

Es gibt verschiedene Tools, die dazu beitragen ein Objekt in seinem Verwundbarkeit zu erkennen (Reconnaissance) und auszunutzen. Hier beschreiben wir die meisten bekannten und verwendet. Zuerst sprechen wir die Reconnaissance-Tools anschließen erklären wir über *exploit-tools*.

jetzt hier über burp, dirbuster, hydra, nmap, metasploit schreiben.

2.4 Penetration Testing im Webanwendungen

3 Durchführung der Aufgabe

- Definition von Projekte
- Quantitative Daten
  - Umfang
  - Frist
  - Anzahl von Teilnehmer
- Durchführung
- Bericht
- Schlussbericht
- Tabelle mit konkreten Beispiele

4 Fazit

- Was wurde gelernt?
- Wie wichtig war das Praxissemester für meinen beruflichen Laufbahn?
- Perspektiven

Literaturverzeichnis

andFarmeena Khan, M. E. (2012). A comparative study of white box, black box and grey box testing techniques. *International Journal of Advanced Computer Science and Applications*, 3.
http://dx.doi.org/10.14569/IJACSA.2012.030603. Zugriff am 31 Juni 2022.

Bishop, M. (2007). About penetration testing. *IEEE Security & Privacy*, 5(6):84–87.

Goel, J. N. and Mehtre, B. (2015). Vulnerability assessment & penetration testing as a cyber defence technology. *Procedia Computer Science*, 57:710–715.
https://www.sciencedirect.com/science/article/pii/S1877050915019870/. Zugriff am 31 Juni 2022.

Healthcare Computing (2021). Was ist bzw. tut das national institute of standards and technology (nist)?
https://www.healthcare-computing.de/was-ist-bzw-tut-das-national-institute-of-standards-and-technology-nist-a-1022210/. Zugriff am 31 Juni 2022.

Hochschule Worms (2018). Fachspezifische prüfungsordnung (fpo 2018).
https://www.hs-worms.de/fileadmin/media/fachbereiche/informatik/AInf/Pruefungsordnung/AnInf_FPO_2017-12-19_FINAL.pdf. Zugriff am 31 Juni 2022.

National Institute of Standards and Technology (2020). Cyber attacke.
https://csrc.nist.gov/glossary/term/Cyber_Attack. Zugriff am 31 Juni 2022.

Openvpn (2022). How cybersecurity has changed in the last decade.
https://openvpn.net/blog/how-cybersecurity-has-changed-in-the-last-decade/. Zugriff am 31 Juni 2022.

Security Insider (2019). Was ist cvss?
https://www.security-insider.de/was-ist-cvss-a-853465/. Zugriff am 31 Juni 2022.

Shebli, H. M. Z. A. and Beheshti, B. D. (2018). A study on penetration testing process and tools. In *2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pages 1–7.
https://doi.org/10.1109/LISAT.2018.8378035. Zugriff am 31 Juni 2022.

Triaxiom Security (2018). Why are rules of engagement important to my penetration test?
https://www.triaxiomsecurity.com/rules-of-engagement-important-to-penetration-test/. Zugriff am 31 Juni 2022.

Wallsec Security (2022). About us.
https://www.wallsec.de. Zugriff am 31 Juni 2022.

Wendzel, S. (2018). *IT-Sicherheit für TCP/IP- und IoT-Netzwerke*. Springer Vieweg, Wiesbaden.

Wendzel, S. and Plötner, J. (2007). *Praxisbuch Netzwerk-Sicherheit: Risikoanalyse, Me-*

thoden und Umsetzung; für Unix-Linux und Windows; VPN, WLAN, Intrusion Detection, Disaster Recovery, Kryptologie. Galileo Computing, Bonn.

Yeboah-Ofori, A. (2018). Cyber intelligence and osint: Developing mitigation techniques against cybercrime threats on social media. *International Journal of Cyber-Security and Digital Forensics*, 7:87–98.
http://dx.doi.org/10.17781/P002378. Zugriff am 31 Juni 2022.