DEPI Graduation Project Overview

Date: May 10, 2025

Project: SAR-001

Team Members

Name	Title	Contact Information
DEPI Raiders		
Khaled Shaaban	Penetration Tester	kshaaban325@gmail.com
Abdelrahman Tarek	Penetration Tester	Boda.tarek94@gmail.com
Abd Elrhman Emad	Penetration Tester	emadabdelrhman041@gmail.com
Eslam Salem	Penetration Tester	as6295857@gmail.com
Mohamed Ali	Cybersecurity Specialist	mo5665ali@gmail.com
Sandra Adel	Cybersecurity Specialist	sandraaguindy@gmail.com

Project Scenario

The project involves a hypothetical scenario where a company, CodeByte Technologies, requests a Security Assessment against its infrastructure from DEPI Raiders. CodeByte Technologies is a tech company specializing in software engineering.

The agreement involves three main stages; *external penetration testing,* where the testers attempt to break into the network through exploiting the vulnerabilities they detect in CodeByte's public facing infrastructure. In this case, the public facing infrastructure includes six (6) websites. Upon successful completion, the testers begin the *internal penetration testing (Production Environment)* phase, where they attempt to compromise the production environment that is used by CodeByte's developers to complete their projects.

Finally, the third phase starts where the testers attempt a full *active directory network* compromise by gaining full control over CodeByte's domain controller. A SAR (Security Assessment Report) is then drafted and presented to the company.

The SAR includes the following information:

- Assessment Overview
- Assessment Components
- Finding Severity Ratings
- Scope
- Executive Summary
- External Penetration Test
- Internal Penetration Test
- Mitigation Strategies.

Creating the Company Environment

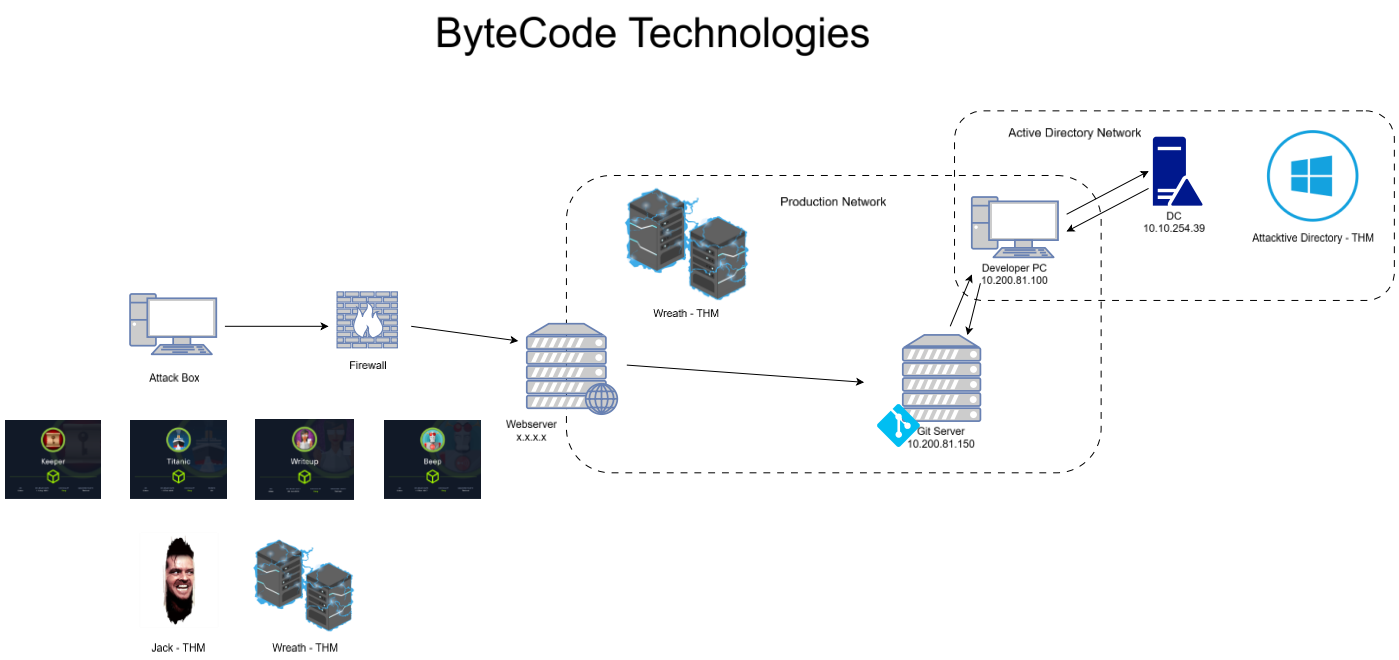
As stated above, CodeByte is a hypothetical company that operates in the software engineering market. In this regard, the team had two options to decide from. The first was to configure a small company's network in-house and conduct a security assessment on that environment, the second was to rely on HackTheBox and TryHackMe platforms to find a sequence of machines and rooms to complete in such a way that it gives off as a company environment.

We went with the latter for one simple reason, *resources*. As a team, deploying a small company network on our in-house resources was not feasible, so using online platforms proved to be the best option.

The boxes/rooms we completed were not randomly chosen, instead they were specifically completed in a certain sequence to mimic a company environment, especially a software engineering company's environment. In total 8 boxes/rooms were completed, ranging from web application exploiting (External Penetration Testing) to internal network and active directory exploitation (Internal Penetration Testing). The table below maps each room completed to its corresponding phase in the security assessment, as well as its relevant exploitations and techniques used.

Box/Room	Platform	Phase	Techniques
Keeper	HackTheBox	External	Thorough Enumeration Old Patching
Titanic	HackTheBox	External	Path Traversal Old Patching
Jack	TryHackMe	External	Old Patching Parameter Tampering Cron Jobs
Writeup	HackTheBox	External	Blind SQL Injection Path Hijacking
Beep	HackTheBox	External	Directory Traversal
Wreath	TryHackMe	External/Internal	Old Patching Pivoting Tunneling Mimikatz.exe Source Code Analysis Unquoted Service Path Firewall Evasion AV Evasion
Attacktive Directory	TryHackMe	Internal	ASREPRoasting SMB Enumeration NTDS.dit

The boxes/rooms above were used to create a company network that includes public facing websites, a production network, and an internal active directory network – all of which are commonly found in software-related organizations. Here is a mapping of these boxes/rooms against the network design:



We believe this network mimics reality but on a smaller scale, which is exactly what we wished to attack throughout the project.

Tasks Divided on Team Members

Name	Tasks
Khaled Shaaban	Penetration Testing (Internal), SAR Documentation
Abdelrahman Tarek	Penetration Tester (External), Team Leader
Abd Elrhman Emad	Penetration Tester (External)
Eslam Salem	Penetration Tester (External)
Mohamed Ali	Mitigation Documentation
Sandra Adel	Mitigation Documentation, Presentation

Learning Experience and Conclusion

This part involves pinpointing the new skills, techniques, and experiences we learnt from throughout the project. This includes technical skills and documentation skills.

At the start, most team members had no background in penetration testing or cybersecurity mitigations. This allowed more experienced members to guide them through the process, which both helped fast track the beginners and emphasize concepts with the more experienced members.

The team was exposed to what a real company network may look like through research, and through piecing together machines to create such a network, the team members gained valuable information concerning how organizations work and the certain services that are found within a software engineering company's network.

Penetration Testing was a big part of the project, as members were exposed to new vulnerabilities and exploits, as well as techniques that will certainly come in-handy in the future, such as pivoting and tunneling.

Of course, finding vulnerabilities and exploiting them is only half of the process. Members were exposed to mitigation strategies, leveraging institutions such as NIST, OWASP, service documentation, and AI to try to find the correct mitigation strategies to help remediate the vulnerabilities found in the network.

Finally, the exposure to report writing, especially the SAR (Security Assessment Report) helped emphasize concepts that were perhaps fading away through thoroughly explaining vulnerabilities and commands used to exploit said vulnerabilities. The report included the analysis and potential impact of each vulnerability aided with screenshots, as well as its respective mitigation strategies.