10Alytics

Specialization: ***Penetration Testing***

Business Focus: ***Health Tech*** *industry*

Tool: ***All Penetration Testing Tools***

Securing Healthcare Systems — A Penetration Testing Engagement for Zero Health Corp

Project Learning Opportunities

Work as Penetration Tester to help ZeroHealth Corp achieve a resilient security posture by identifying and assessing their environment for vulnerabilities and exploiting them to gain root to provide proof-of-concept that would help with mitigating found vulnerabilities

Tools and Technology to be Used

Kali Linux (Attacking machine)
Nmap
Nikto
Owasp ZAP/Burpsuite
Metasploit Framework

10Alytics

Case Study Overview

Problem Statement

ZeroHealth Corp, a fast-growing private health-tech company, is operating multiple clinics and managing large volumes of electronic health records (EHR). With the rise in targeted attacks on the healthcare industry, Zero Health Corp has engaged your team to perform a penetration test on their simulated IT infrastructure to uncover and assess vulnerabilities in their systems before malicious actors do.

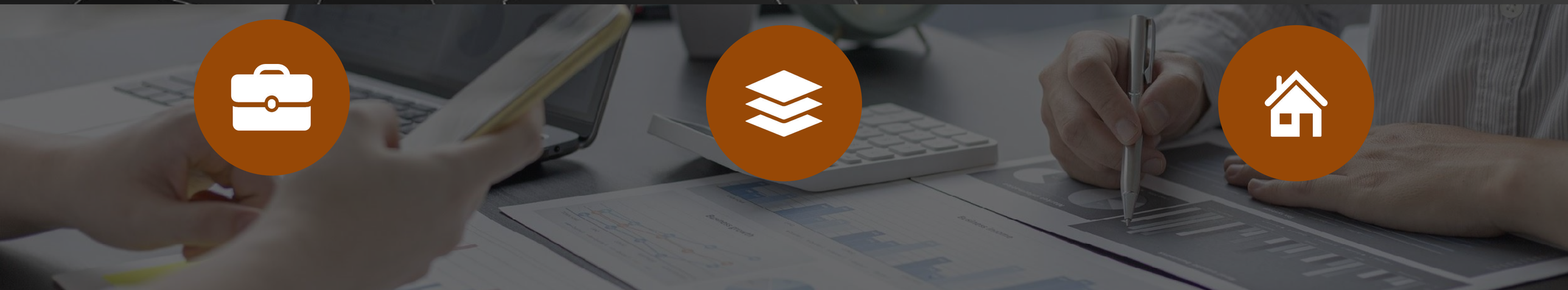
They've asked for a comprehensive security assessment, focusing on external and internal threat vectors that may impact patient data, systems availability, or compliance with HIPAA regulations.

10Alytics

Rationale for the Project

(What is the Importance of the project to the business)

To simulate a real-world attack on Zero Health Corp's infrastructure by walking through **all the phases of penetration testing**, documenting the approach, tools used, vulnerabilities discovered, and remediation strategies, with the goal of improving Zero Health Corp's overall security posture.



10Alytics

Tech Tools Stack Description

1. Kali Linux

- **Purpose: To simulate the real-world attacker's machine, with access to tools typically used**

2. Vulnerable Machine

- **Purpose: To simulate ZeroHealth Corp's environment based off their description.** (Recommended machine – Metasploitable 2)

3. Penetration Testing Tools

- **Purpose: to do a thorough sweep of ZeroHealth Corp's environment using all the phases of penetration testing to help understand their weaknesses and exploitable they are.**

10Alytics

Project Workflow

STEP 1

Phase 1: Planning & Scoping

•Define rules of engagement (no actual harm to the system, testing only simulation).

•Scope: Web server, login portal, internal server (Metasploitable2 or DVWA on local VM).

•Create a testing policy to follow: Only target provided IPs, do not attack outside networks.

STEP 2

Phase 2: Reconnaissance (Information Gathering)

Goal: Gather information about the target without touching the system.

(Pick any company of choice with functional domain as target e.g Tesla)

1.Use WHOIS to find domain ownership (if domain is simulated).

2.Use theHarvester for email and subdomain discovery:

theHarvester -d zerohealthcorp.com -b bing

3.Simulate Social Engineering analysis: Identify likely employee names and job roles.

Deliverable: Document all OSINT findings and how they can aid an attack.

10Alytics

Project Workflow

STEP 3

Key Findings

Vulnerability	Affected System	Severity (CVSS)	Description	Risk Impact
Outdated Apache Web Server	Customer Portal	8.1 (High)	Apache 2.4.29 is known to be vulnerable to RCE	Potential remote code execution
Directory Listing Enabled	Web Server	5.3 (Medium)	Files and folders exposed in `/uploads`	Info leakage, potential exploit vectors
Insecure API Keys	Mobile App API	7.4 (High)	Hardcoded API keys found in mobile binary	Account takeover or abuse
SMB v1 Enabled	Internal Employee Portal	9.0 (Critical)	Legacy file-sharing protocol enabled	Lateral movement opportunity
SSL Certificate Expiring Soon	Portal	4.3 (Low)	Could lead to trust issues for customers	Loss of trust and browser warnings

STEP 4

Phase 3: Scanning & Enumeration

Goal: Identify open ports, services, and vulnerabilities.

1.Nmap Full Scan:

Sample of Syntax: nmap -sS -sV -A <target-IP>

2.Enumerate services (FTP, SSH, HTTP, MySQL).

3. Run Nikto on web server:

Sample of Syntax: nikto -h http://<target-IP>

Deliverable: List of open ports, services, and possible vulnerabilities, Cross-reference vulnerabilities with CVEs using searchsploit. A vulnerability register and a detailed mini-report on vulnerability assessment.

Phase 4: Gaining Access (Exploitation)

Goal: Exploit discovered vulnerabilities using controlled attacks.

1.Use Metasploit and other (Researched) tools to exploit at least 5 vulnerabilities, start from the most critical vulnerabilities in your Findings Table/Vulnerabilities Register.

2.Capture the target using exploits and take screenshots (record/note keeping)

3.When attacking DVWA(the web application), perform SQLi or XSS attack with Burp Suite or OWASP ZAP.

Deliverable: Record attack steps, screenshots, and proof of access.

10Alytics

Project Workflow

STEP 5

Phase 5: Post-Exploitation

Goal: Assess what damage could be done after a breach.

1.Simulate lateral movement.

2.Extract password hashes manually or using hashdump

3.Search for sensitive data in system directories (/etc/passwd, patient records, users, hidden directories).

Deliverable: Summary of data accessed, descriptive screenshots and privilege escalation success (if any).

STEP 6

Phase 6: Reporting & Recommendations

Goal: Present findings in a professional format for non-technical stakeholders.

1.Create an executive summary.

2.Include:

- o List of identified vulnerabilities
- o Screenshots and logs of exploited paths
- o Business impact of each risk
- o Remediation steps: patching, firewall configs, user training

Deliverable: Final report + brief PowerPoint for board-level explanation.

10Alytics

Capstone Deliverables Checklist

Deliverables	Description
Network Scan Report	Nmap and Nikto results
Vulnerability Findings	Details from Research, Metasploit, Burp/ZAP
Screenshots	Proof of exploitation and access
Post-Exploitation Report	Sensitive files accessed
Final Report	Summary, analysis, business impact, recommendations, Appendix
Presentation	10-slide (minimum) presentation to Zero Health Corp’s board

10Alytics

READY TO DELVE IN?