ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Internal Network and **Systems Audit** Service *(Ethical Hacking)*

OVERVIEW

SMEs face a series of complex challenges, spurred by a tremendously agile and constantly evolving market. From economic uncertainty to fierce competition, SMEs must adapt to changing trends and the rapid evolution of technology, staying updated and flexible to ensure the relevance of their products and services. Digitalization is also highlighting the growth of the attack surface, thereby increasing the likelihood of experiencing a cyber incident and the potential consequences it can have for their survival.

KEY FIGURES

- **83% of SMEs** are **not prepared** to respond to a cyber attack.
- **30% of SMEs** fear **phishing** as one of their main cyber threats.
- **91% of SMEs** still do **not** have **cyber liability insurance.**

SOLUTIONS

We deeply understand the needs of SMEs and strive to meet them by designing, implementing, maintaining, and operating comprehensive security plans based on the six functions of NIST (Governance, Identification, Protection, Detection, Response, and Recovery). Among these, our Internal Audit service will shed light on the resilience of your internal network, understanding its main shortcomings so they can be corrected promptly.

How do we evaluate the maturity of an internal network?

Our Internal Audits are based on five main phases:

- Information gathering.
- Analysis of infrastructure vulnerabilities.
- Analysis of application and service vulnerabilities.
- Evidence gathering.
- Report writing.

At Zerolynx, we have developed our own methodology based on the best market standards, such as PTES, OSSTMM, and OWASP. This methodology establishes guidelines for conducting intrusion tests and vulnerability assessments on internal security audits, detailing how to check each vulnerability.

ABOUT ZEROLYNX

European Cybersecurity and Intelligence Provider.
Global Top 100 Providers ranked 2023.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE

ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

Internal Network and **Systems Audit** Service *(Ethical Hacking)*

Within the proposed methodology, the following tests are highlighted:

Endpoint Analysis

- Disk encryption.
- Secure passwords.
- Secure policies (access to PowerShell, session timeout, etc.).
- Local privilege escalation.

Network Attacks

- ARP Spoofing – MiTM.
- Encrypted communications.
- Network segmentation.
- Insecure protocols.
- Default credentials in network devices (switches, firewalls, routers).
- Access to Tor network.
- Data exfiltration (firewall evasion, proxies, etc.).
- Phishing tests (infected USB drives, fraudulent emails, Rogue AP, etc.).

Software Vulnerability Analysis

- Unsupported and/or outdated software.
- Vulnerabilities in installed software.
- Default credentials in services.

Malware Testing

- Malware detection.
- Access to potentially dangerous sites.
- Antivirus/EDR bypass.
- C&C execution and beaconing.

Active Directory Analysis

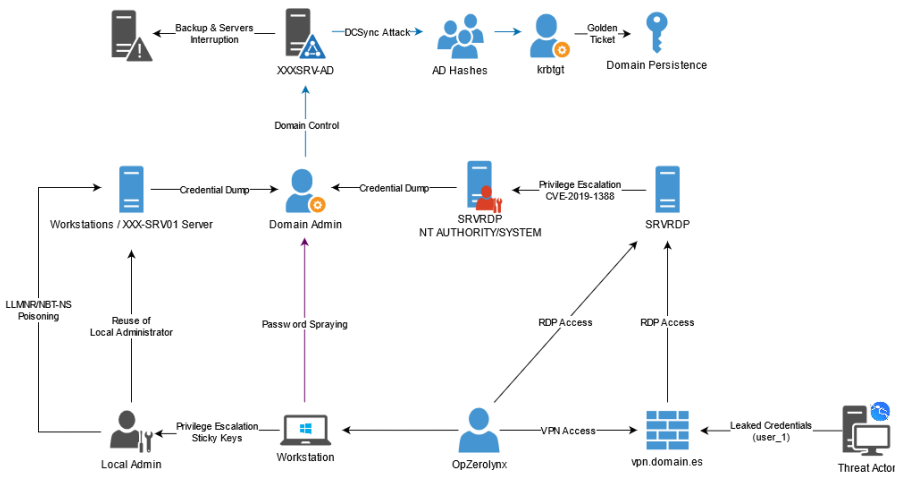
- Analysis of relationships in Active Directory.
- Shortest path analysis to domain administrator.
- Horizontal and vertical movements in the organization (sysvol, golden ticket, pass-the-hash, etc.).
- Credential dumping.

info@zerolynx.com
info@osaneconsulting.com

Internal Network and **Systems Audit** Service *(Ethical Hacking)*

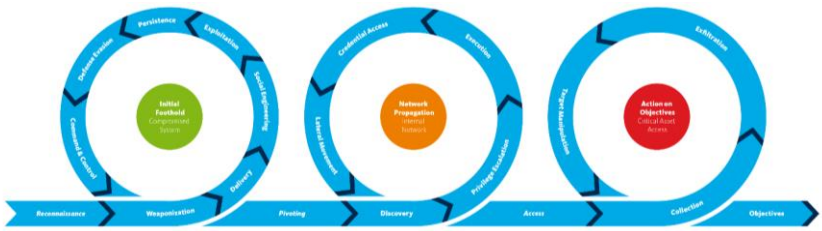
Killchain

Zerolynx always includes a graph detailing all compromise paths obtained in the client's environment, obtained during the project execution to achieve primary or secondary objectives. This graph outlines the different attack vectors that a malicious actor could have followed to accomplish their mission within the organization.



DOMAIN.ES

Along with this graph, a textual description of the attack paths and the impact that each of these scenarios would have had on the company is added. This serves as a high-level summary of the scenarios achieved during the exercise.



The different activities carried out will be framed within the Cyber Kill Chain, aiming to pinpoint the deficiencies detected in the various stages of the lifecycle of malicious actors' attacks.

ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY
CYBERSECURITY & INTELLIGENCE

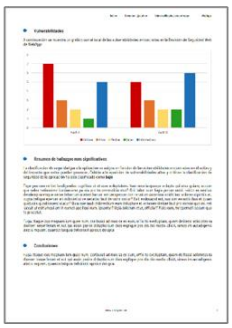
Internal Network and **Systems Audit** Service *(Ethical Hacking)*

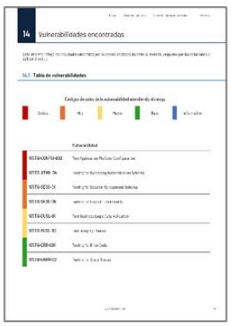
Final Report

By consolidating all the evidence obtained, a comprehensive technical and executive report will be constructed according to the Zerolynx model, and it will include, at a minimum, the following points:

- Audit Object and Scope
- Audited Systems
- Audit Team
- Interlocutors involved in the audit
- Dates of testing
- Reference documentation
- Confidentiality clause
- Detected vulnerabilities, classified according to their importance
- Recommended solutions for vulnerabilities
- Vulnerabilities addressed during the audit
- Observations
- Strengths and areas for improvement
- Conclusions reached

The report will feature an Executive Summary, highlighting the main risks detected and prioritized recommendations for potential resolution. Below are examples of an executive summary and vulnerability cards used by Zerolynx. However, the information in the report and vulnerabilities can be tailored to the needs and requirements of the client if necessary.





Additionally, Zerolynx provides the client with a high-level presentation at the end of the project documenting the main findings and remediations.