Digital forensics in corporate simulations: a study of tool efficacy and analysis techniques

Candidate: Zunino Giacomo

Supervisor: prof. Atzeni Andrea

07/04/2025

Introduction to digital forensic

Definition & purpose:

- digital forensics is a branch of forensic science focused on identifying, acquiring, processing, analyzing, and reporting of electronic data;
- it is used in cybercrime investigations, corporate security, and legal proceedings.

Key phases of investigation:

- identification, preservation, analysis, documentation, and presentation.

Motivations and goals of the thesis

Motivations

- the ongoing evolution of cyber threats
- the increasing frequency of attacks against SMBs
- the impact of these attacks on small medium businesses

Goals

- analyze digital forensic investigation methods
- identify improvements in digital forensic investigations techniques for SMBs
- simulation of attacks to examine their investigation and prevention strategies

Cyber attacks and the importance of digital forensics

The impact of cyber attacks:

- 48% of SMBs experienced cyber incidents in the past year;
- a 150% increase in cyber attacks from 2020 to 2022, with 31,000 daily attacks worldwide;
- cybercrime costs are projected to reach **$10.5 trillion annually by 2025.**

Repercussions of cybercrime

Tools used in digital forensics

Industry-standard tools	Role of automation
Autopsy (file system analysis, deleted file recovery)	scripts for network monitoring
Volatility (memory forensics)	automated analysis of logs
SIEM systems (security event monitoring)	timestamp manipulation detection
Wireshark (network traffic analysis)	

Virtualized environment setup with docker

Why docker?

provides isolation — flexibility — rapid deployment of attack simulations

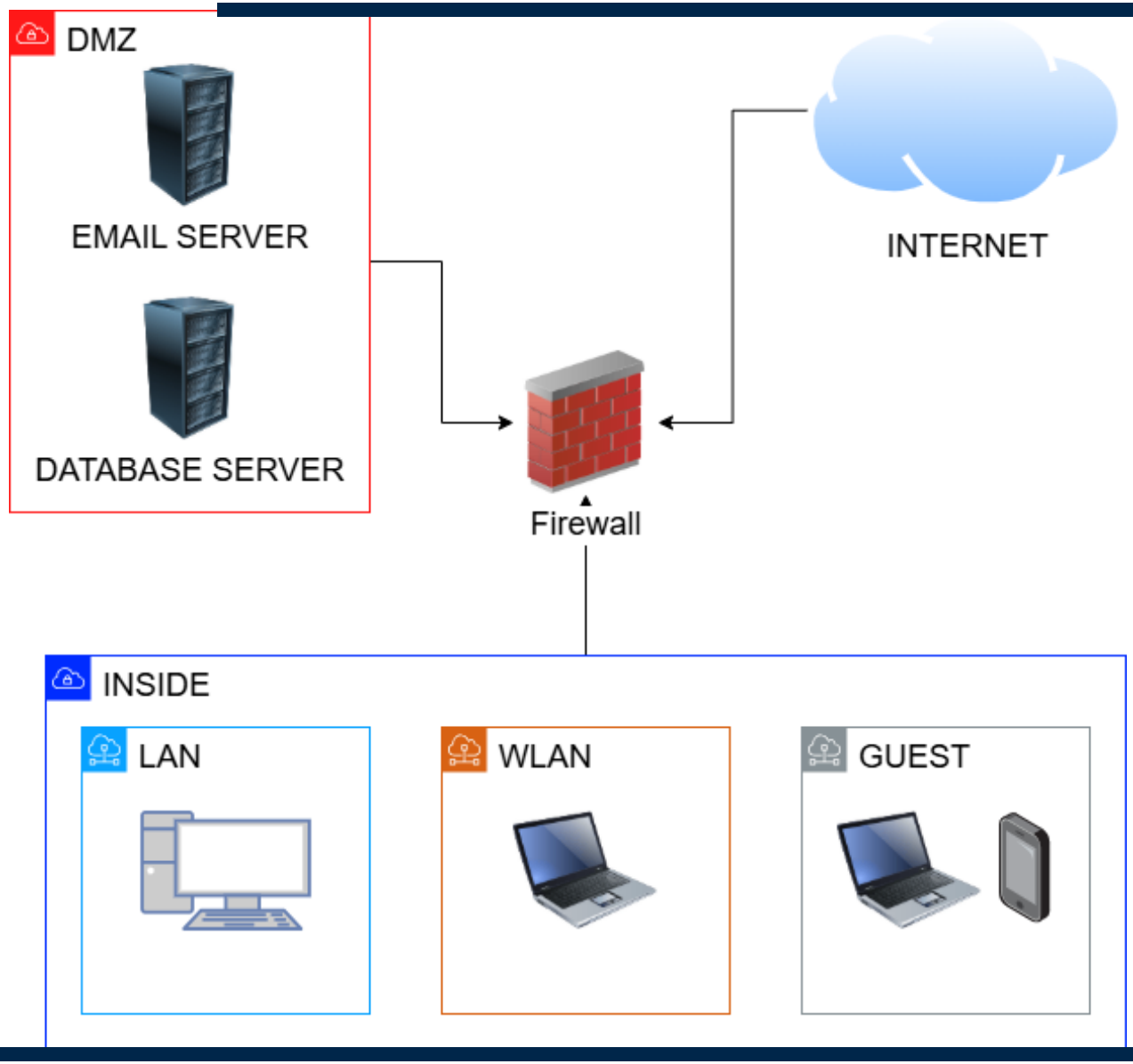
Infrastructure overview:

- **demilitarized zone (DMZ)** – contains servers (database, email);
- **internal network** – workstations and employee systems;
- **external attacker node** – simulating real-world cyber attacks.

Technical Setup:

configured using dockerfiles and bash scripts

Infrastructure



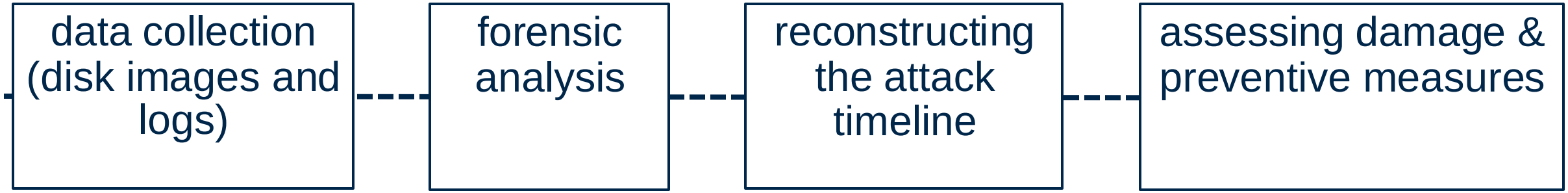
Real case scenarios

Ransomware	• **what is it?** • **example**: in October 2023, a library in Toronto was attacked and refused to pay the ransom but it had no backup
Intellectual property theft	• **what is it?** • **example**: in May 2022, two former employees were accused by Apple for stealing confidential information about SoC
Spear phishing	• **what is it?** • **example**: a CEO fraud, where attackers impersonated a CEO in a fake email targeted at specific employees
APT	• **what is it?** • **example**: in India, attackers used COVID-related themes to trick victims into opening malicious documents and execute some code

Simulated cyber attacks

Attack 1: data breach	• **methods used**: social engineering, unauthorized database access, data exfiltration; • **detection**: email and database logs monitoring.
Attack 2: phishing	• **methods used**: GoPhish, credential theft, unauthorized database access; • **detection**: email and database logs monitoring, network activity.
Attack 3: ransomware	• **methods used**: email spoofing, malicious attachment; • **detection**: file integrity monitoring.
Attack 4: malware	• **methods used**: email spoofing, malicious attachment, scheduled execution via crontab, data exfiltration via SSH; • **detection**: network traffic analysis, forensic memory analysis.

Investigating the attacks: process & methodology



Key findings from the simulated attacks

Malware attack

- malicious script that runs periodically and exfiltrates files via SSH;
- fake update attached via email.

Phishing attack

- suspicious accesses to the db from multiple users originating from an unknown IP;
- phishing email, posing as IT maintenance.

Ransomware attack

- disk images were heavily encrypted, making traditional forensic analysis difficult;
- email logs showed an email with a fake update attached before encryption.

Data breach

- unauthorized database queries extracting sensitive company data;
- identified an insider accomplice who had escalated privileges.

Lessons learned & key takeaways

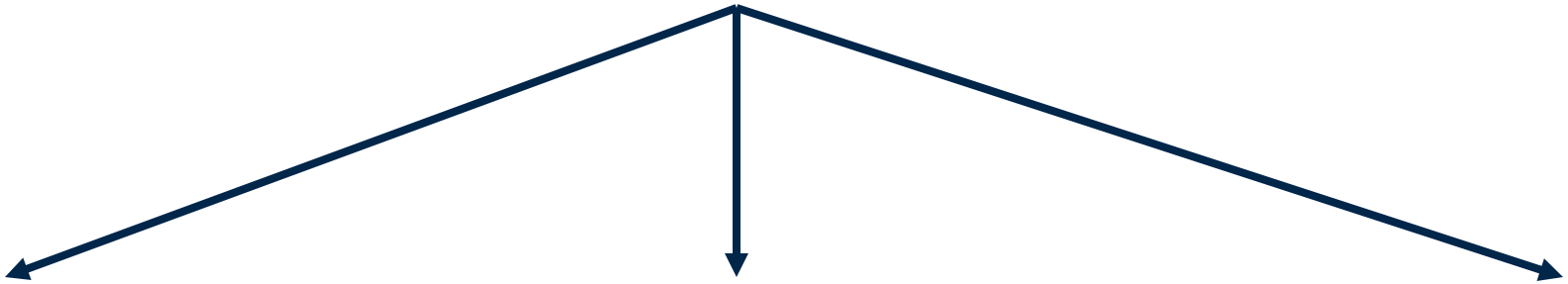
Challenges in digital investigations:

- detecting and analyzing attacks requires correlation of multiple sources (logs, disk images, network captures)
- forensic tools must be complemented with behavioral analysis
- attackers use sophisticated evasion techniques, requiring continuous updates in detection strategies

Key takeaways:

- early detection is key: a rapid response minimizes damage and facilitates forensic investigations.
- comprehensive logging matters: detailed logs across all systems (network, email, databases) improve attack reconstruction.
- user awareness is a weak link: social engineering remains a top attack vector, so ongoing training is essential.

Future improvements and research directions



Expand Attack Simulations

Different environments and platforms

Enhanced infrastructure:

certificate-based authentication with public and private CA

Thank you for your attention