

Assignment 3.1: Open Source and Mobile Intel for Security

Joshua A. Wortz

University of San Diego

CSOL-570

Prof. Melanie Thomas

09/20/2025

Introduction

Protecting an enterprise environment requires defenders to think like attackers. One of the best ways to prepare defenses is to anticipate how adversaries can gather and leverage publicly available information, exploit unsecured devices, and deploy malicious software. Every system connected to the internet or carried in an employee's pocket can be a potential attack vector if not appropriately secured.

This paper reflects on three hands-on lab exercises from TryHackMe: *Passive Reconnaissance*, *Mobile Acquisition*, and *Mobile Malware Analysis*. Each lab demonstrated practical techniques that adversaries use for reconnaissance, data collection, or exploitation. At the same time, these labs showed how defenders (Blue Teams) can repurpose these same tools and methods to harden systems, investigate incidents, and reduce the organization's attack surface. For each lab, this paper will (a) summarize the possible attacks enabled by the technique, (b) explain why the technique is vital to enterprise security, and (c) consider how both Red and Blue Team mindsets apply to the tool or method.

Lab 1 — Passive Reconnaissance

Goals and attack use cases

Passive reconnaissance is the act of collecting data about a target without directly interacting with its systems. The goal is to map the external footprint of an organization while avoiding detection. Tools such as WHOIS, [nslookup](#), and [dig](#) return DNS, registrar, and mail exchanger

records. Online services such as DNSDumpster aggregate passive DNS records to reveal subdomains, while Shodan indexes banner and port data from internet-wide scans.

From an attacker's perspective, the purpose of these tools is to generate a roadmap of exposed services. For example, subdomain enumeration can reveal forgotten development or staging environments, while certificate metadata can point to misconfigured TLS. Shodan data is frequently used in penetration testing and by adversaries to identify outdated or vulnerable services exposed to the public internet. These techniques are not theoretical—APT groups have repeatedly been observed using passive intelligence collection to shape spear-phishing campaigns or prioritize scanning targets (MITRE, 2020).

Why it matters for enterprise security

The risk is not simply that information is public—it is that attackers can correlate these data points into actionable leads. DNS and WHOIS records can identify cloud providers or third-party vendors, while MX records expose which email services an organization relies on. Each of these represents a potential supply-chain risk. Even certificate transparency logs, while necessary for accountability, can be abused to find new or misconfigured subdomains.

For enterprises, running passive reconnaissance against their own domains is essential. This practice reveals what an attacker would see and provides defenders with the opportunity to remove stale records, enforce email protections such as SPF/DKIM/DMARC, and track certificate issuance.

Red vs. Blue perspectives

- **Red Team:** Builds a detailed external asset inventory without triggering alerts, then targets services with exposed management ports, outdated banners, or weak certificates.
- **Blue Team:** Uses the same methods to inform inventories, continuously monitor passive DNS and certificate feeds, and create alerts when new exposures appear.

The TryHackMe *Passive Reconnaissance* lab reinforced that defenders must assume adversaries already know what is visible externally and adjust their security posture accordingly (TryHackMe, n.d.-a).

Lab 2 — Mobile Acquisition

Goals and attack use cases

Mobile acquisition refers to collecting data from a mobile device for forensic or investigative purposes. For an attacker, similar techniques can be abused to exfiltrate sensitive information. The goal of mobile acquisition is to preserve evidence such as text messages, credentials, authentication tokens, and file system data. Tools include Android Debug Bridge (ADB) pulls, iOS backup parsing, and dedicated forensic software.

In adversarial campaigns, gaining access to a mobile device provides high-value returns.

Attackers can capture corporate email, VPN tokens, MFA sessions, or location histories. Public breaches involving compromised smartphones have shown how attackers use mobile data to bypass perimeter defenses and impersonate valid users (Ayers et al., 2014).

Why it matters for enterprise security

Mobile devices are deeply integrated into enterprise operations, often used for email, document access, and secure communication. A lost or compromised phone without strong protections (full disk encryption, MDM enforcement, token expiration) effectively hands an attacker insider-level access. Even more concerning, mobile devices often bridge personal and corporate use, increasing the risk of cross-contamination between insecure apps and sensitive data.

Enterprises must understand mobile acquisition techniques to develop strong incident response playbooks. Forensics teams must be able to acquire data in a forensically sound manner for legal and security investigations. In contrast, security teams must enforce technical controls that limit what an attacker can obtain if a phone is lost.

Red vs. Blue perspectives

- **Red Team:** Views mobile devices as a rich target for data theft, exploiting backups, cached tokens, or weak device protections.
- **Blue Team:** Must anticipate this risk, enforce strong MDM policies, mandate encryption, and ensure employees can remotely wipe lost devices. Forensic readiness ensures investigations are credible and evidence is preserved.

The *Mobile Acquisition* lab highlighted that defenders need both proactive mobile hardening and reactive forensic readiness to reduce risk (TryHackMe, n.d.-b).

Lab 3 — Mobile Malware Analysis

Goals and attack use cases

Mobile Malware Analysis (MMA) involves examining malicious applications to determine their behavior, capabilities, and indicators of compromise. Attackers design malware to harvest credentials, intercept SMS codes, escalate privileges, or maintain persistence. Static analysis examines code and manifests (permissions, libraries, embedded URLs), while dynamic analysis executes the malware in a sandbox to observe runtime behavior.

Mobile malware has been used in significant breaches and espionage campaigns. For example, spyware families such as Pegasus exploited mobile OS vulnerabilities to capture calls, messages, and app data. Commodity malware on Android has harvested banking credentials and 2FA codes, illustrating the destructive potential of malicious mobile apps.

Why it matters for enterprise security

Enterprises often rely on mobile apps for sensitive functions, from secure messaging to financial transactions. Malware targeting these applications can compromise SSO tokens, corporate logins, and protected communications. Understanding analysis techniques enables defenders to detect, block, and remediate infections quickly.

Equally important, malware analysis allows defenders to generate IOCs and update detection rules across the enterprise. By dissecting permissions, network indicators, and persistence mechanisms, Blue Teams can detect malicious behavior early and reduce dwell time.

Red vs. Blue perspectives

- **Red Team:** Learns how malware can evade detection, use legitimate APIs for persistence, and disguise its behavior.

- **Blue Team:** Uses analysis results to build signatures, tune EDR rules, and vet applications before deployment.

The *Mobile Malware Analysis* lab illustrated the dual importance of these skills: attackers weaponize malware to compromise devices, while defenders dissect malware to neutralize threats (TryHackMe, n.d.-c).

Conclusion

Together, these three labs emphasize the **lifespan of an attack chain**: external reconnaissance identifies targets, mobile acquisition extracts sensitive data, and malware maintains persistence or expands the attack surface. From an enterprise security perspective, defenders must prepare at each stage:

1. **Discover and minimize exposure** through regular passive reconnaissance and inventory validation.
2. **Harden and monitor mobile devices** with MDM, encryption, and short token lifetimes to reduce the damage if a device is compromised.
3. **Develop forensic and analysis capabilities** to investigate incidents and neutralize malware efficiently.

Ultimately, one of the best ways to protect an environment is to view it through both Red and Blue lenses continuously. Knowing what attackers can see and steal is the first step toward proactive defense.

References

- Ayers, R., Brothers, S., & Jansen, W. (2014). *Guidelines on mobile device forensics* (NIST Special Publication 800-101, Revision 1). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-101r1>
- MITRE. (2020). *Reconnaissance (TA0043)*. MITRE ATT&CK®. <https://attack.mitre.org/tactics/TA0043/>
- TryHackMe. (n.d.-a). *Passive Reconnaissance* [Online room]. <https://tryhackme.com/room/passiverecon>
- TryHackMe. (n.d.-b). *Mobile Acquisition* [Online room]. <https://tryhackme.com/room/mobileacquisition>
- TryHackMe. (n.d.-c). *Mobile Malware Analysis (MMA)* [Online room]. <https://tryhackme.com/room/mma>
- Ozkaya, Y. D. D. E. (2022). *Cybersecurity — Attack and defense strategies* (3rd ed.). Packt Publishing.