Project process

MindBytes GmbH | Probststraße 15 | 70567 Stuttgart
hallo@mind-bytes.de | +49 711 20709567

Management: Christian Stehle, Nina Wagner, Simon Holl
Stuttgart Local Court | HRB 790784 | VAT ID: DE363069855
Volksbank Alb eG, IBAN DE04 6309 1300 0513 9800 16

TABLE OF CONTENTS

1 Overview

Our projects are divided into the following phases:

1) Preparation: coordination of deadlines, scoping, kick-off, preparation by client and contractor
2) Implementation & documentation
3) Results: Report & final meeting

2 Preparation

- Determining the **implementation period**
- If the request was submitted through our configurator, a **scoping meeting** follows to present the test object and clarify organizational questions and necessary preparatory steps
- We provide a **checklist** for the preparation
- **Kickoff meeting** for final preparation and coordination to ensure a smooth implementation start

2.1 Preparation & input by the client

The client provides all information necessary for the implementation of the project. The information required is discussed during the scoping meeting and provided in the form of a checklist.

2.1.1 For pentests

The following is typically required for pentests:

- **A defined test object**, such as the URL of a web application or IP ranges of the infrastructure to be tested
- **Accessibility of the test object**, such as activation for access to protected applications or VPN access to an infrastructure
- **Access to test objects**, such as user accounts for systems or applications with authentication means, such as passwords, certificates and tokens
- Further information, such as documentation or source code of the application, if applicable
- **Exceptions in protection systems**: any protection systems, such as web application firewalls (WAF) and intrusion prevention systems (IPS), are configured for the implementation of the project so that data traffic from the IP address of MindBytes can pass unhindered - if desired, tests can be carried out with connected systems at the end of the project
- **Focus:** Define desired focal points if necessary

2.1.2 For Red Teamings

The preparation of a Red Teaming typically proceeds as follows:

Kickoff meeting (approx. 1 hour)

- Agreement on the **objectives of the Red Teaming**, such as accessing a specific system
- Agreement on the desired type of **communication** during the project (frequency, channels). Generally, the following applies:
    - The Red Team stays in close contact with the White Team (people involved on the client's side) throughout the entire project.
    - If the Red Team finds critical vulnerabilities, an immediate notification is sent.
    - If test cases of the Red Team could potentially lead to disruptions, the team discusses with the White Team how to proceed beforehand.
- Definition of the rough **timeframe** for implementation
- Definition of the **White Team**:
    - Agreement on the composition of the White Team and, if necessary, addition of persons in relevant positions to de-escalate when the attack is detected
    - Contact details and availability of the White Team
- If agreed/requested: **provision of certain information** such as domain names, IP address ranges and lists of email addresses
- Definition of the **Rules of Engagement (RoE)** for the Red Team:
    - Permitted attack surface
    - Starting point of the Red Team
    - In-scope controls
    - Out-of-scope controls
    - Permitted TTPs (tactics, techniques & procedures)
    - Excluded TTPs
- For **on-site tests**:
    - Addresses of the target buildings and, if necessary, building plans for precise delimitation
    - Preparation of "get-out-of-jail" letters for the Red Team (authorization letters for possible encounters with security services or police)

Scenario development

- Scenarios can be developed by the Red Team upon request, in consultation with the client

Coordination meeting before implementation (approx. 30-60 minutes)

- Selection of scenarios
- Specification of the schedule for the implementation of the scenarios

3 IMPLEMENTATION & DOCUMENTATION

At the beginning of the implementation and after completion of all tests, we send an e-mail for information.
In the event of critical vulnerabilities, an immediate notification is sent.

3.1 In pentests

Depending on the test object, the procedure during the pentest is based on **recognized standards**, such as

- Study "Implementation concept for penetration tests" by the Federal Office for Information Security (BSI)
- OWASP Web Security Testing Guide (WSTG)
- Penetration Testing Execution Standard (PTES)

In pentests, the **execution of the tests is obvious**, i.e. no efforts are made to hide test activities or to remain undetected by any monitoring systems.

The tests are always performed **manually** with the support of **specialized software** and **automated** state-of-the-art **scans.** The choice of software depends heavily on the test object and the test environment. The following list is an excerpt of the software used:

- Nessus Professional
- Burp Suite Professional
- Cobalt Strike
- Various open-source tools, such as Nmap, Hashcat, Bloodhound and Rubeus

3.2 In Red Teamings

A Red Teaming consists of the following steps:

- **Information gathering**: Red Team collects information about the permitted attack surface
- **Refining the scenarios**: We discuss and define the selected attack scenarios in detail with the White Team based on the collected information
- **Preparing the scenarios**: Red Team prepares the selected scenarios for implementation
- **Implementation**: Red Team implements the scenarios, logging any activities, insights and observable reactions by the Blue Team (client's team responsible for detecting and responding to attacks)

  During implementation, the Red Team goes through multiple phases:

  - Reconnaissance
  - Initial Compromise

- Establish Persistence
- Lateral Movement & Escalate Privileges
- Complete Mission

Details about the process model as well as the deployed methods and tools can be found in the appendix.

Due to the individual nature of each project, the actual process may vary from the one described. For example, phases may be skipped if projects start at an advanced stage on the assumption that an attacker has already reached this starting point.

If all tests remain undetected during the course of the project, we might (in consultation with the client) adapt our activities to be more conspicuous in order to check at which point the Blue Team would react.

3.2.1 What happens if the Red Team is detected?

If the Blue Team detects the Red Team, there are various options for continuing the project, depending on the current project phase:

1) **Continue Red Teaming:** The red team continues the attacks from other source systems, possibly after a cool-down period. This can be useful if there is still enough time left in the project for a new attempt and the Blue Team has detected an attack but has not yet been able to immediately conclude that it is a Red Teaming project.
2) **Switch to Purple Teaming:** The project mode switches to a Purple Teaming approach. The Red Team continues to carry out typical attack activities in coordination with the Blue Team. The Blue Team analyzes whether the activities are detected in order to remedy any blind spots.

The White Team and the Red Team will decide together how to proceed with the project in this situation.

3.2.2 Important information for the client

- In order to ensure realistic conditions for the project, as few people as possible should be made aware of this project on the client side.
- The client is responsible for ensuring that the data protection and legal requirements for this project are met.

4 Results

4.1 Report

The results of the project are provided in either German or English as a PDF report and in tabular form as an Excel file.

4.1.1 For pentests

Our pentest reports contain:

- A management summary with a risk perspective on the overall picture, the need for action and an overview of the recommended action with priority, estimated time to remedy and costs incurred
- A technical summary with a summary of the results from a technical perspective, presentation of any links between Findings and recommended next steps
- For each Finding a description of the possible security-relevant effects, a classification according to CVSS v3.1 and a recommendation for rectification

4.1.2 For Red Teamings

Our Red Teaming reports contain:

- A **management summary** with a risk perspective on the overall picture, the need for action and an overview of the recommended action with priority, estimated time to remedy and costs incurred
- A **technical summary** with a summary of the results from a technical perspective, presentation of any links between findings and recommended next steps
- The **attack narrative**, i.e. a detailed textual description of all test activities and observations in chronological order, including a visualization of the Red Team's actions and, if applicable, the Blue Team's responses, on a timeline
- For each **finding**, a description of the possible security-related effects, probability of occurrence, risk classification, detailed description, and recommendations for remediation
- Description of the **project scope**
- **Red team activity log**: A tabular list of the Red Team's activities with the corresponding timestamps (log) so that the Blue Team can see which activities were detected or not detected; also includes “Indicators of Compromise” (IoCs)
- **Overview** of the findings in Excel format
- If required, other attachments with additional technical details

4.2 Meetings and follow-up

4.2.1 For pentests

As standard, we plan the following meetings:

Final meeting (approx. 0.5–1 hours)

- Participants: Pentest project leads, pentesting team
- Timeframe: 1–3 weeks after the pentest
- Objective: Presenting the results based on the report, answering any questions

Management presentation (approx. 15–30 minutes)

- Participants: Management, pentest project leads, pentesting team
- Timeframe: Any time after the pentest
- Objective: Summarizing the results at the management level

Follow-up (approx. 30 minutes)

- Participants: Pentest project leads, pentesting team
- Timeframe: 2–3 months after the pentest
- Objective: Discussing the remediation progress, helping with any challenges, if required

4.2.2 For Red Teamings

As standard, we plan the following meetings:

Final meeting (approx. 1–2 hours)

- Participants: Blue Team, White Team, Red Team
- Timeframe: After Blue Team and White Team have reviewed the report (approx. 1–2 weeks after receiving the report)
- Objective: Presenting the project and findings from the Red Team's perspective based on the report, answering initial questions from the Blue Team

Q&A session (approx. 1 hour)

- Participants: Blue Team, Red Team, potentially White Team
- Timeframe: After the Blue Team has reviewed the results in more detail
- Objective: Answering questions from the Blue Team, for example about what can be seen in logs

Management presentation (approx. 15–30 minutes)

- Participants: White Team, Management, Red Team, potentially parts of the Blue Team
- Timeframe: Any time after the Red Teaming

- Objective: Summarizing the results at the management level

Follow-up (approx. 30 minutes)

- Participants: White Team, Red Team, potentially Blue Team
- Timeframe: 2–3 months after the Red Teaming
- Objective: Discussing the remediation progress, helping with any issues and challenges, if required

5 APPENDIX

5.1 Further details about the Red Teaming

5.1.1 Detailed description of the methods and tools used

Our methodology is based on realistic attack scenarios. Tactics and techniques from the MITRE ATT&CK Matrix are used as a basis.

5.1.1.1 Methods

The methods used in a Red Teaming are selected based on the specific circumstances of the project. The table below provides an overview of common methods for the phases described above.

Phase	Typical methods
Reconnaissance	Technical: - Open-source intelligence (OSINT) to outline the technical attack surface (IP addresses, domains, accessible services, metadata) - Search for leaked credentials Building/physical: - Gathering information about card readers (with logs, if applicable), locks, and sensors, for example - Reviewing detection measures such as CCTV cameras and alarm systems People: - Social media - Information on websites, e.g. the company's website - On-site: Observing typical processes, e.g. of external service providers who access the buildings regularly
Initial Compromise	Technical: - Exploiting vulnerabilities in software - Exploiting misconfigurations - Exploiting publicly known credentials - Attacks on logins/user accounts, e.g., password spraying Building/physical:

	- Exploiting weaknesses in protocols, e.g., to clone keycards - Opening locks, e.g., by lock picking - Tricking sensors, e.g. on sliding doors that should only open from the inside People: - General: social engineering attacks - Phishing - Vishing - Tailgating - USB dropping - Pretexting (pretending to have a credible excuse)
Establish Persistence	- Set up a command-and-control channel - Use automation to ensure that the connection is restored after a possible interruption

Lateral Movement & Escalate Privileges	- Attacking now accessible neighboring systems and applications and taking over other user accounts
	- Iteratively applying the methods and techniques from newly reached starting points for further propagation (possibly also from previous phases)
	- Typical techniques:
	  o Enumerating the internal environment
	  o Exploiting vulnerabilities in software
	  o Exploiting misconfigurations
	  o Exploiting weak protocols at the network level
	  o Examples in Active Directory: relaying, ADCS, Kerberoasting, pass-the-hash, DCSync, exploiting of domain trusts
	  o Exploiting access to highly-privileged accounts
	  o Exploiting weaknesses in authentication, such as password reuse, attacks on password hashes and tickets, and lack of MFA
	  o Exploiting unsecured or inadequately secured (administrative) endpoints

Complete Mission	- Achieving the Red Team's goals, such as
	  o Exfiltrating data
	  o Proving access to specific systems like backup servers, for example
	  o Complete takeover of Active Directory

5.1.1.2 Tools

The tests are always performed by manually executing targeted commands and tools, supported by state-of-the-art specialized software. The choice of software depends heavily on the test object and the test environment. The following list is an excerpt of the software used:

- C2-Framework: Cobalt Strike or Sliver with customizations
- Burp Suite Professional as HTTP-Proxy
- Tools/exploits developed by our own team
- various common tools like Bloodhound, Rubeus, Nmap, Spiderfoot, Gophish, Hashcat

5.1.2 Description of the process model

Depending on the defined project rules, the red team selects appropriate attack options and techniques. A red teaming project can be divided into several phases, which are explained below.

Due to the individual nature of each project, the actual process may vary from the one described. For example, phases may be skipped if projects start at an advanced stage on the assumption that an attacker has already reached this starting point.

5.1.2.1 Reconnaissance

In this phase, information about the company is gathered from sources such as company websites, social media profiles, and websites with compromised credentials. This approach is known as "open-source intelligence" (OSINT). In addition, technical sources are evaluated to determine the company's IP addresses and domain names as well as accessible services.

If physical intrusion attempts are permitted, the Red Team can gather information about local conditions and typical daily routines on the internet or through on-site observations, for example.

5.1.2.2 Initial Compromise

In this phase, the collected information is analyzed to find and exploit vulnerabilities. Phishing attacks are often used to trick employees into revealing their credentials or executing files that give the Red Team access to the company's internal network.

5.1.2.3 Establish Persistence

After the Red Team has gained access to the internal network in the previous phase, this phase ensures persistence. For example, it ensures that if the connection to a compromised server is interrupted, the connection can be restored without re-exploiting the vulnerability. This is usually achieved with a command-and-control framework.

5.1.2.4 Lateral Movement & Escalate Privileges

The Red Team attacks neighboring systems or users in order to gradually move and spread throughout the environment. In this phase, the Red Team usually attempts to gain administrative access to a system. From new starting positions, information about the environment is collected iteratively to determine the next possible attacks.

5.1.2.5 Complete Mission

Depending on the project goals, data is downloaded or access to a specific system, such as a backup server, is demonstrated.

LEGAL INFORMATION

MindBytes GmbH
Probststr. 15
70567 Stuttgart
Germany

+49 711 20709567| hallo@mind-bytes.de | https://mind-bytes.de

Local Court: Stuttgart, HRB 790784 | VAT number: DE363069855

Represented by **Christian Stehle, Nina Wagner, Simon Holl**