RED TEAMING:

The tactics and methods involved in full-scale cyberattack simulations

GROUP IB

TABLE OF CONTENTS

01 INTRODUCTION

Organizations regularly face waves of malicious activity, from technical intrusions to social engineering attacks. To protect against such threats, businesses strive to use the most effective measures and defense tactics available.

However, breaking news headlines about successfully prevented attacks do not always reflect reality. More often, a company's internal information security team is unable to identify signs that hackers are planning to compromise its systems. This is because attackers nowadays use the most advanced tools and the latest malware that even the most highly protected IT infrastructures and systems are not prepared for.

There are many security-testing services on the market, including solutions for system and application security analysis, perform penetration testing, and assess employee awareness of information security issues. Despite how effective these measures are when it comes to monitoring security, they only offer a point-by-point assessment over a short period of time.

Research shows that the number of incidents only increases every year, which means that organizations must prepare for real-life attacks that are not limited by any framework.

There is no doubt that security capabilities must regularly be tested against the latest cyber threats.

The most realistic and advanced approach to security testing is Red Teaming. Red Teaming involves the continuous assessment of system security, the preparedness of specialists to respond to incidents, and the ability of systems to resist new types of attack, including advanced persistent threats (APTs).

02 WHAT IS RED TEAMING?

Red Teaming is the most comprehensive and realistic way to test an organization's ability to prevent complex cyberattacks. The process utilizes the most advanced tactics, techniques, and procedures (TTPs) from hackers' arsenals.

During Red Teaming, the client's security team is purposefully not informed about the engagement. Group-IB's Red Team simulates the actions of real-life attackers based on specialized threat analysis and hacks the organization in a controlled and effective way. In the long term, the testing helps eliminate gaps in the organization's information security.

Objects of the engagement

Technologies:
network, applications, etc.

People:
employees and partners

Assets:
offices and warehouses

Basic Red Teaming scenarios

Red Teaming engagement scenarios differ for every client and depend on the goals set. Most often, scenarios include:

- AD (Active Directory) forest takeover
- Client data exfiltration
- Access to a top manager's device
- Intellectual property exfiltration

Advantages of Red Teaming

- Long-term service
- Useful for companies with a "mature" understanding of information security
- Focused on achieving specific goals such as obtaining access to network nodes or intercepting information through any means available

These full-scale cyberattack simulations help answer the following questions:

01 | How effectively do the organization's existing security measures protect important data?

02 | Is the organization's alert and monitoring system configured correctly?

03 | To what extent is the company's security team prepared to counter attacks conducted by highly skilled hackers?

04 | What possibilities become available to attackers within the infrastructure if users or their devices are compromised?

This approach mirrors the behavior of real-life attackers as closely as possible to not only clearly demonstrate potential scenarios involving hacker attacks but also ensure that information systems are protected effectively.

Red Teaming results help assess the risks linked to APTs.

03

RED TEAMING VS.
Penetration Testing

Even though both Red Teaming and Penetration Testing (“pentesting”) use similar methods, their goals and results differ greatly.

Red Teaming

Red Teaming simulates real targeted attacks on the entire organization. The advantage of Red Teaming lies in its continuous investigation into information systems in order to achieve set goals. This in-depth check provides a full-scale understanding of perimeter security, employee awareness, and how the organization’s internal processes react when the company is under attack.

As such, the focus is on the depth of the engagement.

Penetration Testing

Pentesting detects as many technological vulnerabilities and flaws as possible within a pre-defined IT infrastructure. After detecting a vulnerability, pentest specialists usually try to exploit it and increase their access rights to understand the potential risks involved. As such, penetration testing does not assess how prepared an organization is to detect and respond to security incidents.

Therefore, the focus is on the scope of the testing.

In Group-IB’s experience, Red Teaming and pentesting complement each other perfectly. Both types of tests are important and useful in their own right, but as a combination they provide for both passive systems protection and overall active company security.

Moreover, Red Teaming complements other forms of testing (e.g., code analysis) and, as an organization grows, is included in information security testing plans.

Main differences between Red Teaming and Penetration Testing:

	Red Teaming	Penetration Testing
Project goals	Focus: Depth of the engagement. Task: Reach targets in the most in-depth way possible. Only targeted results are included in the report. Main goal: Check and strengthen the organization's ability to detect and respond to complex cyberattacks.	Focus: Scope of the engagement. Task: Cover as many attack vectors as possible. Main goal: Hack as many systems as possible and detect all potential vulnerabilities within a limited time frame.
Attack methods and vectors	All possible methods, including disruptive ones if approved by the client. Aim: Achieving goals, and testing people, processes, and technologies.	Technical methods of attack on agreed objects, excluding damaging attacks. Social engineering, if approved by the client. Aim: Testing specific assets belonging to the organization.
Conformity	Engagement simulates the TTPs used by real-life hackers.	The test is conducted in accordance with the methodologies adopted within the industry.
Bypass of detection systems	Bypassing intrusion detection systems is important.	Detecting the system's technical vulnerabilities and not evading intrusion detection systems are important.
Post-exploitation of vulnerabilities	Uses vulnerabilities to capture the necessary data and develop the attack further.	Testing is stopped if access to data is obtained.
Results	Detailed report containing the following information: • How the Red Team achieved its goals • The engagement's main stages • What assets were compromised • What scenarios were played out and what was accessed Executive summary	Detailed report including: • Descriptions of all the vulnerabilities detected and an assessment of how critical each of them is • Information about the conducted assessments and results Executive summary

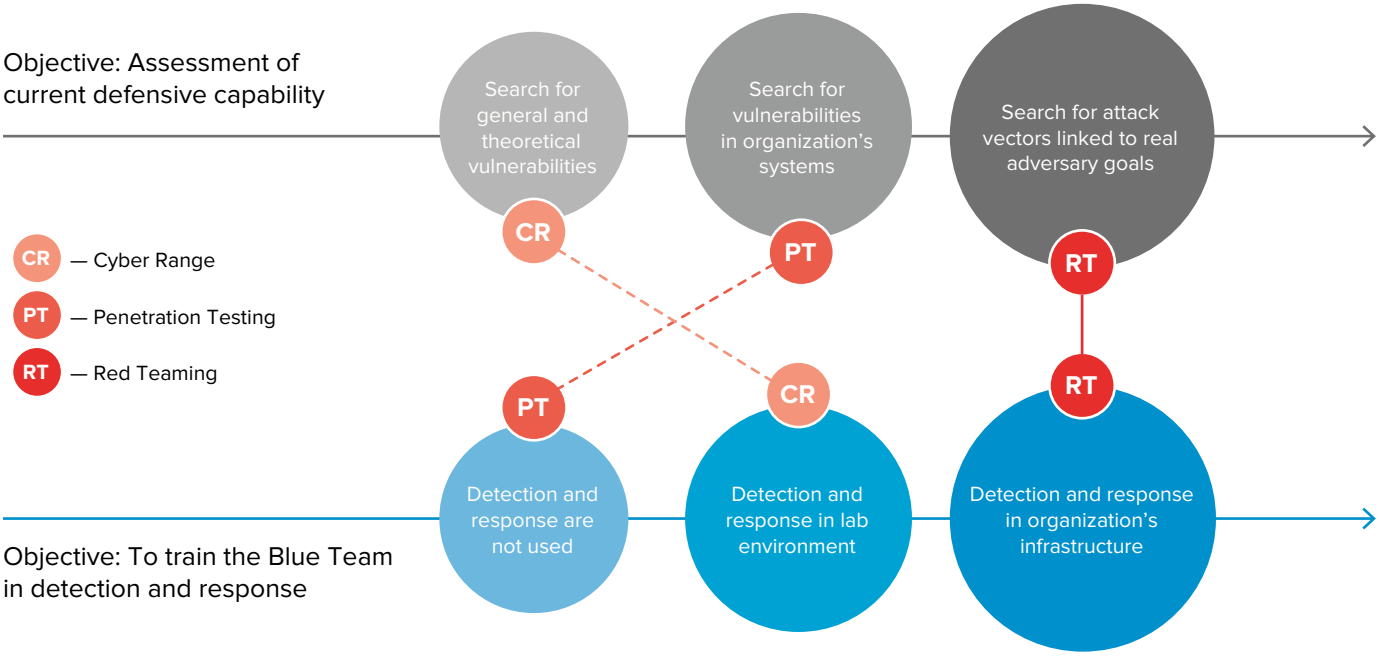


Figure 1. **Comparison of goals and results of testing similar to Red Teaming**

04 GROUP-IB'S APPROACH TO RED TEAMING

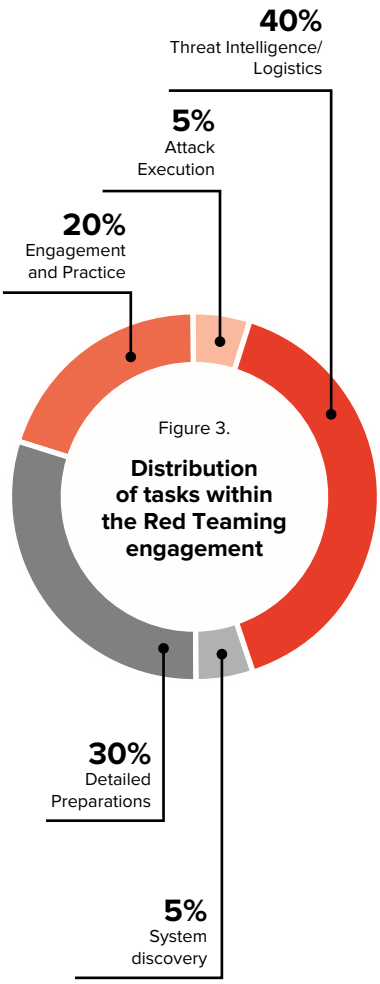


Figure 3.
Distribution of tasks within the Red Teaming engagement

The Red Teaming process can be divided into several consecutive stages:

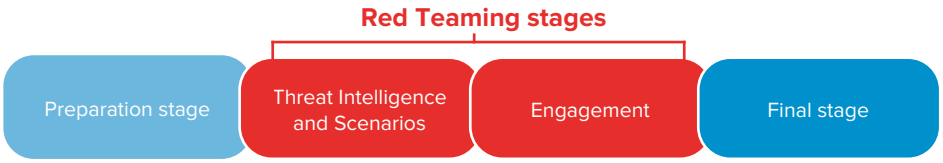


Figure 2. **Main stages of Red Teaming**

For greater effectiveness, some actions within the main stages can be started earlier or completed at the same time as others, depending on time constraints.

The parties involved (client and contractor) should adhere to this process for all Red Teaming engagements to ensure that they are standardized in accordance with all requirements.

The parties directly involved in the Red Teaming are:

On the client side:

- Blue Team: the client's information security service being assessed and whose prevention, detection and response capabilities are being tested without prior notice
- White Team: a small team within the target entity who are responsible for the overall planning and management of the Red Teaming engagement

During the engagement, the White Team works with the Red Team and, if necessary, becomes involved (e.g., when testing affects critically important processes).

On the contractor side:

- Red Team
- Appointed testing manager

The testing manager works closely with the White Team to organize the Red Teaming process, engage in consultations throughout the various operation stages, and ensure transparency of communications.

1. Preparation stage

Duration: 4-6 weeks

Task: Assess the organization's current needs and the scope of the work involved.

Action plan:

- Create a working group made up of client and contractor representatives.
- Define the range of work (duration, scope, legal limitations, prohibited actions).
- Sign cooperation protocols and formats.
- Form the Red Team in accordance with the needs of the current project.

At this stage, the prerequisites for Red Teaming are established, and the project is officially launched.

Results:

- Agreed engagement area
- Agreed goals and tasks involved
- Approved project plan and means of communication
- Formed working groups to monitor and manage all simulations

2. Red Teaming execution stage

Duration: 12+ weeks

Tasks:

- Perform reconnaissance (in the form of Threat Intelligence)
- Develop scenarios based on critical system functions and threat models
- Create a plan and attempt to penetrate the agreed targets (systems and departments that perform one or more critical functions)

Results:

- Engagement plan
- Checklist of potential attack scenarios for further engagement
- Technical report with engagement results

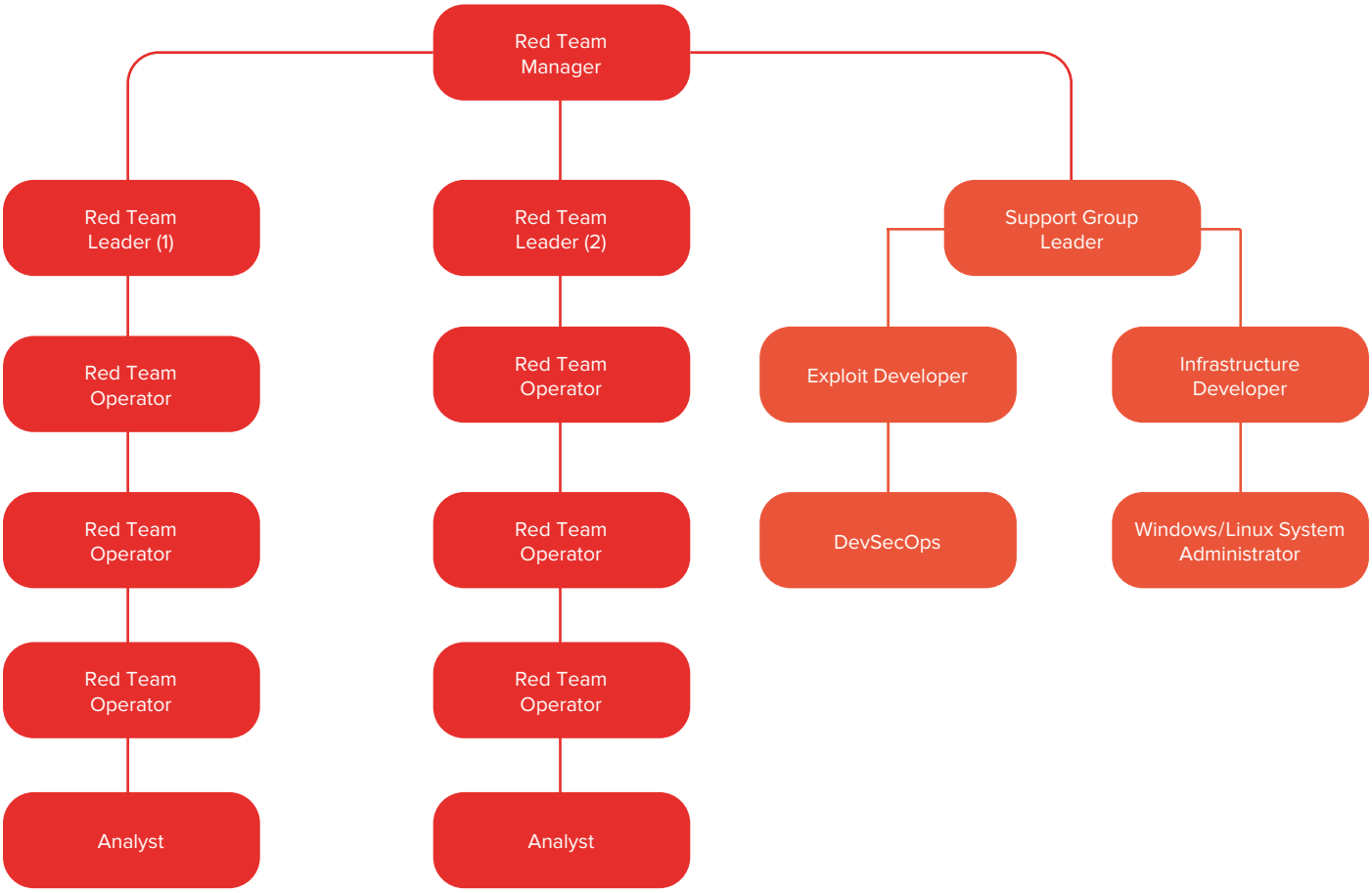


Figure 4. **The project's Red Teaming team**

Step 1: Threat Intelligence and Scenarios

The Red Team carries out Threat Intelligence (TI). The client can turn to a third-party TI vendor for targeted threat analysis (TTI Report) of the investigated object. The vendor will then focus their efforts on more detailed reconnaissance to give the Red Teaming provider more bespoke and specific information on the entity, which will in turn allow meaningful attack scenarios to be developed and a more effective test to be done.

The Red Team performs extensive reconnaissance that would usually be completed by hackers when planning a targeted attack. The goal here is to study the organization's profile, structure, and activities. Reconnaissance also helps determine the most relevant criminal threats that are unique to the organization's jurisdiction and obtain an overview of the key nodes and targets from the hacker's point of view.

Based on the information collected, initial scenarios involving potential attacks are developed so that the Red Team can test them. Scenarios are designed from the point of view of attackers who target crucial functions of the organization.

Step 2: Red Team engagement

The Red Team acts based on the plan and scenarios developed during Step 1 and:

- Conducts covert attacks on identified critical functions/assets of the target systems
- Sets the key points (i.e., the testing goals that were agreed and that could be updated throughout the process of analyzing target threats)
- Develops alternative ways of achieving the test objective using TTPs employed by advanced attackers, if obstacles occur

The Red Team is dynamic, which means that experts from narrow fields and specializations can be added to it.

All operations are carried out by working closely with the responsible managers, and all actions performed by the Red Team are recorded for the report.

3. Final stage

Duration: approx. 2-4 weeks

The Red Teaming engagement officially ends either when all steps have been successfully completed or when the allocated time for the operations has run out.

Action plan:

- The Red Team reviews and assesses the Blue Team's ability to respond to the cyber threats faced during the engagement.
- The Red Team drafts a report that includes descriptions of actions taken, conclusions, findings and observations from the test and sends it to the Blue Team. If required, the report is complemented with recommendations on how to improve technical monitoring, enhance policies and procedures, and raise employee awareness.
- The Blue Team receives the Red Team's conclusions and drafts its own report based on them. The report will map out the Blue Team's actions alongside those of the Red Team.
- Participants in the process exchange results, analyze them, and make improvements to further enhance the cyber resilience of the entity.

Results:

- The Red Team's report on the engagement performed and recommendations
- The Blue Team's report on the engagement performed and comparison of results
- A workshop with a replay organized in which teams jointly review the steps taken by both parties during the test
- An action plan relating to strategic security management and general conclusions

05 EXECUTION METHODOLOGY

To conduct an attack simulation on a set target, Group-IB specialists use verified methodology that they tailor to every client. Group-IB addresses the organization's specific requirements and activities so as not to disrupt critical business processes.

The following formats are available:

1. The client's information security teams and system administrators (except directors) are not informed about the engagement so that their ability to identify and respond to cyberattacks can be assessed.
2. Security levels are tested together with the client's relevant departments.

The Red Teaming lifecycle is based on the Cyber Kill Chain® model:

Reconnaissance

Goal: Collect as much information as possible about the target.

Reconnaissance is one of the most important steps because it provides a substantial amount of new information about people, technologies, and the environment. This step can include building or acquiring special tools and data.

Weaponization

Goal: Thoroughly analyze all the collected information about the infrastructure, objects, and employees.

The Red Team then sets their goal and establishes the main actions required to achieve it.

Delivery

Goal: Actively launch the full operation.

The Red Team conducts the actions intended to reach the targets (or flags) such as social engineering, analyzing vulnerabilities, planting hardware Trojans for remote network persistence, and establishes the optimal conditions for further exploitation.

Exploitation and installation

Goal: Break into servers/applications/networks and exploit targeted staff using social engineering.

This step paves the way for the next phase (i.e., the acquisition of administrator rights).

Control and movement

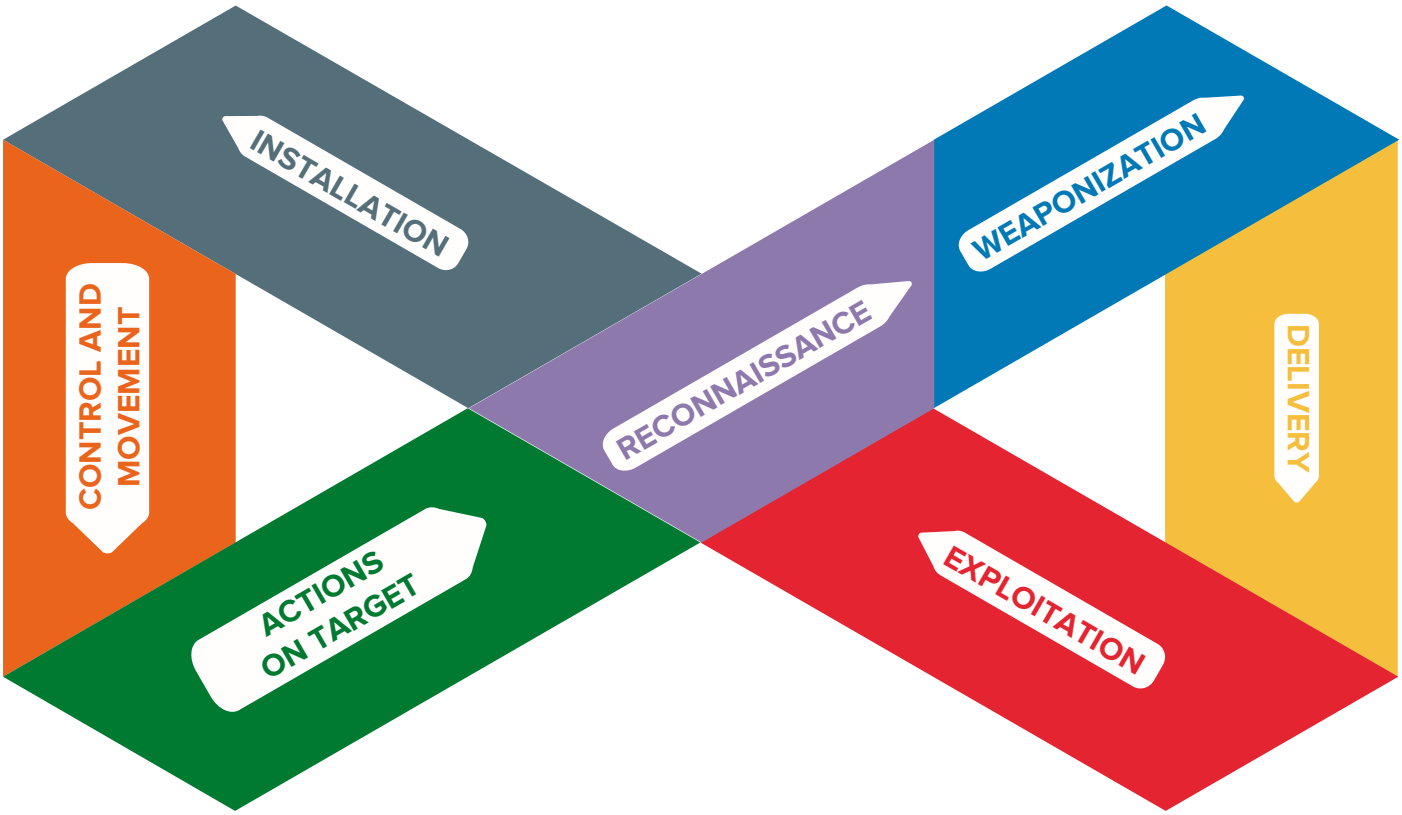
Goal: Move from initially compromised systems to more vulnerable or valuable ones.

This includes lateral movement between internal systems, and continually reusing any increased access obtained to eventually compromise agreed targeted systems.

Actions on target

Goal: Gain access to compromised systems and previously agreed targeted data.

The Red Team strives to complete the engagement and achieve the objectives agreed upon and set by the entity during the scoping and threat intelligence processes.



Preparation
- Set targets, choice of tools
- Collect information about the infrastructure and employees

Gaining access
- Prepare for exploitation
- Gain initial access
- Implant in the system

Data exfiltration
- Open command channel
- Privilege escalation, collection and data exfiltration, removal of traces

Figure 5. **Red Team investigation methodology**

06 CASE STUDIES BY GROUP-IB

CASE 1 STUDY

Gaining access to Active Directory

Customer: Group of companies (manufacturing industry).

Goal: Gain administrative access to the Active Directory domain controller at the company's headquarters.

Situation: The customer uses multi-factor authentication (smart cards) for all types of access at the headquarters, including remote and external services (see Figure 6).

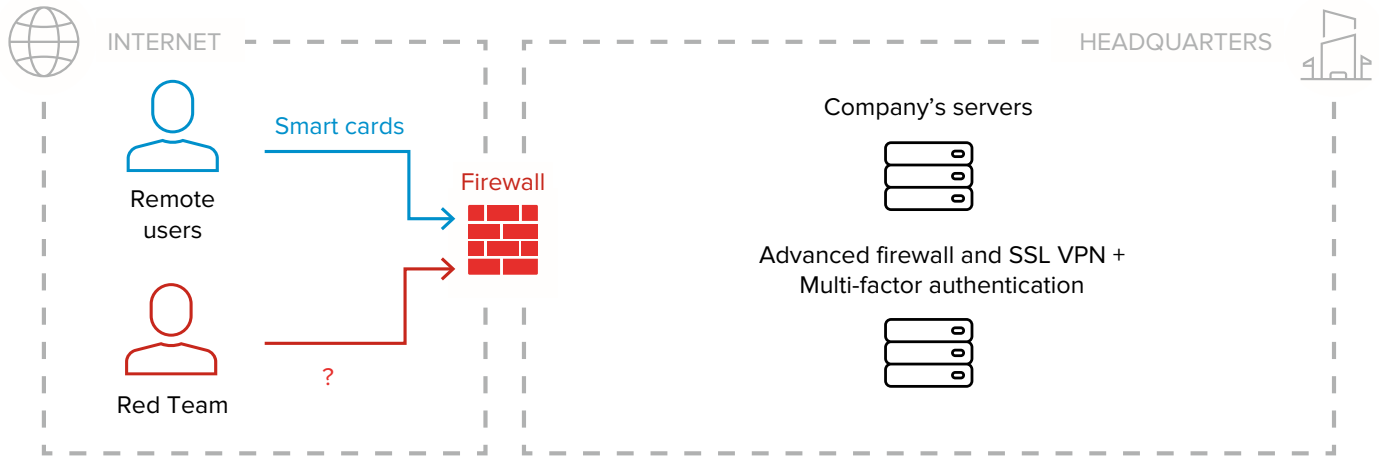


Figure 6. **Manufacturer's infrastructure**

Group-IB's actions and results

Group-IB's reconnaissance revealed that the headquarters had bought 14 companies, which during the Red Teaming operation were being restructured into branch offices. Group-IB's Red Team was given permission to carry out attacks of all the group's companies. A poorly protected subsidiary was then breached, including branch1.domain.com domain controllers, leading to the discovery of a VPN between departments' local networks (site-to-site full-mesh VPN).

The customer had their Active Directory domain forest built for half of their branch offices but did not manage to properly strengthen the external network (Figure 7).

The connection to the network was well protected. The trust mechanisms between the domains in the Active Directory forest did not work for controllers at branch1.domain.com, so the attack was extended to branch2.domain.com, where domain administrator rights were obtained.

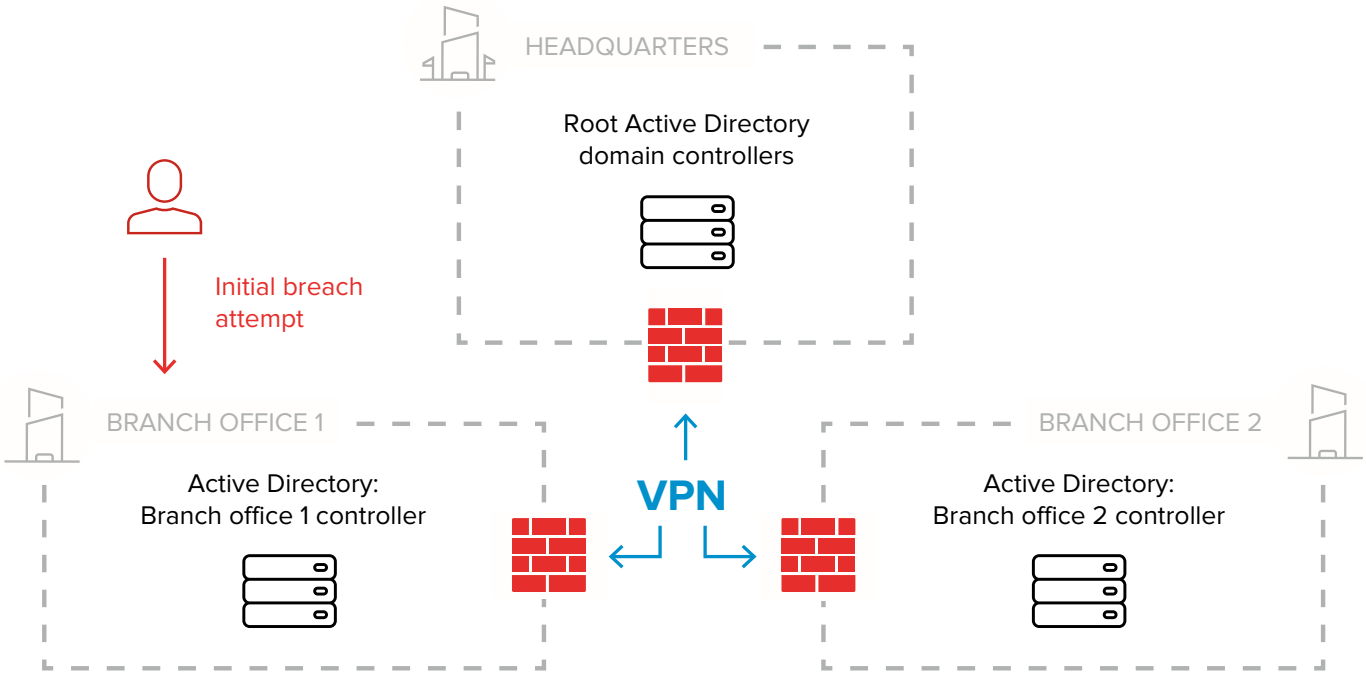


Figure 7. **Initial attempt to breach Active Directory**

The Red Team carried out a Domain Forest-Wide Golden Ticket Kerberos attack and bypassed the smart card protection using the specifics of the Kerberos protocol implementation. By exploiting the trust mechanism between Active Directory domains, the Red Team obtained administrative rights at the headquarters (Figure 8).

The domain controllers at the company's headquarters were breached, meaning that Group-IB's specialists had achieved the goal set for the Red Teaming project.

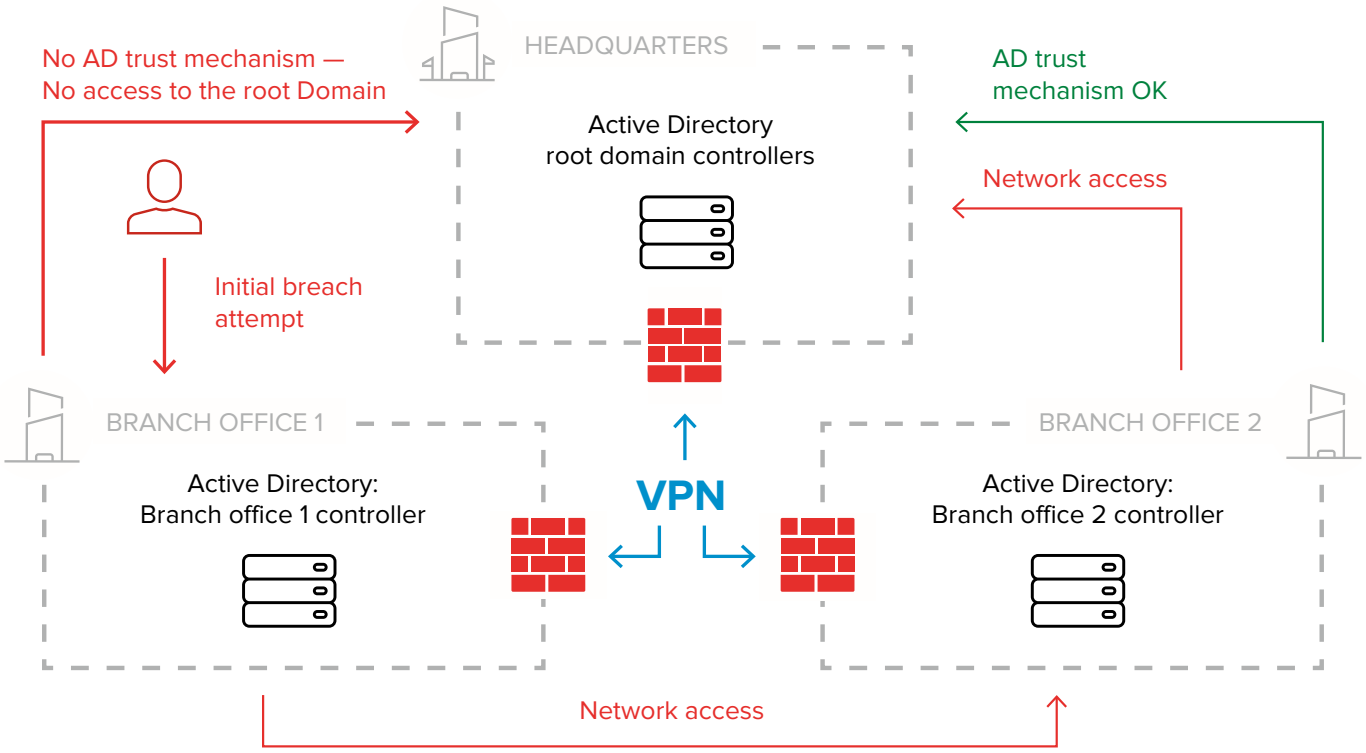


Figure 8. **Gaining access to Active Directory**

CASE 2 STUDY

Gaining access to financial systems

Customer: Major retailer

Goal: Gain access to internal financial systems at the headquarters

Situation: The external perimeter of the headquarters includes several externally accessible servers, which are well protected. Most of the systems are cloud-based and publicly available. Attacks on branch offices are prohibited since the customer considers this an ineffective attack vector. The branch offices are not connected to the information systems of the headquarters (Figure 9).

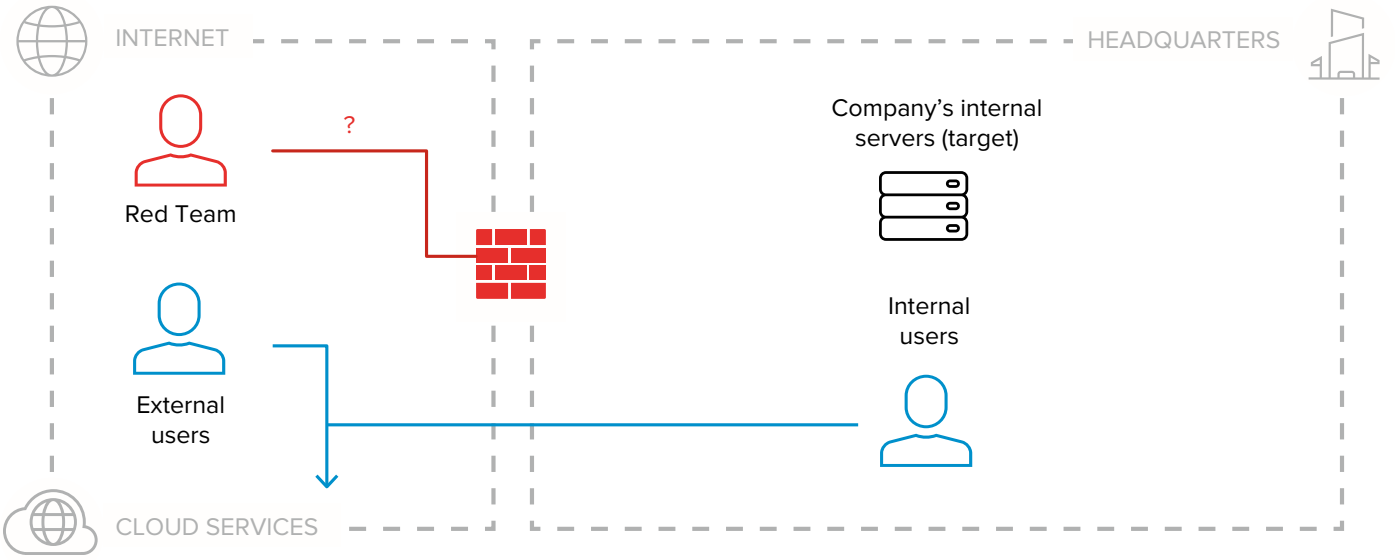


Figure 9. **Retailer's infrastructure**

Group-IB's actions and results

Group-IB's Red Team determined that the server of one of the customer's contractors was mentioned in a DNS SPF record and could send out emails on behalf of the company. This server was not part of any publicly available cloud service and its purpose was unclear. The server had several webpages undergoing development, which were related to the customer, and an OpenVPN TCP port with a non-standard number — the same as that of a server on the customer's external perimeter. This could indirectly indicate a tunnel between the server and the customer's local network. The Red Team identified the owner of the server, contacted them, and obtained official permission to carry out a penetration test in exchange for a free minireport about the security of this server (Figure 10).

Group-IB's Red Team breached the server and discovered that it hosted several systems undergoing development and created for the customer by a subcontractor. The server essentially acted as a testing ground for these services. Moreover, to upload data from the organization's internal systems to this server, the customer had earlier created a VPN tunnel to its local network. The Red Team's initial assumption was confirmed; the team copied the OpenVPN configuration and gained access to the network. The VPN was configured incorrectly: the list of available IP addresses within the customer's network was only limited by routing on the OpenVPN client (Figure 11).

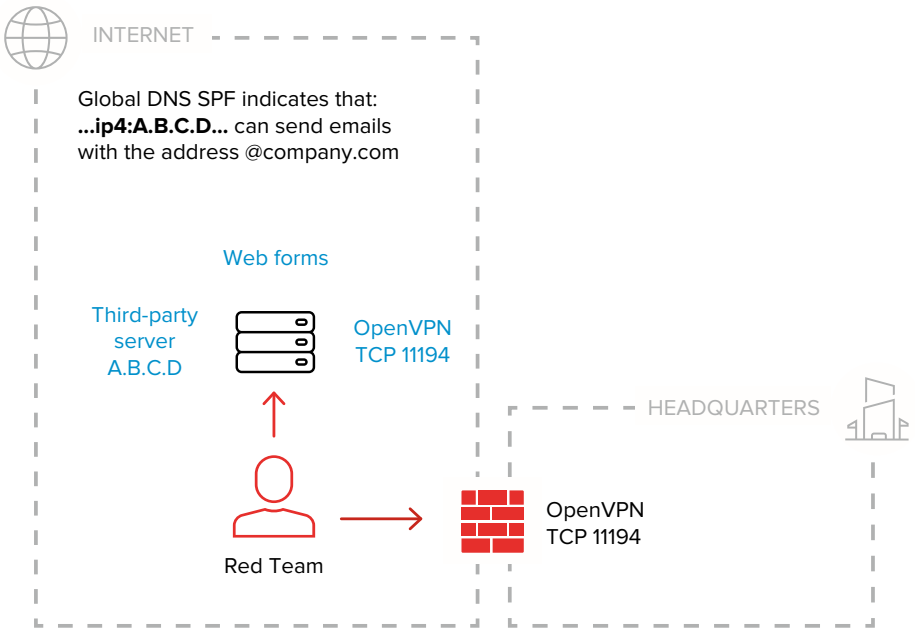


Figure 10. **Contractor's server with an OpenVPN TCP port**

Reconfiguring routing on the client gave the VPN unlimited access to the local network. Once initial access to the local network was gained, the Red Team used traditional methods of attacking Windows-based networks (lateral movement) to obtain Active Directory domain administrative rights and gain access to internal financial systems.

As a result, Group-IB specialists achieved the goal of the Red Teaming project.

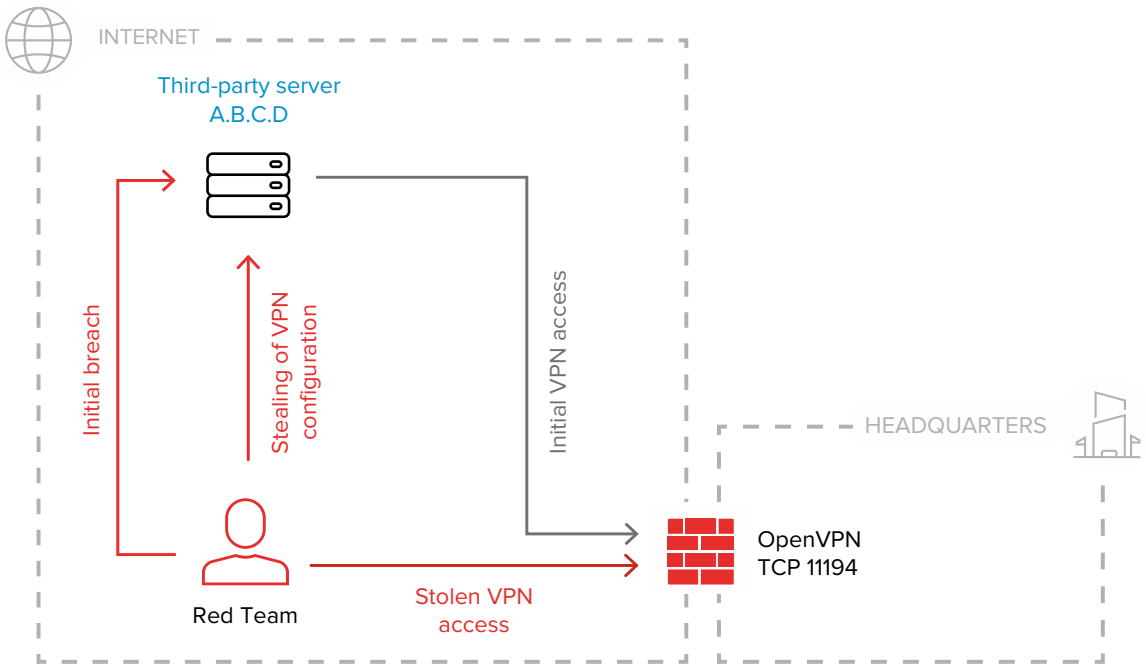


Figure 11. **Gaining unlimited access to the local network**

07 CONCLUSION

Red Teaming gives organizations an idea of their cybersecurity strengths and weaknesses and helps them assess and create a plan for future improvements.

Addressing flaws identified during Red Teaming ensures that business processes are not disrupted and that valuable data remains protected.

Key opportunities offered by Red Teaming are:

- Evaluate cyber risks to the most important assets
- Detect unknown vulnerabilities and weaknesses
- Check whether all security systems and processes are working correctly
- Identify the internal security team's strength and weaknesses
- Improve the ability to respond to cyberattacks
- Increase the staff's digital and physical security

When it comes to cybersecurity, no organization is 100% protected. However, internal security teams can improve their ability to detect previously unnoticed threats and learn how to stop technically competent, resourced and persistent attackers at an early stage by conducting Red Teaming and practicing responding to controlled attacks. This ultimately prevents damage to businesses.

By including Red Teaming as part of their security strategy, companies can measure security improvements over time. The methodology behind Red Teaming helps determine the basic state of security and quantify improvements after a set time frame has passed. What's more, quantifiable results can be used to conduct feasibility studies for additional security projects and introducing necessary technical protection frameworks.

Group-IB is one of the global leaders in detecting and preventing cybercrime and online fraud as well as protecting intellectual property online.

According to Gartner, IDC, and Forrester, Group-IB is one of the key providers of Threat Intelligence in the world, with more than 100,000 profiles of cyber criminals in its database.

Group-IB's clients include top banks and financial organisations, business corporations and transport companies, IT companies and telecommunications service providers, and retail and FMCG brands in more than 60 countries.

65,000+
hours
of response

1,200+
investigations
worldwide

OSCE — Recommended by the Organization for Security and Cooperation in Europe (OSCE)

EUROPOL INTERPOL — Official partner

FIRST TI — CERT-GIB is an accredited member of international communities of security response teams such as FIRST and Trusted Introducer. This means that Group-IB is able to quickly block dangerous online resources worldwide.

Learn more about
Group-IB Red Teaming

group-ib.com/red-teaming
aps@group-ib.com