RED TEAMING

How to identify gaps in your security strategy by thinking like the enemy

context

CONTENTS

context

01

INTRODUCTION

Red teaming forces you to think about your business the way a hacker would

A red team exercise is a simulated, targeted cyber-attack that mirrors the way a hacker works. It reveals how effective your organisation's defences are against an attack and pinpoints the bad practice that leaves you open to a cyber-threat.

Limitations in existing assurance methods, increasingly sophisticated attacks and the introduction of regulations like the Bank of England's CBEST scheme — a framework to test the cyber resilience of UK financial services firms — have increased awareness among companies from every sector.

This guide explains what red teaming is, how to get the most from it and the business benefits it brings.

WHY YOU NEED RED TEAMING:

- → Improved readiness of your organisation
- → Better training for defensive practitioners
- → An opportunity to inspect security performance levels
- → Assess the organisation at all levels, including systems, people and processes

WHAT IS RED TEAMING?

Red teaming targets people, processes and technology

A red team attack plan is informed by your organisation's operations, based on surveillance and research, as well as knowledge of the tactics, techniques and procedures used by real hackers. It provides a holistic and real-world view of what can happen if someone ties the individual risks together into a single coherent cyber-attack.

For example, a security consultancy's threat intelligence team may have seen real-world attackers targeting financial services organisations by abusing configuration flaws in web servers, and through malicious downloads from sector-specific lure websites.

The red team can emulate this attack by performing reconnaissance to determine the target's exposed web presence, and by creating a fake website themed around financial services industry topics known to be of interest to key staff; these sites can then be used to deliver a red team's simulated malware to targeted visitors to the site.

The threat intelligence-led approach has been mandated by regulators, such as the Bank of England's CBEST scheme, as it requires the security testing to be performed in a rigorous way that mirrors the behaviours seen in a real, targeted attack.

An organisation that can endure a comprehensive, threat intelligence-led, red teaming exercise can have greater confidence in its ability to deal with advanced attacks.

RED TEAMING VS. PENETRATION TESTING

Red team exercises mimic a real-life attack against a company to evaluate the effectiveness of its security defences, including people and processes. Penetration testing focuses on identifying as many technical vulnerabilities as possible in a pre-defined IT system that could leave your organisation open to an attack.

03

Penetration testing

A penetration test requires clients to provide the relevant information such as IP addresses to scan or the credentials to access an application. Once a vulnerability is found, a pen tester will usually try to exploit it further and attempt to escalate privileges in order to understand the risk associated with an issue.

The important thing to note is that this is usually done in isolation, avoiding other out-of-scope systems, and therefore doesn't necessarily provide a holistic view on what could be a much larger risk to the organisation.

Red teaming

A red team exercise tests an organisation's entire security defence. It provides a more in-depth view of border protection, employee awareness and how well processes and procedures cope when faced with a real-life attack scenario. It assesses an organisation's capability to detect and respond to these threats.

A red team often starts from a 'no-knowledge' perspective, the same as many real attackers. While red team exercises include penetration testing skills (and tools) the objectives and outcomes can differ. Red teams and penetration tests complement each other, playing a vital role in safeguarding your organisation and keeping you compliant.

04

HOW RED TEAMING WORKS

Red team exercises begin with an analysis of the real-world threats faced by the target organisation. These are used to define a number of scenarios to be covered in the test.

A common scenario is a targeted attack against an organisation from the internet. Here the test would start with a reconnaissance phase using public data such as social media and information available on the internet.

The information gathered is used to plan and deliver a multi-stage attack, identifying assets of interest such as key systems and critical data.

A detailed report provides mitigation advice where vulnerabilities have been identified. This enables you to understand the security risks and to consider what steps can be taken to mitigate these risks.

HOW RED TEAMING WORKS: THE APPROACH

The phases are generally aligned to the kill chain. However, as organisations have different threat profiles these are often dynamic and will be altered as required.

01
RECONNAISSANCE

- OSINT (open source intelligence derived overtly from publicly available sources)
- Social networking
- Email harvesting
- Domain identification

02
STAGING

- Domain registration and set up
- Browser profiling
- Payload creation/ customisation

03
EXPLOITATION

- Phishing campaign
- Attached payload
- Watering hole attack
- Code execution and established presence

04
CONTROL AND MOVEMENT

- Enumerate workstation properties
- Assess patch level
- Bypass security software
- Elevate local privileges
- Enumerate user domain
- Enumerate network shares

05
ACTIONS ON TARGET

- Performed as a risk managed exercise

06
PERSISTENCE AND EGRESS

- Stage data on the workstation
- Exfiltrate data
- Remain active

HOW TO GET MORE FROM A RED TEAM EXERCISE

Red teaming highlights an organisation's exposure to threats. It is not an instant gratification exercise: it is typically a fairly major undertaking and testing usually lasts between 4 and 6 weeks.

05

Mature organisations

Red teaming can be combined with blue teaming to identify whether a detection and response capability is strong or weak.

Mature organisations can combine a red teaming exercise with a test of their defence team. It works like this: if the hackers are the 'red team', then your internal security team are the defensive 'blue team', who will attempt to detect and respond to the red team's activities.

You can support the blue team during the exercise by temporarily embedding into it experts in offensive security testing; these experts will help the defensive team, and assist them in detecting and stopping the red team. This is known as a 'purple team' exercise.

A purple team approach may not be appropriate for every test: when your organisation is attacked your defensive staff will need to detect the incident themselves before calling on specialist advice. However, it helps assess the performance of your organisation's defences, and provide training and direct engagement during the exercise, or feedback to improve detection and response activities. The embedded experts in your defence team can also model the specialist technical services an incident response consultancy would provide in a real security incident.

Purple teaming approaches are recommended: the better your defensive team understand an attacker's actions, the better they can defend against them in the future.

White teaming

White teaming can be useful when trying to model attacks against complex internal systems or assets that are too critical to test safely in a real world attack simulation. White teaming uses a combination of architecture review and interviews with key system owners to identify likely attack paths and test key points in each attack path where the strength of defences in the system is unknown.

Scenario-based exercise

For smaller companies that don't have the resources for a full-scale red teaming exercise, it is possible to do shorter scenario-based red team exercises.

A scenario-based test is a good follow-up to red teaming, as part of a regular programme of testing. For example, instead of repeating a whole red team exercise, a consultancy can then carry out a specific scenario-based test to see whether they have addressed the issue properly.

What do the colours mean? Here's a definition of each one.

Organisations underestimate how much damage can be done just by using information that's available internally on intranets, documents or network drives. So, it's a mistake only to protect the exterior of your systems.

RED TEAM

External or in-house teams who test the effectiveness of a security strategy by simulating a cyber-attack.

BLUE TEAM

Internal security team or a blue team is the 'defence' team — usually staff from the company's Security Operations Centre (SOC) — who are responsible for detecting security breaches.

PURPLE TEAM

Representing a collaborative mix of 'red' and 'blue' teams: your defensive team are strengthened, informed and trained by the security consultancy's offensive experts.

WHITE TEAM

A non-intrusive method of assessing the ability of an organisation to resist attack, working with the client using a range of table-top, interview and penetration testing techniques to identify the various paths that an attacker might take to achieve a threat-targeted objective.

06

THE BUSINESS BENEFITS OF RED TEAMING

The outcome of a red team assessment is evidence of flaws and security weaknesses that have been exploited within your organisation by the red team. These findings can be used to get buy-in from senior staff and to make security improvements across the organisation.

After a red teaming exercise, you will:

- Understand the impact of a security breach
- Discover weaknesses in your development and testing processes
- Collect evidence to justify security spending
- Identify vulnerabilities in applications and systems
- Measure the resilience of your organisation's cyber defence
- Provide a practical training opportunity for SOCs

Post red teaming checklist:

- Action the recommendations from the red team
- Measure the results against KPIs
- Once implemented, repeat the process and improve it
- Then measure KPIs across all red teams to identify performance trends
- Refine your SOC capability until it can deal with an array of attack types and actors
- Remain vigilant!

RED TEAMING: CASE STUDY

Context broke into an organisation's network and gained access to its entire HR database — the process worked like this:

01
The red team trawl social media and work community sites for company employees' information, i.e. names, email addresses, job titles and locations.

02
This knowledge is used to develop a convincing cover story for a targeted phishing email. The email invites the individuals to speak at an alumni event relevant to their job role, details of which can be found in a brochure linked from the email. When accessed, the brochure installs a malicious 'implant' onto the user's computer. This is controlled by Context's servers, and communicates using requests and responses that mimic innocent Gmail traffic.

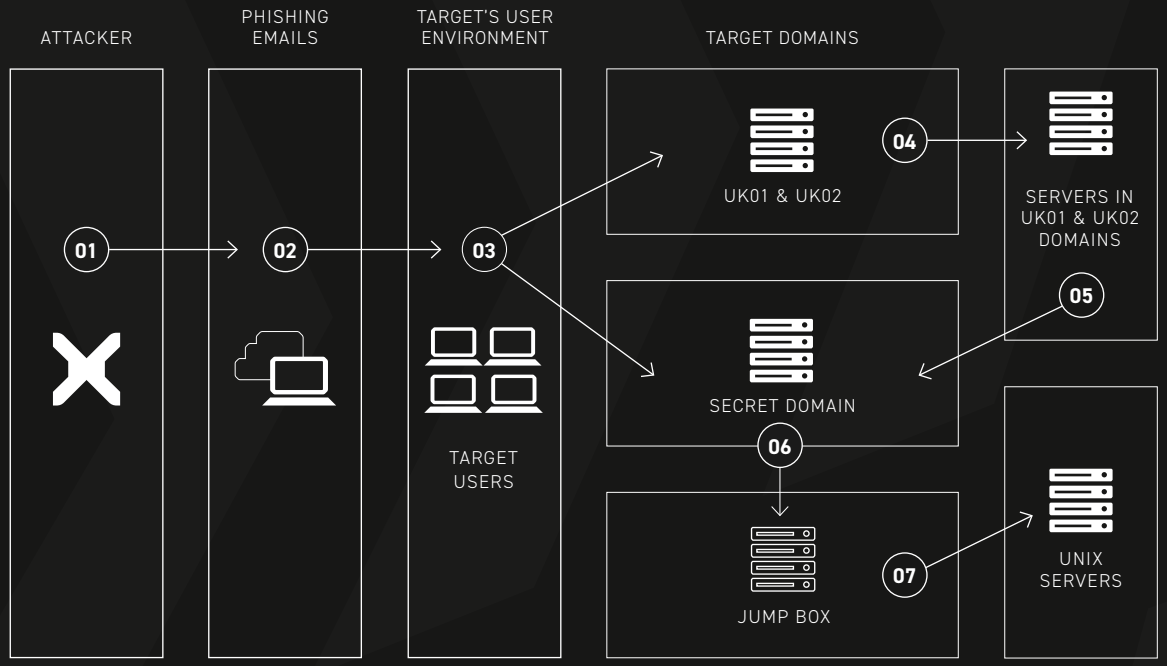
03
Obtain Administrator credentials from world-readable network shares. The red team are now inside the organisation's network and explore for files of interest. They find a custom server-monitoring app which they securely extract back to Context's offices for analysis (with approval). The red team also dump credentials on the target user's computer gaining low privilege access to secret domain systems.

04
User Administrator credentials to access servers in domains. Context analyse the underlying functionality of this software using 'reverse engineering' and uncover hardcoded usernames and passwords, giving the red team access to more servers. From this, they get their hands on top-level domain administrator credentials for the UK01 and UK02 domains.

05
Obtains Domain Administrator credentials to access servers in domains. Using their top level access to the UK01 and UK02 domains, the red team are able to retrieve administrator credentials for the previously discovered secret domain.

06
Obtains passwords for Unix accounts via configuration files on Jump Box. Using the secret domain administrator account, the team access a 'jump box' which is used to access the organisation's segregated UNIX environment.

07
Authenticate to Unix systems using the SSH tools available of Jump Box. The red team gain access to the UNIX environment including an Oracle database which contains HR information. Using the credentials and a configuration flaw, the red team are able to dump the contents of this database and exfiltrate the data out of the network.



The diagram illustrates just one way a red team can attack a major company.

CONCLUSION

Make red teaming part of your organisation's security strategy by assembling an in-house team, or you can hire an outside company **(like Context)** to lead a red teaming exercise.

More advice on how to defend against a cyber-threat:

01 Deploy border controls such as URL reputation filtering / whitelisting with SSL MiTM, and email content filtering

02 Patch everything, especially workstation software

03 Improve user awareness, particularly around reporting suspicious emails

04 Develop capability to respond to alerts e.g. anti-virus or traffic monitoring

05 Restrict and minimise use of domain admin and privileged accounts

06 Audit password quality e.g. ensuring default passwords are not used and lifetime of passwords

07 Segregate systems where possible

08 Restrict access to network shares, and monitor shares for sensitive information

"Red teaming is not a better planning process; it is a process that makes your plans better."

B Hoffman

Talk to us now about our red teaming exercises and penetration testing.

GET IN TOUCH

info@contextis.com
www.contextis.com

context