RED TEAMING

Secura

Secura delivers world-class security services. One of our most sophisticated services, and the service with the highest value to the overall security of our customers, is Red Teaming. Secura brings extensive penetration testing experience and many years of Red Teaming experience to our Red Teaming offering, combined with many other skills and capabilities.

IN CONTROL WITH SECURA

Secura has worked in information security and privacy for nearly two decades. This is why we uniquely understand the challenges that you face like no one else and would be delighted to help you address your information security matters efficiently and thoroughly. We work in the areas of people, processes and technology. For our customers we offer a range of security testing services varying in depth and scope.

RED TEAMING

Security in 2018 is a wide, wild landscape. With a large number of risks that belong to the category of 'unknown unknowns' and pushed by sophisticated cybercriminals and nation state threat actors, companies and states are combatting an ongoing flood of attacks. Dealing with such events requires more than a dedicated Security Operations Center (SOC), it requires hands-on training and learning by doing. An increasingly popular way of testing and training in a controlled way is 'Red Teaming'.

BACKGROUND

Originating in the military arena, Red Teaming is a security discipline that is gaining popularity in all sectors of critical national functions, the financial sector, highly secured private companies and governments. By simulating full-spectrum cyber attacks, defenders get to practice their detection and mitigation skills in a managed and measurable way. If you want to know how good you are at detecting spearphishing attacks by sophisticated cybercrime actors, or whether your detection capabilities are indeed seeing Advanced Persistent Threats (APT's), then there really is only one way to know, and that is to test these processes by actually performing these attacks like a malicious attacker would. The Blue Team, responsible for defending, can be involved in various ways (or not at all). The White Team (the observers) can escalate and de-escalate when necessary.

SECURA'S OFFERING

Secura has more than a decade of experience in the execution of Red Teaming projects. We offer four flavours of Red teaming, that are appropriate for all sectors and budgets. We will gladly walk you through these variants and select the appropriate one.

From the perspective of client being red-teamed, a simulated full-scope cyber attack needs to be managed in a controlled way. The reasons are obvious: handling risks around reputation damage and additional attack surface are non-negligible. From setting up communication channels to defining (de-)escalation paths and working with the 'white team': careful realism and preparation are key.

Other important factors are attribution and OPSEC. Concerning attribution, it is key to provide fast and clear insight on whether the RT party is responsible for reported incidents or an actual attack is taking place. It is highly likely that throughout the exercise, real attacks are performed by actual cybercriminals. The white team must be able to contact the red team 24/7 and find out if it was actually Secura that performed a detected attack. Additionally, our own operations security (OPSEC) always has our attention: we are dealing with sensitive files and privileged access to our customers' infrastructure, applications and data. Managing our own security during an engagement is therefore a generic critical success factor and therefore we have set up dedicated infrastructure for each Red Teaming assignment.

PLANNING AND PREPARATION

Managing the process starts with planning and careful preparation. At Secura, we take this phase very seriously. A dedicated project manager works together with the Red Team lead and the White Team to create a schedule and a dedicated set of rules of engagement. Throughout the engagement, this schedule is followed (you can see a sample below), and adjusted where necessary. Risks and scenarios are assessed ongoing.

In between by the Planning (& Preparation) and Clean Closure project steps as described above, lies the heart of any Red Teaming process: the 'attack chain'. These are the steps and activities that lead us to actual compromise, and from there, to the crown jewels that we are after. With near-military precision, we execute our playbooks, leverage any access we gain, moving sideways through the network while elevating privileges until we gain access to the desired goals, after which we exfiltrate (data) or execute (transactions). Red teaming is like playing chess. We carefully put our pieces on the board, performing multiple and layered attacks, while protecting our king (hiding our presence). Below we will take you through each step.

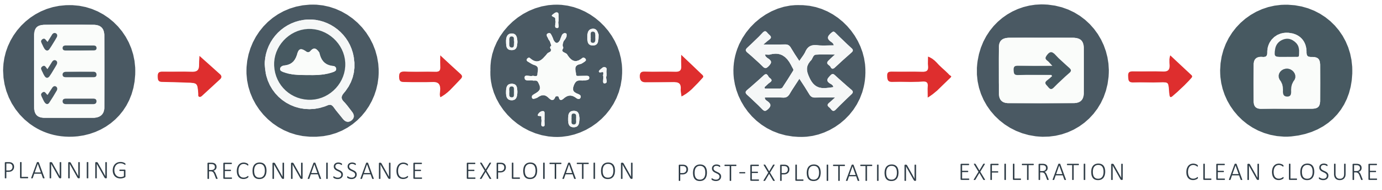
RECONNAISSANCE

An important objective is to emulate realistic scenarios, using techniques and methods exactly like those used by real attackers. This is where the 'Threat Intel' comes into play.

SECURA'S FOUR FLAVORS OF RED TEAMING

TRADITIONAL RED TEAMING	• Red Team is free to choose scenarios (within ethical and legal boundaries). • RT exercise is known to upper management/board/CISO only.
PURPLE TEAMING	• Co-operation of red and blue team (hence purple), to maximise knowledge exchange. • Red Team attacks, while blue team observes, learns and provides direct feedback.
THREAT INTEL BASED	• Emulating known attacks and modus operandi of threat actors. • (Similar) Threats are replayed and detection capabilities are tested.
RED CELL ATTACKS	• Separate 'menu'-selectable attacks and scopes, such as social engineering, physical attacks, WiFi attacks, Open Source Intel gathering, phishing, pentests and many more. • Limited scope and budget.

SECURA'S RED TEAM ATTACK CHAIN



PLANNING → RECONNAISSANCE → EXPLOITATION → POST-EXPLOITATION → EXFILTRATION → CLEAN CLOSURE

If an attacker were to see your organisation as a target, and wanted to learn as much as possible about your internal processes, infrastructure and data, what could they find out? Any Red Teaming strategy starts with an information position, and the better the position, the better the strategy. A lot can be found out about a company and its employees by using Open Source Intelligence (OSINT) sources. People divulge a lot of information on social media and websites such as LinkedIn, Twitter and Facebook, but also on technical forums such as StackOverflow, Tweakers and others.

If, at a later stage, a scenario that includes physical access will be played out (for instance placing a rogue device in the network), then we will need to know how to get in to the offices of the target. Simple physical reconnaissance is therefore often required to find out things like what physical security measures are in place.

Phishing can also be used as a reconnaissance method, since people who read the phishing mail or click on links contained in them, disclose a lot of information about IP addresses, software versions, browser configuration and operating systems used. Everything combined, there is a wealth of information that can aid an attacker (and the red team) in their attacks.

EXPLOITATION

Delivering a malicious payload into the target network can take many forms but currently the easiest and very efficient is, again, (spear)phishing. It can be used to harvest credentials for core applications, but also deliver malware directly. Delivery of a payload can however also be done through a physical USB device, rogue network device, or compromised laptop. In all cases, the delivery leads to the following step: exploitation of a vulnerability to gain a foothold.

Ultimately though, it is the detectability (by the blue team) of this step that is key. Early on in the engagement, we will deploy the most stealthy scenarios. The more noisy attacks with a higher detection probability are only executed later on in the exercise. This is to maximize blue team training and identify what “attack level” the blue actually detects. Alerting the blue team cannot be undone: once they are actively threat hunting, subsequent attacks have a higher chance of also being detected. This build-up in attacks is often seen by our clients as an unique advantage of our approach to Red Teaming, as it supports the learning curve for the blue team.

POST-EXPLOITATION

Gaining a foothold is achieved by successfully delivering an exploit, not being detected, and executing that exploit. This usually leads to a compromised system in the network of the target. The compromise itself can take the form of an installation of our own piece of custom ‘controlled malware’.

Moving through the network, closer and closer towards the crown jewels, we pivot through the network, jumping from one server with certain access rights to another with more privileges. Gaining domain administrator rights in a Windows network is usually the last step before access to the crown jewels can be achieved.

EXFILTRATION

Once the crown jewels (or anything else interesting such as captured network traffic, the database of domain password hashes, or exchange email server database) have been reached, it is time to exfiltrate this data. This tests detection capabilities on out-bound traffic and detection of transfer of funds (as well as capabilities to respond to these actions). When this has been achieved, the attack chain has been fulfilled.

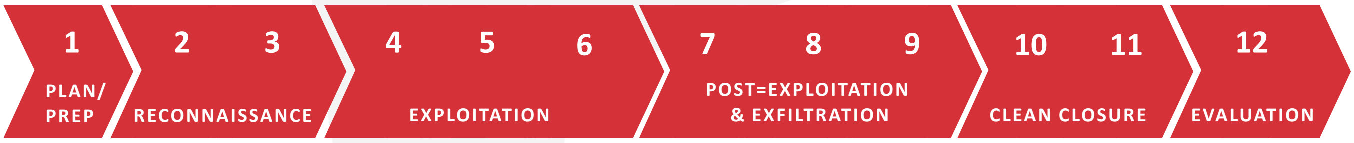
CLEAN CLOSURE

Clean closure does not only mean managing the leftover digital remnants of the executed attacks. It also means providing the blue team with one or more evaluation sessions where the full timeline is replayed in a workshop, which maximize learning and awareness. The clean closure and evaluation also contain a detailed report and our perspective on your overall security maturity in your threat landscape.

SAMPLE TIMELINE

Generally Red Teaming execution takes place over several months. Below you find a sample of the phasing with indicative week numbers and commonly used check points.

WEEK NUMBER



CHECK POINTS

SUCCESS

When is a Red Teaming exercise a success? Some would say "when the crown jewels or flags have been reached without being detected by the blue team". However, this definition also implies that the blue team will have learned little. On the other hand, it means that a plausible and realistic attack path has been exposed, that can now be closed or mitigated. We consider it a success when the Red Team has had a proper challenge, yet identified many new attack paths or unknown vulnerabilities requiring solutions. In the end, you will know your systemic cyber risks, and will be capable of mitigating them. This is the ultimate goal of Red Teaming.

Secura's experience in red teaming, combined with our capabilities, passion and sector-specific experience, provides our customers with the best possible basis for the clean, solid execution and management of Red Teaming engagements.

RELATED SERVICES

Secura provides a full spectrum of security services. Typically, our customers have more needs than just Red Teaming services. Related services that Secura offers are for instance:

- **Vulnerability Analysis and Penetration Testing**: with a more focused scope, Secura can investigate specific applications, infrastructures and networks. Using the mindset of a hacker, we identify vulnerabilities and provide remediation advice.
- **Mobile App testing**: Mobile apps these days are an integral parts of our lives. When testing the security of apps, we do not just look at the app, but at the full chain, from user, through device, frameworks, resources, network and back-end server.
- **Source code analysis**: When testing an application, we can investigate the important parts of the source code. But it is also possible to take an automated look at the source code. This will provide you with not only security vulnerabilities, but also a view on code quality, maintainability and readability.
- **Continuous Application Scanning**: In modern development environments, a bi-weekly release schedule is common. In those cases, in-depth manual testing is not always feasible, both time-wise and budget-wise. Nevertheless we can offer an extremely valuable automated, periodic scanning service for on-line applications where we use state-of-the-art application vulnerability scanners, combined with our human experience to provide a periodic report with technical security findings and trend analyses.

INTERESTED?
Would you like to learn more about our services?
Please do not hesitate to contact us.

Follow us on

Vestdijk 59
5611 CA Eindhoven
Netherlands

Karspeldreef 8
1101 CJ Amsterdam
Netherlands

T +31 (0)40 23 77 990
E info@secura.com
W www.secura.com