Claranet Cyber Security – Service Description Document

Red Team Assessment

Service Description

Version 1.1

claranet cyber security®

Table of Contents

Non-disclosure Statement

This document and all written advice and materials provided by NotSoSecure Global Services Limited ("NotSoSecure") are the intellectual property of NotSoSecure.

The client may use these materials freely for its own business purposes, but may not distribute or reproduce this document, in whole or in part, or otherwise supply it for use by any third party, without the prior written consent of NotSoSecure.

NotSoSecure owns all intellectual property rights, including copyright, trade secrets, know-how and methodologies, in everything developed by NotSoSecure for the client, in whatever form and regardless of when such rights came into existence.

NotSoSecure appreciates your co-operation in protecting its intellectual property.

Legal Notice

While every precaution has been taken in the preparation of this document, NotSoSecure assumes no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein. Use of NotSoSecure's services cannot guarantee 100% security of a system, or that computer intrusions will not occur.

Version Information

Version	Date	Author	Comments
0.1	06/12/2022	Karun J. Thomas	Initial Draft
0.2	06/12/2022	Ajay Prashar	Technical Review
0.3	06/12/2022	Karun J. Thomas	Amendments
0.4			Quality Assessment
1.0			Final Document

Service Overview

A Red Team assessment is an all-out covert exercise to achieve the defined objectives by any methods available, over a prolonged period of time. Red Team exercises are performed using a black-box testing approach where no prior information about the target organization is given. During a Red Team engagement, the defending side is unaware of the exercise and is expected to respond as it would during a genuine attack. Red Team assessments usually includes social-engineering attacks (such as phishing and vishing), compromising external and internal assets, but also includes compromising wireless networks and assessing physical boundaries and controls.

The trophies for each assessment are tailored to the customer's learning objectives and their business-critical assets/crown jewels. However, the following objectives are commonly defined for this type of assessment:

Objectives
• Foothold: Standard user access (shell / GUI) gained from outside
• Privilege Escalation: Administrative user privileges gained
• Defence Evasion: Evade and remain undetected from external/internal security alerting systems
• Persistence: Remote access is not being dependent on a single user account or a single device

• Lateral Movement: Traversal to multiple points on a network
  ○ *Discovery*
  ○ *Credential Access*

• Full Compromise: Domain / Enterprise Admin account or equivalent compromised

• Collection: Action on trophies:
  ○ *Sensitive File Access: Contents of a specific file located in sensitive location is exposed*
  ○ *Privileged Access to a sensitive network share or server*
  ○ *PII Data Access: Broad access gained to data held in any internal HR/Finance systems*

• Exfiltration: Covert data exfiltration of sensitive data outside the customer's network

Assessment Scope

During the initial Scoping phase an experienced security consultant will work closely with you to create a service suited to your specific requirements and agree the scope of work. You may have a clear idea of this already or we can use our extensive experience to help you find the right scope. It may be driven by compliance requirements, best practices, visibility, awareness or a combination of all.

Initial discussions

During this stage, we will discuss the challenges and requirements you have and how the test can assist in meeting these. Your engagement will be technically scoped by an experienced consultant, carefully mapping the target to ensure that the agreed attack surface can be covered during the engagement and that the results are comprehensive within a critical timescale.

As part of a collaborative goal-based discussion between NotSoSecure and the client, a call or meeting will be arranged to discuss the relevant Tactics, Techniques and Procedures (TTP's) to be utilised by NotSoSecure when mimicking Adversarial Actors (e.g. "script kiddies", hacktivists, organised crime, nation-state/state-sponsored attackers) and which Threat Models/techniques should be used per kill-chain stage (following the MITRE ATT&CK Methodology),

We define the White Team\Need-to-Know Team, which usually includes the CISO and other pertinent individuals from security audit teams, the Security Operations Center (SOC) manager and the building owner/manager (if physical intrusion is in scope). A Point of Contact (POC) is defined, who will interface with the Red Team, ideally, the SOC manager. The POC's job is to communicate with the Red Team via email/text/phone, perform internal deconfliction if necessary, and inform the defensive team of an ongoing engagement when the time is correct.

Scoping Document

The Scoping Document will allow for a defined Statement of Work (SOW) to be produced along with a prescription of the number of days the engagement will take to complete. Most Red Team assessments can be defined by a set of trophies and learning objectives. These will form the basis of the Scoping Document, which will include:

- Identify the drivers and goals for the assessment
- Cover all crown-jewels, enterprise-wide that require assessment
- Detail any exclusions

Areas commonly considered during the scoping will include:

- Network infrastructure, web & mobile applications
- Routers, switches, laptops, workstations and other devices
- People and processes
- Physical infrastructure & Wireless networks

Statement of Work

Once the Scoping Document has been completed, the consultant will examine the information provided and apply a rigorous and consistent approach to ensure that sufficient time is allocated to the engagement to meet the objectives; the result of this exercise is the Statement of Work. Where it is not possible to complete a Statement of Work from the Scoping Document or the information available at the time of scoping, a statement of requirements can be defined, and time-based tests can be conducted. However, these may result in an incomplete or inconsistent assessment of the target and require careful consideration and agreement to ensure that expectations are met while maintaining the quality of the service provided.

Recommendation

NotSoSecure will make recommendations regarding the structure of your assessment and return a Statement of Work to you. Engagements will be defined by the type and complexity of the target(s), their location (standard testing is delivered remotely unless there is a technical reason why the test should be delivered onsite), and the duration of the engagement defined by how many days a tester will need to complete the assessment based on the appropriate NotSoSecure methodology for each target. A quote, or proposal document where appropriate, will be provided defining the costs, including any expenses, of the exercise. A sales order form will be produced as a final document for signature.

Methodology

NotSoSecure follows an eight-stage cyber-attack lifecycle, coupled with the MITRE ATT&CK framework, as shown in Figure 1:

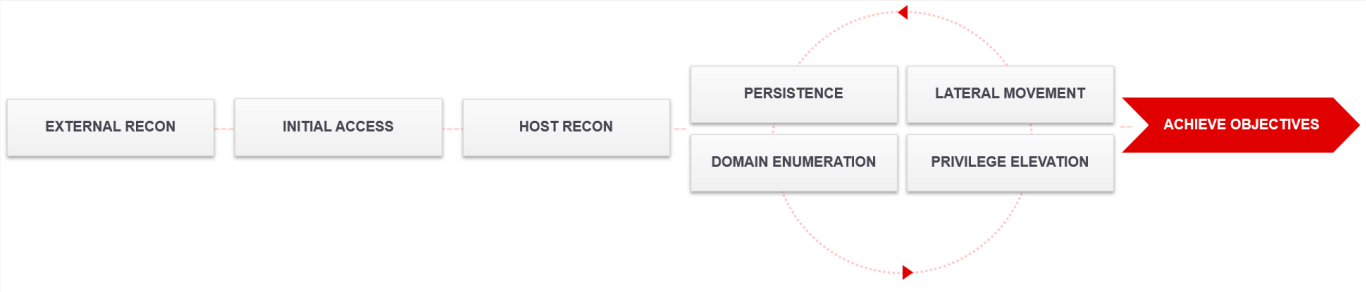

Figure 1: Red Team Assessment Methodology

During the testing, our consultants will be on-hand to directly discuss any issues and update you on the progress. Any high priority findings will be flagged to you daily.

Phase 1: Planning and Information Gathering

The assessment commences with an "Attack Surface Appraisal" that uses OSINT techniques to determine the "external footprint" of the target. In concrete terms, this comes down to "What is known about the customer from public sources". This can be done from different angles such as identifying the target's network infrastructure (IPs, subdomains, technology etc.), profile security solutions and other protections used internally, harvesting employee information, information which can be found on the dark web (compromised accounts, vulnerabilities) and more. This information is ultimately useful for, among other things, specific spear-phishing campaigns, manipulation, and aid in the success of an attack. By performing an "Attack Surface Appraisal" you get an idea about what adversaries can find about you. It also provides insight into what information can be misused and where the risk lies. The smaller the footprint, the less information is disclosed that can be misused or manipulated.

NotSoSecure develops a customised scenario plan mapped against the MITRE ATT&CK framework for Phase 2. Based on the intel gathered, NotSoSecure registers phishing websites, stands up phishing infrastructure and creates plausible spear-phishing pretexts or other methods of delivering a payload to the customer. NotSoSecure deploys covert command-and-control infrastructure, often using the same technology or cloud service providers used by the customer, in an attempt to 'blend-in'.

Phase 2: Assessment Execution

NotSoSecure attempts to gain initial access to the target environment by scanning and probing internet facing IP address space used by the client, seeking out systems for exploiting misconfigurations or vulnerabilities in exposed applications, spraying weak credentials on authentication portals or conducting novel social engineering attacks to compromise an end-user's workstation. This process can range from broad targeting, through to specific interactions e.g., targeting HR staff via job application portals.

Following initial access, we perform situational awareness including host controls, user profiling, enumeration of defensive products and capabilities. We may transfer tools and install backdoors on the beachhead host to maintain persistent access to the environment.

In the event, NotSoSecure is unable to breach the external perimeter, the engagement follows an assumed-breach model. In this case, the Point-of-Contact would choose an end-user known as a 'trusted insider', who will cooperate with the Red Team. This may include clicking links, opening attachments, executing payloads, or even screen sharing. Typically, this would be an individual who doesn't work in a group that might have elevated permissions, but somebody that might see a lot of exposure in terms of emails and phishing, such as sales, HR, or legal departments.

Activities in this phase would be driven by the pre-defined scenarios. The aim is to pivot within the network from a single compromised machine or access point to control multiple systems and ultimately demonstrate control over or access to crown-jewel targets through any non-disruptive means necessary.

We attempt to enumerate the internal environment via domain and admin enumeration, to identify important systems and users. Attacking a network is complex and often involves multiple steps, such as harvesting credentials from memory or exposed network shares and document management systems, exploitation of weaknesses within Active Directory or misconfigured network services. Attack techniques are tailored to the client's environment, such that we blend in with normal user behaviour and network traffic to remain under the radar of the defenders. Gaining Domain Admin privileges is not a necessity unless explicitly defined as a goal. Once access to the objectives has been achieved, we take the appropriate level of evidence.

We will closely monitor and assess the impact of each technique we execute in the environment along with the techniques that get detected as well. The team will document the results and guidance around the detection of techniques that go undetected.

The engagement may end at this point, or we may choose to provide leads to the defenders to gauge their detection threshold.

Phase 3: Reporting

Key to the above exercise is concise reporting as this will help you with your remediation activity. This part of the project will draw together all the results and findings and we will document this in a comprehensive report that will also be designed to tell a story about how we went about the test and the associated findings along with lessons learned. We write in this style so that the journey can be shared with the customer's Tech or Exec audience alike. Thus, whilst it will be a professionally constructed report, it will document and depict how we were able to break into Applications and Networks, access data etc., where possible. The detailed report contains both tactical and strategic recommendations which allow you to prioritise actions to improve your security. We can join you on a debrief call to walk through your findings.

At a high-level, the report includes:

- **Executive summary**: This provides a high-level summary of the strengths and weaknesses of the customer's security posture. The results are provided in context. (e.g. in order to exploit this vulnerability a hacker would have to be connected to the internal system). This section includes any constraints and restrictions of the test.
- **Graphical summary**: This provides a graphical view of the number of high, medium and low rated vulnerabilities measured against risk categories or impact and probability.
- **Attack narrative:** This provides a walkthrough from the Red Teamer's perspective (chronological timeline of the attack) highlighting the key actions taken in achieving the objectives, what access was yielded as a result, and where any detection or defensive decisions were introduced.
- **Detailed findings:** The technical reporting is presented in order of risk. Full details are provided which include: Business impact, affected assets, exploitation path and evidences. We will document recommendations for the internal security team in a manner so that they can learn from the attack approaches and incorporate them in their defenses.

Phase 4: Lessons Learnt, and Training (Optional)

Building on the overall assessment, its learnings (for both NotSoSecure and client's internal security team) and NotSoSecure's training programs, we will provide custom workshops for the internal teams in the last phase of the engagement so that they understand the attacker tradecraft better and are better prepared to detect and respond to attacks in future as a result improving the overall security maturity of the client.

An example training will be - In case we are able to compromise Active Directory inside the client's network, we would deliver a session which will provide a walkthrough of our attacks and their corresponding logs and data sources to detect them.

Phase 5: Retesting (Optional)

Following a period of remediation, there may be a requirement for retesting of the vulnerabilities found, to validate that the fixes have been successful in addressing the risk. NotSoSecure will encourage internal detection and response teams to be present and participate with us when performing the tests. A purple team engagement consists of joint exercises between the red and blue teams to test, measure and improve the organisation's overall ability to detect and/or prevent threat actors. This is a chargeable exercise and will be discussed at the Scope stage. Once the results from the initial test are identified, this can be discussed again in order to determine the potential benefit and timescales. Where remote testing has been delivered, it will be possible to organise cost-effective retesting of the target infrastructure to validate the remediation.

A: Handling of Sensitive Data

Part of the objective of a Red Team exercise is to assess the risk to sensitive information or to compromise high-value digital assets. Contact with potentially sensitive information is common and therefore will be managed accordingly.

Validating the presence of a vulnerability ensures accuracy in the reported results of a Penetration Test. Proving that a vulnerability exists within the systems containing sensitive data is achieved in a number of ways, for example; obtaining screenshots of database schemas and file permissions, or displaying files without displaying the contents.

Consultants will act in accordance with the Claranet Cyber Security practice for handling of your sensitive data and general best business practice. Consultants will, where possible, avoid coming into the possession of Personally Identifiable Information

B: About Us

About Claranet Cyber Security

Claranet Cyber Security is Claranet's dedicated security division committed to helping organisations develop their security posture and build resilience in the face of changing cyber risk. In the never-ending race to keep up with new threats and secure new technologies, we help you make modern happen.

We ask the right questions to uncover the rationale for change behind your security requirements, identifying your business drivers, people and process challenges, and critical threats. This leads us to the solution you really need – something flexible, scalable, and outcome-driven.

Our capabilities span continuous offensive security, SOC-enabled cyber defence, risk consultancy, and training, all of which are underpinned by a 25-year pedigree in penetration testing.

About Claranet

With £325 million in revenue, over 6,500 customers and more than 2,000 employees based in 24 offices and 43 data centres across seven European countries and Brazil, Claranet is an award-winning Managed Service Provider. The company has a reputation for technical innovation and excellence and is one of only a few MSPs to achieve the highest partner accreditation status with AWS, Google, and Microsoft.