Red Queen Security, LLC

901 N. Pennsylvania St
Denver, CO 80203

Service Catalog

Updated April 30, 2021

Executive Overview

This document outlines the standard services provided by Red Queen Security, LLC. Our primary focus are **assessment services** which focus on evaluation and testing of people, products, policies, procedures and technology. They include things like vulnerability assessments and penetration tests.

In addition to the specific services we offer, this document also defines certain terms and aspects of our services such as Rules of Engagement, Visibility levels, and on-site versus remote considerations.

Inquiries may also be made directly for non-standard or modified services not covered within this catalog. Please direct such inquiries to proposals@rqsecurity.io

Assessment Services

We offer 4 distinct assessment services, each serving a specific goal:

- Vulnerability Assessment/Scan (VA)
- Web Application Assessment (WebApp)
- Penetration Test (PenTest)
- Adversary Emulation (Red and Purple Teams)

Every assessment service includes specific *Rules of Engagement*, or ROE, that tailor how the assessment will be executed, where (both logically and geographically) it will be executed, and what will be considered “in scope” during testing. Additionally, clients will also be able to choose how much visibility we will receive before and during the assessment, commonly referred to as White/Grey/Black Box assessments, or Full Knowledge/Partial Knowledge/No Knowledge, respectively.

Rules of Engagement

The rules of an engagement are specific to each assessment and can be 100% customized to a client's needs. The following are the bare minimum rules that must be explicitly allowed or denied for every assessment:

- Code Execution
- Phishing
- Social Engineering
- Denial of Service (DoS)

Please note that these rules of engagement **do not** affect price, *however*, if extremely prohibitive rules are placed on an assessment, the quality of the work will suffer. For instance, if all work is required to be done during a 4 hour per day testing window with only one week to conduct the assessment, the report may not adequately reflect the true risk to your network, simply due to time constraints. We will advise and recommend alternative solutions should a desired rule present possible danger to the quality of your assessment.

Code Execution

Code execution is **only optional for Vulnerability Assessments**. All other assessment types fundamentally include code execution in some manner. Please note that you have great flexibility here with how you allow code execution on your systems. For example, you can require specific working hours, restrict it to specific systems or applications, or require prior consent per execution or at any juncture in an assessment. There are an indefinite amount of conditionals you may place on this rule to ensure proper business operations are not disrupted. Even without specific mention in an ROE document, and unless specifically told otherwise, we will seek consent for any action that has a reasonable chance of disrupting your network.

Phishing

Phishing is **required for Red Team Assessments** and **not applicable** to vulnerability or web application assessments**.** Phishing can include simple spam-like phishing to very tailored spear phishing of individual targets based on open source intelligence (OSINT) of their likes and behaviours.

Unless specifically requested, phishing provided by Red Queen Security is not a metrics-based assessment and will include code execution and/or post-exploitation operations.

Social Engineering

Social engineering (or SE) is **not applicable** to vulnerability or web application assessments.

SE is intentionally separated from phishing to distinguish between simple phishing and more tailored targeting of humans such as phone calls and in-person interactions.

Denial of Service (DoS)

Generally **not recommended**. This is typically only allowed if a client would like to test specific protections they have incorporated to prevent denial of service or distributed denial of service to a core business function.

Visibility

No Knowledge (Black Box)

No knowledge assessments, sometimes referred to as “black box” assessments, may be preferred by a company’s security team for their perceived realism. However, they can be expensive due to the longer intelligence gathering phase and may not identify certain vulnerabilities that would otherwise be detected with more knowledge. This assessment focuses on “low hanging fruit” and the path of least resistance into your network. They are generally not recommended if you have something very specific you wish to test, as it may not even be seen in this type of assessment.

Full Knowledge (White/Crystal Box)

The opposite of a no knowledge assessment, this type of assessment visibility means full knowledge of the test environment. As much information as possible should be provided to better explain the business context of what is being tested. This can often include source code, network maps, network space, domains, etc. This is generally the recommended approach for web applications, very sensitive environments such as SCADA/ICS[1], or very business critical devices/applications.

Partial Knowledge (Grey Box)

Generally the preferred compromise between full knowledge/white box and no knowledge/black box. In this type of assessment, a limited set of information is provided. For example, the specific targets or network space you wish to test, employee email addresses, domains, and other aspects of what is referred to as the scope of an assessment.

[1] Supervisory control and data acquisition (SCADA)/industrial control system (ICS) is a system of software and hardware elements often utilized by industrial organizations.

Vulnerability Assessment

Vulnerability assessments evaluate given networks with a focus on identifying vulnerabilities that are then categorized as Critical, High, Medium, Low, or Informational. If *code execution* is allowed in the *Rules of Engagement* (or ROE), we will also manually verify findings when safely possible to reduce false positives. If a finding could not be safely verified, the reasons will be noted in the report (e.g., the vulnerability was a *denial of service* and such testing was not explicitly approved).

Note that this is different from a Penetration Test in several key aspects:

- Even with *Code Execution,* we will stop after confirming the vulnerability. Further impact of that vulnerability or how vulnerabilities could be chained together is not tested and thus the full risk and impact may not be discovered.
- Vulnerabilities that are specific to business context cannot be found by a vulnerability scanner. *For example*: a scanner often doesn't know that a public page on your website contains sensitive information to your business.
- Tactics and techniques specific to post-exploitation are not tested. For instance, vulnerability scans cannot identify how susceptible your network is to lateral movement techniques.

Vulnerability assessments are ideal for organizations wanting an initial and/or periodic validation of basic security practices and controls on their external perimeter and/or internal network.

Web Application Assessment

This assessment is specific to web applications and will thoroughly test a web application inside and out following OWASP[2] guidelines and best practices. While very similar to a traditional penetration test, the web application variant focuses specifically on vulnerabilities and risk as it relates to a single web application and its relationship to the greater network, the business, and its purpose. This assessment uses mostly manual attack techniques supplemented by automated vulnerability scanning and expert analysis. Many vulnerabilities and risks are assessed, including but not limited to:

- SQL/OS/LDAP/etc Injection
- XSS (Cross Site Scripting)
- XXE (XML External Entities)
- Deserialization Attacks
- Broken access controls and/or authentication
- Sensitive data exposure
- Security misconfigurations

[2] The *Open Web Application Security Project is a non-profit foundation that works to improve the security of software.*

Penetration Test

The most general assessment type. If you are unsure what exactly you want, this is the safe choice. This assessment includes everything you would get in a Vulnerability Assessment with code execution while also:

- Identifying the impact of a vulnerability on your organization beyond the direct impact of the vulnerability itself
- Demonstrating the full impact of a potential breach, including multi-step attack paths[3]
- Assessing how well your organization's policies and procedures hold up to a concentrated attack
- Testing and providing recommendations for improving your security posture against tactics, techniques, and procedures (TTPs) not found on a vulnerability assessment

This assessment also contains some aspects of a Web Application Assessment if web applications are found in scope. Please note that it does not replace a full comprehensive Web Application Assessment, being more focused on quick exploitation than fully testing the web application. This is particularly true for issues that pose a business risk (e.g., sensitive data exposure), but are not inherently a vulnerability.

[3] An “attack path” is a set of actions taken by an actor to achieve an end goal, with each subsequent step being enabled by/dependent on the previous one They are generally used to characterize impacts that an actor cannot achieve in a single act (exploiting a vulnerability, leveraging a misconfiguration, etc)

Adversary Emulation

Our Adversary Emulation services consist of Red and Purple Teams. Red and Purple Teaming can be described as adversary simulation and emulation using real-world tactics, techniques, and procedures with the goal of educating and measuring people, process, and technology.

Adversary Emulation is a goal-oriented series of scenarios emphasizing significant depth of tradecraft while foregoing the large breadth of vulnerability coverage a Penetration Test would offer.

Emulation vs Simulation

To **simulate** an adversary, we would use specific TTPs associated with that adversary in order to mimic a threat as closely as possible.

To **emulate** an adversary, we would use whatever TTPs available, often the best or most appropriate, to mimic a theoretical adversary as best as possible. This is often what a typical red team will consist of unless specific scenarios call for mimicking an actual known adversary or TTPs.

Red Team Assessment

The currently popular assessment type. Be advised that while this type of assessment is in high demand right now it is only recommended for mature organizations. This assessment type will not be as beneficial to you as a penetration test if your organization doesn't have a dedicated SOC[4] or MSSP.[5]

This type of assessment is more focused than any other type we offer. The assessment is composed of one or more **exercises** where each exercise contains one or more **scenarios** designed to test very specific human and/or technical controls. Typically red teams work against a *blue team* which is usually the organization's Security Operations Center, or SOC. This is why without a SOC this assessment type is severely hindered.

Red Queen Security red team exercises and scenarios are custom built for each client during the proposal process. While many red teams focus very heavily on "winning" we put strong emphasis on educating the blue team with real world tactics, techniques, and procedures (TTPs) as they would be used by a persistent adversary.

[4] Security Operations Center
[5] Managed Security Services Provider

Purple Team Assessment

Purple Teaming is very similar to a Red Team Assessment. Like an RTA, it is only recommended for mature organizations. If your organization doesn't have a dedicated Security Operations Center (SOC) or Managed Security Services Provider (MSSP) this assessment type will not be as beneficial to you as a penetration test.

Similar to the RTA, this assessment is composed of one or more **exercises** where each exercise contains one or more **scenarios** designed to test very specific human and/or technical controls. The difference is that typically red teams work **without** coordination with a blue team (usually the organization's Security Operations Center and/or MSSP). During a Purple Team, we work directly with the blue team in a more collaborative approach. While a RTA gives defenders experience responding to breaches and the unknown, a Purple Team allows for more focused and methodological testing of people, processes, and technology for gaps in the defense of an environment or organization.

Red Queen Security Purple Team exercises and scenarios are custom built and focus on a breadth of tactics, techniques, and procedures to determine the scope and effectiveness of an organization's defensive controls. While many other red teams focus very heavily on "winning", we put strong emphasis on educating the blue team with real world tactics, techniques, and procedures (TTPs) as they would be used by a persistent adversary.

On-Site vs Remote Assessments

Red Queen Security supports both remote and on-site assessments but there are some things to consider when choosing on-site work:

- We are often capable of conducting internal assessments from a remote location. (Exact implementation varies)
- On-Site assessments will have an increased cost due to travel and lodging expenses.
- On-Site assessments are great for extremely sensitive or restricted environments such as SCADA, environments that must not be externally accessible, or when you need a more personal and hands-on approach.