



Red Team Testing Methodology



Revision History			
Issue	Date	Author	Reviewed by
Version 1.0	3/1/2011	Iftach Ian Amit	Yoram Golandsky

Contents

1. Abstract.....	3
2. Methodology	4
2.1. Information and Intelligence Gathering	4
2.2. Threat Modeling	6
2.3. Vulnerability Analysis	7
2.4. Exploitation.....	8
2.5. Risk Analysis and Quantification	9
2.6. Reporting.....	12

1. Abstract

Red Team Testing is a concept that derives its name from military jargon, where the aggressor uses various threat actors, equipment, and techniques that are obscured from the defender.

Security Art's Red Team service does not focus a single effort into exploring security gaps, instead it operates on all fronts on behalf of the organization, evaluating all information security layers for possible vulnerabilities. The Red Team is composed of experts in many fields of practice, who are collectively able to simulate a real-world attack using blended-threat scenarios against the organization. A valuable advantage of the Red Team service is the live feedback regarding the true level of the security of the organization.

The Red Team evaluation provides an in-depth understanding of how sensitive information is externalized, and also highlights exploitable patterns and instances of undue bias in control and planning. Additionally, the organization's maturity model for its information security and risk management practices, and any detection, alerting, and incident handling capabilities, are measured.

For example, as part of the Red Team evaluation, specially crafted payloads that fit the organization are developed, and their deployment measures how the organization deals with an "APT" (Advanced Persistent Threat) class attack. This essential exercise provides the organization ways to hone its defense strategy, and reflects its readiness to deal with such threats.

It's worth noting that the SANS institute has defined Red Team testing as one of its "20 Critical Security Controls" for organizations.

2. Methodology

Security Art's Red Team testing is comprised of 6 stages; five being active stages, and one analytical/reporting stage. Of the entire engagement (which usually takes 2.5-3 months), only about 20% requires the organization's resources and attention. The attack simulation takes place within a time span of 30 days, where Security Art executes simulated attacks without specifically coordinating the timing (except for in rare cases, and even then the information is privileged to specific parties inside the organization so that it cannot be used to "prepare" for the attacks).

The 6 stages of Red Team testing are:

- i. Information and intelligence gathering
- ii. Threat modeling
- iii. Vulnerability assessment
- iv. Exploitation
- v. Risk analysis and quantification of threats to monetary values
- vi. Reporting

A detailed explanation of each stage now follows, including examples of expected deliverable highlights.

2.1. Information and Intelligence Gathering

Nowadays, organizations are highly exposed to core information leaks, which can give an adversary a head start on profiling an attack or infection vector. Such information is not limited to technology use only, and includes the physical premises of the business, its employees, internal policies and procedures, and even the involvement of 3rd parties.

In this stage, Security Art's intelligence specialists gather and analyze information on the business processes of the organization, collect information on key individuals and the corporation as a whole, map the physical and technical infrastructure, and map out the business social media presence.

Although this stage can be done without any cooperation or assistance from the organization, it is highly recommended that for at least the business processes analysis, that some resources are made available, as this greatly enhances the Red Team's capability to accurately identify and quantify the value of the key business assets at risk.

The key results from this phase appear on the final report in the form of the OSINT (Open Source Intelligence) view of the organization from the outside. This view enables the organization to keep track of how it is perceived from the outside, and to track any information that may be used later for crafting an attack.

Some examples of the elements gathered and documented during this phase are:

- Business physical addresses: building layout, access paths, utility feeds and their backups (power, water, sewage, internet), onsite security (number, frequency, mobility, capabilities), access controls (gates, loading docks, delivery entry, and so on).
- Business financial information: SEC filings, 3rd parties involved SEC filings, Edgar/Hoover's profiles, public relations information (website, PRs, advertisements, job openings, previous employees), competitor coverage, business process identification (depending on industry type).
- Social media profiling: everything related to the organization (blogs, articles, official twitter and social media profiles), key personnel profiles (LinkedIn, Twitter, Facebook, any other social media), organizational chart, externally accessible documents (court documents, public documentation, filings, conference material, and so on)
- Technological footprinting: IP addresses, domain names, phone trunks, mobile phones, email addresses, software mapping, use of "cloud" or hosting providers, use of wireless technologies, open services on servers, mapping of technology processes (website business logic).

2.2. Threat Modeling

Based on the findings of the intelligence gathering phase, threat models are created using two key methods: asset-centric and threat-centric.

Key business assets and business processes are analyzed and documented in order to identify both the “soft targets” that an adversary may choose to use, as well as the most valuable assets that are likely to be targeted. All the related human, technical, and procedural elements surrounding these assets are mapped out so that an attack tree can be created.

Additionally, from a threat perspective, the relevant threat communities are identified, and a capability analysis is performed in order to create the true to life simulation scenarios. Factors such as available resources, skills, accessibility, and frequency of contact with the target, are taken into account and documented as part of this process.

The following threat model data is recorded during this stage:

- Business asset mapping: asset retention policy, asset expected lifetime, asset valuation (over multiple realms; competitive, legal, marketing, process, replacement value, productivity, 3rd party impact, customer impact, long-term liability, and so on).
- Threat community mapping: competitor, random group, internal, terrorist, foreign state.
- Threat community capability mapping: accessibility to information, accessibility to physical location, accessibility to tools and technology, technical skills, resource availability (financial), familiarity with the business.

2.3. Vulnerability Analysis

The vulnerability analysis stage is performed only after all the necessary elements related to intelligence gathering and threat modeling are complete. This stage may sometimes be considered an extension to threat modeling (as it provides the software/technology-centric threat modeling approach), and sometimes as part of the exploitation stage that follows. We believe that vulnerability analysis is a stage in its own right as it includes not only the technical elements of vulnerabilities, but also an assessment of the business processes, social elements, and other avenues that may be vulnerable.

In this stage, a target list is prepared and attack paths are calculated. All the relevant protection mechanisms (again, both technical and social, such as policies and procedures) are mapped out in order to identify potential roadblocks to the attack.

Only then the more technical footprint is applied to internally- and externally-used technology, and these are included in the vulnerability analysis report.

Some of the topics that are covered in the vulnerability analysis are:

- Business process logical flaws.
- Organizational policy logical flaws and gaps.
- Customer support and identification process flaws.
- Application security logical flaws, including reverse engineering client applications, and any code that can be obtained through the engagement (in source or binary form).
- Core application platform security vulnerabilities (covering custom applications, application servers, web servers, database servers, and operating systems).
- Network security flaws, including routing, segmentation, information disclosure, pivoting, and direct flaws at the network layer.
- Mobile application security issues, including authentication, impersonation, DoS, abusing business processes, and so on.

2.4. Exploitation

The exploitation stage is where the organization is being subjected to the actual direct attacks. This stage is commonly conducted within a predefined window of 30 days, in which activity is allowed (but not specifically coordinated).

The exploitation takes place through all pre-identified attack paths, utilizing any assets and resources that have been analyzed in prior phases. Such attacks include both “traditional” ones, as well as customized ones wherever a sophisticated attacker is being simulated. In this way, the organization being tested can measure itself against threats that otherwise it would not be exposed to up until the moment of truth; threats such as APT (Advanced Persistent Threat) attacks, and other targeted exploits.

The exploitation stage does not end when a code has been executed on an internal asset, as testing continues to close the loop, showing how information can be exfiltrated from the organization, thereby testing any DLP (Data Leak Prevention/Protection) mechanisms and content filtering solutions that the organization may have deployed.

During the test, the chosen targets also reflect business-impacting attacks in order to see how the organization's incident response would cope with such attacks. During this phase, we also gain the understanding of the effectiveness of the organization's control resistance to the attacks, and this is reflected in the final report, where specific cost-effective recommendations are made.

2.5. Risk Analysis and Quantification

The Red Team evaluation is not designed to just prove that someone can get into the organization. It is designed to provide the organization with actionable data regarding its security posture, and to assist the organization in maintaining a defensive strategy that would be applicable to its actual threats. As such, one of the critical stages of the test is to provide quantifiable risk analysis based on the testing performed.

When performing such risk analysis, we establish all the basic elements of the risk equation (together with the company), and assign actual values to them. We utilize the FAIR methodology as it has proven to be one of the more accurate, reliable, and repeatable methods to quantify risk. Elements such as threat event frequency (TEF), control resistance strength (RS), and loss event frequency (LEF), are calculated as a direct result from the testing. Later on, a primary and a secondary loss magnitude are established, based on the information asset value, and the other variables, all in order to derive a final risk value that can be acted upon and used by the organization.

An example of the risk analysis and quantification would look very much like a standard FAIR case report, such as the following:

Loss Exposure

Total Loss Exposure					
5%	25%	50%	75%	95%	Most Likely (Mode)
\$50M	\$110M	\$205M	\$900M	\$1.5B	\$185M

Although ABC's aggregate exposure is most likely to be just shy of \$200M, the distribution of possible outcomes has a long tail toward the high end of the scale, which suggests that there is potential for the actual loss exposure to be significantly greater. For example, over the course of 10,000 monte carlo simulations, 25% of the results totaled more than \$900M in exposure and 5% of the results totaled more than \$1.5B.

Asset Groups (Top 5 by Exposure)	Exposure
Internet Applications	\$99M
Personal Systems - Desktops	\$42M
Internet-facing Windows Servers	\$19M
Mobile Media	\$10M
Data Warehouses	\$3M

The top five asset groups (out of 23 overall) represent over 95% of the organization's total loss exposure. Note that the top 3 asset groups all are subject to Cyber Criminal attacks via the Internet.

Loss Event Type	Exposure
Confidentiality Breach	\$165M
Data Integrity Compromise	\$12M
Data/System Availability	\$8M

Confidentiality loss events overwhelmingly represent the greatest exposure. Note that availability exposure is low because of the high degree of redundancy built into ABC's architecture as well as the fact that outages generally result in delayed revenue rather than a loss of revenue.

Risk Management Capabilities

Asset Groups Visibility	Percentage
Mobile Media	3%
Non-ABC Personal Systems	10%
Unmanaged Databases	25%
Internet Perimeter Devices	60%
Internet-facing Servers	80%

The table to the left identifies the five asset groups where visibility is worst (e.g., ABC only has visibility into approximately 3% of the mobile media used in the organization). These visibility gaps significantly affect ABC's ability to make well-informed risk management decisions.

Execution Factors	Percentage
Choice	75%
Insufficient Awareness	20%
Insufficient Resources	3%
Insufficient Skills	2%

A root cause analysis of thirty risk issues within ABC's environment suggests that 75% of the issues were the result of a choice by personnel not to comply with published security standards.

Choice Factors	Percentage
Prioritization	70%
Self-Interest	15%
Error	10%
Maliciousness	5%

Approximately 70% of noncompliance choices were driven by prioritization against other business imperatives. Note that the appropriateness of those choices was not determined.

Risk Reduction Opportunities

Asset Group	Mitigation Component	Exposure Reduction
Internet Applications	Code Compliance	\$33M
Personal Systems	Patch & Configuration Management	\$27M
Internet-facing Windows Servers	Patch & Configuration Management	\$5M
Data Warehouses	Access Privileges Management	\$2M

Analysis identified four risk management opportunities exist that have the potential to reduce the organization's aggregate exposure by as much as \$67M (~30% of the aggregate total).

2.6. Reporting

The Red Team evaluation would be completely insignificant if it would conclude with a simple standard vulnerability report. Nevertheless, we do appreciate the importance of a technical report, so that the technical audience in the organization gains the right tools and directions to assist them with amending any security gaps. As such, Security Art delivers a two-pronged final report.

The first part of the report is executive level. This part focuses on the risk management practice, and quantifies the risks in a way that allows an informed decision making process to be applied to the security practice. In addition, it helps the organization to keep track of the exposure over time as all the figures are traceable, and can be recalculated when the security posture of the organization changes, either from the threat side, from the control side, or even from the business assets perspective. The report also includes all the relevant documentation from all the Red Team test stages as described above (intelligence report, the full threat models that were created, vulnerability analysis, documentation of exploitation and exfiltration techniques).

Some of the following elements are covered in this part of the report:

- Risk management maturity model
- Risk analysis for each scenario tested and identified: including full calculation of threat, vulnerability and impact using the FAIR methodology.
- Timeline of attack: especially when attacks are staged and the scenario is composed of a blended threat and/or dependent phases.

The second part of the report is technical, and includes:

- General metrics: number of systems in scope, number of systems compromised, number of attack scenarios, number of detected scenarios.
- Description of every technical finding: including method of exploitation, technical impact of the finding, skill factor required, examples and screenshots, test cases.
- Identification of root-cause analysis.
- Incident response findings (correlated with general attack trees/scenarios).