Full-Force Red Teaming

Offensive security testing has developed and grown over the past few decades, and we have advances in our nation's military to thank for it In the private sector, systems penetration testing arrived mid-century. Social engineering testing arrived not long after. And for many, physical red teaming is the new kid on the block. Certainly no one can be blamed for the staggered evolution of offensive security testing. However, it has affected how the three testing strategies, Physical Security Testing, Social Engineering, and Technical Penetration Testing, are used in the private sector.

Throughout this chapter, I will refer to the three testing strategies, **physical security testing**, **(technical) penetration testing**, and **social engineering** as the Red Team Triad.

The Red Team Triad

SYNOPSIS

Technical penetration testing, social engineering, and physical security testing make up the three domains of the gold standard for the offensive

security testing triad. As you might have already deduced, a holistic approach toward security testing is a step in the right direction. Full-Force Red Teaming is comprised of comprehensive, correlated operations on technology, people, and facilities to provide the most effective actions and increasing the likelihood of success.

Social Engineering	Physical Intrusion	Technical Penetration

• Spear Phishing
• Telephone/SMS phishing
• FaoSMS
  • In-Person
  • Baiting
  • Staff, Vendors, Partners
	• Mantrap, Guards
	• Fencing, Barriers
	  • Cameras, Motion Sensors
	  • RFID, Biometrics
	  • IR, Radar, Door Locks
	  • Offices, Buildings, Refineries, Substations, Plants, etc.
		• Web Applications
		• Networks
		• IoT & Medical Devices
		• Mobile Apps
		• WiFi Networks
		  • Network Devices

The following section briefly describes one possible approach toward meeting this goal.

One of the initial keys to safeguarding a proper physical. red team test is to conduct a profile of the target organization. This profile should take into account the organization from a high level. Aspects that include its industry, size, and so on should be taken into account as part of an overall profile of what threats the organization is likely to encounter. Only then will the operators know which TTPs are relevant and the level of complexity that is needed to ensure a realistic and commensurate test.

That said, profiling an organization is much easier said than done. Here are a few key exposure factors to consider when doing so. Please keep in mind, this is not a complete and comprehensive list, but it will add a layer of depth necessary to root out additional perspective.

Exposure Factors

Industry - ls the organization's industry a likely target? Banking, retail, and hospitality are highly targeted by attackers. Is it in a controversial industry (gambling, abortions, tobacco, firearms)?

Size - How many employees, contractors, partners, agents? More humans generally mean more social engineering target opportunities.

Geographic Footprint- How many offices, stores, places of business? How widespread are physical assets disbursed around the office, building, campus, city, state, country, world? Are they located in distressed neighborhoods, cities, or countries?

Prominent Characters -Are there any prominent characters associated? Famous people, politicians, high-net-worth families/individuals, or outspoken leaders whose actions/beliefs may introduce additional risk into the environment?

Political Involvement - Does the organization maintain a known political leaning through partisan viewpoints, support, and/or political donations? How does this partisan stance affect the organization?

Customers - Who makes up the majority of customers? Hundreds of business customers? Millions of consumers of everyday goods and services? Do the majority of the customers come from the United States or from unfriendly nations?

Technology Adoption - To what degree does the organization adopt technology into their environment? Does the organization still have Windows XP machines? Is everything in the cloud? How progressive are their technological defenses?

This is by no means a full and complete list. However, the outcome of examining feedback from these exposure factors will ultimately play into building a test plan that addresses likely organizational threats. What's more, it will have a lot to say about the complexity of TTPs to be utilized in order to provide a commensurate and realistic test.

At the very least, running through an exposure factors exercise will provide a clearer picture of the attacker or attackers, what they might be

targeting, how they might launch their attack, and their level of sophistication. As a physical red team operator, this information becomes very valuable in crafting an operation of value.

Vulnerability Ranking

Full-Force Red Team methodology calls for employing social engineering, physical testing, and technical penetration testing. The next important component is to rank findings not only comprehensively, but as they correlate to one another.

In this section, I will present a sample risk rating methodology that aims to rank findings comprehensively, while correlating with other identified risk aspects in the security triad. This ranking should be done

According to NIST SP 800-30, we have the de facto standard for calculating risk.

RISK = LIKELIHOOD x IMPACT

Likelihood - The realistic likelihood of successful exploitation and operation

Impact - The magnitude of harm to confidentiality, integrity, availability, and accountability of data and resources

Risk - Represents the total amount of risk exposure

There are many ways to evaluate risk exposure by using risk ranking frameworks that adapt to this equation. To keep things simple, I will illustrate the point using a set of granular factors that should be considered when arriving at likelihood and impact. Finally, I'll introduce a quantitative approach my team uses to determine risk.

The image shown in Figure 115 depicts an example of a Likelihood and Impact Table whose purpose is to align with Full-Force Red Teaming. It does this by diving deeper through the use of 12 factors for likelihood and twelve factors for impact. These factors aim to fully represent each side respectively.

Let's take a closer look below.

Likelihood

Bad Actors	Objective	0 - 9
	Resources	0 - 9
	Ability	0 - 9
	Immensity	0 - 9

Organizational	Industry	0 - 9
	Size/Employees	0 - 9
	Geographic	0 - 9
	Customers	0 - 9

Flaws	Exploitability	0 - 9
	Detectability	0 - 9
	Widespread	0 - 9
	Identification	0 - 9

Impact

Assets	Confidentiality	0 - 9
	Integrity	0 - 9
	Availability	0 - 9
	Traceability	0 - 9

Customers	Monetary	0 - 9
	Reputational	0 - 9
	Privacy	0 - 9
	Litigation	0 - 9

Organizational	Perception	0 - 9
	Monetary	0 - 9
	Compliance	0 - 9
	Employees	0 - 9

Sample Likelihood of Success and Impact Table

Likelihood of Success and Impact are broken down into three categories each (e.g. Bad Actors, Organizational), and each category has a group of four attributes called factors. As you can see from the example above, each and every factor has a potential numeric rating of 0 to 9. A rating of 9 indicates the highest estimated measure of presence for any given factor. For instance, a rating of 9 for the factor titled Ability in the Bad Actors category for Likelihood of Success would indicate a highly sophisticated level of technical prowess by the attacker. A rating of 0 for the same factor would indicate the attacker is likely to have virtually no technical aptitude, and so on.

Likelihood of Success & Impact Factors

Before we go any further, let's extrapolate the factors to understand how they work. Each of the categories and their respective factors have been developed with the sole purpose of evaluating risk on a grander level. To do that, twenty-four factors are broken up into six categories help make that happen.

To start, let's unpack each of the factors by first beginning with Likelihood of Success and then provide guidance on how to use them.

Likelihood		
Bad Actors	**Factor**	**Description**
	Objective	How substantial is the reward? How motivated is the attacker?
	Resources	How well-resourced is the likely attacker?
	Ability	How skilled is the likely attacker?
	Immensity	How large is the group of attackers?

Likelihood of Success Risk Factors Explained for Bad Actors