A PRIMER TO RED TEAMING

AS PART OF A HOLISTIC CYBERSECURITY PROGRAM

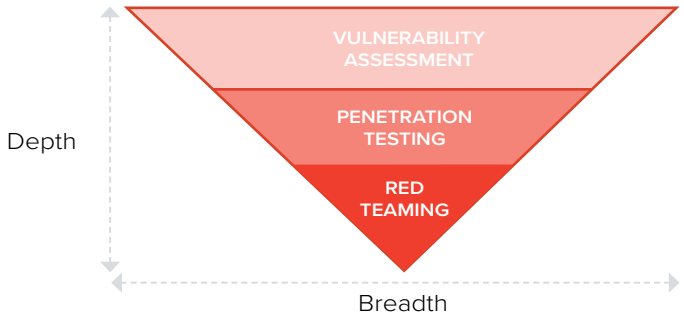
Bishop Fox Guide - Updated July 2018 - MJK

CONTENTS

INTRODUCTION

In order to fully understand red teaming, it might be best to first decouple it from penetration testing. The two are often conflated, and that only serves to lessen the quality of the decision-making around which to choose.

Red teaming exercises have a distinct value to organizations that differs from pen testing. Red teaming involves a much larger team of specialists hired from the outside — mature security programs may choose to create their own red teams — who take a mile-wide approach to infiltrating an organization. Penetration tests can have narrower focuses on specific applications or customer-facing network segments and expose vulnerabilities and weaknesses that need immediate attention and are prioritized for patching and/or updated policy-making.



Enterprises that employ red teaming as part of a regular security assessment want these crack outfits of white-hat hackers to kick down the doors any way possible. No approach is out of bounds, be it a physical infiltration coupled with a malware attack, or a simple social-engineering scheme to establish a foothold inside, red-teaming is an assault against an organization carried out much in the same way as a coordinated targeted attack.

The value of a red-teaming exercise is that it puts an organization's detection and response capabilities and procedures to the test. It's about much more than finding unpatched bugs and long-forgotten servers still connected to the internet. It's about putting a company's digital and physical security to as close to a real-world test as possible and evaluate how robust your response is.

In this guide to red teaming, we will showcase the strategy behind red teaming and its execution as part of a holistic cybersecurity program. It will also cover how tabletop exercises, threat-based assessments, and continuous testing can contribute to an organization's strengthened security posture.

Red teaming isn't for every organization. But mature programs do benefit from the practice — its roots are in the military and intelligence operations — as part of a continuous assessment of cyber and physical security. Threats to enterprises go well beyond cybercrime and data breaches. Some rogue nation-states are supplementing national economies with hacking, and the theft of intellectual property and penetration of critical infrastructure brings these threats closer to more and more security teams every day.

Red teaming goes beyond penetration testing of applications and network segments to one where defenses and response is tested against determined adversaries before there is real-world damage. To have a regular, carefully planned, and resourced assessment of digital and physical defenses is an imperative that few organizations in sensitive, critical industries can no longer afford to ignore.

WHAT IS A RED TEAM EXERCISE & WHY DO YOU NEED IT?

Red teaming is a simulation of a cyberattack in which the red team is allowed to leverage a variety of methods in order to capture a "trophy." This trophy is previously identified by the organization engaging in a red team exercise; it might be gaining access to a set of credentials or establishing a foothold in a sensitive internal network. With red teaming, it is not the how of getting to a destination that matters, it's the "destination."

Red teaming takes many forms (e.g., in the three following case studies), whether it's a black-box engagement such as in the transit authority case study below, or a mix of external network, web application, and physical penetration testing including social engineering. Or something akin to an application penetration test combined with a network penetration test.

Red teaming is not a penetration test. A traditional penetration test is limited by the confines of scope and other pre-determined conditions. These boundaries serve their purposes in such engagements, but they can provide a narrow glimpse into your organization's weaknesses. After all, hackers do not acknowledge such arbitrary boundaries; they don't care if your information is hosted in the cloud, if you're using legacy systems, or if a third-party vendor is responsible.

Red team assessments are generally longer in duration than pen testing assessments and often involve a team of several people who test several detection and response capabilities simultaneously. While you may pay attention to one particular attack vector, or focus on remediating vulnerabilities in your web applications, a red team engagement will exploit neglected security issues in your internal network or take advantage of the security challenges posed by non-technical employees.

CASE STUDIES

RED TEAMING CASE STUDY
01 TRANSIT AUTHORITY

A major transit authority requested we attempt to access the network that powered its infrastructure, which is relied upon by tens of thousands of commuters and travelers every day.

With this task defined, we began the engagement with zero knowledge of the systems in place. After performing reconnaissance during a period of a few weeks, we determined what would be the most efficient path for exploitation: weak passwords.

By cracking passwords in use by members of the organization, we obtained access as a domain administrator, which allowed us to escalate privileges and eventually gain complete access to the authority's systems. In the hands of an attacker, this would have been a risk to the security of a major metropolitan area and would have resulted in mass chaos.

Because this was a red team assessment and not a typical penetration test, our team succeeded in mimicking how a cyberattack would play out.

RED TEAMING CASE STUDY
02 RETAIL

For a notable retail client, we were able to leverage red teaming to reveal that the client was susceptible to sensitive information disclosure, which included (but wasn't limited to) the financial information of its customers. Since directory browsing was enabled on more than a dozen web servers, our team scanned these directories to find configuration information, such as database credentials and encryption keys.

We worked carefully with the client in the remediation process to disable the functionality that was causing these issues. Exploitation by an attacker would have impacted thousands of people.

RED TEAMING CASE STUDY
03 FINANCE

During a red team engagement for a large finance organization, the client asked us to do the following: escalate privileges on the Active Directory infrastructure, gain access to Amazon Web Services (AWS) environments, and identify vulnerabilities in the internal and external networks.

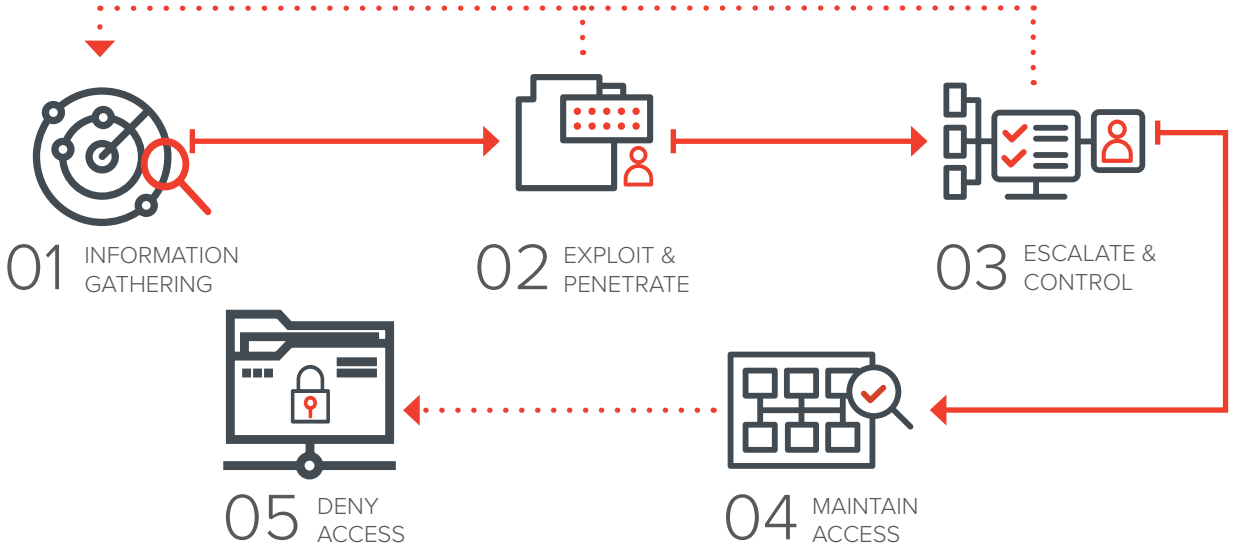
We found more than 200 unpatched Microsoft systems in addition to a handful of privileged accounts accessing non-critical systems, which played a critical role in our team capturing the trophies. We even surpassed what was established by the client to escalate more privileges and gain access as a domain administrator.

Our team collaborated with the client to strengthen its network attack detection capabilities while the engagement continued and helped to remediate weaknesses we pinpointed.

WHAT DOES IT MEAN TO RED TEAM?

The red team's objective is to "capture" a trophy, which could be anything an organization deems of importance, be it customer personally identifiable information (PII), persistent network access, or administrator credentials.

After this trophy is determined by the targeted organization, the red team works a variety of methods to find the best suited to reach its destination. It's a case of anything goes. It's also important to note that organizations have the option to request the level of knowledge the red team has in the engagement. It can be a full zero-knowledge engagement, or consultants may have some level of pre-existing knowledge of network and system architecture.



Stages of a red team engagement

01 INFORMATION GATHERING

Gather information (footprint, domains, email addresses, etc.), analyze and determine attack methods.

02 EXPLOIT & PENETRATE

Exploit human or technical vulnerabilities and/or misconfigurations, penetrate and transmit attack via different vectors, and compromise.

03 ESCALATE & CONTROL

Install customized malware or backdoor, gain the remote control of victim's system.

04 MAINTAIN ACCESS

Maintain the remote control and "make a persistence".

05 DENY ACCESS

Perform the actions to achieve actual goals inside the victim's network (persistence, lateral movement, search, exfiltration, etc.).

However, for an organization, the objective of a red team engagement will naturally differ. While the successful capture of the trophy is beneficial because it calls attention to an area of focus, your organization's real prerogative may be to test your incident response capabilities or determine how effective your security controls are when faced with a viable threat.

ELEMENTS OF AN ENGAGEMENT
WAYS TO RED TEAM

There are different varieties of red teaming security assessments. Below is a quick overview:

TABLE TOP EXERCISES

Table top exercises involve reviewing what your most immediate and dangerous threats are — and how you would react if those threats manifested into reality. All relevant stakeholders play a part in this exercise. Perhaps you are worried about one of your employees falling victim to a phishing email and infecting your internal network with malware; perhaps you are worried about a ransomware attack wreaking havoc on your organization; or maybe you lose sleep over a denial-of-service attack bringing productivity to a halt. A table top exercise gives you the opportunity to map out all these threat models as well as how you would handle such a situation. Plan for unexpected issues when conducting a table top exercise – you may have to consider panicking executives, the fatigue of overworked employees, or possibly news breaking about the attack.

THREAT-BASED SIMULATIONS

To up the ante, your organization may try a threat-based simulation. At first glance, it seems an awful lot like a traditional penetration test, but there is a more to-the-point timeline involved, not all types of vulnerabilities will be assessed for, and the red team will have to do some reconnaissance beforehand. During a threat-based simulation, you focus on the threats you have previously identified — and, in a safe (but realistic) environment, you simulate them. These threats may be those that you feel you are particularly protected against or are more urgent than others.

If you think you're ready for the challenge at hand, engage in one of these simulations. After performing a threat-based simulation, you'll have a more pragmatic sense of your preparedness for such a situation.

CONTINUOUS ASSESSMENTS

A continuous assessment is perhaps the most closely resembling a real cyberattack. This is due to the factor of time — since it's ongoing, it represents the actual amount of effort an attacker would put in to infiltrating your organization. Several approaches will be tried to reveal where your security stance could be fortified.

TEAM SPEAK
RED, BLUE, & PURPLE

WHAT IS A RED TEAM?

A red team is meant to play the role of an attacker in a simulation. However, we've also mentioned the concept of a blue team. But what does a blue team do? And what's the purpose of a purple team?

WHAT IS A BLUE TEAM?

Think of a blue team as your first responders, like those who show up after a natural disaster in the physical world and begin the process of recovery. They are your defenders; they are those who are responsible for detecting a compromise. A red team's success does not inherently spell failure for a blue team; rather, it's a way for a blue team to gauge its current level of effectiveness and where they need to focus on growing and improving. In some cases, a blue team may completely miss a compromise during an engagement; use these moments as learning opportunities.

WHAT IS A PURPLE TEAM?

A purple team is a rarer component than the traditional blue or red team. It combines the capabilities of both — often segmented — groups and acts as a collaborative effort designed to implement offensive and defensive techniques. Communication is constant between those doing offensive work and those doing defensive work, whereas traditionally these two units do not interact more than necessary. You may wish to hold off conducting any sort of purple team exercise until your security team arrives at the right maturity stage.

Do you need all these teams? A red team and a blue team complement each other, so you will need something like a blue team if you do a red team engagement. A purple team, though, is reserved for more advanced security testing – and when you are at the point where both the red and blue team skill level is on par with each other.

WHERE TO GO FROM HERE?

Should you think red teaming might be a solution to your organization's security woes or a proactive step to help bolster efforts before a breach or incident induces chaos, you have several options in pursuing it.

RED TEAMING

INTERNAL TRAINING

If you have the resources available in house to do red teaming, by all means, use them to your advantage. You may prefer to use your team for budgetary, privacy, or compliance-based reasons. If you choose to use your employees, you may want to begin with table top exercises and then ascend the red teaming hierarchy.

WORK WITH THE RIGHT PARTNER

Red teaming can attract the wrong kind of security professionals. Partnering with an experienced third party vendor is another option that provides you with a true outsider view of your infrastructure — most closely resembling an attacker's perspective. A third party will take the blinders off your security efforts and reveal weaknesses that may be missed by unintentionally biased insiders.

SOCIAL ENGINEERING

Social engineering is a component in many red team assessments (not necessarily all of them). If direct contact with people is part of what you're seeking to test, then you need to include an element of social engineering in the red-teaming engagement.

A good methodology on social engineering can be summed up by the following: Use an array of tools to learn about an organization's employees. In today's social-media-happy world, this isn't entirely a challenge. People expose countless facts about themselves on sites like Twitter, Instagram, and Facebook. Additionally, corporate websites, web applications, internet-facing servers, personal blogs, and public data generated by third parties are goldmines of information for a social engineer. Red teams then use this information to elicit details from employees about potential vulnerabilities.

Social engineering can consist of physical penetration testing, phishing, or confidence scenarios. In a confidence scenario, the red team creates essentially a trap to lure unsuspecting employees in. Sometimes this looks like an email from an authority figure, demanding that a more subordinate employee downloads a file containing malware.

It is this personal interaction that enables a red team to successfully achieve their objectives in an engagement. Social engineering opens the doors for other attack vectors to be further exploited.

As said time and time again, people are by far the weakest link for many organizations. Social engineering proves —and exploits — this fact.

ARE YOU READY FOR RED TEAMING?

Red teaming is more impactful when your organization is larger (typically — although not always the case), owns more assets, including the ones you may not know about, and is more advanced in terms of security. If you're a startup that has only begun to prioritize security, then you will likely want to hold off on red teaming until you have some established defenses and a mature cybersecurity strategy implemented. You need a solid baseline in order to measure success.

If you are only starting to invest in security, you will need to take some time to conduct traditional penetration testing and understand your weak areas. Rushing into red teaming is not the best idea for a multitude of reasons — truly, you're not at the right stage for it, and it might be overwhelming to confront all of your vulnerabilities at once.

Think of a house analogy; if you're inspecting your house for the first time, you're going to want to take the process in small, manageable increments. When you feel more comfortable with a sense of your perimeter, you'll want to move on to more complicated ways someone might break in.

THE BENEFITS OF RED TEAMING

Any red teaming method you choose will provide you with visibility into where your organization needs to devote more resources to improving security. Red teaming is by far the most effective and holistic method of mimicking how an attacker would likely compromise your organization. And it brings to light issues you wouldn't have otherwise considered. By defining where you are struggling most, your organization can enhance detection and response, and decrease the risk of an attacker finding a known vulnerability already exploited in the wild.

Red teaming allows you to evaluate the value of your security controls. There is no better barometer of what works and what doesn't work than putting your protections to the ultimate test. Also, red teaming can help you assess the capabilities of your incident response plans (aka the preparedness of your blue team). In the postmortem phases of a red teaming project, if there were breakdowns in communications or delays in detecting compromise, you will have the opportunity to improve those areas — ideally before a real incident occurs.

A successful red team assessment will also enable you to request more security budget from the C-suite. After determining which controls you have that are not functioning properly, where you may need to further staff your security team, and which tools you need to invest in, you can present a compelling case to allocate more budget to prioritize security in your organization.

FURTHER RESOURCES

How to Use Red Teaming in Your Cybersecurity Program – A Forbes article authored by Bishop Fox's Christie Terrill
https://www.forbes.com/sites/christieterrill/2017/03/30/how-to-use-red-teaming-in-your-cybersecurity-program/#761f97d675a4

Microsoft Enterprise Cloud Red Teaming – A whitepaper by Microsoft detailing how they conduct red teaming
https://blogs.msdn.microsoft.com/azuresecurity/2016/02/25/updated-microsoft-cloud-red-team-white-paper/

How your red team penetration testers can help improve your blue team
https://www.scmagazineuk.com/how-your-red-team-penetration-testers-can-help-improve-your-blue-team/article/534767/

The Rise of the Purple Team
https://www.rsaconference.com/writable/presentations/file_upload/air-w02-the-rise-of-the-purple-team.pdf

PENETRATION TESTING VS RED TEAMING

	PENETRATION TESTING	RED TEAMING
Skill Level Required	High	Higher
Scope	Defined by organization	Identified by red team
Objective	Confined results	Uncover many vulnerabilities
Threat Emulation	Partial	Advanced and persistent
Systems Testing	Independently	Simultaneously
Rules	Well defined	Anything goes
Employee Awareness	Typically aware	Limited number
Targeted Users	✓	✓
Vulnerability Scanning	✓	✓
Manual Testing Simulating Attackers	✓	✓
Social Engineering, people	—	✓
Physical Testing, offices, warehouses, data centers, etc.	—	✓
Hardware Security	✓	✓
Software Security	✓	✓
Vishing	—	✓
OSINT to gather additional targets	—	✓
Wireless	—	✓

ABOUT
THE AUTHOR

MJ Keith (Security+, i-Net+, Network+) is a Senior Security Associate at Bishop Fox, a security consulting firm providing services to the Fortune 500, global financial institutions, and high-tech startups. In this role, MJ focuses on red teaming, external penetration testing, web application security assessment, and Android security. As a consultant at Bishop Fox, MJ's experience runs the gamut of penetration testing. He is considered an internal subject matter expert on all things Android security. Accomplishments related to Android security include developing a technique to fuzz applications more effectively on the OS. Prior to joining Bishop Fox, MJ served as a Senior Security Analyst at Alert Logic where he developed attack detection signatures and assisted customers with incident response. MJ also worked as a Senior Security Analyst for Methodist Hospital in Houston.

BISHOP FOX®

We provide security consulting services to the Fortune 1000 and high-tech startups.

We help our clients secure their businesses, networks, cloud deployments, applications, and products.

Find out more at bishopfox.com.
Keep in touch with the foxes on Twitter @bishopfox and on LinkedIn Bishop Fox.

Copyright ©2018 Bishop Fox®