Professional Red Teaming

Conducting Successful Cybersecurity Engagements

Jacob G. Oakley

Apress®

Professional Red Teaming

Conducting Successful Cybersecurity Engagements

Jacob G. Oakley

Apress®

Professional Red Teaming: Conducting Successful Cybersecurity Engagements

Jacob G. Oakley
Owens Cross Roads, AL, USA

ISBN-13 (pbk): 978-1-4842-4308-4 ISBN-13 (electronic): 978-1-4842-4309-1
https://doi.org/10.1007/978-1-4842-4309-1

Library of Congress Control Number: 2019934346

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Coordinating Editor: Rita Fernando

Cover designed by eStudioCalamar

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/9781484243084. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

To my children.
You can do anything you set yourself to.

Table of Contents

About the Author

Dr. Jacob G. Oakley spent more than seven years in the U.S. Marines and was one of the founding members of the operational arm of Marine Corps Forces Cyberspace Command at the National Security Agency (NSA), Ft. Meade, leaving that unit as the senior Marine Corps operator and a division technical lead. After his enlistment, Dr. Oakley wrote and taught an advanced computer operations course and eventually returned to mission support at Ft. Meade. He later left government contracting to conduct threat emulation and red teaming at a private company for commercial clients, serving as principal penetration tester and director of penetration testing and cyber operations. He currently works as a cyber subject matter expert for a government customer. Dr. Oakley completed his doctorate in information technology at Towson University, researching and developing offensive cybersecurity methods. He is the technical reviewer of the book *Cyber Operations,* second edition, by Mike O'Leary.

About the Technical Reviewer

Michael Butler has nearly a decade of experience in cybersecurity, including training and operational experience with US Army Cyber Command and the NSA at Ft Meade. As a soldier, he received several medals for both his academic and operational success. After his enlistment, he developed content for and taught an advanced cyber operations course. He then joined a private cyber security company as the lead of penetration testing, where he led and personally conducted offensive security operations in support of contracts with both government and commercial entities. He currently works as the vice president of offensive services at Stage 2 Security.

Acknowledgments

I thank my beautiful wife and family for sacrificing their nights and weekends to let me write this book, and for loving and supporting me through this and other nerdy endeavors.

I thank my father for exemplifying hard work and for all he did to give me the best chance to succeed in life.

To Mike O'Leary, who nudged me in the right direction, and Mike Butler, who performed the technical review, this book was not possible without you.

To all you keyboard-wielding cyber warriors out there protecting freedom, I salute you.

Introduction

This book is intended as a resource for those who want to conduct professional red teaming, as well as for those who use their services. The text is not intended to teach you how to hack a computer or organization, but rather how to do it well and in a way that results in better organization security. It takes a lot more than sweet hacking skills to perform offensive security assessments. Whether you are looking to employ ethical hackers, work with them, or are one, after reading this book you should understand what is required to be successful at leveraging cyber threat emulation to mitigate risk.

CHAPTER 1

Red Teams in Cyberspace

There exists a mountain of discourse in both digital and print form that discusses new exploits or tools that aid in the compromise of information systems. These texts are valuable implements to be used by offensive security practitioners in carrying out their profession. There are certainly hallmark publications that contribute to the craft of ethical hacking; however, many and most are timely in nature. In fact, much of the reason for the largess of this body of work is that each day there is new code written or tools developed and new vulnerabilities and exploits to leverage that can obsolete previous works.

The dizzying speed of innovation in both offensive and defensive technologies is tantamount to an arms race. Offensive tools may be outdated by improved security posture provided by newer defensive tools, or may simply be outpaced by better and more effective offensive ones. Weaponized vulnerabilities may be nullified by patching or heuristic measures as well as potentially new exploits that are less volatile and more likely to succeed.

Despite the great attention and efforts to modernize continually the tools of offensive security and the body of knowledge detailing their use, scant attention has been paid to the professional process itself. One hoping to become an offensive security professional can find quickly dozens of books that tell readers how to hack this system or that with code, exploits, and tools. Conversely, it is rather challenging to find literature on how to use all those abilities and tools successfully to affect customer security posture in a positive nature through professional processes.

The greatest challenges of any engagement are often not discovering and leveraging vulnerabilities, but rather are those challenges manifested throughout the engagement life cycle itself. These obstacles can be difficult customers, suspect rules of engagement, or inaccurate scoping, to name a few. Offensive security techniques such as penetration testing or red teaming represent some of the premiere tools used in securing information systems. As such, it seemed extremely important to me that I contribute to the field of

J. G. Oakley, *Professional Red Teaming*, https://doi.org/10.1007/978-1-4842-4309-1_1

offensive security with at anecdotal guidance and best practices involved in carrying out professional offensive security engagements. This book serves as a resource to both those wishing to enter the field or those already practicing.

For the purpose of this book, the term "red team" is used interchangeably and as an umbrella word that refers to the offensive cybersecurity methodologies of red teaming and penetration testing. Although many in this profession argue differences between the two, all will benefit from the information provided herein. In this chapter I explain provide what red teaming is, how it was tailored to cybersecurity, and the intention for cyber red teaming, as well as its advantages and disadvantages.

Red team is a term with alleged ties to the Cold War, when a "Red" force was used to represent the enemy in tests against organizations under attack from the Soviets. The concept of simulating attacks to test defenses and responses is much older. Although the term red team can refer to attacks of a military nature, this book focuses on the aspects of integrating this attack simulation concept into the cyber realm. Unless stated explicitly, red teaming refers to cyber red teaming—or offensive security engagements in general—and not those of a kinetic military nature.

Intentions

The intent of a cyber red team is to simulate attack against an organization to test information systems and their related facilities. This is an overly broad generalization, and the term "attack" is often inappropriately aggressive regarding the behavior of both red teams and the malicious actors they mimic. In many cases, the purpose of a malicious actor is to gain intelligence or steal information. Such goals are affected negatively by aggressive attack actions, as the actor in these scenarios is likely intent on staying unnoticed for as long as possible. Adversary emulation is perhaps the most appropriate and accurate description of the activity of red teams. The intent of this emulation is to improve understanding of capabilities and inadequacies in the defense, detection, and responses regarding threat actors.

Adversary emulation by red teams comes in many forms and can be classified broadly as a holistic compromise attempt, a specific compromise attempt, or assumed compromise. A holistic compromise attempt is one in which the red team is going after the entirety of the target organization's attack surface, with the goal of compromising as much as possible (Figure 1-1). Specific compromise attempts are those in which a certain subset of the attack surface is prioritized for assessment and the rest of the

organization is off-limits. Assumed compromise is a red team engagement during assessment begins from access granted to the assessors that is predicated by an assumed successful actor infiltration. Each of these classes of red team engagements come with their own challenges and complexities and subclasses, and each are appropriate in different test scenarios.

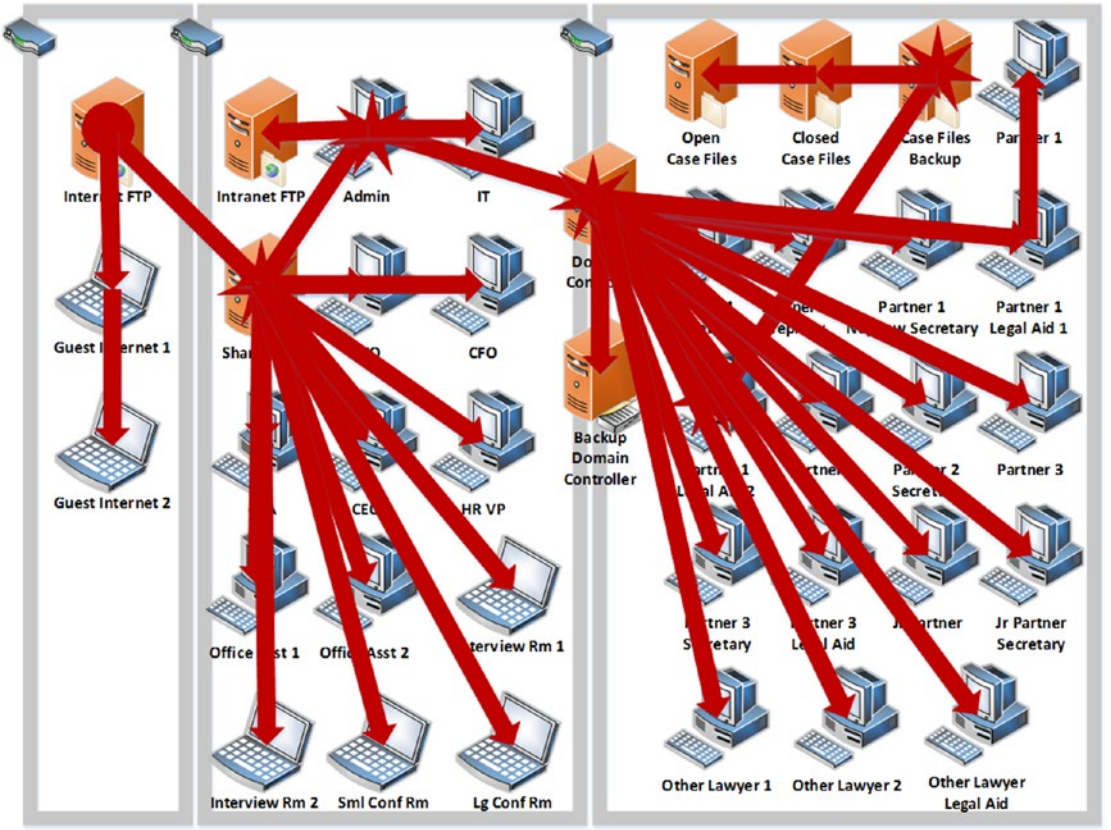

Figure 1-1. *Holistic compromise*

Holistic compromise may be considered the truest form of adversary emulation as the goal is complete compromise, and the point of origin for the assessors is likely the Internet. In this situation, the organization gets the most realistic simulation to test defenses: detection and response against. However, this type of assessment is also the least efficient and is likely to provide incomplete results. If the assessment is unable to compromise a given portion of the organization because of time limits or skill deficiencies, the results of the engagement may offer a false sense of security.

Holistic compromise attempts can also be considered in several subclasses. Although the entirety of the organization is the target, the avenues of attack delivery are often specified. A completely holistic attack, for instance, is one in which any avenue is considered appropriate. These avenues may be Internet connections, physical attempts at breaking into the facility to enable cyberattacks, supply chain interdiction, or tapping into communication pathways such as physical cables or wireless networks used by the organization. Most of the time, a holistic red team attack is going to be conducted over a subset of or one of these avenues. The most common holistic compromise engagement by a red team is likely to target the entire organization using Internet-connected avenues of approach only.

Specific compromise engagements offer a more efficient and tailored assessment of an organization (Figure 1-2). They do not provide the potential big picture of the security posture that can be accomplished via holistic compromise. However, specific compromise is likely to lead to successful discovery—and, therefore, mitigation of—vulnerabilities present in a subset of the organization. As long as this subset is comprised of appropriately prioritized assets, it can be an extremely efficient and effective way to conduct red teaming.

Different types of targets delineate the various subclasses of specific compromise assessment. Specific compromise can be as narrow as a specific application running on a specific device with a specified user access level. This type of testing is common in rollouts of new and important application software within an organization. This attack surface, although small, contains potentially some of the greatest risk an organization may face. Specific compromise can also be a prioritized subset of users, systems, or applications within the organization. The specific (or combination of) security objects and types on which the engagement focuses drives the assessment process.

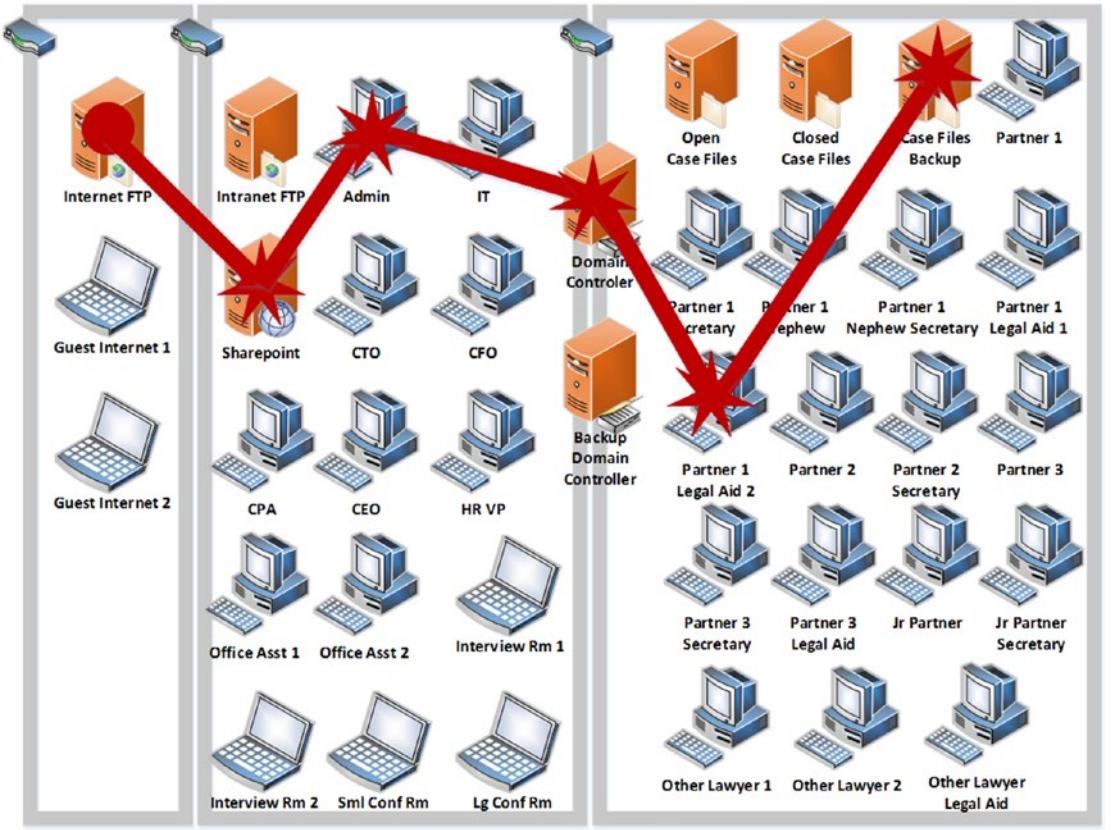

Figure 1-2. *Specific compromise*

Assumed compromise engagements are ones that lean toward being more efficient while giving a potentially less-realistic picture of an adversary. When performed and scoped correctly, though, this type of red team engagement offers perhaps the best cost benefit toward improving security posture.

Assumed compromise can be broken down into the types of access from which the assessment begins and their location within an organization. If holistic and specific compromise attempts leverage an e-mail-propagated malware campaign against an organization, assumed compromise assessments simply begin the assessment from the type of access such a campaign would enable if successful. In this scenario, assumed compromise engagements save potentially weeks of time waiting for a user to open malware in an e-mail, and bypasses the potential ethical and legal risks of such operations. Whether the access given in assumed compromise engagements is a specific user access or an entire machine added to an organization, it sacrifices some realism for efficiency.

The security training of employees with regard to malicious e-mail may not be tested in assumed compromise. However, operating under the assumption that someone will be fooled eventually allows for time to be spent discovering more dangerous and mitigatable vulnerabilities than the ever-present vulnerability of human error.

Advantages

Red team engagements offer advantages over other methods and technologies in improving the security posture of an organization. Red teams are the sharpest tool in the metaphorical shed of information security implements. This is not to say that it is the best, or the best in any given situation; it is simply the sharpest. As mentioned earlier, red teaming can identify the capabilities and shortcomings of an organization's various security assets, which provides a unique assessment of the preparedness of an organization to withstand the efforts of a malicious actor. It is important to understand that this assessment is only as good as the ethical hackers conducting it, and the assessors are as limited or empowered as the scope and rules of engagement to which they are held. All things considered adequate to the situation, red teaming provides a greater cost efficiency in improving security posture when compared to addressing security concerns reactively—*after* they are leveraged by malicious hackers.

Red teaming is considered a sharp tool because it is surgical in its application and can be extremely dangerous in untrained or unethical hands. Conducted by a competent team, it is the only proactive precompromise tool available. Where many security technologies are built around the concept of reacting, red teaming allows an organization to pursue securing and mitigating issues before compromise attempts are initiated, not after. It may be argued that activities such as vulnerability scans and good patch management are proactive as well. It is important to note, though, that although not based on a reaction to a security event within an organization, both are reactions to security events elsewhere that provide details for new vulnerabilities for which to scan or fix. One other tool is considered by some to be proactive in nature—threat hunting—which aims to identify indicators of compromise from actors already within the organization that may or may not already be known aggressors. Unlike red teaming, though, threat hunting is a postcompromise activity.

Evaluating Preparedness

The unique advantage of these proactive and precompromise attributes is that red teaming provides an *understanding* of preparedness whereas other information security tools are attempts to prepare better. Other security tools may better prepare organizational defenses to thwart malicious actors, monitoring to detect them or aid in the effectiveness or resilience of response. Red teaming identifies whether those technologies are effective in increasing an organization's preparedness. It also helps identify wasted or redundant resources within the organization via missed detections, or unnecessary duplication of security event detection and recording from different technologies.

Evaluating Defenses

A successful red team campaign tests the many defensive facets of an organization via interaction with systems, users, and applications, and identifies the ability of these objects to impede the actions of the assessors. An example of a defensive system in an organization is a firewall. This system is meant to stop unsolicited or malicious traffic from traversing from one point to another. The red team tests the firewall in both direct and indirect manners. Indirect testing of a defensive object such as a firewall results from scanning and other reconnaissance activity with systems or services that were intended to be stopped but were allowed through the firewall for one reason or another, such as misconfiguration or a flaw in the system itself. In either case, the defensive preparedness of the firewall system was tested without the assessor having specific knowledge that their actions were supposed to be stopped. Directed testing is when the assessor knowingly tries to get past a defensive mechanism. This type of attempt falls into the two subcategories of subversive exploitation or direct exploitation.

Subversive exploitation is when the assessor knows of the device and attempts to bypass its defensive capabilities by leveraging flaws specific to it or by probing for misconfigurations that allow assessor to get past them. Direct exploitation is when the assessor leverages a flaw or misconfiguration in the system to gain remote code execution in an effort to change the defensive settings of the device to get past it.

Other types of defensive security objects may be evaluated in the same manner. An operating system may have a defensive setting that prevents scheduled scripts from executing with a certain privilege. A flaw in that setting's implementation may allow a red team to run the script at that privilege. Or, the red team may actively pursue a bypass