The Business of Hacking

Creating, Developing, and Maintaining an Effective Penetration Testing Team

—

Michael Butler · Jacob G. Oakley

Apress®

The Business of Hacking

Creating, Developing, and Maintaining an Effective Penetration Testing Team

Michael Butler
Jacob G. Oakley

Apress®

The Business of Hacking: Creating, Developing, and Maintaining an Effective Penetration Testing Team

Michael Butler
Falls Church, VA, USA

Jacob G. Oakley
Owens Cross Roads, AL, USA

ISBN-13 (pbk): 979-8-8688-0173-0
ISBN-13 (electronic): 979-8-8688-0174-7
https://doi.org/10.1007/979-8-8688-0174-7

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Susan McDermott
Development Editor: Laura Berendson
Project Manager: Jessica Vakili

Distributed to the book trade worldwide by Springer Science+Business Media New York, 1 New York Plaza, New York, NY 10004. 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 booktranslations@springernature.com; for reprint, paperback, or audio rights, please e-mail bookpermissions@springernature.com.

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 the Github repository: https://github.com/Apress/The-Business-of-Hacking. For more detailed information, please visit https://www.apress.com/gp/services/source-code.

Table of Contents

About the Authors

Michael Butler is a 14-year veteran of the offensive cybersecurity industry. He got his start by conducting cyber warfare operations with the US Army and NSA. He then went on to build two commercial penetration testing teams, teach multiple offensive cybersecurity classes at Black Hat and other conferences, and become an expert in hacking cloud environments. In 2023, he founded Final Frontier Security to elevate quality assessments and client experience through all aspects of offensive cybersecurity. He has previously collaborated with Dr. Oakley as the technical reviewer for the book *Professional Red Teaming* and is the co-author of *Theoretical Cybersecurity: Principles and Advanced Concepts* (Apress, 2022).

Dr. Jacob G. Oakley is a cybersecurity journeyman, author, speaker and educator with 17 years of experience. A foremost expert on offensive cybersecurity, cyber warfare, and space system cybersecurity, he has advised Department of Defense (DoD) and Fortune 500 executives on strategic mitigation of risks and threats to globally distributed, multi-domain network architectures. He is an adjunct professor at Embry-Riddle Aeronautical University and Steering Committee member for the IEEE Space System Cybersecurity Standards Working Group. His books, *Professional Red Teaming*, *Waging Cyber War*, *Cybersecurity for Space*, *Theoretical Cybersecurity*, and *The Business of Hacking* are published by Springer/Apress.

CHAPTER 1

Introduction

Hacking Is Different

There aren't many books on the subject of leading hackers. Trust me, I've looked. But if you look for a book on how to hack, you'll find them by the truckload. In fact, if you took the number of books on offensive cybersecurity and compared it to the number of books written about other areas of cybersecurity or even information technology (IT) in general, you could easily assume that the field of hacking is one of the largest within IT. Of course, anyone familiar with the field will tell you that penetration testing is a relatively small subset within the cybersecurity industry. The majority of cybersecurity professionals are working to identify, defend, detect, and respond to threats. So why then is the literature on the technical subject of offensive cybersecurity so prolific?

The answer might be fairly obvious – hacking is exciting! It's interesting and flashy. The idea of getting paid to break into IT systems can be very attractive, especially when compared to jobs that may seem more mundane on the surface such as security analysis and engineering. The profession is also very different from its sister professions. To the initiate in cybersecurity, this difference is first made clear by the diverging paths of education. At some point early in the development of their cybersecurity skills, a professional will have to choose whether to focus on the offensive

M. Butler and J. G. Oakley, *The Business of Hacking*,
https://doi.org/10.1007/979-8-8688-0174-7_1

or defensive side of the house. While there is some overlap, the tools, techniques, and even mindsets of professionals on these paths are radically different.

Hacking is different. The skill repertoire a professional hacker cultivates includes identifying a vulnerable server hidden within thousands of data points, deceiving people into giving up sensitive data, and hiding in the noise on a network wire to stay under the threshold of detection. It is understandable that this would require a different approach and mindset than other areas of cybersecurity. While this difference seems to be generally accepted, my years in building and leading offensive cybersecurity teams have led me to another conclusion – leading hackers is different.

Recruiting, motivating, developing, and retaining offensive cybersecurity professionals come with unique challenges, but the differences don't end there. They extend into team scaling, marketing, and sales. The needs of the clients of an offensive cybersecurity team are different and require different strategies to meet. The operational flow is different. The parameters for success are different. The way in which an engagement is approached mentally is different.

These differences arise from the place that hacking has within an organization's cybersecurity programs. It is used to set the direction for the next iteration in security engineering and as the last step in validating the progress that each iteration has made. This is starkly different from other cybersecurity disciplines that are concerned with either the operation and monitoring of defenses (security analysts) or the construction of new defenses to meet threats identified through hacking or other means.

The management-level differences hide pitfalls that catch those new to building and managing an offensive cybersecurity capability by surprise. The differences aren't obvious, making them difficult to anticipate and adequately address. It can take years of stumbling, experimentation, and stressful nights to find the way to navigate the pitfalls. I'm speaking from experience. Even the years I spent as an offensive cybersecurity professional did not prepare me for leading a team and then later building a capability from the ground up. I can look back now on my experiences and see myself groping in the dark for an adequate solution that wouldn't appear for years. I have no doubt that I am not the first person to encounter many of these challenges. In fact, I have spoken to and heard of other teams struggling with the same things I have struggled with. And I often see the same sense of lost frustration in leaders that I had and, to some degree, still have. I am also certain that I am not the first person to find solutions to many of these challenges, but as mentioned at the start of this chapter, I haven't found many that wrote their solutions down afterward.

Bad Team, Good Team

My experience in offensive cybersecurity capability (OCC) management comes from building and leading two different teams over the course of roughly 10 years each. Both teams represented the offensive offering of small cybersecurity consulting firms.

I joined the first team as a penetration tester executing long-term staff augmentation contracts. For the uninitiated, staff augmentation is when a member of a consultant company's staff joins the client's team in a semi-permanent position that is renewed typically on a 6-month to 1-year basis. Before long, I was the contract director, team lead, and senior penetration tester for a contract with a very large commercial organization and a second contract with a very large government agency. I was very busy.

My time building that team helped me to develop an appreciation of the variety of clients that needed offensive cybersecurity services, how their requirements differed, and the techniques that seemed to work best for each. While I very much enjoyed my time on that first team, the team's construction was flawed from the start. The team was created as a reaction to client requests for offensive cybersecurity services. There was no structure, vision, or collaboration. The pentesters on the team were handed engagements by the management and then executed them in a silo.

Much like the team's construction, its management was also reactive in nature. Problems were addressed when they became significant enough to warrant attention. New pentesters were only hired when new work needed to be executed. Tools and techniques were not actively developed unless a team member wanted to put in their own time outside of the contract requirements.

In that team, there were few efforts to foster a connected, supportive, and growing team environment. The team members met once weekly via video call. The call was rather awkward, and the testers retreated to their contract silos the moment it ended.

I am not criticizing any one person other than myself with the lackluster leadership of that team. As one of the earliest testers on the team and the director of the largest contract that included an offensive cybersecurity component, I became one of the de facto leaders of the team. I had a lot to learn about leading an offensive cybersecurity capability (OCC), and my lack of experience and vision did the team no favors. What I did obtain from that experience was an understanding of the problems and challenges inherent to leading that kind of team, a few good ideas, and a lot of knowing what not to do.

I was given a second chance when I was asked to build an offensive cybersecurity capability from the ground up at a new cybersecurity startup. I had a vision and I had learned enough from the first team to know what I didn't want. Over the next several years, the team grew and went through several phases of maturity. From our infancy with just two testers doing whatever it took to make our clients happy to the startup phase of a small team building internal tooling and improving processes to the professional phase with a large team and fine-tuned practices and automation. These phases of growth each presented a unique set of challenges and required me and the leaders within the capability to mature to address them. Our vision developed to include a deeper understanding of the following areas of management:

- Agile experimentation
- Client management
- Capability structure
- Development of team members
- Inspiring collaboration and camaraderie
- Standards of deliverables
- General penetration testing standards

Through this book, we will discuss each of those management domains and their place within the framework of building a successful team that is also capable of growing to meet new challenges.

The difference between these teams is stark but it comes down to two things: a defined vision and a willingness to engage with challenges proactively. I believe these two principles are the bedrock of successful management both in and out of the offensive security world.

In the chapters to come, I will refer back to these two teams, their successes and failures, to demonstrate the right and wrong ways to approach challenges.

Why This Book Matters

My hope and goal for this book is to clearly frame the challenges that anyone involved in the creation, development, and management of an offensive cybersecurity capability will encounter. I will present my own experiences, mistakes, and solutions as I have developed them thus far in my career. This book is not intended to be the definitive source of solutions; rather, it is intended to help begin a larger conversation about leadership in the offensive cybersecurity world.

To that end, I have enlisted the help of my good friend and colleague, Dr. Jacob Oakley. Together we bring 30 years of experience in the offensive cybersecurity industry. That experience spans military leadership, the US intelligence community, defense and non-defense contracting, cybersecurity for space vehicles, and commercial companies that run the gamut from local startups to those listed on the Fortune 100 not to mention extensive time within academia.

Together, we will cover how to build an offensive cybersecurity capability from the ground up, develop it, scale it, and understand your stakeholders. We'll discuss effective assessment practices and how to develop reports and touch a bit on marketing. Finally, we will look to the future of our industry with topics such as cyber arms, cybersecurity in space, and artificial intelligence (AI).

CHAPTER 2

The Service

Definitions

Our exploration of building and managing an offensive cybersecurity service begins with a few definitions to establish a common language between the various types of services.

Offensive Cybersecurity Service (OCS)

An offensive cybersecurity service is the mechanism by which an organization is able to acquire, manage, and execute offensive cybersecurity tasking as well as all elements involved in the management, development, and growth of the service and its personnel. This is not the same as a red team or a penetration testing team although it encompasses such teams. An OCS represents all elements of the service to perform offensive cybersecurity within an organization including elements that are not usually directly associated with a red team or penetration testing team such as sales, marketing, client management, team management, capability development, and more.

This book will explore all areas of an offensive cybersecurity service and not only the topics that are important to the penetration testing team itself. Therefore, you will often see this term used.

M. Butler and J. G. Oakley, *The Business of Hacking*,
https://doi.org/10.1007/979-8-8688-0174-7_2

The definition of this term is broad by design because within the offensive cybersecurity field, there are few subtypes of teams and professionals. In my experience, the various subtypes are far more similar than they are different, and for most of the points in this book, they can be grouped together under the offensive cybersecurity banner. There are of course a few notable exceptions. For example, internal red teams may not find the content on marketing particularly useful. But generally speaking, all types of professionals and teams can benefit from an exploration of the topics in this book.

Team Types

There are two primary labels given to teams of offensive cybersecurity professionals: red teams and penetration testing teams. These terms are often used interchangeably and sometimes one team will fill both roles, but there is an important difference in the objectives for each type of team. We will explore each one to gain an understanding of the differences and where they overlap.

Penetration Testing Team

A penetration testing team consists of IT professionals trained in offensive cybersecurity techniques. The objective of a penetration test is to identify vulnerabilities within the engagement scope. Once vulnerabilities are identified, the team will work to demonstrate the impact of the vulnerabilities through exploitation if the client allows.

The outcomes of a penetration test for the client are

- Identification of previously unknown vulnerabilities
- A deeper understanding of the risks the environment faces
- Identification of weaknesses in the systems and processes that develop and deploy the environment

Let's look at an analogy to express these outcomes. A penetration testing team is assigned to assess a web application. The team identifies a low complexity SQL injection vulnerability and uses it to access sensitive client information. In the engagement report, the team provides the details of the vulnerability and makes recommendations on how to remediate it. In addition, the team suggests more robust dynamic and static scanning be added to the lifecycle of the application to help prevent similar vulnerabilities in the future.

In this analogy, the client would work to remediate the identified vulnerability and improve the application development pipeline to include better security practices, and they would have a greater understanding of the potential impact of a real-world attack.

A penetration test is an important part of the security of any application, system, or environment. They give a real-world perspective and leverage the attacker's mindset. This isn't something that those involved with the development or securing of the system can do. They will not usually have the skills or mindset to carry out an offensive cybersecurity assessment of their environment, and they will most likely make assumptions about the system due to their understanding of it.

Red Team

A red team also consists of IT professionals trained in offensive cybersecurity techniques, but their objective is quite different. The objective of a red team is to test and assess the detection and response capabilities of an environment.

The outcomes of a red team assessment for the client are

- Identification of blind spots in the environment's ability to detect a compromise
- Identification of weaknesses in an environment's ability to respond to a compromise scenario
- An understanding of the level of sophistication required to bypass detection and response measures

As an example, a red team is given access to a host that is joined to the internal network of an organization. The members of the red team emulate the actions of a sophisticated adversary by slowly and stealthily enumerating the aspects of the network that the compromised host gives them access to. This is what is known as an "assumed breach" scenario.

By moving slowly and blending in with normal network traffic, the red team is able to stay under the threshold of detection and thereby cirvumvent network defenses. They work to identify hosts within the network that could provide the team with additional access, escalated privileges, and/or access to services or processes that are critically important to the business of the organization (commonly referred to as "critical terrain"). Once identified, the red team will attempt to find vulnerabilities within these hosts and exploit them to demonstrate the impact of flawed detection and response mechanisms.

As the engagement proceeds, the red team will use less and less stealth and sophistication until they are caught. This provides the client with a real-world understanding of the level of attacker their current defenses are capable of detecting and the level of sophistication necessary to bypass them.

After the engagement is complete, the client can use the results to drive improvements in their internal network's detection and response systems and processes with the goal of detecting attackers that operate at a higher level of sophistication.

Purple Team

One final team type that we need to discuss is the purple team. The purple team is a more collaborative approach to the assessment of the blue team's capabilities. It combines the blue and red teams; therefore, purple! In a purple team engagement, the offensive side executes attacks and other actions within the protected network and the defensive side makes sure that (1) the action is detected and (2) the response is adequate. The great benefit of this approach is the real-time improvement of defenses.

Purple team engagements can go a step further by leveraging frameworks of documented behavior by various groups of attackers. For example, the MITRE ATT&CK framework is a knowledge base for adversary tactics and techniques based on real-world observations. A purple team can use the MITRE ATT&CK framework to emulate the behavior of an adversary that is likely to target the organization. This allows the organization to prioritize efforts to defend itself against specific threats that it most likely faces rather than attempting to be secure against all threats simultaneously.

It is not common for organizations to staff a dedicated purple team, and since the skillset of the red team significantly overlaps with that of the purple team, the red team will often be given both responsibilities. In my experience, when a red team performs purple team engagements, it has an unexpected benefit. It can cool tensions between the red and blue teams who are usually seen as adversarial in their work and can easily become adversarial in their relationship.

Some competition is good. It helps to keep both team sharp when they have some skin in the game. However, I have witnessed organizations that allowed this natural competitiveness to grow to an unhealthy level, which negatively affected the usefulness of the engagements. The collaborative aspect of purple team engagements helps re-establish healthy relationships between the security teams and reminds them that they are all on the same side.

Team Differences

The primary differences between these two types of offensive cybersecurity teams lie within their objectives and client outcomes, but there are secondary differences as well. Red team engagements are most effective when the blue team (the defenders of the environment) are not alerted that the assessment is happening. This creates a more real-world scenario where the blue team must identify and respond to any alerts from the red team as if they are an actual compromise.

On the other hand, pentesting engagements do not require any level of secrecy. In fact, it is often beneficial to have all parties involved in the development and maintenance of the target environment included in the test so that they can provide feedback and suggestions to the testers.

When a pentester identifies a vulnerability, they will report it and may attempt to exploit it to determine the severity of the vulnerability. Red teams test a system until they find a vulnerability that grants a higher level of access, and then they move on to testing the next system. While this methodology does not thoroughly test each system the red team member encounters, it does simulate how a real-world threat actor would move through the environment.

The end product of each engagement, the engagement report, also contains some differences. While both teams will produce a report that highlights vulnerabilities and impact, the red team report will primarily evaluate the alerts and actions that occurred in response to their testing.

We have discussed these two teams as if they are two separate entities, but in practice, both engagements are almost always the responsibility of the same team due to the significant overlap of skills required. Not only does one team handle both types of engagements, but both types of engagements may be found in the same assessment. For example, a team may perform an assessment of a web application and find a significant vulnerability that gives them access to the server that hosts the application. With the client's approval, the team may pivot into the client's internal network and evaluate the blue team's response or lack thereof. A pentester can simultaneously evaluate an environment and evade detection.

Internal vs. Consultative

The second major difference between the teams within offensive cybersecurity is their client base. Some teams serve the needs of a single client. These teams are either contractors or employees brought on board to consistently provide offensive cybersecurity services to the organization. These kinds of teams only exist in rather large organizations who have a need for a dedicated internal team. My first exposure to commercial penetration testing was with such a team. I worked for a small cybersecurity firm that had a contract to supply fulltime offensive cybersecurity professionals to a very large commercial company.

Other teams serve a variety of clients. These clients only need the services occasionally, perhaps annually or quarterly. These kinds of teams exist at services-based cybersecurity companies who market their capabilities and services to bring in clients and scale the team to meet the market demand. The engagements these teams perform typically last anywhere from 2 weeks to a few months before the pentesters involved move on to another client. The second team I joined was primarily consultative. The team executed engagements for multiple clients every week.

It's important to recognize that although there are some differences, these two types of teams are more alike than they are different. The challenges present in one type are generally present in other type with a few notable exceptions. The differences between internal and consultative teams are significantly reduced once you consider that even when serving a single organization, an internal team is responsible for testing multiple departments, networks, and applications. Interacting with those various departments is no different than a services-based team interacting with multiple clients. For ease, I will refer to anyone who requires offensive cybersecurity services and to whom the final report is delivered as a client, whether that party is an internal department or an external customer.

Establishing the Service

Vision

If you've worked within the offensive cybersecurity field for a few years, you'll most likely have encountered teams that were started without any real consideration as to their structure. This lack of vision results in a structure that is developed in reaction to the needs of the work. The outcome is a haphazard patchwork of short-term band-aid solutions put in place to solve immediate problems without consideration for the long-term health of the service.

The first commercial penetration testing team that I joined took this approach, or lack of an approach, and the result was the following team dynamic that has become all too familiar in our industry:

A single senior technical leader begrudgingly takes the responsibility of organizing the team and their engagements while, often publicly, wishing they were able to spend more time on the technical side of the job and less time doing project management. The team itself is made up of mostly mid- to senior-level pentesters who work remotely and rarely communicate unless they are collaborating on a given project. The team meets once a week or less to discuss projects and possible operational issues in a video call where very few team members turn on their camera. The call contains many awkward pauses that go on for just a little too long, and the team members are happy to end it as quickly as possible.

This service structure is less than ideal. It results in team members having little reason to remain on the team other than their paycheck. It does not attract motivated and hungry testers to join the team. It does not produce engaged testers who are passionate about their work and who develop tools to assist the team as a whole. The quality of the engagement output drops over time, and team member turnover becomes a serious challenge.

Of course, no one sets out to build this kind of team structure. It is the result of there being no planned structure, no vision. It can begin from an upper management-level decision to create an offensive cybersecurity service due to an internal or market requirement. The management then hires someone who knows a lot about the technical aspects of offensive cybersecurity to lead the new team, and then they consider the job done as the requirement has been met. If the construction of the service lacks vision from the onset, it is unlikely to suddenly attain a purpose once it is established. As a friend of mine once said, "You can't accidentally do well for the long term."

So we have to start with a vision. The vision needs to be clear and simple enough to be easily communicated and implicitly understood. This might seem a bit daunting at first, but it's not as intense as you might initially assume. In fact, it is preferrable that the initial service vision is very simple.

The vision should consist at minimum of the basic priorities of the service and an idea of what the service and its team will look like in one year. Even this very simple vision will give the team a much higher chance of success than a team without a vision.

The service vision will change and be adapted over time as the service members and their leader mature and develop a greater understanding of their mission, what works, and what doesn't work. A basic vision will lend itself to this growth and adaptability from the start.

Structure

Management of an offensive cybersecurity service consists of five domains:

- Lead
- Project
- Client

- Team
- Capability

When an OCS is first established, its structure will be rather simple. This is not because some of these five domains do not exist in new OCCs. Rather, it is because multiple domains are managed by the same person or people. This is casually referred to as wearing multiple hats. So even though a new OCS will not require dedicated personnel or as much dedicated effort to each domain as a more mature OCS, it is still important to note the domains and track the service's maturity across them.

Lead

The lead domain is concerned with all operations that occur between the initial notification that a lead exists and the lead becoming a schedulable project. This domain exists even for internal OCCs even though they do not require a traditional sales/lead pipeline. A lead for an internal team is defined as a request or requirement to execute an assessment of a specific environment. For example, a product may have a new update that requires a pentest before it can be pushed to production. A lead for a team of consultants is defined as a potential project from a client who is interested in the services of the OCC.

For consultative teams, this domain may seem misplaced. You may be thinking, "aren't leads the responsibility of the sales team?" While that idea is mostly correct for teams that work with a sales team, the sales team will need technical support from the OCS to communicate the technical details of the project's requirements and the types of assessments the service provides to the client. Sales people rarely possess the technical education to convince clients of the service's quality and to adequately scope the client's project. They will often lean on the members of the OCS to provide that support.

Within the lead domain, the OCS develops processes to educate clients (even internal clients) on OCS services, help the client develop project requirements, establish project scope, discuss testing requirements (access, credentials, lists of target IP addresses, etc.), ensure the paperwork contains language necessary for project execution, establish a schedule for the project, and select a calendar date for the project to begin.

Project

A lead becomes a project once any necessary paperwork is signed and a date on the calendar is selected. The project domain is responsible for ensuring that the team is ready and able to execute the given engagement. That means that there is space on the team's calendar, team members with the skills that the engagement requires are assigned to it, any special considerations or objectives are communicated with the assigned team members, and all technical requirements such as scope and access have been negotiated and provided to the team.

Once the engagement begins, project management is responsible for monitoring the engagement to ensure that all aspects of it are executed and that any unique client requirement is met. At the end of the engagement, the project management handles the deliverables and communication of findings to the client and discusses any further activities that might be necessary before the engagement is closed. An example of further activities would be re-testing identified vulnerabilities once the developers of a given system have implemented patches.

Client

Clients are the single most important factor for any offensive cybersecurity service, and client satisfaction is the primary metric for team success and output quality. This might be difficult to swallow for many offensive cybersecurity professionals. Our job is technical. We find vulnerabilities, exploit them, and report. Someone else can manage the clients! This