HADRIAN

EBOOK

Through the Hacker's Eyes

Automating Offensive Security for External Assets

Table of Contents

Introduction

The external "hacker perspective" is essential for robust cybersecurity because it introduces a level of scrutiny and insight that internal teams often cannot provide. While in-house security experts are critical in maintaining and strengthening an organization's defenses, they are often bound by institutional knowledge, limited viewpoints, and familiarity with the system, which can inadvertently create blind spots. Hackers, on the other hand, approach a system with no preconceived notions or constraints, simulating real-world adversaries who exploit these very weaknesses.

A critical aspect of this external perspective is its ability to identify vulnerabilities from an attacker's standpoint. Hackers don’t just follow known tactics; they adapt, innovate, and think creatively about how to bypass defenses. By simulating their approach, organizations can uncover weaknesses that would otherwise be overlooked by internal teams, who may focus on more routine or theoretical vulnerabilities. Ultimately, an external perspective allows for a more comprehensive approach to cybersecurity—one that mirrors the dynamic, constantly shifting nature of real-world attacks.

What is Offensive Security?

Even the best security can be circumvented if is it not properly implemented or continuously tested. Offensive security refers to the proactive approach of simulating the behavior, tactics, and techniques of an attacker to assess and test an organization's security posture.

Unlike traditional defensive security, which focuses on protecting systems and responding to attacks, offensive security flips the equation. It places security professionals in the role of the "hacker," intentionally trying to breach the organization’s defenses to uncover gaps and vulnerabilities.

The goal of offensive security is to emulate the strategies of real adversaries—whether they are external hackers, insider threats, or even nation-state actors—so that organizations can identify and patch weaknesses before they are exploited in an actual attack.

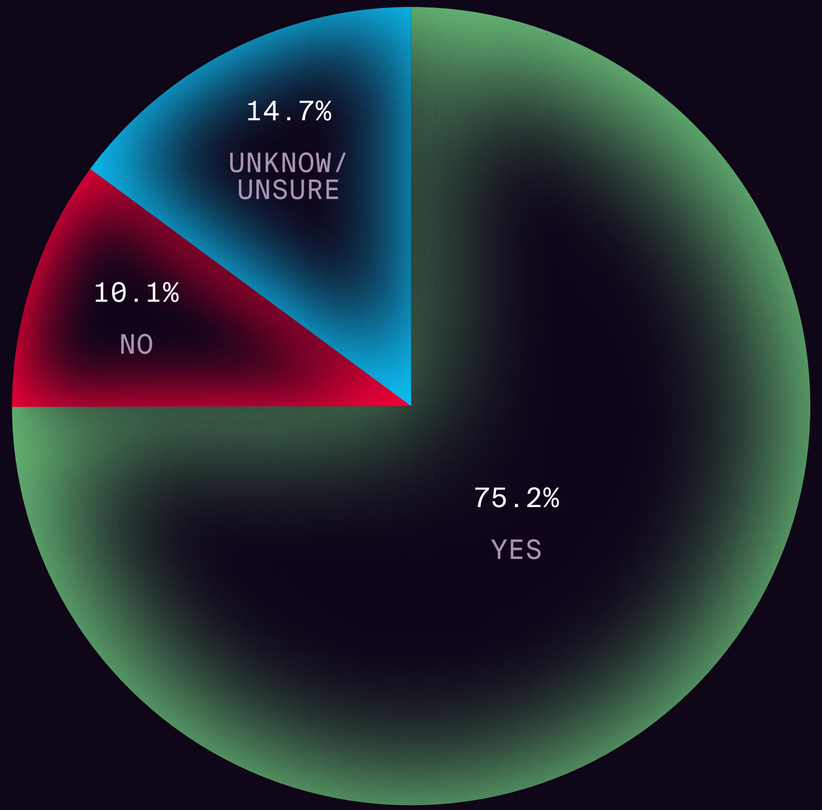
7/10

of organizations have experienced an attack targeting an unknown, unmanaged, or poorly managed external-facing asset.[1]

69%

of organization’s say their security approach is reactive and incident driven.[2]

Is unknown risk causing you to increase offensive/proactive security practices?[3]



[1] ESG, Security Hygiene and Posture Management (2022) | [2] Ponemon, The Cybersecurity Illusion: The Emperor Has No Clothes (2019) |
[3] SANS, Building a Resilient Offensive Security Strategy (2023)

Why Focus on the External Attack Surface?

An external attacker's approach might exploit a vulnerability or weakness that internal teams didn't foresee or considered too low risk to prioritize. This makes the hacker's perspective an invaluable tool in verifying the strength of security defenses, ensuring they are resilient against current and evolving threats.

Attackers innovate faster than defenses can be developed. The only way to stay ahead is to continuously challenge your defenses with the mindset and methods of those who seek to exploit them. Without this outside-in approach, organizations risk underestimating the sophistication and persistence of modern threats, leaving critical gaps in their security strategy.

Checklist for The Hacker Perspective:

- ✓ Have we mapped out all the entry points into our network and systems?
- ✓ Do we have ongoing monitoring of our external-facing assets (websites, APIs, cloud platforms)?
- ✓ When was the last time we conducted a Red Team or penetration test, and did it cover all aspects of our environment?
- ✓ Are we aware of all the assets within our environment, including shadow IT, and cloud services?
- ✓ Are we considering third-party vendors and contractors that might be introducing new risks into our environment?

Stages of Offensive Security

The hacker perspective is revealed by applying an offensive security methodology.

Reconnaissance

Reconnaissance, the first step in offensive security, focuses on collecting information about the target's systems, networks, and organizational structure. This phase helps identify potential attack vectors and weaknesses by mapping out assets and relationships, allowing attackers to pinpoint the most vulnerable entry points.

Contextualization

This phase systematically examines discovered systems to extract key information such as live hosts, open ports, running services, and technology stacks. By using fingerprinting techniques, attackers identify underlying systems and vulnerabilities, helping to locate weak spots in the environment.

Validation

In this stage, weaknesses are targeted to gain unauthorized access or escalate privileges. The goal is to test whether these vulnerabilities can be exploited to achieve the attacker's objectives, such as accessing sensitive data or breaching internal networks, while also evaluating the effectiveness of security controls and incident response.

Prioritization

After identifying exploitable weaknesses, prioritization assesses the severity and risk posed by these vulnerabilities across systems, networks, and applications. This phase helps determine which issues should be addressed first based on potential impact.

Remediation

The final phase, remediation, involves compiling findings into a report for the organization to act on. The report includes the attack path, exploited vulnerabilities, and recommendations for fixes, serving as both an immediate guide for corrective actions and a strategic roadmap for long-term security improvements.

Automating Offensive Security

Automation and AI can enhance offensive security at every stage.

Reconnaissance

AI quickly gathers and analyzes vast amounts of data from external assets, networks, and systems, automating tasks like asset discovery, data collection, and threat intelligence aggregation.

Outcome: Increases visibility of the external attack surface and expands testing to all assets.

Contextualization

Automation identifies live hosts, open ports, services, and technologies faster and with greater accuracy, correlating them with known exploits and attack techniques, providing deeper insights into potential risks.

Outcome: Enhances threat detection accuracy by identifying every potential vulnerability.

Validation

Automation simulates attacks to validate exploitable vulnerabilities, while AI mimics sophisticated adversary tactics, helping test the effectiveness of security controls.

Outcome: Ensures realistic testing of security defenses and eliminates false positives.

Prioritization

AI helps rank vulnerabilities based on potential impact, exploitability, and organizational risk, enabling security teams to focus on the most critical issues.

Outcome: Improves resource allocation by identifying the highest-impact vulnerabilities.

Remediation

Automation generates actionable reports with tailored recommendations and tracks progress on fixes, while AI optimizes remediation strategies based on organizational context and resource constraints.

Outcome: Streamlines remediation efforts and ensures long-term security improvements.

Comparing Offensive Security Approaches

The use cases and strengths of each approach are distinct and should be layered for holistic security testing.

	Vulnerability Scanning	Penetration Testing	Red Teaming	Automated Offensive Security
Scope	Known Assets	Critical Infrastructure	Objective Based	All External Assets
Speed	Hours	Days to Weeks	Weeks to Months	Minutes
Sophistication	Basic	High	High	Medium
Frequency	Scheduled	Quarterly to annually	Annually	Event-based
Tooling	Automated	Mixed	Manual	Automated
Cost	Low	Medium	High	Low
Aim	Tests for known vulnerabilities and compliance issues	Identifies vulnerabilities in specific systems or applications	Evaluates overall security response and resilience	Reveals the hacker perspective for proactive remediation

The Value of Automated Offensive Security

Thinking like a hacker reveals how real-world attacks could compromise applications and infrastructure. Automated offensive security enables organizations to understand this perspective and proactively mitigate threats.

Hadrian reveals exploitable vulnerabilities by continuously assessing threats across your entire external attack using the same techniques and behaviors as hackers.

Unlike static penetration tests, Hadrian offers a dynamic, evolving approach to security that adapts to your changing attack surface. With automated insights and prioritization of critical risks, Hadrian equips security teams to stay ahead of threats and fortify their defenses before attacks occur.

10x VISIBILITY OF CRITICAL RISKS	Gain real-time visibility into every asset and exposure in your digital attack surface. Hadrian's 24/7/365 analysis keeps you constantly aware, minimizing the window of vulnerability.
10 HOURS SAVED PER WEEK ON AVERAGE	Focus on exploitable risks and eliminate false positives with in-depth penetration testing. Hadrian's fully automated assessments are seamless and enriched with threat intelligence.
80% REDUCTION IN MEAN TIME TO REMEDIATE	Accelerate response time and create a step change in security posture. Hadrian triggers and orchestrates workflows to streamline remediation and prevent threat actors from attacking.

Key Stakeholder Benefits

Stakeholder	Benefit	Areas Improved
CISO	CISOs gain a deeper understanding of the organization's security posture, enabling more informed decision-making around risk management	▪ Reduced risk exposure ▪ Improved board-level reporting ▪ Better resource allocation
Penetration Testers	Automation streamlines time-consuming tasks like vulnerability scanning and data analysis, allowing testers to focus on high-priority issues.	▪ Rapid testing of zero-day exploits ▪ Automation of time-consuming tasks ▪ Actionable recommendation
SOC Team	For the SOC team, adopting a hacker mindset helps anticipate advanced attack methods and fine-tune detection capabilities.	▪ Faster detection of risks ▪ Fewer false positives ▪ Lower remediation time
Development Teams	Developers can seamlessly integrate security into the deployment process, leading to more secure applications in production	▪ Fewer vulnerabilities in production ▪ Faster patching post-release ▪ Lower risk of brand damage
Finance Department	The finance team can better quantify the potential financial impacts of cyber threats and help prioritize investment decisions	▪ Clearer financial impact of cyber risks ▪ Improved budgeting for investments ▪ Better ROI on security spending

About Hadrian

Hadrian is revolutionizing offensive security through automation, enabling security teams to operate faster and scale effortlessly. To uncover threats, our autonomous Orchestrator AI tests continuously to comprehensively assess internet-facing assets. The cutting-edge technology is cloud-based, completely agentless, and constantly updated and improved by Hadrian's ethical hacker team.

Trusted worldwide by market leaders

NBC	amadeus	CRÉDIT AGRICOLE
AUTODESK	ABN·AMRO	London Business School
RITUALS...	SIEMENS energy	BLINQX

The Orchestrator AI