FORTRA

GUIDE (Core Security)

The Complete Guide To Layering Offensive Security

What does offensive security really mean? In today's world, cyberattacks happen every few seconds and can result in catastrophic damage. In fact, according to the Ponemon Institute, the average cost of a data breach is now $4.4 million globally. How is it that some businesses seem better protected against the harmful, and often long-term, consequences of such threats? It's the difference between being solely reactive and introducing a proactive component to your cybersecurity strategy.

Offensive security is when organization takes steps to actively anticipate and prevent cyberattacks instead of only reacting once an attack has occurred. The best offensive security takes a layered approach to identify vulnerabilities and exposures. No single tool or technique comprehensively delivers an offensive security strategy. Instead, through a combination of solutions and practices, businesses can create an in-depth understanding of their organizational threat landscape, viewing weaknesses as an attacker would perceive them.

This guide will investigate how your organization can layer offensive security tactics into a holistic security strategy.

Offensive Security 101

Conventional security approaches are typically reactive or defensive, waiting for bad actors to make a move before addressing attacks. However, there are often delays in detecting attacks that can still threaten an organization. Most companies take an average of 277 days to identify and contain breaches. Offensive security uses a proactive, adversarial approach, employing the same methods that cybercriminals use to test security protocols and technologies, and therefore catching security gaps before attackers can find and exploit them.

Benefits of Offensive Security

Offensive security is not any single type of attack, process, or technology. Instead, it's a collection of methodologies, many of which employ tactics real-world attackers utilize. These methods are tailored to assess security strategies, gathering threat intelligence to minimize the risk of damaging or disrupting business operations and infrastructure.

Attacks commonly used in an offensive security engagement include fuzzers, port scanning, vulnerability scanning, and network traffic capturers. Attackers use the information gathered from these tools to determine an operational attack plan geared toward likely exploitable targets rather than blindly poking at the infrastructure until they identify an exploit. Security teams can use that same information to identify possible gaps or vulnerabilities in security posture.

These gaps can range from misconfigurations to simply having applications with unresolved vulnerabilities. Finding the flaws in an organization's security posture before outside attackers do creates an opportunity to fix or mitigate the weaknesses before they can be exploited.

Employing both offensive and defensive security practices results in a more well-rounded cybersecurity program and makes an organization more resilient to attacks. Offensive security also helps validate defensive security.

Detection and response capabilities get a controlled test during offensive security engagements, showing exactly how effective they are. Identifying flaws in implementation and operations should be the initial goal, followed by risk-based prioritization and a remediation and improvement phase that brings both teams together to strategize optimizations.

Building an Offensive Security Team

One of the first questions organizations must tackle when creating an offensive security team is who will be conducting the testing. Organizations are not restricted to internal resources. They also can consider outsourcing the task to third-party services like a red team or combining the two with a hybrid approach. According to the 2022 Pen Testing Report, 63% of those surveyed used both internal and external teams to some degree. Choosing the appropriate team makeup requires assessing the engagement's scope and determining if the available resources and skill sets are a good match or if external help is needed for some or all of the operation.

No matter who ends up making up the team, deploying an offensive security operation in your organization involves more than simply assigning security engineers to the task and expecting insightful findings. Effective offensive security projects are methodical and choose the right tools and personnel to accomplish the pre-determined scope. This may include anything from routine scans determining a baseline to teams gauging the organization and efficiently performing surgical attacks against it, similar to how real attackers work.

Defining Scope

Offensive security practices are most effective when scoped to focus on specific goals or aspects of an organization rather than the entire organization, which can be too broad. Much like building a skyscraper, it is a big task and has to be taken in phases to be effective. Testing is very similar, with the most value gained from focused testing rather than just attacking the entire organization. With a concentrated test, teams can

conduct an in-depth analysis of targeted systems and services rather than using a scattershot approach to hope for a successful exploit.

For example, by scoping only parts of the environment relevant to PCI, testers can concentrate on whether these systems meet the compliance mandates.

The same idea holds for applications, such as an enterprise resource planning (ERP) system. It creates a smaller pool of resources that must be analyzed and tested, allowing testers to take time to investigate rather than taking a cursory glance and moving on to other targets.

Gathering Intelligence

At the heart of offensive security is the adversarial mindset starting with reconnaissance. Intelligence gathering comes from several tools that help testers understand the environment. Offensive engagements may be clear-box, where all the infrastructure, ports, services, and other components are presented to the attacker at the onset. Alternatively, it could be closed-box testing where nothing is known from the beginning, requiring ethical hackers to invest time in analyzing the infrastructure before starting attacks. Also, a hybrid approach gives testers some information, reducing the intelligence gathering phase without giving away all the secrets.

No matter the design of the testing, intel gathering is crucial for a high-value test. Even if organizations present all known information, details may be unknown or accidentally omitted, so some intelligence gathering will still occur in any engagement. For example, in an assumed breach scenario, testers may access to the environment, but they'll need to learn more in order to pivot and escalate privileges to attain sensitive data or root control. Quality tools are crucial for helping testers identify where elements such as unlisted systems and services may have been omitted.

Tools

There are a wide variety of tools available to testers to help them not only gather information but also execute on findings. These tools may come as individual applications or be bundled into a complete toolkit to consolidate findings and pass information as input from one tool to another.

Commonly used testing tools include:

- **Port scanners** - Scan the network for open ports to indicate possible services being available.
- **Vulnerability Scanners** - Analyze different endpoints looking for indicators of known vulnerabilities that may be exploitable.
- **Decompilers** - Take in binary applications and attempts to deconstruct them into source code to locate flaws and information such as hard-coded API keys that they can use in attack phases.
- **Static Application Security Testing (SAST)** - Reviews source code to identify coding issues that might be exploitable such as buffer overflows or injectable APIs.
- **Profiler** - Recon tool that gathers site information as a user, identifying available applications and plugins on the host site.
- **Fuzzers** - A type of dynamic application security testing (DAST), these automated testers provide invalid and unexpected input to applications for identifying potential input exceptions.
- **Pen Testing Suites** - Full suite pen testing toolkits provide an array of functionalities together to streamline testing and centralize analysis.
- **Exploitation Tools** - Apply exploitation scripts against targets to validate if identified vulnerabilities are exploitable.
- **Capturing/Manipulation** - Sit in between network connections allowing testers to modify inputs on the fly to circumvent controls on the visible interface

- **Agents** - Are injected into a target's memory to execute tasks on the attacker's behalf as the target.
- **Simulation Solutions** - Implanted data trackers and rootkits that mimic common malicious actor tactics, helping to highlight flaws in detection capabilities.
- **Command and Control (C2) Frameworks** - Manage compromised machines using hard-todetect communications, allowing attackers to take remote actions stealthily.

Conducting Engagements

In conducting security assessments, there are two distinctly different goals depending on the type of engagement. Attacks goals are dictated by the type of testing and come in two major varieties:

Red Team - Teams conduct a full attack simulation in order to gain control or capture high value data using the same tactics as a threat actor which may include initial breach, escalation of privileges, or achieving persistence

Penetration Testing - Teams are looking to determine the true potential a vulnerability has for compromise, determining the attack path that could result if exploited.

The attack process for both of these tests can look similar. Once testers understand where the flaws in the infrastructure exist, they start exploring in earnest. Obvious vulnerabilities are probed to see if actionable exploitation can occur. This information drives further exploitation and pivots into the infrastructure, making this more fluid than information gathering, as it is results driven. However, there are distinct differences between these engagements. For instance, while pen testing uses attack techniques to test security controls, the scope is more finite, meaning testers may limit their movements.

It is important to note that if not done correctly, security testing can result in accidents that cause an unintentional outage/interruption. Preparation and communication is crucial for not impacting vital operational systems both during or after engagements. Testers need to have active contact with system owners and be prepared to stop if an exploit leads to an unintended denial of service (DoS). They also need to perform thorough cleanup so that backdoors opened and used during testing are not unintentionally left open. Low-quality toolsets do not always detect these conditions.

Comprehensive Reporting and tracking

The testing aspects of Offensive security are pointless without translating the findings into actionable insights. Testers take results and distill them down to information ingestible by other teams. Doing this requires more than a copy-paste as many assets, especially those that are cloud-based, may not have the same IP as when the testing occurred. Testers need to ensure that findings for endpoints have been correlated with hostnames in an asset reconciliation process to ensure that team members remediating problems can identify the actual host. Reporting is such an essential part of offensive security that reporting capabilities are the most common feature that security professionals look for in pen testing solutions.

Prioritized Remediation

Organizations need to take the information gathered by testers and determine remediation prioritization. The truth is that not all vulnerabilities need remediation, which is just as well because most teams have limited resources. By using a risk-based approach to remediation prioritization, teams can optimize resources and focus their attention on only those weaknesses that pose the greatest risk to their unique organization. Often the most actionable or highest impact findings can be addressed immediately, dealing with lesser results over time.

Getting the Job Done

Organizations implementing offensive security testing need the right people, processes, and technology to get the job done. Companies get the best of both worlds by using tools that streamline security efforts and empower teams to do more effective and efficient work. For best results, identify tools for your stack work well together, either through integrations or interoperability, or with vendor consolidation which enables centralization of tools and support. This symbiosis will simplify each step, from assessment and scoping to testing and remediation.

See how our Offensive Security Bundles can help strengthen and streamline your security efforts.

Maximize Your Security Stance by Bundling Your Offensive Solutions

Explore the Offensive Security Bundles and find out more about the benefits of combining vulnerability management, pen testing, and adversary simulation solutions.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.