Cybriant
strategic. adaptive. resilient.

PENETRATION TESTING SERVICES - OVERVIEW

Enterprises with mature security environments implement monthly internal & external vulnerability scans along with annual penetration tests. These types of tests are traditionally carried out by third-party vendors who are highly specialized in this type of work: And from a legal perspective an organization can avoid issues related to "Auditor Independence" and "Conflict of Interest" by utilizing an unbiased outsider, which is an industry best practice approach. These important, and proactive tests are used to expose vulnerabilities in organizational systems before hackers, cybercriminals and bad actors have a chance to exploit them. It is important that you protect your enterprise assets and those of your customer base. Our Technical Security Testing will provide you with actionable intelligence data that you can use to achieve your goals.

Your Cybriant Strategic Services Team

Steve Strater, VP Strategic Services
CISSP, CRISC, ISO/IEC 27001 ISMS Certified Lead Auditor CHPSE, CISA, CDPSE, CCSK v4, AWS CP, PCIP, MBCP/PSP Candidate, CCSK v4, CCNP, CCNA, CCDA, JNCIA, Former QSA

Jamie Beth Maragas, Lead Auditor
CISSP, CRISC, CDPSE, ISO/IEC 27001 ISMS Certified Lead Auditor, CBCP, CCSK v4, AWS CP Candidate

The Technical Testing Team
Our highly specialized team of information technology and security specialists come from backgrounds with the Department of Defense, Department of Energy, Cisco, National Grid, NASA and many other global organizations. Our Pen-Testers hold prominent cybersecurity industry certifications such as CISSP, SANS/GIAC, GPEN & GXPN, and OffSec OFCP, OFWP, & OSCE, among many others. They are experienced, talented ethical-hacking, penetration testing and social engineering experts who have safely performed thousands of these proactive cybersecurity tests offering our clients a level of assurance and protection for their assets.

Types of Penetration Tests

Black Box testing refers to a Penetration Testing method whereby an ethical hacker has no prior knowledge of the target system. The goal of a Black Box penetration test is to determine the vulnerabilities that are exploitable from outside the network by malicious intruders, hackers or cyber warfare attack. Our team of expert penetration testers are highly skilled in the tools and methodologies for manual penetration testing and can create their own mapping of the target network as they seek to find the vulnerabilities that exist. The downside of this approach is that the limited information provided to the pen-testers increases the probability that vulnerabilities will be overlooked and decreases the efficiency of the test. Since testers do not have the information necessary to target their efforts towards the most high-value, exposed and vulnerable targets, if in fact the testers are unable to breach the perimeter, any vulnerabilities of the internal services will remain undiscovered and therefore, still at risk of being exploited.

Grey Box testing is the next step up from Black Box testing, as the Penetration Testing Team is provided access, credentials, and knowledge levels of a user, potentially with elevated privileges on the target system. Gray Box pen-testers typically have some knowledge of a network's internals, which may include the design and architecture information as well as an account internal to the network. Armed with this information, the pen-testing team can better focus their efforts and increase their coverage on the systems with the greatest value and risk from the start, rather than spending time ascertaining this information on their own. Access to internal account credentials also allows for testing of security inside the hardened perimeter, which walks through a series of tasks cultivated especially for identification and simulates the activities of a malicious inside-user attack, or that of an intruder with longer-term access to the network.

White Box testing is the opposite of Black Box testing, and may also be referred to as Clear Box, Crystal Box or Open Box testing. White Box Penetration Testers are given full access to the target systems' source code, network architecture/infrastructure, credentials, etc., creating the challenge of sorting through the massive amount of data provided to identify vulnerabilities and potential points of weakness, but provides the most comprehensive analysis and assessment of both the outward-facing and internal networks and greatly improves the probability of discovering weaknesses and vulnerabilities. Thus, White Box testing is the most time-consuming, and most expensive type of penetration testing.

RED TEAM vs BLUE TEAM TESTING

RED TEAM TESTING simulates an authentic, targeted cyberattack in an effort to locate the weaknesses and vulnerabilities in an organizations' technical infrastructure and/or physical defenses. By emulating a malicious hacker working in "stealth" mode, we can test the effectiveness of your internal security controls, policies and procedures, monitoring/detection/alerting, and incident response capabilities under various real-world attack scenarios.

Using the multitude of sophisticated intrusion techniques available to real hackers, a Red Team exercise tests the resilience of websites, web applications, network infrastructure, and internal applications, incorporating social engineering tricks and phishing emails to obtain login credentials to breach existing defenses and obtain sensitive data, or install malware. Conducted over a much longer period than a typical penetration test, this comprehensive engagement will provide invaluable insight and information as to how an organization responds internally to various malicious attack attempts and evaluate the true state of its' cybersecurity infrastructure, holistically.

The **Blue Team** are the organizations' internal security professionals and staff - the defenders of the exercise. In some cases, an organization may choose to inform its internal teams of the exercise, allowing the Red and Blue Teams to collaborate and work actively together (becoming a Purple Team) in identifying weaknesses and vulnerabilities, however, this will not produce authentic incident detection/response results.

The Penetration Testing Process

Reconnaissance

The Cybriant team will gather evidence and information on the target of the attack, using both active and passive techniques, in an attempt to find publicly exposed information that could lead to a security threat.

Scanning and Enumeration

Following the Reconnaissance stage, Cybriant will perform a variety of information gathering assignments in order to enumerate resources, hosts and services that the team may be able to access. We will assess the security of the selected applications, focusing on remotely exploitable vulnerabilities, security architecture, design and implementation, and controls with respect to user access, privilege levels, development and delivery of the applications and collect the necessary evidence to document the presence of the vulnerability. The target system will be given due care so as not to damage it.

Vulnerability Mapping and Penetration
Cybriant will look for vulnerabilities in enumerated computers and devices and attempt to exploit them. We use a combination of manual techniques and enterprise-grade software to analyze all discoverable network resources and enumerate security issues. We will review all aspects of the in-scope network, and where successfully penetrated, we will attempt to move laterally and escalate privileges in order to determine the full extent of any issues, including the points at which sensitive data can be accessed. This stage includes looking for:

- Vulnerabilities
- Missing security patches
- Malware
- Backdoors
- Rogue network traffic, such as hosts communicating with botnet-infected systems
- Known/unknown processes
- Web services linking to malicious content
- Rogue or forgotten devices
- Potentially unwanted or unmanaged software
- Misconfigured devices
- Unintended user access capabilities

Philosophy
We perform the bulk of our testing manually, with an effective real-world approach that ensures the best outcome for our clients. Unlike many of our competitors, we do not simply use automated tools such as Nessus or MetaSploit, preferring to use hands-on techniques to safely and effectively attack, evaluate and document the security of your infrastructure. In addition to ensuring that we provide the most thorough and accurate assessment possible, our methods greatly reduce the risk of unintended Denial-of-Service (DoS) attacks during the exercise, which is a potential risk when automated testing techniques are used.

Approach
Cybriant will assess the security of the designated External Network, including the front-end, back-end, and underlying hosting architecture. Our work approach for web application penetration tests is modeled around the Open Web Application Security Project (OWASP) testing methodology and as such follows the current OWASP recommendations and best-practices. We built our proprietary testing methodology specifically around the OWASP testing guide as it is the definitive resource for web application penetration tests. Using this approach allows us to be creative in our approach while staying within a secure framework.

Methodology
Cybriant uses a balanced methodology of both code review and penetration testing. Generally, we mirror the site we are testing with a web spider that downloads all the pages and front-end code to make a local copy. We go through and take a look at any included JavaScript, framework-specific generated code, third party plugins, and any other dynamically generated DOM/HTML. The team then gets together to brainstorm on what the possible issues and attack scenarios would best fit the product.

At this point the team splits up tasks, again keeping the tasks roughly mapped to the OWASP top-ten application vulnerabilities. One portion of the team maps any user input and traces its path throughout the application. Another portion of the team visits the site via an intercepting-proxy - mapping, altering, and modifying all headers and cookies. The final portion of the team looks for vulnerabilities in the webserver software itself, the back-end technologies, framework and any other server specific areas. The user input audits determine such things as what filters are applied to input, where and how user input is stored and routed, how is the input modified as it travels through the application, and where our input can be seen as output. This is where we discover primary injection vulnerabilities (e.g., XSS, CSRF, ...). The team members that focus on visiting the site via an intercepting proxy will look for any kind of vulnerability or error condition that can be generated by modifying or altering cookies, session data, encoding, variables representing authentication, or HTTP headers - in summary, any data between the client and the server whose purpose is information, session management, or authentication. Also included in these audits will be such things as reviewing robots.txt, attempting to discover hidden directories, discovering backup files (e.g., .index .aspx .bak), and other similar audits for source code, file, logging, or access exposure.

Finally, the team looks at vulnerabilities in the web server software itself, in the framework used (if one was used), in back-end technologies, and any vulnerabilities in discovered exposed information that could be used for social engineering, phishing, or any other attacks used primarily to increase access or gain a foothold.

Final Penetration Test/Red Team Exercise Report(s)

Throughout the penetration test, Cybriant will document and record the exercise. Cybriant will provide a full report of the penetration test which will include:

- **Executive Summary** for Upper Management and Stakeholders that gives a brief high-level overview of the results.

- **Attack Summary** for Upper Management, that gives a concise explanation of the exercise and results without overwhelming technical jargon. This includes showing the protective measures that worked effectively and all discovered issues that lead to penetration of the network. Findings will be ranked in order of severity Critical, High, Medium, Low or Informational.

- **Full Attack Narrative** for Technical and Security teams, that gives granular detail of the entire exercise and everything discovered, complete with screenshots, proof of penetration, code, and technical details.

- **Remediation Actions**, ranked in order of severity, detailing the exact steps that need to be taken in order to fix all vulnerabilities and issues discovered in the exercise. This section provides a clear roadmap for your technical personnel to expeditiously close all security vulnerabilities and gaps discovered.

  The Final Report will be kept strictly confidential.