Security Services Training Materials

OnDefend Cyber Security Services

Overview

OnDefend is a leading provider of preventative cyber security testing and consulting services who works with its corporate clients to reduce their exposed IT surface area while improving their overall security posture. Simply said, we help prevent corporate cyber attacks.

OnDefend provides the following preventative cyber security services:

- Vulnerability Assessments
- Network Penetration Testing
- Web/Mobile Application Security Testing
- Email Phishing Campaigns

Next we will discuss what each of these services provides and why your clients need them.

Vulnerability Assessment - Overview

A vulnerability assessment is the process of identifying and quantifying security vulnerabilities in an environment. It is an in-depth evaluation of your information security posture, indicating weaknesses as well as providing the appropriate mitigation procedures required to either eliminate those weaknesses or reduce them to an acceptable level of risk

Vulnerability assessments consist of:

- Defining and classifying network or system resources
- Assigning relative levels of importance to the resources
- Identifying potential threats to each resource
- Developing a strategy to deal with the most serious potential problems first
- Defining and implementing ways to minimize the consequences if an attack occurs

Vulnerability Assessment – Our Service

Our vulnerability assessment services offer a complete solution for finding vulnerabilities and tracking the remediation within the client enterprise.

<u>Vulnerability Management Process:</u>

1. System and Service Discovery/Scoping
2. Vulnerability Identification & Manual Verification
3. Remediation Building Development
4. Reporting
5. Tracking of Findings
6. Testing to Confirm Remediation
7. Report & Presentation
8. Reassessment

Network Penetration Testing - Overview

A network penetration test simulates the actions of an external and/or internal cyber attacker that aims to breach the information security of the organization. Using many tools and techniques, the penetration tester (ethical hacker) attempts to exploit critical systems and gain access to sensitive data.

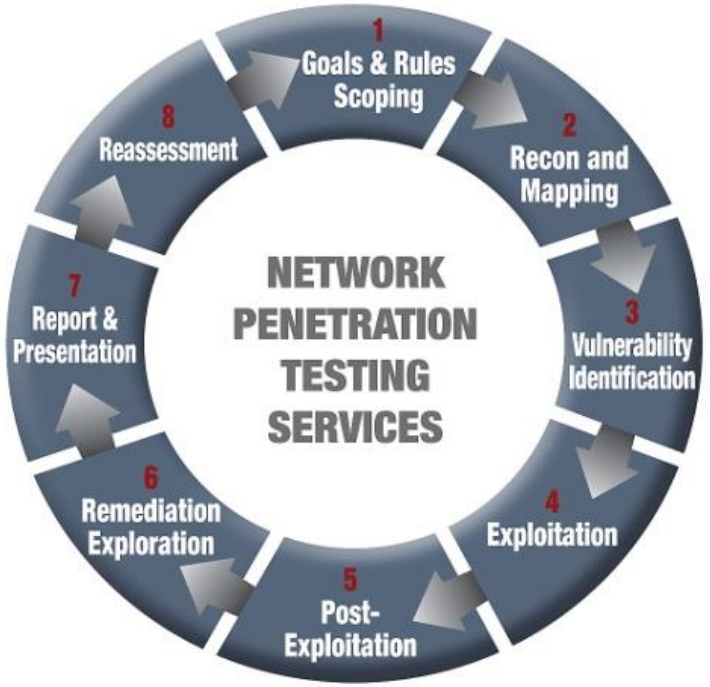
A penetration test doesn’t stop at simply uncovering vulnerabilities: it goes the next step to actively exploit those vulnerabilities in order to prove (or disprove) a real-world attack would be successful and what systems and data that attacker could gain access to.

Network Penetration Testing – Our Service

Our network penetration test services follows the Penetration Testing Execution Standard (PTES) framework which provides the most comprehensive and dependable results and mitigation guidance.

Network Penetration Testing Process:

1. Goals and Rules Scoping
2. Intelligence Gathering – Recon and Mapping
3. Vulnerability Analysis and Identification
4. Exploitation
5. Post Exploitation
6. Remediation Exploration
7. Report and Presentation
8. Reassessment



Vulnerability Assessment vs Network Pentest

Simply said, a vulnerability assessment identifies vulnerabilities in an external (web facing) and internal network as well as instructions on how to fix these vulnerabilities. It would be like getting an opinion from your home security company on where a robber would potentially break in your home and how to secure it.

A penetration test is the next step after you have had a good vulnerability assessment(s). The penetration test finds any remaining external (web facing) and internal network vulnerabilities, but the test also exploits these vulnerabilities to access systems and data, which helps to display your actual risk. Using the home security example, it would then be like getting a “ethical robber” to try to break into your home and if a break in is successful, what the robber could destroy or steal…hence how much you would lose.

Web/Mobile Application Security Testing - Overview

A web or mobile application security test is broken down into Dynamic (app facing and most common) or Static (code based) tests. The primary objective is to identify exploitable vulnerabilities in applications before hackers are able to discover and exploit them. Web application testing will reveal real-world opportunities for hackers to be able to compromise applications in such a way that allows for unauthorized access to sensitive data or even take-over systems for malicious/non-business purposes.

This type of security testing helps clients:

- Identify application security flaws present in the environment
- Understand the level of risk for your organization
- Help address and fix identified application flaws

Web/Mobile Application Security Testing – Our Service A

Our web and mobile application security testing provides services follows the Penetration Testing Execution Standard (PTES) framework which provides the most comprehensive and dependable results and mitigation guidance.

Web/Mobile Application Security Assessment Process:

1. Goals and Rules Scoping
2. Intelligence Gathering – Recon and Mapping
3. Vulnerability Analysis and Identification
4. Exploitation
5. Post Exploitation
6. Remediation Exploration
7. Report and Presentation
8. Reassessment

Web/Mobile Application Security Testing – Our Service B

Dynamic Testing: We identify software vulnerabilities, demonstrates the impact of the weaknesses, and provides recommendations for mitigation. During a web application security test, we have two primary objectives: the obtainment of unauthorized access and/or the retrieval of sensitive information. Our security assessors use a combination of commercial and custom-built tools to test the target application, using manual and automated methods to ensure complete coverage of test cases.

Static Testing: By conducting a Static code testing, we can pinpoint root causes of security vulnerabilities in source code, receive prioritized results sorted by severity of risk, and get guidance on how to fix vulnerabilities in line-of-code detail. As a result you can ensure your software is trustworthy, reduce the costs of finding and fixing application vulnerabilities, and establish the foundation for secure coding best practices.

Deliverable: We identify the root causes for security flaws, perform hardening to secure the environment and provide a detailed report with recommendations for reasonable and practical steps to mitigate future risks. During the hand-off, our security assessors will fully brief your designated representative on all the details of the test, walk them through the results, and provide any necessary work artifacts. Your representative will be fully knowledgeable in the details of the testing, and will have all the information necessary to recreate the findings.

Email Phishing Campaign - Overview

Email phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in an email. Typically a victim receives a message that appears to have been sent by a known contact or organization. An attachment or links in the message may install malware on the user's device or direct them to a malicious website set up to trick them into divulging personal and financial information, such as passwords, account IDs or credit card details.

An email phishing campaign simulates such an attack to help a company see which employees are opening suspicious emails, what they are clicking on and what information they are providing. This service creates employee awareness and promotes a more defensive posture when handling inbound emails.

Email Phishing Campaign

What we do: Our team crafts and implements phishing campaigns that mirror the types of messages used by attackers. We track every aspect from delivery to receipt as well as all activity actions taken by your employee. We provide easy to understand reports to show which employees and departments are practicing safe email handling and which need additional training.

End Result: Our Phishing campaign will boost your employee's ability to handle phishing email attempts thereby protecting your corporate data, client's information and overall businesses stability.