OnDefend

CYBER SECURITY REALIZED

Network Penetration Testing Services Info Guide

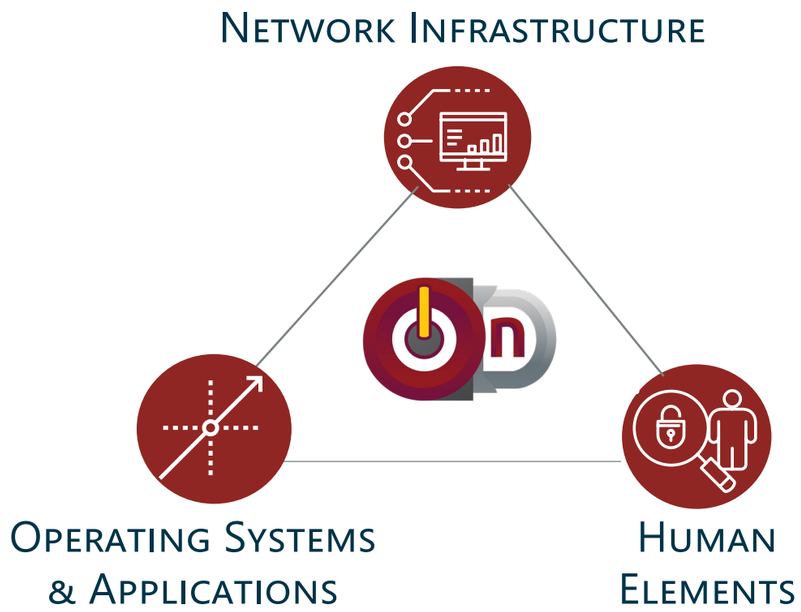
ONDEFEND.COM

WELCOME TO OUR WORLD

We protect our clients from successful cyber-attacks and cyber criminals by providing the testing, consulting, and tools they need to decrease their vulnerable IT surface area thereby improving their overall security posture. OnDefend's mission is to help organizations of all sizes, budgets and other factors that impact their security decisions.

Our Holistic Approach

Each service offering provides different perspectives into the security posture of an organization, with a focus on testing all layers of the technology (and people) stack in an understandable way that focuses on the true risks facing your organization.



A Snapshot In Time

Security tests are a snapshot which provide detailed information on what an attacker can do once they take advantage of that first vulnerability. Enterprises are like living things, always changing as new systems come online, upgrades to applications are made, infrastructure changes are made to accommodate business needs, and patches are released. New vulnerabilities are announced every day, meaning that a system that is fully patched and secure today may not be tomorrow. As such, security testing needs to be a continuous process, not just a single effort completed every once in a while.

OnDefend works with your organization to understand your maturity in the security testing space and builds a testing plan that meets a cadence your organization can support. This ensures you receive a frequency of testing to provide valuable data while providing enough time for remediation activities in between testing engagements.

NETWORK PENETRATION TESTING

Overview

A network penetration test goes beyond just finding known vulnerabilities about the systems themselves – it provides detailed information on what an attacker can do once they take advantage of that first vulnerability. Network penetration tests look to find as many ways into the enterprise as possible, always targeting the most critical assets in the organization. Where a vulnerability analysis goes up until the actual exploitation of a potential vulnerability, a network penetration test exploits that vulnerability, gains access to the system and sees what an attacker could then access.

This type of testing is critical to understanding the resiliency of your security program to defend against this type of attack, your security team's ability to detect and stop the attack in progress and understand where gaps and blind spots exist within the network.

OnDefend
CYBER SECURITY REALIZED

Methodology

OnDefend provides external and internal penetration testing via black-box (see Attack Simulation Testing), white-box and gray-box methodologies. Overall, the testing teams use the Penetration Testing Execution Standard (PTES) framework when conducting these types of assessments. Following this framework, we execute the following phases in our network penetration testing service:

Network Penetration Testing Phases

1. Goals & Rules Scoping
2. Intelligence Gathering
3. Discovery & Enumeration
4. Vulnerability Identification
5. Exploitation
6. Post Exploitation
7. Analysis & Reporting
8. Remediation Testing

NETWORK PENETRATION TESTING

1. Goals & Rules Scoping

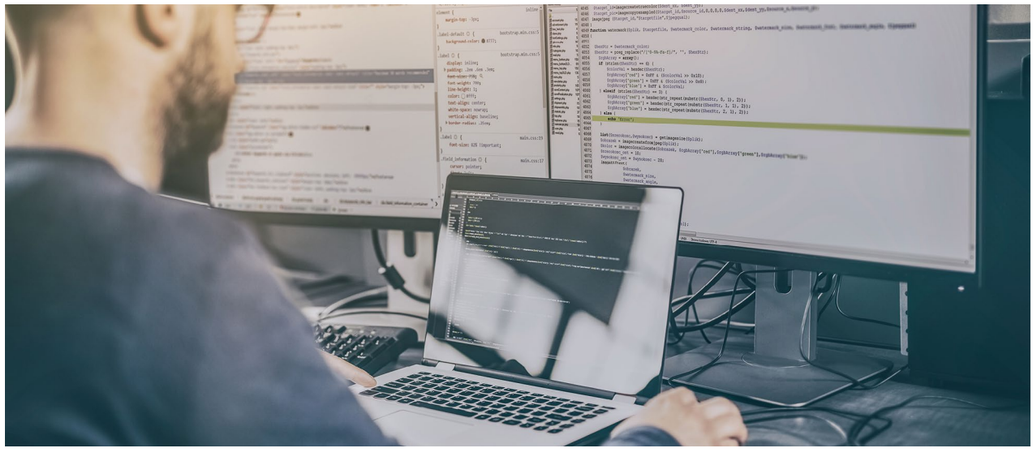
Effective communication with the client organization is emphasized here to create an operating environment comfortable to both parties. During this phase, we accomplish:

- Outline which assets of the organization are open to being tested.
- Determine the specific scenario you want to model, and what the final target of the assessment is.
- Develop a Rules of Engagement agreement to ensure that all parties are aware of the rules.

2. Intelligence Gathering

Profiling involves gathering as much as information as possible about the target network for discovering the possible ways to exploit vulnerabilities into the target organization. This involves determining the target operating systems, web server versions, DNS information, platforms running, existence of vulnerabilities & exploits for launching the attacks. The information can be gathered using various techniques such as Whois lookup, enumerating DNS entries, Google searches, social networking sites, emails, websites, etc.

3. Discovery & Enumeration



Discovery involves using automated and manual tools and techniques to identify live hosts present in the network. This includes determining the target system's operating system, identifying open ports and network services.

Enumerating an internal network allows the penetration tester to identify the network resources, services, machine names, and applications. The identified information then allows the Penetration tester to identify system attack points and perform password attacks to gain unauthorized access to information systems.

OnDefend
CYBER SECURITY REALIZED

NETWORK PENETRATION TESTING

4. Vulnerability Identification

This phase involves identifying vulnerabilities present in network services, information systems and perimeter security controls. This work involves both automated and manual testing methods using some commercial tools, some open source software applications, and custom software created by OnDefend. Manual verification helps eliminate the false positives and identify the possible findings that the automated testing may have missed.

5. Exploitation

This stage uses the information gathered on active ports and services with the related vulnerabilities to safely exploit the services exposed. Attack scenarios for production environment will use a combination of exploit payloads in strict accordance with agreed rules of engagement. It involves research, test exploits and launch payloads against the target environment using penetration test frameworks such as Metasploit and Cobalt Strike.

6. Post Exploitation

Post Exploitation is where the network penetration test separates itself from other types of testing. In this phase, OnDefend consultants will demonstrate the activities possible once the initial compromise is completed, providing you valuable information to understand what those vulnerabilities translate to in terms of the potential for actual loss and damage. It is this phase where the OnDefend team moves through the network towards the objective, identifying additional places to add both preventative and detective security measures.

OnDefend
CYBER SECURITY REALIZED

NETWORK PENETRATION TESTING

7. Analysis & Reporting

All exploitable security vulnerabilities in the target system are recorded and associated risk-based severity scores are reported to the client. The identified security vulnerability is thoroughly explained and reported along with appropriate recommendation or mitigation measures.

Test reports include:

- Details on how each finding was identified and confirmed
- Severity rankings
- Effective remediation recommendations
- Full narrative of the engagement
- Detailed recommendations of additional detection strategies
- Identifying the effective controls that prevented various attacks from working

Client may request results in alternative formats to facilitate importing into GRC tool or ticketing system as necessary. See Sample Test Report to view our test results deliverable.

OnDefend
CYBER SECURITY REALIZED

8. Remediation Testing

As an additional service, our team can retest certain findings after they have been remediated. We will retrace our steps from the engagement to ensure changes were implemented properly. Our engineers will also search for new vulnerabilities associated with the updates, such as misconfigurations in the network or flaws in a new software implementation. At this point, we will update our previous assessment to reflect the new state of the system.

Tools and Techniques

OnDefend testers focus on the fundamentals of the systems and applications that are being tested, rather than focusing on specific software testing tools. This adaptive approach enables OnDefend testers to leverage commercial products, open source tools, and custom developed scripts and applications to conduct testing. OnDefend consultants are constantly learning and teaching new skills and techniques and contribute to open source projects in the information security ecosystem.

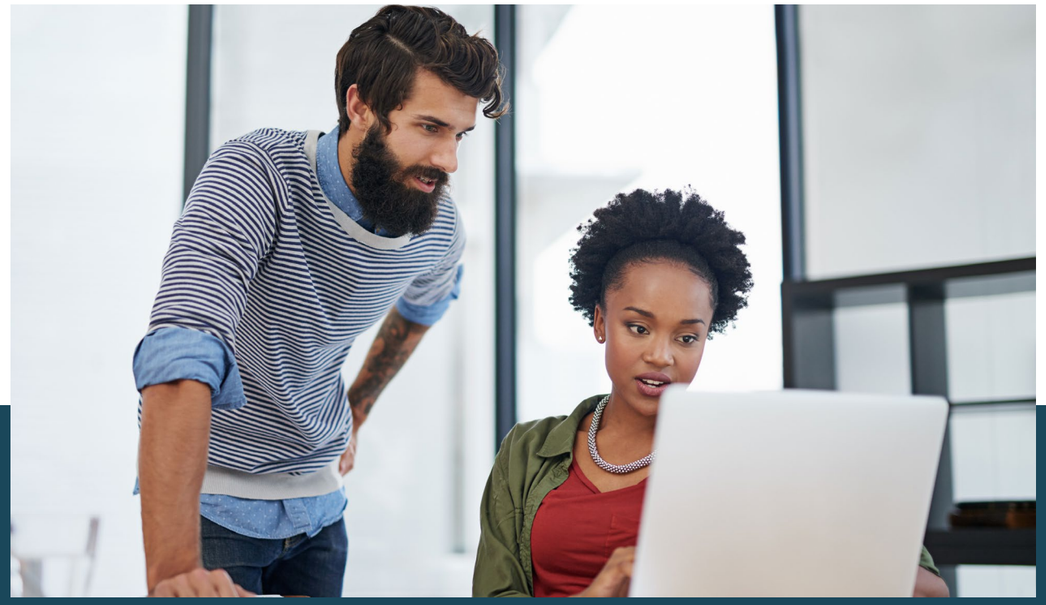
BLUE TEAM WORKSHOPS

Overview

OnDefend also provides optional Blue Team workshops as part of these engagements. In these workshops, OnDefend security testers conduct in-depth technical training, based on feedback from the customer after the report draft is delivered. OnDefend consultants tailor the workshop based on customer feedback.

The Workshop

Sometimes these courses are focused on teaching the methods used during an engagement to enable a customer's team to reproduce the findings in the report. Other sessions are built to teach tactical and strategic actions to reduce the exposure of those specific findings, or help with other security related concerns, such as incident response planning and reviews. This workshop is typically a one-day course, usually 3-4 hours of content, for up to 10 members of the customer's team.



OnDefend
CYBER SECURITY REALIZED

THE ONDEFEND TESTING TEAM

OnDefend's testing services are only as good as the talented testers we utilize to provide these services. We spend significant time and resources ensuring our testers meet our standards and are constantly improving their skills and expanding their knowledge.

Qualification Program

PRACTICE ASSESSMENT

This real-world work sample method lets us see what a tester will be able to provide for our customer, not just what trivia questions he or she could answer in an interview.

PEER REVIEW

A successful outcome in the practice assessment moves the candidate along to the final interview with some of the senior team members.

EXTENSIVE BACKGROUND CHECK

OnDefend testers must pass an extensive background check in order to be hired.

SHADOW AND RECERTIFICATION

Once hired, the tester shadows other senior testers for a few engagements. All testers undergo annual recertification reviewed by our Principal Consultants.

Testing Team Credentials

OnDefend's typical tester candidate requirements:

- At least 7 years of direct security assessment experience
- A bachelor's degree in Computer Science or Software Development or comparable work experience
- Hold certifications like the EC-Council Certified Ethical Hacker (CEH) and Offensive Security Certified Professional (OSCP)
- Active members of their local information security community
- Present at various conferences and events on security related topics
- Participate in vulnerability research contests and bug bounty programs, to further develop their skills and broaden their experiences

OnDefend provides advanced training for all testers, and such training is an integral component of the employee review process. We host internal training sessions where team members share knowledge and techniques, and also sponsor "hackathons" where testers get the opportunity to work exclusively on solving a problem to make them more effective, whether building a new tool, integrating new methods into the process, or extending the platform to improve the effectiveness of our services. These events often generate ideas that we bring into production as part of the formal process, and ensure our processes and tools are driven by the quality of the testing they enable.

OnDefend
CYBER SECURITY REALIZED

OnDefend
CYBER SECURITY REALIZED

Contact Us Today

Industry Leading Professionals are here to answer any questions you may have regarding our cyber security services & solutions.

Visit us at:

OnDefend.com

Or contact us via:

Email: contact@ondefend.com

Call: 800.214.2107