MERIMETSO

External Network Penetration Test

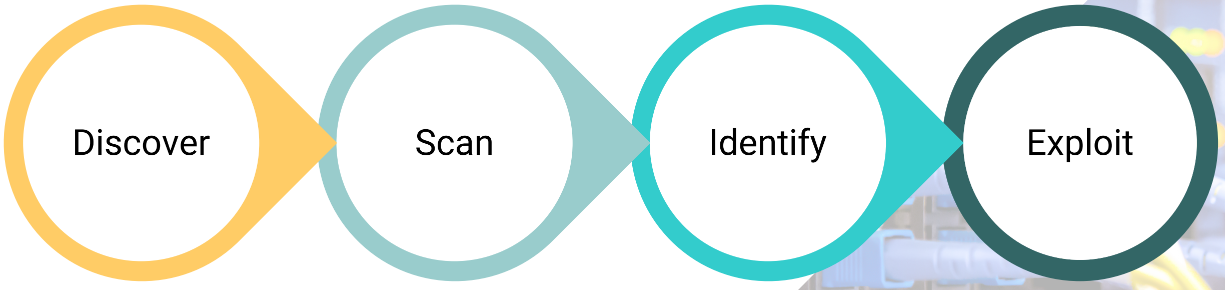
Service Description Introduction

An External Infrastructure penetration test checks the entire, or nominated, exterior assets of a client infrastructure (i.e. anything that connects to the internet), using a variety of discovery and attack methods.

The purpose of the test is to learn more about the External Infrastructure security status, and gain intelligence into mitigating potential threats before harm is done. External Infrastructure assessments help provide assurance that a network is safe from external threats as breaches of external networks can result in significant loss of data as well as brand damage and instability of key business functions.

External Infrastructure security testing should be part of an organisation's risk assessment phase prior to changing or launching any new live services. Merimetso can provide scheduled monthly, or at hoc, External Infrastructure penetration testing services to a client to ensure their entire exterior is secure on an ongoing basis.

Our Approach



Discover

Scan

Identify

Exploit

@merimetsocyber

@merimetso

contact@merimetso.net www.merimetso.net

Engagement Structure

In depth penetration testing of all identifiable services such as email, VPN, file transfer and remote administration testing will be performed over the internet from the Merimetso offices. A base line assessment of web applications in line with the OWASP Top 10 standards will also be carried out where web applications are discovered. In depth web application testing will require a separately scoped test. Testing is not intended to cause any interruption to services. Testing will begin with fingerprinting the IT infrastructure and services followed by manual exploitation with a full review of the results by a senior penetration testing consultant.

Methodology

Discover

Reconnaissance for Public Information and Information Leakage

A thorough public discovery exercise will be undertaken to look for information leakage that could be used to formulate an attack.

- Domain names and IP addresses will be investigated using appropriate databases and other online resources.
- Internet search engines will be crawled to retrieve distributed material relating to the company or employees.
- Web applications will be checked for information that has been intentionally made public, which may cause a security risk.
- Domain Naming Services (DNS) will be queried and attempts will be made to brute-force sub-domains, identify mail and name servers.

Scan

Port Scan and Service Enumeration

The externally facing IT systems will be subjected to vigorous interrogation, with the external threat surface being mapped using a mixture of automated and manual testing techniques:

- The external threat surface of discovered hosts will be evaluated with a full system scan for open ports running services.
- A service enumeration exercise will be conducted to determine software type and version information for the services running on each open port.
- Operating System identification using fingerprinting techniques.
- Firewall rulesets will be analysed for effectiveness and misconfigurations.

Identify

Vulnerability Identification

A fully comprehensive vulnerability scan will be run against each host and a full manual review of exposed services will be carried out. Vulnerabilities discovered in this phase of the assessment will be validated through exploitation or further verification:

- Industry-leading vulnerability scanners and security auditing frameworks will be used to enumerate running services for known vulnerabilities
- Discovered services will be checked for common misconfigurations and software versions will be checked to ensure that all vendor updates have been applied
- The results of the vulnerability scan will be scrutinised by the tester and manually validated

Exploit

Exploitation and Further Vulnerability Identification

Testing consultants will use manual techniques to further probe discovered services.
Vulnerabilities will be further exploited following client approval.
A light touch black box test will be carried out on any web applications identified in the form of an automated OWASP Top 10 application review. Any critical vulnerabilities will be highlighted to the client immediately. Scope for further more in depth application testing can be discussed and scheduled if required.

Deliverables

In-depth report, broken down into 3 main parts:

1. Management Summary
2. Technical Overview
3. Detailed Technical Findings

Highlighting the vulnerabilities:

1. Type of RISK
2. The EFFECT of that RISK
3. Recommendations on how to address and mitigate vulnerabilities
4. Estimate of effort required to remediate any vulnerabilities identified

Project Management

Project Management resource will be assigned throughout the engagement but will not be allocated full time.

Key roles and responsibilities:

- Run engagement kick off workshop.
- Run engagement closure.
- Maintain and communicate engagement risks and issues log.
- Weekly status meetings and engagement tracker.

Prerequisites

The following pre-requisites are required from the client:

- Physical access to the device or exported configuration files
- Make and Model of the Firewalls
- Written permission from the client to test
- Login credentials and digital certificates (if applicable)
- Point of Contact details

Deliverable Acceptance Criteria

Merimetso may present interim deliverables to the customer for review throughout the engagement. Should Merimetso present an interim deliverable, the customer will review, and either accept, or document specific corrective items in writing within three (3) business days. In the absence of any comments, deliverables produced by Merimetso will be deemed accepted after three (3) business days.

Limitations & Exclusions

- This engagement covers only the activities detailed in this document. Additional Merimetso offerings may be purchased as add-ons, otherwise additional consulting work not contained in this engagement is deemed out of scope.
- Working time is defined as Monday to Friday (excluding local bank/statutory holidays), 9am-5pm, with a 60-minute break for lunch.
- Merimetso is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities.
- Only third-party software and infrastructure identified during the pre-sales phase will be in scope for the engagement. There will be no change of scope where third-party software or infrastructure has been changed by the customer during the course of the engagement, or this will incur additional cost.

Customer Responsibilities

1. The customer must provide appropriate resources during the engagement from commencement date.
2. The customer must provide Merimetso representatives with information and resources to ensure Merimetso is able to successfully execute the engagement. This can include, without limitation, providing access and credentials to systems, completing installation prerequisites, providing resources, and attendance in planning, execution, or training meetings.
3. Customer will ensure resources are available in a timely manner to undertake tasks such as change control and documentation review.
4. Customer must ensure it has the necessary escalation and communication channels to resolve any blockers in a timely manner, including dependencies on third parties customer vendors, suppliers, and consultants.
5. If the consultant should travel to a customer location for the delivery of this engagement, there will be additional travel and expense costs. These travel and expense costs can be paid for prior to the engagement, or at actuals, at engagement completion.
6. The customer shall provide at least seventy-two (72) hours' notice for the cancellation or postponement of any work already scheduled as part of the engagement. In such scenario of a cancellation or postponement Merimetso reserves the right at its sole discretion to charge the customer for additional resources at Merimetso's then current daily rate for the delay period.
7. Customer must have a right to use the software and licenses. This requires that the customer must have purchased, or have converted, the appropriate license rights to the target environment.
8. Hardware requirements are the responsibility of the customer, and it is the customer's responsibility to ensure the hardware requirements are met prior to the engagement.

Merimetso may subcontract all or a portion of the services and/or have the services performed by one of its affiliates.

Note: The services described in this Service Description are subject to the terms and conditions by Merimetso Terms

Our Senior Testing Team

Dr Andrew Blyth - Founder and Director of R&D

Dr Blyth received his PhD in Computer Science in 1995 from Newcastle University, UK. Dr Blyth held the position of Professor of Computer Forensics at the University of South Wales, UK, throughout his illustrious career. Co-authored a textbook on Information Assurance, supervised 15 successful PhD candidates, created several BSc and MSc Computer Forensics and Cybersecurity Programmes. He was instrumental in the University of South Wales being the first University in the UK to behave an MSc in Computer Forensics accredited by the UK Government's National Technical Authority (GCHQ/NCSC).

He was the Cybersecurity Technical Lead at the UK Ministry of Defence's (MOD), Defence Science and Technology Laboratory (DSTL). During that time, he created and ran the Computer Network Defence Technical Demonstrator programme and defined various other research programmes within DSTL. He has over 50 peer-review publications and managed millions of dollars of research funding.

Campbell Murray - Founder and COO

Campbell is an established global leader in the field of information security. With over 25 years of experience ranging from offensive security assessments and security engineering in a vast range of environments providing Campbell with rare detail and insight into the field of cybersecurity. Campbell established himself as a penetration testing consultant in 2000. A firm believer in knowledge transfer, Campbell was a founding director of the TigerScheme in 2007 and the Cyber Scheme in 2013.

The Cyber Scheme is the recognised course used by NCSC to affirm CHECK status on any penetration tester who wishes to work on Government infrastructure in the UK. Campbell is now the chair of the technical panel for the Cyber Scheme and is one of only a handful of GCHQ appointed CHECK Team Leader assessors.

David Mound - Founder and CTO

David is a highly experienced Cyber Security Researcher with a demonstrated history of working in the Computer & Network Security industry and threat intelligence. Skilled in Penetration Testing, Reverse Engineering, Computer Forensics, Red Teaming and Threat Intelligence, he has worked with numerous global agencies within the 5 Eyes community, including GCHQ and the NSA delivering, advising on Red Team methods and engagements to assess Blue Team capabilities.

David's current speciality and focus are cloud-based technologies, and he holds multiple cloud certifications such as AWS Certified Security Specialist. David is an ex-Naval officer and is currently a member of the Army Reserves, where he coordinates threat hunting and assists network defence within the UK MOD and Gov estates. David brings his extensive technical capability to design the innovation to the Merimetso Cyber Technical Training platform.