CyberOne

Penetration Testing

G-Cloud 15

Service Description

Service Description
Penetration Test

This Schedule forms part of Schedule 3 to the Agreement between Customer and Provider and sets out a description of the Services in relation to penetration tests as given on a Service Order.

Penetration test results are stored in the Supplier's penetration test platform "Jerico". This is hosted in Azure in the UK and authentication is forced to include MFA.

Jerico is the Supplier's bespoke report dissemination system. It allows us to deliver reports to clients (including in client-defined formats where required) through this platform, in a straightforward and secure manner. It is a 'digital' report with features to track the process of taking each test "finding" through the stages of a remediation process, download the report in a PDF format.

1. What Is Included in Penetration Test Service?

Below is a list of services which will be included in each engagement:

- **Full Scoping Process** – We want to ensure you are paying for exactly what you require, and all questions have been asked prior to starting. i.e., A pen tester or project manager will confirm the scope in detail by means of a direct conversation with you once you have agreed in principle to proceed.

- **Pre-Testing Establishment** – We want to ensure the environments being accessed can be reached prior to the assessment starting to avoid any time delays on the day(s).

- **Full Assessment** – We will conduct a comprehensive assessment of the systems / applications within the statement of works and utilise all testing hours, where applicable.

- **Reporting** – We will write a detailed report with all findings, risk ratings and remediation advice, plus confirmation of testers CREST credentials. This will be delivered in the form of a secured PDF document.

- **Remediation Advice** – We will be available to help you understand issues that were uncovered and help remediate them where possible. We can perform remediation work if required, subject to a separate Scope of Work.

2. Preparations

The following requirements are recommended to allow CyberOne to conduct a full penetration test of in-scope systems without disruption:

- Any relevant office and/or data centre full address and any access requirements.
- List of IP Address ranges in scope for testing the external infrastructure.
- Send firewall configuration files to CyberOne for review.
- Confirm systems are owned by client or the client has the necessary permissions from provider.
- ·(Optional) Whitelisting CyberOne IP Address(es) in your firewall.

3. Pre-Engagement

The penetration tester will prepare for the security assessment with the required tools, operating system, and environment. A “Rules of Engagement” document will be provided by CyberOne as a single point of reference. This will document the agreed scope and any further requirements prior the engagement are verified. For example: credentials for different user access levels.

4. Infrastructure Testing Methodology

Outline

A penetration test is a method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security using the same tools and techniques as an adversary might.

CyberOne conduct CREST-accredited, relevant, comprehensive, and thorough cyber security assessments and provide visibility of ongoings to relevant stakeholders. The below shows the typical approach to a full-gamut penetration test; however, you may decide through the Supplier’s scoping process that you only want to conduct one or many but not all types of testing.

Pre-Engagement

The scope is acquired and authorised by the client, any requirements prior the engagement are verified. For example, credentials for different user access levels are verified, access to the in-scope environment, etc. We work with the client to create a Rules of Engagement that defines all the relevant details related to the engagement that everyone can refer to at any time. The penetration tester will prepare for the security assessment with the required tools, operating system, and environment.

4. External Infrastructure

This involves testing any publicly accessible infrastructure (i.e. anything internet-accessible). Here we follow the below methodology on each in-scope host to try to identify and exploit vulnerabilities with the aim of compromising them to take control. If a host is compromised, we can either continue with the assessment to assess what damage could have been done by an attacker or remove that host from the future scope and provide immediate remediation details.

Wireless Infrastructure

Nowadays, this is nearly always infrastructure providing wireless access to networks over Wi-Fi. We are enumerating the security controls in place and attempting to bypass them, looking at:

- What type of security is being used?
- What can you access once connected to the wireless network?
  - Anything sensitive?
- Is there a dedicated locked-down subnet?
- Are guest networks actually isolated?
- Can we touch internal servers?

Internal Infrastructure (w/Active Directory)

It's generally recommended to start the internal infrastructure engagement as a blind / black-box / uncredentialed test with the option to transition to a grey-box / credentialed / assumed breach scenario if we haven't compromised AD after a certain amount of elapsed time. This tests the widest variety of different attack vectors and helps ensure that the customer will get the most value out of their assessment even in a scenario where the network is locked down to unauthenticated network users.

If we have not compromised the network from the external point-of-view, and the test is being conducted remotely, then we will work with your team to install a pentest 'dropbox' on-site that will allow us to act as if we were sat in the room plugged into the network. We will then begin blind testing the in-scope hosts for vulnerabilities that may allow us to compromise them or the network further (printers, servers, etc.). We will also be attempting to compromise AD or Local accounts on user workstations.

Once an account has been compromised, we move onto privilege escalation and actioning on the Supplier's objectives. This objective may be attempting to achieve domain administrator access or targeting a specific resource such as a database with sensitive data.

Post-Engagement

Clean Up - The security consultant removes all persistent malicious payloads and attacks that were found during the security assessment. This is to avoid an active malicious attackers attempting to take advantage of problems that have been identified throughout the engagement.

Delivery - Reporting is prepared with an executive summary and graph outlining vulnerabilities discovered during the engagement aimed towards senior management, with further detailed information expanding on the issues found, how to replicate the issues discovered, an approach to remediating the vulnerabilities and to prevent these vulnerabilities occurring again in the future.

It is important that both senior management and technical employees clearly understand the business impact caused through the vulnerabilities identified. This enables you to prioritise the mitigation steps to reduce the greatest risks to your organisation first.

We assure the report is of a high-quality standard by going through the CyberOne quality assurance process to verify the issues found. The report is issued to the client securely via Jerico, the Supplier's bespoke in-house report dissemination platform. Jerico allows the reports to be downloaded as PDFs and to be accessed in a live, online manner to ease management of remediation effort.

5. Higher-Level Methodology

CyberOne's Cyber Security Consultants follow a standardised set of procedures as described under the Penetration Testing Execution Standard (PTES). Due to the varied nature of environments and applications, CyberOne will tailor the general testing methodology per target. We use both an automated and manual approach with industry leading tools for performing security assessments.

Infrastructure testing entails performing a penetration test to identify vulnerabilities that could be exploited by an attacker. Testing is conducted from inside and outside the organisation. The methodology to conduct this type of testing is described below.

Intelligence Gathering

This section defines the information collection activities during a penetration test. We detect the number of active devices through actively enumerating the disclosed IP range, discovering servers, switches, routers, and end-user devices on the network

Threat Modelling
The threat modelling stage of the penetration testing exercise is critical for both the tester and the organisation. The Supplier's Cyber Security Advisor performs a SWOT analysis to discover the strengths and weaknesses from the point of view of an attacker in relation to the organisation, focusing on business targets.

An example of this is a tester comes across an application accessible using default credentials or vulnerable to a publicly available exploit, which provides access to its backend database. The database holds customer information and the organisation's employee information. Here, the customer information would be considered the primary target, and the employee details a secondary target.

Vulnerability Analysis
A process discovering flaws in applications and systems ranging from host misconfigurations to insecure application designs leveraged by an attacker. CyberOne's approach involves passive testing to monitor traffic and metadata analysis, followed by active testing to directly interact with network components, systems and services.

Exploitation
The aim is to bypass system limitations and access system resources by identifying main entry points and high-value assets of the organisation. Evasion techniques are deployed to prevent detection and presents a simulated attack against the organisation.

Attacks are customised to suit the systems and services on the network, publicly available exploits are tailored for targeting infrastructure. We do not test for Denial of Service (DOS) and Distributed Denial of Service (DDOS) unless requested by the client, as this may result in loss of data or system crashes.

The objective is to gain unauthorised access to critical infrastructure without detection, for potential damage to the organisation's reputation and functionality.

Post-Exploitation
Access to compromised devices is maintained to allow pivoting towards more valuable devices on the network. We follow the rules of engagement, making sure client systems are not susceptible to unwarranted risk.

For example, a persistent backdoor is implemented taking security into consideration, authentication is required to access the system and is removed during the clean-up process.

Towards the end of the security engagement, the Cyber Security consultant initiates the clean-up process followed by the report.

Clean Up
The Cyber Security Advisor removes all persistent malicious payloads and attacks that were found during the security assessment. This is to avoid an active malicious attacker attempting to take advantage of problems that have been identified throughout the engagement.

Delivery
Reporting is prepared with an executive summary and graph outlining vulnerabilities discovered during the engagement aimed towards senior management, with further detailed information expanding on the issues found, how to replicate the issues discovered, an approach to remediating the vulnerabilities and to prevent these vulnerabilities from occurring again in the future.

It is important that both senior management and technical employees clearly understand the business impact caused through the vulnerabilities identified. This enables you to prioritise the mitigation steps to reduce the greatest risks to your organisation first.

We assure the report is of a high-quality standard by going through the CyberOne quality assurance process to verify the issues found.

The report is delivered via CyberOne's secure penetration testing and vulnerability management platform, Jerico.

7. Additional Terms and Conditions

The following terms and conditions relate to the Penetration Test Services:
7.1 The Customer consents, for itself and on behalf of the End User, to the Supplier performing the Penetration Testing Service and that it has procured, where necessary, the consent of all its (and its group companies) employees, agents and sub-contractors and those of the End User that the Supplier shall be permitted to carry out the Penetration Testing Service. The Company will be carrying out the Penetration Testing Service in the belief that it has all appropriate consents, permits and permissions from the Customer and its group companies (and their employees, agent and sub-contractors) and those of the End User.

7.2 To procure that the End User makes appropriate backups of the end User Technology and End User Data prior to the commencement of the Penetration Testing Service.

7.3 The Customer will indemnify the Supplier for any direct losses incurred as a result of a claim from a third party arising out of any failure of the Customer to comply with clauses 7.1 and 7.2.

7.4 That, whilst the Supplier will conduct the Penetration Testing Service in line with accepted best practice and make all reasonable commercial efforts to avoid disruption of the End User's Technology network, the tools and techniques used may cause disruption to the End User's Technology and/or possible loss of or corruption to End User Data and the Customer agrees to requests the End User takes such backups and provide such redundant systems as are prudent in the circumstances. The Supplier will notify the Customer in the event where activity would lead to loss of service where this is known to the Supplier.

7.5The End User shall notify the Supplier immediately if there are any periods during the Service when the Supplier should stop work due to critical business processes (such as batch runs) or if any part of the End User Technology is business critical so that the Supplier can, if needs be and with the End User's consent, modify its testing.

Penetration Testing

Uncover Hidden Vulnerabilities—Before Attackers Do.

Strengthen Your Security with Real-World Testing

CyberOne's Penetration Testing service simulates sophisticated attack scenarios to uncover vulnerabilities across your IT environment. Our CREST-certified experts leverage cutting-edge tools and ethical hacking methodologies to help you proactively identify and remediate weaknesses before they can be exploited.

Proactive Vulnerability Discovery

CyberOne's Penetration Testing services provide comprehensive security assessments, helping you identify vulnerabilities and strengthen your cyber security posture with tailored actionable insights.

Our experienced team of CREST-certified testers verifies the abilities of your systems across networks, applications, endpoints and insider threats. We work with you to select the most suitable approach to enable you to identify, evaluate and remediate your vulnerabilities safely, efficiently and quickly.

Our Approach

At CyberOne, our comprehensive methodology is designed to rigorously evaluate your security posture. We define clear testing scopes, conduct thorough reconnaissance, perform detailed vulnerability analysis and exploitation and follow through with secure clean-up and debriefing. This approach ensures minimal disruption while providing you with actionable insights to bolster your defences.

1. Scoping

We work with you closely to define the scope of the test.

2. Reconnaissance

Using publicly available information we build intelligence used to try to compromise your business.

3. Mapping

The network infrastructure is fully assessed to gain a complete picture of your attack surface.

4.Vulnerability Analysis

An in-depth audit of applications residing on target hosts to identify security vulnerabilities to exploit.

5. Service Exploitation

We attack vulnerabilities to gain access to your systems and data.

6. Pivoting

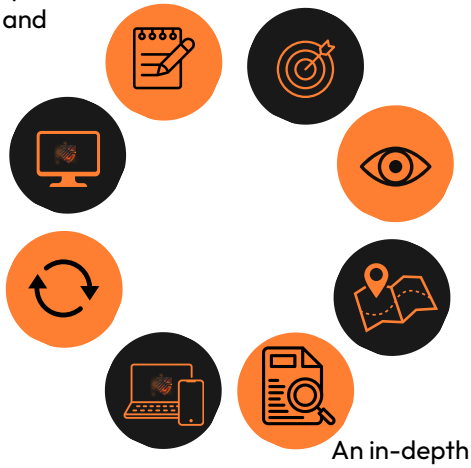
We attack further assets by leveraging compromised systems.

7. Clean-Up

We safely remove the data used in our testing from your systems.

8. Reporting & Debriefing

Written, virtual or face-to-face the in-depth report provides clear recommendations and guidance for remediation.



Types of Penetration Tests We Offer

Our expert ethical hackers use advanced tools and techniques to assess networks, applications, endpoints and wireless systems. We conduct:

External Network Testing

Evaluate the effectiveness of your perimeter security controls to prevent and detect attacks. This test identifies vulnerabilities in internet-facing assets such as web, email and FTP servers.

Internal Network Testing

Assess the potential impact of lateral movement within your network. This simulation mirrors insider threats, whether intentional or accidental, to reveal the extent of internal vulnerabilities.

Web Application Testing

Detect data leakage points within your web applications. We examine your source code for adherence to best practices and check for bugs, particularly during the design phase.

Mobile Application Testing

Identify platform-specific vulnerabilities in Apple and Android environments. Our assessments expose insecure mobile app functionalities and suboptimal security strategies.

Wireless Testing

Uncover weaknesses in your wireless architectures to prevent unauthorised network access and data leakage.

Social Engineering Testing

Test your employees' security awareness by simulating phishing emails, credential theft and unauthorised computer access, ensuring robust human-centric security controls.

Key Features of CyberOne's Penetration Testing

Learn about the advanced tools, innovative methodologies and tailored testing strategies that form the backbone of our Penetration Testing service. Discover how we simulate real-world attacks to expose vulnerabilities across your business while delivering clear, actionable insights that empower you to enhance your security posture safely and effectively.

Cutting-Edge Tools & Techniques

Utilise the most advanced methodologies to simulate real-world attack scenarios and detect emerging vulnerabilities.

Ethical & Professional Standards

Leverage CREST-certified professionals with years of experience working under strict ethical, legal and technically diverse environments.

Safe & Controlled Engagements

Engage in clearly defined, controlled testing environments that ensure business continuity while exposing vulnerabilities.

Actionable Insights & Reporting

Comprehensive summary reports and audit-ready insights that convert technical findings into clear, prioritised recommendations for remediation.

Tailored Testing Strategies

Customised assessments address your unique infrastructure challenges, ensuring targeted and effective security improvements.

Compliance Support

Supports regulatory requirements with PCI DSS, ISO 27001, GDPR and other frameworks to reduce compliance risk.

About CyberOne

CyberOne is a Microsoft Security Solution Partner and member of the Microsoft Intelligent Security Association (MISA). We deliver one of the UK's most advanced AI-augmented Managed eXtended Detection & Response (MXDR) services, recognised with Microsoft-verified Managed XDR solution status, enabling organisations to move with confidence from risk to resilience. Powered by Microsoft's market-leading security technologies and realised by CyberOne's accredited experts, we help businesses anticipate and contain modern threats so they can thrive.

With 24x7x365 Global SOC coverage, NCSC accredited Cyber Incident Response, CREST SOC and Penetration Testing accreditations and guaranteed SLAs, CyberOne combines Microsoft Security with expert consulting, professional and managed services to protect operations, achieve compliance and build lasting resilience.

Accreditations & Certifications

CyberOne's services are backed by the world's leading standards bodies including NCSC, CREST and ISO as well as our key technology partners, whilst our experts are backed by industry-leading certifications, cementing our role as leaders in cyber security.

CyberOne

hello@cyberone.security

+44 (0) 3452 757575

cyberone.security