BigData

BigData Penetration Testing Services

Realise your resilience

Find your weak points before someone else does

Motivated cybercriminals will do whatever they can to break into your systems; penetration testing replicates this behaviour through controlled ethical hacking that tests the strength of your security controls.

BigDetech Penetration Testing Services are consultant-led security assessments which seek out security vulnerabilities in your systems, networks, or applications that an attacker could exploit. We have a comprehensive range of testing services to meet any situation from wireless to network, web application to active directory, and many more.

BigData Penetration Testing services

BigData work with you to ensure you receive the most appropriate assessment for your situation. You can explore our services in greater depth with one of our experts who will recommend which ones would be suitable for your organisation's circumstances, business objectives and obligations. Our penetration testing services are ISO 27001 certified.

Contents

Network Penetration Test

What is it?

A network-based penetration test is an objective-based security assessment of your internet facing services, or internal network's security posture.

A typical example of an objective could be:

- Identify and exploit vulnerability in an internet facing service, use it to gain access into an internal network, such as an office or a datacentre, and access Personally Identifiable Information (PII) of customers or staff members
- From a network connection in an office, identify and exploit any vulnerabilities in an internal network that could be used to compromise an internal system of importance, such as a finance or HR system

Does this involve exploitation of vulnerabilities?

Yes. Any vulnerabilities found during the engagement may be used by the penetration tester towards achieving their objective.

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of vulnerability is caused by a business process

Web Application Testing

What is it?

The Web Application Testing is a comprehensive assessment of your web applications following the Open Web Application Security Project (OWASP) Top 10 testing methodology. The assessment can be carried out from following perspectives:

Black Box Assessment – Taking on the position of an anonymous malicious threat actor, the penetration tester is provided only the URL of the application. If there is a signup or registration element to the application this can also be included in the scope of work.

Grey Box Assessment – Representing a threat to the application from an authorised user, the penetration tester is provided with access to the application, but no information on its architecture, user base or the technologies used.

White Box Assessment – the penetration tester is provided with access to the application, full details of its architecture, user rights assignment and the technologies used to build it.

Does this involve exploitation of vulnerabilities?

Vulnerabilities will be exploited through to their logical conclusion to demonstrate the risk posed by the identified issue.

What configuration is reviewed?

The Web Application Testing methodology focuses on the following areas of application security:

- Input validation
- Session management
- Encryption mechanisms and security for data in transit and at rest
- Information leakage
- Access control
- Functional flaws
- Third party libraries and components
- Administration access

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

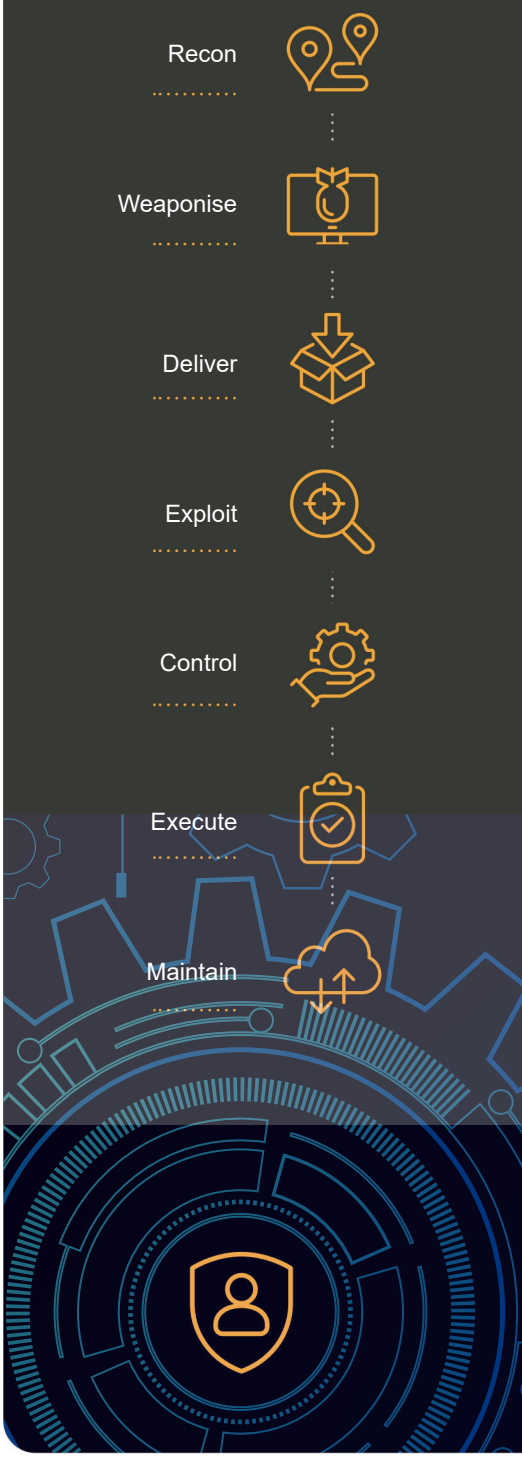
Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of vulnerability is caused by a business process

Red Team Operations

Overview

The Red Team Operations service is designed to simulate the actions of real cyber attackers who might target your organisation. Red Team Operations uses all types of penetration testing methodology and is modelled around the MITRE ATT&CK for Enterprise framework:



Skills and Experience

Our Red Team use all the skills from their penetration testing experience and have undergone extensive industry-recognised training to ensure the Tactics, Techniques and Procedures (TTPs) simulate a real-life attack against your organisation.

The members of the red team are chosen carefully, ensuring that they have skills in the each of these disciplines:

- Reconnaissance using open-source intelligence gathering techniques (OSINT) and threat intelligence
- Weaponisation using the current techniques and tactics
- Delivery of payloads using the stealthiest techniques
- Exploitation of both publicly known security vulnerabilities and configuration weaknesses
- C2 using the latest techniques of threat actors including redirection and fronting of C2 traffic
- Execution of code on target systems using ingenious bypasses of Endpoint Detection and Response (EDR) products
- Real world communication smuggling replicating the techniques used by the most skilled threat actors

Safety and Risk Management

The attack infrastructure used by our Red Team is heavily fortified to ensure any access into your organisation is protected. As defined by the Practice Director, the actions used by the Red Team are non-destructive and the team's methodology minimises the risk of introducing real-world threats into your organisation. This is achieved by the following:

- C2 traffic is encrypted twice in transit. The data is encrypted with symmetric key encryption and transmitted through a secure channel, such as HTTPS
- Access to C2 server(s) is secured with two factor authentication (2FA), to ensurethat only authorised members of the Red Team can access attack infrastructure
- Attack infrastructure employs access control lists using firewalls at each hop to ensure that only intended infrastructure can communicate with the Red Team's C2 infrastructure

Reporting and Debrief

The Red Team Operations methodology ensures that any action undertaken by the Red Team is logged in a timeline of events allowing Incident Responders, Blue Teams or Security Operations teams to correlate actions against event logs. All TTPs used by the Red Team are directly mapped to Mitre's ATT&CK Matrix, a centralised and industry-recognised list of techniques used by real-world threat actors. BigDetech's Red Team will happily host debriefing sessions with your organisation's executives anddefenders, so that any actions executed during the engagement window can be fully explained.

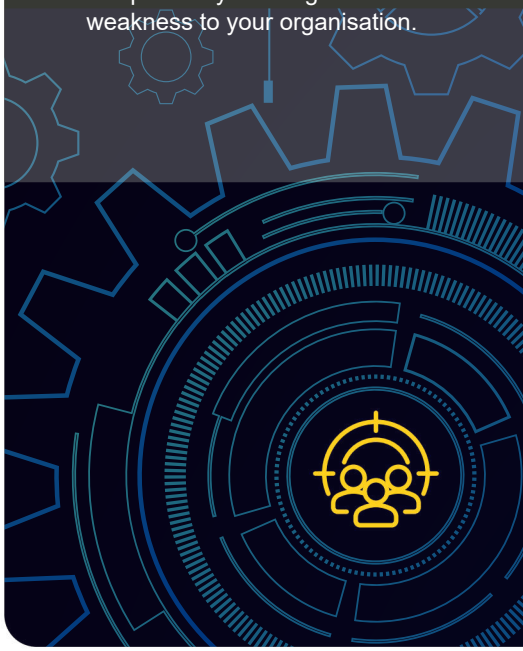
Client Security Evaluation

What is it?

A Client Security Evaluation will review your organisations End User Device (EUD) such as an employee's workstation, desktop, or laptop, against security best practices and industry standards. The review is carried out from an authenticated perspective. It uses the permission level of a typical end user and looks for any configuration weaknesses or security vulnerabilities that could be exploited by a threat actor or malicious user to escalate their privilege level and use the access to the workstation to compromise other devices in your network or domain.

Does this involve exploitation of vulnerabilities?

Vulnerabilities will be exploited through to their logical conclusion to demonstrate the risk posed by a configuration weakness to your organisation.



What configuration is reviewed?

The Client Security Evaluation will review the entire EUD's configuration and identify any weaknesses that could be exploited by a malicious user or threat actor who has gained access to the client. The vulnerabilities in the following areas will be identified, but not limited to:

- Physical Security
- Software installation and configuration
- Patches and patch management policies
- Service configuration and permissions
- Password policy and password management
- System logs and auditing
- Privileged system configuration access control
- Any configuration weakness that could be exploited to access another client or server in the network or domain

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - Thevulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of vulnerability is caused by a business process

Server Build Review

What is it?

A Server Build Review is a comprehensive review of a server's build and configuration. The review is carried out from an authenticated perspective and will highlight any configuration weaknesses that could be exploited by a malicious user to escalate their privilege level and access the server to compromise other devices in your network or domain.

Does this involve exploitation of vulnerabilities?

No. No exploitation is typically within scope of this assessment, this is an authenticated whitebox configuration review performed using administrative credentials.

What configuration is reviewed?

The Server Build Review will look at the entire server's configuration and identify weaknesses in its build that could affect the integrity of the server. The review will follow a defence in depth approach and identify any host weaknesses or software components that could be exploited to escalate privilege level and use the initial compromise to targets other domains or networks.

Vulnerabilities will be identified in, but not limited to, the following areas:

- Software installation and configuration
- Patches and patch management policies
- Service configuration and permissions
- Password policy and password management
- System logs and auditing
- Privileged system configuration access control

Any configuration weakness that could be exploited to access another client or server in the network or domain

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of vulnerability is caused by a business process

What standards are met in this review?

The Server Build Review methodology is built from industry recognised standards including:

- Centre for Internet Security (CIS) Benchmarks
- Payment Card Industry Data Security Standard (PCI DSS)
- DISA Security Technical Information Guides (STIG)
- National Institute of Standards and Technology (NIST) recommendations.

The methodology also benefits from our team's cyber security experience in Penetration Testing and research into the Techniques, Tools and Tactics (TTP) used by real-world attackers. This ensures that any configuration weaknesses that could aid an attacker are identified, appropriately risk rated, and configuration changes to remediate the risk are given.

Firewall Security Testing

What is it?

A full review of your firewall's configuration and security posture can be performed as an offline audit of an extracted configuration or from an authenticated management console session. We will test your firewall using various techniques to test the access controls in place. We recommend this task is performed alongside an inspection of the firewall's access control lists.

Does this involve exploitation of vulnerabilities?

No. Firewall and network device assessments are configuration-based reviews performed with credentials or configuration files.

What configuration is reviewed?

Rule base Review

To complement the firewall network exposure testing the firewall rule bases are subjected to analysis against the firewall policy and best security practice with the aim of identifying:

- Insecure firewall rules including 'ANY ANY' rules and those deemed overly permissive
- A complete listing of permissible protocols including those restricted to specific source addresses unidentifiable from a network
- Plaintext protocols permitted though the firewall and those used for management of the firewall itself
- Undocumented rules
- Absence of stealth and logging rules
- Other rule base misconfiguration
- Possibility of firewall performance optimisation

Segregation, Segmentation, and Exposure Testing

To determine which Layer 4 protocols are allowed through your firewalls, we subject them to exposure testing where attached networks are scanned using a variety of tools, with the aim of identifying:

- Firewall type and footprint, including running services and responses to identification type scans, such as ICMP (all types) scans
- Permissible inbound protocols
- Permissible outbound protocols
- Network map of hosts accessible through the firewallFirewall response to SYN, ACK, FIN and NULL packet scanning
- Firewall response to common packet level attacks, including malformed packets, fragmentation attacks (small and overlapping packets) and SYN flooding attacks (only conducted on request)
- Firewall misconfiguration with regards to source port manipulation scans

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of a vulnerability is caused by a business process

Mobile Application Assessment

What is it?

Mobile testing will examine and identify security vulnerabilities in mobile applications built for smart phones or tablets. The assessment encompasses the complete mobile application and any server-side APIs the application uses. It is also recommended that the application's source code is provided as this improves both the quality of findings and any recommendations.

Does this involve exploitation of vulnerabilities?

Yes. Identified vulnerabilities will be exploited to demonstrate the risk posed where possible.

Approach

The first attack phase consists of manual testing using a range of tools and techniques. The tools used include network monitoring, man-in-the-middle proxies, and reverse engineering tools. The precise tests that are performed will vary depending on the nature of the application. Typically, these will include:

- Analysis of data stored on the mobile device
- Analysis of transport layer security
- Analysis of the use of cryptography within the application
- Analysis of any binary protections that may be in place
- Validation of authentication and session management
- Source code review
- OWASP Top Ten Mobile Risks

The second attack phase consists of manual and automated testing of the server-side end point of a client-server mobile application. The tools used include network scanners, automated testing tools, and man-in-the-middle proxies.

The testing will look for flaws of various types including:

- Input manipulation flaws such as SQL injection, Xpath injection and path manipulation
- Flaws in authentication and authorisation
- Business logic flaws
- Session management errors

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of a vulnerability is caused by a business process

Mobile Device Assessment

What is it?

Mobile device testing will examine and identify security vulnerabilities in your organisation's smartphones and tablets' configuration, whether Android or iPhone devices. This can be carried out either independently or as part of a standard network infrastructure penetration test. This service provides a thorough overview of the current security state of your devices and provides the necessary remedial actions.

Does this involve exploitation of vulnerabilities?

Vulnerabilities will be exploited through to their logical conclusion to demonstrate the risk posed by a configuration weakness to your organisation.

Mobile Device Testing

A mobile device test is a comprehensive review of the following:

- Data at rest encryption, including backups
- Phone call encryption
- PIN and authentication strength
- Server and handset policy
- Data leakage via removable media, SD, and SIM cards
- Data leakage via screen shots and log files
- Data leakage via use of email, SMS services, apps, and Internet usage
- Potential to bypass device's security controls
- Sandbox effectiveness
- Bluetooth security, for example phone book transfers for audio pairing
- Malware threats from outdated software (OS or app layer)
- Use of antivirus software
- BYOD (Bring Your Own Device) scenarios
- Remote and local device locking and wiping
- CIS and NCSC guidelines, where applicable

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of a vulnerability is caused by a business process

Source Code Review

What is it?

The Source Code Review methodology is designed to identify areas of an application that could be exploited by a user of the application to cause detriment to the confidentiality, availability and integrity of the application and the data it processes.

To ensure efficiency and value in this service, we will work with application developers to identify areas of the code base that:

- Accept user input
- Process user input
- Access databases or data stores
- Interact with third party services

These areas are considered untrusted and are the focus of the source code review. The Trustmarque team currently review C# or Java languages.

Areas of review:

Best Practices Adherence

The source code is assessed for adherence to best practices with regards to:

- Bounds checking
- Memory allocation
- Insecure library functions
- Documentation
- Code maintainability and performance

Input Validation Assessment

- Cross Site Scripting
- Buffer Overflow
- SQL Injection
- Command Injection

Error Handling Assessment

- Any errors produced by the application are handled securely and do not leave the application in an insecure state
- Error handling does not provide any feedback to an attacker which may assist in further attacks such as error messages detailing inner workings of the application

Session Management Assessment

- Session identifier construction including predictability
- Session identifier creation with regards to session fixation attacks
- Secure session termination
- Secure session transportation including encryption
- Session lifecycle including session timeout analysis

Authentication Assessment

- Authentication methods in use
- Password complexity restrictions
- Account lockout configuration
- Password storage methods

Cryptographic Assessment

The source code will be reviewed to assess the application's use of encryption particularly for the inclusion of:

- Inappropriate encryption libraries
- Proprietary cryptographic algorithm usage
- Cryptographically insecure encryption algorithms, for example DES
- Weak encryption key lengths

Logging Assessment

- Successful and unsuccessful authentication
- Authorisation requests
- Data manipulation
- Session activity (logout events)

Denial of Service Assessment

- Improper resource handling

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - Risk ratings for each vulnerability
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of a vulnerability is caused by a business process

Wireless Assessment

What is it?

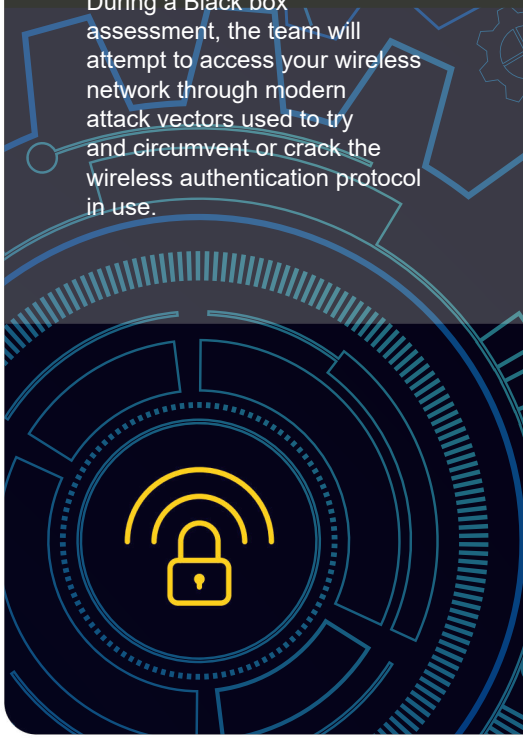
The Wireless Assessment can be carried out as a Black Box or White Box assessment to determine if someone can gain access to your organisation's network and beyond.

Black Box - where no information is provided about the wireless network and is attacked simulating the actions of a malicious threat actor.

White Box - where access to the wireless network is provided and the network's configuration is reviewed against security best practices.

Does this involve exploitation of vulnerabilities?

During a Black box assessment, the team will attempt to access your wireless network through modern attack vectors used to try and circumvent or crack the wireless authentication protocol in use.



What configuration is reviewed?

The Wireless Assessment methodology reviews the following elements of wireless networks:

- Detection of wireless network in a physical location, including sweeping for rogue access points or devices
- Authentication protocols and mechanisms
- Traffic analysis
- Encryption strengths
- Segmentation of wireless networks, if in place

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating.
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of a vulnerability is caused by a business process

Social Engineering

What is it?

The Social Engineering service is designed to test the security awareness of your organisation's personnel and processes. This service can be a physical site visit, telephone calls or targeted emails. We will work with you to define an approach that will help you meet your business objectives and understand about cyber security awareness in your organisation.

What is the approach?

As with other forms of testing, Social Engineering starts with information gathering and reconnaissance. We will identify vulnerable people and processes and then find ways in which they might be exploited.

When carrying out Phishing or Physical site tests we will work with you to tailor and agree the thresholds for each test to ensure that your business operations are not affected or compromised.

Information Gathering

We will find the electronic profiles of your organisation and employees to ascertain; office locations, social media presence, contact names, job titles, email addresses and telephone numbers.

Reconnaissance

To confirm the identity of the contact details of individuals discovered during the information gathering phase, we will carry out reconnaissance by physical means, e-mail, or telephone. We are trying to gain more in-depth information about your organisation and gain trust or establish a connection.

Our reconnaissance methods could be:

- Telephone cold calling
- Email campaigns
- Covert physical review of your locationand security controls

Once completed, we will have identified specific targets and potentially gained their trust, we will then perform targeted attacks against those targets.

Physical Security Testing

We will try to gain access to a building or facility via bypassing security controls by pretending to be a legitimate person or via an entrance, such as:

- A delivery person
- Employee with or without fake ID
- Visitor
- Employee only entrance
- Vendor
- Lock picking / non-destructive break in

Once our tester has access to the building, they will perform one or more of these covert actions:

- USB device drop
- Wireless ACL bridge to LAN installation
- Hardware keyboard logger installation
- Remote covert camera installation, covert voice recorder installation
- Carry out a penetration test of your network, with or without a specific defined goal

Telephone

Using telephone communication methods our testers will try to extract sensitive information from users through external calls (cold call or spoofing caller id), fake internal calls (masquerading as helpdesk or reception), via voicemail, or SMS spoofing.

Mail

Using letters, spoofed advertising, USB devices containing malicious code, CD / DVD's containing malicious code and other physical mail methods, we will request sensitive information or try to trick users into replying or to perform an action.

E-Mail

Requesting sensitive information or tricking users to reply or to perform an action electronically using links or attachments in malicious emails.

What is the output from this assessment?

A full technical report will include the following:

- Executive Summary – explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed and recommendations of any remedial action that should be taken
- Summary of Findings – a table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state
- Detailed Findings:
  - The vulnerability's risk rating
  - The system, URL or process that contains the vulnerability
  - How the vulnerability was exploited
  - The risk posed to the organisation
  - Full technical details of how to replicate the vulnerability
  - Remediation advice
- Appendices – vulnerability output that was noted in the engagement

When evaluating the overall risk rating for each vulnerability, the following factors will be considered:

- Impact – the impact that exploitation of this vulnerability will have on the business or organisation
- Risk – the risk posed to the organisation if this vulnerability was exploited
- Likelihood – the likelihood that this vulnerability could be exploited

Each vulnerability will have a remediation recommendation, which will include either:

- Official fix, such as a firmware upgrade for hardware, or a patch for a publicly disclosed vulnerability
- When there is no official fix a workaround can be used
- Process improvement for when exploitation of vulnerability is caused by a business process

Additional Services

Additional Penetration Testing Services

We offer a number of additional penetration testing services which can either be carried out in conjunction with other testing phases or as a stand-alone assessment. However, if your organisation has a bespoke application or system that needs testing and is not covered here, please speak to our Cyber Security team or your BigDetech Account Manager to see where we can help.

Active Directory Review

It is paramount that your Microsoft Active Directory is configured securely as common misconfigurations can lead to unauthorised access to your infrastructure and data. Our Active Directory audit is an in-depth assessment marked against current best practices such as SANS and CIS together with our own experience to highlight vulnerabilities and recommended changes.

API Assessment

The Application Programming Interface (API) assessment methodology is a comprehensive assessment of an application's API following the Open Web Application Security Project (OWASP) testing methodology. The assessment can be carried out from black, grey, or white perspectives. All XML and RESTful API types can be tested.

Blended Vulnerability Assessment

The blended vulnerability assessment uses a combination of automated scans and manual testing to assist you in effective periodic and ongoing management of system vulnerabilities, whether they be on web servers, database servers, firewalls, routers, or other key components of your IT infrastructure.

Breakout Testing

Breakout testing is the process of evaluating locked down environments and attempting to use both known, and unknown, techniques to circumvent security controls that prevent users from accessing areas or applications unnecessary to their role or duty.

Kubernetes Testing

A Kubernetes platform audit will help you identify configuration issues at the various different layers in your environment. Ranging from API and management access to container build and configuration. We will work with you to understand your Kubernetes deployment and suggest security testing from a number of perspectives.

Malware Defence Testing

Malware defence testing involves measuring your organisation's security controls when non-malicious malware is introduced to either an endpoint, such as a workstation, laptop, or mobile device, or to a mail gateway or mail server.

Network Device and Access List/ Rule Review

Network devices, such as routers, switches, firewalls, or wireless access points can be reviewed for best practice security configuration, and access lists/rules can be reviewed. We use licensed software to conduct reviews of devices supported by Titania Nipper Studio, an industry standard tool, for performing configuration and audit reviews.

Purple Teaming

Our Purple Team service tests Security Operations Centre's (SOC) ability to detect, protect and respond to security events in a protectively monitored environment. The service provides collaboration between offensive (red) and defensive (blue) security teams, whereby the offensive team simulate Tactics, Techniques, and Procedures (TTP's) of real-world attackers and the defensive team tune their detections, defences, and incident response processes in reply.

Additional Cyber Security Capabilities

In addition to penetration testing services, we offer several aligned security professional services: Please speak to our Cyber Security team to find out more.

Security Consultancy

Our Turkey consultancy practice comprises of operational experts in security governance, risk, audit, and compliance. Our expertise includes risk and maturity assessment, security strategy, risk management, and standards compliance including ISO 27001:2013 (Information Security Management).

Vulnerability Management

Our TR-based vulnerability assessment team traces its origins back to 2017. Our team of experienced vulnerability analysts deliver vulnerability management, continuous and scheduled vulnerability assessments, network discovery scans, PCI ASV testing, and remediation advice and support.

About BigData

We understand that for most organisations' security today isn't straightforward. Our experts will help you simplify the inherent complexity of cyber security and ensure that you find and implement the right solutions for you.

With over 6 years' experience customer focussed cyber security team. They know that our customers are atdifferent points in their security evolution, and achieving your desired state isn't aone size fits all approach

Technical experts and highly knowledgeable sales teams; we have more expertise than ever before. Our strong relationships with market-leaders company , ensure our teamsare fully informed of new releases to keep you informed and in step with the latest industry developments.

IT is all about you

info@bigdata.tr | www.bigdata.tr

BigData Artificial Intelligence Technologies Company

Ankara/ Turkey