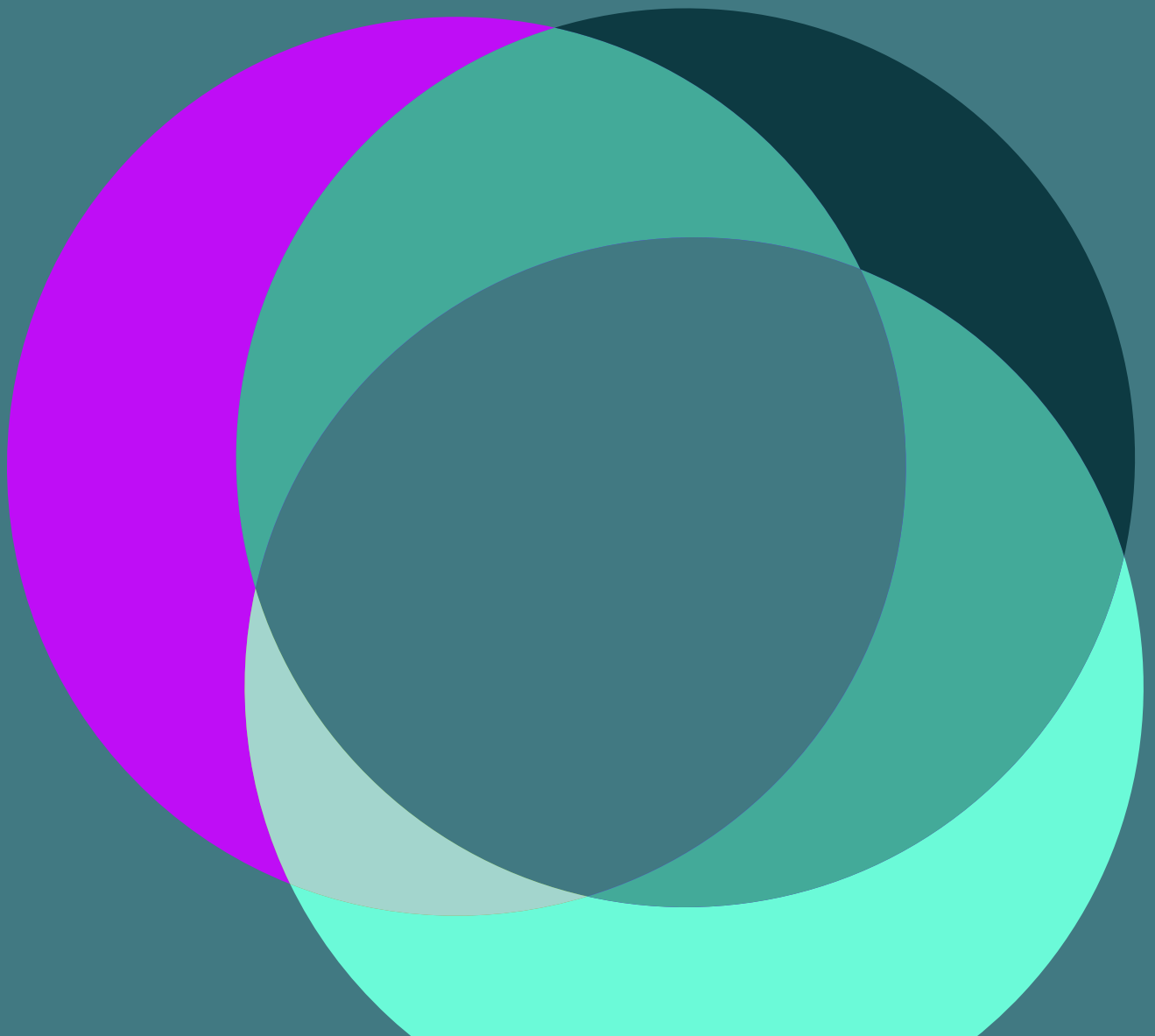




TRUSTMARQUE
Trusted. Technology. Together.

Penetration Testing services

Realise your resilience



Find your weak points before someone else does.

The purpose of Penetration Testing is to discover the weaknesses within your IT environment before malicious actors do and remediate them.

Trustmarque 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, including wireless, physical networks, web applications, active directory, and many more.

Trustmarque Penetration Testing services

Trustmarque 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 team hold professional certifications from CREST, the CyberScheme and are members of CHECK, which is run by NCSC.

If you require PCI-DSS Security Testing, PSN Code of Connection Testing for Public Sector, or HSCN/N3 Testing for healthcare, our services and staff clearances meet those needs.



Contents

Network penetration testing _____	4
Web application testing _____	5
Web service testing _____	6
Server build review _____	7
Client security evaluation _____	8
Breakout testing _____	9
Network device review _____	10
Segregation testing _____	11
Wireless testing _____	12
Social engineering _____	13
Red Team operations _____	15
Additional services _____	17
Assessments standard outputs _____	18
Why Trustmarque for your Penetration Testing _____	19

Network penetration testing

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:

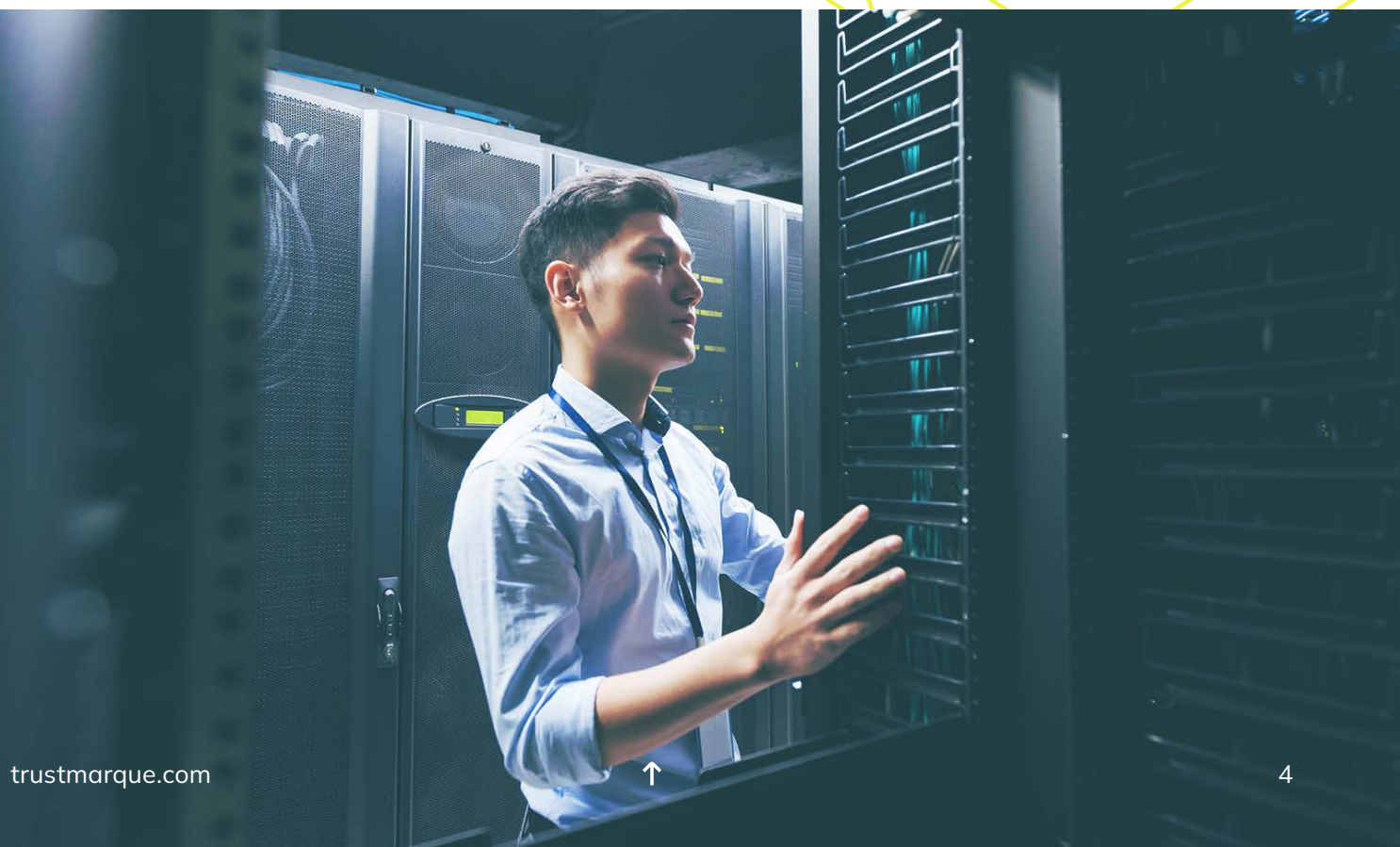
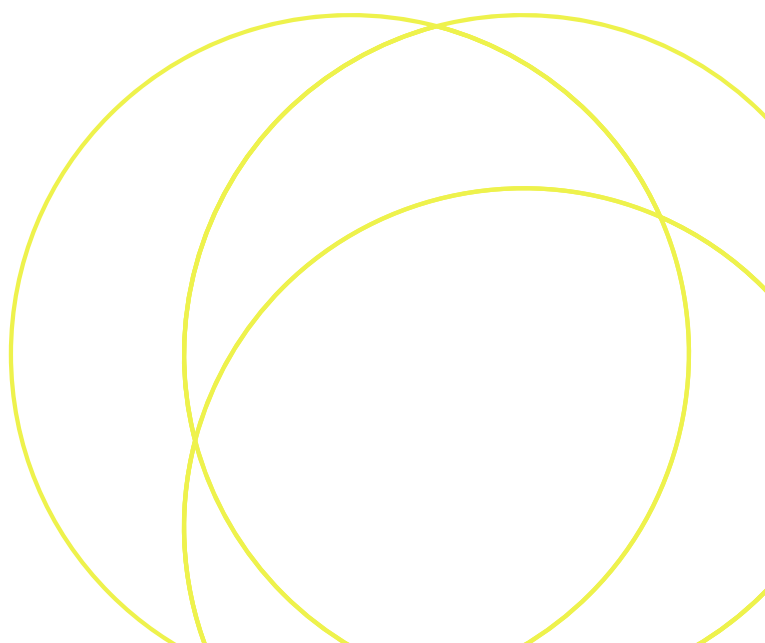
- Identify and exploit a vulnerability in an internet facing service, use it to gain access into an internal network, such as an office or a datacentre, and access Personally Identifiable Information (PII) of customers or staff members
- Once access has been gained to an internal network, this foothold can be used to compromise adjacent networks and target high value systems or users

What is the output from this assessment?

Also viewable on page 18

Does this involve exploitation of vulnerabilities?

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



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) 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 and details of its architecture, user rights assignment and the technologies used to build it.

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

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 is the output from this assessment?

Also viewable on page 18



Web service testing

What is it?

A web service penetration test aims to analyse and pinpoint security weaknesses in non-browser web services and APIs. This assessment focuses on identifying vulnerabilities at the application layer, considering both unauthenticated perspectives (anonymous attackers with malicious intent) and authenticated perspectives (testing access-controlled areas and user privileges). The objective is to identify any potential risks or flaws that could be exploited by attackers to compromise the security of the web service or API.

What is the output from this assessment?

Also viewable on page 18

Does this involve exploitation of vulnerabilities?

The primary objective is to accurately assess the security of the web service or API by actively exploiting vulnerabilities. The exploitation is carried out in a safe manner, avoiding any actions that could lead to potential negative consequences such as denial-of-service conditions.

To minimise disruption, testing often takes place in a pre-production environment to allow the application to be fully tested. By following this careful approach, you can gain valuable insights into the security of your web service or API and take appropriate measures to address any weaknesses.

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. These may be used to escalate their privilege level and access the server to compromise other devices in your network or domain.

Does this involve exploitation of vulnerabilities?

Typically, there is no exploitation within scope of this assessment, this is an authenticated standard configuration review performed using administrative credentials.

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 procedures (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.

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 target 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?

Also viewable on page 18

Client security evaluation

What is it?

A client security evaluation will review your organisations end user device (EUD) such as an employee's 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 device. 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?

Also viewable on page 18





Breakout testing

What is it?

A breakout test assesses the user environment's configuration and security posture from an authenticated perspective. It takes a standard user account and establishes whether appropriate restrictions are in place to prevent the user from breaking out of the locked down environment and into the underlying system. Breakout testing can be performed against a variety of platforms such as from Virtual Desktop Infrastructure (VDI), remote desktop services and kiosk mode environments.

What is the output from this assessment?

Also viewable on page 18

Does this involve exploitation of vulnerabilities?

The breakout test's primary objective is to accurately assess the security of the environment by actively exploiting vulnerabilities. The exploitation is carried out in a safe manner, avoiding any actions that could lead to potential negative consequences such as denial-of-service conditions. By following this careful approach, you can gain valuable insights into the security of your environment and take appropriate measures to address any weaknesses.

Network device review

What is it?

A network device review is a comprehensive configuration analysis of a network device such as a firewall, router or switch. This includes, the devices management configuration, services, timekeeping, logging, access control lists, and firewall rules. The audit is usually performed offline but can be done online via a web interface or command line access using secure shell (SSH).

Does this involve exploitation of vulnerabilities?

A network device review is an audit performed with credentials or configuration files and doesn't involve exploitation of vulnerabilities.

What configuration is reviewed?

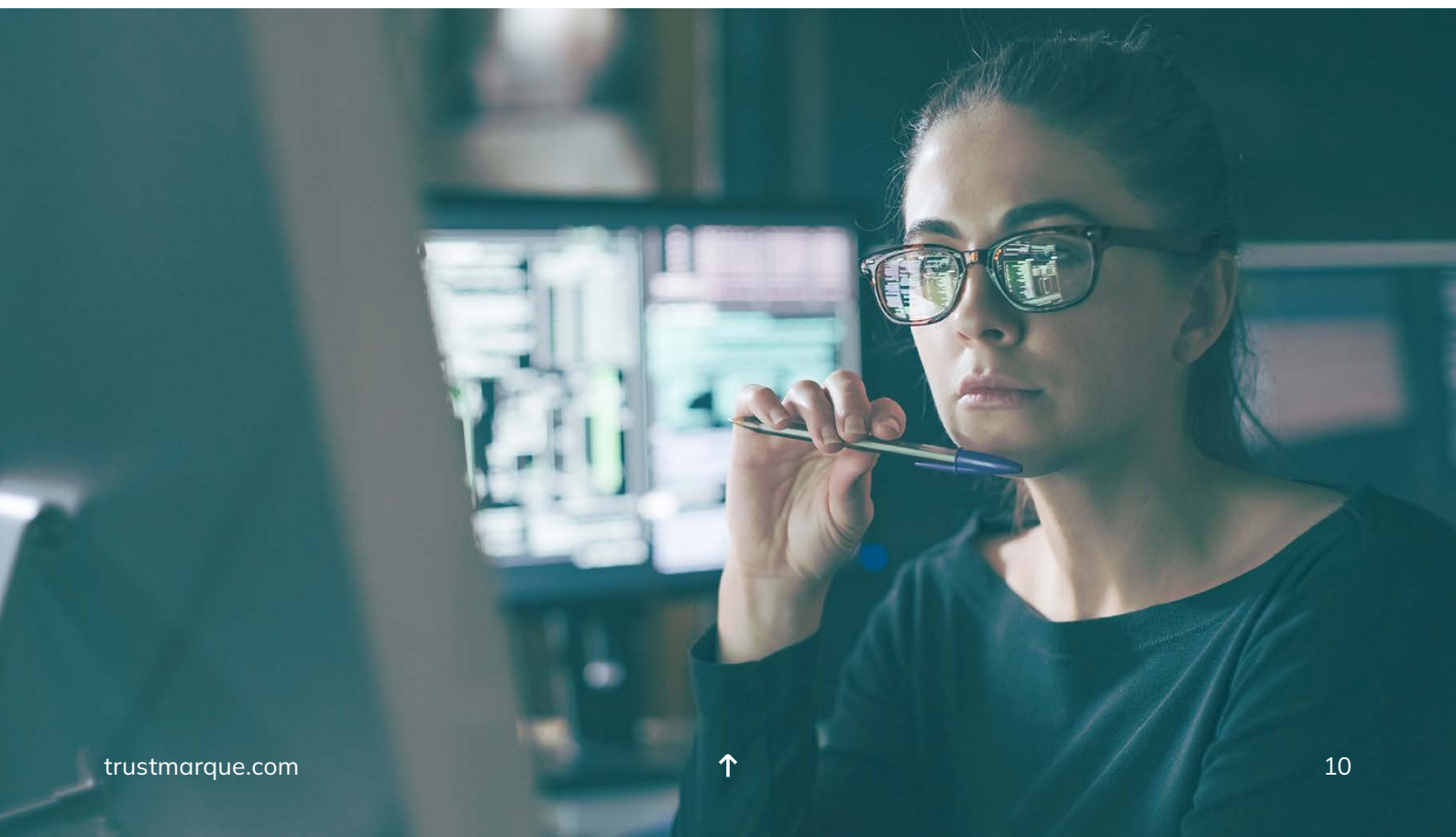
The management plane is responsible for configuring, monitoring, and maintaining the device. The review includes authentication and authorisation, session management, management services, and logging.

The control plane is responsible for deciding how packets are forwarded and processed. The review includes routing protocols, control protocols, and control plane protection mechanisms.

The data plane is responsible for the actual forwarding and processing of packets. The review includes assessing the access control lists and firewall rules for their permissiveness or other issues around their necessity and suitability.

What is the output from this assessment?

Also viewable on page 18



Segregation testing

What is it?

A segregation test is used to verify that network controls are effective in restricting network traffic as required. This checks that firewall rules and access control lists have been configured and deployed correctly, and that only expected traffic is able to traverse network boundaries. A consultant is positioned in a source network location and attempts to communicate with hosts in target network locations.

Does this involve exploitation of vulnerabilities?

A segregation test is an audit and therefore does not involve exploitation of vulnerabilities.

What is the output from this assessment?

The report provided after segregation test encompasses an executive summary and details regarding traffic that could traverse network boundaries. These results should then be compared with internal documentation that details expected results and determines whether there is any misconfiguration that needs to be resolved.

What is the output from this assessment?

Also viewable on page 18



Wireless testing

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.

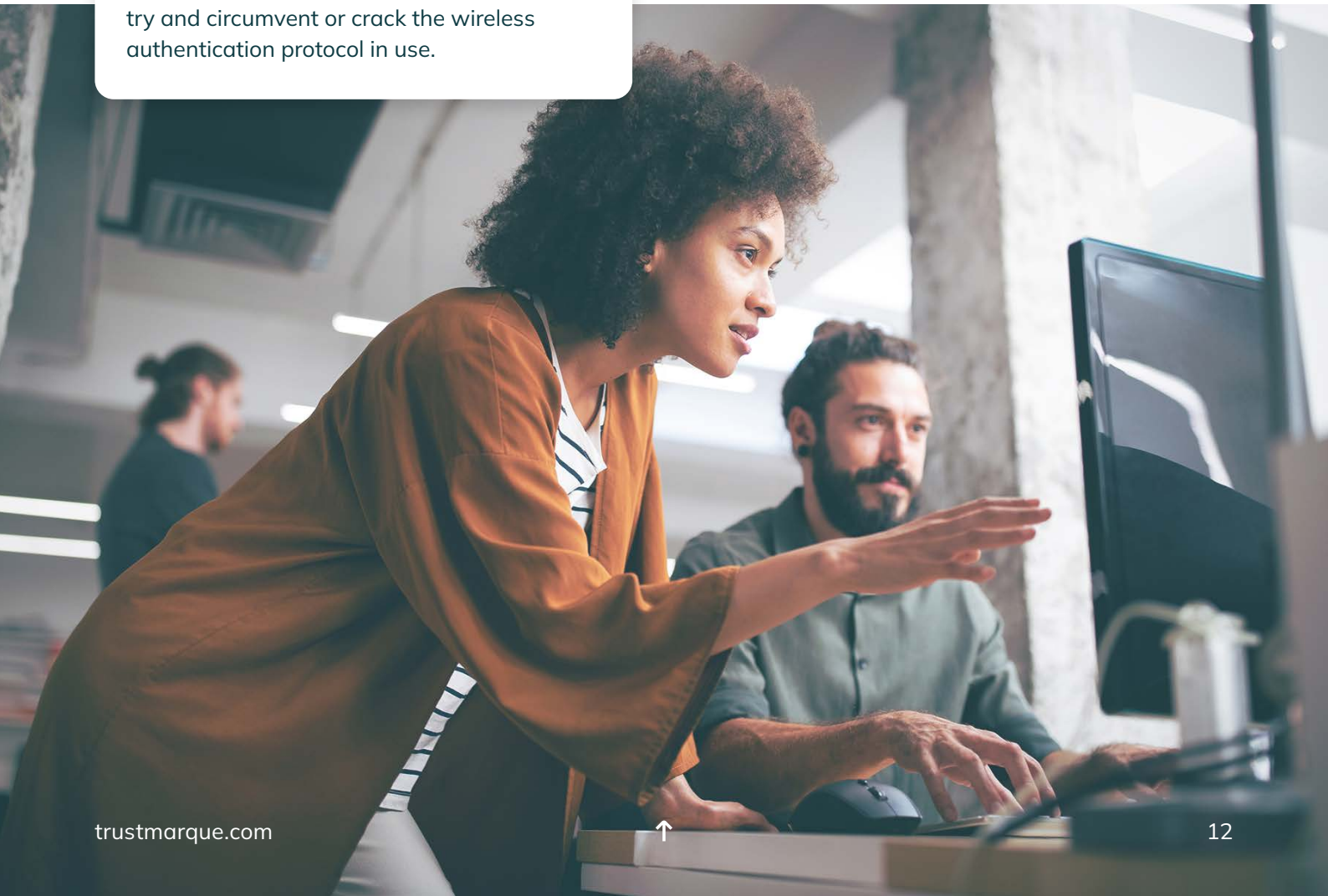
What configuration is reviewed?

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
- Attempt to reach adjacent networks and devices after connecting

What is the output from this assessment?

Also viewable on page 18



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 contain some methods such as targeted phishing emails, telephone based vishing, SMS based smishing and even physical security. 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, typically through open source intelligence gathering.

When carrying out social engineering 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.

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 location and security controls

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

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.



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?

Also viewable on page 18

Red Team operations

Overview

The members of our Red Team have specific areas of expertise, which they use to mirror a realistic attack, within the constraints of the agreed scope. The activities of a Red Team during the engagement are the same as malicious actors would use. The engagement will be tailored to your unique environment and objectives.

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.


What is the output from this assessment?


Also viewable on page 18


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 bypasses of endpoint detection and response (EDR) products
- Real world communication smuggling replicating the techniques used by the most skilled threat actors

 Recon


 Weaponise

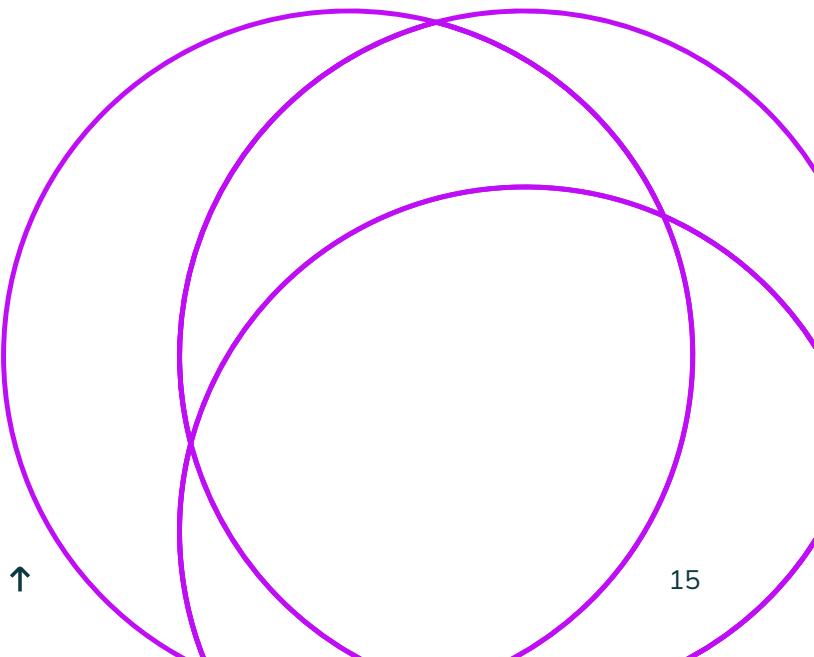
 Deliver

 Exploit

 Control

 Execute

 Maintain





Safety and risk management

The attack infrastructure used by our Red Team is heavily fortified to ensure any access into your organisation is protected. 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 ensure that 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. Trustmarque's Red Team will happily host debriefing sessions with your organisation's executives and defenders, so that any actions executed during the engagement window can be fully explained.

Additional 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 standalone 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 Trustmarque Account Manager to see where we can help.

Active directory review

This evaluates the configuration and deployment of your Microsoft Active Directory service. We also recommended that a server build review should be performed on a representative domain controller in combination with your active directory review. This will give a holistic view of the security posture of your domain deployment and management.

Application / thick client testing

An application / thick client test examines and identifies security vulnerabilities in a binary (thick client) application. This will include data at rest and data in transit.

Azure config review

Azure config review is aligned with CIS benchmarks and designed to ensure CIS security best practices have been considered when deploying an Azure cloud environment.

Kubernetes review

A Kubernetes review will help identify configuration issues at the different layers of your environment ranging from the API to management access to container build and configuration.

Mobile application testing

Mobile application testing will examine and identify security vulnerabilities in smartphone applications.

Mobile device review

Mobile device review will examine and identify security vulnerabilities in smartphone configuration.

Vulnerability management

Vulnerability assessment uses automated tooling to examine and identify security vulnerabilities in systems at the network layer with a broad coverage. The test does not include exploitation but does include some manual verification to exclude false positives. This can be performed unauthenticated or authenticated.





Assessments standard outputs

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
 - CVSSv2 and CVSSv3 scores
 - References
- **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

Why Trustmarque for your penetration testing

Our full defence cyber solutions pose a real threat to hackers. It's how we protect your people, processes and data. In a connected world, technology is evolving faster than ever, but external influences and sophisticated cybercriminal tactics are also accelerating the need for change. So, what can you do?

For 20 years we have nurtured an in-house team of cyber security experts to help you stay protected. Our portfolio of cyber solutions and world-class partners means we deliver game-changing professional services, technology and 24x7 UK based managed services to meet every one of your cyber security needs.



CREST Member Company – CREST accreditation services

CREST Qualified Consultants

- CREST Practitioner Security Analyst
- CREST Registered Penetration Tester
- CREST Certified Infrastructure Tester
- CREST Certified Web Application Tester

Vulnerability Assessment (VA)

- CREST Qualified Consultants
- CREST Practitioner Security Analyst
- CREST Registered Penetration Tester
- CREST Certified Infrastructure Tester

Application Status:

- Application Audited

[Visit CREST](#)



The Cyber Scheme

We are honoured to be sponsors for The Cyber Scheme and contribute to project design and help improve the cyber security industry from within.

[Visit The Cyber Scheme](#)



Penetration testing certifications

Trustmarque Cyber Security is an NCSC approved CHECK company offering penetration testing of IT systems to identify potential vulnerabilities and recommend effective security countermeasures.

[Visit CHECK service](#)



Cyber Essentials Plus

The Cyber Essentials Plus certification reassures our customers that we are constantly working to secure our IT against cyber attacks and have cyber security measures in place. It is also a requirement for some Government and Public Sector contracts.

- Sector: IT
- Certificate level: Cyber Essentials
- Certification Body: IASME

[Visit Cyber Essentials](#)

Resilient cyber security for uncertain times.

Cyber security from Trustmarque

With over 150 technical experts and highly knowledgeable sales teams; we have more expertise than ever before. Our strong relationships with market-leaders like Microsoft, Trend Micro, Check Point, Proofpoint, and Sophos, ensure our teams are fully informed of new releases to keep you informed and in step with the latest industry developments.

