FORFEND

INFORMATION SECURITY

Assured Service Provider

in association with National Cyber Security Centre

CHECK Penetration Testing

CREST

PEN TEST

THE CYBER SCHEME

CERTIFIED TESTERS

Protecting Your Digital World

Founded in 2022 and based in Birmingham, Forfend Information Security is an independent cyber security consultancy, CREST, and NCSC CHECK member delivering a complete range of technical penetration testing services.

With a commitment to excellence and innovation, Forfend ensures that your business is equipped to navigate the modern digital landscape securely.

Forfend operates a fully certified ISO 27001 Information Security Management System and ISO 9001 Quality Management System.

Our Mission

Our mission is to provide top-tier affordable security solutions. We understand that every client has unique needs, and our goal is to deliver bespoke penetration testing solutions that mitigate risks and enhance your security posture.

Our penetration testing services simulate real-world attacks to evaluate the effectiveness of your security measures. By identifying weaknesses before malicious actors can exploit them, we help clients strengthen their defences and protect their critical data and assets.

"Forfend's testing exceeded that carried out by other suppliers in previous tests and our requirements were fully understood due to Forfend's previous experience with similar clients."

UK Government Client

Why Choose Forfend?

Expertise

Our team is led by technical security experts with decades of combined experience in the field of information security.

Customisation

We tailor our services to meet the unique needs of each client, providing personalised solutions that deliver quality results.

Innovation

We stay ahead of the curve by continuously researching and implementing the latest security testing methodologies.

Commitment

The security of our clients is our top priority, and we are dedicated to providing the highest level of protection and service.

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

Contents

Network Penetration Testing

What is it?

Network infrastructure often presents the largest attack surface to an attacker. Whether internet or internal facing, each system in the environment represents an opportunity for an attacker to gain access to corporate data.

Infrastructure assessments examine the security posture of all the systems and services running in the environment and identify any vulnerabilities that could be exploited by an attacker.

Penetration Testing vs Vulnerability Assessments

Penetration testing and vulnerability assessments both play key roles in cyber security but have different focuses:

Penetration testing goes further by actively exploiting vulnerabilities to simulate real-world cyberattacks, assessing the actual risk and effectiveness of security defences. While vulnerability assessments focus on detection, penetration tests test the impact of those weaknesses in practice.

A vulnerability assessment identifies and evaluates potential security weaknesses in a system using automated tools and provides a list of vulnerabilities to be addressed.

Application Penetration Testing

What is it?

Applications are a key focus for attackers as they often serve as gateways to sensitive data and critical business functions, and vulnerabilities in these can lead to serious security breaches.

Application penetration testing involves simulating attacks to identify weaknesses in the software's code, design, or configuration. This testing goes beyond surface-level issues, focusing on finding vulnerabilities such as role based access controls (RBAC) misconfigurations, insecure APIs, or flaws in user authentication mechanisms. The objective is to uncover potential security risks before they can be exploited by malicious actors.

Regardless of the application type, Forfend will work with you to create a tailored testing model to address its specific security challenges based on the Open Web Application Security Project (OWASP) testing methodologies.

What types of applications can be tested?

Application penetration testing can be performed on all types of applications, each with its unique security considerations:

- Web applications which are accessible through browsers are common targets due to their internet exposure.
- Mobile applications typically installed on smartphones and tablets, introduce risks related to local data storage, insecure API usage, and insufficient platform security controls.
- Desktop applications run on user-operated machines and can be vulnerable to local privilege escalation and insecure file handling that attackers might exploit.
- Cloud applications, typically hosted on SaaS platforms, are tested for security risks related to integrations and data access.
- APIs (Application Programming Interfaces) expose application logic and data to other services and applications. Insecure APIs are a leading cause of data breaches, and testing typically targets authentication flaws, excessive data exposure, and input validation issues.
- Microservices which often make up larger distributed applications are tested to ensure secure communication and data handling across networks.

Cloud Configuration Review

What is it?

A cloud configuration security review assesses the settings and configurations of cloud environments to ensure they follow best practices and security standards. This review involves examining cloud services, such as virtual machines, storage, networks, and databases, to identify misconfigurations or vulnerabilities that could expose the system to unauthorised access or data breaches.

The improper configuration of cloud environments can introduce security vulnerabilities such as improper access controls, weak authentication mechanisms, insufficient encryption, and excessive permissions. The goal is to proactively identify and rectify potential risks before they can be exploited, helping your organisation to maintain secure and compliant cloud infrastructure.

What standards are the configurations reviewed against?

When conducting a cloud configuration security review, several standards and frameworks are commonly referenced to ensure best practices are followed. One key set of guidelines is the Center for Internet Security (CIS) benchmarks, which provide a comprehensive collection of security best practices for all cloud platforms including Azure, AWS, and Google Cloud Platform.

These benchmarks cover areas such as access control, encryption, network security, and auditing, offering a proven and structured approach to securing cloud environments.

Additionally, Forfend's own expertise in cloud security comes into play, as our deep knowledge of cloud architecture and potential vulnerabilities allows us to apply industry best practices and tailor security recommendations to each organisation's specific needs.

Operating System Build Review

What is it?

A build review is the process of evaluating and verifying the security configurations of an organisation's devices, systems, or software builds to ensure they are securely configured before deployment.

This involves reviewing baseline build images, which are pre-configured system images used as templates for deploying devices across an organisation. These images are thoroughly examined to ensure that they are free of vulnerabilities, misconfigurations, or unnecessary services that could create security risks.

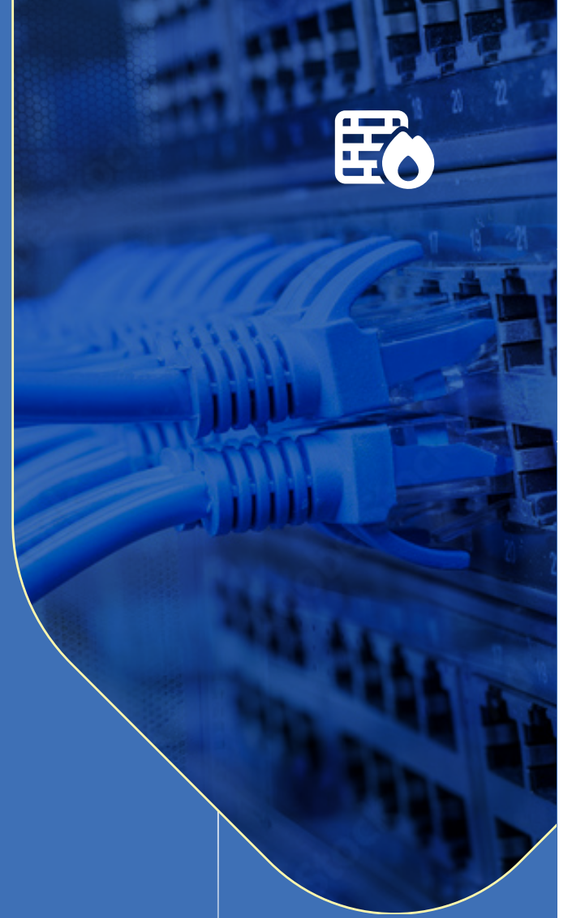
The review checks for proper settings including user access controls, patch management, installed software and versions, and network configurations. The goal is to ensure that devices are securely configured from the outset, minimising the potential attack surface and reducing the risk of security breaches.

What devices can be reviewed?

A build review can be conducted on various types of devices within an organisation to ensure their security configurations are robust and consistent. This includes user devices like desktops and laptops, which often serve as entry points for attackers if not properly secured.

Servers, both on-premises and cloud-based, are reviewed to ensure they are hardened against threats, with proper configurations for roles, permissions, and network access. Mobile phones and tablets also require security reviews, as they store sensitive data and connect to corporate networks, making them prime targets for exploitation.

Network Device Configuration Review



What is it?

A network device configuration review is the process of assessing and validating the security settings of devices that manage and control your organisation's network infrastructure, such as routers, switches, firewalls, and access points.

These devices play a crucial role in directing and securing network traffic, so ensuring they are properly configured is vital for protecting against unauthorised access, data breaches, and network attacks.

What is checked?

The review involves checking configurations like access control lists (ACLs), firewall rules, VPN settings, and network segmentation to ensure the devices follow best practices and align with the organisation's security policies. The goal is to identify any vulnerabilities or misconfigurations that could be exploited, ensuring the network infrastructure is secure, resilient, and able to defend against both internal and external threats.

Breakout Assessment

What is it?

A breakout assessment is a type of security review that focuses on evaluating the security of systems where users interact with isolated environments.

The goal is to assess whether an attacker could break out of the controlled environment to gain unauthorised access to the underlying host system or other parts of the network.

What systems can be tested?

In a breakout assessment, systems such as Citrix environments, remote desktop solutions, kiosk systems, and virtualised desktop infrastructure (VDI) setups are commonly tested. These systems often provide users with access to applications or resources in a controlled, isolated environment, but if not properly configured, they can become entry points for attacks.

The assessment checks for issues like improper session isolation, weak authentication mechanisms, or vulnerabilities in the software that could allow attackers to break out of their virtualised environment and gain unauthorised access to the underlying operating system or network resources.

Social Engineering

What is it?

A social engineering assessment is a security evaluation that tests an organisation's vulnerability to manipulation or deception tactics aimed at gaining access to sensitive information or systems by targeting authorised users.

These attacks exploit human psychology rather than technical vulnerabilities. The assessment simulates real-world social engineering techniques to identify gaps in your employees' awareness, training, and organisational policies, helping to improve defences against these types of threats.

What types of social engineering are available?

There are several common types of social engineering attacks, including phishing, smishing, and vishing, which target individuals through different communication channels:

- **Phishing** involves attackers sending fraudulent emails that appear to be from legitimate sources, such as internal teams, banks, or service providers, designed to entice the recipient into revealing sensitive information such as login credentials or financial details.
- **Smishing** is a variation of phishing that occurs through SMS text messages, where attackers send deceptive messages that contain malicious links or phone numbers to steal personal information.
- **Vishing** (voice phishing) targets victims through phone calls, where attackers impersonate trusted figures like tech support agents or bank representatives to manipulate individuals into providing sensitive data or performing actions that compromise security.

These techniques exploit trust and manipulate individuals into revealing information or taking actions that can lead to significant security breaches.

AI Testing

What is it?

AI testing involves evaluating the security, reliability, and performance of artificial intelligence (AI) systems, including machine learning (ML) systems and large language models (LLMs), to ensure they function as intended and are resistant to attacks, manipulation, data leakage, or misuse.

This type of testing assesses areas like data integrity, model robustness, and the system's ability to handle edge cases or adversarial inputs. AI testing helps organisations ensure that their AI models are secure from vulnerabilities that may lead to the compromise of their data, or impact their reputation.

What vulnerabilities might be identified?

AI testing helps identify several key vulnerabilities, including:

- Adversarial attacks, where malicious inputs manipulate AI decisions.
- Data poisoning, where corrupted data affects model training.
- Model inversion, allowing attackers to extract sensitive information from the AI.
- Bias and discrimination can arise from skewed training data, leading to unfair outcomes, while overfitting can cause models to perform poorly on new data.

Identifying these vulnerabilities ensures AI systems are secure and reliable.

Red & Purple Teaming

What is it?

Red and purple teaming are both designed to improve your organisation's security posture by simulating real-world attacks and improving defences.

Red teaming is an adversarial approach where security experts (the red team) simulate real-world cyberattacks using tactics, techniques, and procedures (TTPs) that a malicious actor might employ. The goal is to exploit vulnerabilities and bypass defences, providing a realistic threat intelligence-based assessment of your organisation's security weaknesses.

Using the MITRE ATT&CK framework, the focus is on testing the effectiveness of security systems and response protocols under real-world attack conditions.

What's the difference between red and purple teaming?

The difference between red teaming and purple teaming lies in collaboration and the overall objective.

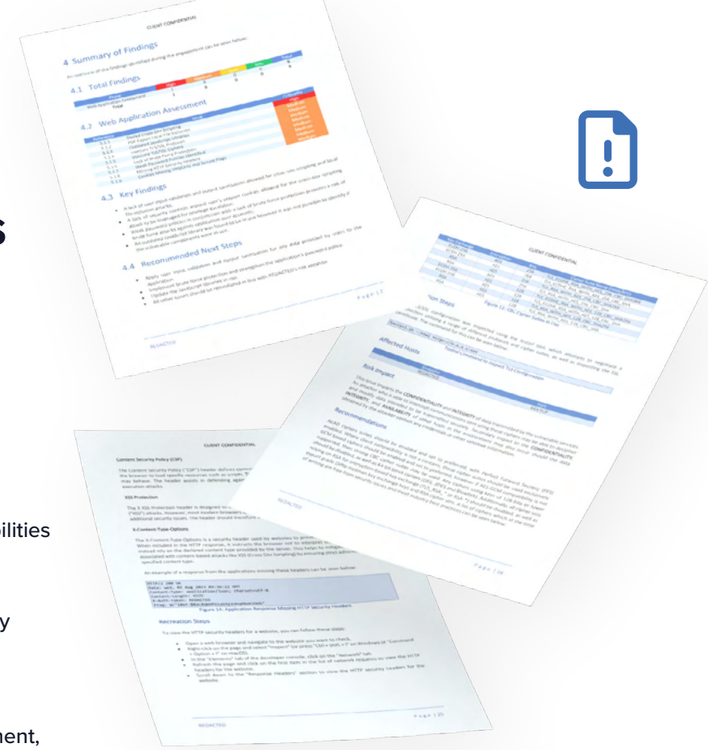
Red Teaming

Red teaming involves a dedicated group simulating realistic attacks to test your organisation's security from an adversary's perspective. By emulating real-world threats without prior coordination with the defenders, red teams expose gaps in detection, response, and prevention, offering valuable insights to strengthen your overall security posture.

Purple Teaming

The offensive and defensive teams work together, with the red team sharing insights about their tactics and the blue team applying countermeasures in real-time. This collaboration ensures that both offensive and defensive teams learn from each other, improving your organisation's overall security posture by identifying weaknesses and enhancing response capabilities in a more integrated way.

Assessment Standard Outputs



What is the output from each assessment?

A full technical report will include:

- An Executive Summary in plain English including an explanation of the vulnerabilities encountered, the risk they pose to your organisation, whether the objective was completed, and recommendations of any remedial actions that should be taken.
- A Summary of Findings table of all vulnerabilities noted during the assessment, the vulnerability title, its risk rating, and the vulnerability's current state.
- Detailed findings and 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, and full technical details of how to replicate the vulnerability.
- Remediation advice using CVSS scores.
- References and Appendices.

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 recommended workaround that can be used.
- Process improvement recommendation for when exploitation of vulnerability is caused by a business process.

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

Impact

The impact exploitation of this vulnerability will have on your business.

Risk

The risk posed to the organisation if this vulnerablilty was exploited.

Likelihood

The liklihood that this vulnerability could be exploited.

Additional Services

Active Directory (and Entra) Review

An Active Directory or Entra Review assesses the security configurations and policies within an organisation's directory services. It focuses on areas like user permissions, access controls, group policies, and overall infrastructure to ensure that they align with best practices and minimise vulnerabilities, systems and response protocols under real-world attack conditions.

Password Complexity Review

A password complexity review evaluates the strength and security of password policies across your organisation. It ensures that passwords are sufficiently complex, following industry guidelines for length, character variety, and expiration to prevent unauthorised access and reduce the risk of brute-force attacks.

M365 Review

Microsoft 365 security is a shared responsibility model with open and collaborative working configurations set by default. These default configurations can often lead to account compromise and data loss. An M365 review will assess the security of your M365 configuration and identify risks to your services and data based on best practices, providing pragmatic recommendations for improving M365 security.

Additional Services

Wireless Network Testing

Wireless network testing involves assessing the security of an organisation's Wi-Fi infrastructure, including encryption standards, authentication methods, and network segmentation. It identifies weaknesses like misconfigured access points or poor encryption that could expose the network to unauthorised access or attacks.

OSINT (Open-Source Intelligence) Gathering

OSINT involves gathering publicly available information from sources like websites, social media, and forums to identify potential security risks. It helps organisations identify vulnerabilities, leaks of sensitive data, or potential threats that could be exploited by malicious actors.

Segmentation Testing

Segmentation testing evaluates how well an organisation's network is divided into isolated zones to limit the movement of threats. It checks whether internal networks are properly segmented, preventing unauthorised lateral movement and helps contain potential breaches within specific network areas

Bespoke Testing

If you have requirements that are not covered by any of the testing types within this document, please let us know and we'll be happy to discuss your requirements.

Forfend are here to help.

Contact us to learn more about our services and how we can tailor solutions to meet your cybersecurity needs.

enquiries@forfendinfosec.com

0121 769 1922

FORFEND
INFORMATION SECURITY