secarma®
CYBERSECURITY EXPERTS

SERVICE OVERVIEW

Infrastructure Penetration Testing

Infrastructure Penetration Testing aims to exploit vulnerabilities in your company's networks and servers, to improve your resilience to internal and external attacks. We provide context around the vulnerability, threat and impact, as well as tailored advice on how to protect your critical operating systems and networks.

WHO IS IT FOR?

Infrastructure testing is for organisations who wish to gain a real-world view of their security posture.

For example, you may want to know if your customer data or staff payroll information is being stored and transmitted in a secure manner.

Alternatively, you might need to know the security weaknesses in your Internet-facing IT systems — such as email servers, routers, and web servers that host e-commerce websites.

If you've changed your systems, vulnerabilities could have been introduced. We may also find services that you didn't know you had exposed.

HOW CAN WE HELP?

We use a range of manual techniques, automated security tools and a proprietary methodology, to identify, validate, and exploit security vulnerabilities. Each test we conduct is individually tailored to your company's requirements, and the specific systems to be tested.

We're able to test individual systems right through to complex and extensive enterprise-wide infrastructures. We can also focus our investigation on your company's responsiveness to a particular type of attack, such as social engineering or ransomware.

WHAT WE TEST

By utilising similar tools and techniques to real-world threat actors, our team will identify, verify and priorities exploitable weaknesses within your infrastructure. Our tests include:

- **Known Vulnerabilities** - Missing security updates is a common weakness that can lead to services, operating systems and applications being compromised.
- **Default Misconfiguration** - Systems are often configured by default with compatibility in mind which can lead to insecurities such as weak encryption being used
- **Access Control** - Authentication systems often have weaknesses such as username enumeration, lack of bruteforce protection, or even just common and weak passwords.
- **Service Flaws** - Services accounts may have weaknesses that allow a threat actor to leverage the service for privilege escalation, such as insecure permissions or executable storage.

secarma®
CYBERSECURITY EXPERTS

METHODOLOGY OVERVIEW

Infrastructure Penetration Testing

Infrastructure testing aims to simulate common and likely attacks against networked assets, with the goal of demonstrating business risk. The following lists the stages of an infrastructure assessment, along with a flavour of the checks:

INFORMATION GATHERING

Before the engagement begins, we will map the attack surface to discover alive hosts, services and versions. This can include:

Open Source Intelligence - Online sources of information will be used to gather intelligence about the target organization, such as social media sites.

DNS Review - Domain Name Systems can allow new targets to be found or disclose information about targets.

Host Discovery - Alive hosts can be found passively by monitoring network traffic and actively with mapping tools.

Port Scanning - TCP and UDP services are discovered using port scanning techniques.

Service and OS Finger Printing - The exposed service and running operating system is discovered by monitoring network traffic and details of exposed services such as the type and version.

NETWORK ANALYSIS

Once target systems are discovered we will aim to find vulnerabilities within exposed services and in-use network protocols.

Username Enumeration- Methods of determining valid usernames include attacks such as ASREP Roasting and through inference in login system response differences.

Weak Network Protocols - Insecure protocols can include protocols such as Telnet which do not securely transmit credentials and data or protocols such as LLMNR which can lead to interception attacks and

EXPLOITATION

Exploitation involves discovering weaknesses within exposed services and systems and leveraging those weaknesses:

Known Vulnerabilities - Missing security updates is a common weakness that can lead to services, operating systems and applications being compromised.

Default Misconfiguration - Systems are often configured by default with compatibility in mind which can lead to insecurities such as weak encryption being used

Access Control - Authentication systems often have weaknesses such as username enumeration, lack of bruteforce protection, or even just common and weak passwords.

Service Flaws - Services accounts may have weaknesses that allow a threat actor to leverage the service for privilege escalation, such as insecure permissions or executable storage.

EXAMINE

Once access to systems has been gained business impact will be demonstrated through highlighting methods of accessing, modifying, or denying access to critical data.

Sensitive Data Access- Once high-level access has been achieved, access to specific business critical information such as financial information or other business-specific confidential data can be demonstrated.

Persistence - Once access has been gained, persistence can be demonstrated such that if a threat actor is discovered access cannot be revoked.

It is not possible to file a flight-plan for every single check that will be conducted. However, the above steps will always be applicable generally. The same process is followed for both remote and on-site engagements. We can also assess internal networks over VPN connections or using our bespoke "Virtual On-site Tester" solution.