External Infrastructure Penetration Testing

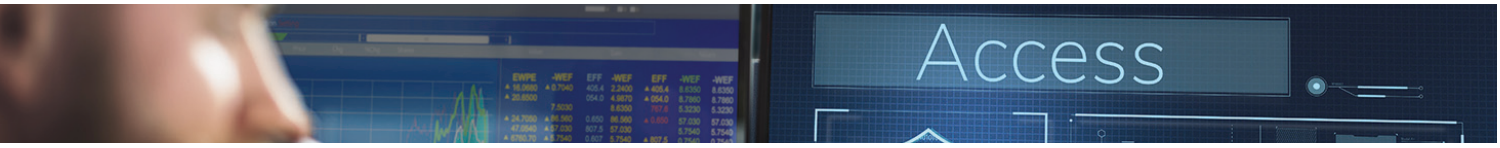
An External Security Test is conducted remotely, targeting systems specified by the Client. This assessment can be performed in two ways:

Vulnerability Testing - Assessing the network to highlight key vulnerabilities and weak systems that can be abused by an attacker.

Goal based testing - This assessment attempts to simulate a real world attack scenario, with the Client being able to carry out a specific scenario. The Client specifies a key system (or systems) and the Consultants attempt to compromise the specified host using a multiple, appropriate attack types.

Contact us:
01422 416000
sales@cognisys.co.uk www.cognisys.co.uk

Continued overleaf....



Both assessments aim to highlight vulnerabilities and mis-configurations of systems, privilege escalation, data theft or gain a foothold in the supporting network. The methods used for each assessment will be different, depending on the network, organisation and type of environment, and will take into account client concerns and risk appetite.

Along with assessing the actual technical risk, our consultants use analysis techniques to help your organisation mitigate the issues as quickly as possible. This will help reduce the risk posed to your company and users, reducing the likelihood of reputational damage.

After reporting the issues discovered during the assessment, Cognisys consultants are also available for further follow-up calls to clarify certain issues or help your organisation understand the risks posed. Our service can be fully tailored to the needs of your business, with reporting delivered in your preferred format where possible.

OVERVIEW

The following high-level areas are included within the assessment:

- Host discovery & port scanning
- Vulnerability assessment
- Manual identification and fingerprinting of services
- Privilege escalation
- Password evaluation
- Cryptographic storage analysis
- Exfiltration of data
- Assessment steps
- Discovery and enumeration
- The hosts are scanned, with exposed services being assessed using a combination of manual and automated techniques. This includes a vulnerability assessment of all exposed hosts and their services.
- Analysis and exploitation
- The assessment commences, analysing the findings and attempts are made, where safe and permitted, to exploit any vulnerabilities discovered. If access is gained to the internal network, attempts will be made to access key systems on the internal network.

REPORTING

The assessment is documented in a simple, easily digestible format.

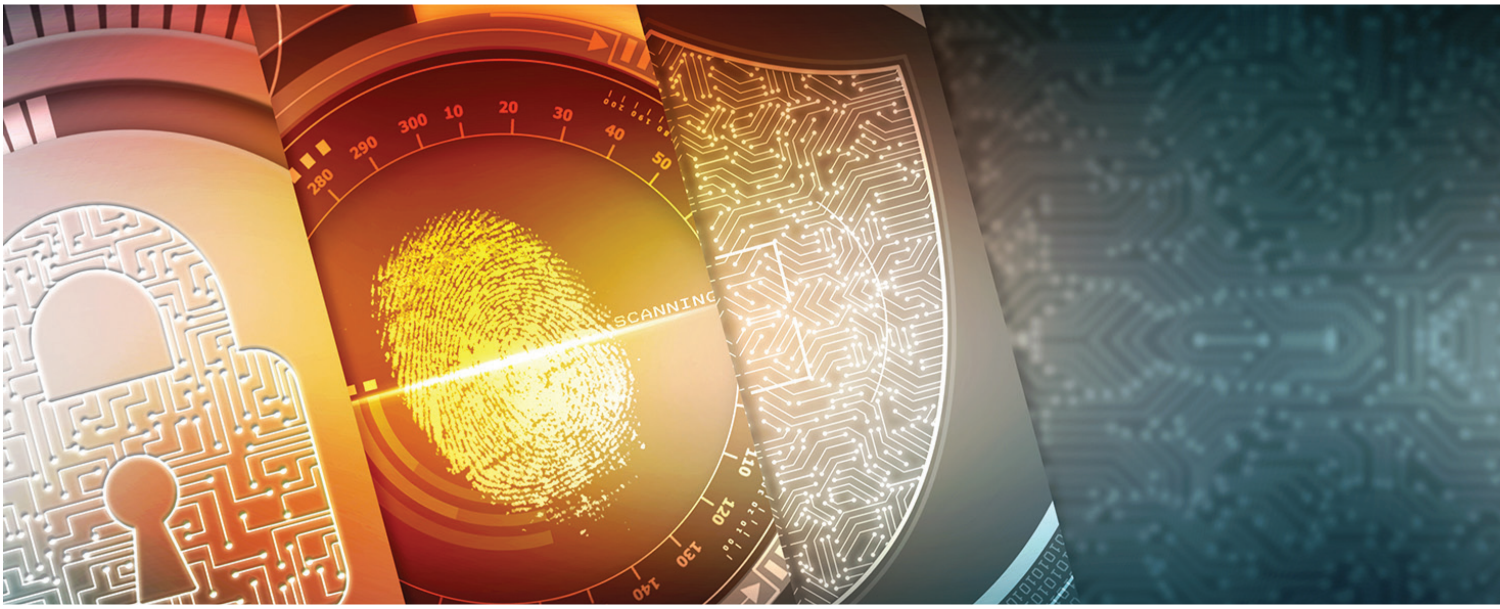
Contact us:

01422 **416000**

sales@cognisys.co.uk www.cognisys.co.uk

COGNISYS
Smarter Cyber Security

WEB APPLICATION SECURITY TESTING
SECURITY AUDITING INTERNAL PENETRATION TESTING
EXTERNAL PENETRATION TESTING PCI COMPLIANCE
MANAGED SECURITY CYBER ESSENTIALS
ISO27001 GAP ANALYSIS LOST/STOLEN LAPTOP TEST



Internal Penetration Testing

An Internal Security Assessment is conducted on client premises, targeting systems specified in advance by the Client. This assessment can be performed in two ways:

Vulnerability Assessment - Assessing the network to highlight key vulnerabilities and weak systems that can be abused by an attacker.

Goal based testing - This assessment attempts to simulate a real world attack scenario, with the Client being able to carry out a specific scenario. The Client specifies a key system (or systems) and the Consultants attempt to compromise the specified host using a multitude of attack types, as well as any machine attached to the network.

Contact us:

01422 416000

sales@cognisys.co.uk www.cognisys.co.uk

Continued overleaf....

COGNISYS
Smarter Cyber Security

WEB APPLICATION SECURITY TESTING
SECURITY AUDITING INTERNAL PENETRATION TESTING
EXTERNAL PENETRATION TESTING PCI COMPLIANCE
MANAGED SECURITY CYBER ESSENTIALS
ISO27001 GAP ANALYSIS LOST/STOLEN LAPTOP TEST

Both assessments aim to highlight vulnerabilities and mis-configurations of systems, which can allow a user who is not on the domain to perform privilege escalation, data theft or gain a foothold into another attached network. The methods used for each assessment will be different, depending on the network, organisation and type of environment, and will take into account any client concerns and risk appetite.

Along with assessing the actual technical risk, our consultants use analysis techniques to help your organisation mitigate the issues as quickly as possible. This will help reduce the risk posed to your company and users, reducing the likelihood of reputational damage.

After reporting the issues discovered during the assessment, our consultants are also available for further follow-up calls to clarify certain issues or help your organisation understand the risks posed.

Our service can be fully tailored to the needs of your business, with reporting delivered in your preferred format where possible.

OVERVIEW

The following high-level areas can be included within the assessment:

- Host discovery & port scanning
- Vulnerability assessment
- Manual identification and fingerprinting of services
- Privilege escalation attempts to access the "crown jewels" of the network
- Password evaluation
- VLAN hopping
- Analysis of VOIP services
- Cryptographic storage analysis
- Exfiltration of data
- Assessment steps
- Discovery and enumeration
- The hosts are scanned, with exposed services being assessed using a combination of manual and automated techniques. This includes a vulnerability assessment of all exposed hosts and their services.

ANALYSIS AND EXPLOITATION

The assessment commences, analysing the findings and attempts are made, where safe and permitted, to exploit any vulnerabilities discovered. If access is gained to the internal network, attempts will be made to access key systems on the internal network.

REPORTING

The assessment is documented in a simple, easily digestible format.

Contact us:

01422 **416000**

sales@cognisys.co.uk www.cognisys.co.uk