AMICIS
GROUP

Together, we'll build cyber resilience.

Amicis Group Delivery
AutomatedPenetration Testing
Services – G-Cloud 14
Service Description
May 2024

hello@amicisgroup.co.uk

www.amicisgroup.co.uk

External Infrastructure Penetration Test and Vulnerability Assessment

What we'll do

An external infrastructure penetration test, also known as an external network penetration test or external security assessment, is a type of cybersecurity assessment conducted by automated testing software to evaluate the security of an organisation's external network and infrastructure. The primary goal is to identify vulnerabilities and weaknesses that could be exploited by malicious actors from outside the organisation.

Our automated network penetration testing methodology follows the **exact same** process as a manual test, but we are able to conduct it in a fraction of the time, repeatedly and consistently.

It is important to note that while we deploy automated technologies to execute the test itself, we will work with you through every step of the test.

How we'll do it

Scope Definition

We will begin by clearly defining the objectives of the penetration test and vulnerability assessment, by ensuring we understand our client's goals and expectations. We will work with the client to define the scope of the assessment by identifying the specific external systems, networks, and applications that will be tested.

We will confirm the rules of engagement, including permissible testing methods, testing hours, and the extent of potential disruptions.

Information Gathering

We will gather publicly available information about the target organisation, such as domain names, IP ranges, and employee details.

We will then conduct active scanning to identify live hosts, open ports, and services running on external infrastructure.

Vulnerability Assessment

We will utilise automated vulnerability scanning tools to identify known vulnerabilities in the external infrastructure components.

We will support the above activities by performing manual verification of identified vulnerabilities to eliminate false positives and identify potential security weaknesses that automated tools may miss.

Penetration Testing

We will attempt to exploit the vulnerabilities identified during the vulnerability assessment to gain unauthorised access or control. If successful, we will escalate privileges to demonstrate the impact of a successful attack.

If possible, we will maintain access to the target systems to assess persistence.

What you'll receive

Analysis and Reporting

We will analyse the results of the vulnerability assessment and penetration testing to determine the impact of vulnerabilities and potential risks. We will then rank and prioritise the identified vulnerabilities based on their severity, potential impact, and likelihood of exploitation in line with the Common Vulnerability Scoring System (CVSS).

We will draft a detailed report that includes an executive summary, technical findings, recommendations, and remediation steps.

Remediation Assistance

We will provide actionable recommendations for mitigating identified vulnerabilities and improving the security posture of the external infrastructure. Plus, we will offer assistance to the client in implementing remediation measures and verifying their effectiveness.

Post-Testing Activities

We will conduct a thorough debriefing session with the client to discuss the findings, recommendations, and any additional insights.

We will maintain comprehensive records of the assessment process, findings, and remediation efforts. We will also encourage the client to implement continuous monitoring of their external infrastructure to detect and address future vulnerabilities.

Quality Assurance

We will have a qualified team member review the assessment to ensure the quality and accuracy of the findings and recommendations.

Compliance and Legal Considerations

We will ensure that all testing activities comply with relevant laws and regulations, including obtaining necessary permissions and approvals in advance of the commencement of any testing activities.

Client Education

We will offer training and educational resources to help the client's team understand the vulnerabilities and security best practices.

Follow-Up Engagement

We will recommend periodic external infrastructure penetration tests and vulnerability assessments to maintain security vigilance.

By following this methodology, Amicis Group can systematically assess the external infrastructure of its clients, identify vulnerabilities, and provide valuable recommendations to enhance their security posture. It's important to note that we will adapt the methodology to specific client needs and industry standards. Additionally, we will always maintain ethical and legal standards throughout the assessment process.

Internal Infrastructure Penetration Test and Vulnerability Assessment

What we'll do

In an internal infrastructure penetration test and vulnerability assessment we will aim to identify security weaknesses and vulnerabilities within your organisation's internal network and systems which could be exploited by malicious actors if they are able to gain access to these resources.

Our automated network penetration testing methodology follows the **exact same** process as a manual test, but we are able to conduct it in a fraction of the time, repeatedly and consistently.

It is important to note that while we deploy automated technologies to execute the test itself, we will work with you through every step of the test.

How we'll do it

Scope Definition

We will begin by clearly defining the scope of the assessment, including the target systems, networks, and objectives. We will determine what the client wants to achieve through this assessment, such as identifying vulnerabilities, assessing security controls, or testing incident response procedures.

We will ensure that all legal and compliance requirements are met. We will obtain necessary permissions and agreements from the client organisation and ensure that testing activities comply with relevant regulations (e.g., GDPR, HIPAA).

We will identify the team members and resources required for the engagement, including skilled penetration testers, testing tools, and any hardware or software needed for the assessment.

Information Gathering

We will deploy network scanning tools to identify all active hosts, services, and open ports within the internal infrastructure.

We will examine network diagrams, system documentation, and any available information (where provided) to understand the architecture and configuration of the internal infrastructure.

Vulnerability Analysis

We will conduct vulnerability scans using automated tools to identify known weaknesses in the infrastructure, such as outdated software, misconfigurations, or missing patches. We will also perform a manual vulnerability assessment to identify vulnerabilities that automated tools might miss, including logic flaws or complex misconfigurations.

Exploitation and Penetration Testing

We will attempt to exploit identified vulnerabilities to assess their real-world impact. We will, though, remain cautious to avoid causing damage to systems or data. We will then try to escalate privileges from a low-level user to assess the effectiveness of access controls and privileges management. If achieved, we will test the ability to move laterally within the internal network, simulating an attacker's progression.

Post-Exploitation

If access is gained, we will attempt to maintain it to assess the organisation's ability to detect and respond to such persistent threats. If it is within the agreed scope of the test, we will attempt to exfiltrate sensitive data to evaluate data protection mechanisms.

What you'll receive

Analysis and Reporting

We will analyse the results of the vulnerability assessment and penetration testing to determine the impact of vulnerabilities and potential risks. We will then rank and prioritise the identified vulnerabilities based on their severity, potential impact, and likelihood of exploitation in line with the Common Vulnerability Scoring System (CVSS).

We will draft a detailed report that includes an executive summary, technical findings, recommendations, and remediation steps.

Remediation Assistance

We will provide actionable recommendations for mitigating identified vulnerabilities and improving the security posture of the external infrastructure. Plus, we will offer assistance to the client in implementing remediation measures and verifying their effectiveness.

Post-Testing Activities

We will conduct a thorough debriefing session with the client to discuss the findings, recommendations, and any additional insights.

We will maintain comprehensive records of the assessment process, findings, and remediation efforts. We will also encourage the client to implement continuous monitoring of their external infrastructure to detect and address future vulnerabilities.

Quality Assurance

We will have a qualified team member review the assessment to ensure the quality and accuracy of the findings and recommendations.

Compliance and Legal Considerations

We will ensure that all testing activities comply with relevant laws and regulations, including obtaining necessary permissions and approvals in advance of the commencement of any testing activities.

Client Education

We will offer training and educational resources to help the client's team understand the vulnerabilities and security best practices.

Follow-Up Engagement

We will recommend periodic external infrastructure penetration tests and vulnerability assessments to maintain security vigilance.

By following this methodology, Amicis Group can systematically assess the internal infrastructure of its clients, identify vulnerabilities, and provide valuable recommendations to enhance their security posture. It's important to note that we will adapt the methodology to specific client needs and industry standards. Additionally, we will always maintain ethical and legal standards throughout the assessment process.

Web Application Penetration Test & Vulnerability Assessment

What we will do

In a web application penetration test and vulnerability assessment we will provide you with a comprehensive evaluation of the security of your web application. We will attempt to identify and exploit vulnerabilities within the application which could be of use to malicious actors.

Our automated network penetration testing methodology follows the **exact same** process as a manual test, but we are able to conduct it in a fraction of the time, repeatedly and consistently.

It is important to note that while we deploy automated technologies to execute the test itself, we will work with you through every step of the test.

How we will do it

Scope Definition

We will begin by understanding the client's requirements and objectives for the penetration test. We will define the scope, including the target web applications to be tested, testing environments and any specific testing goals or areas of concern.

We will ensure that all legal and compliance requirements are met. We will obtain necessary permissions and agreements from the client organisation and ensure that testing activities comply with relevant regulations.

We will identify the team members and resources required for the engagement, including skilled penetration testers, testing tools, and any hardware or software needed for the assessment.

Information Gathering

We will collect publicly available information about the target application(s), including domain names, IP addresses, subdomains, technologies used, and any relevant infrastructure details. We will also obtain and review any available documentation related to the application's architecture, design, and functionality.

Threat Modelling

We will analyse the application's architecture and functionality to identify potential threats and attack vectors.

We will then prioritise those threats based on their potential impact on the application and business, as well as the likelihood of exploitation.

Vulnerability Scanning

We will deploy automated scanning tools and software to identify common vulnerabilities such as SQL injection, cross-site scripting (XSS), and security misconfigurations.

Manual Testing

We will conduct manual testing to identify more complex vulnerabilities, including business logic flaws, authentication issues, and authorisation problems. Plus, we will evaluate session management mechanisms to ensure they are secure and not vulnerable to session fixation or hijacking.

Authentication and Authorisation Testing

We will test the strength of authentication mechanisms and verify the resistance to brute-force password brute-force hacking.

We will also verify that users can only access the resources they are authorised to and that there are no privilege escalation vulnerabilities.

Data Validation and Input Testing

We will assess how the application handles user inputs and test for vulnerabilities like XSS, CSRF, and command injection.

We will also examine the security of file upload functionalities, ensuring that malicious files cannot be uploaded or executed.

API Testing (if applicable)

If API testing is also within the scope of the assignment, we will test the security of APIs, including authentication, authorisation, and data validation. We will also check for rate limiting and throttling mechanisms to prevent abuse.

What you will receive

Analysis and Reporting

We will analyse the results of the vulnerability assessment and penetration testing to determine the impact of vulnerabilities and potential risks. We will then rank and prioritise the identified vulnerabilities based on their severity, potential impact, and likelihood of exploitation in line with the Common Vulnerability Scoring System (CVSS).

We will draft a detailed report that includes an executive summary, technical findings, recommendations, and remediation steps.

Remediation Assistance

We will provide actionable recommendations for mitigating identified vulnerabilities and improving the security posture of the external infrastructure. Plus, we will offer assistance to the client in implementing remediation measures and verifying their effectiveness.

Post-Testing Activities

We will conduct a thorough debriefing session with the client to discuss the findings, recommendations, and any additional insights.

We will maintain comprehensive records of the assessment process, findings, and remediation efforts. We will also encourage the client to implement continuous monitoring of their external infrastructure to detect and address future vulnerabilities.

Quality Assurance

We will have a qualified team member review the assessment to ensure the quality and accuracy of the findings and recommendations.

Compliance and Legal Considerations

We will ensure that all testing activities comply with relevant laws and regulations, including obtaining necessary permissions and approvals in advance of the commencement of any testing activities.

Client Education

We will offer training and educational resources to help the client's team understand the vulnerabilities and security best practices.

Follow-Up Engagement

We will recommend periodic web application tests and vulnerability assessments to maintain security vigilance.

By following this methodology, Amicis Group can systematically assess web applications of its clients, identify vulnerabilities, and provide valuable recommendations to enhance their security posture. It's important to note that we will adapt the methodology to specific client needs and industry standards. Additionally, we will always maintain ethical and legal standards throughout the assessment process.