

**Internal Infrastructure Scoping**

**Internal Penetration Testing Assessment**

Provide company name, your name, email and job title.

|  |
| --- |
| Company Name:Your Name: Email Address:Job Title: |

*Provide your company name, your name, corporate email address and job title.*

Please provide a list of all IP addresses, domains, subdomains, and network ranges that need to be tested.

|  |
| --- |
|  |

*For example IP Addresses: 192.168.1.10 – Domains: example.com – Subdomains: api.example.com – Network Ranges: 192.168.1.0/24.*

Are there any specific IP addresses, domains, or subdomains that must not be tested?

|  |
| --- |
|  |

*For example IP Addresses: 192.168.1.10 – Domains: example.com – Subdomains: api.example.com – Network Ranges: 192.168.1.0/24.*

Are authenticated patch scans required? If yes, what percentage would be enough to meet your requirements?

|  |
| --- |
|  |

*For example, 10% is required as a minimum for PSN*

What are the primary business objectives driving this test? (e.g. compliance, yearly security assessment)

|  |
| --- |
|  |

Is there a date on which the testing must be completed? If yes, provide the date.

|  |
| --- |
|  |

Is there anything else you would like us to know?

|  |
| --- |
|  |

**Cyber Security Assessment Process**

|  |  |
| --- | --- |
| Checklist with solid fill | Scoping Document CompletionThe first step involves completing the scoping document. This document will help us understand your systems, applications, and objectives. It outlines the areas that need to be assessed and ensures we capture all essential information to deliver a thorough and accurate cybersecurity assessment. |
| Speaker phone with solid fill | **Scoping Call (If Required)**If further clarification is needed, we will arrange a scoping call. We recommend having application developers present to address technical questions and provide insights. During the call, we also request a live demonstration of the application to better understand its functionality and potential areas of risk. |
| Contract with solid fill | **Proposal Submission**Based on the scoping document and any additional information gathered during the scoping call, we will provide a formal proposal. This outlines the scope of the assessment, including what is in and out of scope, the estimated duration of testing, and the associated costs. This ensures full transparency and alignment before the assessment begins. |
| Monthly calendar with solid fill | **Project Management**Once the proposal is accepted, we initiate project planning to ensure the assessment is delivered on time and meets your internal deadlines. We will coordinate with you to schedule the assessment, define key milestones, and identify any dependencies. Our team will maintain clear communication throughout the project, ensuring expectations are aligned, and any logistical or technical challenges are addressed promptly. |
| Scientist male with solid fill | **Cybersecurity Assessment**When the project plan is in place, our experienced cybersecurity professionals will conduct the assessment. Using industry-recognised standards and our proprietary Cyber Alchemy methodology, we thoroughly evaluate your systems to identify vulnerabilities and assess risks. Throughout the assessment, our consultants will provide regular updates on progress and promptly report any critical issues or concerns. This ensures you remain informed and can address urgent matters without delay. |
| Document with solid fill | **Report Delivery**Upon completion of the assessment, we compile a comprehensive report. This includes a management summary, detailed findings with CVSS scores, likelihood and potential impact of exploitation, proof of concept for critical vulnerabilities, and clear mitigation steps. This report serves as a valuable resource for both technical and non-technical stakeholders. |
| Online meeting with solid fill | **Post-Assessment Review**We offer a post-assessment review meeting to walk you through the report. This session allows your team to ask questions, clarify findings, and understand exploitation methods and mitigation strategies. Our goal is to ensure your developers can address vulnerabilities effectively and avoid similar issues in the future. |

**Infrastructure Assessment**

**Approach:**

Infrastructure assessments can be performed remotely or on-site, depending on the accessibility of the assets in scope. The assessment aims to identify any vulnerabilities that can be exploited to attack the system or other users, bypass controls, escalate privileges, or extract sensitive data.

The consultants will use proven non-invasive testing techniques during the assessment to quickly identify weaknesses. Cyber Alchemy’s infrastructure testing methodology is given below.

**Methodology:**

The first step of the engagement is to set primary contacts on both sides, define the testing objectives and set the context. From this, a bespoke approach can be crafted to extract the maximum amount of value from the engagement. Once this has been done, Cyber Alchemy will begin the assessment, covering the following techniques. Examples of the type of testing and its objectives are given for each category. Specific testing will depend on the technology and protocols implemented and the testing objectives.

**Network Scanning**

* Conduct automated scans of given IP addresses, drawing a network topology.
* Identify all active hosts in the scope of the assessment.
* Determine key assets and potential entry points.
* Included scans:
	+ Nmap TCP scan (all 65535 ports)
	+ Nmap UDP scan (standard ports)

**Network Segmentation Assessment**

* Evaluate each segment’s isolation characteristics.
* Test boundaries and cross-segment access.
* Monitor traffic patterns for anomalies.
* Check for proper segmentations against best practices.

**Profiling Systems and Services**

* Identify the type and version of operating systems.
* Catalogue active services and applications.
* Determine software versions to spot outdated systems.
* Prioritise systems based on potential vulnerability risks.

**Vulnerability Detection**

* Scan systems and networks for known vulnerabilities.
* Analyse potential risks and their implications.
* Rank vulnerabilities based on potential impact and exploitability.

**Vulnerability Verification and Exploitation**

* Confirm the legitimacy of detected vulnerabilities.
* Conduct controlled exploitation attempts only where it is safe to do so.
* Document successful exploitation paths.
* Analyse the system and data exposure for each vulnerability.
* Examples of detected vulnerabilities:
	+ Outdated operating systems
	+ Over-exposed external ports
	+ SMTP server spoofing and unauthorised relay
	+ User enumeration risks
	+ Weak SSL/TLS configurations
	+ Access via Telnet
	+ Firewall misconfigurations

**Privilege Escalation**

* Examine systems for potential privilege escalation vectors.
* Test privilege escalation techniques in a controlled manner.
* Document the highest level of privilege attained.
* Evaluate implications of escalated privileges on system security.