Penetration Test Scoping Questionnaire

We generally prefer doing a short, 30-minute scoping call to discuss the scope and your needs. If you do too, or you have any questions about anything in the document, reach out!

Firstname Lastname

Email address

Mobile number

|  |  |
| --- | --- |
| External Penetration Test Test your internet-facing services from the perspective of an external attacker.  (Bespoke web apps not included; fill-in Web App Pentest section for that.) | |
| How many external IP addresses (in total) do you own? |  |
| How many of those are live? (hosting at least 1 service) |  |

|  |  |
| --- | --- |
| Internal Penetration Test Test your internal environment from the perspective of an attacker who has broken through the perimeter. | |
| How many servers are there (both physical and virtual)? |  |
| How many networking devices are there (routers, switches, access points etc...)? |  |
| How many user devices are there (workstations, laptops)? |  |
| How many IoT devices are there (cameras, phones, printers, anything else with an IP address)? |  |
| Is there a Windows Domain (Active Directory)? |  |
| What physical location are we testing from? |  |

|  |  |
| --- | --- |
| Wireless Penetration Test Can your wireless networks be used as an entry point for attackers? | |
| How many physical locations are we testing from? Where are they? |  |
| For each location, how many wireless networks (SSIDs) are there (e.g. corporate & guest)? |  |

|  |  |
| --- | --- |
| Web Application Penetration Test Test your custom-built web application for security vulnerabilities.  The easiest way to scope a web app is to have our consultants look at it. | |
| What URL should we use to access the app? |  |
| Are we testing from an Authenticated perspective?  (Authenticated pentesting is the most thorough way to test an app since we can also test features hidden behind a login page.) |  |
| If you chose an Authenticated pentest, please send test credentials so we can take a look inside. | Don’t write them here. Send them via a separate, encrypted channel. |

|  |  |
| --- | --- |
| Mobile Application Penetration Test Test your custom-built mobile application for security vulnerabilities.  The easiest way to scope a mobile app is to have our consultants look at it. | |
| Is this app on Android, iOS or both? |  |
| How can we get access to app (e.g. AppStore, TestFlight, custom apk file)? |  |
| Please send test credentials so we can take a look inside. | Don’t write them here. Send them via a separate, encrypted channel. |

|  |  |
| --- | --- |
| Phishing Campaign How aware are your staff of phishing attacks?  (Phishing is best discussed over a call, but some preliminary questions are below.) | |
| How many users are we targeting? |  |
| How many campaigns (rounds) are we performing? |  |

|  |  |
| --- | --- |
| Other Services We offer many more services that are best scoped over a short, 30-minute call. | |
| Bespoke Penetration Test | Find vulnerabilities in your bespoke system. |
| Red Team | Simulate an adversary targeting your organisation. Test your SOC and incident response playbooks. |
| Cloud Security Assessment | Check the configuration of your AWS, Azure or Microsoft 365 environment. |
| Security Review | Check the configuration of your Active Directory, Windows 10 SOE, Exchange and other products. |
| Vishing campaign | Phone-based social engineering to test the security awareness of your staff. |
| SMishing campaign | SMS-based social engineering to test the security awareness of your staff. |
| USB Drops | Test the security awareness of your staff against malicious USB flash drives. |
| Physical Intrusion | Test your physical security controls against attacks. |
| Governance, Risk & Compliance | Security strategy, execute education and gap analysis services check your security governance against NIST, ISO 27001, ACSC Essential 8 and more. |