Penetration Testing Service Definition.

Prepared for: **G Cloud 14**
Version: **1.0**
Date: **02/05/2024**

Penetration Testing Services

Illume offer several different types of penetration testing, namely external testing, internal testing, and web application testing. To provide an accurate price and to ensure compliance with UK law, a small questionnaire is required to be completed, followed by a scoping document.

External Penetration Testing

Illume penetration testers will conduct testing against external internet facing infrastructure. As with all testing, it is difficult to provide an exhaustive list of the tests that will be performed, as every test is different and tailored to the environment being tested. Nevertheless, the team will often conduct the following as standard;

- Using OSINT (Open Source Intelligence) to gain access to the network, through leaked credentials or metadata stored in documents etc.
- Social Engineering members of staff to obtain credentials, through phishing emails or phone phishing if required.
- Vulnerability assessment of the external network
- Manual analysis and the exploitation of any vulnerabilities identified, attempting to use any credentials captured previously on portals etc.

The Illume testing team will be available throughout the test if there are any questions or queries.

Deliverables

- Interactive report via the Illume portal containing an executive summary, route to exploitation (The steps taken by the testing team to gain access), notable findings and vulnerability overview
- Tips and recommendations as to remediate the identified vulnerabilities and secure the organisation from malicious threat actors
- Aftercare and support are available to answer any questions arising from the test or the report

Internal Penetration Testing

Following a completed scoping call, Illume penetration testers will perform the testing in one of two ways; either by a site visit, with the testers conducting the testing locally or by a remote VPN device. Depending on the scope, the team will often conduct the following, but are not limited to;

- Using OSINT (Open Source Intelligence) to gain access to the network, through leaked credentials or metadata stored in documents etc.
- Social Engineering members of staff to obtain credentials, through phishing emails or calling
- Unauthenticated vulnerability scan of the network, and manual exploitation of any vulnerabilities identified, such as
- User Enumeration
- Various methods for weak password identification
- Full password analysis, if sufficient access is gained to the network ❖ Access corporate network from guest network
- Leveraging credentials to identify any administrator level access across the network
- Accessing client machines, capturing video and desktop
- Gain access to confidential data, file servers etc. and searching for password documents
- Attempting to break the WiFi credentials

The Illume testing team will be available throughout the test if there are any questions or queries

Deliverables

- Interactive report via the Illume portal containing an executive summary, route to exploitation (The steps taken by the testing team to gain access), notable findings and vulnerability overview
- Tips and recommendations as to remediate the identified vulnerabilities and secure the organisation from malicious threat actors
- Aftercare and support are available to answer any questions arising from the test or the report

Web Application Penetration Testing

Web application testing of internet facing applications is conducted remotely. The size and complexity of a Web Application test can vary depending on the technology in use, thus the testing team may request credentials/access to the site prior to providing a quote. The testing team will often test for the following;

- Testing aligned with OWASP.
- Testing of authentication mechanisms
- Permission privileges, testing for IDOR etc.
- Data input validation and sanitisation, SQL Injection, Cross-site Scripting (XSS)
- Path traversal
- System enumeration
- Configuration file identification and analysis

The Illume testing team will be available throughout the test if there are any questions or queries.

Deliverables

- Interactive report via the Illume portal containing an executive summary, route to exploitation (The steps taken by the testing team to gain access), notable findings and vulnerability overview
- Tips and recommendations as to remediate the identified vulnerabilities and secure the organisation from malicious threat actors
- Aftercare and support are available to answer any questions arising from the test or the report