IT COMPANY
IT SERVICES & SOLUTIONS

CERTIFIED ISO 27001 Information Security

PENETRATION TESTING

Questionnaire

Scoping Questionnaire for Penetration Testing

BACKGROUND INFORMATION

1. What are the business requirements for this penetration test? For example, is the driver for this to comply with an audit requirement, or are you seeking to proactively evaluate the security in your environment?

- ◯ This is required by a regulatory audit or standard?
- ◯ A proactive internal decision to determine all weaknesses?

2. Will you also conduct a white box pen test or black box test or BOTH?*

- ◯ A white box pentest
- ◯ A black box pentest
- ◯ Need both

**Please Note: [White Box can be best described as a test where specific information has been provided in order to focus the effort. This tests the threat of internal attacks, say originating from people who have access to your network and know a lot about the services, ports, apps, servers etc.*
Black Box can be best described as a test where no information is provided by the client and the approach is left entirely to the pen tester (analyst) to determine a means for exploitation – This helps you understand the threat of external attacks]?

3. How many IP addresses and/or applications are included as in-scope for this testing? Please list them, including multiple sites, DNS etc. * In case you need a white box pen test, provide the following:

IP address range (Internal & External).

Few of the staff's email addresses, usernames and domain read-only access for assessing the level of security scan.

4. What are the objectives?

- [ ] Mitigating the all vulnerabilities
- [ ] Review all vulnerabilities impacted by CVEs
- [ ] Actual exploitation of vulnerabilities in a network, system, or application
- [ ] Obtain privileged access; exploit buffer overflows, SQL injection attacks, etc. The level of test would carry out the exploitation of weaknesses and can impact system availability

*Select all objectives that apply

5. What is the "target" of the Penetration test? Is it

- ◯ An Application
- ◯ A Website
- ◯ A network
- ◯ Application and networking
- ◯ Wireless
- ◯ Others (Please explain)

6. Do you also want the following tests to be performed?
Social Engineering test – to gain sensitive information from one or more of your employees (to infer or solicit sensitive information)
Please explain fully:

7. Will this testing be done on a production environment?

**You need to understand that certain exploitation of vulnerabilities to determine and/or prove a weakness could crash your system or cause it to reboot.*
Company is not liable for downtime caused by proving the system's weakness to attack

8. If production environments must not be affected, does a similar environment (development and/or test systems) exist that can be used to conduct the pen test?*

9. Are the business owners aware of this pen test?

Are key stakeholders (business owners) aware that the nature of a pen test is to attack the system as a hacker (or hostile actor) would, in order to learn and prove the system's weakness?
In addition to identifying vulnerabilities, if found, we will attempt to exploit them and then show you the results.

10. At what time do you want these tests to be performed?

- ◯ During business hours
- ◯ After business hours
- ◯ Weekend hour
- ◯ During the system maintenance window
- ◯ Anytime, please explain fully
- ◯ Others, please explain

11. Who is the technical point of contact?

Name

Email Address

Phone Number

12. Additional Information

13. Consent Letter:

Please provide a formal consent letter on business letterhead, approved by an authorized person, for the penetration test, the duration, and the date and time of the test.

Thank you for taking the time to fill this questionnaire. Please submit this questionnaire to support@itcompany.services