FINNISH CYBER SECURITY CONSULTING

QUESTIONNAIRE

General Information

To be filled

Name of the Customer

Related department

Related Department of the Customer

Certification, checking the level of security, or other

Project goals

Name *Phone, mail, messenger*

Contact person

Comments

Will employees be notified of penetration testing?

☐ Yes

☐ No

Comments

Do you plan to check the response of Information Security employees to the testing process

☐ Yes

☐ No

Number of calendar days *Before DD.MM.YYYY*

Maximum testing period

No / Yes, dated DD.MM.YYYY

Have there been previous security audits and penetration tests? If yes, when ? Please provide the results

---

Is translation required ☐ Yes ☐ No

Types of testing

☐ **External Infrastructure Penetration Testing**

☐ **Internal Penetration Testing**

☐ **Wireless Penetration Testing**

☐ **Web application penetration testing**

☐ **Mobile application penetration testing**

FCSC
FINNISH CYBER SECURITY CONSULTING

EXTERNAL INFRASTRUCTURE PENETRATION TESTING

What type of testing is required?

Please choose only one option

☐ BlackBox ☐ GrayBox ☐ WhiteBox

Blackbox: testing is carried out with almost no information about the company's infrastructure. Only its name and some details about the customer are communicated to the penetration testers.

Graybox: penetration testers receive a list of IP addresses to be tested and also some general information about the targeted infrastructure.

Whitebox: penetration testers receive all the necessary data about the company's infrastructure, the existing defense systems, the type of hardware and software equipments used, etc. When dealing with a web or a mobile application, the source code of these applications can also be provided to the penetration testers for a complete audit (automated and manual review).

Is exploitation of vulnerabilities allowed?

Please choose only one option

☐ Yes

☐ Yes, but in a limited way (the exploitation of each vulnerability is to be agreed on with the customer).

☐ No exploitation is allowed (this option will not be considered as a full penetration test but will consist in a preliminary vulnerability assessment).

If you answered «no» to the previous question, please fill in the vulnerability assessement scoping questionnaire:

How many web applications do you need to scan?
Please state if all machines are hosted externally

How many IP addresses do you need to scan?
Please state if all applications are hosted externally

Is DoS (Denial of Service) testing authorized? ☐ Yes ☐ No

Are social engineering attacks authorized? ☐ Yes ☐ No

Do you wish to mention any additional information or particularities we should be aware of?

FCSC
FINNISH CYBER SECURITY CONSULTING

SOCIAL ENGINEERING

Social engineering is a type of attack that is specifically aimed at your employees (through SMS, email, phone call, etc) in order to obtain useful information (such as credentials) which will eventually help attackers compromise your infrastructure. We really encourage you to opt for social engineering testing if you want your penetration testing to be as realistic and efficient as possible. In the recent years, social engineering accounts for more than 90% of cyberattacks around the world.

Fill in this specific form only if you opted for social engineering in one of the aforementioned testings.

Would you want to test social engineering scenarios through phishing simulation?	☐ Yes ☐ No
If yes, please specify if users can be phished using fake website or through sending malicious files?	
Would you want to test your employee awareness through physical intrusion simulation?	☐ Yes ☐ No
If yes, how many physical sites are to be tested?	
Would you want to test your employee awareness through phone calls simulation?	☐ Yes ☐ No
How many employees do you wish to target?	

FCSC
FINNISH CYBER SECURITY CONSULTING

INTERNAL PENETRATION TESTING

Please choose only one option

What type of testing is required? ☐ BlackBox ☐ GrayBox ☐ WhiteBox

How many physical locations are there?

How many servers are to be tested in each physical location?

Are all physical sites accessible from a single network location?

Please list the internal IP addresses of the servers you would like to be tested

☐ Yes (specify)

Are there any IP addresses that are specifically out of scope? (please specify)

☐ No

How many workstations are there in each physical location? (PC, laptop, virtual machine)

How many other network equipment are there in each physical location? (e.g. printers, MFPs, etc)

Is remote access to be provided ? ☐ Yes ☐ No

Do you wish to mention any additional information or particularities we should be aware of?

WIRELESS PENETRATION TESTING

Names of Wireless SSID(s)

How many physical sites are there?

Type of Wireless Access (e.g. captive portal, portal access, enterprise access)

Will enumeration of rogue access points be necessary? ☐ Yes ☐ No

Will the team be assessing wireless attacks against clients? ☐ Yes ☐ No

If you answered «yes» to the previous questions, how many clients will be using wireless access at the time of the assessment?

Do you wish to mention any additional information or particularities we should be aware of?

FCSC
FINNISH CYBER SECURITY CONSULTING

WEB APPLICATION PENETRATION TESTING

What type of testing is required? *Please choose only one option*

☐ BlackBox ☐ GrayBox ☐ WhiteBox

Is exploitation of vulnerabilities allowed?
Please choose only one option

☐ Yes

☐ Yes, but in a limited way (the exploitation of each vulnerability is to be agreed on with the customer).

☐ No exploitation is allowed (this option will not be considered as a full penetration test but will consist in a preliminary vulnerability assessment).

If you answered «no» to the 2nd question:

How many web applications do you need to scan?

Please state if all applications are hosted externally

Number of Static Pages

Number of Dynamic Pages

Is there a login function? ☐ Yes ☐ No

Is there a payment function? ☐ Yes ☐ No

If you answered «yes» to the previous question, are card payments taken and stored on-site or is this controlled by a third party? *Please specify*

Do the IP addresses associated to the web application belong to your own infrastructure or are they hosted externally?

☐ They are hosted in our own infrastructure.

☐ They are hosted externally.

For applications accessible only from the internal network, will you be providing VPN access? ☐ Yes ☐ No

Do you wish to mention any additional information or particularities we should be aware of?

*CODE REVIEW

Source code auditing is the most comprehensive service that can be applied to a given application: it can exhaustively detect the vulnerabilities affecting an application by reviewing the source code.

Fill in this part only if you opted for whitebox web application penetration testing.

How many lines of code are there?

What code languages are used?

What are the Third Party / Open Source components used in the application?

Would there be a test environment available? ☐ Yes ☐ No

Would the design documents be available? ☐ Yes ☐ No

FCSC
FINNISH CYBER SECURITY CONSULTING

MOBILE APPLICATION PENETRATION TESTING

What type of testing is required? *Please choose only one option*

☐ BlackBox ☐ GrayBox ☐ WhiteBox

Blackbox: testing is carried out with almost no information about the company's infrastructure. Only its name and some details about the customer are communicated to the penetration testers.

Graybox: penetration testers receive a list of IP addresses to be tested and also some general information about the targeted infrastructure.

Whitebox: penetration testers receive all the necessary data about the company's infrastructure, the existing defense systems, the type of hardware and software equipments used, etc. When dealing with a web or a mobile application, the source code of these applications can also be provided to the penetration testers for a complete audit (automated and manual review).

Please provide us with the name(s) of the mobile application(s) and the link(s) to download it/them

What is/are the functions (brief explanation) of each application?

Is it possible to get an application build without pinging/obfuscation? ☐ Yes ☐ No

*CODE REVIEW

Source code auditing is the most comprehensive service that can be applied to a given application: it can exhaustively detect the vulnerabilities affecting an application by reviewing the source code.

Fill in this part only if you opted for whitebox web application penetration testing.

How many lines of code are there?

What code languages are used?

What are the Third Party / Open Source components used in the application?

Would there be a test environment available? ☐ Yes ☐ No

Would the design documents be available? ☐ Yes ☐ No