**Penetration Testing Questionnaire**

**Contents**

[**Introduction** 2](#_Toc128407162)

[**What is this questionnaire?** 2](#_Toc128407163)

[**Internal Infrastructure / External Infrastructure Testing** 3](#_Toc128407164)

[**Web Application Testing** 5](#_Toc128407165)

[**Mobile Application Testing** 7](#_Toc128407166)

# **Introduction**

Thank you for taking an interest in using CyBEARSec, please fill this questionnaire out to the best of your abilities, if you have any questions or require more information regarding anything then please get in contact with us.

# **What is this questionnaire?**

Great question, this questionnaire is used to collect information about your systems and setup. From the information that you provide in this questionnaire it will allow us to provide a much more accurate estimation on the total price of the testing, so please be as detailed as possible.

If you have anything you wish to have tested that falls outside of the categories below, then please get in contact with us and we can discuss this more in detail and provide you with a quote estimate.

# **Internal Infrastructure / External** **Infrastructure Testing**

|  |  |  |
| --- | --- | --- |
| Question | Answer | Description |
| What type of testing is required? | - Black Box  - White Box  - Grey box | **Black Box** – Purely just giving us your IP address and/or domain name.  **White Box** – Provide us with IP addresses, domain names, whitelisting on firewalls and any other defensive systems, Architectural network plan provided.  **Grey Box** – A mixture of both Black and White box testing. |
| What type of infrastructure testing is required? | - External Infrastructure  - Internal Infrastructure  - Both  - Other (Please specify) | If ‘Other’ Explain here… |
| What services are expected to be exposed? | Type answer here… | Would we see management ports like SSH and RDP or possibly OWA (Outlook Web Access). |
| \* How many IP addresses / Domain names are there to be tested? |  | This can be an estimate of the number of targets to put into scope. |
| Any special testing conditions we should be made aware of? |  | Time of day for testing, Internal Applications might require VPN access. |
| Are there any deadlines or timeframes that we need to be made aware of? |  | Please specify in days/weeks if there are any deadlines. |

*All Questions marked with a* ***\**** *are required.*

# **Web Application Testing**

|  |  |  |
| --- | --- | --- |
| Question | Answer | Description |
| What type of testing is required? | - Black Box  - White Box  - Grey box | **Black Box** – Purely just giving us your IP address and/or domain name.  **White Box** – Provide us with usernames and passwords to authenticate, Directory listing provided, Whitelisting on any WAF in place.  **Grey Box** – A mixture of both Black and White box testing. Only URLs and credentials provided. |
| What services are expected? | Type answer here… | Apache, PHP, Django? |
| \* How many different types of users / groups exist in the application? | Type answer here… | Administrators, clients, customers, editors, authors etc. |
| \* How many URLs are there to be tested? | Type answer here… | Please list all URLs to be tested. |
| \* Are there any subdomains, are they included in the testing? | Type answer here… | Subdomains are like the following:  Login.example.com  Api.example.com |
| \* How many user input fields are there throughout the application? | Type answer here… | These are fields that a user of the application can input data, such as a form that asks the user to input details about themselves (name, address, email). |
| Are there any API Services that need testing?  - Yes  - No | Please Provide any information… | We will ask for the API documentation, POSTMAN files, and any authentication mechanisms. |
| Any special testing conditions we should be made aware of? |  | Time of day for testing, Internal Applications might require VPN access. |
| Are there any deadlines or timeframes that we need to be made aware of? |  | Please specify in days/weeks if there are any deadlines. |

*All Questions marked with a* ***\**** *are required.*

# **Mobile Application Testing**

|  |  |  |
| --- | --- | --- |
| Question | Answer | Description |
| What type of testing is required? | - Black Box  - White Box  - Grey box | **Black Box** – Purely just giving us the application name on the relevant mobile app store.  **White Box** – Provide us with APK and IPA packages that do not include SSL pinning. Credentials provided for the application testing.  **Grey Box** – A mixture of both Black and White box testing. |
| What services are expected to be exposed? | Type answer here… | Provide any details as to what services the application may expose. |
| \* What type of application is to be tested? | - iOS Application  - Android Application  - Both | This can be an estimate of the number of targets to put into scope. |
| Are there any API Services that the application makes use of?  - Yes  - No | Please Provide any information… | We will ask for the API documentation, POSTMAN files, and any authentication mechanisms. |
| Are there any credentials for the application? | - Yes  - No | Please provide any credentials in the authorisation form, this will be sent later. |
| Any special testing conditions we should be made aware of? |  | Time of day for testing, Internal Applications might require VPN access. |
| Are there any deadlines or timeframes that we need to be made aware of? |  | Please specify in days/weeks if there are any deadlines. |

*All Questions marked with a* ***\**** *are required.*

# **Wi-Fi Assessments**

|  |  |  |
| --- | --- | --- |
| Question | Answer | Description |
| What type of frequencies are used? | - 2.4 GHz  - 5 GHz  - 6 GHz |  |
| What are the SSID names? | Type answer here… | Wi-Fi names people connect too. |
| \* Authentication Mechanisms? | Type answer here… | e.g., open, WEP, WPA, WPA2, etc. |
| \* What is the target audience for the Wi-Fi? | Type answer here… | Internal employees, guests, customers. |
| \* How is the Wi-Fi managed? | Type answer here… | Central management application. |

*All Questions marked with a* ***\**** *are required.*

For Wi-Fi assessments to be done remotely, a device called a Wi-Fi Pineapple would be configured and sent out to you (the client). This device would then need to be plugged in to a power source AND an ethernet cable with public internet access.

The Wi-Fi Pineapple then connects back to a Command & Control (C2) server that we can use to issue commands back down to the Wi-Fi Pineapple device to perform actions like, scan the area for available SSID’s, perform deauthentication attacks etc.