Clark Nuber PS

PENETRATION TESTING SCOPING QUESTIONNAIRE

The intent of this form is to gather initial information about your technology infrastructure and testing intent so that we can properly plan a penetration test / security exercise. Our services will safely evaluate the security of your resources against attacks from a malicious source. Based on our findings, we recommend methods to bolster and prevent such attacks from occurring. **All information provided in this form is strictly confidential.** Send completed forms to Steve Vasconcellos at svasconcellos@clarknuber.com.

1. **WEBSITE** FOR YOUR ORGANIZATION:

2. DO YOU WANT AN **EXTERNAL PENTRATION TEST**? ☐ YES

How many **estimated** live internet-exposed resources are in-scope, such as servers, VPN gateways, websites, and firewalls?

Explanation: Our team of ethical hackers will simulate an attack from an external perspective, assessing the security of your internet-exposed resources and recommending methods to further harden your network.

3. DO YOU WANT AN **INTERNAL NETWORK PENETRATION TEST**? ☐ YES

How many **estimated** internal hosts are in-scope, such as computers and servers?

Explanation: Via a secure remote connection device, our team of ethical hackers will simulate an attack from the perspective of an attacker who has gained access to your internal network, such as via a phishing attack or a malicious insider, assessing your security and recommending methods to further harden your network.

4. DO YOU WANT A **WIRELESS NETWORK PENETRATION TEST**? ☐ YES

How many wireless networks are in-scope for testing?

Can all wireless networks be reached from one location?

If not, how many locations need testing?

Explanation: Via a secure remote connection device, our team of ethical hackers will simulate an attack from the perspective of an attacker who is in-range of your wireless networks, assessing your security and recommending methods to further harden your network(s).

5. DO YOU WANT A **WEB APPLICATION PENETRATION TEST**? ☐ YES

How many web applications are in-scope for testing?

Please list the URL for each in-scope web application:

How many sets of credentials are to be tested for each application?

How many **estimated** dynamic pages does each application contain?

Are there calls to your own API(s) made by the application(s) that are in-scope for testing?

If so, how many **estimated** API calls are in-scope for each application?

Explanation: Our team of ethical hackers will assess the security of your web application from the perspective of an external attacker. In addition, with provided credentials, we will assess the security of the entire application from the perspective of an authenticated user. We will review various attack threats, such as the OWASP Top Ten Security Vulnerabilities, and recommend methods to further harden your application. If your application architecture utilizes your own APIs that are called by the application, please indicate the total number of calls so we can assess each for security issues.

6. DO YOU WANT **PHISHING / SOCIAL ENGINEERING** WORK PERFORMED? ☐ YES

Do you want us to perform **Email Phishing**, where we send various phishing emails to your users?

If so, how many **estimated** users are to be tested?

Explanation: Our team of ethical hackers will send various levels of phishing emails to your users, attempting to trick them to violate security policies, such as visiting a pseudo-malicious website or revealing sensitive information. We can either mine the internet for email addresses, as a malicious attacker would, or be provided a list to ensure complete coverage.

Do you want us to perform SMS Phishing, where we send phishing text messages to your users?

If so, how many **estimated** users are to be tested?

Explanation: Our team of ethical hackers will send phishing text messages to your users, attempting to trick them to violate security policies, such as visiting a pseudo-malicious website or revealing sensitive information. You will need to provide us with a list of authorized numbers.

Do you want us to perform **Phone Phishing**, where we call your users/numbers and attempt to elicit sensitive information?

If so, how many **estimated** users are to be tested?

Explanation: Our team of ethical hackers will call your users, with both live phone calls and automated calls, attempting to trick them to violate security policies, such as revealing passwords and sensitive information. We can either call numbers we discover via reconnaissance, as a malicious attacker would, or be provided a list to ensure complete coverage.

Do you want us to perform **On-Site Social Engineering**, where we visit your facility/office and attempt to bypass security measures and gain access to the facility and/or internal network?

If so, please list each location to be tested:

Explanation: A member of our team of ethical hackers will visit your location(s) and attempt to bypass security measures and gain access to the facility and/or internal network, such as using social engineering techniques to get staff to allow us to gain access to unauthorized areas.

7. ARE THERE ANY **ADDITIONAL NOTES**, CONCERNS, OR PARAMETERS THAT NEED TO BE CONSIDERED?