

**SCOPING QUESTIONNAIRE FOR PENETRATION TESTING**

PathMaker Group adheres to the OSSTMM penetration testing methodology and code of ethics regarding this level and classification of test. The analysts performing these tests will each be certified security practitioners holding at least one certification of Certified Information Systems Security Professional (CISSP).



Penetration tests can range in a number of varieties from testing one application based on known vulnerabilities to far-reaching tests where no vulnerability information is provided and every system and network is in-scope. Additionally, a penetration can go as far as to gain control of the system by any means (aggressive) or to simply illustrate that it “could” be done by “taking these next steps”, without actually taking the steps.

The following questions are intended to determine and refine the scope and extent of a desired penetration test. This template should be reviewed by our client and answered as thoroughly as possible. In the event that the client is not able to answer these questions, it is recommended that a PathMaker Group security practitioner review each question with the client to ensure adequate information is obtained.

United States laws require that PathMaker Group obtain written permission by an authorized representative of the client to perform a penetration/security assessment. Please reference Appendix A entitled, Security Testing and Penetration Testing Authorization Agreement.

#	QUESTIONS	ANSWER	COMMENTS
1)	<p>What is the business requirement for this penetration test?</p> <ol style="list-style-type: none"> <li>1. This is required by a regulatory audit or standard?</li> <li>2. Proactive internal decision to determine all weaknesses?</li> </ol> <p>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?</p>		
2)	<p>Will this be a <u>white box test</u> or a <u>black box test</u>?</p> <p><b>White Box</b> can be best described as a test where specific information has been provided in order to focus the effort.</p> <p><b>Black Box</b> can be best described as a test where no information is provided by the client and the approach is left entirely to the penetration tester (analyst) to determine a means for exploitation.</p>		

#	QUESTIONS	ANSWER	COMMENTS
3)	How many IP addresses and/or applications are included as in-scope for this testing? Please list them, including multiple sites, etc.		
4)	What are the objectives? a.) Map out vulnerabilities b.) Demonstrate that the vulnerabilities exist c.) Test the Incidence Response d.) Actual exploitation of a vulnerability in a network, system, or application. Obtain privileged access, exploit buffer overflows, SQL injection attacks, etc. This level of test would carry out the exploitation of a weakness and can impact system availability. e.) All of the above		
5)	What is the "target" of the Penetration test? Is it; a.) An Application b.) A Website c.) A Network d.) Application and Network e.) Wireless f.) Other, please explain		
6)	Do you also want the following tests to be performed? a.) Physical security test – to gain access to physical space by evading physical security controls b.) Social Engineering test – to gain sensitive information from one or more of your employees (to infer or solicit sensitive information)		

#	QUESTIONS	ANSWER	COMMENTS
7)	<p>What protocol should be followed for alerting on vulnerabilities found?</p> <ul style="list-style-type: none"> <li>a.) Wait until the end of the testing to report all vulnerabilities</li> <li>b.) Report vulnerabilities as we find them</li> <li>c.) Daily report on the status of the testing</li> <li>d.) Report only critical findings immediately</li> </ul>		
8)	<p>Will this testing be done on a production environment?</p> <p>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. PathMaker Group is not liable for downtime caused by proving the system's weakness to attack.</p>		
9)	<p>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?</p>		
10)	<p>Are the business owners aware of this pen test?</p> <p>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?</p>		

#	QUESTIONS	ANSWER	COMMENTS
11)	At what time do you want these tests to be performed? a.) During business hours b.) After business hours c.) Weekend hours d.) During system maintenance window		
12)	Who is the technical point of contact, assuming this is not a covert (black box) test of the incident response function?  Name: Cellular phone number (available during this project)  Alternate Name: Cellular phone number (available during this project)		
13)	Additional Information?		

**APPENDIX A – SECURITY TESTING AND PENETRATION TESTING AUTHORIZATION AGREEMENT**

## **Security Testing and Penetration Testing Authorization Agreement**

To authorize technical security assessment or penetration testing, please complete this form and fax to:

PathMaker Group  
Information Security Services  
Facsimile: 817-685-7980

<b>Contact and Scope Definitions</b>
--------------------------------------

Client/Company Name: *(please print)* \_\_\_\_\_

Technical Contact Name: \_\_\_\_\_

Technical Contact Telephone: \_\_\_\_\_

Technical Contact E-mail: \_\_\_\_\_

IP Addresses / Ranges to be tested: *(please identify internal or external addresses)*

---

---

---

---

---

Domain Name(s): \_\_\_\_\_

Requested Date and Time of Assessment(s): \_\_\_\_\_

---

Please *initial* each of the boxes indicating your acceptance of the following statements:

- [ \_\_\_\_\_ ] I am authorized to authorize PathMaker Group to test the IP address(s) listed herein and hereby permit PathMaker Group's representatives to perform penetration testing of said IP address(s).
  
- [ \_\_\_\_\_ ] I have been informed and understand that testing of this nature may or may not impact the uptime of the network and/or the hardware being tested. I have been informed of options for scheduling testing to be run at hours convenient to my business, allowing me to limit the impact of events that could occur.

**Client Authorizing Name and Signature (required)**

→ {  
Authorized Name: *(please print)* \_\_\_\_\_  
Authorized Signature: \_\_\_\_\_  
Date: \_\_\_\_\_