Black Box Questionnaire: ***Form 1***
Scoping Questionnaire for Black Box (External) Penetration Testing

Cyber criminals are on the rise. And no one is safe, however secure you feel your network is. The bad guys have the time and resources to keep prowling the internet for the next prey. If you use computers, laptops, mobile devices, and the Internet you could already be losing something without your knowledge.

You need to undertake a penetration test of your network to assess the threats of loss of your intellectual property, very confidential client data and details and business secrets.

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

Uganda laws require that Summit Consulting obtain written permission by an authorized representative of the client to perform a penetration/security assessment. You will be expected to provide a written consent letter on company headed paper and stamped with the company seal/stamp authorizing for the penetration test to take place.

#	Question	Your Answer	Your Comments
1	What is the business requirement for this penetration test? 1. This is required by a regulatory audit or standard? 2. Proactive internal decision to determine all weaknesses? 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?		
2	Will you also conduct a white box pen test or black box test or 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, etc running *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 penetration 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, etc. In case you need a white box pen test, provide the following:		

#	Question	Your Answer	Your Comments
	1. IP address range (Internal & External). 2. Few of the staff's email addresses & their names for assessing level of security awareness.		
4	What are the objectives? 1. *Map out vulnerabilities* 2. *Demonstrate that the vulnerabilities exist* *Test the Incidence Response* 3. *Actual exploitation of vulnerability in a network, system, or application.* 4. *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.* 5. *All of the above*		
5	What is the "target" of the Penetration test? Is it; 1. An Application 2. A Website 3. A Network 4. Application and Network 5. Wireless 6. Other, please explain 7. All of the above – please specify		
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. Summit Consulting is not liable for downtime caused		

#	Question	Your Answer	Your Comments
	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? 1. During business hours 2. After business hours 3. Weekend hours 4. During system maintenance window 5. Anytime, please explain fully		
11	Who is the technical point of contact, assuming this is not a covert (black box) test of the incident response function? 1. Names: 2. Tel: 3. Mobile: 4. Email:		
13	Provide a dated written consent letter on company headed paper and stamped with the company seal/stamp authorizing for the penetration test to take place and showing duration of test		
14	Additional information?		