JUNIOR PENETRATION TESTER

LETTER OF ENGAGEMENT V1.1

1. Exam Configuration and Tests

Before you start your Penetration Testing exam process, make sure you have your environment properly configured. Once you are connected through the VPN please test your connection to the exam environment by pinging the following IP address: 192.168.193.211.

If the host replies, you can start your Penetration Test.

2. Scope of Engagement

You need to perform an onsite Black Box Penetration Test against the web applications and networks of the organization named **Motville**.

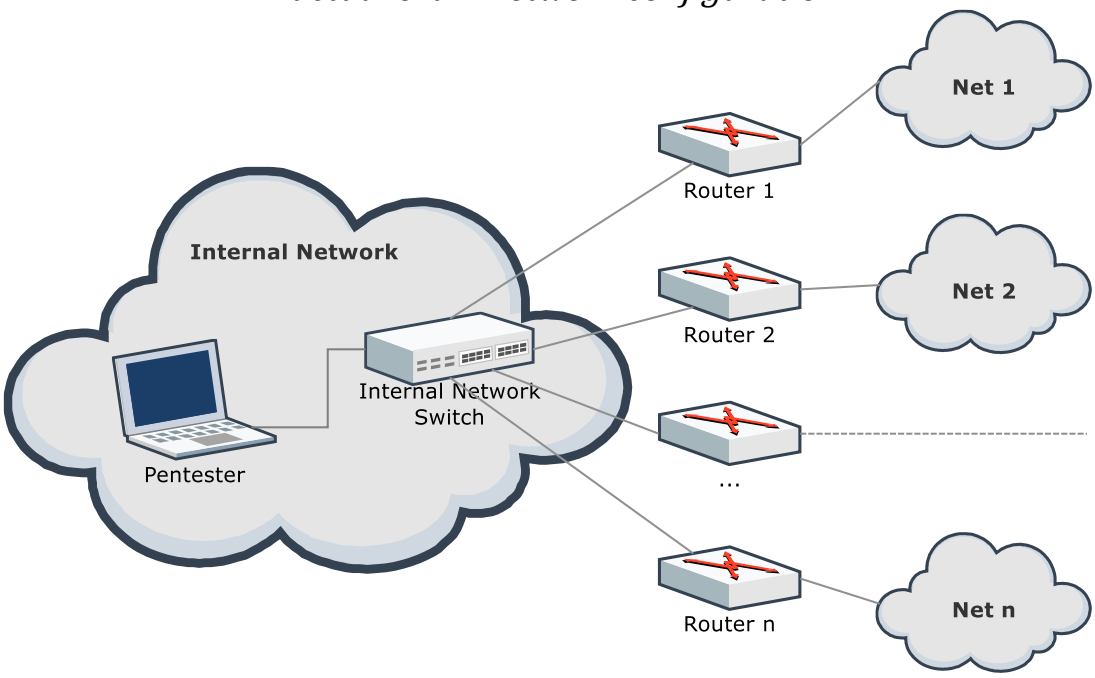
This is what the client organization defined as **scope** of the tests:

- The network you will be connected to
- Any other network you will be able to reach

The network contains production services so you are allowed to run brute force login attacks and vulnerability scanners **on hosts connected to the internal network only (to avoid Denial of Service on production services).**

You will be **directly connected to Motville internal network**. Your machine will automatically receive an IP address. You will not receive routing information (routes).

Please note that the following diagram is a guideline and does not reflect the actual exam network configuration.



From the internal network it is possible to reach some other networks. All the networks are /24 networks. You have to find the routing information and the network addresses on your own by analyzing the traffic capture you can find in the compressed archive containing this letter of engagement.

In the file, you can also find two dictionaries of common usernames and passwords, should you have to perform a brute force attack.

3. Exam objectives

Please note that you are required to perform a penetration test on all the hosts in scope. The questions in the test area will cover most of your findings. You can freely choose if you want to answer the questions during the penetration test or after completing it.

Keep in mind that both the quiz area and the exam scenario in Hera Lab will be accessible at the same time, for three (3) days.

You have to correctly answer at least 15 questions to pass.

4. Recommended tools

You are free to use any environment to perform your penetration test. The following is a suggested list of tools that might be useful during the exam:

- Kali Linux / Backtrack / Pentoo / Backbox…
- Burp Suite
- Nessus
- Metasploit
- Nmap
- Hydra

Please note that you will need the OpenVPN client in order to connect to the exam environment. This comes pre-installed in Kali Linux and other Linux distributions.

5. Hints for the best outcome

- Do not think about the exam as a "Capture the Flag." It is not.
- Keep track of all of your actions, commands, discovered hosts, etc. while you perform your tests. Another great idea is to answer the questions while you proceed with your Penetration Test. (Carefully read the question, then perform your tests in the lab)
- Any attack, tool or technique, according to the rules of engagement, is allowed during the exam.

GOOD LUCK!