# eJPT

Letter Of Engagement - V1.0

## Exam Configuration

The eJPT Exam environment is an in-browser lab environment that provides you with access to a pre-configured Kali Linux system with all tools, scripts and wordlists required to successfully answer and complete the questions/challenges associated with the exam.

The in-browser lab architecture ensures that you can begin, progress and complete the exam from any device from any location with a stable internet connection and without the need to set up your own Virtual Machines.

The Kali Linux system provided to you during the exam doesn't have an internet connection, as a result, you can utilize your host operating system's browser for research.

Furthermore, all required exploit modules and exploit code are accessible on the Kali Linux system via the Metasploit Framework and the Exploit Database (Exploit-DB).

**NOTE: You do not need to download or install any custom scripts or tools on to the in-browser Kali Linux system you have been provided access to. The Kali Linux system has everything you need to successfully complete the exam.**

## Scope Of Engagement

You have been hired to perform an onsite Black Box Penetration Test against the hosts,

web applications and networks of an organization named **Syntex Dynamics**.

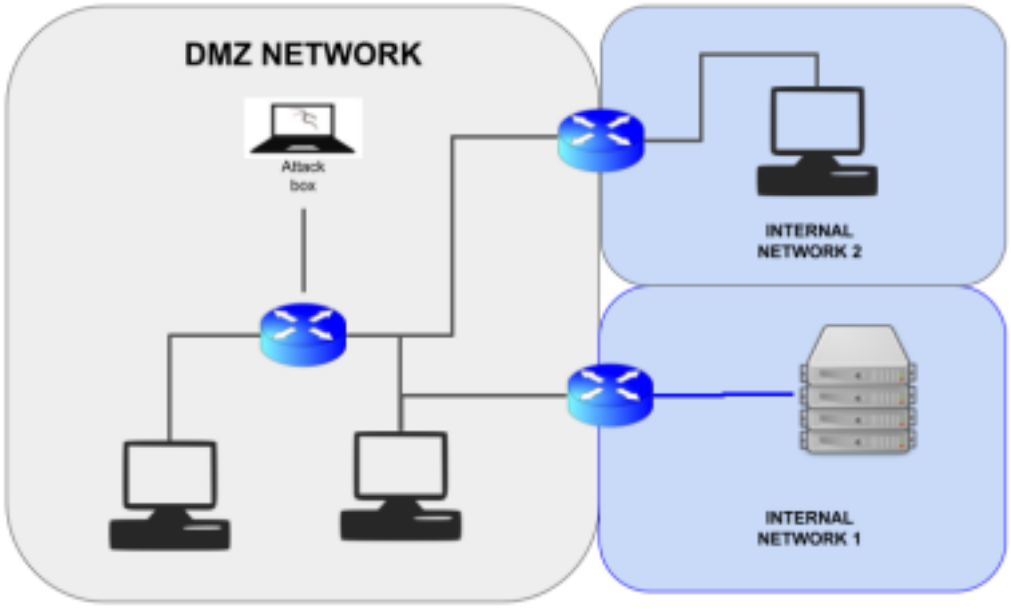
This is what the client organization has defined as the scope of the tests:

- The DMZ network you will be connected to.
- Any other internal network you will be able to reach/access.

When you first initiate your exam lab environment, you will automatically be connected to the DMZ network, this network contains production servers and web applications that you can potentially gain access to via brute-force attacks and via the exploitation of misconfigurations or vulnerabilities.

You are also required to identify any internal networks, pivot into them, identify hosts within these internal network/networks and gain access to these systems.

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




From the DMZ network it is possible to reach some other internal networks/network. All the networks are /24 networks. You have to find the routing information and the network addresses by identifying a pivot point that interconnects the two networks.

The Kali Linux system contains all the dictionaries of common usernames and passwords,

should you have to perform a brute force attack.

# 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 eJPT findings. You can freely choose how and in what order you want to answer the questions during the penetration test.

Keep in mind that both the quiz area and the exam lab environment will be accessible simultaneously for the entire period of the exam (48 Hours).

# 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:

- Nmap
- Dirb
- Nikto
- WPScan
- CrackMapExec
- The Metasploit Framework
- Searchsploit
- Hydra

Please note that all of the aforementioned tools come pre-installed on the Kali Linux system provided to you.

# Hints For A Successful Penetration Test

- Do not think about the exam as a “Capture the Flag.” It is not.
- Refer to the Lab Guidelines document provided to you along with this document for information on how the in-browser lab works.
- Take notes and save your findings on an external note-taking application on your host operating system. (This is because any data you store on the Kali Linux system will be deleted if you reset your lab environment.
- 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.