eJPT v2 Syllabus Breakdown

1. Host and Network Penetration Testing (35%)

This is the most heavily weighted domain, focusing on the core skills of exploitation and lateral movement.

Exploitation:

- Identify and modify exploits for use in a target environment.
- Conduct exploitation using the Metasploit Framework.

Password Attacks:

- Conduct brute-force password attacks against services.
- Perform offline password hash cracking.

Pivoting:

- Demonstrate pivoting by adding a route to a new network segment.
- Demonstrate pivoting by using port forwarding to access services on other machines.

2. Assessment Methodologies (25%)

This domain covers the initial reconnaissance and information gathering phases of a penetration test.

Reconnaissance:

- Extract company information from public sources.
- Gather email addresses and technical information from public sources.

Scanning & Enumeration:

- Locate and identify endpoints on a network.
- Identify open ports and running services on a target.
- Identify the operating system of a target.

Vulnerability Identification:

- Identify vulnerabilities in discovered services.
- Evaluate the criticality and potential impact of identified vulnerabilities.

eJPT v2 Syllabus Breakdown

3. Host and Network Auditing (25%)

This domain focuses on the post-exploitation phase, detailing what to do after gaining initial access to a system.

Information Gathering (Post-Exploitation):

- Compile information from files found on a compromised target.
- Enumerate network information (e.g., other hosts, routes) from a compromised target.
- Enumerate system information (e.g., users, processes) on a compromised target.

Credential Gathering:

- Gather user account information on a target.
- Gather password hashes or cleartext passwords from a target.

File Transfers:

- Transfer files to and from a target machine.

4. Web Application Penetration Testing (15%)

This domain covers the fundamental skills required to assess web applications for common security flaws.

Web Reconnaissance:

- Conduct thorough web application reconnaissance.
- Locate and identify hidden files and directories.

Web Exploitation:

- Conduct brute-force login attacks against web authentication forms.
- Identify and exploit common web application vulnerabilities (e.g., XSS, SQLi, LFI).