eJPT Certification

Section: Penetration Testing

08/7/2020

Learning Objectives:

* Penetration testing general terms and conditions.
* How to approach a penetration testing engagement from legal and organizational standpoint.

**Lifecycle of a Penetration Test**

1. **Engagement** 
   1. Define fee for pentesting of network, web app or whole organization.
      1. Type of engagement
      2. How time-consuming the engagement is
      3. The complexity of the applications and services in scope
      4. Number of targets, i.e. IP addresses, domains, machines, etc.
   2. Submit proposal
      1. Proposal should keep in mind the client’s needs and infrastructure.
         1. Get requirements.
      2. Make it clear the your methodology you Intend to use along with what tools you’ll be using, testing, whether it’s remote or onsite, etc.
      3. Risks and benefits.
      4. Define the scope of the engagement.
   3. Stay in scope of the engagement
      1. Scope should be well defined prior to the start date of the project.
   4. Incident handling
      1. Refer to notes.
2. **Information Gathering**
   1. Information gathering starts after the legal paperwork is complete but before the testing period.
   2. General Information gathering
      1. Examples:
         1. Board of directors (names and emails)
         2. Investors (names and emails)
         3. Managers and employees (names and emails)
         4. Branch location and addresses
      2. The information just listed is extremely important and useful if social engineering is allowed by the rules of engagement, as you will be able to mount effective targeted attacks.
   3. Understanding the Business
      1. When performing penetration testing on a business it is critical to mimic the effects of a black hat hacker on a specific business.
         1. Understanding the business risks involved for the client is critical to a successful pentest.
   4. Infrastructure Information Gathering
      1. Here you begin to transform the IP addresses or the domains in scope into actionable information about servers, operating systems, and much more.
      2. The goal here is to give meaning to every IP address in scope by determining:
         1. If there is a live host or server using it.
         2. If there are one or more websites using that IP address.
         3. What OS is running on the host or the server.
      3. All of this will help us:
         1. .Focus our efforts to actual live clients and servers.
         2. Target your attacks.
         3. Sharpen your tools for the exploitation phase, when you have to find out the vulnerabilities and the exploitability of the client systems.
   5. Web Applications
      1. If there is a web application in scope, we must know:
         1. Domains
         2. Subdomains
         3. Pages (website crawling)
         4. Technologies in use like PHP, Java, .NET, etc.
         5. Frameworks and content management systems in use, like Drupal, Joomla, WordPress, and others.
      2. Treat web apps as complete separate entitles that require separate study.
3. **Footprinting and Scanning** 
   1. Deepen your knowledge of the in-scope servers and services.
   2. Fingerprinting the OS
      1. Provides information about host OS and helps narrow down the number of potential vulnerabilities to check for.
      2. Tools exists that make educated guesses on the OS version and even patch level of a remote server, making life easier for the pentester.
   3. Port Scanning
      1. Help you determine which ports are open on a remote system; this is crucial because any mistake made here will impact next steps.
      2. The go to port scanner is nmap, which will be taught later.
   4. Detecting Services
      1. Once the open port(s) is found next we must find out the service listening on that port.
         1. Admins can configure a service to listen to any TCP or UDP port.
         2. Nmap is a tool that can be used to ID services listening to ports.
      2. By understanding the services running on a machine, a penetration tster can infer;
         1. The OS.
         2. The purpose of a particular IP address: for example, if it is a server or client
         3. The importance of the host in the client’s business. For example, an e-commerce enterprise will heavily rely upon its website and database servers
4. **Vulnerability Assessment**
   1. Objective is to build a list of vulnerabilities present on the target systems.
   2. The penetester has to carry out a vulnerability assessment on each target found in the previous steps.
   3. Assessments can be conducted by manually using data collected in the previous steps or by utilizing automated tools.
      1. Vulnerability assessment tools are scanners that send probes to the target systems to detect whether a host has some well-known vulnerabilities.
      2. once the vulnerability scan is complete, the scanner will deliver a report to the pentester, which can then be used to drive exploitation in the next phase.
      3. It’s crucial to properly configure a vulnerability scanner.
5. **Exploitation**
   1. Exploit the vulnerabilities ID during the assessment.
   2. During the exploitation phase a pentester checks and validates a vulnerability and also widens an increases the pentester’s privileges on the target systems and networks.
   3. A penetration test is a cyclic process.
   4. The process ends when there are no more systems and services in-scope to exploit.
      1. Penetration tests are used to find any and all vulnerabilities.

A screenshot of a cell phone

Description automatically generated

1. **Reporting**
   1. The Report:
      1. The report must address:
         1. Techniques used
         2. Vulnerabilities found
         3. Exploits used
         4. Impact and risk analysis for each vulnerability
         5. Remediation tips
            1. Targeted tips on how to effectively remediate each vulnerability are the real value for the client.