CompTIA Security + 1.0 Threats,Attacks and Vulnerabilities

Filename: comptia-secplussy0501-1-4-penetration_testing_concepts
Title: Penetration Testing Concepts
Subtitle: CompTIA Security+ (SY0-501)

1.4 Penetration Testing Concepts

- 1.4 Explain penetration testing concepts.
  - Active reconnaissance
    - This infomation gathering involves port scanning
    - This infomation gathering involves getting around or through the firewall by exploitation
    - In this type of information gathering, activities can be traced
  - Passive reconnaissance
    - This is information gathering using Open Source Intelligence (OSINT) or only using public resources
    - Used when information gathering activities have a requirement to not be detected
    - Can be difficult to perform as sometimes the only information that is available could be archives or outdated information
    - There is also **semi-passive** is information that will look like the regular network traffic and behavior, like querying public DNS records, inspecting metadata in published documemts.
  - Pivot
    - Pivoting is the unique technique of using an instance (also referred to as a 'plant' or 'foothold') to be able to "move" around inside a network. Basically using the first compromise to allow and even aid in the compromise of other otherwise inaccessible systems
    - Pivoting is a powerful technique in the arsenal of a web application penetration tester (pen tester). Once a host has been compromised, the pen tester looks for information to plunder.
    - Information Plundering
      - Accounts
      - Password hashes
      - Knowledge of other systems
    - Techniques
      - Netcat Relays
      - SSH local Port forwarding
      - SSH Dynamic Port Forwarding
      - Nmap, Nikto, Burp Suite
  - Initial exploitation
    - The intial exploit trys to find loophole in an application to grant access to the system the application is running on through **escalation of priviledge**
    - Access is gained through:
      - Command Line Interpreters (terminals, shells, Windows Command Prompt, PowerShell)
      - Rogue code execution
      - Physical Access
      - Command injection
      - Phishing
  - Persistence
    - Persistence Penetration Testing A persistence is the approach taken by many real-world attackers. A malicious party does not limit their attack to a two week time period. Instead, they watch and wait, looking for an opening in which to strike. When one presents itself, they take action, after this initial attack is completed. After the attacker will continue to monitor the target network.
  - Escalation of privilege
  - Black box
    - Black Box Testing, also known as Behavioral Testing, is a software testing method in which the internal structure/ design/ implementation of the item being tested is not known to the tester. These tests can be functional or non-functional, though usually function
  - White box
    - White Box Testing (also known as Clear Box Testing, Open Box Testing, Glass Box Testing, Transparent Box Testing, Code-Based Testing or Structural Testing) is a software testing method in which the internal structure/ design/ implementation of the item being tested is known to the tester.
  - Gray box
    - Gray box testing, also called gray box analysis, is a strategy for software debugging(combination of white and black box testing) in which the tester has limited knowledge of the internal details of the program. A gray box is a device, program or system whose workings are partially understood.
  - Pen testing vs. vulnerability scanning
    - Vulnerability Scanning seeks to identify and quantify the vulnerabilities and provide mitigation techniques
    - Pentesting tries to simulate the actions and attacker can use against an organization in order to exploit weaknesses that are found. The pentest or attack simulation can orginate internally or inside of the organization. A pen-test can also be an externally simulated attack and last several weeks