2.1.2 Penetration Test Process and Types Facts

A penetration tester's job is extremely important. Computers and networks are constantly under attack. To combat these hackers, organizations hire penetration testers.

Penetration testing is the practice of finding vulnerabilities and risks with the purpose of securing a computer or network system. The terms penetration testing and ethical hacking are often used interchangeably. However, ethical hacking is an all-embracing term that includes all hacking methods. Penetration testing is a part of ethical hacking.

This lesson covers the following topics:

- Red team vs. blue team
- Ethical hacking methodology
- Penetration testing life cycle
- Penetration testing frameworks
- Penetration testing types

Red Team vs. Blue Team

Offensive security specialists are known as the red team, or ethical hackers. The defensive security specialists are known as the blue team.

Ethical Hacking Methodology

There are five phases in the ethical hacking methodology:

Phase	Description
Performing reconnaissance	In this phase, the hacker begins gathering information about the target. This can include gathering publicly available information, using social engineering techniques, or even dumpster diving.
Scanning and enumeration	Scanning is a natural extension of reconnaissance. The hacker uses various tools to gather in-depth information about the network, computer systems, live systems, open ports, and other features. Extracting information such as usernames, computer names, network resources, shares, and services is known as enumeration. Enumeration is a part of the scanning step.
Establishing access	In this phase, the hacker uses all the information gathered through reconnaissance and scanning to exploit any vulnerabilities found and gain access.
Maintaining access	Once the hacker has gained access, he can use backdoors, rootkits, or Trojans to establish permanent access to the system.
Clearing tracks	The final step in the hacking process is clearing tracks. The hacker overwrites log files to hide the fact they were ever there.

Penetration Testing Life Cycle

Another methodology is the penetration testing life cycle. The penetration testing life cycle is almost identical to the ethical hacking process. The steps are:

1. Performing reconnaissance
2. Scanning and enumeration
3. Establishing access
4. Maintaining access
5. Reporting

The only difference is the focus on the documentation of the penetration test. A detailed report of the tests performed and everything that was discovered is important.

Penetration Testing Frameworks

Multiple penetration testing frameworks have been developed and are be used in appropriate situations.

Framework	Description
Open Web Application Security Project (OWASP)	Describes techniques for testing the most common web applications and web service security issues.
Open Source Security Testing Methodology Manual (OSSTMM)	Attempts to create one accepted method for a thorough security test.

National Institute of Standards and Technology Special Publication 800-115 (NIST SP 800-115)	Is a guide to the basic technical aspects of conducting information security assessments.

Penetration Testing Types

The following table identifies the different types of penetration tests:

Type	Description
Black box	The ethical hacker has no information regarding the target or network. This type of test best simulates an outside attack and ignores the insider threats.
White box	The ethical hacker is given full knowledge of the target or network. This test allows for a comprehensive and thorough test, but is not very realistic.
Gray box	The ethical hacker is given partial information of the target or network, such as IP configurations or emails lists. This test simulates an insider threat.