04-Vulnerability Analysis

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online that have the services running and vulnerable

Advanced: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.
Advanced: capture encrypted packets, using decryption process from capture discussion

Attacker Data: Kali/ Parrot

Objectives

To extract information about the target system:

- Network vulnerabilities
- Service bindings on IP:TCP/UDP ports
- Application and services configuration errors/vulnerabilities
- OS version running
- Applications installed
- Accounts
- Files and folders
- Unnecessary default services
- Security misconfiguration of common applications
- Computers containing reported vulnerabilities

Overview of Vulnerability Assessment

How do we know how to secure a network? An administrator needs to perform patch management, install proper antivirus software, check configurations, solve known issues in third-party applications, and troubleshoot hardware with default configurations.

Lab Tasks

1. Perform vulnerability research with vulnerability scoring systems and databases
    1.1. Perform vulnerability research in Common Weakness Enumeration (CWE)

1.2. Perform vulnerability research in Common Vulnerabilities and Exposures (CVE)

1.3. Perform vulnerability research in National Vulnerability Database (NVD)

2. Perform Vulnerability Assessment using Various Vulnerability Assessment Tools

2.1. Perform vulnerability analysis using OpenVAS*

2.2. Perform vulnerability scanning using Nessus

~~2.3. Perform vulnerability scanning using GFI LanGuard~~

~~2.4. Perform web servers and applications vulnerability scanning using CGI Scanner Nikto~~

*Indicates capture