05-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

In class process:

Typically you will NOT have access to Nessus or OpenVAS as a penetration tester.
At this point you have the reconnaissance data with a minimum of IP/PORT/OS/SERVICE/VERSIONS that the client has had a chance to accept or reject as truly in scope. If Nmap data is in database format / output to a readable spreadsheet (use it again from the database as an input to metasploit.

I am going to give you a very narrow scope output from reconnaissance for you to research in class. (soon)

As you have the reconnaissance data with a minimum of IP/PORT/OS/SERVICE/VERSIONS.
Now you go hunting for vulnerabilities using:

1. https://www.exploit-db.com/ = Is there a proof of concept exploit?
2. https://packetstormsecurity.com/files/tags/exploit/ = Can you download an exploit?
3. https://cve.mitre.org/cve/search_cve_list.html = Does the whole planet know?

Next stage (practice exploitation)

4. Setup a test victim that matches your reconnaissance data.
5. Do you have the skills to push #1 & #2 to your test victim?

For class just do #3 https://cve.mitre.org/cve/search_cve_list.html

Here is the scope for you to research in class:
The Windows 2019 server is open on TCP port 3389 and UDP port 3389. It was last patches in December 2020.
What is it susceptible / vulnerable to? List the CVE IDs in the Instructor Q&A.

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

For the exam you must know OpenVAS. Read this for the new version as of 2021-06-15
https://docs.greenbone.net/GSM-Manual/gos-21.04/en/web-interface.html
https://docs.greenbone.net/GSM-Manual/gos-21.04/en/scanning.html

The full docs:

Greenbone Security Manager with Greenbone OS 21.04

Online Version, Status: 2021-06-14

Greenbone Security Manager with Greenbone OS 20.08

Online Version, Status: 2021-06-15

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