Vulnerability Assessment Lab

Fully assessing a company's security posture is a critical job to maintain intellectual property integrity, and protect customer information. As a security auditor your job is to identify known vulnerabilities and risks that could harm your client's organization. Audits are usually performed in three parts, namely procedure & policy audit, disaster recovery audit, and technical audit.

Objective

You are tasked with a technical audit of a small group of machines listed below.

- **Part 1 – Nessus / OpenVas**
  - Scan the Metasploitable VM for vulnerabilities using Nessus and OpenVas vulnerability scanners using the Backtrack5R3 VM (do not run both scans simultaneously).
  - Identify as many vulnerabilities as you can for an audit report. Find proof of concept exploit code for at least two of the vulnerabilities identified for each scanner (four total).

- **Part 2 – Nikto**
  - Scan the DVWA VM for vulnerabilities using the Nikto Web scanner

Turn In

- **Part 1 – Nessus / OpenVas**
  - A "Technical Report" describing the system's current security posture, risks, and all audit reports. Include answers to the following: How many vulnerabilities did each scanner find? How many open ports /which ones? What services are highly vulnerable? What type of attack is the selected service vulnerable to? What versions of the service are affected by the vulnerability? What security advisories are available for further research on the security bug?
  - Include proof of concept exploits for the four vulnerabilities selected in the objective section. This can be turned in with a link to a site that provides the exploit code.

- **Part 2 – Nikto**
  - Incorporate the Nikto audit report as part of the write up in part one.

Keys to success

- **Read entire lab document**
- Use the Metasploitable, DVWA, and Backtrack5R3 VMs.
- Use these sites to find exploit code for the vulnerabilities found in the scans:
  
  - http://www.exploit-db.com
  - http://www.1337day.com
  - http://www.securityfocus.com
Starting the VMs

1) Start Backtrack5R3 VM (Auditor)
   IP = 10.0.0.10
   Login to BT
   user: root
   password: toor
   Start GUI interface: startx

2) Start Metasploitable VM
   IP = 10.0.0.13

3) Start DVWA VM
   IP = 10.0.0.12

4) Verify connectivity between the Backtrack VM and Metasploitable and DVWA VMs.
   (use 'ping' command)

Nessus

Nessus is the industry’s most widely-deployed vulnerability and configuration assessment product. Nessus features high-speed discovery, configuration auditing, asset profiling, sensitive data discovery, patch management integration, and vulnerability analysis. It can detect, scan, and profile numerous devices and resources to increase security and compliance across any network.

Starting Nessus

Open a new terminal. type:
/etc/init.d/nessusd start

or from the GUI:
   Application->Backtrack->Vulnerability Assesment->Vulnerability Scanners->Nessus->nessus start

To verify nessus service is running you can quickly check what ports are listening on your machine. Nessus daemon operates on port 8834. Verify nessus started up correctly:

   netstat -ant | grep LISTEN (should display port 8834 as LISTENING)

Using Nessus

Open a browser to https://127.0.0.1:8834

Login to nessus
   user: lab
   password: secure?

Click on Scans -> Add
   Name - metasploitable
   Type - Run Now
   Policy - Internal Network Scan
   Scan Targets - 10.0.0.12
Once scan details have been filled in, click on 'Launch' to start scanning the remote system.

Once scan finishes click on 'Reports'
  double-click the completed metasploitable scan or select the scan and click 'Browse'

Read through the audit report looking for vulnerabilities and the information needed for the write up in the turn in section.
OpenVAS

The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The actual security scanner is accompanied with a daily updated feed of Network Vulnerability Tests (NVTs), over 20,000 in total. All OpenVAS products are Free Software. Most components are licensed under the GNU General Public License (GNU GPL).

Starting OpenVAS

Open a new terminal, and type the startup commands:

- `opvasasd` (Starts the scanner - will load the signatures available in NVTs)
- `opvasmd -p 9390 -a 127.0.0.1` (Starts Openvas Manager - runs as daemon)
- `opvasad -a 127.0.0.1 -p 9393` (Starts Openvas Administrator)
- `gsad --http-only --listen=127.0.0.1 -p 9392` (Starts greenbone Security Assistant)

Verify opvas service started up correctly:

```
netstat -ant | grep LISTEN (ports 9390/9391/9392/9393 should be listening)
```

Using OpenVAS

Open http://localhost:9392/

```
user: lab
password: secure?
```

Once logged in, you have to create a target to scan against, then create a scan task.

Target Creation

On the Left hand menu, Click on Targets
Enter the name and IP address information.
Click Create Target
Task Creation
On the Left hand menu, Click on New Task
Enter the Name
Under Scan Config
Select Full and fast
Under Scan Targets
Select the target created in previous step
Click Create Task

Task Initialization
On the Left hand menu, Click on Tasks
Select the task created in previous step
Click on “play” arrow
Scan Report

Once the scan has completed. Click on task 'details' or the date of the last completed scan.

The scan results should look something like the following diagram.

Read through the audit report looking for vulnerabilities and the information needed for the write up in the turn in section.
Nikto

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6400 potentially dangerous files/CGIs, checks for outdated versions of over 1000 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software.

Installation

Nikto is simple a compressed download which when extracted is executable as is. Nikto does not need root access to run. There are many parameters to nikto. To do a simple scan against a web server enter the following command.

    cd ~/pentest/web/nikto

    ./nikto -host www.example.com