# CIT 285 - Lab #4: Vulnerability Scanning

## Introduction

* In this lab, we will discover and research vulnerabilities using the Nessus vulnerability scanner, which is already installed on the Kali Linux VM.
* The Metasploitable 2 VM will be the TARGET of most scans performed in the lab. of all scans.
* Both VMs should be running.

**References**

1. Nessus documentation, <http://www.tenable.com/products/nessus/documentation/>
2. Nessus videos, <http://www.tenable.com/videos/>

## 1: Finding Vulnerabilities with Nessus

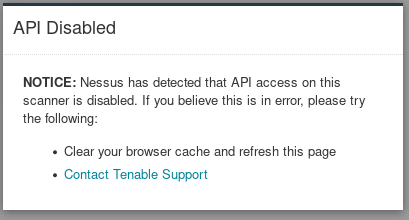
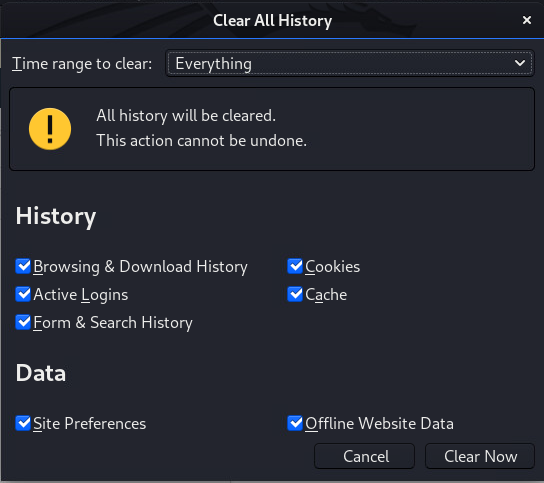
Nessus has been download and configured on your Kali VM. You will need to start Nessus from the terminal, then use a web browser to reach the user web interface. Start Nessus with the following command.

**# /etc/init.d/nessusd start**

Open Firefox and **clear** the **entire history** (including cookies and other cached data), then type the address <https://localhost:8834/>  in the URL bar.

1. Once Nessus finishes loading (*this may take several minutes*), enter the following credentials
2. UN = **nessus**
3. PW = **285toor285**

At the Nessus Essential web interface, complete the following to begin a new scan. If an ‘API Disabled’ message appears, clear the Firefox browser history again. Be sure your ‘Clear History’ window matches the image below.

1. Click on Create a New Scan.
2. Click on Basic Network Scan.
3. For Name, enter “Lab #4” and a brief description if you like
4. For Targets, enter the IP address of the TARGET VM (i.e. your Meta VM).
5. Do not modify any of the other fields.
6. Click on Save

When you save a new scan, it should begin running immediately. If for some reason it does not start, click on the Launch icon (the little play arrow) to start the scan. The scan will take between 5 and 10 minutes to complete.



Once the scan finishes, click on the scan name to view the summary of results. Click on the color-coded bar showing all the vulnerabilities to view vulnerability details.

1.1: How many vulnerabilities were found in total?

There was a total of 67 vulnerabilities total

1.2: Provide the number of vulnerabilities in each severity level in the table below.

* Write one severity level per line below. Click on the ‘Vulnerabilities’ tab for more information.

|  |  |  |
| --- | --- | --- |
| Severity Level | Number Reported | Example Name |
| **Critical** | **8** | **Bind Shell Backdoor Detection** |
| **High** | **4** | **Rsh service detection** |
| **Medium** | **14** | **SMB signing not required** |
| **Low** | **4** | **X server detection** |
| **Informational** | **117** | **Service detection** |

## 2: Understanding Vulnerabilities

Click on the first vulnerability of critical severity to see the details Nessus reported. Each vulnerability has multiple attributes, the most important of which are

1. **Nessus plugin ID number:** 
   * + *Identifies the plugin that reported the vulnerability*.
2. **Nessus plugin name:** 
   * + *The name of the plugin that reported the vulnerability*.
3. **CVE (Common Vulnerabilities and Exposures) vulnerability identifier:**
   * + *Some vulnerabilities will not have this identifier, but vulnerabilities that do are recorded in the National Vulnerability Database (nvd.nist.gov) and can be looked up there or at* [*www.cvedetails.com*](http://www.cvedetails.com/)*. A single Nessus vulnerability may correspond to multiple CVE identifiers. These identifiers are of the form CVE-YEAR-####.*
4. **Other vulnerability identifiers:**
   * + *Many vendors, such as Microsoft (MS-## format) and the Mozilla Foundation (MFSA-YEAR-####) record vulnerabilities in their own databases, which may provide more information than Nessus shows or that can be found in CVE databases. Other identifiers include OSVDB numbers for the Open Source Vulnerability Database and BID numbers for the Bugtraq database at securityfocus.com*.
5. **CVSS base score:** 
   * + *The Common Vulnerability Scoring System (CVSS) provides a numerical indication of vulnerability severity ranging from 0 to 10. Critical vulnerabilities will have CVSS scores near 10. The current CVSS version is 2.0. More details can be found at https://nvd.nist.gov/cvss.cfm*.
6. **Exploit available:** 
   * + *Indicates whether or not an open source (like Metasploit) or commercial (like Canvas or Core Impact) exploit framework has an exploit for this vulnerability. Even if no exploit exists for a vulnerability in a popular framework, individual exploit scripts may be found on sites like Exploit DB* (www.exploit-db.com).
7. **Exploitable with:** 
   * + *Names which frameworks have exploits for this vulnerability*.
8. **See also:**
   * + *This section contains additional references to the vulnerability, which may help to better understand its impact or aid you in finding exploits for the vulnerability*.

2.1: **For each of the critical severity vulnerabilities reported** by Nessus, enter all of the items in the list above in order except for the last attribute (#8). For attribute #4, other vulnerability identifiers, only list CVE identifiers if available; otherwise, list the first other identifier reported. **Make as many copies of the table below as needed.**

|  |  |
| --- | --- |
| **Critical Vulnerability Name** | **Debian open SSH/OpenSSL package random number generator weakness** |
| **Nessus Plugin ID** | **32314** |
| **Nessus Plugin Name**  *(if applicable)* | **N/A** |
| **CVE Identifier**  *(if applicable)* | **CVE-2008-0166** |
| **Other Vulnerability Identifier**  *(if applicable)* | **CWE: 310 and BID: 29179** |
| **CVSS base score** | **10** |
| **Exploit available?** | **Yes** |
| **Exploitable with** | **Core impact** |

|  |  |
| --- | --- |
| **Critical Vulnerability Name** | **Bind Shell Backdoor Detection** |
| **Nessus Plugin ID** | **51988** |
| **Nessus Plugin Name**  *(if applicable)* | **N/A** |
| **CVE Identifier**  *(if applicable)* | **N/A** |
| **Other Vulnerability Identifier**  *(if applicable)* | **N/A** |
| **CVSS base score** | **9.8** |
| **Exploit available?** | **No** |
| **Exploitable with** | **N/A** |

|  |  |
| --- | --- |
| **Critical Vulnerability Name** | **NFS Exported Share Information Disclosure** |
| **Nessus Plugin ID** | **11356** |
| **Nessus Plugin Name**  *(if applicable)* | **N/A** |
| **CVE Identifier**  *(if applicable)* | **CVE-1999-0170** |
| **Other Vulnerability Identifier**  *(if applicable)* | **CVE-1999-0211 and CVE-1999-0554** |
| **CVSS base score** | **10** |
| **Exploit available?** | **Yes** |
| **Exploitable with** | **Metasploit (NFS Mount Scanner)** |

|  |  |
| --- | --- |
| **Critical Vulnerability Name** | **Rexecd Service Detection** |
| **Nessus Plugin ID** | **10203** |
| **Nessus Plugin Name**  *(if applicable)* | **N/A** |
| **CVE Identifier**  *(if applicable)* | **CVE-2008-0618** |
| **Other Vulnerability Identifier**  *(if applicable)* | **N/A** |
| **CVSS base score** | **10** |
| **Exploit available?** | **No** |
| **Exploitable with** | **N/A** |

|  |  |
| --- | --- |
| **Critical Vulnerability Name** | **Unix Operating System Unsupported Version Detection** |
| **Nessus Plugin ID** | **33850** |
| **Nessus Plugin Name**  *(if applicable)* | **N/A** |
| **CVE Identifier**  *(if applicable)* | **N/A** |
| **Other Vulnerability Identifier**  *(if applicable)* | **N/A** |
| **CVSS base score** | **10** |
| **Exploit available?** | **No** |
| **Exploitable with** | **N/A** |

|  |  |
| --- | --- |
| **Critical Vulnerability Name** | **UnreallRCd Backdoor Detection** |
| **Nessus Plugin ID** | **46882** |
| **Nessus Plugin Name**  *(if applicable)* | **N/A** |
| **CVE Identifier**  *(if applicable)* | **CVE-2010-2075** |
| **Other Vulnerability Identifier**  *(if applicable)* | **BID: 40820** |
| **CVSS base score** | **10** |
| **Exploit available?** | **Yes** |
| **Exploitable with** | **Metasploit and CANVAS()** |

|  |  |
| --- | --- |
| **Critical Vulnerability Name** | **VNC Server ‘password’ Password** |
| **Nessus Plugin ID** | **61708** |
| **Nessus Plugin Name**  *(if applicable)* | **N/A** |
| **CVE Identifier**  *(if applicable)* | **N/A** |
| **Other Vulnerability Identifier**  *(if applicable)* | **N/A** |
| **CVSS base score** | **10** |
| **Exploit available?** | **Yes** |
| **Exploitable with** | **N/A** |

## 3: Exploiting Reported Vulnerabilities

3.1: Find the backdoor exploit named Bind Shell Backdoor Detection in the list of Critical vulnerabilities. Select this vulnerability and review its information. In your words, provide a brief description and explanation of how this vulnerability can be exploited.

**There is a shell that is listening on the remote port that doesn’t have any authentication. This can cause an attacker to connect and send commands directly. We can exploit this by verifying the host and if its been compromised and if so uninstall the system.**

3.2: Attempt to exploit this vulnerability using the command below, which uses the netcat (nc) to make a remote connection. **If you are not able to exploit the vulnerability, go back and reread the details section of the vulnerability**.

**# nc Metasploit\_IP Vulnerability\_PORT**

A prompt of *root@metasploitable:/ #* means you have successfully exploited the vulnerability. Once connected to the TARGET machine, determine which user you are logged in as and which directory you are currently in. Include both command outputs below.

**# id**

**# pwd**

Graphical user interface, text

Description automatically generated

3.3: Let's use this backdoor shell login, to learn more about the system. In particular, we can determine which network services are running on the target. Issue the following while the connection is still in place.

**# lsof -i -n -P**

In a new terminal use nmap to scan your TARGET machine.

**# nmap -sT Metasploit\_IP**

3.3: Once the scan completes, compare the output from nmap to the output reported by lsof to determine the ports **lsof** found that **nmap** did not report?

**When comparing the two we can see lsof has listed ports 940, 50970, 56766, 953, 137, 138, and much more compared to the nmapp.**

Graphical user interface, text

Description automatically generated

3.4: Next, exploit another critical vulnerability named VNC Server 'password' Password to access the VNC remote desktop on the target. Find this vulnerability and review it’s details.

From a new terminal, issue the command below. The number 0 following the target IP address indicates the first VNC remote desktop on the target. If multiple desktops are running, you will need to experiment with changing that number to 1, 2, 3, etc. to reach the remote desktop. **If you are not able to exploit the vulnerability, go back and reread the details section of the vulnerability.**

**# xtightvncviewer Metasploit\_IP:0**

Run the **id** command once logged into the target.

* Which user's remote desktop are you accessing?
  + You are accessing the root user of the Metasploitable
* Provide a screenshot of this output below

A picture containing text, monitor, screenshot, electronics

Description automatically generated

Close all terminal windows with remote connections open.

Close your browser window and shutdown Nessus from the terminal

**# /etc/init.d/nessusd stop**

## Submission

Upload a completed copy of this document to Canvas by the due date.