Lab 4 - Vulnerability Scanning with Nessus

There are two deliverables for this lab.

1. Vulnerability report exported from Nessus
2. Analysis one of Critical vulnerability

You should already have Nessus installed on your Kali system during the previous lab. Please follow the instructions below to complete the lab

Vulnerability Report

Steps.

```
1. Start your Kali machine and login with Username: kali , Password: Kali

2. Type “sudo systemctl start nessusd”

3. Accept the Self Signed certificate and login with the account you created during
the installation process

4. Go to Scans and select New Scan

5. On the scan templates page select the “Advanced Scan” template

6. Enter the name of your scan “MetasploitableV2 Scan”

7. Under target enter the IP address of your metasploitable machine

8. Save the scan (this should take you to my scans page)

9. From My Scans page hit the play button which will start the scan
```

Once the scan has completed, please select it and the click on the Vulnerabilities tab. Answer the following questions:

```
1. How many “Critical” vulnerabilities were found

2. How many “High” vulnerabilities were found?

3. How many “Medium” vulnerabilities were found?
```

Please export the report in PDF format and upload it to the assignment (Detailed Vulnerabilities by host).

Vulnerability count overview

1. Number of Critical vulnerabilities: 14
2. Number of High vulnerabilities: 7
3. Number of Medium vulnerabilities: 27

Analysis of a “Critical” vulnerability

Select one of the “Critical” vulnerabilities and explain the following (please note that using the Nessus explanation is not enough to answer this question. You should research the vulnerability online or use references provided by Nessus):

- What is the vulnerability?
- How can it be exploited?
- What are the remediation steps?

Critical vulnerability analysis

1. Unsupported Web Server Detection - Tomcat 5.5
2. Systems that use the default password for the admin account allows an attack to gain access by guessing the username such as 'root' or 'admin'
3. For the administrator of the system to update the default password for the web server

`https://www.cvedetails.com/cve/CVE-2009-3548/`