|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| **Lab Report** |
| COURSE: Cyber 262  Lab : GROUP Lab – OpenVAS Scan-Patch-Verify  Submitted BY: Jack Morgan  Date: 02/23/2022  Instructor: Hozza |
| *By submitting this report I certify that this is my work and was not copied from other sources. Any use of public materials is cited.* |

Table of Contents

[INTRODUCTION 3](#_Toc50470226)

[SCREEN CAPTURES 4](#_Toc50470227)

[REFLECTION 5](#_Toc50470228)

# INTRODUCTION

# SCREEN CAPTURES

***Figure (1.1):*** *Take a screenshot showing your ‘create user’ command along with the generated password*

Graphical user interface, application

Description automatically generated

***Figure (1.2)****: Take a screenshot showing that you have started the scan. Make sure your screenshot shows your PSU-ID login in the top-right, as well as the status of your scan. ‘Requested’ or ‘1%’ status is fine.*

Graphical user interface

Description automatically generated

***Figure (1.3):*** *Perform some research and find where log files are stored on the machine. Play the part of a Security Admin and use the* ***tail -f*** *command to show evidence from at least one system log file to show you are being actively scanned by an adversary (192.168.0.3). Show at least 3 concerning connection attempts in your screenshot (Extra credit if you can capture the* ***Magic Fairy Dust***

Graphical user interface, text

Description automatically generated

***Figure (1.4):*** *On the Canvas page for this lab, you will find a compelte OpenVAS scan report of the Metasploitable machine. Take a look at the vulnerabilities present on the machine.* ***Each Team Member should choose 2 vulnerabilities from the report and explain how these could severely impact an organization. Relate your answer to the CIA Triad. Answers should explain the issue and the potential fallout in a short paragraph or two. List the name of the team member and their two contributions below.***

1. *NVT: vsftpd Compromised Packages Backdoor Vulnerability: After doing some research for the previous question, I found a file called vsftpd.log which was the only log I did not have permission to read. According to the canvas page, the impact is listed as saying that the exploit can execute arbirtrary commands given the context of te applocations. It also states that succesful attacks will compromise the affected applocation. The listed solution is through VendorFix which is a repaired package that can be downlaoded from given link. In terms of the CIA triad, this mostly affects integrity which deals with the protection of information or modification which is what the vulnerability acordingly attempts to alter.*
2. *NVT: TWiki XSS and Command Excrution Vulnerabilities: According to the canvas page, the summary lists that the host ‘is running TWiki and is prone to Cross-Site Scripting (XSS)’ Cross-site scripting is a type of security vulnerability that can be found in web applications that enables an attacker to inject scripts into web pages. Usually they are used to bypass access controls which directly impacts the confidentiality and protection of data. Bypassing access controls directly affects the strength of security of a system and shows that the system is not secure to unauthorized ediotrs and readers.*

***Figure (2.1):*** *Take a screenshot showing your output of the Nmap command.*

Graphical user interface, text, application

Description automatically generated

***Figure (2.2):*** *Once you have opened a session, type ‘whoami’ to prove you are root, then type ‘hostname’ to prove you are connected to Metasploitable.*

Graphical user interface, text, application

Description automatically generated

***Figure (2.3):*** *Prove that your patch worked. Take a screenshot of at least 2 failed exploit attempts.*

Graphical user interface, text, application

Description automatically generated

***Figure (3.1):*** *Take a screenshot showing the result of your netcat command*

Graphical user interface, text, application

Description automatically generated

***Figure (3.2):*** *Prove that your patch works. Redo the netcat command above and take a screenshot of the results.*

***3.3:*** *How did you patch this vulnerability? Document and provide the changes you made to the Metasploitable machine. Be as through as possible in your documentation.*

***4.1:*** *Which vulnerability did each team member choose? Be specific in what information you gained from the OpenVas Scan Report?*

***Each team member did a separate vulnerability.******I decided to create a patch for the 2121/TCP vulnerability which is titled, “FTP Unencrypted Cleartext Login”. From the OpenVas Scan Report I gained information such as: a description of the vulnerability, how the vulnerability was detected, potential solutions and some insight into the vulnerability itself.***

***4.2:*** *How/Where did you research this vulnerability? What information did you gather? Were you able to exploit the vulnerability?*

***After using the OpenVas Report, I performed separate research on port 2121’s uses and how to perform the given solution.******I gathered information specifically on how to mitigate the problem which centered around enabling FTPS and enforcing connections with the ‘AUTH TLS’ command as listed in the OpenVas report.***

***4.3:*** *Were you able to patch the vulnerability? In a short paragraph, explain the steps you took to remediate the vulnerability, and whether your patch was effective or not.*

***To patch the vulnerability, the OpenVas report explains that Mitigation is the best solution, specifically enabling FTPS or enforcing the connection through the ‘AUTH TLS’ command.******According to RFC 2228, this command is used to authenticate TLS or SSL to secure both the data and control channel in a connection. Enabling FTPS depends on the system you are using, however for Linux we can follow a list of instructions located in the following links. I was not able to patch the vulnerability as I frequently got stuck on the second step of mentioning certificates and key file locations, however with some more knowledge on encryption and practice I know there is an easy mitigation process to this vulnerability.***

[***https://www.opensourceforu.com/2015/03/set-up-an-ftps-server-in-linux/***](https://www.opensourceforu.com/2015/03/set-up-an-ftps-server-in-linux/)

***4.4*** *Pretend you found this vulnerability on an Organization’s machine. How would you explain to them the present risk, and why they should patch the vulnerability?*

***I would explain this vulnerability by first addressing the risk it provides to the organization. The impact of this specific vulnerability is that an attack can discover login names and passwords by simply using a packet sniffer on existing traffic to an FTP service. If a patch is not created for said vulnerability, attackers can easily steal login names and passwords and send them to an unreachable file. This could result in major security concerns as foreign entities would be able to login to our organizations machines from remote locations and quietly gather even more sensitive data about the organization and its employees.***

# REFLECTION