|  |
| --- |
| Ethical Hacking and Defence |
| Assignment 2 – Penetration Testing Report |

Family Name: David Selvam

Given Name: Visahl Samson

Student Number: 10498743

Unit code and Title: CSI3208 Ethical Hacking and Defence

Name of Lecturer: James Lau

Campus: PSB Academy, Singapore

Course: Bachelor of Science in Cyber Security (FT)

Due Date: 12th November 2020 (02:00 PM)

Contents

[Executive Summary 3](#_Toc55999104)

[Introduction 3](#_Toc55999105)

[Methodology 4](#_Toc55999106)

[Penetration Test Log 6](#_Toc55999107)

[Recommendations 13](#_Toc55999108)

[Appendix 15](#_Toc55999109)

[References 20](#_Toc55999110)

# Executive Summary

The scenario given is to do penetration testing on the given “ALHEIM-LABS” machine. The successful completion required to accomplish root privileges by using appropriate tools and techniques. The penetration testing has been conducted based on the methodology that was provided in the analysis plan that previously submitted before beginning the penetration testing. The methodology proposed in the analysis plan was, penetration testing execution standard (PTES) which consists the process of pre-engagement activities, information gathering, threat modelling, vulnerability assessment, exploitation, post-exploitation, and reporting.

All the five flags have been found along with various security vulnerabilities and poor security practices which impacts the organization in multiple tracks. Also, while the end of the penetration testing, it has been confirmed that corporate espionage is going on in the organization which needs to be addressed with high priority.

To conclude, this report provides a detail explanation of how each flag has been discovered by utilizing the multiple vulnerabilities along the way. Also, it details on various tools and techniques involved in the assessment. At the end of the report, recommendations are provided to enhance the security measures to protect the organization assets from unauthorized exploitation.

# Introduction

The main objective of this penetration test is to exploit the target system where the high priority was given to attain root privileges by using appropriate tools and techniques. This given report is based on the penetration test carried and to make sure the client can understand the vulnerabilities exist in their system. Also, step-by-step explanation of the whole test process starting from finding the IP address, to finding out the corporate espionage has been briefed in this report.

In the information-gathering phase, the IP address of the target machine has been found. In the scanning phase, all the open ports were discovered, in the exploitation phase proper port has been exploited based and try error method. Once the system has been exploited, the post-exploitation has been done by using poor security practices and misconfigurations. Since, the client did not disclose any specific information about the system, the test categorized under Blackbox method. Nmap, Metasploit, Burpsuite were the tools involved in this test. Thus, this report briefs each action and attack performed against the target and the result of them.

# Methodology

As stated earlier in the analysis plan, penetration testing execution standard (PTES) has been followed here. This methodology involves pre-engagement activities, information gathering, threat modelling, vulnerability assessment, exploitation, post-exploitation, and reporting. Since threat modelling does not have any significant requirement here it has been avoided in the test.

1. **Pre-engagement activities**

In Penetration Testing, the pre-engagement activities involve business activities such as signing a non-disclosure agreement, reviewing the analysis plan, signing a contract/agreement (Khawaja, 2018). In our scenario, the pre-engagement phase has been done by submitting an analysis plan.

1. **Information Gathering**

A typical information gathering phase involves the finding of basic information about the target such as IP address, OS, etc (Weidman, 2014) In our case, Nmap has been used to find out the IP address of the target system running.

1. **Vulnerability assessment**

Once, the information gathering has been done, the Nmap scan has been performed on the IP address to find out any vulnerabilities that can be exploited. Once the scan results arrive, based on the software/service versions a search for suitable Common Vulnerabilities and Exposures (CVE) has been done using Exploit DB and searchsploit. For each search, the most recent exploit has been selected to get more accuracy.

1. **Exploitation**

In penetration testing exploitation phase primarily focuses on launching access to a target system. To start this phase vulnerability assessment needs to be done properly (PTES, 2014). In our case, the target machine has been exploited after trying to compromise multiple services and ports. The exploitation phase has been done with the usage of Metasploit (MSF Console) with the command RHOST (target system IP)

Once the access has been gained, the tester needs to confirm it by using the common commands such as whoami, PWD. Once confirmed then the tester can browse for directories, and files or even try to gain root privileges. In our case, once the service exploited successfully, the **ls** command has been used to find out the Flag1. Also, further enumerations such as user enumeration, service enumeration have been performed. Main directories that are explored in this phase was **irclogs** which consists of all the communication between the user Paul and others. And the various steps carried on this phase helped to find out the flag 1 – flag 4.

1. **Post Exploitation**

Post exploitation is a phase where the tester needs to find out all the sensitive things and to perform unauthorized access to reveal potentials vulnerabilities such as gaining root privileges, downloading sensitive information, etc.. In our case, the post-exploitation has been done by utilizing the information gathered during the exploitation phase which involves usage of SSH which revealed the flag 5.

# Penetration Test Log

The complete penetration test that was undertaken has been tabulated below with the actions that were carried out.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| No | Phase | Action | Explanation | Result | Reference |
| 1 | Information Gathering | Usage of **ifconfig** command | To see the IP address of Kali Linux Machine | IP address of Kali Linux Machine was 172.16.209.134 |  |
| 2 | Using the command nmap 172.16.209.134/24 | To find out the IP address of target machine | IP address of the target machine was 172.16.209.132 | Screenshot 1 |
| 3 | Scanning | Usage of nmap -SV -p- 172.16.209.133 | To see all the 65535 ports | Displayed all the open ports | Screenshot 2 |
| 4 | Vulnerability identification | Usage of ExploitDB | To see exploit for ProFTPD | Selected most recent exploits to try |  |
| 5 | Usage of ExploitDB | To see exploit for drb service | Found a exploit written in 2011 |  |
| 6 | Exploitation | MSFconsole | To try FTP exploit | Not vulnerable |  |
| 7 | Msfconsole serch druby command | To configure drb exploit | Selected the exploit | Screenshot 3 |
| 8 | Setrhost 172.16.209.133 | To select the target system | Finalised the target | Screenshot 4 |
| 9 | Run command | To execute the exploit | Exploit started successfully with reverse connection |
| 10 | Using shell | For reverse connection with the target | Successfully started a session |
| 11 | **Whoami and ls** command | To see the username and files in the directory | Found out logged in as paul, and received flag 1 **#A}?S/UL”&DZ**  **r}jFGN4Fc)$**  **MU>uq3FUcM”’**  **A}3>YVhj)mKpECV** |
| 12 |  | **cd irclogs/localhost/tac Allison.log** command | To enumerate useful information | Found Paul has contact with Allison and granted her sudo permissions | Screenshot 5 |
| 13 |  | **tac dr\_balustrade.log** | To enumerate useful information | Found Paul has transferred FTP password to Dr Balustrade in cleartext Password: KYNZh9t51nCLiIK | Screenshot 6 |
| 14 |  | **cd /ftp** | To enumerate useful information | Permission denied |  |
| 15 |  | **wget -r – no-passive-ftp ftp://anonymous:** **KYNZh9t51nCLiIK@**  **172.16.209.133/** | To login and download the FTP as anonymous | Login incorrect | Screenshot 7 |
| 16 |  | **wget -r – no-passive-ftp ftp://backup:** **KYNZh9t51nCLiIK@**  **172.16.209.133/** | To login and download FTP as backup (Since, in the conversation log Dr Balustrade mention as backup user | Loggedin and downloaded the FTP directory |
| 17 |  | **cd /Desktop/172.16.209.133**  **ls**  **cat flag2** | To browser the FTP folder and to enumerate useful information | Found the flag 2 Flag 2 = Po1He  Epeixai  9oJ6eim  eeh1ahbu2om | Screenshot 8 |
| 18 |  | **cd etc**  **cat shadow** | Changed the working directory to etc then found, and viewed password hashes | The file listed the hashes for Allison, Dr Balustrade, Paul, Root, and Backup | Screenshot 9 |
| 19 |  | **John –wordlist=/usr/share/**  **wordlists/rockyou.txt shadow hashes.txt** | Using john the ripper the hashes were cracked | Credentials for Dr Balustrade has been found  Username : dr\_balustrade, Password: Pink |  |
| 20 |  | **Exploiting web server and entering the credentials of Dr balustrade** | Results in scanning phase indicated a web server running on the machine, so using firefox browser the webpage has been accessed where it was a login page, the credentials of Dr Balustrade has been used to login. | The landed page was a Samba admin panel and no useful information has been obtained |  |
| 21 |  | **ssh dr\_balustrade@172**  **.16.209.133**  **ls**  **cat flag 3** | By using the same credentials that were found previously, this time attempted to logged into ssh | Successfully logged inside the machine  Directories has been listed  Found flag 3 **Y|O`r6A5g2`-]z]}pC/$iw]T**  **AVKLBSp0U**  **[F8G\*:x=dE"13U'"w** | Screenshot 10 |
| 22 | Post Exploitation | **cd webtemp**  **cat checklogin.php** | Changed the work directory to webtemp and found PHP file  Viewed checklogin.php file | Found the hard coded credentials where the username was web, and password was supersecret,  Also, found the Database name, and table name | Screenshot 11 |
| 23 |  | **mysql -u web -p -h localhost**  **show db**  **use web**  **show tables**  **select \* from members;** | To login into mysql service that is running in the target system  By using the hardcoded details tried to obtain useful information from database | Using the credential supersecret successfully logged into the mysql  Successfully found the username : drB, and Password: Rainb0wD  4ash1sBe$tP0ny | Screenshot 12 |
| 24 |  | **Browsing for 172**  **.16.209.133/index.php**  Entering the credentials username: drB, and Password: Rainb0wD  4ash1sBe$tP0ny | To see whether the credentials allowing to login and to find out useful information | The credentials allowed to login and found an empty page with a list-box option and text displaying login successful | Screenshot 13 |
| 25 |  | **Using Burp suit to modify the user response from Display = SELECT+\*+FROM+test&Submit=Display to**  **Display=SHOW+tables& Submit=Display** | Burpsuit is one of the most popular web application testing tool | After the user response modified, the displaystats.php gave hint to the flag 4 | Screenshot 14 & 15 |
| 26 |  | **Changing the inspect element value in login\_success.php page from value=”SELECT \* FROM test**  **To**  **value=”SELECT \* FROM flag4**  **also to**  **value=”SELECT \* FROM statsadmin** | In previous step, the hardcoded details displayed the array values where 0 was used for flag 4, and 1 was assigned to statsadmin so applying this in inspect element page to get hints | As expected changing the value to flag 4 gave the flag4: j}Cq5-;&GcfC8j<9:yje%k+vE(<6{Rb{V(SWb;6JA  and statsadmin provided few credentials where the username was allison but the details where in unknown format | Screenshot 16, 17, 18, 19 |
| 27 |  | **Using Google Translate** | To find out what was written in the unknown format | It revealed that it was written in Korean language, and the credentials of Allison account. The password is **-**이 SSH에 대한 비밀번호입니다!@#$ |  |
| 28 |  | **ssh** [**allison@172.16.209.133**](mailto:allison@172.16.209.133)  **ls**  **cat flag 5** | Logging into Allison account through SSH | Successfully logged into Allison account and listed down the files and found flag 5 - zhK~bbTLh.6/f2G'[gy%Qu3<k,\*=xwY"/v@.@hz"q`E"3{a4(r | Screenshot 20 & 21 |
| 29 |  | **cd irclogs/localhost/cat kim\_chin\_ho.log** | From Allison account, the irclogs has been inspected | The conversation reveals Allison passing company’s data to a userhandle Kim Chin Ho. In the conversation, Allison mentioned that she has the data, as a reply Kim mentioned korea-dpr.com:7656. Which is a political website. Also, by looking at Allison credentials written in Korean language, it shows the possibility of corporate espionage | Screenshot 22 |

# Recommendations

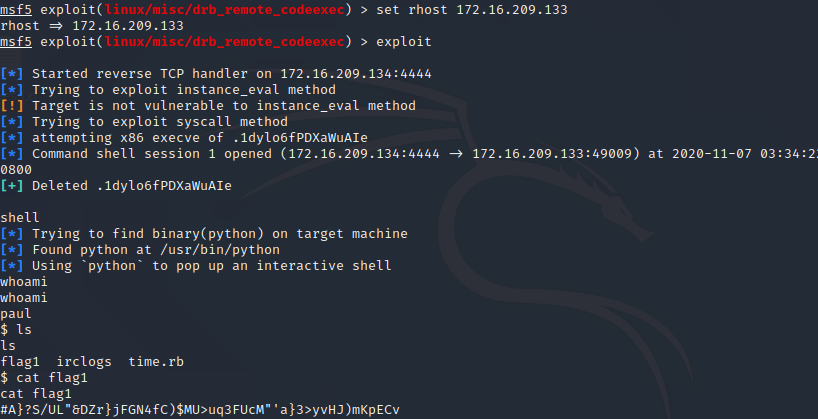
This section includes adequate countermeasures to counter the vulnerabilities identified and reported. The vulnerability score has been calculated based on the Common Vulnerability Scoring System Version 3.1. It is a vendor-neutral open framework to represent the severity of the vulnerability (Cisco, n.d.) . The CVSS calculation has carried on by utilizing the CVSS calculator site from NIST(NIST, n.d.) .The respective ratings for severatiy are None – 0.0, Low 0.1-3.9, Medium 4.0-6.9, High 7.0-8.9, Critical 9.0-10.0

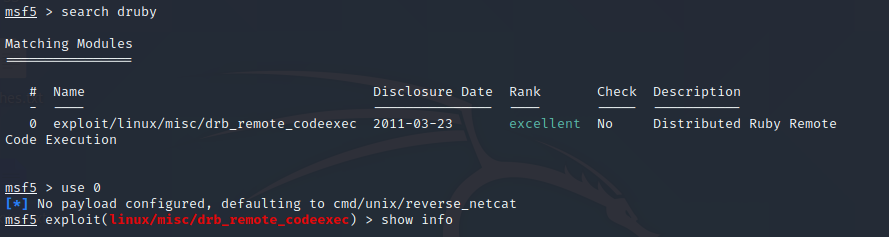
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vulnerability** | **CVSS Score** | **Severity** | **Outcome** | **Mitigation** |
| Corporate Espionage | AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H | Critical 9.8 | Since Allison already had root privileges it’s easy to share the sensitive data outside. Corporate espionage can easily impact the organisation in several ways including revealing trade details, etc… | Since Allison already had the root privileges and enough evidence to prove the corporate espionage, it’s advisable to take legal actions. Also, it’s recommended to revoke all the access from her.  To mitigate this threat conducing SETA program will be a better recommendation (Nancy, 2011) |
| DRUBY RBI Exploit | AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H  CVE 2017-7949 and CVE 2019-10092 | Critical 9.6 | Exploiting this vulnerability allows the attacker to get initial access to the system | The easiest and most recommended mitigation would be applying port filtering (Barry, 2017) and closing |
| Providing higher privileges to unauthorised users | AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H | High 8.4 | Providing root/higher privileges to unwanted users impacts in several ways, and leads to data loss, data destruction, unauthorised access | Usage of employee monitor software.  SETA programs.  Policy audits in periodic intervals |
| Usage of weak credentials | AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H  CWE-521(CWE, 2020) | Critical 9.6 | Dr Balustrade used password Pinky, which is very weak and easy to crack. Using such a weak password allows the attacker to gain control in an easy manner (Paul, 2018) | Implementing enforcement of mixed character password policies and Auto password expiration (CWE, 2020) |
| Storing credentials in cleartext | AV:N/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:N  Unprotected Storage of Credentials | Medium 6.1 | In mysql database the credentials were not encrypted, which affected the confidentiality of data | Encrypting the database,  Hashing the data before storing it into the database. |
| SQL injection | AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | High 8.8 | SQL injection has been performed while finding the flag 4. This vulnerability also allows the attacker to do malicious executions in database | Implementation of Web Application Firewall and Input validation is the most recommended options (PTS, 2018) |

# Appendix

Screenshot 1 Finding target IP

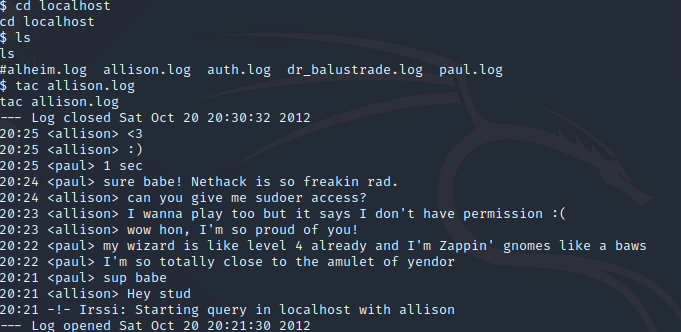
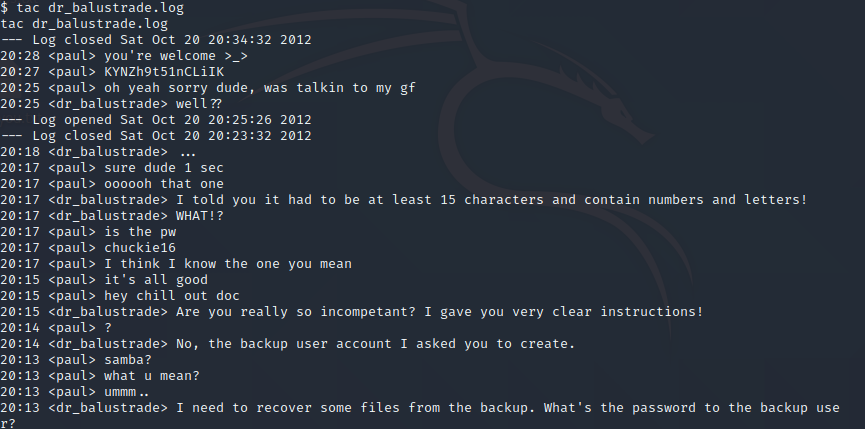
Screenshot 2 Port Scan on Target System





Screenshot 4 Launching exploit and finding flag 1

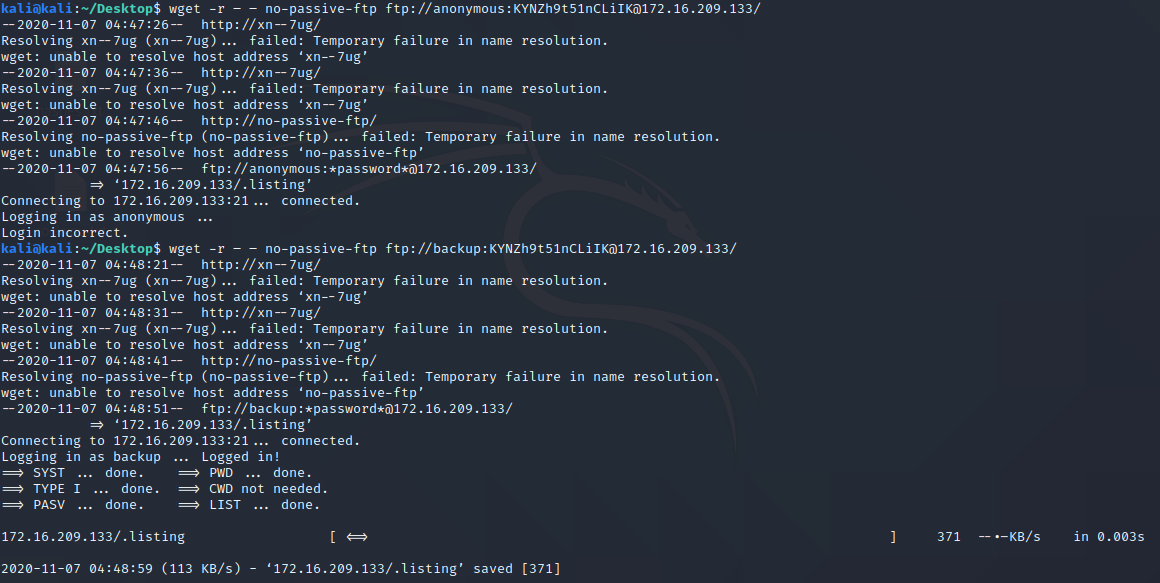
Screenshot 3 Payload Selection

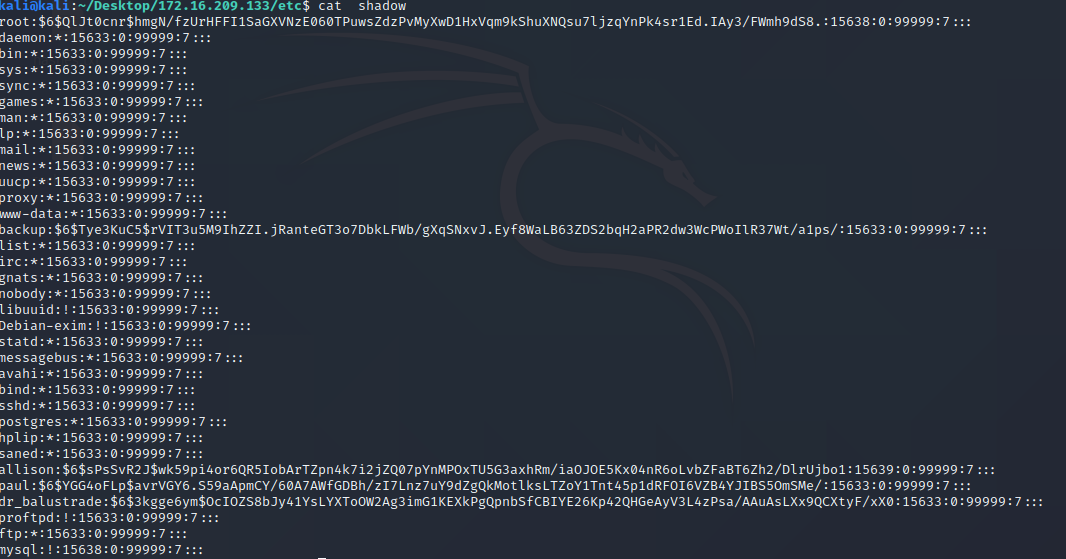
 ‘

Screenshot 5 Paul's chat log with Allison

Screenshot 6 Paul's chat log with Dr Balustrade



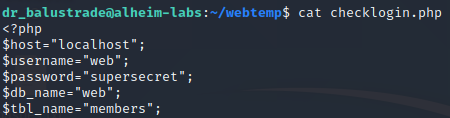




Screenshot 8 Flag 2

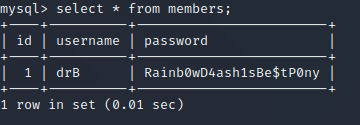
Screenshot 9 Shadow file and hashes

Screenshot 7 Downloading FTP

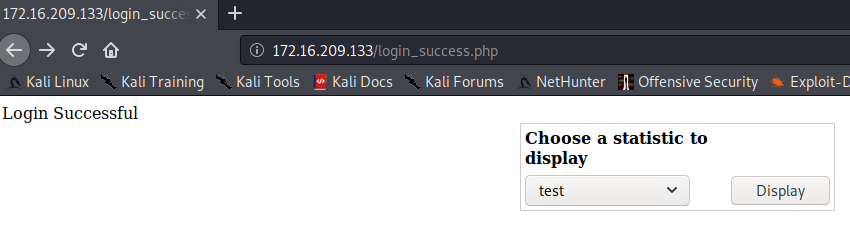


Screenshot 10 Logged into Dr Balustrade SSH and Flag 3

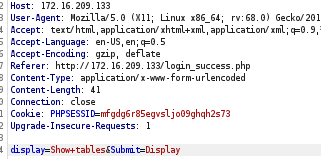
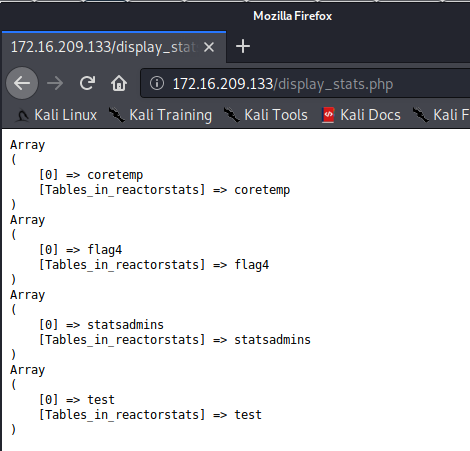
Screenshot 11 Exposure of DB information



Screenshot 12 Login credentials from DB

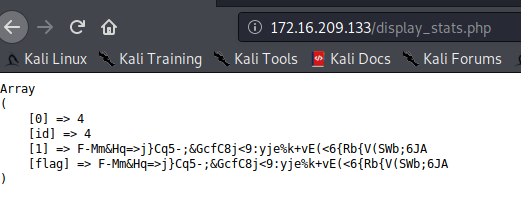


Screenshot 13 Login successful



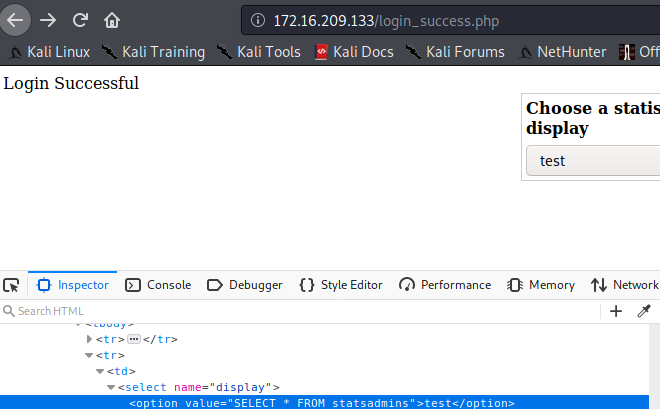
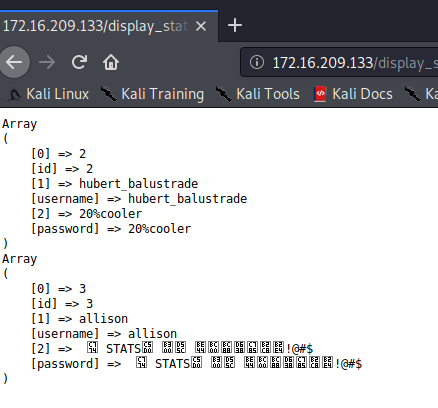
Screenshot 15 Hardcoded information

Screenshot 14 Changing User-Response in burp-suite



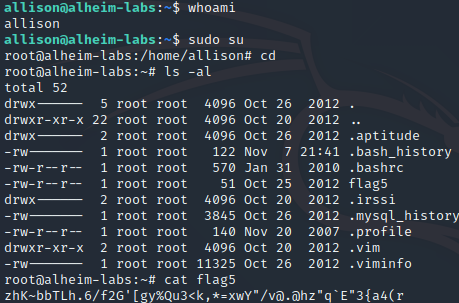
Screenshot 17 Flag 4

Screenshot 16 Inspect element modification for flag 4



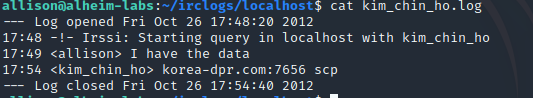
Screenshot 19 Credentials found for Allison

Screenshot 18 Inspect element modification to statsadmin



Screenshot 21 Flag 5

Screenshot 20 SSH login into Allison account



Screenshot 22 Chat log between Allison and Kim

# References

Barry, G. (2017). *Filtering Exploitable Ports and Minimizing Risk to and from Your Customers - SENKI*. SENKI. Retrieved from https://www.senki.org/exploitable-port-filtering/.

Cisco. *Common Vulnerability Scoring System Q & A*. Tools.cisco.com. Retrieved from https://tools.cisco.com/security/center/resources/cvss\_q\_a.html.

CWE. (2020). *CWE - CWE-521: Weak Password Requirements (4.2)*. Cwe.mitre.org. Retrieved from https://cwe.mitre.org/data/definitions/521.html.

Khawaja, G. (2018). *Practical Web Penetration Testing* (p. Chapter 6). Packt Publishing Ltd.

Nancy, J. (2011). *How to Mitigate the Threat of Corporate Espionage*. TCDI. Retrieved from https://www.tcdi.com/mitigating-the-threat-of-corporate-espionage/.

NIST. Nvd.nist.gov. Retrieved from https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator.

Paul, C. (2018). *Weak Passwords are still the Biggest Security Risk - Triella*. Triella. Retrieved from https://www.triella.com/weak-passwords/.

PTES. (2014). *Exploitation - The Penetration Testing Execution Standard*. Pentest-standard.org. Retrieved from http://www.pentest-standard.org/index.php/Exploitation.

PTS. (2018). *How to prevent SQL injection attacks*. Ptsecurity.com. Retrieved https://www.ptsecurity.com/ww-en/analytics/knowledge-base/how-to-prevent-sql-injection-attacks/.

Weidman, G. (2014). *Penetration testing a Hands-on introduction to Hacking*. No Starch Press.