

COMP6544

Network Penetration Testing

Documentation Report

**Quiz 2**

**O223-COMP6544-JF02-01**

# Document Information

|  |  |
| --- | --- |
| Assessment Information | |
| **Assessors** | **Client** |
| Lado Mahardika Cahyono  2440019825 | Software Laboratory Center  Bina Nusantara University  Jalan Kebon Jeruk Raya no. 27  Jakarta Barat, Indonesia |
| **Assessment Period** | |
| 18 Januari 2022 | |

# Assessment Scope

|  |  |
| --- | --- |
| Enumeration | Description |
| Assessment Type | External Black-box |
| Vulnerability Scanner | Kali Linux 2021.2 |
| Server IP Address | **192.168.254.0** |

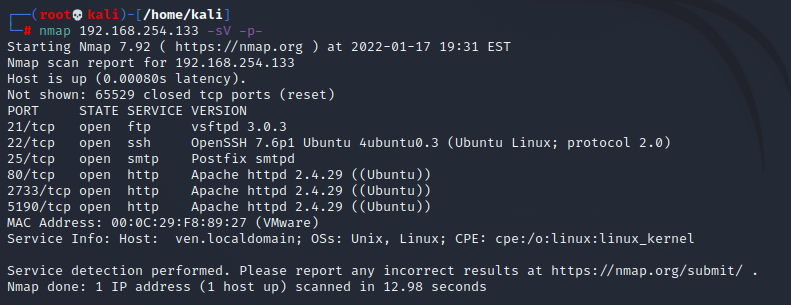
# Executive Summary

## Background

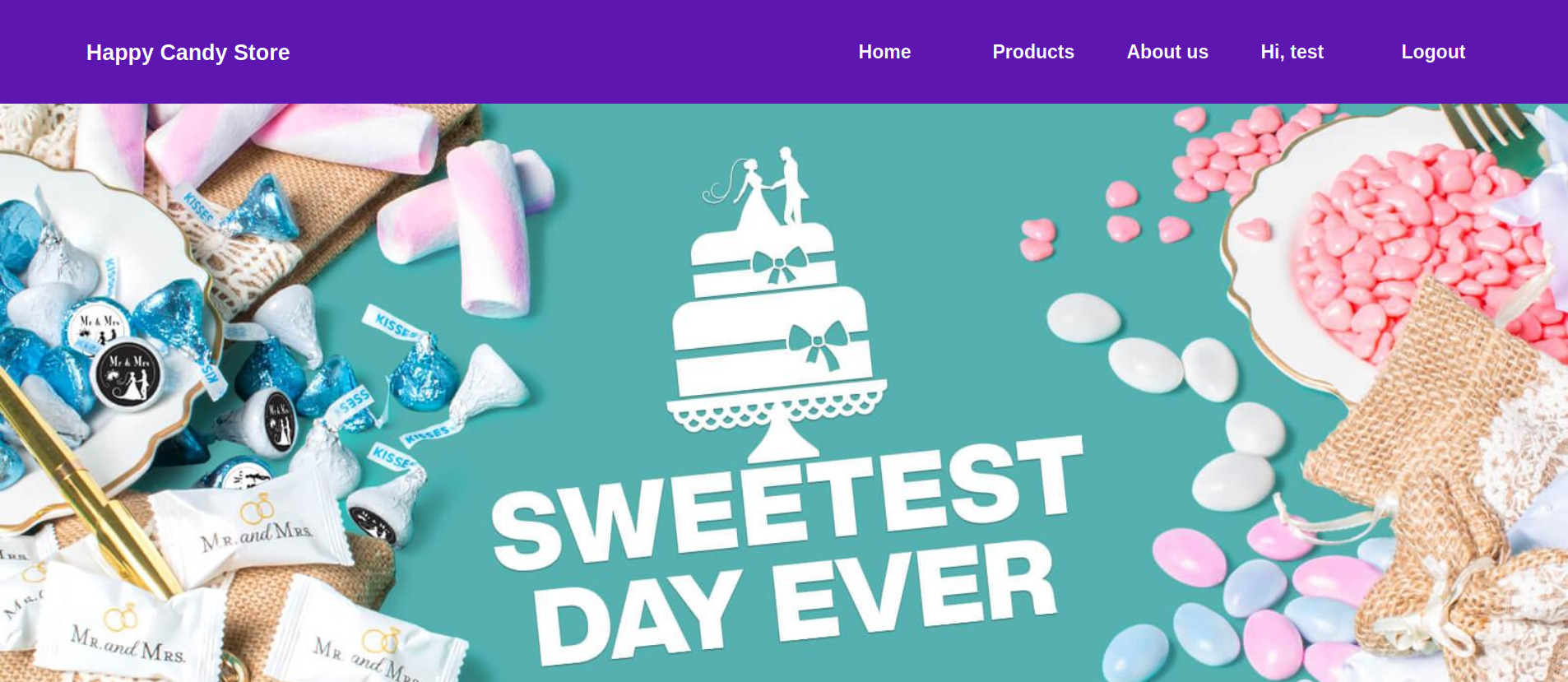
Latar belakang pada Penetration Testing ini adalah untuk menemukan bukti bahwa Happy Candy Store terlibat dalam perdagangan narkoba. Dan bukti nya berbentuk file .cvs dan sudah saya lampirkan pada zip file.

## Summary of Result

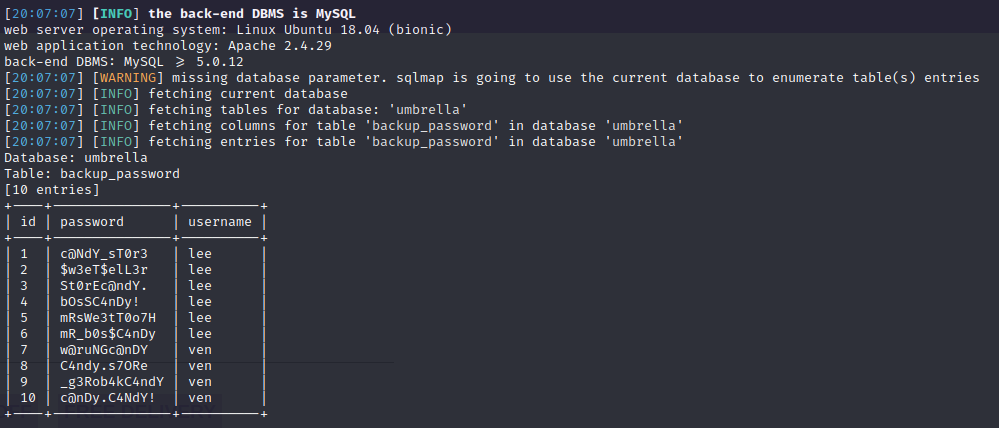
1. Hal pertama yang saya lakukan adalah Enumeration dengan menggunakan tools nmap pada IP server target 192.168.254.133



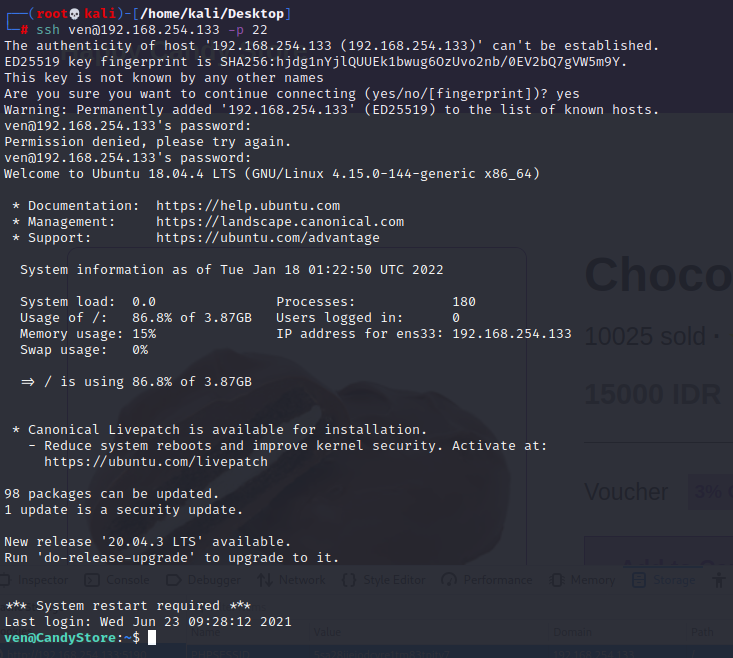
1. Lalu saya ke page yang akan saya serang yaitu port 5190, <http://192.168.254.133:5190/>

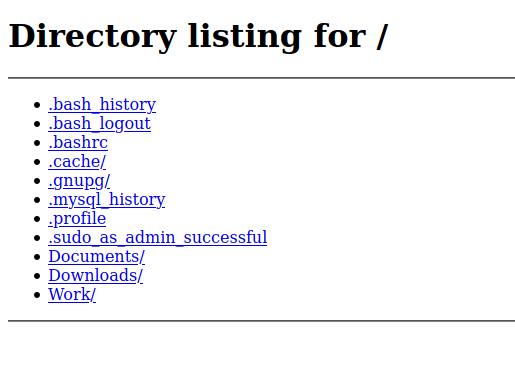


1. Lalu saya ke product page agar URL nya di belakang ada ?id=1 agar dapat di SQLmap. Dan saya mendapatkan hasil dari SQLmap yang berupa username dan password untuk login SSH.



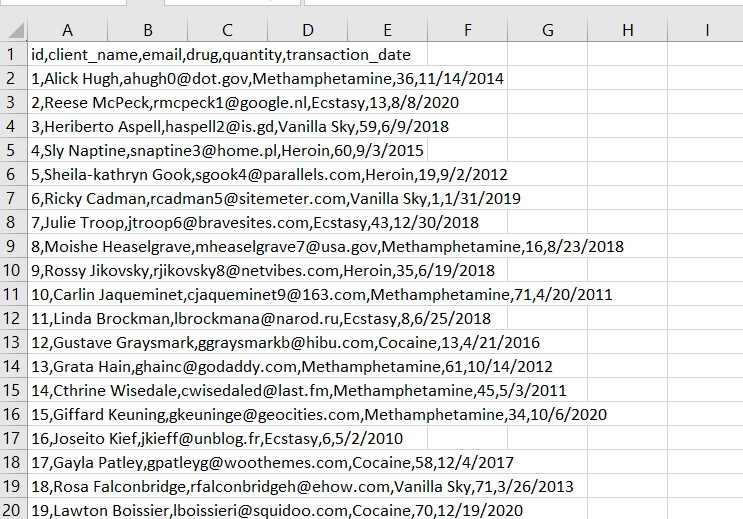
1. Setelah itu saya login ke SSH nya dan mendownload file-fiel yang menjadi bukti perdagangan narkoba.



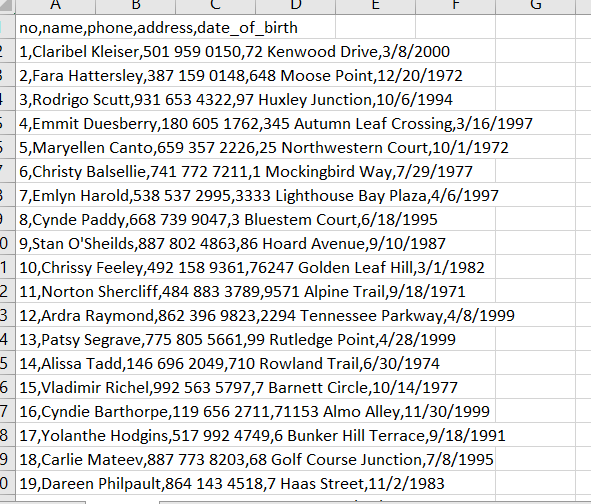


1. Dan saya menemukan file nya yaitu :

transactions.cvs



client.cvs



## Strategic Recommendation

Jadi rekomendasi saya untuk menanggulangi masalah tersebut adalah :

1. Prepared Statement
2. Allow-list Input Validation
3. Escaping All User-Supplied Input
4. Use antivirus
5. Using encryption for SSL
6. Always check for new update server

# Information Gathering

|  |  |
| --- | --- |
| Server IP Address | |
| Command Used | nmap 192.168.254.\* |
| Result |  |
| Description | Setelah saya memakai comman **nmap 192.168.254.\*** saya menemukan beberapa IP sebagai berikut :   1. 192.168.254.1, merupakan gateaway IP saya. 2. 192.168.254.2, merupakan router default IP. 3. 192.168.254.254, merupakan broadcast IP. 4. 192.168.254.130, merupakan IP dari VM saya sendiri.   **192.168.254.133**, yang tersisa terakhir berarti dia merupakan IP target. |

|  |  |
| --- | --- |
| OS Fingerprinting | |
| Command Used | nmap **192.168.254.133** -O |
| Result |  |
| Description | Saya menjalankan command nmap **192.168.254.133** -O untuk mendapatkan informasi tentang OS server target. Dan disini saya menemukan bahwa server target menggunakan OS Linux 4.15 – 5.6. |

|  |  |
| --- | --- |
| All Open Ports and Software Versions | |
| Command Used | nmap **192.168.254.133** -sV -p- |
| Result |  |
| Description | Saya menggunakan command nmap **192.168.254.133** -sV -p- dan saya menemukan ada 3 http service dengan versi Apache http 2.4.29 ((Ubuntu)). Pada port 80, merupakan port dummie. Pada port 2733 dan 5190, adalah service http yang mungkin dipakai. |

|  |  |
| --- | --- |
| Target Web Application Location | |
| Listen Port | 80, 2733, 5190 |
| Preview | port 80    port 2733    port 5190 |
| Description | Saya menggunakan website dengan port 5190, karena port 80 adalah website mati, dan port 2733 adalah Static Website |

# Web Application Penetration Testing

|  |  |
| --- | --- |
| Web Application Penetration and Information Retrieval | |
| Attack Method | SQL Injection for Bypass |
| Payload or Command Used | Pada port 5190, saya mencoba untuk register biasa agar dapat masuk ke website nya dan berhasil  email : [qwerty@gmail.com](mailto:qwerty@gmail.com)  password : 12345 |
| Step-by-Step Action | 1. Saya mencoba untuk masuk ke website dengan register      1. Lalu saya membuat akun dengan nama test;email [qwerty@gmail.com](mailto:qwerty@gmail.com); dan password 12345 2. Lalu saya mencoba login dengan credential tersebut.      1. Dan saya berhasil masuk ke websitenya. |
| Result |  |

|  |  |
| --- | --- |
| Web Application Penetration and Information Retrieval | |
| Attack Method | SQL Injection dengan SQLmap |
| Payload or Command Used | Payload 1  sqlmap -u [http://192.168.254.133:5190/product\_detail.php?id=1--cookie="PHPSESSID=5sa28iiejodcvre1tm83tpjtv7](http://192.168.254.133:5190/product_detail.php?id=1--cookie=%22PHPSESSID=5sa28iiejodcvre1tm83tpjtv7)"  Payload 2  sqlmap -u [http://192.168.254.133:5190/product\_detail.php?id=1--cookie="PHPSESSID=5sa28iiejodcvre1tm83tpjtv7](http://192.168.254.133:5190/product_detail.php?id=1--cookie=%22PHPSESSID=5sa28iiejodcvre1tm83tpjtv7)" –dbs  Payload 3  sqlmap -u [http://192.168.254.133:5190/product\_detail.php?id=1--cookie="PHPSESSID=5sa28iiejodcvre1tm83tpjtv7](http://192.168.254.133:5190/product_detail.php?id=1--cookie=%22PHPSESSID=5sa28iiejodcvre1tm83tpjtv7)" --dump |
| Step-by-Step Action | Payload 1      Disini terlihat bahwa website tersebut dapat kita SQL Injection.  Payload 2    Disini saya menemukan ada 5 database yaitu information\_schema, mysql, performance, sys, umbrella.  Payload 3        Disini saya menemukan database yang penting bernama umbrella dan isinya adalah password dan username untuk login ke server nanti. |
| Result | Berikut adalah hasil yang akan dipakai untuk server exploit. |

*Note: You may add more table if needed. For every attack point, you need to separate the report table.*

# Server Penetration Testing

|  |  |
| --- | --- |
| Server Penetration and Information Retrieval | |
| Attack Method | Hydra |
| Payload / Command Used | hydra -L username.txt -P password.txt ssh://192.168.254.133 -s 22 |
| Step-by-step action |  |
| Result | Hasil nya adalah dengan credential  login : **ven**; password : **mR\_b0s$C4nDy**  Saya bisa masuk ke server melalui service SSH yang terbuka/open. |

*Note: You may add more table if needed*

|  |  |
| --- | --- |
| Retrieval File from Server | |
| Tools Used | Python |
| Command Used | ssh ven@192.168.254.133 -p 22  python3 -m http.server |
| Step-by-step action | 1. Masukkan payload untuk masuk ke server ssh nya.   Payload :  ssh ven@192.168.254.133 -p 22   1. Dan masukkan password dari username ven.   password : **mR\_b0s$C4nDy**   1. Dan saya berhasil masuk sebagai ven. 2. Lalu saya memasukkan payload python3 -m http.server pada service ssh. 3. Lalu saya masuk ke 192.168.254.133:8000.      1. Dan saya berhasil masuk ke directory server. 2. Pada /Work/Business/Financial/, saya menemukan file yang menarik dengan nama transactions.cvs      1. Saya buka isinya dan ternyata betul, ini adalah bukti transaksi narkoba     \*file nya saya masukkan juga pada zip file.   1. Saya juga menemukan ada file yang menarik pada bagian /Work/Transactions/Customers/      1. Isi dari client.cvs     \*file ini akan saya lampirkan pada zip file |
| Result | transactions.cvs  client.cvs |

*Note: You may add more table if needed*