

COMP6544

Network Penetration Testing

Documentation Report

**Quiz 1**

**O223-COMP6544-JF02-01**

# Document Information

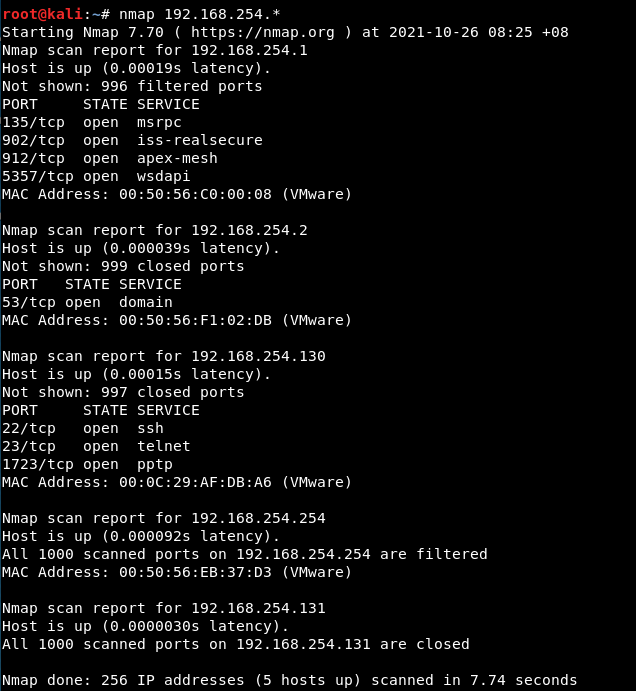
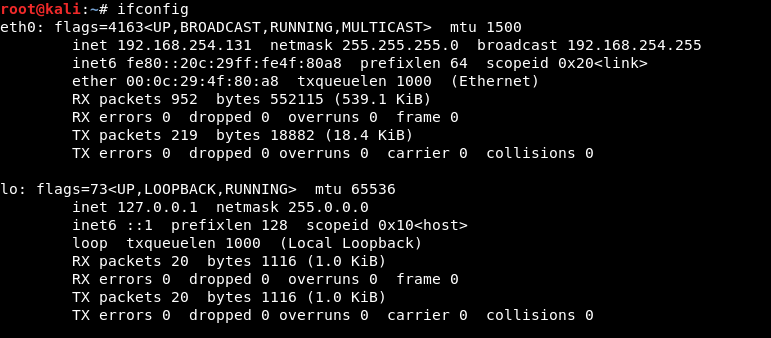
|  |  |
| --- | --- |
| Assessment Information | |
| **Assessors** | **Client** |
| Lado Mahardika Cahyono  2440019825 | Software Laboratory Center  Bina Nusantara University  Jalan Kebon Jeruk Raya no. 27  Jakarta Barat, Indonesia |
| **Assessment Period** | |
| 26 October 2021 | |

# Assessment Scope

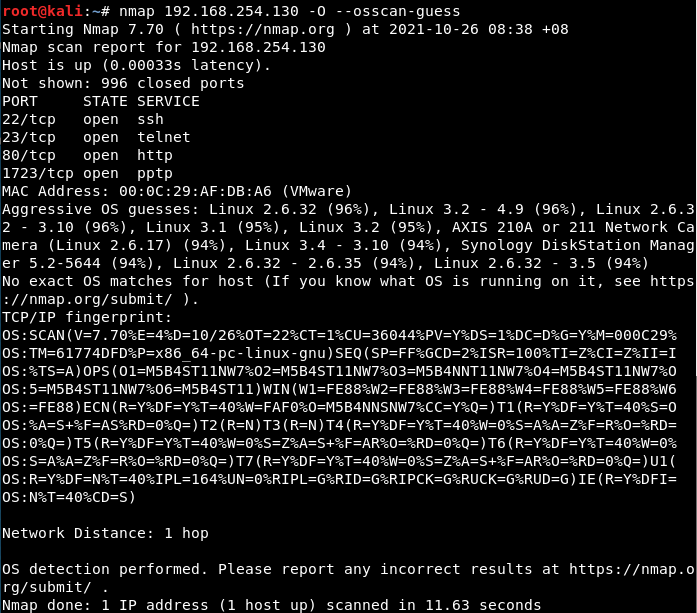
|  |  |
| --- | --- |
| Enumeration | Description |
| Assessment Type | External Black-box |
| Vulnerability Scanner | Kali Linux 2019.1 |
| Network IP Address | **192.168.254.0** |

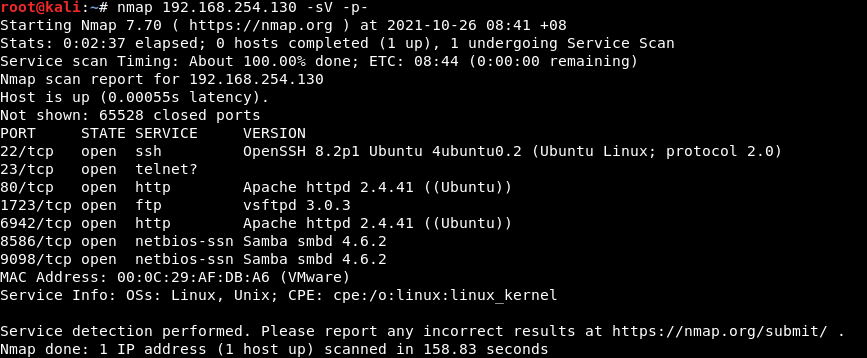
# Executive Summary

## Summary of Result

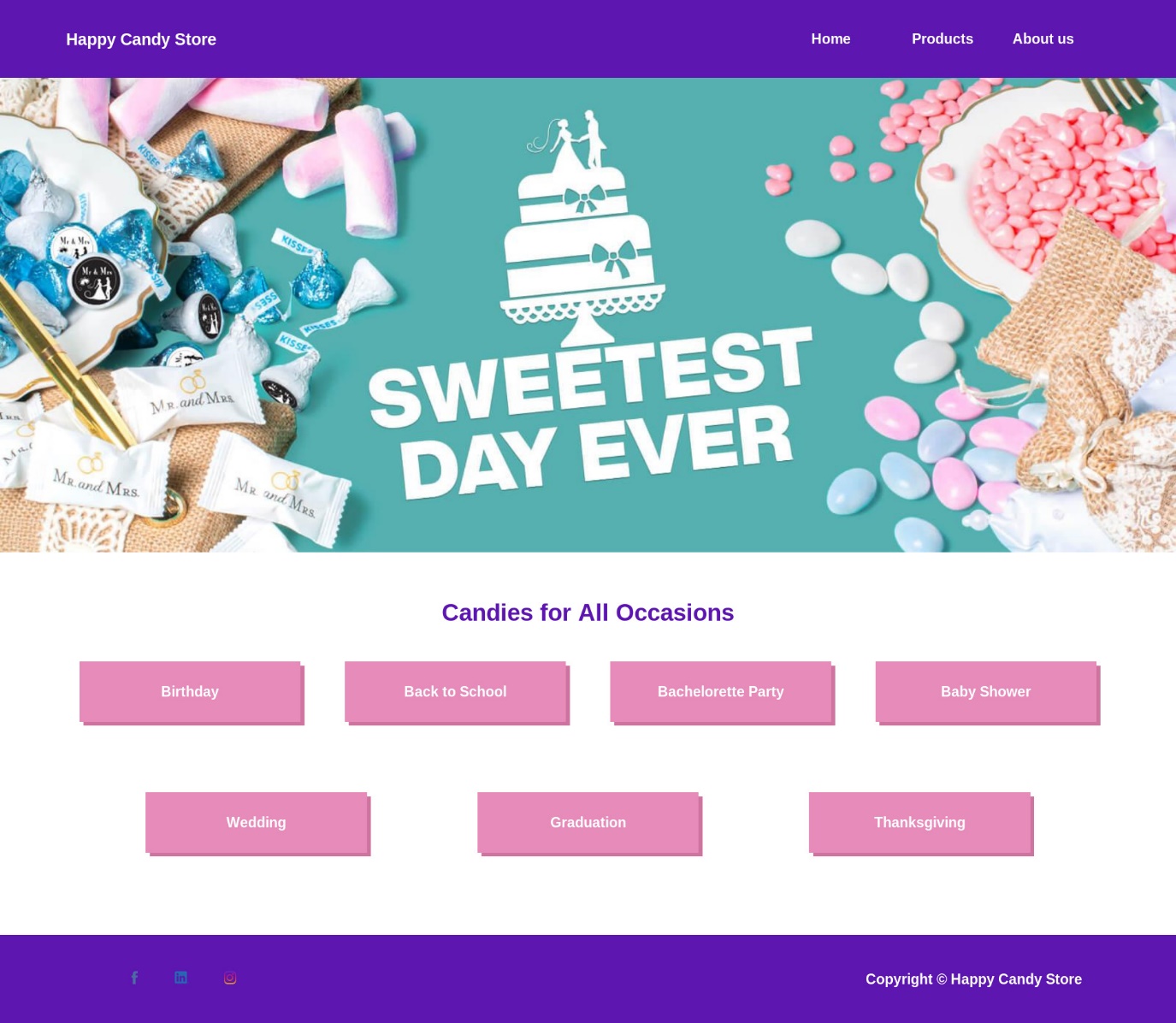
Setelah saya mendapatkan IP saya dengan cara “**ifconfig”**, saya melanjutkan dengan menggunakan nmap untuk mencari IP target dengan command “**nmap 192.168.254.\*”**. Dan saya menemukan IP target yang merupakan 192.168.254.130. Berikut hasil comman nya :

Lalu saya lanjut untuk mengetahui OS apa yang dipakai oleh target dengan menggunakan comman **“nmap 192.168.254.130 -O”** tapi dengan menggunakan comman itu saya tidak bisa mendapatkan exact OS nya jadi saya menggunakan command **“nmap 192.168.254.130 --osscan-guess -O”** dan mendapatkan kira-kira OS apa yang dipakai oleh target, dan ternyata target menggunakan OS Linux 2.6.32. Berikut hasil nya :

 Setelah mendapat OS nya saya, mau mengetahui versi service apa saja yang dipakai dan pr tapa yang terbuka dengan command **“nmap 192.168.254.130 -sV -p-“** dan saya mendapatkan bahwa ada 2 port untuk html yaitu port 80 dan port 6942, berikut hasilnya :



Setelah itu saya mencoba untuk membuka websitenya dengan memasukkan **“http://192.168.254.130:6942/”,** berikut hasilnya :

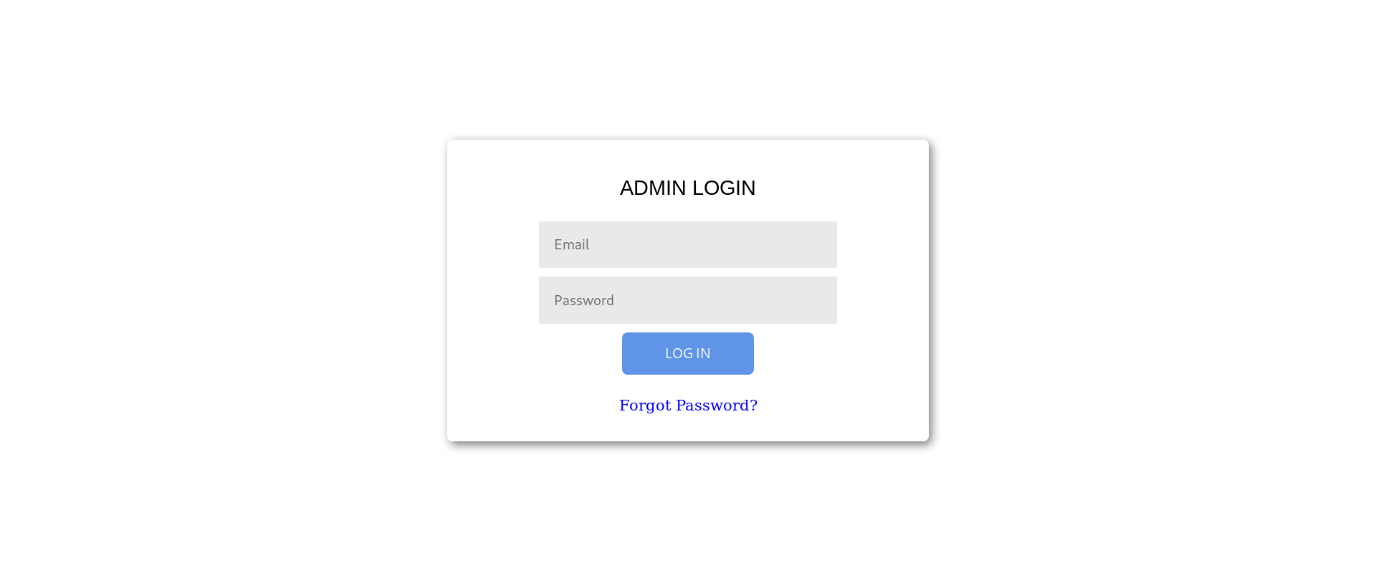


Lalu saya mau mencari apakah ada hidden file dan hidden page dalam website tersebut, jadi saya memakai tools **dirbuster** dengan input website nya **“http://192.168.254.130:6942/”** dengan wordlist **“/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt”** dan extention yang saya pakai **“txt, csv, xlsx, xls, doc, docx, pptx, rtf, pdf, wpd, dat, xml, html, log”**. Tapi waktu untuk menemukan hidden file nya tidak cukup untuk VM saya, saya hanya menemukan hidden pagenya berikut hasilnya :

<http://192.168.254.130:6942/admin/administration.html>



<http://192.168.254.130:6942/secret/account_login.html>



# 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. 192.168.254.131, merupakan IP dari VM saya sendiri. 5. 192.168.254.130, yang tersisa terakhir berarti dia merupakan IP target. |

|  |  |
| --- | --- |
| OS Fingerprinting | |
| Command Used | nmap 192.168.254.130 -O  nmap 192.168.254.130 -O --osscan-guess |
| Result |  |
| Description | Saat saya menjalankan command biasa yaitu **nmap 192.168.254.130 -O**, saya tidak bisa mendapatkan exact matchnya. Dan akhirnya saya memakai **nmap 192.168.254.130 --osscan-guess -O** dan mendapatkan bahwa OS yang dipakai target adalah Linux 2.6.32 |

|  |  |
| --- | --- |
| Software Version | |
| Command Used | nmap 192.168.254.130 -sV -p- |
| Result |  |
| Description | Saya menjalankan comman **192.168.254.130 -sV -p-,** -sV untuk mendapatkan versi dari setiap servicenya, dan -p- untuk menpadatkan semua port yang server target punya. Dan disini saya mendapatkan bahwa ada 2 port untuk http 80 dan 6942. Yang 80 merupakan dummie. |

|  |  |
| --- | --- |
| Target Web Application Location | |
| Listen Port | 6942 |
| Preview |  |
| Description | Berikut merupakan hidden website dari Happy Candy Store. |

# Web Enumeration

|  |  |
| --- | --- |
| Web Application Content Discovery | |
| Tools Used | dirbuster |
| Payload | **/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt** |
| Step-by-step action | 1. Buka dirbuster 2. Masukkan [**http://192.168.254.130:6942/**](http://192.168.254.130:6942/)**.** 3. Lalu masukkan wordlistnya, saya menggunakan **/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt.** 4. Lalu masukkan extention nya, **txt, csv, xlsx, xls, doc, docx, pptx, rtf, pdf, wpd, dat, xml, html, log.** 5. Lalu start. |
| Result | saya hanya mendapatkan secret page nya karena tidak cukup waktunya :  <http://192.168.254.130:6942/secret/account_login.html>  <http://192.168.254.130:6942/admin/administration.html> |
| Description | Saya menemukan hidden page yang menjual drugsnya (<http://192.168.254.130:6942/admin/administration.html>) dan login admin nya (<http://192.168.254.130:6942/secret/account_login.html>) |