



# COMP6544

## Network Penetration Testing

### Documentation Report

---

#### Quiz 1

## Document Information

Assessment Information	
Assessors	Client
Leonhard Andrew 2440112872	Software Laboratory Center Bina Nusantara University Jalan Kebon Jeruk Raya no. 27 Jakarta Barat, Indonesia
Assessment Period	
26 Oktober 2021	

## Assessment Scope

Enumeration	Description
Assessment Type	External Black-box
Vulnerability Scanner	Kali Linux 2019.1
Network IP Address	<b>192.168.136.128</b>

## Executive Summary

### Summary of Result

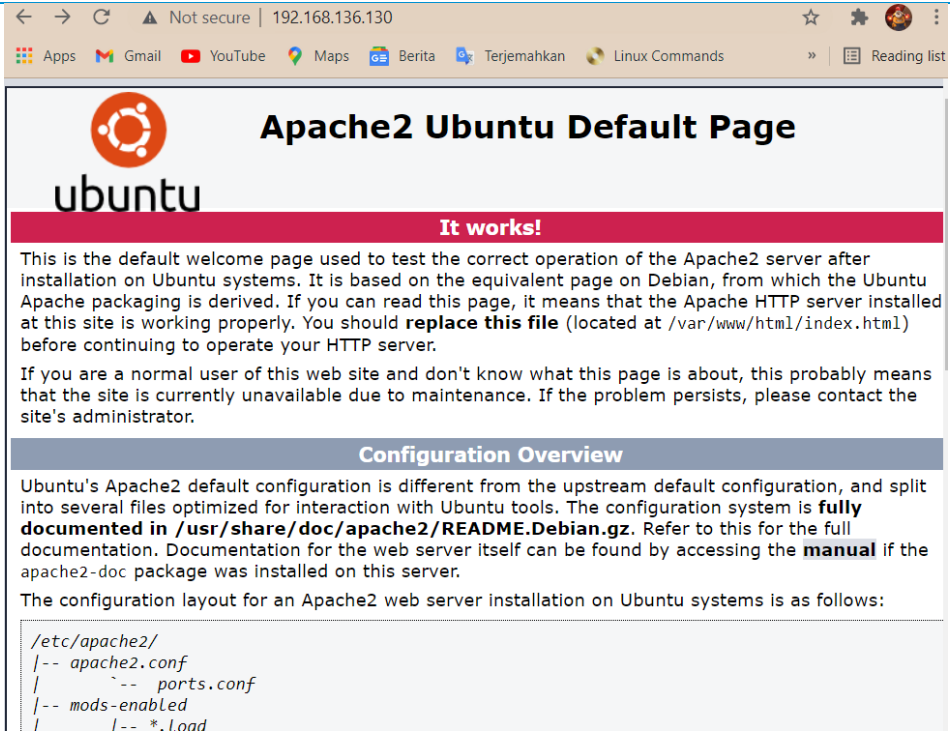
Jadinya pertama kali kita memakai nmap untuk scan ip kita untuk menemukan ip target nya. Setelah kita menemukan ip target nya melalui nmap, sekarang kita nmap ip target nya untuk mengetahui port mana saja yang terbuka. Setelah kita mengetahui port mana saja yang terbuka, kita tau kelemahan website tersebut. Setelah itu kita mencari hidden directory dari website tersebut untuk mengetahui hidden page yang terdapat di website tersebut.

## Information Gathering

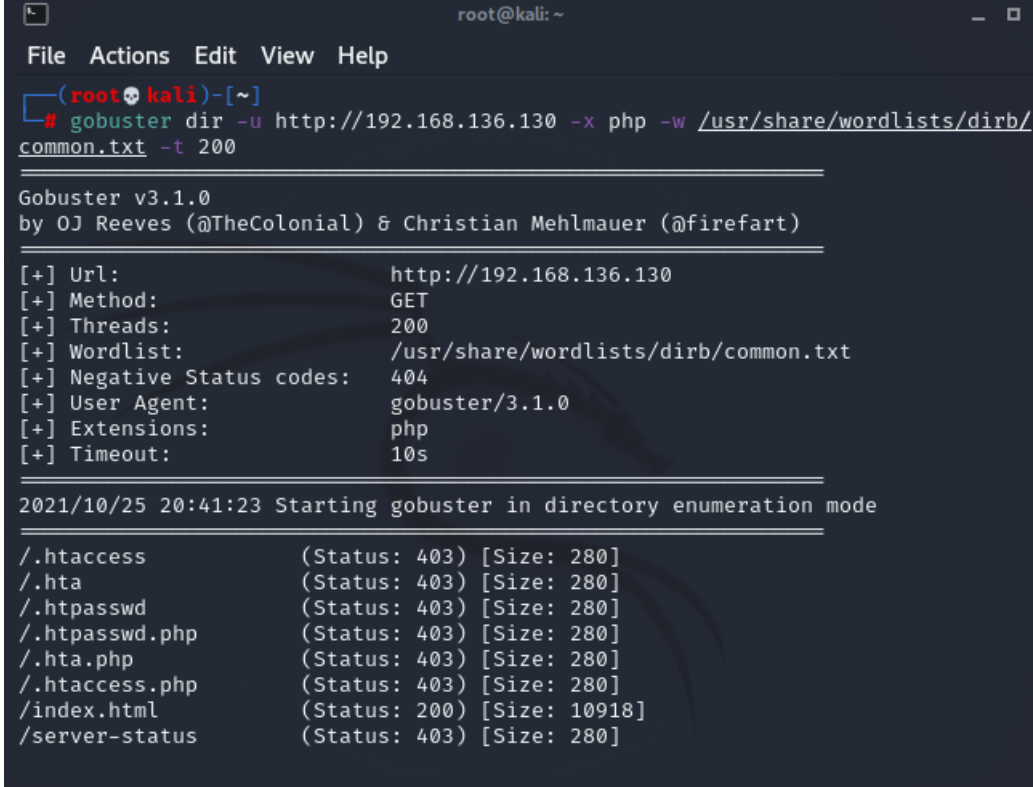
Server IP Address	
Command Used	Nmap 192.168.136.128
Result	<pre> (root@kali)-[~] # nmap 192.168.136.128/24 Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-25 20:29 EDT Nmap scan report for 192.168.136.1 Host is up (0.00067s latency). Not shown: 997 filtered ports PORT      STATE SERVICE 135/tcp    open  msrpc 902/tcp    open  iss-realsecure 912/tcp    open  apex-mesh MAC Address: 00:50:56:C0:00:08 (VMware)  Nmap scan report for 192.168.136.2 Host is up (0.000075s latency). Not shown: 999 closed ports PORT      STATE SERVICE 53/tcp    open  domain MAC Address: 00:50:56:FA:85:A9 (VMware)  Nmap scan report for 192.168.136.130 Host is up (0.00025s latency). Not shown: 996 closed ports PORT      STATE SERVICE 22/tcp    open  ssh 23/tcp    open  telnet 80/tcp    open  http 1723/tcp  open  pptp MAC Address: 00:0C:29:A6:39:F3 (VMware)  Nmap scan report for 192.168.136.254 Host is up (0.00026s latency). All 1000 scanned ports on 192.168.136.254 are filtered MAC Address: 00:50:56:F4:8C:C7 (VMware)  Nmap scan report for 192.168.136.128 Host is up (0.0000020s latency). All 1000 scanned ports on 192.168.136.128 are closed  Nmap done: 256 IP addresses (5 hosts up) scanned in 11.98 seconds </pre>
Description	<p>Saya memakai nmap lalu menembak ip saya sendiri untuk mengetahui ip apa saja yang terdapat pada jaringan saya</p> <p>192.168.136.128 merupakan ip saya</p> <p>192.168.136.2 merupakan ip vmware</p> <p>192.168.138.130 merupakan ip target karena kita mengetahui disitu terdapat ssh</p>

OS Fingerprinting	
Command Used	Nmap -sV 192.168.136.130
Result	<pre> (root@kali)-[~] # nmap -sV 192.168.136.130 Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-25 20:37 EDT Nmap scan report for 192.168.136.130 Host is up (0.00015s latency). Not shown: 996 closed ports PORT      STATE SERVICE VERSION 22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; prot 2.0) 23/tcp    open  telnet   Linux telnetd 80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu)) 1723/tcp  open  ftp      vsftpd 3.0.3 MAC Address: 00:0C:29:A6:39:F3 (VMware) Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel  Service detection performed. Please report any incorrect results at https: p.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds </pre>
Description	Saya memakai nmap dengan perintah -sV untuk mengetahui mana-mana saja port yang terbuka dan version nya berapa agar mengetahui website tersebut sudah memakai system keamanan yang terbaru atau belum.

Software Version	
Command Used	Nmap -sV 192.168.136.130
Result	<pre> (root@kali)-[~] # nmap -sV 192.168.136.130 Starting Nmap 7.91 ( https://nmap.org ) at 2021-10-25 20:37 EDT Nmap scan report for 192.168.136.130 Host is up (0.00015s latency). Not shown: 996 closed ports PORT      STATE SERVICE VERSION 22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0) 23/tcp    open  telnet   Linux telnetd 80/tcp    open  http     Apache httpd 2.4.41 ((Ubuntu)) 1723/tcp  open  ftp      vsftpd 3.0.3 MAC Address: 00:0C:29:A6:39:F3 (VMware) Service Info: OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel  Service detection performed. Please report any incorrect results at https://nma p.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 14.62 seconds </pre>
Description	<p>Untuk mengetahui version berapa</p> <p>Port 22 merupakan ssh dengan version OpenSSH 8.2p1 dan status nya open</p> <p>Port 80 merupakan http dengan version apache 2.4.41 dan status nya open</p> <p>Port 23 merupakan telnet dengan version linux dan statusnya open</p> <p>Port 1723 merupakan ftp dengan version vsftpd 3.0.3 dan statusnya open</p>

Target Web Application Location	
Listen Port	80
Preview	 <p>The screenshot shows a web browser displaying the Apache2 Ubuntu Default Page. The page has a blue header with the Ubuntu logo and the text 'Apache2 Ubuntu Default Page'. Below the header, there is a red banner that says 'It works!'. The main content area contains text explaining that this is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It also mentions that the configuration system is fully documented in /usr/share/doc/apache2/README.Debian.gz. At the bottom, there is a section titled 'Configuration Overview' which provides a brief overview of the configuration layout for an Apache2 web server installation on Ubuntu systems, including a list of files and directories to be checked.</p>
Description	Kita sudah menemukan website nya

## Web Enumeration

Web Application Content Discovery	
Tools Used	Gostbuster
Payload	Wordlist common.txt
Step-by-step action	Gobuster dir -u http://192.168.136.130 -x php -w /usr/share/wordlists/dirb/common.txt -t 200
Result	 <pre> root@kali: ~ File Actions Edit View Help (root@kali)-[~] # gobuster dir -u http://192.168.136.130 -x php -w /usr/share/wordlists/dirb/ common.txt -t 200  Gobuster v3.1.0 by OJ Reeves (@TheColonial) &amp; Christian Mehlmauer (@firefart)  [+] Url: http://192.168.136.130 [+] Method: GET [+] Threads: 200 [+] Wordlist: /usr/share/wordlists/dirb/common.txt [+] Negative Status codes: 404 [+] User Agent: gobuster/3.1.0 [+] Extensions: php [+] Timeout: 10s  2021/10/25 20:41:23 Starting gobuster in directory enumeration mode  /.htaccess (Status: 403) [Size: 280] /.hta (Status: 403) [Size: 280] /.htpasswd (Status: 403) [Size: 280] /.htpasswd.php (Status: 403) [Size: 280] /.hta.php (Status: 403) [Size: 280] /.htaccess.php (Status: 403) [Size: 280] /index.html (Status: 200) [Size: 10918] /server-status (Status: 403) [Size: 280] </pre>
Description	<p>Saya memakai gobuster untuk mencari hidden file directory. Saya memakai command -u untuk IP lalu -x untuk extension nya lalu -w untuk wordlist nya dan -t untuk kecepatan nya.</p> <p>Lalu kita menemukan directory</p> <ul style="list-style-type: none"> <li>/.htaccess</li> <li>/.hta</li> <li>/.htpasswd</li> <li>/.htpasswd.php</li> <li>/.hta.php</li> <li>/.htaccess.php</li> <li>/index.html</li> <li>/server-status</li> </ul> <p>Dan index.html yang</p>