



COMP6544

Network Penetration Testing

Documentation Report

Quiz 1

O223-COMP6544-LT03-01

Document Information

Assessment Information	
Assessors	Client
Maximilianus Raymond Kusnadi 2440040904	Software Laboratory Center Bina Nusantara University Jalan Kebon Jeruk Raya no. 27 Jakarta Barat, Indonesia
Assessment Period	
Thursday, October 28, 2021	

Assessment Scope

Enumeration	Description
Assessment Type	External Black-box
Vulnerability Scanner	Kali Linux 2019.1
Network IP Address	192.168.232.0

Executive Summary

Summary of Result

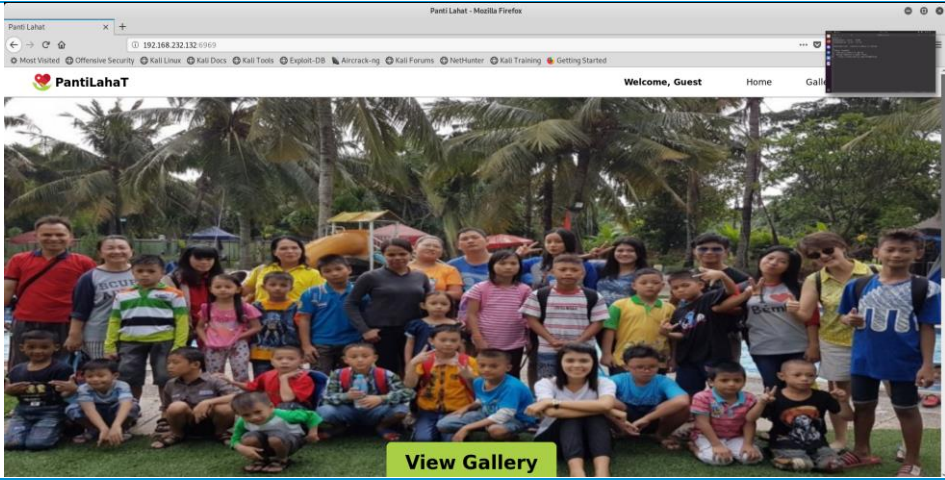
- ➔ Yang pertama, nmap 192.168.232.0-255, untuk IP yang terlihat mencurigakan.
- ➔ Yang kedua, nmap 192.168.232.132 -O -ossan-guess, untuk melihat jenis OS yang digunakan oleh IP tersebut.
- ➔ Yang ketiga, nmap 192.168.232.132 -sV -p- untuk melihat port mana didalam IP tersebut yang mencurigakan

Information Gathering

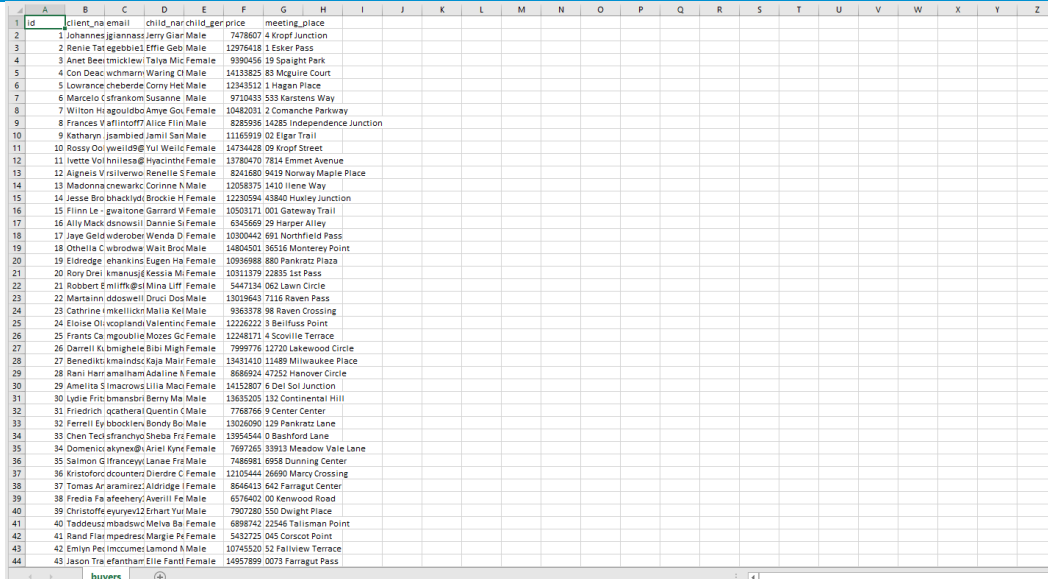
Server IP Address	
Command Used	<code>nmap 192.168.232.0-255</code>
Result	<pre> root@kali:~# nmap 192.168.232.0-255 Starting Nmap 7.70 (https://nmap.org) at 2021-10-28 14:29 +08 Nmap scan report for 192.168.232.1 Host is up (0.00071s latency). Not shown: 996 filtered ports PORT STATE SERVICE 80/tcp open http 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds MAC Address: 00:50:56:C0:00:08 (VMware) Nmap scan report for 192.168.232.2 Host is up (0.00011s latency). Not shown: 999 closed ports PORT STATE SERVICE 53/tcp open domain MAC Address: 00:50:56:F3:5F:D7 (VMware) Nmap scan report for 192.168.232.132 Host is up (0.00025s latency). Not shown: 994 closed ports PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http 111/tcp open rpcbind 2049/tcp open nfs 6969/tcp open acmsoda MAC Address: 00:0C:29:52:35:B2 (VMware) Nmap scan report for 192.168.232.254 Host is up (0.00016s latency). All 1000 scanned ports on 192.168.232.254 are filtered MAC Address: 00:50:56:F3:35:6D (VMware) Nmap scan report for 192.168.232.131 Host is up (0.0000020s latency). All 1000 scanned ports on 192.168.232.131 are closed Nmap done: 256 IP addresses (5 hosts up) scanned in 7.84 seconds </pre>
Description	Terdapat IP yang akan di lakukan pentest yaitu pada IP 192.168.232.132

OS Fingerprinting	
Command Used	<code>nmap 192.168.232.132 -O -osscan-guess</code>
Result	<pre> root@kali:~# nmap 192.168.232.132 -O --osscan-guess Starting Nmap 7.70 (https://nmap.org) at 2021-10-28 14:36 +08 Nmap scan report for 192.168.232.132 Host is up (0.00046s latency). Not shown: 994 closed ports PORT STATE SERVICE 21/tcp open ftp 22/tcp open ssh 80/tcp open http 111/tcp open rpcbind 2049/tcp open nfs 6969/tcp open acmsoda MAC Address: 00:0C:29:52:35:B2 (VMware) Aggressive OS guesses: Linux 2.6.32 (96%), Linux 3.2 - 4.9 (96%), Linux 2.6.32 - 3.10 (96%), Linux 3.4 - 3.10 (95%), Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), Synology DiskStation Manager 5.2-5644 (94%), Netgear RAIDiator 4.2.28 (94%), Linux 2.6.32 - 2.6.35 (94%) No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/). TCP/IP fingerprint: OS:SCAN(V=7.70%E=4%D=10/28%OT=21%CT=1%CU=30232%PV=Y%DS=1%DC=D%G=Y%M=000C29% OS:TM=617A44E6%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10A%TI=Z%CI=Z%II= OS:I%TS=A)OPS(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7% OS:O5=M5B4ST11NW7%O6=M5B4ST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W OS:6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S= OS:0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%RD OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0 OS:S=A%A=Z%F=R%O=0%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)U1 OS:(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI OS:=N%T=40%CD=S) Network Distance: 1 hop OS detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 11.80 seconds </pre>
Description	Berdasarkan OS Guess operating system yang digunakan adalah Linux 2.6.32, karena tidak ada operating system yang exact match.

Software Version	
Command Used	<code>nmap 192.168.232.132 -sV -p-</code>
Result	<pre> root@kali:~# nmap 192.168.232.132 -sV -p- Starting Nmap 7.70 (https://nmap.org) at 2021-10-28 14:46 +08 Nmap scan report for 192.168.232.132 Host is up (0.0010s latency). Not shown: 65523 closed ports PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 3.0.3 22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0) 80/tcp open http Apache httpd 2.4.41 ((Ubuntu)) 111/tcp open rpcbind 2-4 (RPC #100000) 2049/tcp open nfs_acl 3 (RPC #100227) 2224/tcp open netbios-ssn Samba smbd 4.6.2 2240/tcp open netbios-ssn Samba smbd 4.6.2 6969/tcp open http Apache httpd 2.4.41 ((Ubuntu)) 42387/tcp open nlockmgr 1-4 (RPC #100021) 45595/tcp open mountd 1-3 (RPC #100005) 56845/tcp open mountd 1-3 (RPC #100005) 59887/tcp open mountd 1-3 (RPC #100005) MAC Address: 00:0C:29:52:35:B2 (VMware) Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 51.16 seconds </pre>
Description	Terdapat service yang mencurigakan didalam IP tersebut.

Target Web Application Location	
Listen Port	6969
Preview	
Description	Website yang terdapat dalam server tersebut merupakan website Panti asuhan yang bernama PantiLahaT

Web Enumeration

Web Application Content Discovery	
Tools Used	dirbuster
Payload	child children human humans orphan orphans patient patients people peoples orphanage buy buyer buyers sell seller sellers
Step-by-step action	Jadi, Step pertama nya kita buka dirbuster terlebih dahulu, Lalu klik pada bagian target URL yang diminta masukan web nya ketik http://192.168.232.132:6969 , Lalu pilih file wordlist yang sudah dibuat, Lalu masukan berbagai jenis file extension seperti pptx,docx,csv,xlsx,pdf. Lalu klik start
Result	
Description	Terdapat sebuah file yang berextension csv yang berisikan tentang informasi mengenai transaksi perdagangan manusia yang dilakukan.

