Pentest BKPM Production (private network)

IP: 10.50.1.96 (perlu vpn)
host : pdn-portal-satudata
tools : nmap

Result

1. **Ping Scan**

```
PS C:\Users\saya> nmap -sn 10.50.1.96
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 14:36 SE Asia Standard Time
Nmap scan report for 10.50.1.96
Host is up (0.00s latency).
MAC Address: 02:50:41:00:00:02 (Unknown)
Nmap done: 1 IP address (1 host up) scanned in 32.03 seconds
PS C:\Users\saya>
```

Nmap scan report for 10.50.1.96
***Host is up** (0.00s latency).*
MAC Address: 02:50:41:00:00:02

Dari pengecekan IP 10.50.1.96 online.

2. **Tes Port Opened**

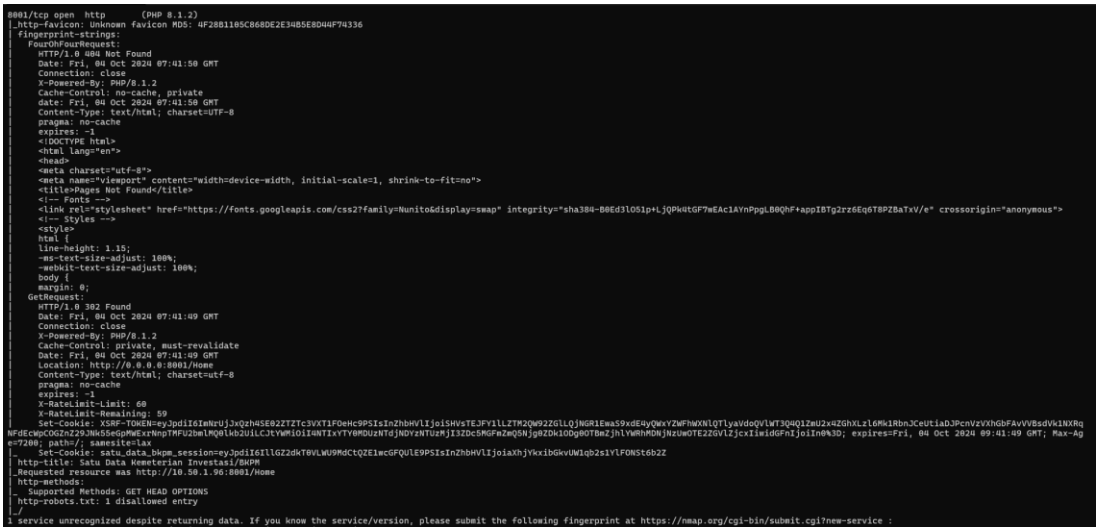
```
PS C:\Users\saya> nmap -T4 -sS 10.50.1.96
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 14:37 SE Asia Standard Time
Nmap scan report for 10.50.1.96
Host is up (0.0073s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
5432/tcp open  postgresql
8001/tcp open  vcom-tunnel
MAC Address: 02:50:41:00:00:02 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 33.75 seconds
```

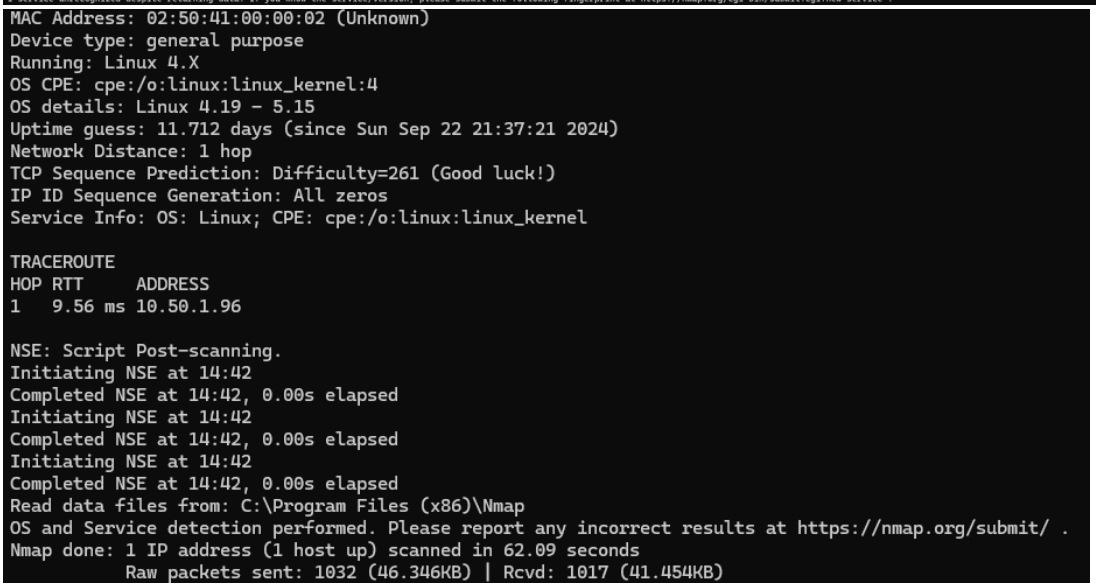
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
5432/tcp open postgresql
8001/tcp open vcom-tunnel

Dari pengecekan IP 10.50.1.96 terdapat 4 port yang terbuka secara private network.

3. **Additional Services (OS – dan lainnya)**

```
PS C:\Users\saya> nmap -T4 -A -v -osscan-guess 10.50.1.96
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 14:41 SE Asia Standard Time
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:41
Completed NSE at 14:41, 0.00s elapsed
Initiating NSE at 14:41
Completed NSE at 14:41, 0.00s elapsed
Initiating NSE at 14:41
Completed NSE at 14:41, 0.00s elapsed
Initiating ARP Ping Scan at 14:41
Scanning 10.50.1.96 [1 port]
Completed ARP Ping Scan at 14:41, 0.14s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:41
Completed Parallel DNS resolution of 1 host. at 14:41, 0.02s elapsed
Initiating SYN Stealth Scan at 14:41
Scanning 10.50.1.96 [1000 ports]
Discovered open port 22/tcp on 10.50.1.96
Discovered open port 80/tcp on 10.50.1.96
Discovered open port 5432/tcp on 10.50.1.96
Discovered open port 8001/tcp on 10.50.1.96
Completed SYN Stealth Scan at 14:41, 0.20s elapsed (1000 total ports)
Initiating Service scan at 14:41
Scanning 4 services on 10.50.1.96
Completed Service scan at 14:42, 20.07s elapsed (4 services on 1 host)
Initiating OS detection (try #1) against 10.50.1.96
NSE: Script scanning 10.50.1.96.
Initiating NSE at 14:42
Completed NSE at 14:42, 5.52s elapsed
Initiating NSE at 14:42
Completed NSE at 14:42, 1.49s elapsed
Initiating NSE at 14:42
Completed NSE at 14:42, 0.00s elapsed
Nmap scan report for 10.50.1.96
Host is up (0.0096s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 b4:7c:3d:a9:6a:ae:7f:e4:37:57:93:be:2f:63:3f:c0 (ECDSA)
|_  256 c6:d5:d0:7a:75:dd:8b:7c:3e:de:72:04:b3:66:2f:9b (ED25519)
80/tcp   open  http       nginx
|_http-title: 403 Forbidden
5432/tcp open  postgresql PostgreSQL DB 16.0 - 16.2
| ssl-cert: Subject: commonName=pdn-portal-satudata
| Subject Alternative Name: DNS:pdn-portal-satudata
| Issuer: commonName=pdn-portal-satudata
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2024-06-19T05:20:57
| Not valid after:  2034-06-17T05:20:57
| MD5:   8497:06fa:1d8a:a008:b3d1:4008:c393:1efd
|_SHA-1: 442f:1a0b:3aea:fcc3:7b5e:7a3e:1956:9584:c2d1:145b
|_ssl-date: TLS randomness does not represent time
```





PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp open http nginx
5432/tcp open postgresql PostgreSQL DB 16.0 - 16.2
8001/tcp open http (PHP 8.1.2)

Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4
OS details: Linux 4.19 - 5.15
Uptime guess: 11.712 days (since Sun Sep 22 21:37:21 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=261 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Dari pengecekan diketahui ssh port 22 menggunakan OpenSSH 9.2p1 (linux), Nginx Webserver untuk HTTP, PostgreSQL di port 5432 versi 16, aplikasi running di port 8001 php8.1.2)

4. **Pencarian Celah**

Pengecekan di sisi aplikasi yang terbuka dengan Port 80 dan 8001

```
PS C:\Users\saya> nmap -p 80 --script http-vuln* 10.50.1.96 -d
Packet.dll present, library version 1.79
wpcap.dll present, library version: Npcap version 1.79, based on libpcap version 1.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 14:56 SE Asia Standard Time
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.4.
NSE: Arguments from CLI:
NSE: Loaded 24 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 14:56
Completed NSE at 14:56, 0.00s elapsed
Initiating ARP Ping Scan at 14:56
Scanning 10.50.1.96 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x02504100 and arp[22:2] = 0x0001
Completed ARP Ping Scan at 14:56, 0.14s elapsed (1 total hosts)
Overall sending rates: 6.94 packets / s, 291.67 bytes / s.
mass_rdns: Using DNS server 192.168.2.1
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
mass_rdns: Using DNS server 172.30.103.249
mass_rdns: Using DNS server 172.30.0.157
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
mass_rdns: Using DNS server 192.168.2.1
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
Initiating Parallel DNS resolution of 1 host. at 14:56
mass_rdns: 0.32s 0/1 [#: 12, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 14:56, 0.03s elapsed
DNS resolution of 1 IPs took 0.32s. Mode: Async [#: 12, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 14:56
Scanning 10.50.1.96 [1 port]
Packet capture filter (device eth0): dst host 172.16.128.127 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 10.50.1.96)))
Discovered open port 80/tcp on 10.50.1.96
Completed SYN Stealth Scan at 14:56, 0.01s elapsed (1 total ports)
Overall sending rates: 142.86 packets / s, 6285.71 bytes / s.
NSE: Script scanning 10.50.1.96.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 14:56
NSE: Starting http-vuln-cve2010-0738 against 10.50.1.96:80.
NSE: Starting http-vuln-wnr1000-creds against 10.50.1.96:80
```

State: NOT VULNERABLE

```
PS C:\Users\saya> nmap -p 8001 --script http-vuln* 10.50.1.96 -d
Packet.dll present, library version 1.79
wpcap.dll present, library version: Npcap version 1.79, based on libpcap version 1.10.4
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-04 15:01 SE Asia Standard Time
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.4.
NSE: Arguments from CLI:
NSE: Loaded 24 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 15:01
Completed NSE at 15:01, 0.00s elapsed
Initiating ARP Ping Scan at 15:02
Scanning 10.50.1.96 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x02504100 and arp[22:2] = 0x0001
Completed ARP Ping Scan at 15:02, 0.14s elapsed (1 total hosts)
Overall sending rates: 7.14 packets / s, 300.00 bytes / s.
mass_rdns: Using DNS server 192.168.2.1
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
mass_rdns: Using DNS server 172.30.103.249
mass_rdns: Using DNS server 172.30.0.157
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
mass_rdns: Using DNS server 192.168.2.1
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
mass_rdns: Using DNS server 1.1.1.1
mass_rdns: Using DNS server 8.8.8.8
Initiating Parallel DNS resolution of 1 host. at 15:02
mass_rdns: 0.32s 0/1 [#: 12, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 15:02, 0.03s elapsed
DNS resolution of 1 IPs took 0.32s. Mode: Async [#: 12, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 15:02
Scanning 10.50.1.96 [1 port]
Packet capture filter (device eth0): dst host 172.16.128.127 and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 10.50.1.96)))
Discovered open port 8001/tcp on 10.50.1.96
Completed SYN Stealth Scan at 15:02, 0.01s elapsed (1 total ports)
Overall sending rates: 111.11 packets / s, 4888.89 bytes / s.
NSE: Script scanning 10.50.1.96.
NSE: Starting runlevel 1 (of 1) scan.
Initiating NSE at 15:02
```

State: NOT VULNERABLE

Dari hasil pengecekan tidak adanya kerentanan pada port/service 80 dan 8001 dengan script http.

5. **Summary**
   Tes dilakukan dari lingkup network Private. Dimana pentester menggunakan VPN yang terkoneksi langsung ke server PDN. Dari pengecekan tidak ditemukan kerentanan sesuai dengan database CVE.
   Untuk port yang terbuka selain HTTP (80), merupakan service yang dibutuhkan oleh tim developer. Sebagai contoh SSH 22 dan PostgreSQL 5432. Hal ini dipastikan hanya bisa diakses/remote melalui VPN saja.
   Saran untuk public network yang dibuka hanya port 80 dan 443 (https support).

VA Test BKPM Production (private network)

IP: 10.50.1.96 (perlu vpn)
host : pdn-portal-satudata
tools : Zap OWASP

ZAP Owasp mengkategorikan menjadi 4 risk level, yaitu :

1. High
2. Medium
3. Low
4. Informational

Summary Risk Level (dari hasil pengecekan/VA ke Private IP)

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	0
Low	4
Informational	5

Terdapat 4 point terkategori LOW pada web data bkpm.

Alerts

Name	Risk Level	Number of Instances
Application Error Disclosure	Low	1
Big Redirect Detected (Potential Sensitive Information Leak)	Low	4
Cookie No HttpOnly Flag	Low	28
Cross-Domain JavaScript Source File Inclusion	Low	208
Authentication Request Identified	Informational	1
Information Disclosure - Suspicious Comments	Informational	23
Modern Web Application	Informational	23
Session Management Response Identified	Informational	33
User Agent Fuzzer	Informational	244

Celah yang dikategorikan sebagai LOW menunjukkan bahwa dampak/eksploitasi celah tersebut tidak signifikan. Walaupun tidak berdampak besar, mengatasi kategori LOW tetap dianjurkan untuk mengurangi kemungkinan dampak dari celah kerentanan tersebut.