DOKUMENTASI

MENCARI SUBDOMAIN DARI KAI.COM MENGGUNKAAN SUBFINDER

```
┌──(kali㉿kali)-[~]
└─$ subfinder -d kai.id -o subdomain_kai.txt

                     __     ____  __
   _____  __  __/ /_  / __(_)__  ____/ /__  _____
  / ___/ / / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / / /_/ / __/ / / / / /_/ /  __/ /
/____/\__,_/_.___/_/ /_/_/ /_/ /_/\__,_/\___/_/

                projectdiscovery.io

[INF] Current subfinder version v2.6.0 (outdated)
[INF] Loading provider config from /home/kali/.config/subfinder/provider-config.yaml
[INF] Enumerating subdomains for kai.id
memsvc-rts40.kai.id
ppsagent02.kai.id
api.kai.id
midsvc-rtsng.kai.id
tesbox.kai.id
rapid.kai.id
groupbooking.kai.id
crm-alpha.kai.id
mail.kai.id
egp.kai.id
ns1.kai.id
www.kai.id
eproc.kai.id
midsvcext-rts40.kai.id
mail-rts5.kai.id
ppsagent09.kai.id
kai.id
lrtjabodebek.kai.id
rdsv3.kai.id
smtp-list.kai.id
smtp-out2.kai.id
ticketing-apidoc.kai.id
```

MENCARI DOMAIN AKTIF DARI SUB DOMAIN YANG TELAH KITA DAPATKAN DARI SUBFINDER

```
┌──(kali㉿kali)-[~]
└─$ httpx -l subdomain_kai.txt -title -status-code -o subdomain_kai_hidup.txt

    __    __  __       _  __
   / /_  / /_/ /_____ | |/ /
  / __ \/ __/ __/ __ \|   /
 / / / / /_/ /_/ /_/ /   |
/_/ /_/\__/\__/ .___/_/|_|
             /_/

                projectdiscovery.io

[INF] Current httpx version v1.7.3 (latest)
[WRN] UI Dashboard is disabled, Use -dashboard option to enable
https://e-recruitment.kai.id [200] [e-Recruitment PT. Kereta Api Indonesia]
https://memsvcs-rts40.kai.id [404]
https://midkci.kai.id [200]
https://booking.kai.id [200] [PT Kereta Api Indonesia -      Reservasi Tiket]
https://midsvc-rts40.kai.id [404] [404 Not Found]
https://memsvcdev.kai.id [404]
https://api.kai.id [404]
https://media.kai.id [302]
https://mail.kai.id [200] [Zimbra Web Client Sign In]
https://middev.kai.id [200] [Kereta Api Indonesia]
https://cargo.kai.id [200] [Web Portal Angkutan Barang]
https://groupbooking.kai.id [200] [KAI - Group Booking]
https://ppid.kai.id [200] [E-PPID PT Kereta Api Indonesia (Persero)]
https://pso.kai.id [200] [PSO Online]
https://rapid.kai.id [301] [301 Moved Permanently]
https://rdsv3-rw.kai.id [200] [Rail Document System - PT Kereta Api Indonesia]
https://rdsv3-ro.kai.id [200] [Rail Document System - PT Kereta Api Indonesia]
https://recruitment.kai.id [301] [301 Moved Permanently]
https://subsidiary-rts40.kai.id [404] [404 Not Found]
https://www.kai.id [200] [Situs Resmi PT Kereta Api Indonesia (Persero)]
https://b2b-apidoc.kai.id [200] [B2B KAI]
```

A RECORD (IP ADDREST)

```
┌──(kali㉿kali)-[~]
└─$ dig kai.id

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30095
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0×0005, udp: 4096
;; QUESTION SECTION:
;kai.id.                                IN      A

;; ANSWER SECTION:
kai.id.                 5       IN      A       103.54.225.47

;; Query time: 2035 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:35:55 EST 2025
;; MSG SIZE  rcvd: 51
```

MX RECORD (MAIL EXCHANGE)

```
┌──(kali㉿kali)-[~]
└─$ dig kai.id mx

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44886
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; QUESTION SECTION:
;kai.id.                                IN      MX

;; ANSWER SECTION:
kai.id.                 5       IN      MX      0 ppsagent07.kai.id.
kai.id.                 5       IN      MX      0 ppsagent01.kai.id.

;; AUTHORITY SECTION:
kai.id.                 5       IN      NS      ns3.kai.id.
kai.id.                 5       IN      NS      ns5.kai.id.
kai.id.                 5       IN      NS      ns4.kai.id.

;; ADDITIONAL SECTION:
ppsagent07.kai.id.      5       IN      A       103.54.225.202
ppsagent01.kai.id.      5       IN      A       103.54.225.214
ns3.kai.id.             5       IN      A       103.44.9.74
ns5.kai.id.             5       IN      A       103.156.130.11
ns4.kai.id.             5       IN      A       103.54.225.18

;; Query time: 67 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:36:26 EST 2025
;; MSG SIZE  rcvd: 220
```

NS RECORD (NAMESERVER)

```
┌──(kali㉿kali)-[~]
└─$ dig kai.id ns

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54967
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;kai.id.                                IN      NS

;; ANSWER SECTION:
kai.id.                 5       IN      NS      ns5.kai.id.
kai.id.                 5       IN      NS      ns4.kai.id.
kai.id.                 5       IN      NS      ns3.kai.id.

;; AUTHORITY SECTION:
kai.id.                 5       IN      NS      ns4.kai.id.
kai.id.                 5       IN      NS      ns3.kai.id.
kai.id.                 5       IN      NS      ns5.kai.id.

;; ADDITIONAL SECTION:
ns5.kai.id.             5       IN      A       103.156.130.11
ns4.kai.id.             5       IN      A       103.54.225.18
ns3.kai.id.             5       IN      A       103.44.9.74
ns4.kai.id.             5       IN      A       103.54.225.18
ns3.kai.id.             5       IN      A       103.44.9.74
ns5.kai.id.             5       IN      A       103.156.130.11

;; Query time: 3 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:36:45 EST 2025
;; MSG SIZE  rcvd: 220
```

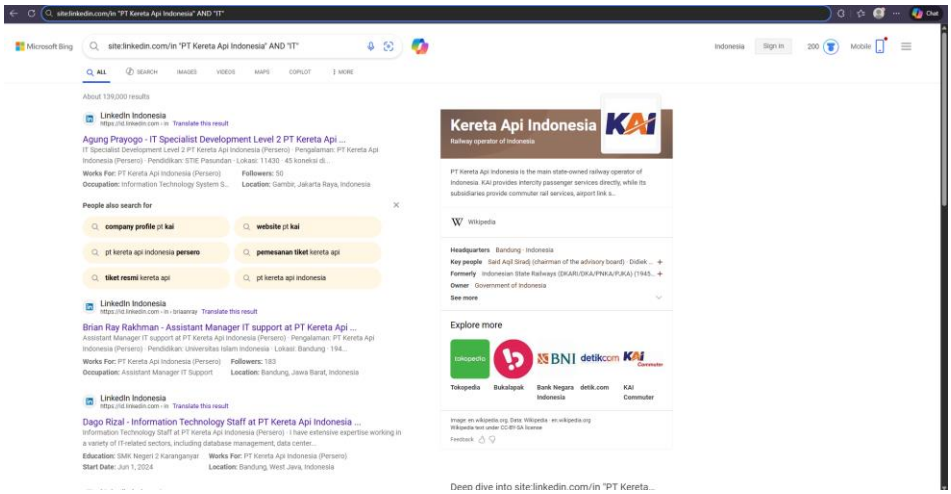
TXT RECORD

```
┌──(kali㉿kali)-[~]
└─$ dig kai.id txt

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38406
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kai.id.                                IN      TXT

;; ANSWER SECTION:
kai.id.                 5       IN      TXT     "yahoo-verification-key=XmDRO9kroQ4cr1Bn8nfhYBHeVBqJPl+CoLiQ58hohwk="
kai.id.                 5       IN      TXT     "tq6qjsr420klo13la7jmsgbpds"
kai.id.                 5       IN      TXT     "MS=A952DF8E8223CF5DAFC3FF9B4CA749D462821B90"
kai.id.                 5       IN      TXT     "globalsign-domain-verification=5bfa44135cf14960b840f9993b814e8d"
kai.id.                 5       IN      TXT     "dtm-domain-verification=OMspuu1W4nNsvLgltL038pkwVmN3iUpW_c6ARL5bHBg"
kai.id.                 5       IN      TXT     "google-site-verification=DGOB3LAFcK2ZAL4spsT7XMQ8GkYFnwfkKVDsBgpeRM0"
kai.id.                 5       IN      TXT     "google-gws-recovery-domain-verification=4817228"

;; Query time: 2043 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:36:58 EST 2025
;; MSG SIZE  rcvd: 496
```

CNAME RECORD

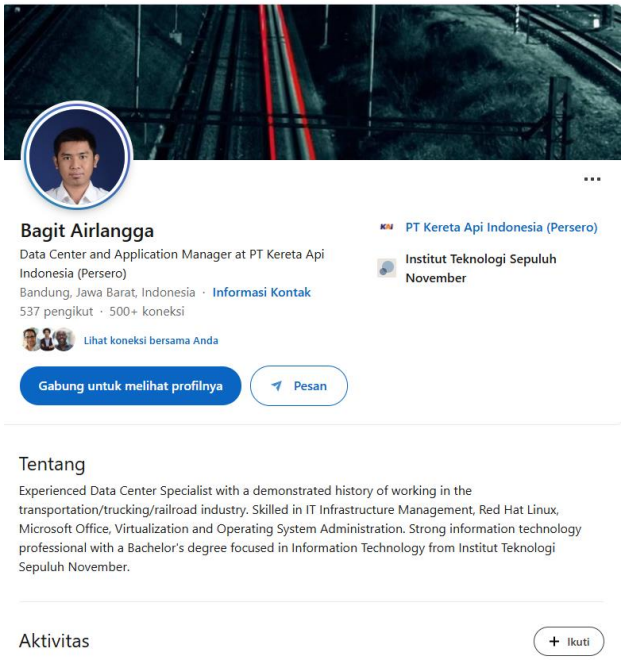
```
┌──(kali㉿kali)-[~]
└─$ dig kai.id CNAME

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id CNAME
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56882
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 3, ADDITIONAL: 3

;; QUESTION SECTION:
;kai.id.                        IN      CNAME

;; AUTHORITY SECTION:
kai.id.                 5       IN      NS      ns3.kai.id.
kai.id.                 5       IN      NS      ns5.kai.id.
kai.id.                 5       IN      NS      ns4.kai.id.

;; ADDITIONAL SECTION:
ns3.kai.id.             5       IN      A       103.44.9.74
ns5.kai.id.             5       IN      A       103.156.130.11
ns4.kai.id.             5       IN      A       103.54.225.18

;; Query time: 95 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:43:28 EST 2025
;; MSG SIZE  rcvd: 130
```

GOOGLE DORKS

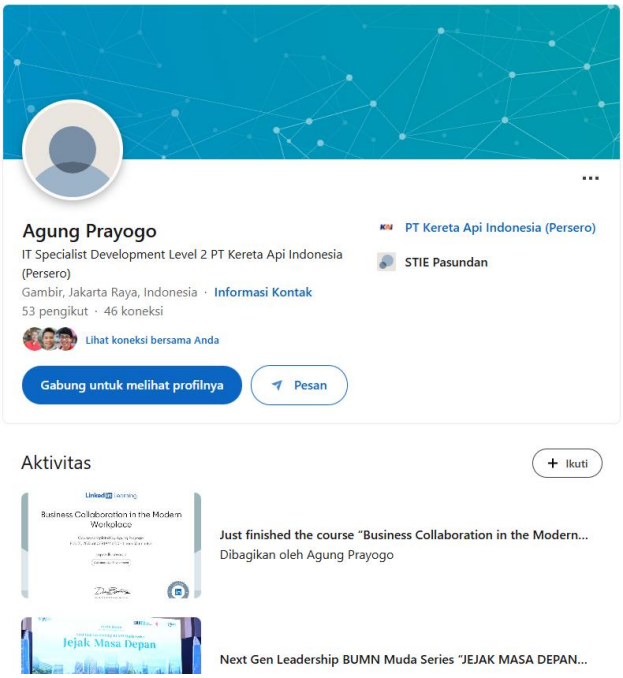


Linkedin

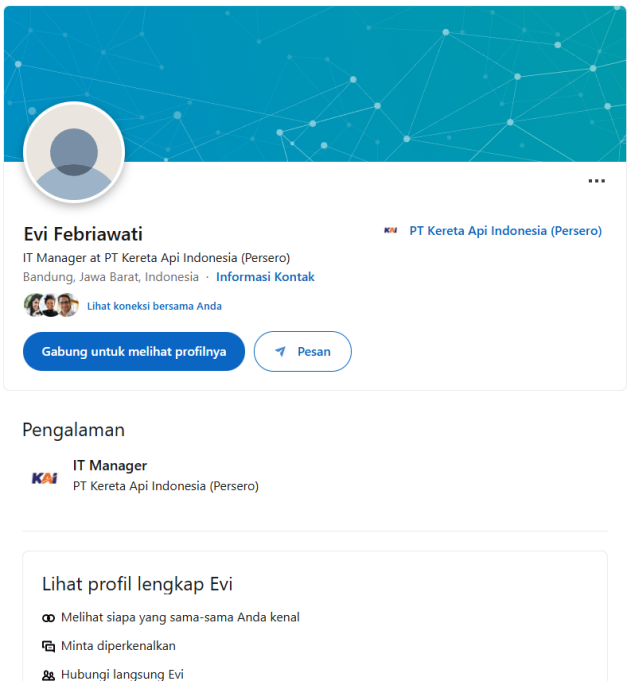
Data Center And Application Manager PT KAI



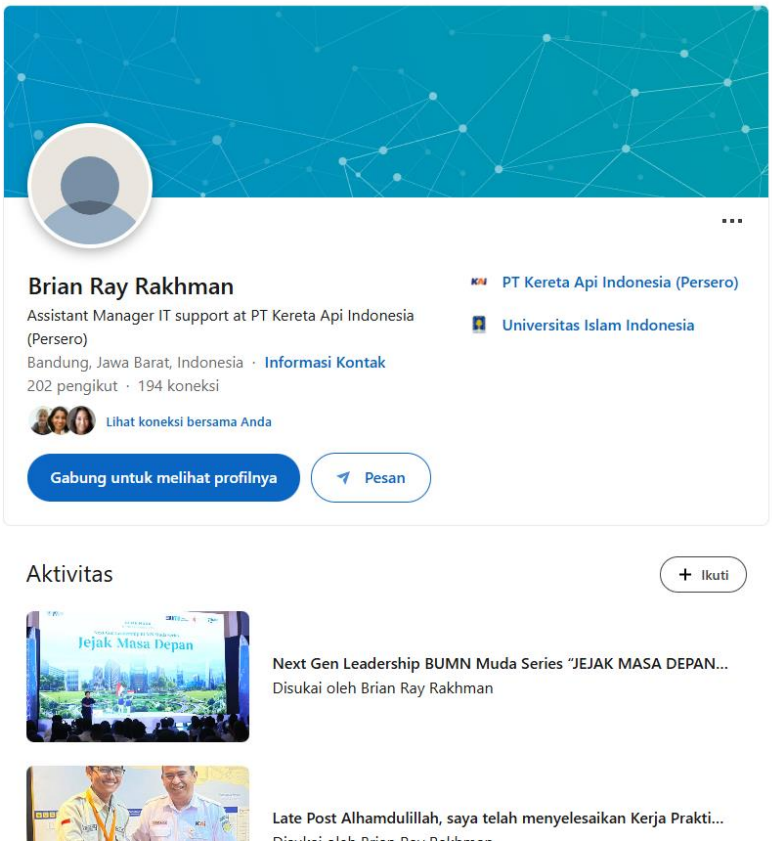
IT Specialist Development PT KAI



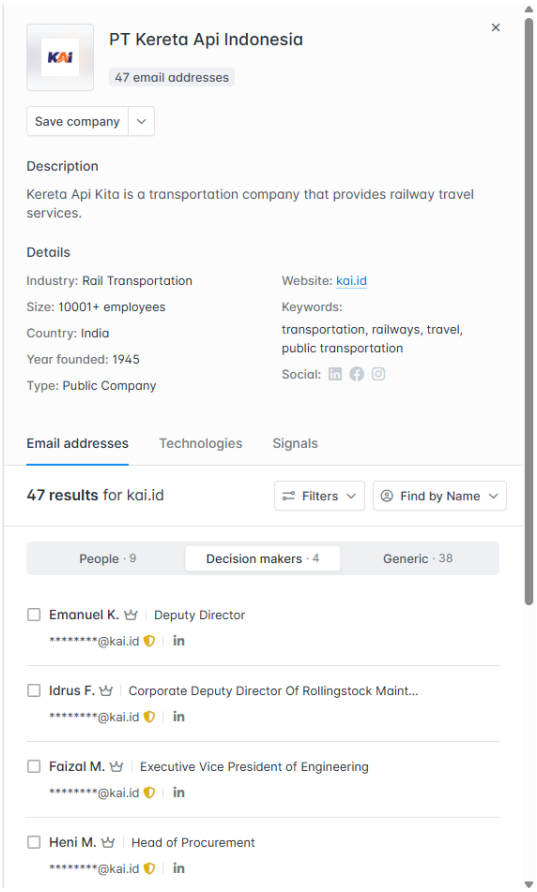
IT Manager PT KAI

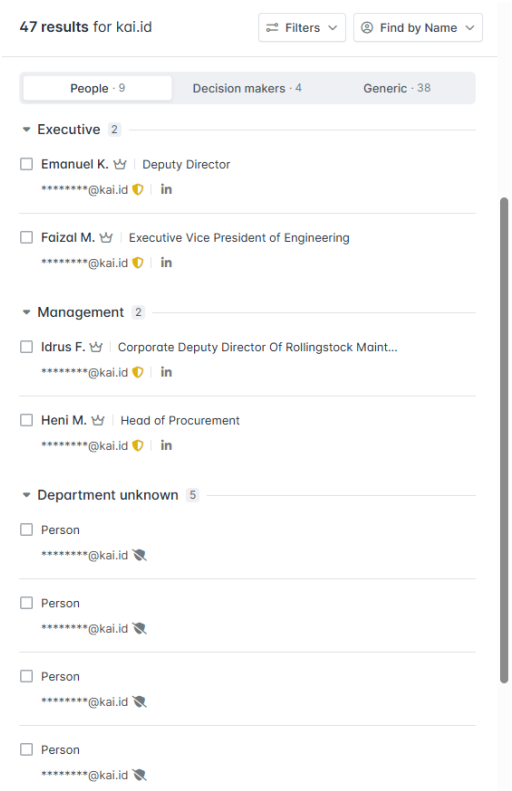


IT ASSISTAN MANAGER / IT SUPPORT PT KAI



EMAIL = SAYA MENGGUNAKAN TOOLS HUNTER.IO UNTUK MENEMUKAN DOMAIN ALAMAT EMAIL YANG DI GUNAKAN


PT Kereta Api Indonesia
47 email addresses
Save company
Description
Kereta Api Kita is a transportation company that provides railway travel services.
Details
Industry: Rail Transportation
Size: 10001+ employees
Country: India
Year founded: 1945
Type: Public Company
Website: kai.id
Keywords:
transportation, railways, travel, public transportation
Social:
Email addresses
Technologies
Signals
47 results for kai.id
Filters
Find by Name
People · 9
Decision makers · 4
Generic · 38
Emanuel K. | Deputy Director
********@kai.id
Idrus F. | Corporate Deputy Director Of Rollingstock Maint...
********@kai.id
Faizal M. | Executive Vice President of Engineering
********@kai.id
Heni M. | Head of Procurement
********@kai.id


47 results for kai.id
Filters
Find by Name
People · 9
Decision makers · 4
Generic · 38
Executive 2
Emanuel K. | Deputy Director
********@kai.id
Faizal M. | Executive Vice President of Engineering
********@kai.id
Management 2
Idrus F. | Corporate Deputy Director Of Rollingstock Maint...
********@kai.id
Heni M. | Head of Procurement
********@kai.id
Department unknown 5
Person
********@kai.id
Person
********@kai.id
Person
********@kai.id
Person
********@kai.id

TEKNOLOGI YANG DI GUNAKAN DARI ANALISIS,AUTHENTIKASI,DNS,FRAMEWORK,KEAMANAN

Technologies used on kai.id

Powered by TechLookup.

Analytics

- Cloudflare Browser Insights

Authentication Services

- reCAPTCHA

Content Management System

- Slick

DNS

- Cloudflare

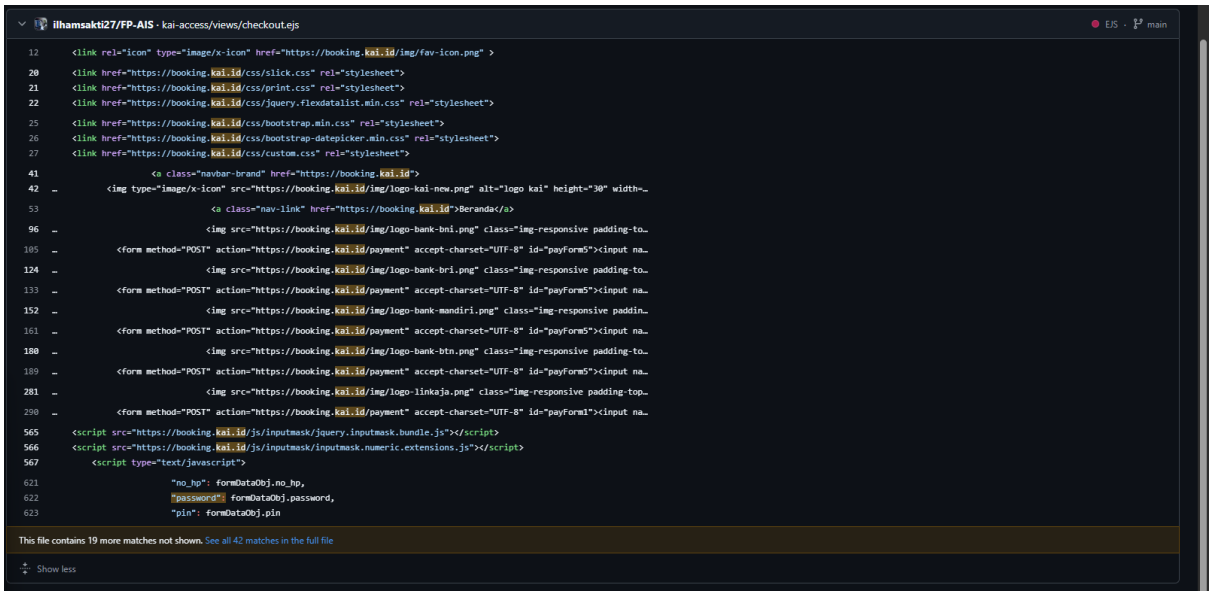
Programming Framework

- Bootstrap
- jQuery
- jQuery UI
- Modernizr
- Select2

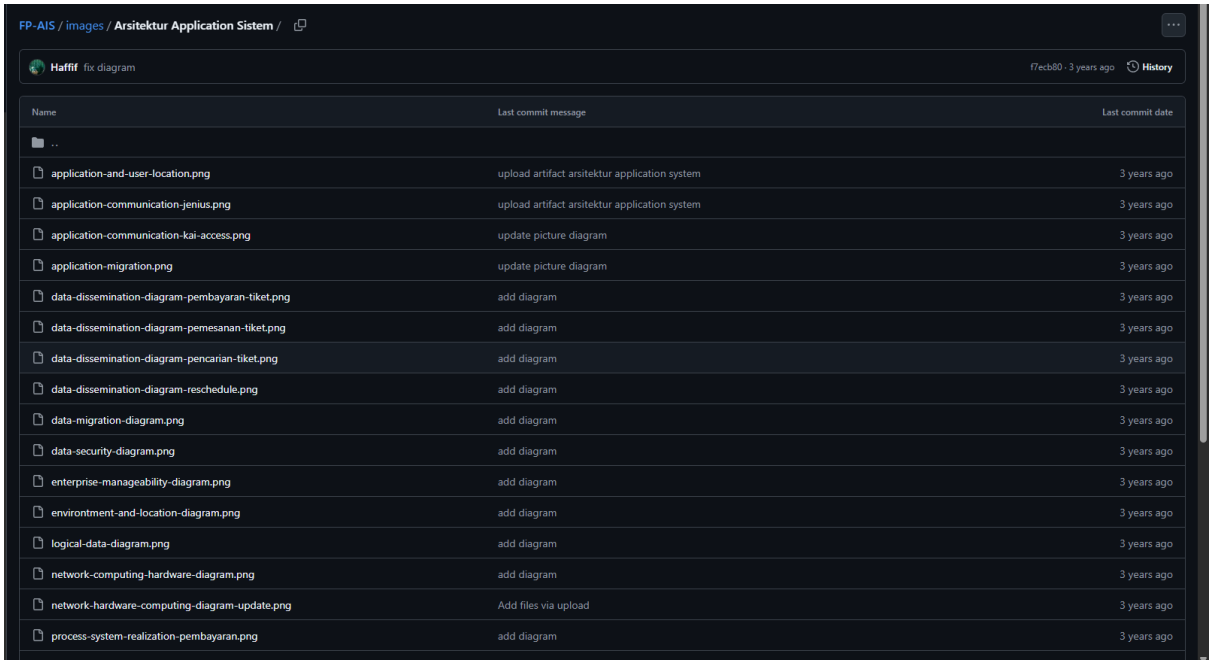
Security

- Cloudflare Bot Management

SENSITIVE GIT PT KAI



ARSITEKTUR APLIKASI SISTEM KAI ACCESS

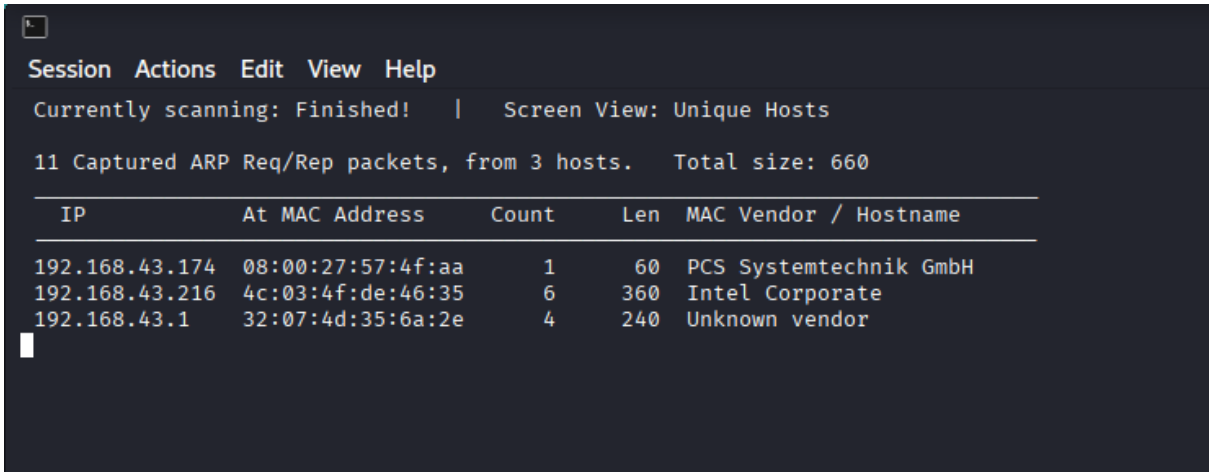


FP-AIS / images / Arsitektur Application Sistem /

Haffif fix diagram — f7ecb80 · 3 years ago — History

Name	Last commit message	Last commit date
..		
application-and-user-location.png	upload artifact arsitektur application system	3 years ago
application-communication-jenius.png	upload artifact arsitektur application system	3 years ago
application-communication-kai-access.png	update picture diagram	3 years ago
application-migration.png	update picture diagram	3 years ago
data-dissemination-diagram-pembayaran-tiket.png	add diagram	3 years ago
data-dissemination-diagram-pemesanan-tiket.png	add diagram	3 years ago
data-dissemination-diagram-pencarian-tiket.png	add diagram	3 years ago
data-dissemination-diagram-reschedule.png	add diagram	3 years ago
data-migration-diagram.png	add diagram	3 years ago
data-security-diagram.png	add diagram	3 years ago
enterprise-manageability-diagram.png	add diagram	3 years ago
environtment-and-location-diagram.png	add diagram	3 years ago
logical-data-diagram.png	add diagram	3 years ago
network-computing-hardware-diagram.png	add diagram	3 years ago
network-hardware-computing-diagram-update.png	Add files via upload	3 years ago
process-system-realization-pembayaran.png	add diagram	3 years ago

MENCARI IP DARI VULNOS MENGGUNAKAN NETDISCOVER



```
Session  Actions  Edit  View  Help
Currently scanning: Finished!   |   Screen View: Unique Hosts

11 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 660

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname

192.168.43.174  08:00:27:57:4f:aa      1      60  PCS Systemtechnik GmbH
192.168.43.216  4c:03:4f:de:46:35      6     360  Intel Corporate
192.168.43.1    32:07:4d:35:6a:2e      4     240  Unknown vendor
```

SCAN PORT UDP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU --top-ports 20 192.168.43.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:47 EST
Nmap scan report for VulnOSv2 (192.168.43.174)
Host is up (0.0017s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   closed        ntp
135/udp   open|filtered msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   closed        snmp
162/udp   open|filtered snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   open|filtered ipp
1434/udp  open|filtered ms-sql-m
1900/udp  open|filtered upnp
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.70 seconds
```

SCAN PORT TCP

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 192.168.43.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:14 EST
Nmap scan report for VulnOSv2 (192.168.43.174)
Host is up (0.00066s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.36 seconds
```

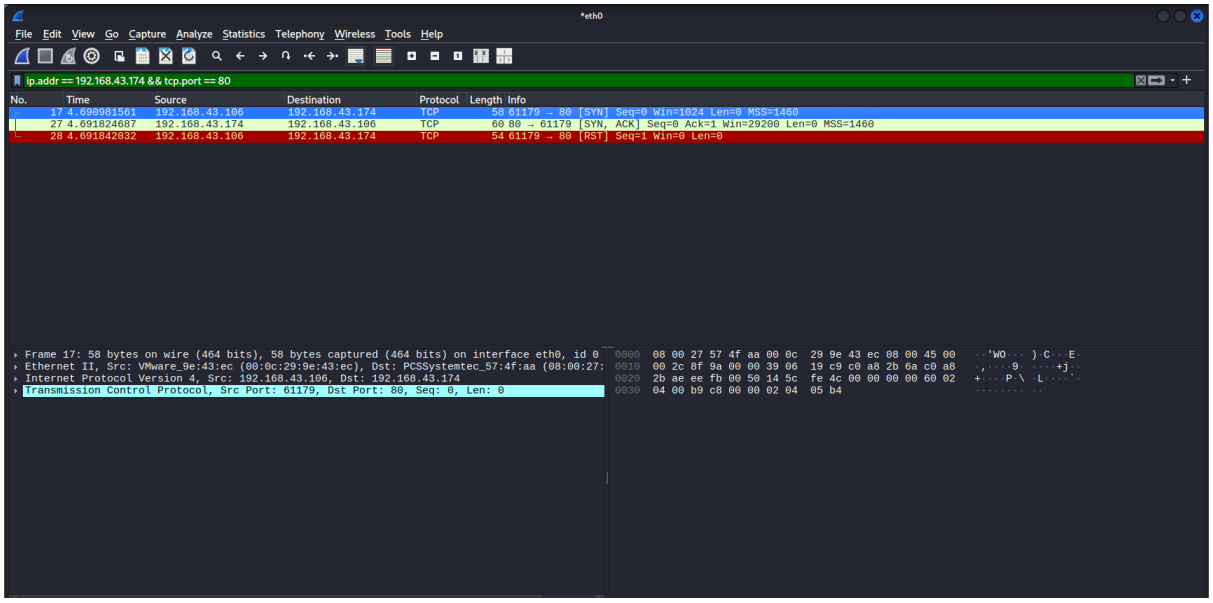
Service and Version Detection

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.43.174
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:43 EST
Nmap scan report for VulnOSv2 (192.168.43.174)
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
6667/tcp open  irc     ngircd
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: irc.example.net; OS: 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 11.77 seconds
```

FINGERPRINT

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.43.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:54 EST
Nmap scan report for VulnOSv2 (192.168.43.174)
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
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 1.71 seconds
```

Wireshark


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.43.174 && tcp.port == 80
No. Time Source Destination Protocol Length Info
17 4.690981561 192.168.43.106 192.168.43.174 TCP 58 61179 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
27 4.691824687 192.168.43.174 192.168.43.106 TCP 60 80 → 61179 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
28 4.691842032 192.168.43.106 192.168.43.174 TCP 54 61179 → 80 [RST] Seq=1 Win=0 Len=0
Frame 17: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface eth0, id 0
Ethernet II, Src: VMware_9e:43:ec (00:0c:29:9e:43:ec), Dst: PCSSystemtec_57:4f:aa (08:00:27:
Internet Protocol Version 4, Src: 192.168.43.106, Dst: 192.168.43.174
Transmission Control Protocol, Src Port: 61179, Dst Port: 80, Seq: 0, Len: 0
0000 08 00 27 57 4f aa 00 0c 29 9e 43 ec 08 00 45 00
0010 00 2c 8f 9a 00 00 39 06 19 c9 c0 a8 2b 6a c0 a8
0020 2b ae ee fb 00 50 14 5c fe 4c 00 00 00 00 60 02
0030 04 00 b9 c8 00 00 02 04 05 b4