

Laporan Cyber Security

TUGAS PRAKTEK-DEMONSTRASI/PRAKTEK



Muhammad Mardiansyah

PUSAT PELATIHAN KERJA DAERAH JAKARTA UTARA

No 1. : Deteksi aktivitas / lalu lintas pada jaringan anda Misal wifi atau jaringan Lokal maupun Publik menggunakan Tool yang anda punya dan kuasai.

A. hasil scan dan port yang terbuka menggunakan NMAP

```
(kali@kali)-[~]
$ nmap 192.168.34.38 -P -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 21:54 EDT
Nmap scan report for 192.168.34.38
Host is up (0.00028s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
80/tcp    open  http             Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
135/tcp    open  msrpc            Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
443/tcp    open  ssl/http         Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql            MariaDB 10.3.23 or earlier (unauthorized)
8000/tcp   open  http             Splunkd httpd
8089/tcp   open  ssl/http         Splunkd httpd
MAC Address: 88:AE:DD:8A:D6:5F (EliteGroup Computer Systems)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 31.98 seconds
```

Pada gambar diatas merupakan hasil dari nmap pada ip windows, dari hasil nmap ditemukan bahwa terdapat beberapa port yang terbuka seperti :

- port 80 terbuka dengan service http menggunakan Apache.
- port 443 terbuka dengan service ssl/http dengan menggunakan apache.
- port 135 terbuka dengan service msrpc dengan menggunakan microsoft windows RPC.
- port 3306 terbuka dengan menggunakan service mysql dengan menggunakan MariaDB 10.3.23.
- port 8000 terbuka dengan service http menggunakan splunk httpd.
- port 8089 terbuka dengan menggunakan service ssl/http splunk httpd.

Karena pada praktik kali ini kita akan berfokus pada web server, maka kita akan berfokus pada port 80/tcp sebagai percobaan untuk kita analisis dan kita berikan tindakan agar port ini tidak dapat di eksploitasi.

B. hasil scan dan port yang terbuka NIKTO

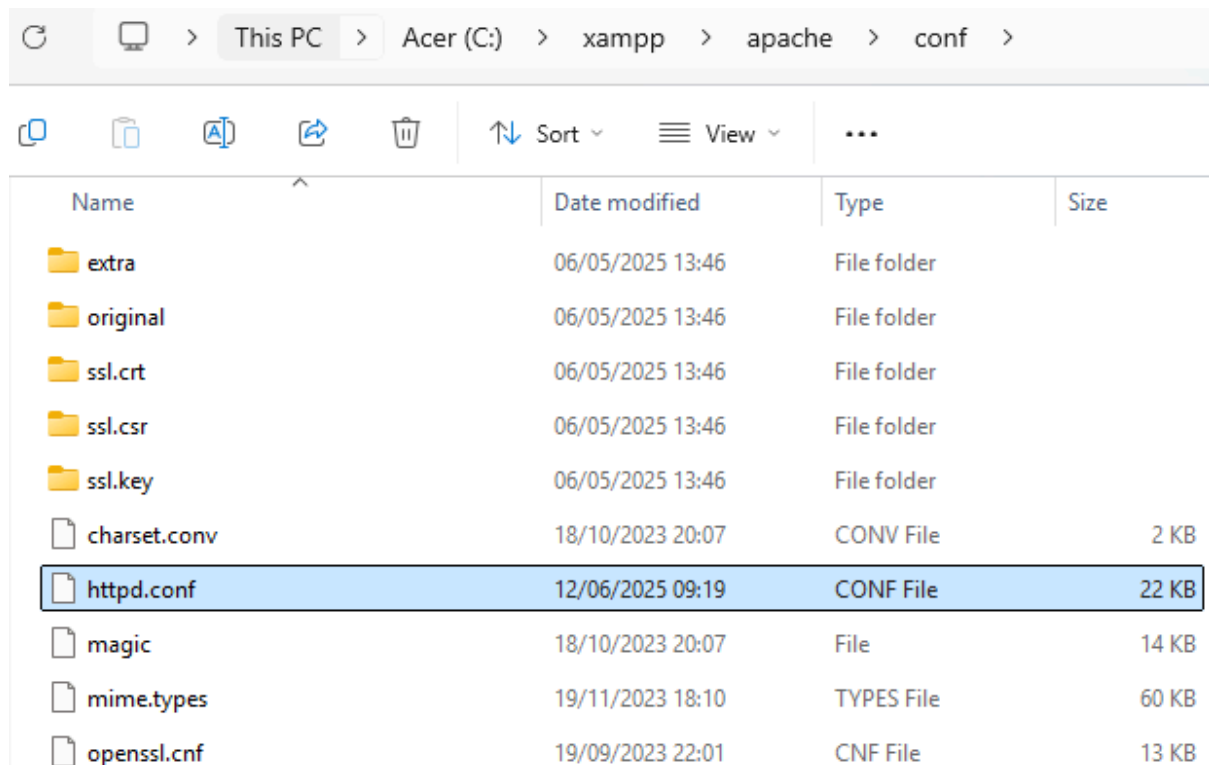
```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ nikto -h 192.168.34.38  
- Nikto v2.5.0  
  
+ Target IP: 192.168.34.38  
+ Target Hostname: 192.168.34.38  
+ Target Port: 80  
+ Start Time: 2025-06-11 22:07:01 (GMT-4)  
  
+ Server: Apache/2.4.58 (Win64) OpenSSL/3.1.3 PHP/8.2.12  
+ /: Retrieved x-powered-by header: PHP/8.2.12.  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ Root page / redirects to: http://192.168.34.38/dashboard/  
+ /: HTTP TRACE method is active which suggests the host is vulnerable to XST. See: https://owasp.org/www-community/attacks/Cross\_Site\_Tracing  
+ /img/: Directory indexing found.  
+ /img/: This might be interesting.  
+ /icons/: Directory indexing found.  
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/  
+ /wordpress/wp-content/plugins/snippets/modules/syntax_highlight.php?libpath=http://blog.cirt.net/rfiinc.txt?Drupal Link header found with value: <http://localhost/wordpress/wp-json/>; rel="https://api.w.org/". See: https://www.drupal.org/  
+ /wordpress/wp-links-opml.php: This WordPress script reveals the installed version.  
+ /wordpress/wp-app.log: Wordpress' wp-app.log may leak application/system details.  
+ /wordpress/wp-admin/: Uncommon header 'x-redirect-by' found, with contents: WordPress.  
+ /wordpress/: A Wordpress installation was found.  
+ /wordpress/wp-content/uploads/: Directory indexing found.  
+ /wordpress/wp-content/uploads/: Wordpress uploads directory is browsable. This may reveal sensitive information
```

Pada gambar di atas merupakan hasil dari scanning pada ip target/windows (192.168.34.38) menggunakan nikto, nikto sendiri berfungsi sebagai alat scanning untuk mendeteksi vulnerability dan ditemukan bahwa :

- informasi web server = apache/2.4.58 dan PHP/8.2.12
- masalah yang terjadi adalah :
- X-frame_option tidak ada, rentan terhadap clickjacking
- Metode Trace tidak aktif
- Banyak sekali file wordpress yang muncul dan kemungkinan bisa dilakukan eksploitasi.
- file wordpress/wp-content/uploads terbuka sehingga ada kemungkinan data bisa dilihat dan didownload jika tidak dilindungi.

C. Tindakan apa yang anda lakukan untuk menangani temuan tersebut.

Untuk menangani hal-hal diatas kita dapat melakukan berbagai cara untuk menanganinya seperti melakukan penutupan port pada ip host, sebagai tindakan kita akan menutup port 80 dan kali linux tidak dapat melakukan scanning vulnerability pada website kita.



Pada gambar diatas adalah file di dalam apache yang berisi konfigurasi http. Pada file ini terdapat beberapa konfigurasi seperti listening port dan lain-lain.

```
#Listen 12.34.56.78:80
Listen 127.0.0.1:80
```

Pada gambar diatas merupakan isi dari file httpd.conf, pada perintah di atas kita merubah listening port yang awalnya port 80 (:80) bisa digunakan oleh semua host, menjadi port 80 hanya bisa digunakan oleh local host (127.0.0.1:80). Dengan kita menggunakan konfigurasi ini, maka kali linux tidak dapat menemukan port 80 dan nikto tidak akan bisa melakukan scanning.

```
(kali@kali)-[~]
$ nmap 192.168.34.38 -P -sV
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-11 22:20 EDT
Nmap scan report for 192.168.34.38
Host is up (0.00017s latency).
Not shown: 993 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
443/tcp    open  ssl/http     Apache httpd 2.4.58 ((Win64) OpenSSL/3.1.3 PHP/8.2.12)
445/tcp    open  microsoft-ds?
3306/tcp   open  mysql        MariaDB 10.3.23 or earlier (unauthorized)
8000/tcp   open  http         Splunkd httpd
8089/tcp   open  ssl/http     Splunkd httpd
MAC Address: 88:AE:DD:8A:D6:5F (EliteGroup Computer Systems)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 31.84 seconds
```

Pada gambar di atas merupakan tampilan nmap setelah kita menutup port 80, pada konfigurasi nmap di atas, kali linux tidak dapat menemukan port 80, karena port ini hanya bisa diakses oleh localhost.

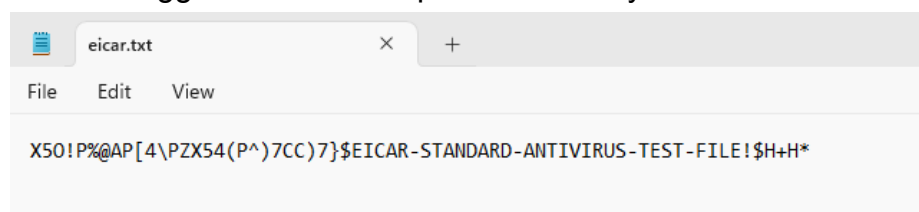
```
(kali@kali)-[~]
$ nikto -h 192.168.34.38
- Nikto v2.5.0

+ 0 host(s) tested
```

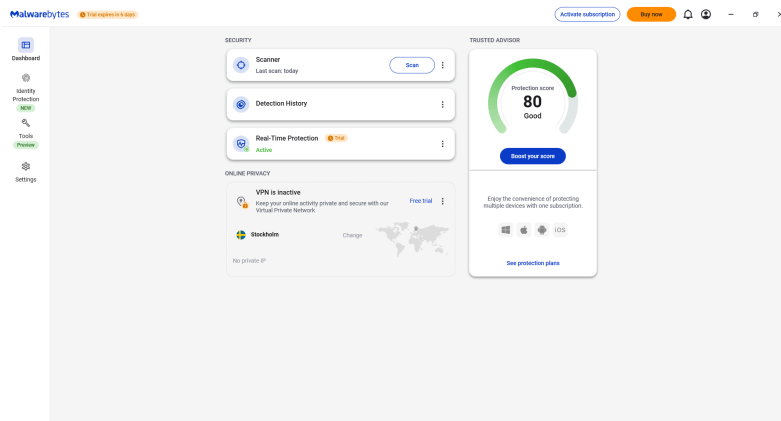
Pada gambar di atas adalah hasil dari nikto setelah port 80 kita tutup, nikto tidak dapat menemukan kelemahan dan celah dari host kita dan web server yang digunakan di windows dapat aman dari berbagai scanning.

No 2.

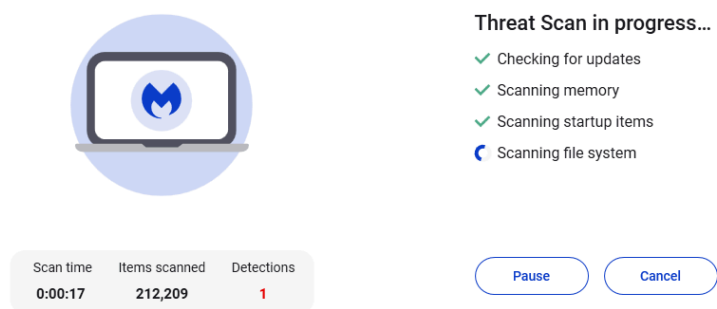
- A. Jelaskan langkah-langkah yang akan Anda ambil untuk melakukan analisis malware menggunakan tools seperti Malwarebytes atau antivirus lainnya.



Pada gambar di atas kita membuat simulasi untuk pembuatan virus sederhana agar, dapat terdeteksi saat melakukan scanning.



Langkah selanjutnya adalah melakukan scanning menggunakan malwarebytes.



Setelah melakukan scanning, terdapat 1 file yang mencurigakan yang di deteksi.

Scanner

Threat Scan results

		Detections	Scan time	Items scanned
		2	22s	216,122

<input checked="" type="checkbox"/>	Name	Type	Object type	Location
<input checked="" type="checkbox"/>	EICAR-AV-Test	Malware	File	C:\USERS\ACER\DOCUMENTS\EICAR.TXT
<input checked="" type="checkbox"/>	EICAR-AV-Test	Malware	File	C:\USERS\ACER\APPDATA\ROAMING\Microsoft\Win...

Berikut adalah file yang merupakan file berbahaya dan kemungkinan adalah virus.

Scan report

Summary

Scan summary

2 items detected

2 items quarantined

Detected items

Threats: 2 PUP: 0 PUM: 0

Name	Type	Location	Action
EICAR-AV-Test	File	C:\USERS\ACER\DOCUMENTS\EIC...	Quarantined

Advanced

Date

12/06/2025 09:29:23

Scan result

Completed

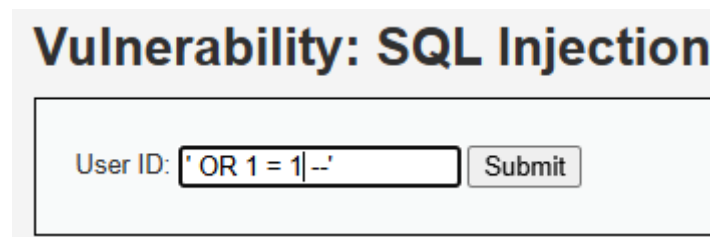
Export

Close

Berikut adalah file yang teridentifikasi sebagai file virus dan selanjutnya adalah quarantined agar file tidak bisa dieksekusi.

No 3.

A. Temuan sql injection



Vulnerability: SQL Injection

User ID:

Pada gambar di atas merupakan payload untuk melakukan sql injection dengan menggunakan logika ' OR 1 = 1 - -', dengan menggunakan logika ini, sql akan mengeksekusi perintah ' OR 1 = 1' ke dalam query yang akan bernilai TRUE, dan penggunaan karakter - - digunakan untuk mengabaikan inputan setelah nilai TRUE tadi.

```
ID: ' OR 1 = 1 -- '  
First name: admin  
Surname: admin
```

Pada gambar diatas, penyerang telah berhasil melakukan sql injection dengan mendapatkan firstname admin, dan dapat mengakses website.

```
127.0.0.1/dvwa/vulnerabilities/sqli/?id=%27+OR+1+%3D+1+--+%27&Submit=Submit#
```

Pada gambar diatas terdapat url yang memiliki kerentanan yang ditandai dengan ?id = %27, url ini mengindikasikan bahwa input dari username langsung dimasukan ke dalam query, tanpa menggunakan prepared statement agar inputan tidak terhubung langsung dengan query.

No 4.

A. firewall berfungsi untuk melindungi dan mengontrol jaringan seperti lalu lintas data masuk dan data keluar, firewall diibaratkan seperti gerbang yang dapat menyaring apakah suatu dapat boleh lewat atau tidak. firewall berjalan di masing- masing layer sesuai kebutuhan :

- Layer 3 & 4 = Network Layer & Transport Layer, firewall memfilter ip address dan protokol jaringan. biasanya firewall pada layer ini digunakan untuk memblokir ip dan blokir trafik dari ip tertentu. pada tampilan di bawah merupakan proses untuk memblokir suatu ip dari firewall.

Scope
Specify the local and remote IP addresses to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports
- **Scope**
- Action
- Profile
- Name

Which local IP addresses does this rule apply to?

☐ Any IP address

☒ These IP addresses:

Add... Edit... Remove

Customize the interface types to which this rule applies: Customize...

Which remote IP addresses does this rule apply to?

☒ Any IP address

☐ These IP addresses:

Add... Edit... Remove

< Back Next > Cancel

- Layer 7 = Application Layer, firewall di layer ini berfungsi untuk menganalisis dan memfilter data berdasarkan isi. biasanya pada layer ini firewall digunakan untuk menganalisis isi data/paket, mendeteksi serangan seperti sql injection dan xss. berbeda dengan firewall di layer 3&4, firewall di layer 7 berfokus pada permintaan seperti (http, https, dns, dan lain-lain). biasanya firewall di layer ini digunakan untuk menjaga keamanan website dan membutuhkan aplikasi tambahan seperti wireshark, owasp zap, dan lain-lain.

B. Web Application Firewall berjalan di layer 7 yang berfungsi untuk menjaga sebuah website dari segala serangan seperti OWASP 10, untuk menjalankan waf kita membutuhkan aplikasi tambahan seperti, cloudflare WAF, AWS WAF, ModSecurity (open source).

No 5.

A. Log adalah catatan yang dibuat oleh sistem, aplikasi, atau perangkat untuk merekam aktivitas, kejadian atau kesalahan. jenis-jenis log utamanya adalah untuk mencatat aktivitas seperti login, logout, dan percobaan akses.

jenis-jenis log =

- system log
- application log
- security log
- web server log
- firewall log
- event log

B. Jenis anomali dalam log.

- Menemukan 404 atau status error

```
for baris in lines:
    cocok = log_pattern.search(baris)
    if cocok:
        data = cocok.groupdict()
        if data['status'] == '404':
            print(f"[{data['timestamp']}] {data['ip']} -> {data['path']} ({data['status']}) ")

[08/Mar/2025:10:23:50 +0700] 10.10.10.5 -> /confidential/hr_data.xlsx ([404])
[08/Mar/2025:08:05:02 +0700] 172.16.0.5 -> /index.html ([404])
[08/Mar/2025:09:00:07 +0700] 192.168.1.10 -> /robots.txt ([404])
[08/Mar/2025:09:20:54 +0700] 192.168.1.66 -> /robots.txt ([404])
[08/Mar/2025:10:08:54 +0700] 192.168.1.66 -> /env ([404])
[08/Mar/2025:09:45:21 +0700] 203.175.9.173 -> /admin/login.php ([404])
[08/Mar/2025:08:19:48 +0700] 10.10.10.5 -> /robots.txt ([404])
[08/Mar/2025:09:41:53 +0700] 45.77.12.88 -> /confidential/hr_data.xlsx ([404])
[08/Mar/2025:08:04:33 +0700] 45.77.12.88 -> /robots.txt ([404])
[08/Mar/2025:08:28:45 +0700] 45.77.12.88 -> /backups/db_backup.zip ([404])
[08/Mar/2025:10:21:07 +0700] 192.168.1.66 -> /env ([404])
[08/Mar/2025:08:07:48 +0700] 192.168.1.66 -> /admin/dashboard.php?id=1 ([404])
[08/Mar/2025:10:34:18 +0700] 10.10.10.5 -> /robots.txt ([404])
[08/Mar/2025:08:08:35 +0700] 10.10.10.5 -> /wp-login.php ([404])
[08/Mar/2025:08:46:19 +0700] 10.10.10.5 -> /admin/login.php ([404])
[08/Mar/2025:08:00:54 +0700] 192.168.1.10 -> /search?q=abc ([404])
[08/Mar/2025:10:43:49 +0700] 45.77.12.88 -> /robots.txt ([404])
[08/Mar/2025:09:24:32 +0700] 45.77.12.88 -> /robots.txt ([404])
[08/Mar/2025:09:19:56 +0700] 192.168.1.10 -> /search?q=abc ([404])
[08/Mar/2025:10:32:31 +0700] 192.168.1.66 -> /robots.txt ([404])
[08/Mar/2025:10:26:50 +0700] 192.168.1.10 -> /admin/dashboard.php?id=1 ([404])
[08/Mar/2025:10:24:47 +0700] 172.16.0.5 -> /confidential/hr_data.xlsx ([404])
[08/Mar/2025:09:20:15 +0700] 203.175.9.173 -> /env ([404])
[08/Mar/2025:10:20:40 +0700] 192.168.1.10 -> /wp-login.php ([404])
[08/Mar/2025:08:39:51 +0700] 192.168.1.10 -> /admin/dashboard.php?id=1 ([404])
```

Log diatas bisa disebut sebagai anomali karena ada percobaan dari ip-ip tersebut untuk mengakses file yang tidak ada, ini menjadi indikasi bahwa ada seseorang yang ingin mencari celah di dalam website.

- Menemukan ip dengan percobaan attempt terbanyak

```
[32] from collections import Counter
import re # Ensure re is imported

# Extract IP addresses directly from the parsed_data list
# This is more efficient as the parsing has already been done.
ips = [data['ip'] for data in parsed_data]

# Use Counter to count the occurrences of each IP address
ip_counter = Counter(ips)

# Print the 10 most common IP addresses and their counts
for ip, count in ip_counter.most_common(10):
    print(f"{ip} melakukan {count} permintaan")
```

```
➡ 100.100.100.100 melakukan 100 permintaan
45.77.12.88 melakukan 38 permintaan
172.16.0.5 melakukan 37 permintaan
192.168.1.10 melakukan 35 permintaan
203.175.9.173 melakukan 34 permintaan
192.168.1.66 melakukan 32 permintaan
10.10.10.5 melakukan 24 permintaan
```

Pada gambar di atas dapat disimpulkan bahwa ip 100.100.100.100 melakukan percobaan attempt terlalu banyak dibanding ip lainnya, ini dapat mengindikasikan bahwa ip ini mencoba untuk mencari celah pada login, dan dapat dicurigai bahwa ip ini menggunakan bot untuk attempt.