# Laporan Tugas Praktek
# Sigma dan yara

Mr.Foxzie
Noctra Lupra Bootcamp Trainee – Cybersecurity & Penetration Testing
IDN NETWORKERS

**Whoami?**
Saya Mr. Foxzie, seorang praktisi keamanan siber dengan fokus pada penetration testing dan bug bounty hunting. Aktivitas peretasan yang saya lakukan semata-mata untuk eksplorasi dan kesenangan (hack for fun), dengan tujuan menemukan dan melaporkan celah keamanan secara etis.

**Apa itu Sigma?**
Sigma adalah standardisasi format rule agnostik yang digunakan untuk mendeskripsikan log event patterns secara umum. Rule Sigma tidak bergantung pada platform SIEM tertentu (seperti ELK, Splunk, Wazuh), sehingga bisa dikonversi ke berbagai format vendor berbeda . format ini telah diadopsi secara luas dalam praktik threat hunting dan log security sebagai standar industri. Referensi seperti buku oleh Martinez (2022) dan Palacin (2021) membahas implementasi Sigma dalam threat intelligence dan incident response.
aturan sigma dari malware 01

```yaml
title: Pemuatan Modul 'kerne132.dll' yang Mencurigakan
id: 5a8a1b2c-3d4e-5f6a-7b8c-9d0e1f2a3b4c
status: stable
description: Mendeteksi upaya pemuatan modul DLL bernama 'kerne132.dll', Terkait dengan Lab01-01.exe.
author: mr.foxzie
date: 2025-07-27
logsource:
    product: windows
    category: image_load
detection:
    selection:
        ImageLoaded|contains: 'kerne132.dll'
    condition: selection
falsepositives:
    - Sangat rendah, karena ini adalah nama file yang tidak valid.
level: high
```

hasil generate rule

```
…/malware-exam/malware_lab  main ✗?  20:22
❯ sigmac -t sysmon -c sysmon deteksi_dll.yml

<!—RuleGroup groupRelation should be `or` <RuleGroup groupRelation="or"> —>

<!—Insert This Rule in <ProcessCreate onmatch="include"> section —>

                <Rule name="Pemuatan Modul 'kerne132.dll' yang Mencurigakan by mr.foxzie" groupRelation="and">
                        <ImageLoaded>kerne132.dll</ImageLoaded>
                </Rule>
```

aturan sigma malware 02

```yaml
title: Pembuatan Layanan Windows 'MalService'
id: 8d7b6c5a-4e3d-2a1f-b9c8-7e6d5c4b3a21
status: stable
description: Mendeteksi pembuatan layanan Windows baru dengan nama 'MalService'. Perilaku ini diketahui
terkait dengan sampel malware Lab01-02.exe.
author: mr.foxzie
date: 2025-07-27
logsource:
    product: windows
    category: service_creation
detection:
    selection:
        ServiceName: 'MalService'
    condition: selection
falsepositives:
    - Hampir tidak ada, karena nama layanan ini sangat spesifik.
level: critical
```

hasil generate rule

```
…/malware-exam/malware_lab  main ✘?  20:23
❯ sigmac -t sysmon -c sysmon deteksi_service.yml

<!--RuleGroup groupRelation should be `or` <RuleGroup groupRelation="or"> -->

<!--Insert This Rule in <ProcessCreate onmatch="include"> section -->

                <Rule name="Pembuatan Layanan Windows 'MalService' by mr.foxzie" groupRelation="and">
                        <ServiceName>MalService</ServiceName>
                </Rule>
```

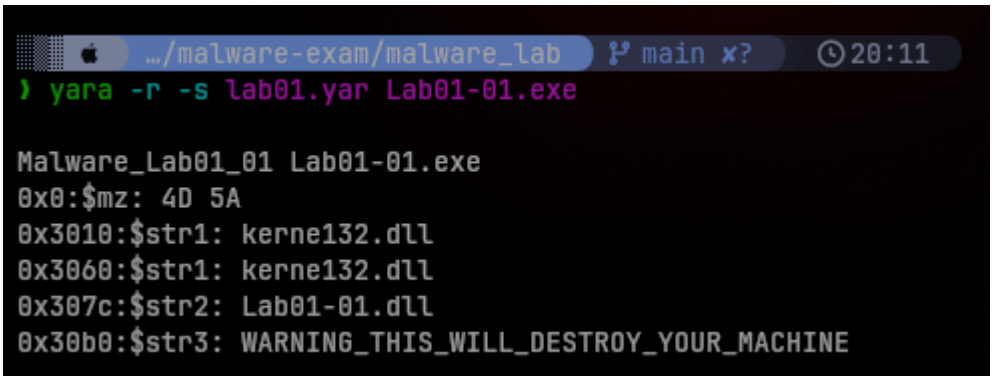
**Apa itu Yara?**

YARA adalah proyek open-source yang dirancang oleh Victor Alvarez sejak 2013, bahasa rule yang memungkinkan peneliti malware membuat deskripsi (signature) berdasarkan pola teks atau biner dalam file atau memory. Setiap rule terdiri dari metadata, bagian strings, dan kondisi Boolean. Rule ini memungkinkan klasifikasi malware secara spesifik berdasarkan byte sequence, ekspresi reguler, atau string teks.

rule yara 01

```
rule Malware_Lab01_01 {
    meta:
        description = "Mendeteksi sampel malware Lab 01-01"
        author = "mr.foxzie"
        date = "2025-07-27"
    strings:
        $mz = { 4D 5A } // Signature "MZ" di awal file
        $str1 = "kerne132.dll" ascii
        $str2 = "Lab01-01.dll" ascii
        $str3 = "WARNING_THIS_WILL_DESTROY_YOUR_MACHINE" ascii
    condition:
        $mz at 0 and (2 of ($str*)) // File harus PE (memiliki MZ di awal) dan mengandung setidaknya 2
dari 3 string mencurigakan.
}
```

hasilnya




rule yara 02

```
rule Malware_Lab01_02_UPX {
    meta:
        description = "Mendeteksi sampel malware terkompresi UPX Lab 01-02"
        author = "mr.foxzie"
        date = "2025-07-27"
    strings:
        $upx1 = "UPX!" ascii
        $upx2 = "UPX0" ascii
        $str1 = "MalService" ascii
        $str2 = "http://www.malwareanalysisbook.com" ascii
    condition:
        (uint16(0) == 0x5A4D) and (all of ($upx*)) and (1 of ($str*))
}
```

hasilnya