高度サイバーセキュリティ PBLIII

28G23027 川原尚己

- 演習 1 ：vSRX の基本設定
  - vSRX-NG の基本設定を行う
    - root ユーザのパスワード設定
      演習環境の vSRX-NG にて，”root”，”cli”，”configure”を実行し，編集環境に入る．
      “set system root-authentication plain-text-password”
      をパスワード=”Enpitpro”で実行する．
    - enpit ユーザの作成
      - “set system login user enpit class super-user”
      - “set system login user enpit authentication plain-text-password”

      を実行する．
      ”show system login”を実行すると，以下の出力を得た．

```
enpit@vsrx# show system login
user enpit {
    uid 2000;
    class super-user;
    authentication {
        encrypted-password "$6
    }
}
```

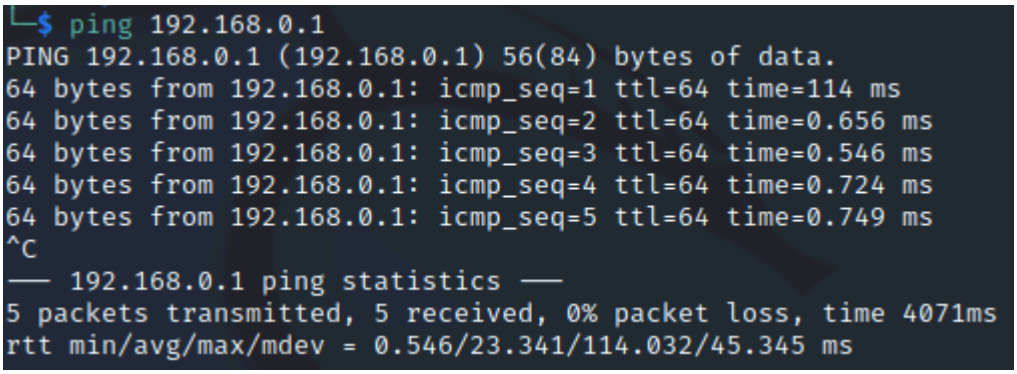
    - ホスト名は vsrx に設定
      “set system host-name vsrx”を実行．
    - 管理インターフェース（fxp0）の設定
      - set interfaces fxp0 unit 0 family inet address 10.10.0.1/16
      - set system services ssh root-login deny
    - telnet，ssh の設定
      以下のコマンドを実行する．
      - set system service telnet
      - set system services ssh root-login deny

  - enpit ユーザで telnet，ssh できることを確認する．
  - vSRX-NG のネットワーク設定を行う
    以下のコマンドを実行する．
    - set interfaces ge-0/0/0 description external

- set interfaces ge-0/0/0 unit 0 family inet address 192.168.0.1/24
- set interfaces ge-0/0/1 description dmz
- set interfaces ge-0/0/1 unit 0 family inet address 192.168.100.1/24
- set interfaces ge-0/0/2 description client
- set interfaces ge-0/0/2 unit 0 family inet address 192.168.200.1/24
- set security zones security-zone external interfaces ge-0/0/0.0
- set security zones security-zone dmz interfaces ge-0/0/1.0
- set security zones security-zone client interfaces ge-0/0/2.0
- set security zones security-zone external host-inbound-traffic system-services ping
- set security zones security-zone external host-inbound-traffic system-services traceroute
- set security zones security-zone dmz host-inbound-traffic system-services ping
- set security zones security-zone dmz host-inbound-traffic system-services traceroute
- set security zones security-zone client host-inbound-traffic system-services ping
- set security zones security-zone client host-inbound-traffic system-services traceroute
- set security zones security-zone external host-inbound-traffic protocols all except
- set security zones security-zone dmz host-inbound-traffic protocols all except
- set security zones security-zone client host-inbound-traffic protocols all except

・ 各ネットワークの サーバ/クライアントから ping での疎通確認を行う

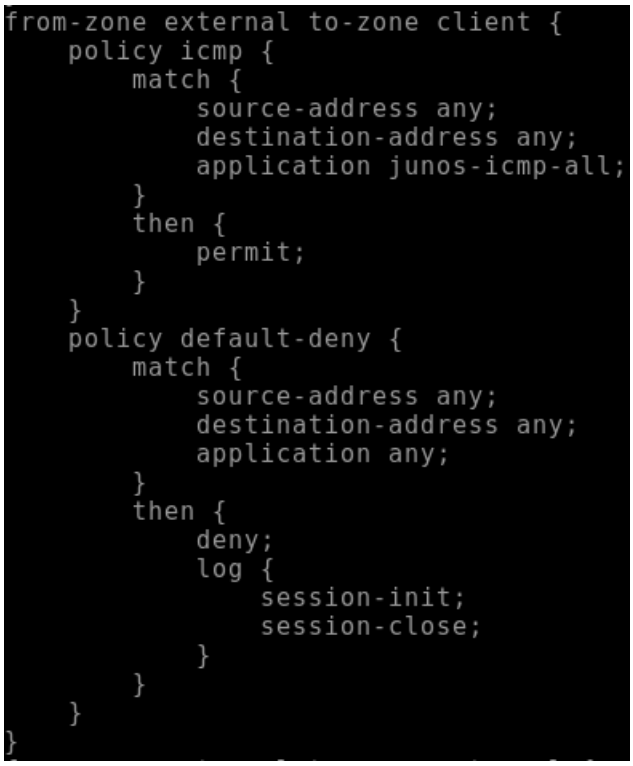
attacker，wordpress，client より，vSRX への ping の疎通確認を行った．以下の画像は attacker からの通信結果である．



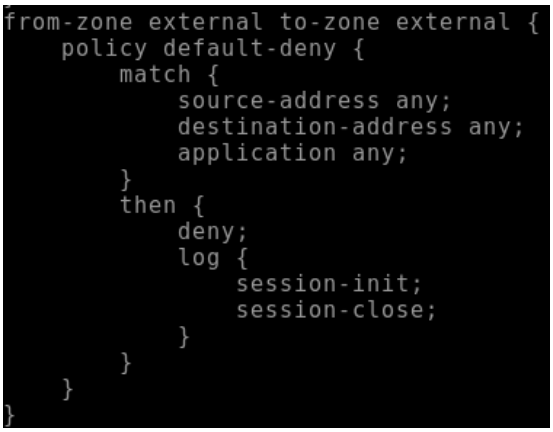
- 演習２：Firewall/Router の設定

  external->client の設定に必要なコマンドを記述する．他の設定に関するコマンドを載せると非常に煩雑であるため，show security policies での表示結果を張り付ける．

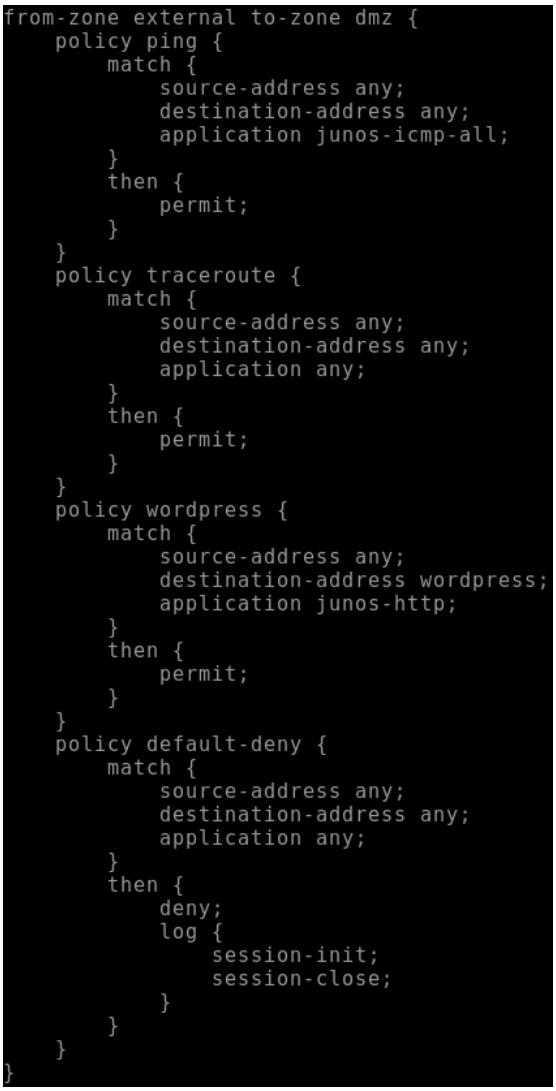
  - external->client の設定
    - set security policies from-zone external to-zone client policy icmp match source-address any
    - set security policies from-zone external to-zone client policy icmp match destination-address any
    - set security policies from-zone external to-zone client policy icmp match application junos-icmp-all
    - set security policies from-zone external to-zone client policy icmp then permit
    - set security policies from-zone external to-zone client policy default-deny match source-address any
    - set security policies from-zone external to-zone client policy default-deny match destintion-address any
    - set security policies from-zone external to-zone client policy default-deny match application any
    - set security policies from-zone external to-zone client policy default-deny then deny
    - set security policies from-zone external to-zone client policy default-deny then log session-init
    - set security policies from-zone external to-zone client policy default-deny then log session-close



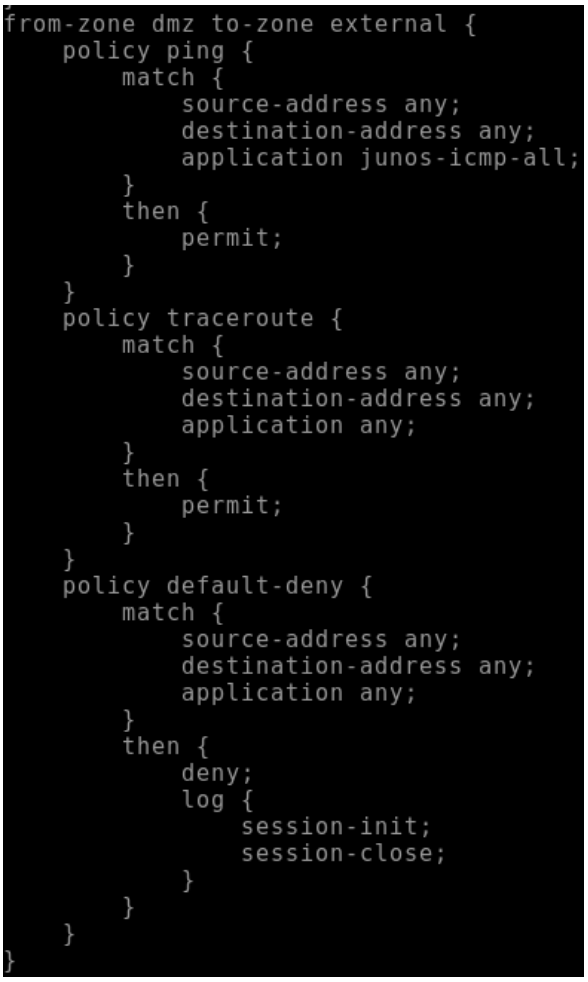
external->client



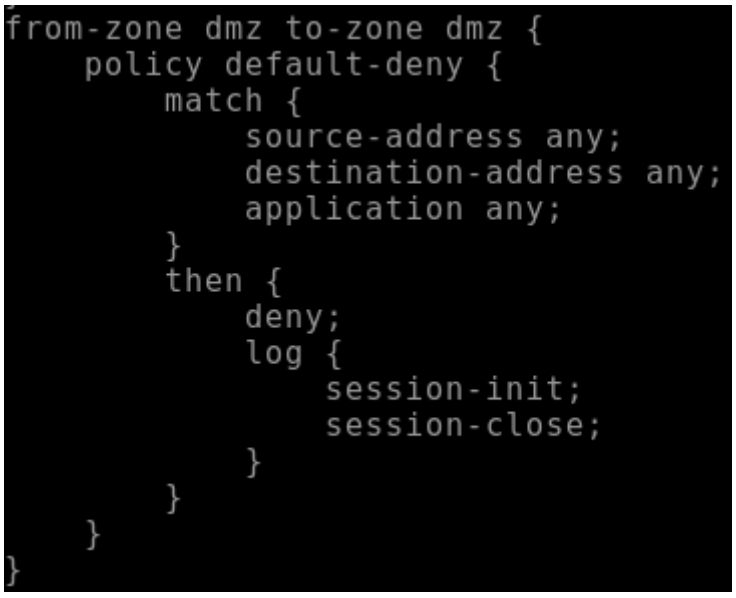
external->external



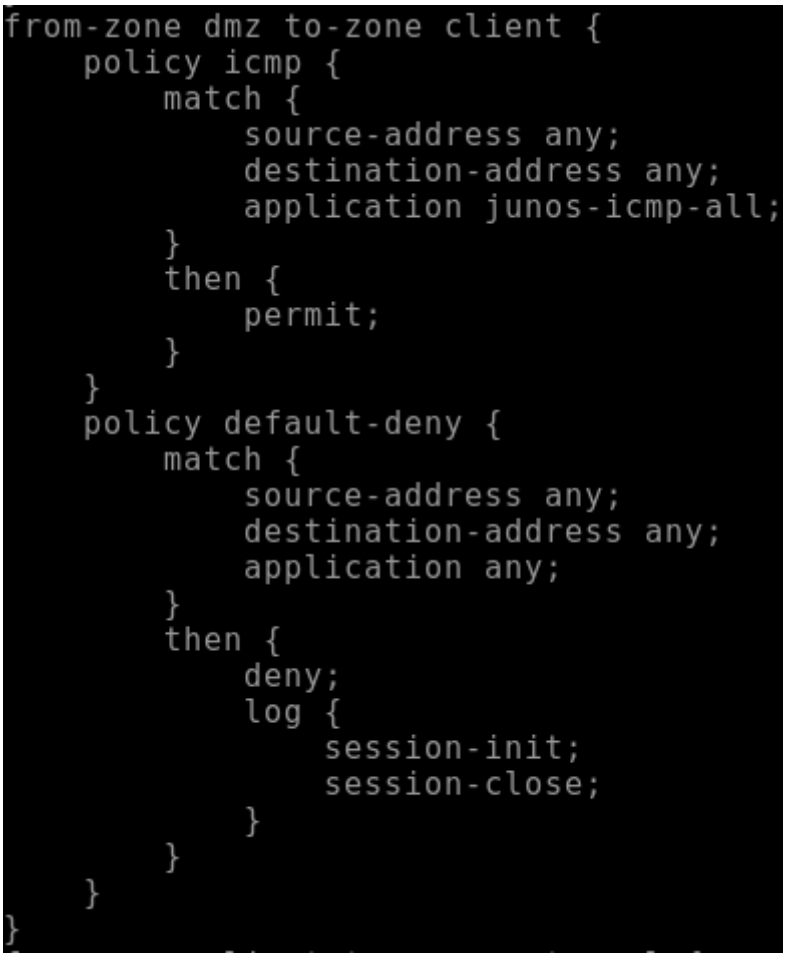
external->dmz



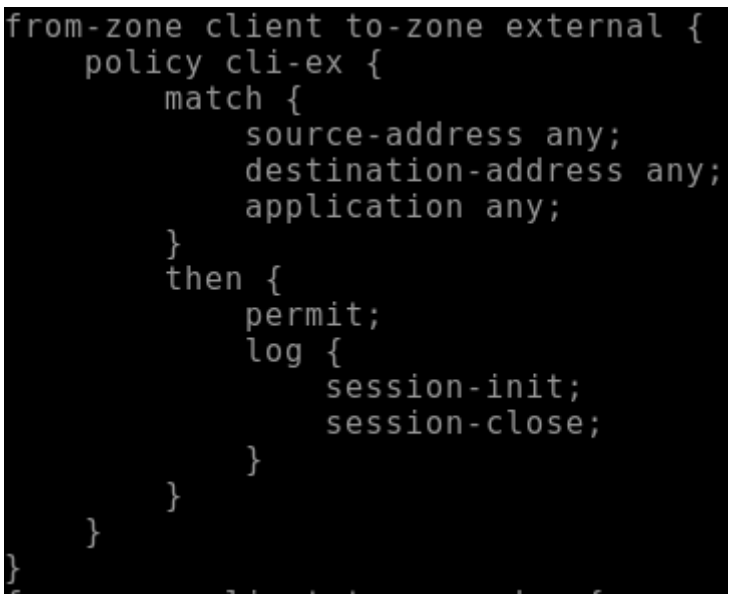
dmz->external



dmz->dmz



dmz->client



client->external

```
from-zone client to-zone dmz {
    policy cli-dmz wordpress {
        match {
            source-address any;
            destination-address wordpress;
            application junos-http;
        }
        then {
            permit;
        }
    }
    policy cli-dmz wiki {
        match {
            source-address any;
            destination-address wiki;
            application junos-http;
        }
        then {
            permit;
        }
    }
    policy cli-dmz ftp {
        match {
            source-address any;
            destination-address ftp;
            application junos-ftp;
        }
        then {
            permit;
        }
    }
    policy cli-dmz ntp {
        match {
            source-address any;
            destination-address ntp;
            application junos-ntp;
        }
        then {
            permit;
        }
    }
}
```

client->dmz

```
from-zone client to-zone client {
    policy cli-cli {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit;
        }
    }
}
```

client->client

また，dmz におけるアドレスブックの設定は以下のように行った．

```
enpit@vsrx# show security zones security-zone dmz
address-book {
    address wordpress 192.168.100.101/32;
    address wiki 192.168.100.102/32;
    address ftp 192.168.100.103/32;
    address ntp 192.168.100.105/32;
}
```

- 疎通確認
  attacker(external,192.168.0.102)　，　wordpress(dmz,192.168.100.101)　，client(client,192.168.200.201)を用い，各 zone から各 zone への 9 通りの疎通確認を ping を用いて行った．
  いずれの場合も先ほどの項での設定を満たすように挙動していた．

- 演習 3 - 1
  Wordpress 内のサーバに入った後
  “vim /etc/httpd/conf.d/mod_security.conf”を実行し，
  “SecurityRuleEngine DetectionOnly”を追加する．
  この後，client サーバから wordpress にアクセスしようとすると，以下のような画面が表示され，アクセスできない．

Service Unavailable

The server is temporarily unable to service your request due to maintenance downtime or capacity problems. Please try again later.

“sudo setsebool -P httpd_can_netword_connect 1”を実行することで設定を変更し，以下の画像のようにアクセスできるようになる．

Skip to content

Enpit CMS

Just another WordPress site

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

 Author adminPosted on October 24, 20221 Comment on Hello world!

Search for: Search ... Search

Recent Posts

- Hello world!

Recent Comments

- Mr WordPress on Hello world!

Archives

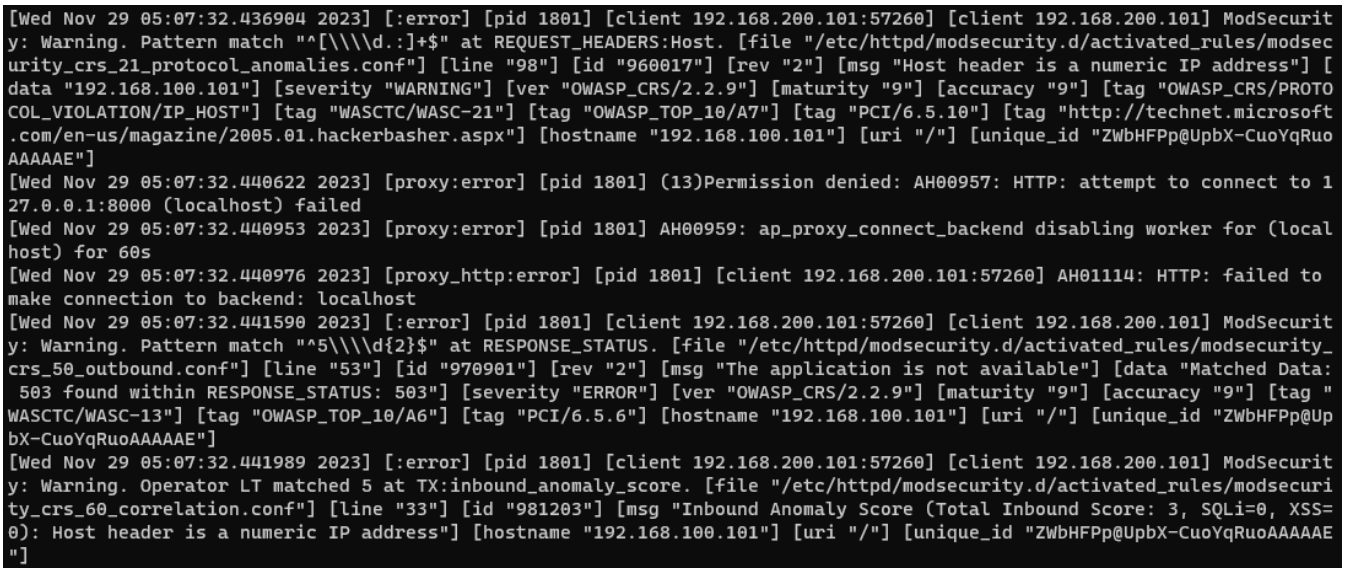
- October 2022

Categories

- Uncategorized

Meta

“sudo cat /var/log/httpd/error_log”により，エラーログを表示すると，以下のように表示された．



Mod security 由来のエラーメッセージは

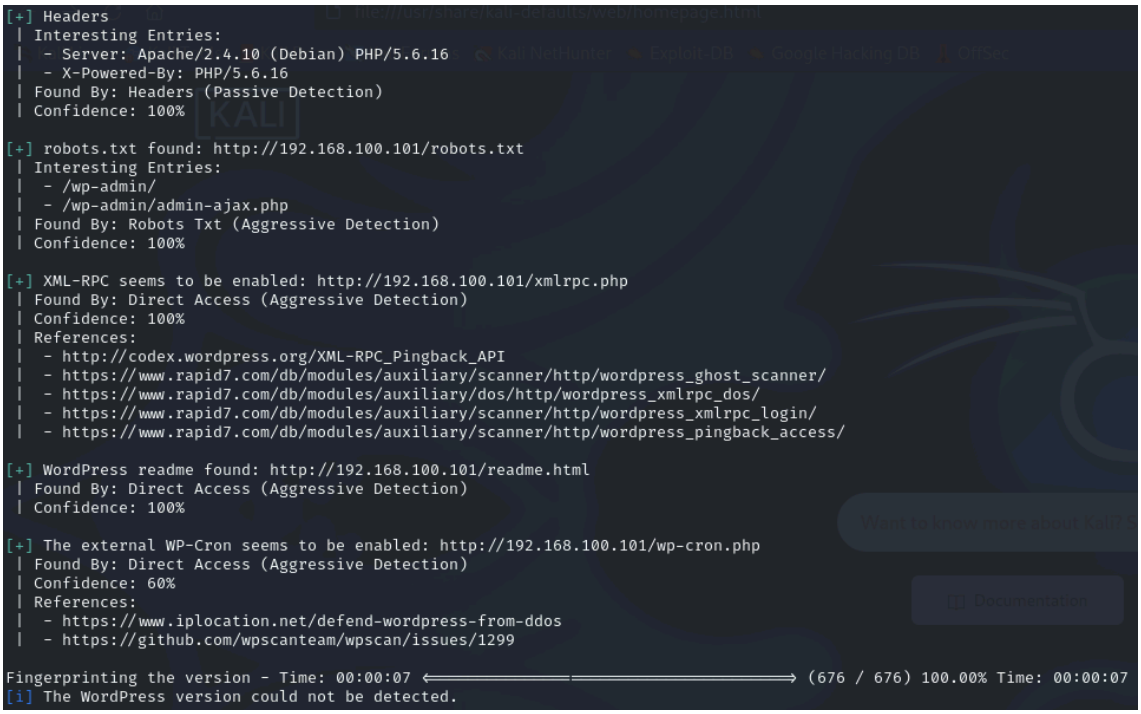
- Pattern match “5¥¥¥¥d{2}” at RESPONSE_STATUS.
- Operater LT matched 5 at TX:invound_anomaly_score

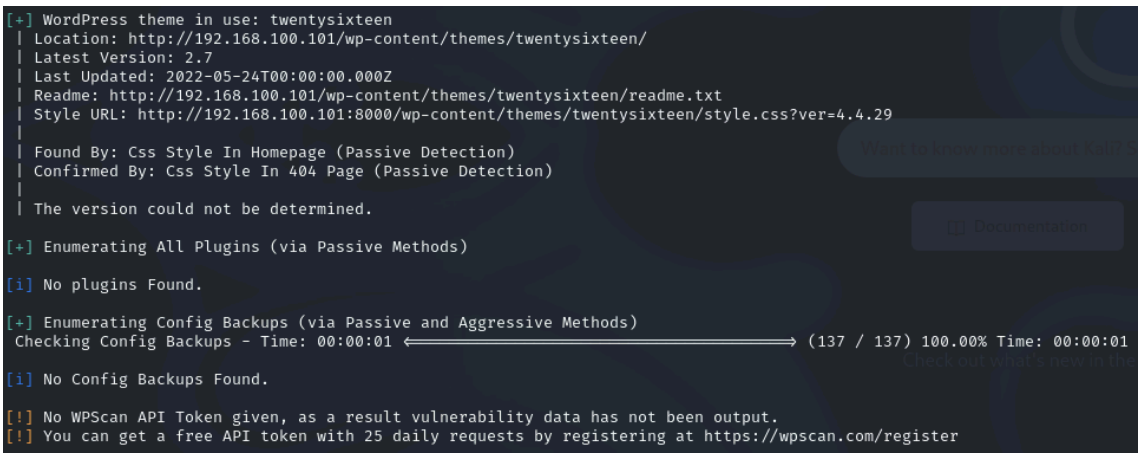
の二種類がある．

前者は RESPONSE_STATUS にて“5¥¥¥¥d{2}”という警告パターンにマッチしていることによる警告，後者は Operater LT が TX:invound_anomaly_score において”5”という警告パターンにマッチしていることによる警告である．

- 演習 3 - 2 ：wordpress の脆弱性診断

  client サーバ内の wpscan にて”wpscan --url 192.168.100.101”を実行し，wordpress の脆弱性診断を行った．





Headers を見ると PHP のバージョンが表示されている．このバージョンから，脆弱性を特定できるため，表示すべきではない．

また”WordPress theme in use: twentysixteen”においてもディレクトリや最新バージョン，最後にアップデートされた時刻などが表示されており，これも脆弱性を攻撃される原因となる可能性がある．