

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。

```

└─$ ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=114 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=0.656 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=0.546 ms
64 bytes from 192.168.0.1: icmp_seq=4 ttl=64 time=0.724 ms
64 bytes from 192.168.0.1: icmp_seq=5 ttl=64 time=0.749 ms
^C
— 192.168.0.1 ping statistics —
5 packets transmitted, 5 received, 0% packet loss, time 4071ms
rtt min/avg/max/mdev = 0.546/23.341/114.032/45.345 ms

```

- 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 destination-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

```

from-zone external to-zone client {
  policy icmp {
    match {
      source-address any;
      destination-address any;
      application junos-icmp-all;
    }
    then {
      permit;
    }
  }
  policy default-deny {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
      log {
        session-init;
        session-close;
      }
    }
  }
}

```

external->client

```

from-zone external to-zone external {
  policy default-deny {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
      log {
        session-init;
        session-close;
      }
    }
  }
}

```

external->external

```

from-zone external to-zone dmz {
  policy ping {
    match {
      source-address any;
      destination-address any;
      application junos-icmp-all;
    }
    then {
      permit;
    }
  }
  policy traceroute {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
  policy wordpress {
    match {
      source-address any;
      destination-address wordpress;
      application junos-http;
    }
    then {
      permit;
    }
  }
  policy default-deny {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
      log {
        session-init;
        session-close;
      }
    }
  }
}

```

external->dmz

```

from-zone dmz to-zone external {
  policy ping {
    match {
      source-address any;
      destination-address any;
      application junos-icmp-all;
    }
    then {
      permit;
    }
  }
  policy traceroute {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
    }
  }
  policy default-deny {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
      log {
        session-init;
        session-close;
      }
    }
  }
}

```

dmz->external

```

from-zone dmz to-zone dmz {
  policy default-deny {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
      log {
        session-init;
        session-close;
      }
    }
  }
}

```

dmz->dmz

```

from-zone dmz to-zone client {
  policy icmp {
    match {
      source-address any;
      destination-address any;
      application junos-icmp-all;
    }
    then {
      permit;
    }
  }
  policy default-deny {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      deny;
      log {
        session-init;
        session-close;
      }
    }
  }
}

```

dmz->client

```

from-zone client to-zone external {
  policy cli-ex {
    match {
      source-address any;
      destination-address any;
      application any;
    }
    then {
      permit;
      log {
        session-init;
        session-close;
      }
    }
  }
}

```

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、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_network_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 [admin](#) Posted on [October 24, 2022](#) [Comment on Hello world!](#)

Search for:

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。

```
[Wed Nov 29 05:07:32.436904 2023] [:error] [pid 1801] [client 192.168.200.101:57260] [client 192.168.200.101] ModSecurity: Warning. Pattern match "^[\\d\\.]+$" at REQUEST_HEADERS:Host. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_21_protocol_anomalies.conf"] [line "98"] [id "960017"] [rev "2"] [msg "Host header is a numeric IP address"] [data "192.168.100.101"] [severity "WARNING"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "OWASP_CRS/PROTOCOL_VIOLATION/IP_HOST"] [tag "WASCTC/WASC-21"] [tag "OWASP_TOP_10/A7"] [tag "PCI/6.5.10"] [tag "http://technet.microsoft.com/en-us/magazine/2005.01.hackerbasher.aspx"] [hostname "192.168.100.101"] [uri "/"] [unique_id "ZWbHFpp@UpbX-CuoYqRuoAAAAAE"]
[Wed Nov 29 05:07:32.440622 2023] [proxy:error] [pid 1801] (13)Permission denied: AH00957: HTTP: attempt to connect to 127.0.0.1:8000 (localhost) failed
[Wed Nov 29 05:07:32.440953 2023] [proxy:error] [pid 1801] AH00959: ap_proxy_connect_backend disabling worker for (localhost) for 60s
[Wed Nov 29 05:07:32.440976 2023] [proxy_http:error] [pid 1801] [client 192.168.200.101:57260] AH01114: HTTP: failed to make connection to backend: localhost
[Wed Nov 29 05:07:32.441590 2023] [:error] [pid 1801] [client 192.168.200.101:57260] [client 192.168.200.101] ModSecurity: Warning. Pattern match "^5\\\\\\\\d{2}$" at RESPONSE_STATUS. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_50_outbound.conf"] [line "53"] [id "970901"] [rev "2"] [msg "The application is not available"] [data "Matched Data: 503 found within RESPONSE_STATUS: 503"] [severity "ERROR"] [ver "OWASP_CRS/2.2.9"] [maturity "9"] [accuracy "9"] [tag "WASCTC/WASC-13"] [tag "OWASP_TOP_10/A6"] [tag "PCI/6.5.6"] [hostname "192.168.100.101"] [uri "/"] [unique_id "ZWbHFpp@UpbX-CuoYqRuoAAAAAE"]
[Wed Nov 29 05:07:32.441989 2023] [:error] [pid 1801] [client 192.168.200.101:57260] [client 192.168.200.101] ModSecurity: Warning. Operator LT matched 5 at TX:inbound_anomaly_score. [file "/etc/httpd/modsecurity.d/activated_rules/modsecurity_crs_60_correlation.conf"] [line "33"] [id "981203"] [msg "Inbound Anomaly Score (Total Inbound Score: 3, SQLi=0, XSS=0): Host header is a numeric IP address"] [hostname "192.168.100.101"] [uri "/"] [unique_id "ZWbHFpp@UpbX-CuoYqRuoAAAAAE"]
```

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
| Interesting Entries:
| - Server: Apache/2.4.10 (Debian) PHP/5.6.16
| - X-Powered-By: PHP/5.6.16
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://192.168.100.101/robots.txt
| Interesting Entries:
| - /wp-admin/
| - /wp-admin/admin-ajax.php
| Found By: Robots Txt (Aggressive Detection)
| Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.100.101/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - http://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.100.101/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.100.101/wp-cron.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 60%
| References:
| - https://www.iplocation.net/defend-wordpress-from-ddos
| - https://github.com/wpscanteam/wpscan/issues/1299

Fingerprinting the version - Time: 00:00:07 ← (676 / 676) 100.00% Time: 00:00:07
[!] The WordPress version could not be detected.
```

```
[+] WordPress theme in use: twentysixteen
| Location: http://192.168.100.101/wp-content/themes/twentysixteen/
| Latest Version: 2.7
| Last Updated: 2022-05-24T00:00:00.000Z
| Readme: http://192.168.100.101/wp-content/themes/twentysixteen/readme.txt
| Style URL: http://192.168.100.101:8000/wp-content/themes/twentysixteen/style.css?ver=4.4.29
| Found By: Css Style In Homepage (Passive Detection)
| Confirmed By: Css Style In 404 Page (Passive Detection)
| The version could not be determined.

[+] Enumerating All Plugins (via Passive Methods)
[!] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:01 ← (137 / 137) 100.00% Time: 00:00:01
[!] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register
```

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。