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．

テキスト

自動的に生成された説明

* 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．

テキスト

自動的に生成された説明

* 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

テキスト

自動的に生成された説明

external->client

テキスト

自動的に生成された説明

external->external

テキスト

自動的に生成された説明

external->dmz

テキスト

自動的に生成された説明

dmz->external

テキスト

自動的に生成された説明

dmz->dmz

テキスト

自動的に生成された説明

dmz->client

テキスト

自動的に生成された説明

client->external

テキスト

自動的に生成された説明

client->dmz

テキスト

自動的に生成された説明

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．

テキスト

自動的に生成された説明

* 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．

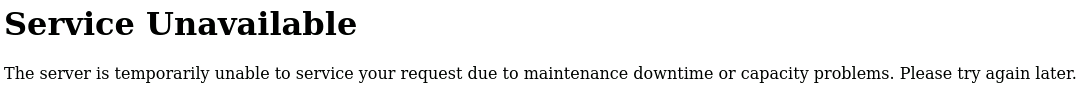
* 演習３-１

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．



“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．

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション, メール

自動的に生成された説明

テキスト

自動的に生成された説明“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．

テキスト

自動的に生成された説明

テキスト

自動的に生成された説明

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．