**※実習5（MailサーバーI）が終わっていることが前提。**

**●実習７－１．ログの運用監視（journald、rsyslog）**

不正なサイトからの攻撃が発生していないかを監視し、必要に応じて攻撃元を確認することが必要です。

　ログの内容を活用し、運用監視に役立てます。

**（１）ログの設定確認**

①カーネルのログを確認しなさい。

**確認コマンド　　→**

sudo journalctl -k

②ログの保存先を確認しなさい。

**確認コマンド　　→**

sudo cat /etc/systemd/journald.conf

Storage=[ auto ]　なので保存先は：［**/var/log/journal** ］

③どこで出力されたログかなどの詳細を確認する

**確認コマンド　　→**

sudo journalctl -o verbose

**（２） 認証ログの監視**

**①認証に関するエラーをログで確認**

**ssh接続において、ログイン認証に失敗した場合のログを確認します**

・Windows側「TeraTerm」を使用して、LinuxサーバーへSSH接続する

　ユーザ名「各自のユーザID」、パスワード「linux」(誤りのパスワード)でログインする。

**・認証に失敗したログを表示**

**コマンド　　 →**

Sudo lastb

（３）Webサーバーアクセスの監視（**まず、nginxの停止、apacheの起動を確認する。**）

①ステータスコード404により、存在しないabc.html ページがアクセスしたログを表示する

・Webサーバーアクセスを監視するため、**追加されたログを常に表示する**

sudo cat /var/log/apache2/access.log

**コマンド　　 →**

・Windows側でブラウザから「 http://サーバーIPアドレス/abc.html 」にアクセスする

下記のようなログが追加されることを確認する。

　　10.200.0.79 - - [11/Jun/2023:10:56:56 +0900] "**GET /abc.html HTTP/1.1" 404 206** "-" "Mozilla/5.0 　(Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

・「Ctrl」＋ｃ を入力し、追加されたログを常に表示するコマンドを終了する

　　②頻発に404のエラーを返している状況がある為、ログから404のステータスコードを返してい

る行のみを抽出して下さい（ステータスコード以外の部分での404に関しては、目視で除外）

　　（指定したログファイルの内容が何も表示されない（空の）場合は、ログローテーションされ

ているので、ファイル名を、「ログ名-最近の日付」にして確認）

　　　　　 抽出コマンド　→

sudo cat /var/log/apache2/access.log | grep 404

③Webサーバーログファイルの保存

②で抽出作成された結果をリダイレクト機能により、「access.kad07.log」の名前で保存する。

**コマンド　→**

sudo cat /var/log/apache2/access.log | grep 404 > access.kad07.log

（４）Mailサーバーアクセスの監視（**実習05のpostfixを使用する。設定や起動を確認**。）

①root@ecccomp.ac.jp宛にメールを送りなさい。タイトルは「test」、本文は「mail test!!」。

メールの受信については、確認は必要ありません。

Mail root@ecccomp.ac.jp

**コマンド　　 →**

②①でのメール送信のログを確認しなさい。（チェック項目１）

sudo cat /var/log/mail.log

**コマンド　　 →**

③①でのメール送信のログをmail.kad07.logに出力しなさい。

**コマンド　　 →**

sudo sh -c 'cat /var/log/mail.log | grep "to=<root@ecccomp.ac.jp>" > /var/log/mail.kad07.log'

**●実習７－２．DNSのログ管理**

DNS(bind)のログを取得できるように設定する。ログは「/var/log/named/」に保存する。

**（１）保存先のディレクトリを作成しなさい。ここでは、オーナー、グループなどの設定も行う。**

①　保存先のディレクトリを作成

**sudo mkdir /var/log/named**

**コマンド→**

② ①で作成したディレクトリにオーナー（bind）、グループ（bind）を設定する。

sudo chown bind:bind /var/log/named

**コマンド→**

③ ②の設定ができているか確認する。

sudo ls -l /var/log/named

**コマンド→**

**（２）ログファイルの指定**

①　ログファイルを「bind.queries.log」に設定しなさい。(/etc/default/named)

**Sudo vi /etc/named.conf.options**

**コマンド→**

追加した内容：［ 　］

②　ログ取得の設定をしなさい。（/etc/bind/named.conf.optionsの修正）

**Sudo vi** /etc/bind/named.conf.options

**コマンド→**

設定内容：

|  |
| --- |
| logging {  　channel bind-queries-log {  　　file "/var/log/named/bind.queries.log" versions 10 size 10m;  　　severity info;  print-time yes;  print-severity yes;  print-category yes;  };  category queries{  ”bind-queries-log";  };  }; |

　DNSのその他の設定も確認しておくこと。（ゾーンファイルやDNSサーバーアドレス設定など）

③　設定ファイルの文法チェックをしてからDNSサーバーを再起動する。

**Sudo systemctl restart named**

**コマンド→**

④　「クラス名.ecccomp.ac.jp」のIPアドレスを確認しなさい。（nslookupまたはdig）

**sudo nslookup sk2a03.ecccomp.ac.jp**

**コマンド→**

⑤　④のクエリーのログ(bind.queries.log)が取得できたか確認しなさい。(チェック項目2)

**Sudo cat bind.queries.log**

⑥ ⑤で確認できた内容をbind.kad07.logに出力しなさい。

sudo sh -c "cat /var/log/named/bind.queries.log > bind.kad07.log"

**●実習７－３．logwatchの設定**

ログの分析や確認ができるツールであるlogwatchをインストールし、設定する。

**（１）logwatchのインストール**

①　logwatchをインストールしなさい。

sudo apt install –y logwatch

**コマンド→**

②　logwatchの一時ディレクトリ(/var/cache/logwatch)作成しなさい。

sudo mkdir /var/cache/logwatch

**コマンド→**

**（２）logwatchの設定**

①　logwatchの設定ファイル(/usr/share/logwatch/default.conf/logwatch.conf)を

/etc/logwatch/conf/にコピーする。

**コマンド→**

sudo cp /usr/share/logwatch/default.conf/logwatch.conf

/etc/logwatch/conf/logwatch.conf

②　logwatch.confファイルを開く。

Sudo vi

**コマンド→**

③　次のように設定を変更しなさい。

|  |
| --- |
| Output = mail　　・・・　メールに送る  Mailto = メールの送信先 (例ie2a99@ecccomp.ac.jp)  Range = Today　・・・　本日 |

④　logwatchを起動する。

Sudo logwatch

**コマンド→**

**（３）ログを指定したメールアドレスに送信する。**

**指定したアドレス（クラス名番号@ecccomp.ac.jp）ログフィアルを送信する。**

1. logwatchからログファイルを指定したメールアドレスへ送信する。

sudo logwatch --output mail

**コマンド→**

1. telnetコマンドを使用して①で送信されたメールの内容を確認する。（チェック項目3）

sudo telnet localhost 110

（**実習05のpop3を使用）**

**コマンド→**

＊ユーザIDとパスワードは送信したメールアドレスのものを入力すること。

③ ②で確認したファイルをlogwatch.kad07logへ出力する。メールはMaildir/cur/に保存され

る。

**コマンド→**

●**チェック項目**

**以下の3つを教員にチェックしてもらうこと**

* **実習7-1（4）②**[**root@ecccomp.ac.jp**](mailto:root@ecccomp.ac.jp)**へのメール送信ログが確認できる**
* **実習7-2（2）⑤　　DNSクエリのログが確認できる**
* **実習7-3（3）②　　logwatchから送信されたメールが確認できる**

**●実習７－４．提出用ファイルの作成と提出**

①access.kad07.log、mail.kad07.log、bnid.kad07.log、logwatch.kad07.logをコピーし（今回はファイルが短いのでcatでもOK）、クラス名番号access.kad07.log、クラス名番号mail.kad07.log、クラス名番号bind.kad07.log、クラス名番号logwatch.kad07.logにそれぞれ名前を変更する。

**●課題提出**

**作成した４つのファイル（クラス名番号access.kad07.log、クラス名番号mail.kad07.log、クラス名番号bind.kad07.log、クラス名番号logwatch.conf）とログファイル（クラス名番号日付.log）を「実習07\_クラス番号氏名」のフォルダに入れてsv23へ提出しなさい。**