Spectrum Technology

V1.0 2017/10/02

抜粋

ホワイトハッカ育成ツール

～ひとりで出来る脆弱性試験、情報セキュリティ人材不足解消～

実践編

KALI BY OFFENSIVE SECURITY

Raspberry Pi

スペクトラム・テクノロジー株式会社

https://spectrum-tech.co.jp

sales@spectrum-tech.co.jp

ST Spectrum Technology

育成ツール　目次

抜粋

注意

自社のサーバに対して実施してください。他のサーバに実施することは犯罪です

育成ツール　目次

既に発売中のWiFiプロトコル・アナライザで対応しますので本資料では割愛します。

抜粋

注意

自社のサーバに対して実施してください。
他のサーバに実施することは犯罪です

Kali運用マニュアル

1. Raspberry Piについて

   既に全世界で1000万台以上販売された手のひらサイズのコンピュータです。LinuxベースのRasbianOSで動作しております。

2. Linux基本コマンド

   ① システム関係

- 起動：電源を入れると自動で起動します。
- 再起動：# reboot

  又は、アプリケーション>ログアウト>再起動；左上のメニューから
- 終了： # shutdown

  又は、アプリケーション>ログアウト>シャットダウン；左上のメニューから
- ログアウト # exit

  又は、アプリケーション>ログアウト>ログアウト；左上のメニューから
- 日本語／英語の入力切替：キーボードのshift+spaceを同時に押します。又は右上のアイコン（右から3個目）からプルダウンで選択

Kali運用マニュアル

2. Linux基本コマンド

② ディレクトリ操作、コピー、移動、削除

root@kali:~# cd /root/Documents　ディレクトリの切り替え

root@kali:/root/Documents# ls　ファイルとディレクトリの表示（表示したら操作したいファイルを右クリックでコピペして操作します

root@kali:~# cp ファイル名　ディレクトリ　配下のディレクトリのファイルを別のディレクトリへコピー

root@kali:~# mv ファイル名　ディレクトリ　配下のディレクトリのファイルを別のディレクトリへ移動

root@kali:~# rm ファイル名　ファイルの削除

便利な機能　rm –help　コマンドのオプションが分からない場合は、ヘルプで問い合わせる。すべてのコマンド共通(マイナスを2個とhelp)

③ ユーザ権限、プロセス他

root@kali:~ $ su -　スーパーユーザ（root)に切り替え、パスワードを入力

root@kali:~# ps a　現状の動いているプロセスを表示

root@kali:~# kill　特定のプロセスを強制終了

root@kali:~# apt-get install pkg　パッケージのインストールなどに使用

root@kali:~# date　日付、時間の設定を行います。

root@kali:~# leafpad /etc/network/interfaces　インタフェースに記述してい内容を変更します。Viよりも使いやすいです。

④ モジュール、usb、メモリ、HDDなどの表示

root@kali:~# lsmod　linuxのモジュールリスト表示

root@kali:~# lsusb　usbのデバイス表示

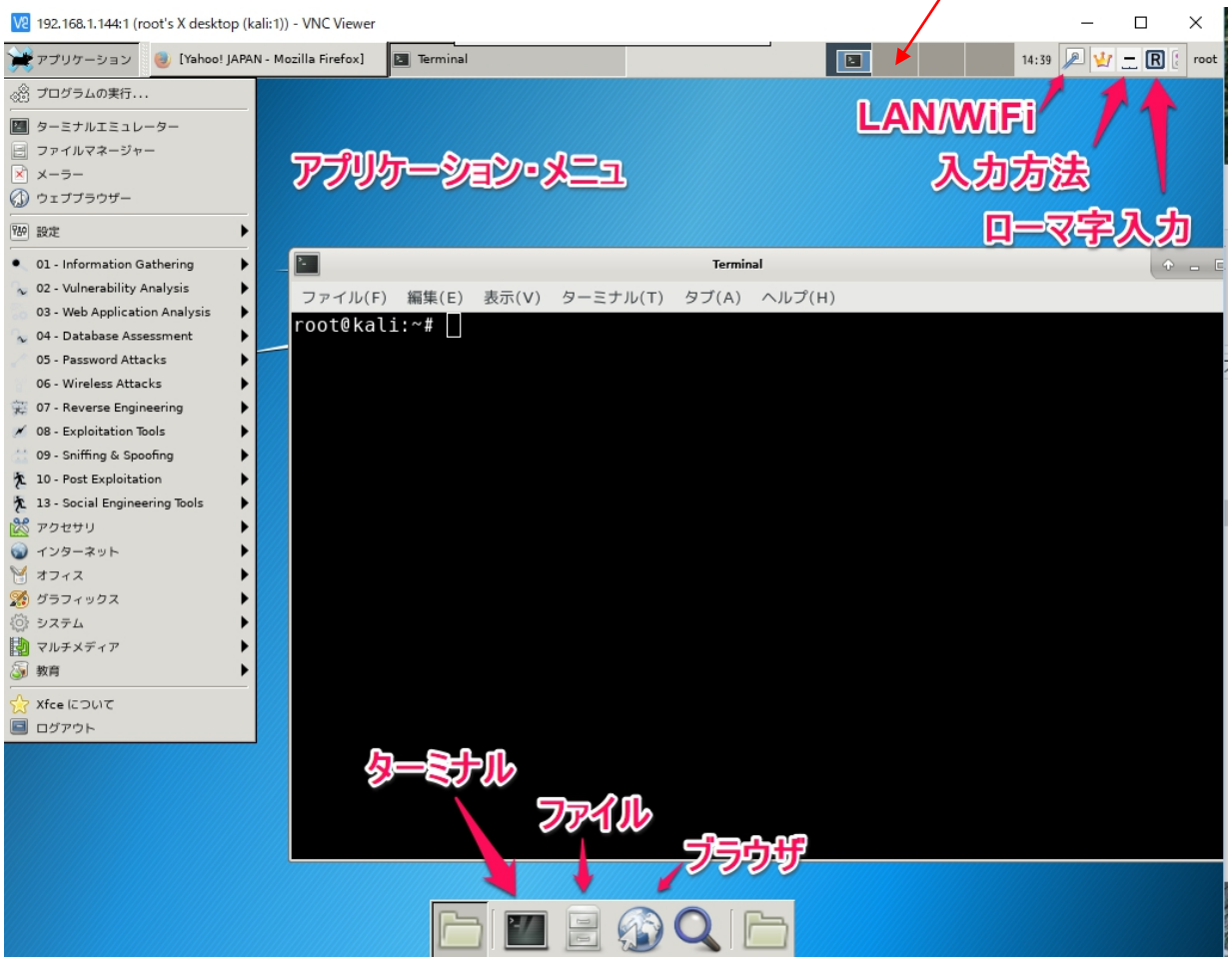
root@kali:~# free -mt　メモリ使用状態表示

root@kali:~# df -h　HDD（マイクロSD）の使用状態表示

Kali運用マニュアル

3. Kali基本操作

① 表示画面と内容



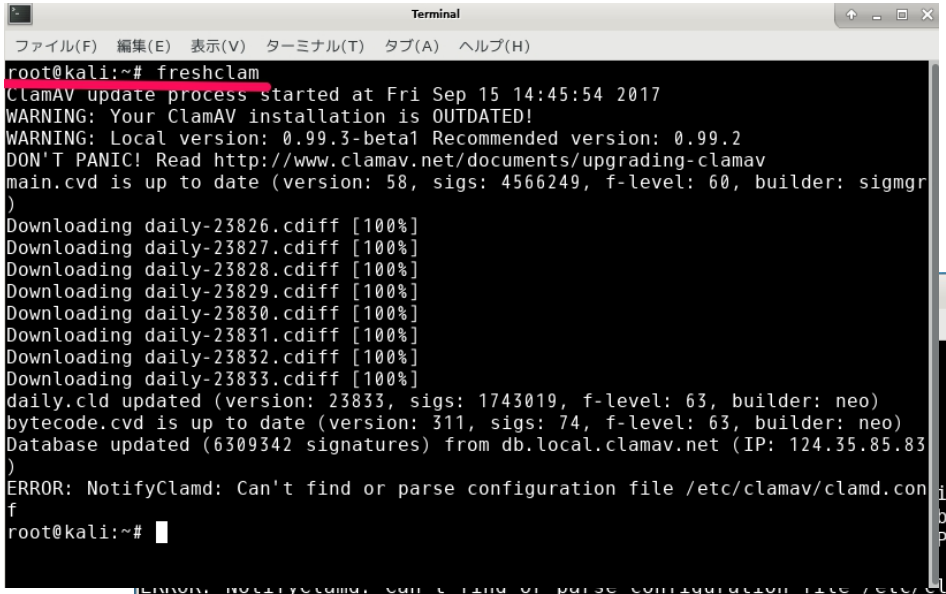
Kali運用マニュアル

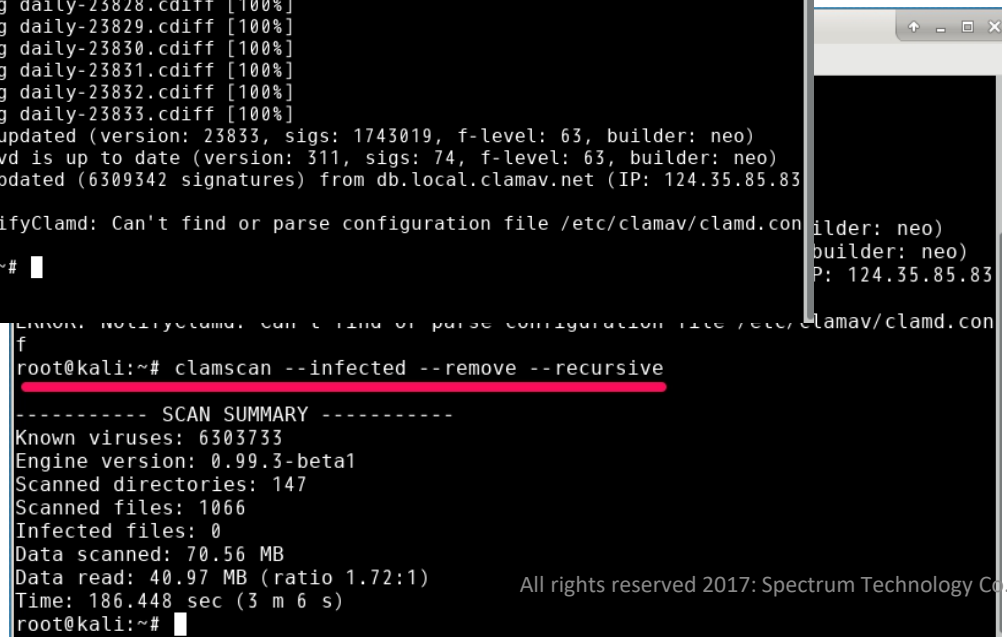
4. 日常運用

① セキュリティ対策（アンチウイルス更新、スキャン）

- アンチウイルス対策として無料のclamAVをインストールしてます。
- 手動での運用を基本としてます。

パターンファイル更新
freshclam　　手動スキャンを実施する場合は自動で更新されます。
手動でスキャン
clamscan --infected --remove --recursive



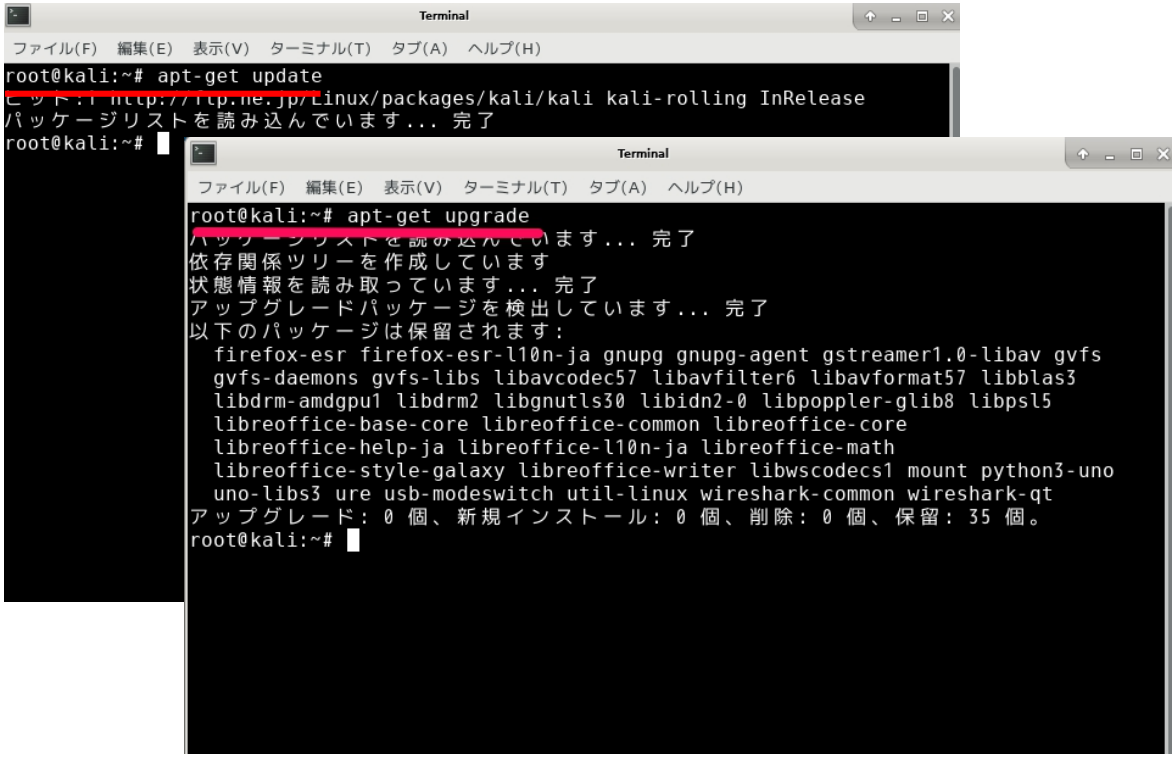


Kali運用マニュアル

4. 日常運用

② インストール済パッケージの更新リスト、アップグレード

- Linuxの場合は、頻繁に更新が発生します。アップグレードを定期的に実施してください。
- 更新前には、バックアップを取ることをお勧めします。特にアップグレードはまれに動作不良、戻せない状態が発生します。自己責任で実施してください。



更新リスト取得
apt-get update
アップグレード実施
apt-get upgrade

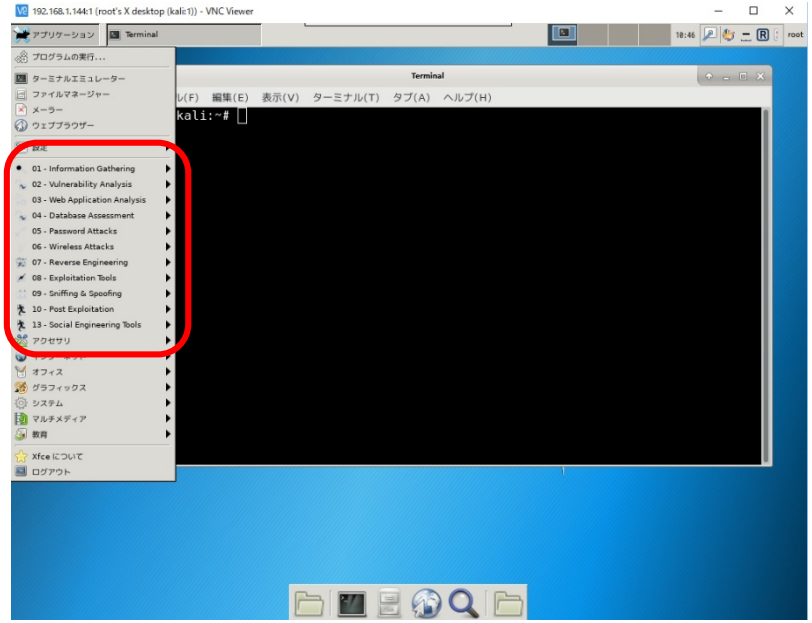
Spectrum Technology

ホワイトハッカ育成プログラム
①. Kaliメニュー

- Kaliとは
  - Kali Linuxは、世界レベルの情報セキュリティトレーニングと侵入テストサービスを提供するOffensive Securityによって維持管理されているオープンソースプロジェクトです。Kali Linuxに加えて、Offensive SecurityはExploit Databaseと無料のオンラインコースMetasploit Unleashedも管理しています。
  - https://www.kali.org/

- Kaliメニュー
  - 今回はよく使われる代表的なアプリをインストールしました。
  - nmap, maltegroce, burpsuite, owasp-zap, sqlmap, hydra, john, metasploit, aircrack-ng, wireshark(*1)

  (*1):vnc接続では動作しません



ホワイトハッカ育成プログラム
①. Kaliメニュー

- nmap　　ポートスキャン（侵入ポートを調査）
- maltego　ce　　ドメイン、サーバなどの情報収集
- burpsuite　webサイト通信確認、web脆弱性診断（有料）
- owasp-zap　　web脆弱性診断（無料）
- sqlmap　　sqlインジェクションのテスト
- hydra　　アカウント・クラック・ツール
- john　　パスワードの強度チェック
- metasploit　　ハッキング・ツール
- armitage　　ハッキング・ツールGUI版
- exploit DB　　脆弱性試験用検体
- wireshark(*1)　　プロトコル・アナライザ
  (*1):vnc接続では動作しません
- aircrack-ng　　wifiの脆弱性チェック、ハッキング・ツール
  既に発売中のWiFiプロトコルアナライザで対応しますので、説明は割愛します。なお、本コマンドを使用するにはユニキャストが見れ、モニターモードになる2．4G　WiFi　USBが必要になります。内蔵のWiFiでは対応できません。
- 他のアプリもたくさんあります。

Spectrum Technology

ホワイトハッカ育成プログラム
②. nmap(ポートスキャン)

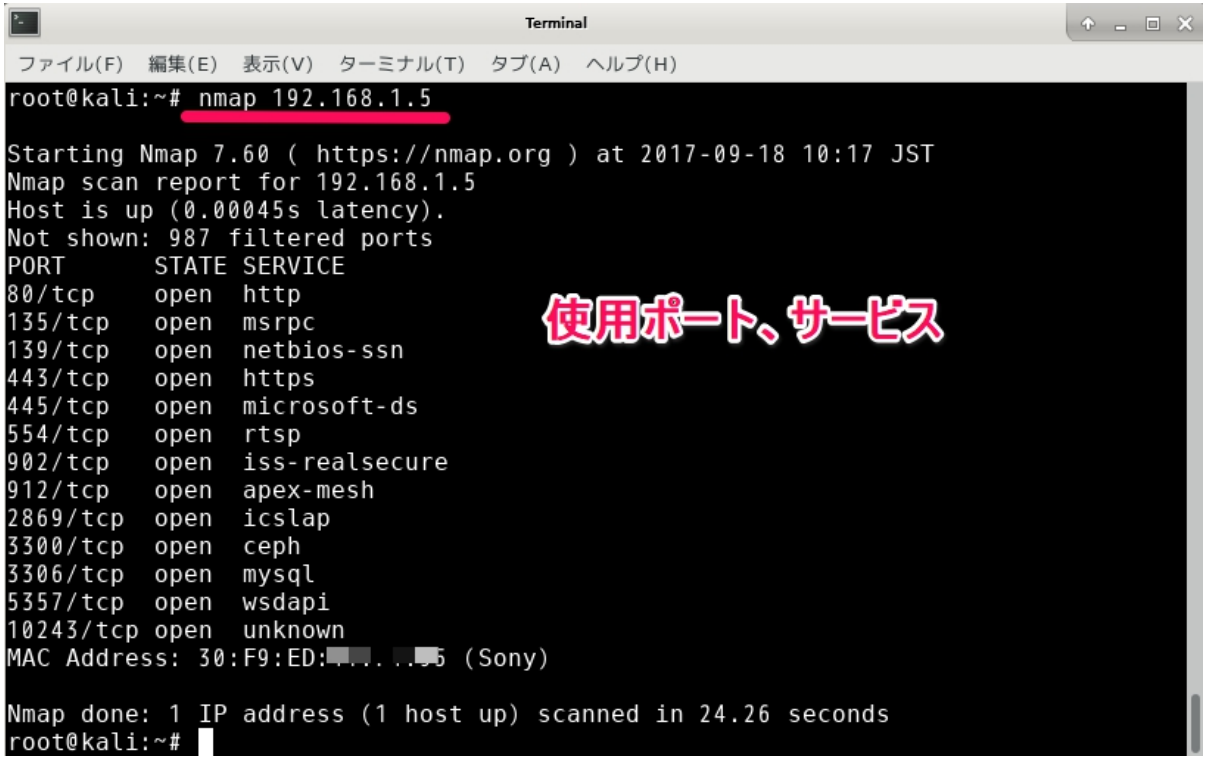
ポート・スキャン
nmap IPアドレス

- ポート・スキャン：特定端末の使用ポート調査

  # nmap 192.168.1.5

  　　調査のIPアドレス

  ・端末が使用している
  ポート、サービスを調査

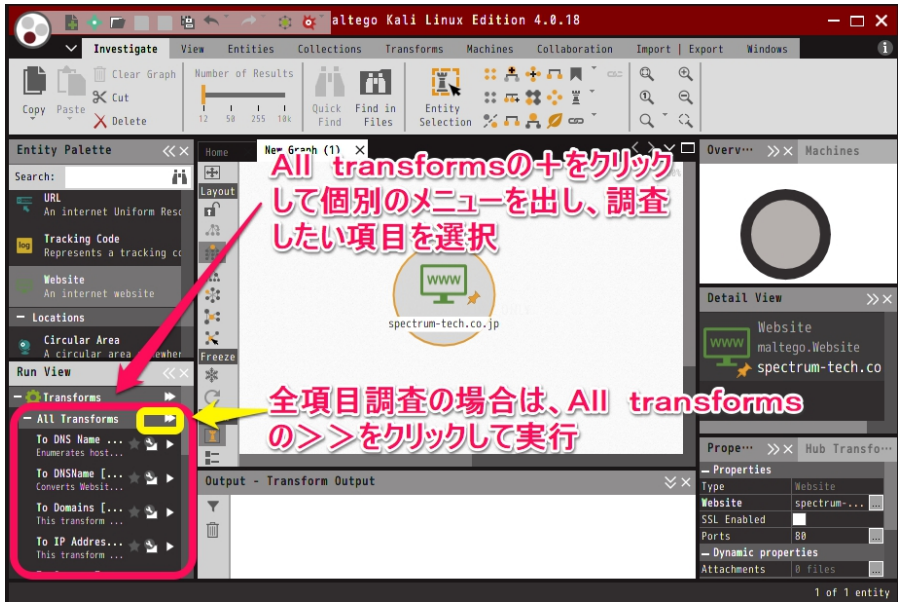


Spectrum Technology

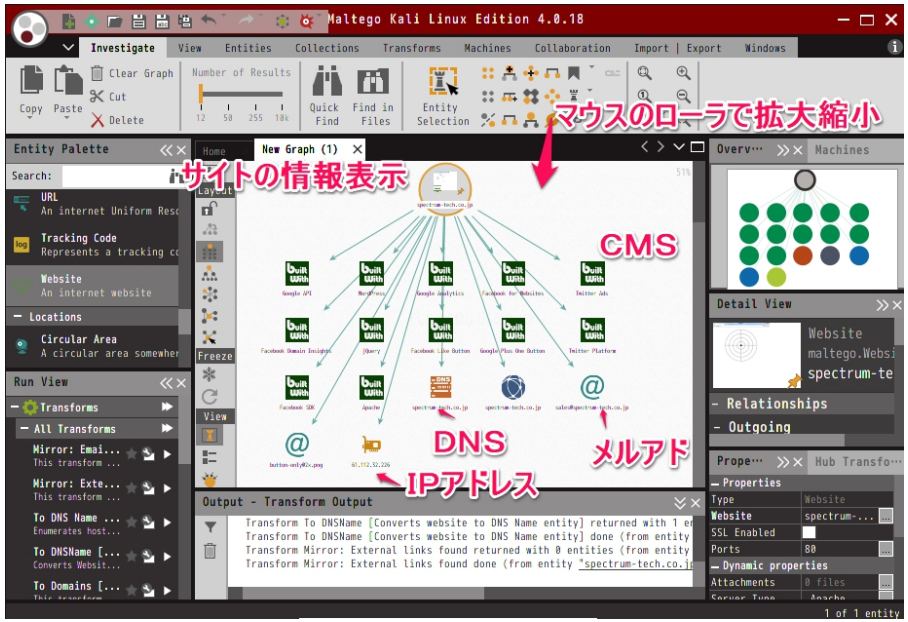
ホワイトハッカ育成プログラム
③. maltego　ce(情報収集)

- maltego運用
  5. webサイト調査
     - D)　左のRun viewからtransforms>all transformsを選び、>>マークをクリックします。
     - E)　サイトの関連情報が表示されます（IPアドレス、DNS，メール、CMSなど）。

D)



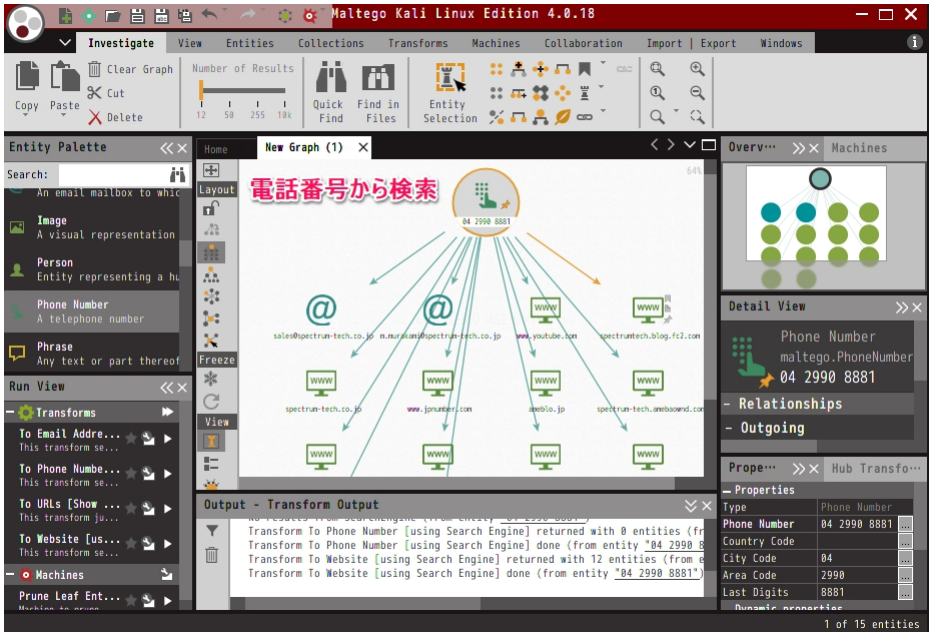
E)



Spectrum Technology

ホワイトハッカ育成プログラム
③. maltego　ce(情報収集）

- maltego運用
  8. 電話番号調査
     - 左のentity paletteからpersonal>phone numberを選びドラッグします。アイコンをダブルクリックして、検索したい電話番号を入力します。（国番号は、空欄にします）
     - Run view>transformの>>をクリックして結果を確認。インターネット上の情報が表示されます。（メルアド、掲載サイトなど）

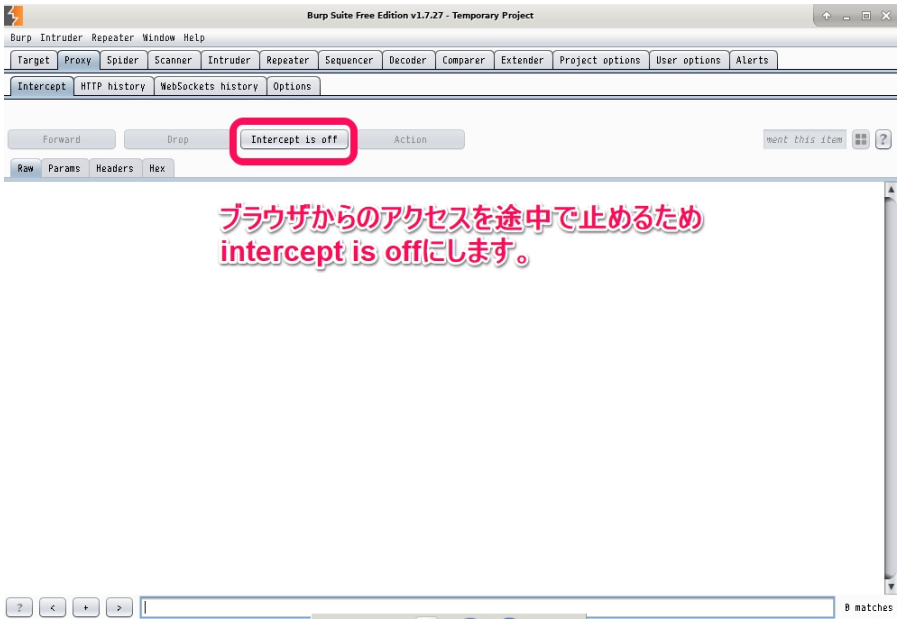


Spectrum Technology

ホワイトハッカ育成プログラム
④. burp suite(web脆弱性診断)

- burp suite運用
  - A) インターセプト中止　proxy>intercept>intercept is off オンにするとブラウザからのアクセスが停止します。
  - B) ターゲットのサイトにFirefoxからアクセスします。

A)



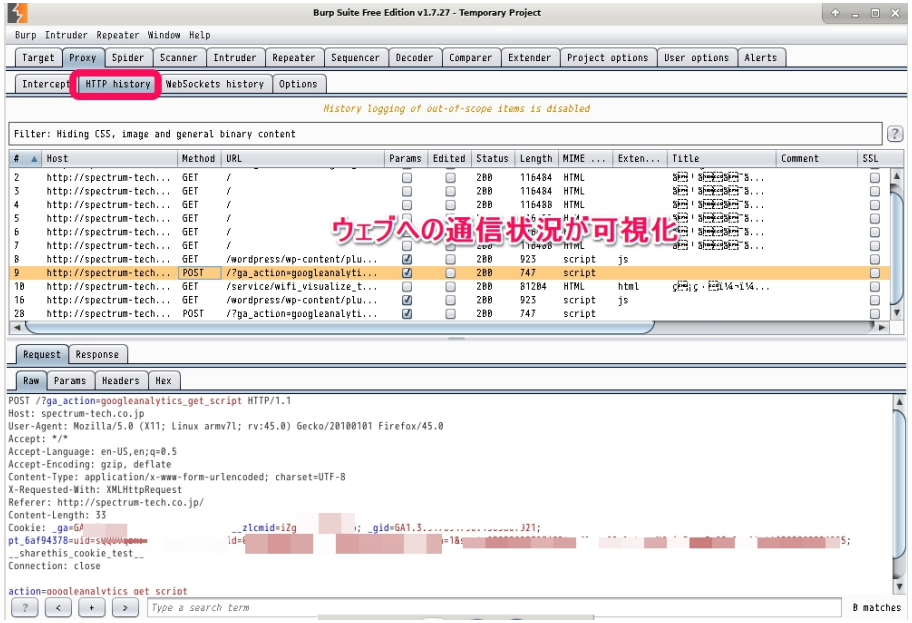
B)

Spectrum Technology

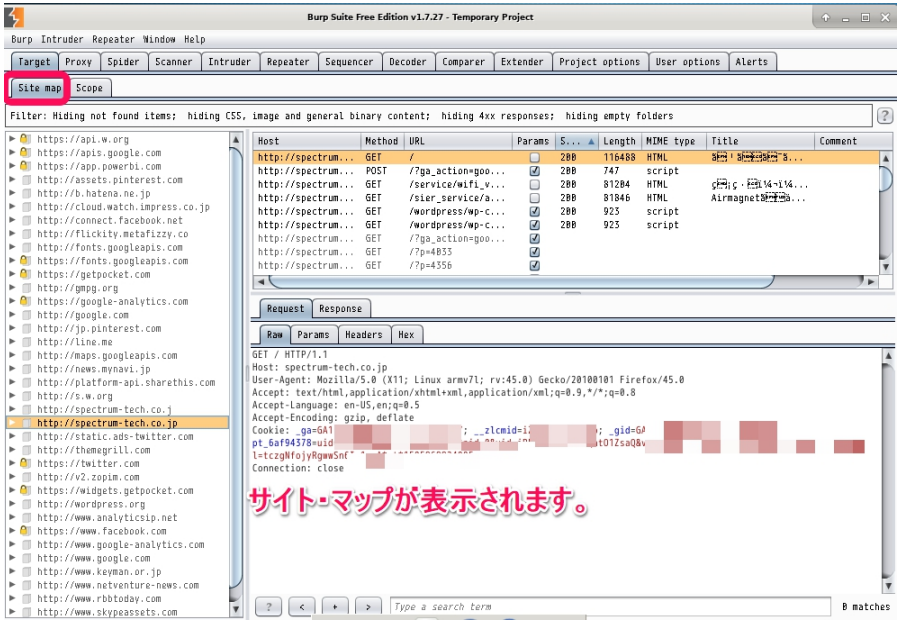
ホワイトハッカ育成プログラム
④. burp suite(web脆弱性診断)

- burp suite運用
  - C) サイトへの通信状況確認　proxy>http history
  - D) サイトマップの表示　target>site map

C)



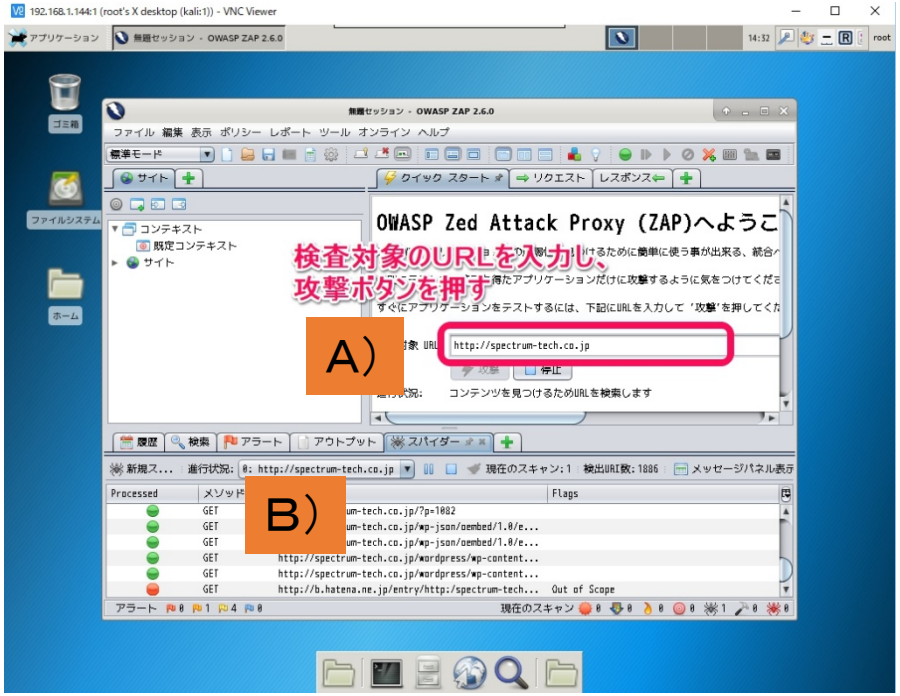
D)

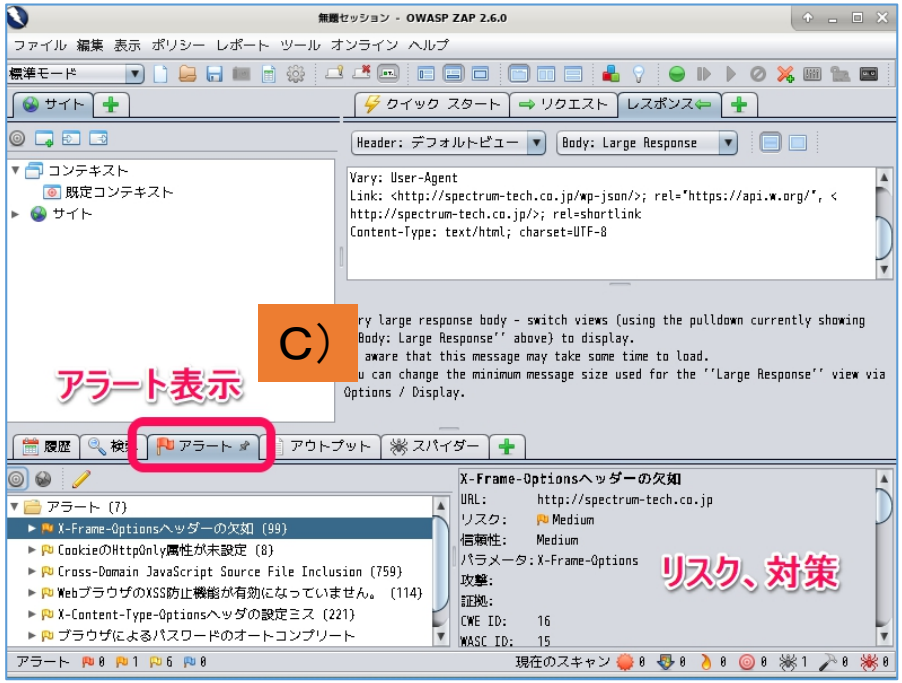


Spectrum Technology

ホワイトハッカ育成プログラム
⑤. owasp zap（web脆弱性診断）

- 診断方法
  - A) 対象サイト設定
  - B) スキャン
  - C) アラート:リスクの高、中、小別に出力され、対策が個別に出ます。



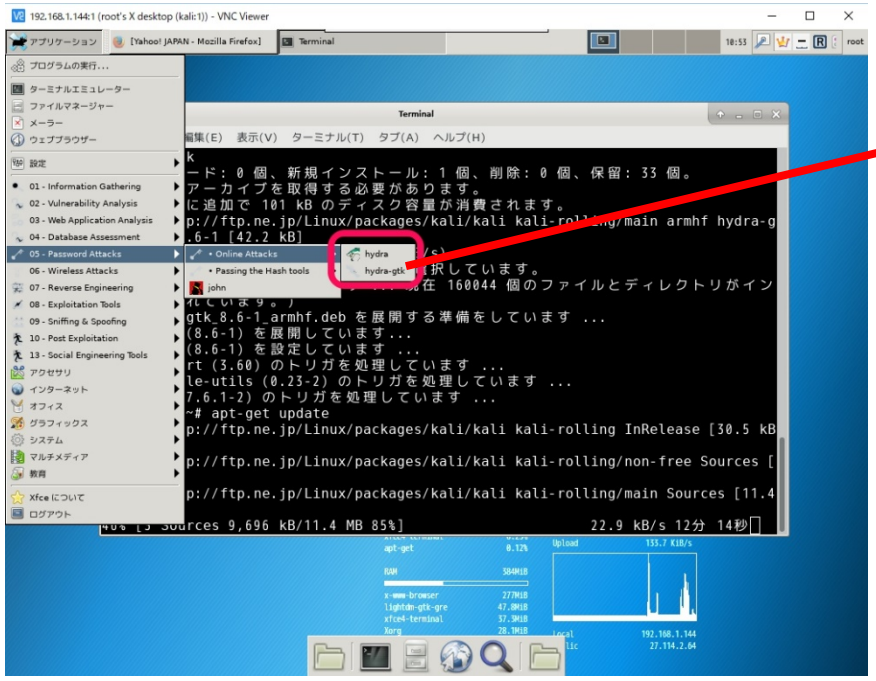


Spectrum Technology

ホワイトハッカ育成プログラム
⑦. hydra(パスワード・クラッキング)

- 運用方法
  - A) hydra立ち上げ
    - 通常は、terminalで使用します。
  - B) gtkバージョン
    - gtk版も利用できます。

A)

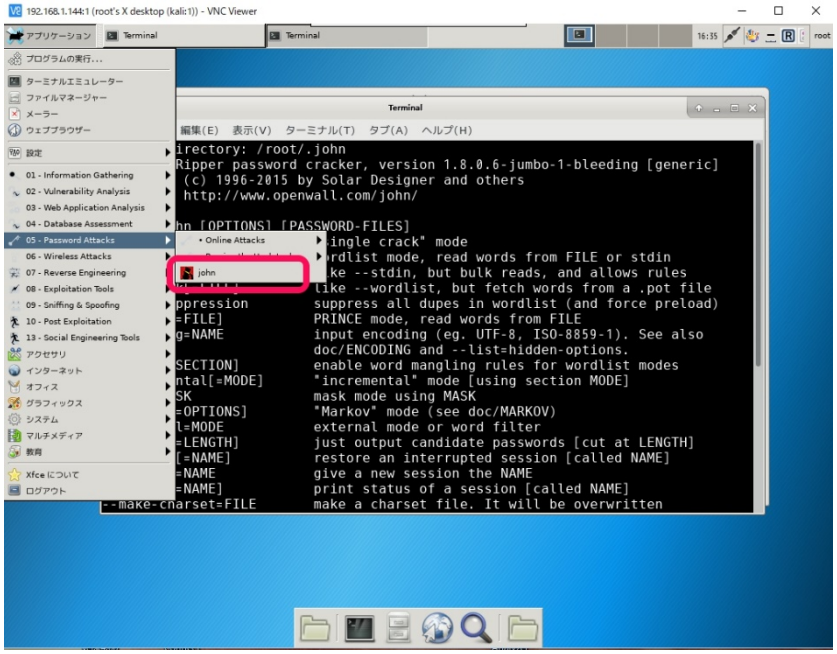


B)

ホワイトハッカ育成プログラム
⑧. john(パスワード・クラッキング)

- 運用方法
  - A) john立ち上げ
  - B) コマンド例

A)



B)

シングルモード

```
#sudo john --users=loginid --single
pass_shadow
```

辞書モード

```
#sudo john --users=loginid --
wordlist=/usr/share/dict/words ps
```

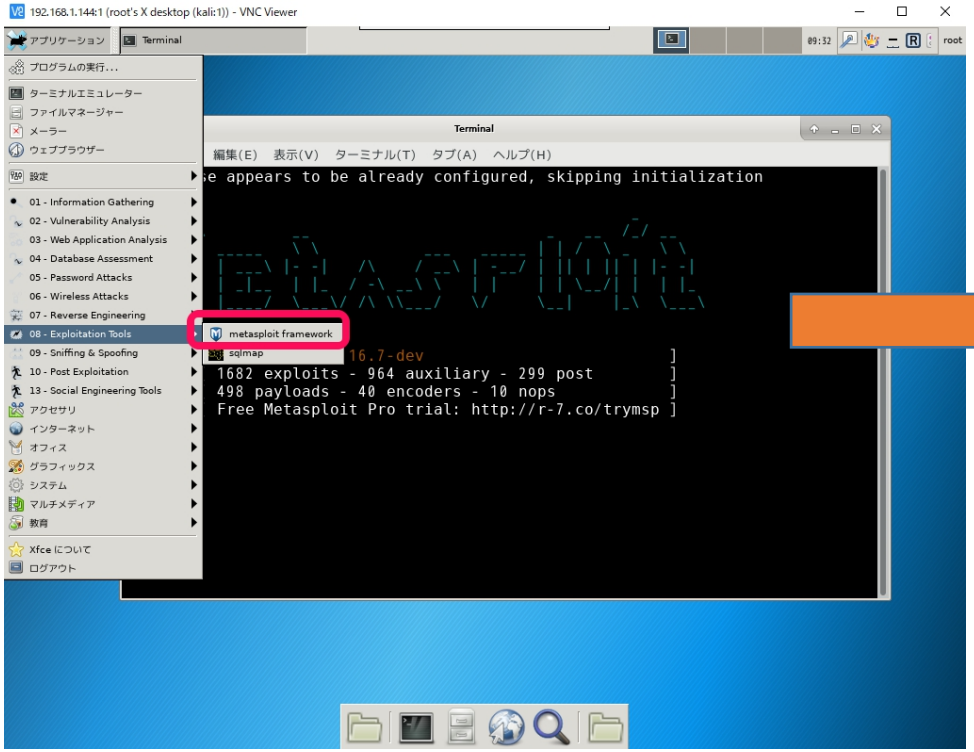
インクリメント：1文字づつ増加

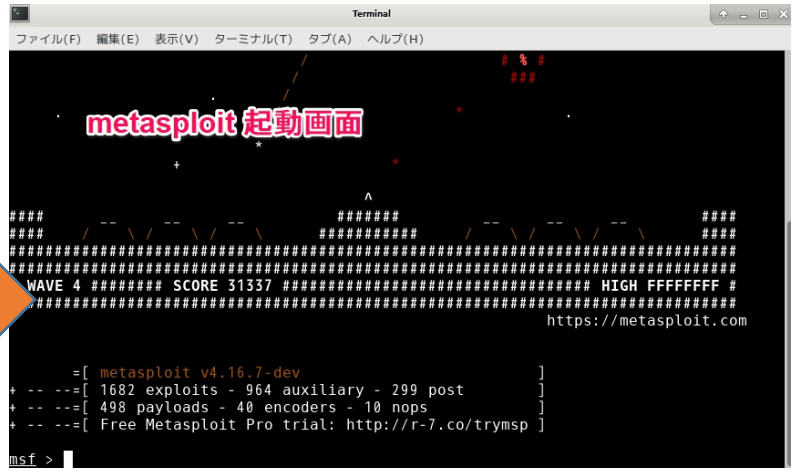
```
#sudo john --users=loginid --incremental
pass_shadow
```

Spectrum Technology

ホワイトハッカ育成プログラム
⑨. metasploit(ハッキング・ツール)

- 運用方法
  - A) metasploit立ち上げ：操作の詳細は、armitageで説明





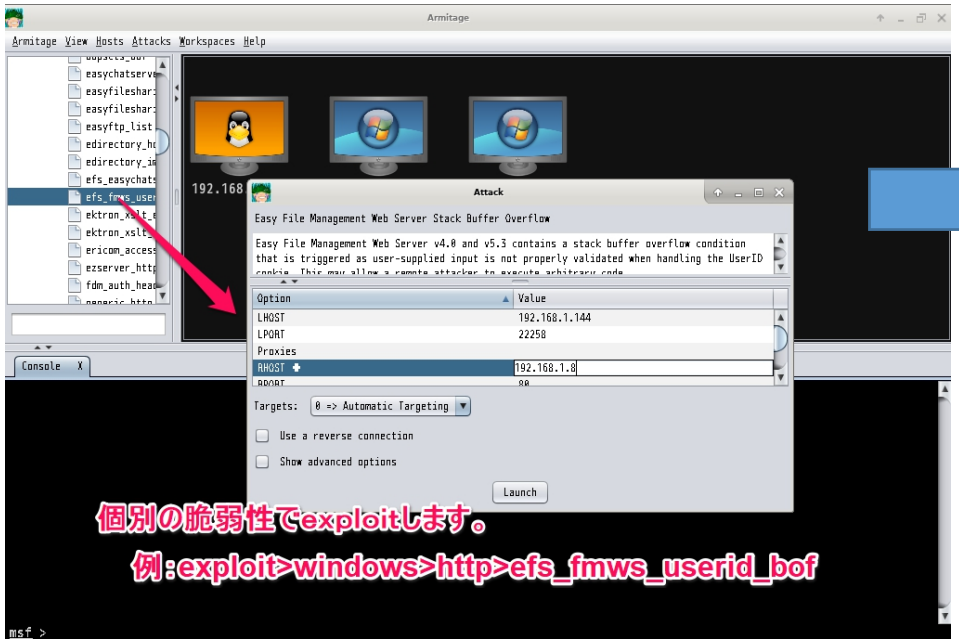
Spectrum Technology

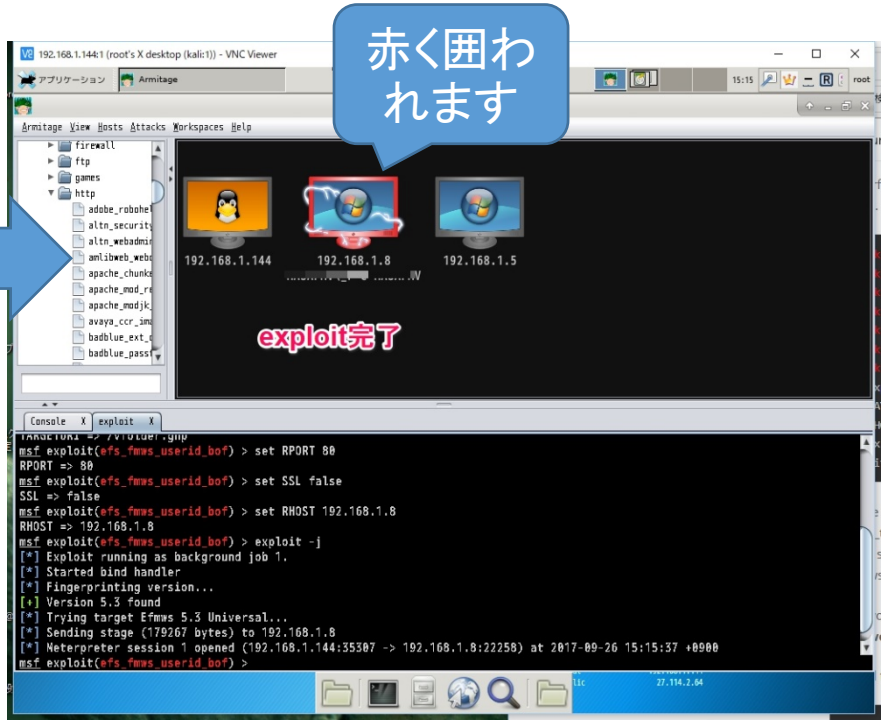
ホワイトハッカ育成プログラム
⑩. Armitage(ハッキング・ツールGUI版）

- 運用方法
  - H) 個別乗っ取り方法：exploit>
    - 相手の脆弱性が分かっている場合は、個別に乗っ取ります。
    - 例：windowにeasy file managementの脆弱性の場合
    - exploit>windows>http>efs_fmws_userid_bof:ダブルクリックでポップアップ。

H）

相手のIPアドレスを入力して、lanch



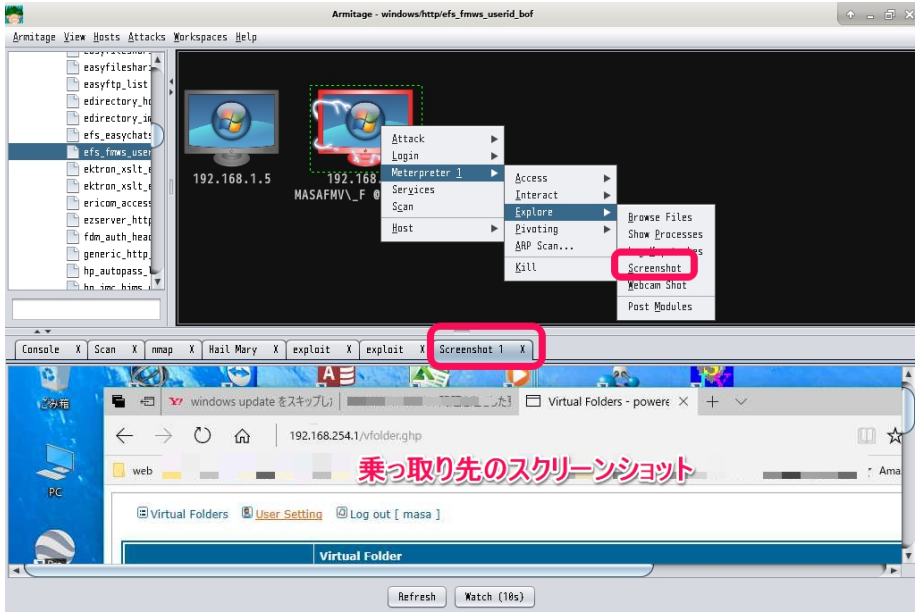


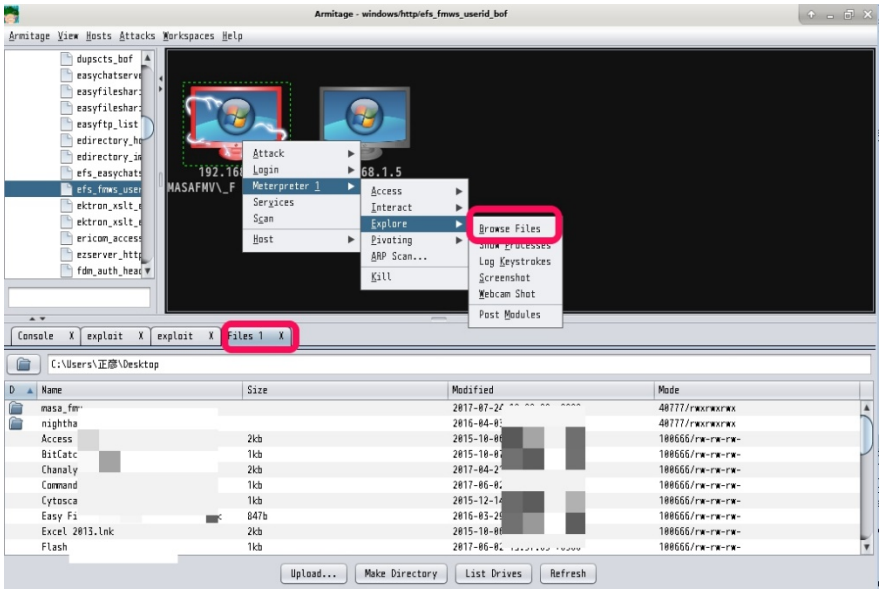
Spectrum Technology

ホワイトハッカ育成プログラム
⑩. Armitage(ハッキング・ツールGUI版)

- 運用方法
  - I) 侵入操作方法：meterpreter>
    - exploitが完了すると、相手の端末のスクリーンショット、ウェブカメラ、キーボード入力、ファイル操作が可能になります。
    - 右クリック：meterpreter 1>explore>screeshot　or browse file

I)





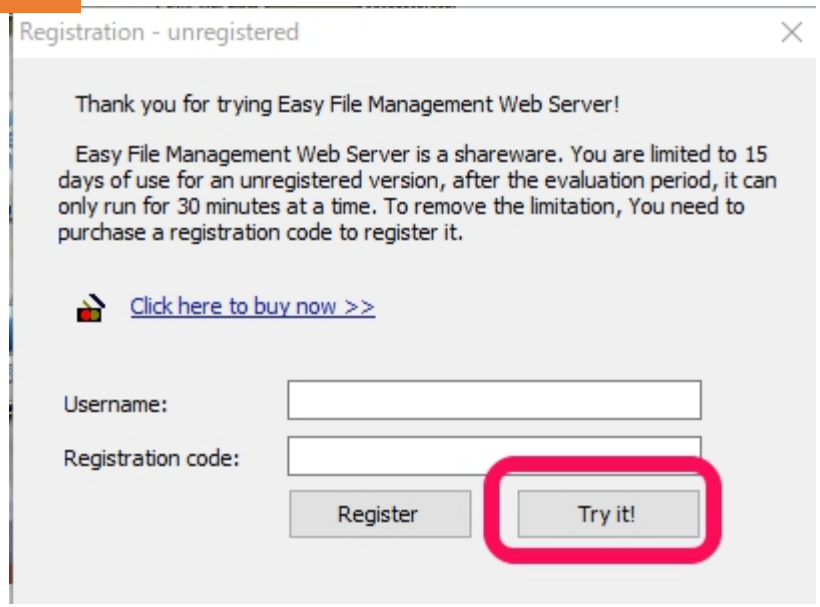
ホワイトハッカ育成プログラム
⑪. exploit DB(脆弱性試験用検体)

- 試験用検体設定
  - インストール：exeファイルをダブルクリックしてインストール
  - 設定
    - デスクトップのeasy file managementをダブルクリック

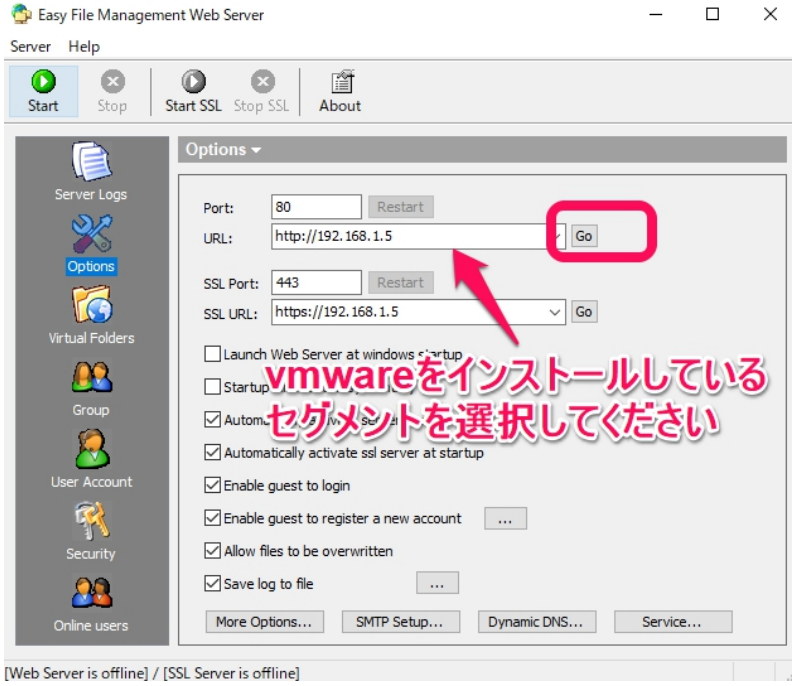
A) 試用をクリック

B) IPアドレスを選択し、Go（すでに80番ポートを使うxamppがある場合は使えません）

A）



B）



ホワイトハッカ育成プログラム
⑫. wireshark(プロトコル・アナライザ)

- 使用方法

  #tshark –i eth0 –w test2　　eth0のインターフェースのデータを取得し、test2のファイルを作成します。

  #tcpdump –r test2　　test2のデータを読み出します。見ずらいので他のPCに取り出してwiresharkで見てください