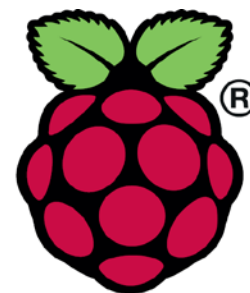


抜粋

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



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

育成ツール 目次

• Kali運用マニュアル	ページ
• RaspberryPiについて	4
• Linux基本コマンド	5
• Kali基本操作	6
• 日常運用(ウイルススキャン、更新、CPU使用率)	7
• ホワイトハッカ育成プログラム	ページ
① Kaliメニュー	10
② nmap(ポートスキャン)	12
③ maltego(情報収集)	15
• maltego設定	15
• maltego運用	19
• webサイト調査	19
• sns調査	21
• e-mail調査	23
• 電話番号調査	24
• 個人情報調査	25

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

	ページ
• ホワイトハッカ育成プログラム	
④ burp suite (web脆弱性診断: 一部有料)	26
• burp suite設定	27
• burp suite運用 (Web通信状況確認)	30
⑤ owasp-zap (web脆弱性診断: 無料)	32
⑥ sqlmap (sqlインジェクション)	34
⑦ hydra (パスワード・クラッキング)	36
⑧ john (パスワード・クラッキング)	39
⑨ metasploit (ハッキング・ツール)	41
⑩ armitage (ハッキング・ツールGUI版)	43
⑪ exploit DB (脆弱性試験用検体)	53
⑫ wireshark (プロトコル・アナライザ)	56
⑬ 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ーして操作します)

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る内容を変更します。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

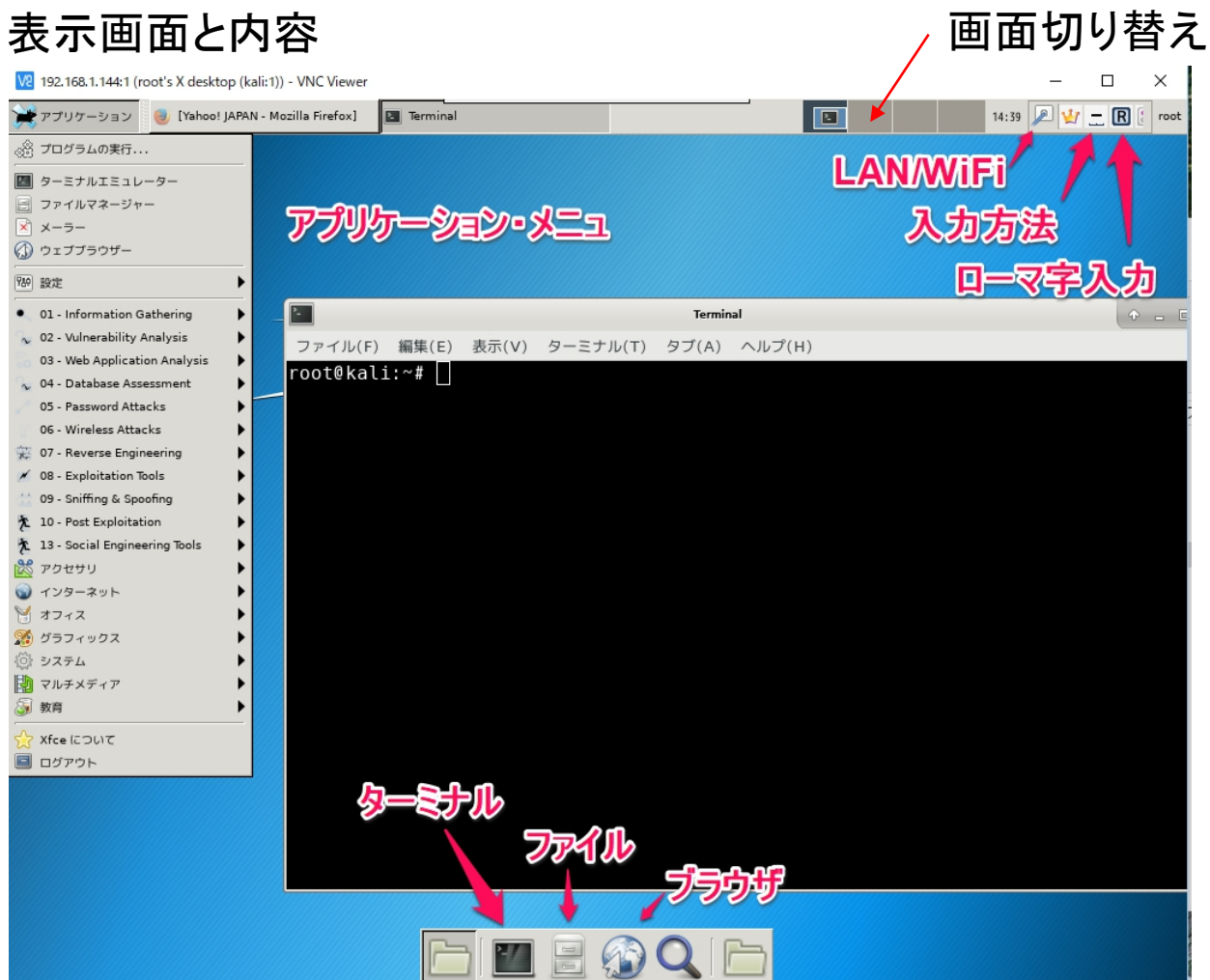
root@kali:~# **free -mt** メモリ使用状態表示

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います。

```
Terminal
root@kali:~# freshclam
ClamAV update process started at Fri Sep 15 14:45:54 2017
WARNING: Your ClamAV installation is OUTDATED!
WARNING: Local version: 0.99.3-beta1 Recommended version: 0.99.2
DON'T PANIC! Read http://www.clamav.net/documents/upgrading-clamav
main.cvd is up to date (version: 58, sigs: 4566249, f-level: 60, builder: sigmgr)
Downloading daily-23826.cdiff [100%]
Downloading daily-23827.cdiff [100%]
Downloading daily-23828.cdiff [100%]
Downloading daily-23829.cdiff [100%]
Downloading daily-23830.cdiff [100%]
Downloading daily-23831.cdiff [100%]
Downloading daily-23832.cdiff [100%]
Downloading daily-23833.cdiff [100%]
daily.cld updated (version: 23833, sigs: 1743019, f-level: 63, builder: neo)
bytecode.cvd is up to date (version: 311, sigs: 74, f-level: 63, builder: neo)
Database updated (6309342 signatures) from db.local.clamav.net (IP: 124.35.85.83)
ERROR: NotifyClamd: Can't find or parse configuration file /etc/clamav/clamd.conf
root@kali:~#
```

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

```
builder: neo)
builder: neo)
P: 124.35.85.83
```

```
root@kali:~# clamscan --infected --remove --recursive
----- SCAN SUMMARY -----
Known viruses: 6303733
Engine version: 0.99.3-beta1
Scanned directories: 147
Scanned files: 1066
Infected files: 0
Data scanned: 70.56 MB
Data read: 40.97 MB (ratio 1.72:1)
Time: 186.448 sec (3 m 6 s)
root@kali:~#
```

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。

```

root@kali:~# apt-get update
Get:1 http://ftp.ne.jp/linux/packages/kali/kali-rolling InRelease
パッケージリストを読み込んでいます... 完了
root@kali:~#

root@kali:~# apt-get upgrade
パッケージリストを読み込んでいます... 完了
依存関係ツリーを作成しています
状態情報を読み取っています... 完了
アップグレードパッケージを検出しています... 完了
以下のパッケージは保留されます:
firefox-esr firefox-esr-l10n-ja gnupg gnupg-agent gstreamer1.0-libav gvfs
gvfs-daemons gvfs-libs libavcodec57 libavfilter6 libavformat57 libblas3
libdrm-amdgpu1 libdrm2 libgnutls30 libidn2-0 libpoppler-glib8 libpsl5
libreoffice-base-core libreoffice-common libreoffice-core
libreoffice-help-ja libreoffice-l10n-ja libreoffice-math
libreoffice-style-galaxy libreoffice-writer libwscodec1 mount python3-uno
uno-libs3 ure usb-modeswitch util-linux wireshark-common wireshark-qt
アップグレード: 0 個、新規インストール: 0 個、削除: 0 個、保留: 35 個。
root@kali:~#
    
```

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

ホワイトハッカ育成プログラム

①. Kaliメニュー

• Kaliとは

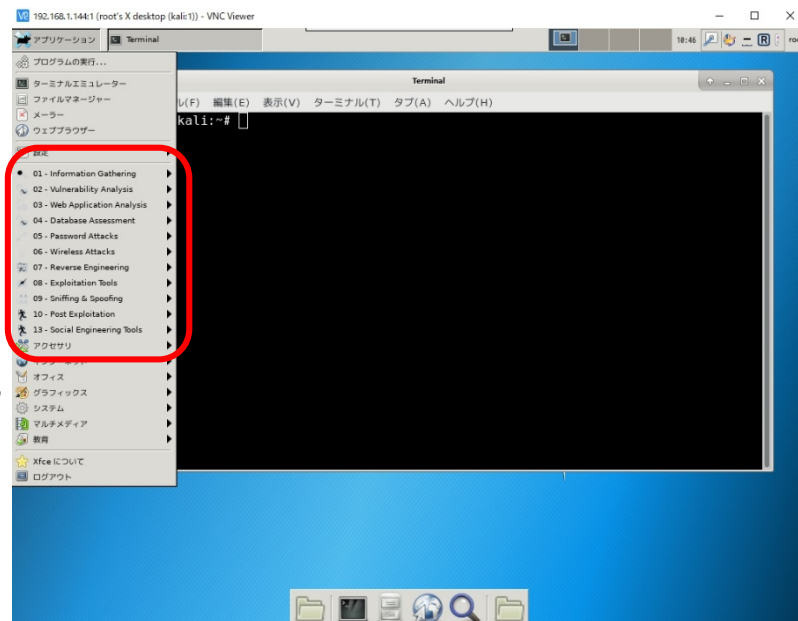
- Kali Linuxは、世界レベルの情報セキュリティトレーニングと侵入テストサービスを提供するOffensive Securityによって維持管理されているオープンソースプロジェクトです。Kali Linuxに加えて、Offensive SecurityはExploit Databaseと無料のオンラインコースMetasploit Unleashedも管理しています。

- <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, maltego, 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。

ホワイトハッカ育成プログラム

②. nmap(ポートスキャン)

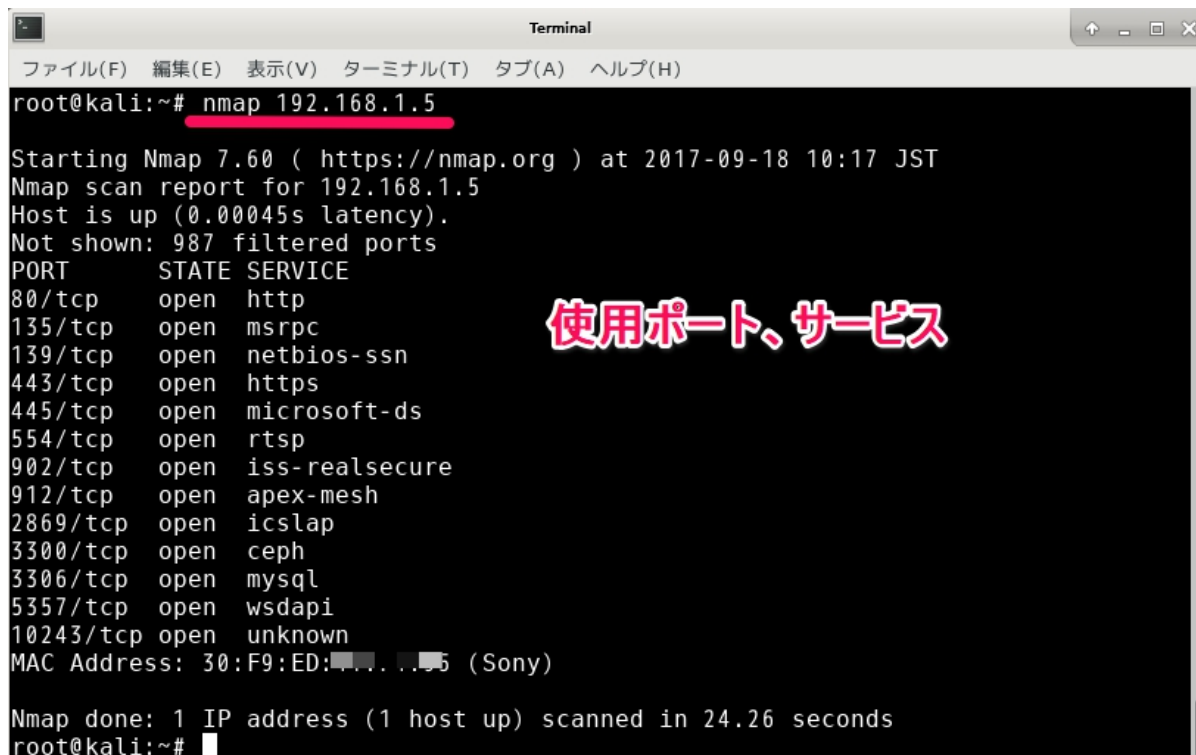
ポート・スキャン
nmap IPアドレス

- 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



```
Terminal
ファイル(F) 編集(E) 表示(V) ターミナル(T) タブ(A) ヘルプ(H)
root@kali:~# nmap 192.168.1.5
Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-18 10:17 JST
Nmap scan report for 192.168.1.5
Host is up (0.00045s latency).
Not shown: 987 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
443/tcp    open  https
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
902/tcp    open  iss-realsecure
912/tcp    open  apex-mesh
2869/tcp   open  icslap
3300/tcp   open  ceph
3306/tcp   open  mysql
5357/tcp   open  wsdapi
10243/tcp  open  unknown
MAC Address: 30:F9:ED: (Sony)

Nmap done: 1 IP address (1 host up) scanned in 24.26 seconds
root@kali:~#
```

使用ポート、サービス

ホワイトハッカ育成プログラム

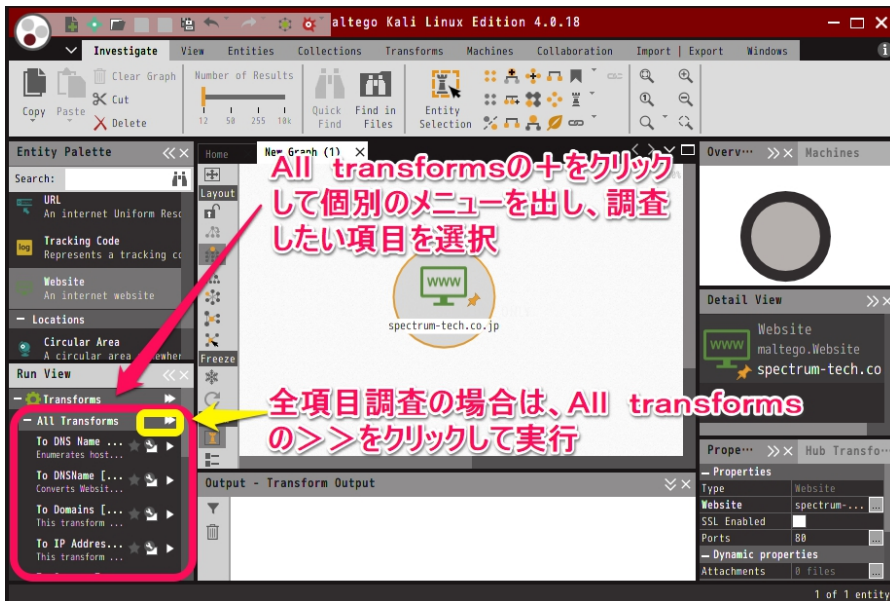
③. maltego ce(情報収集)

- maltego運用

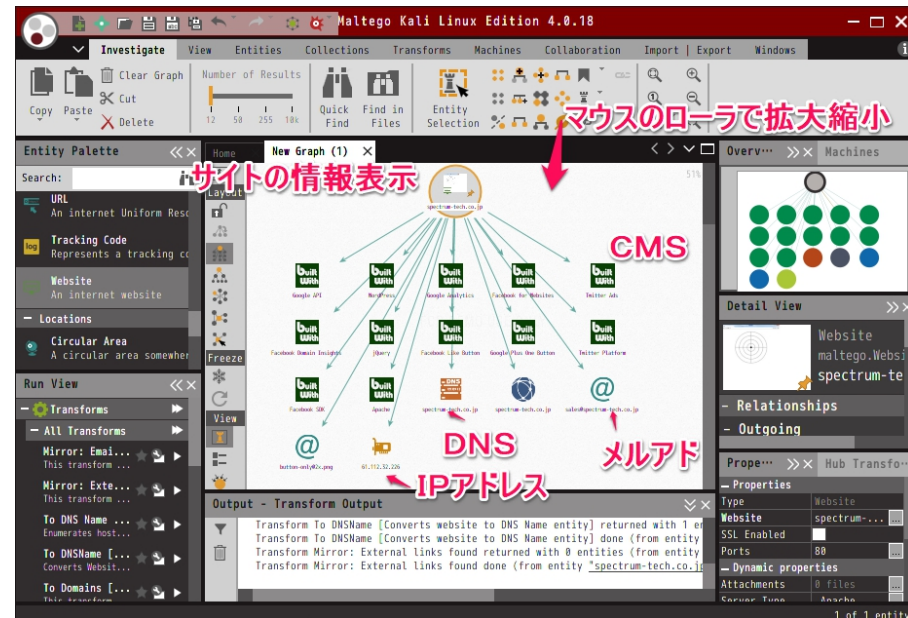
- webサイト調査

- 左のRun viewからtransforms>all transformsを選び、>>マークをクリックします。
- 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)



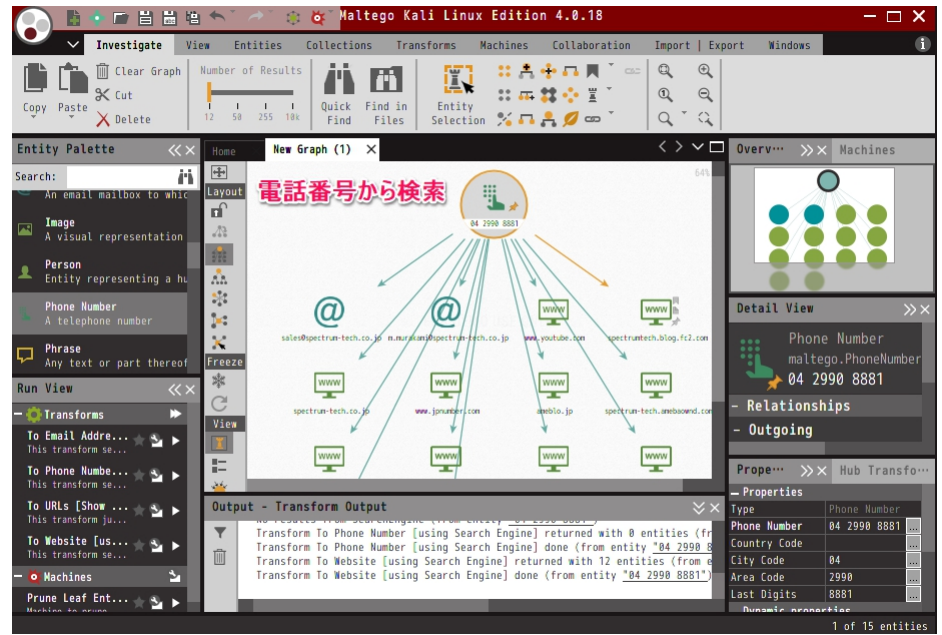
ホワイトハッカ育成プログラム

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)



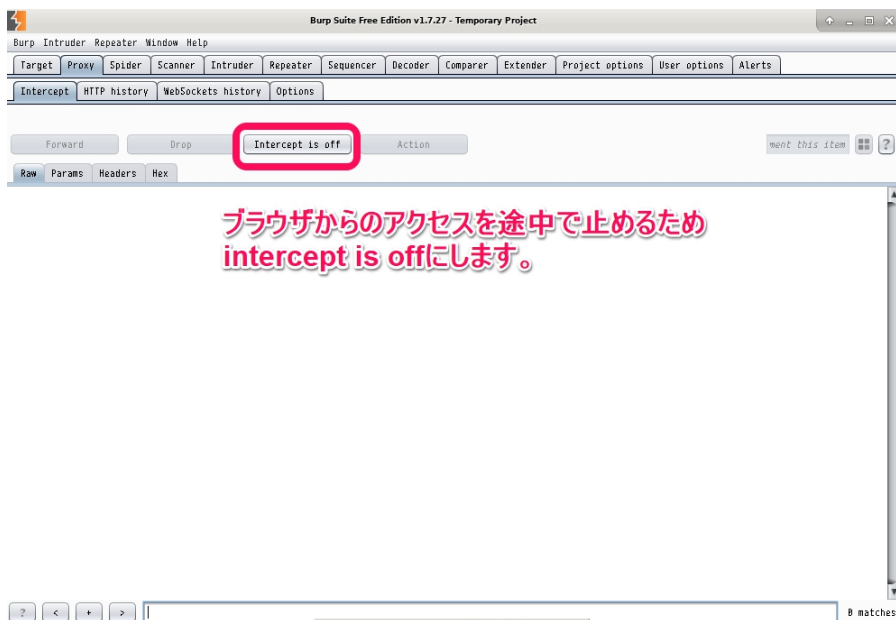
ホワイトハッカ育成プログラム

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)



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)

The screenshot shows the Burp Suite interface with the 'HTTP history' tab selected. A table lists various HTTP requests to 'spectrum-tech.co.jp'. A red box highlights the 'HTTP history' tab. A red text overlay reads 'ウェブへの通信状況が可視化' (Visualization of communication status to the web). Below the table, a detailed view of a selected POST request is shown, including headers like 'User-Agent: Mozilla/5.0 (X11; Linux armv7l; rv:45.0) Gecko/20100101 Firefox/45.0' and cookies.

D)

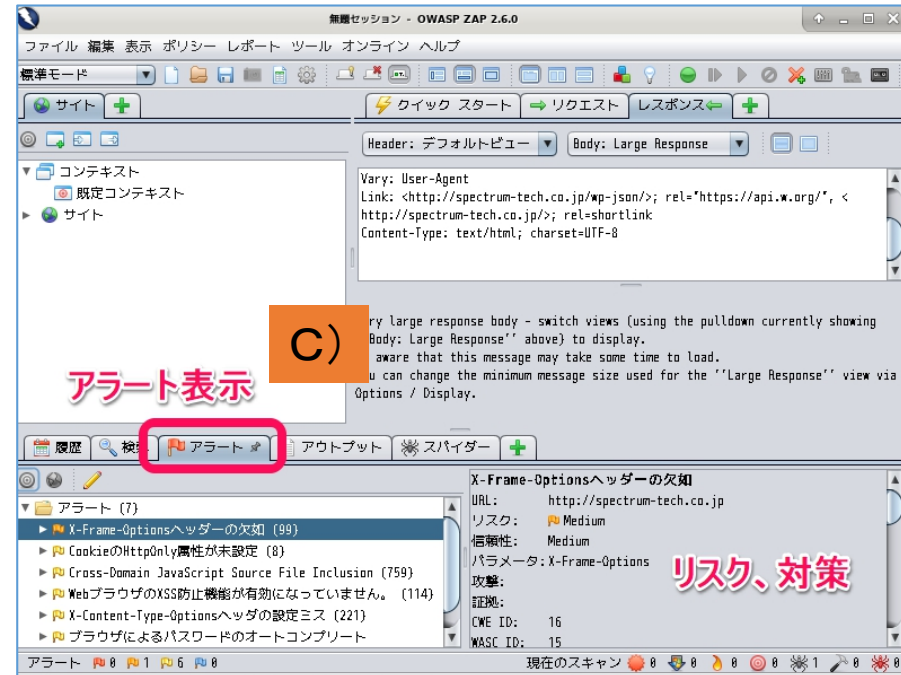
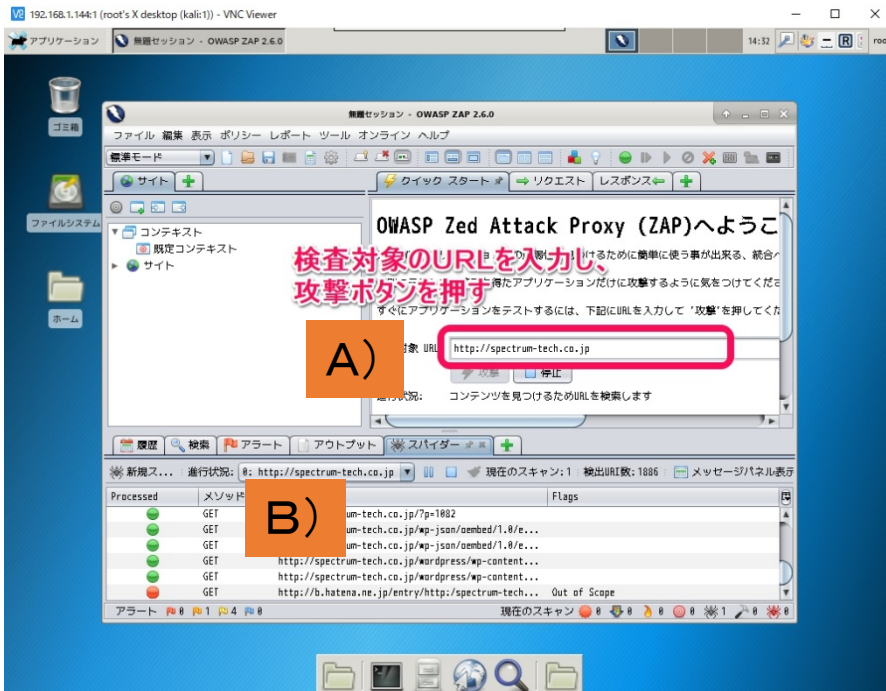
The screenshot shows the Burp Suite interface with the 'Site map' tab selected. A tree view displays the discovered website structure, including folders for 'https://api.w.org', 'https://apis.google.com', and 'https://app.powerbi.com'. A red box highlights the 'Site map' tab. A red text overlay reads 'サイトマップが表示されます。' (The site map is displayed). The bottom part of the window shows the 'Request' and 'Response' details for a selected item.

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。



ホワイトハッカー育成プログラム

⑦. hydra(パスワード・クラッキング)

● 運用方法

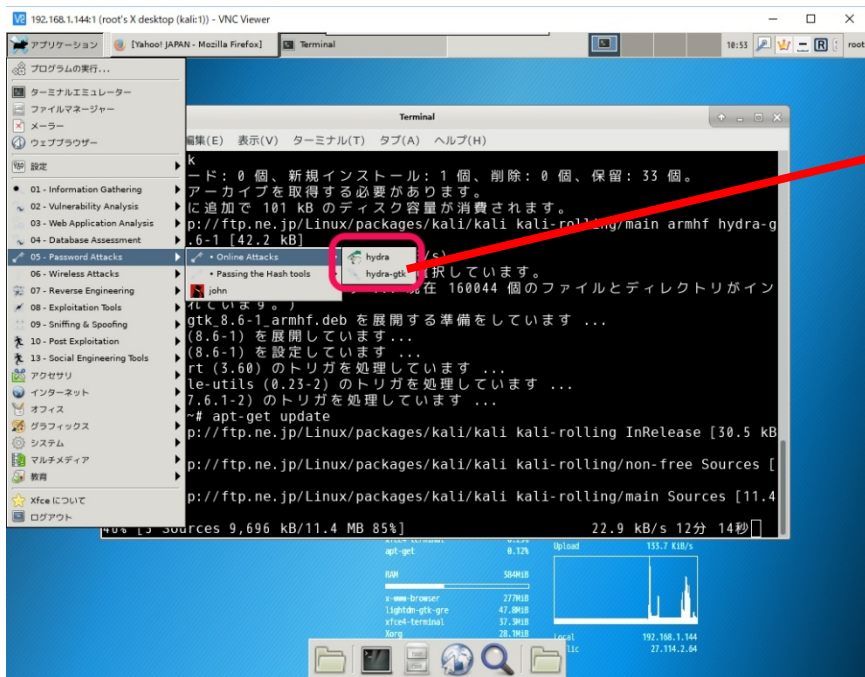
A) hydra立ち上げ

- 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)



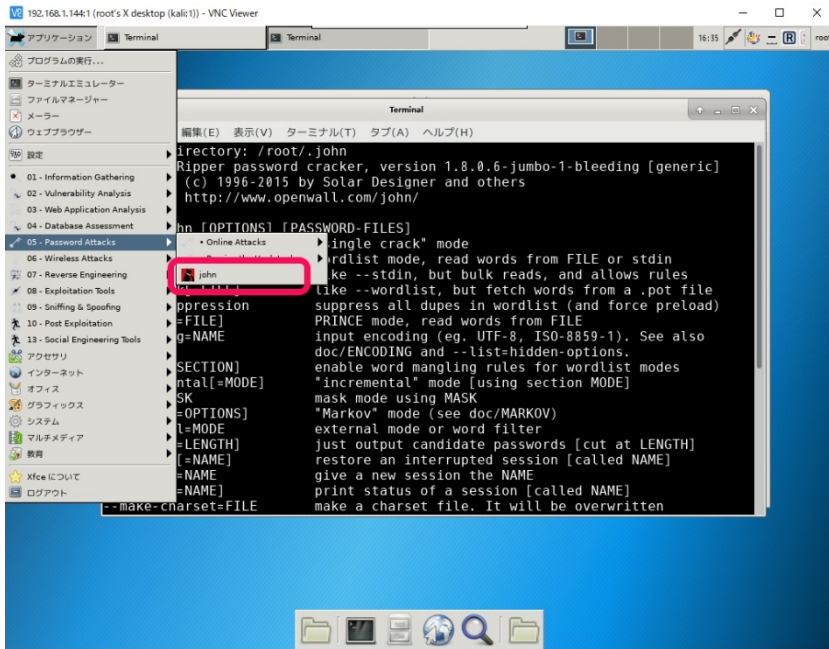
ホワイトハッカ育成プログラム

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文字ずつ増加

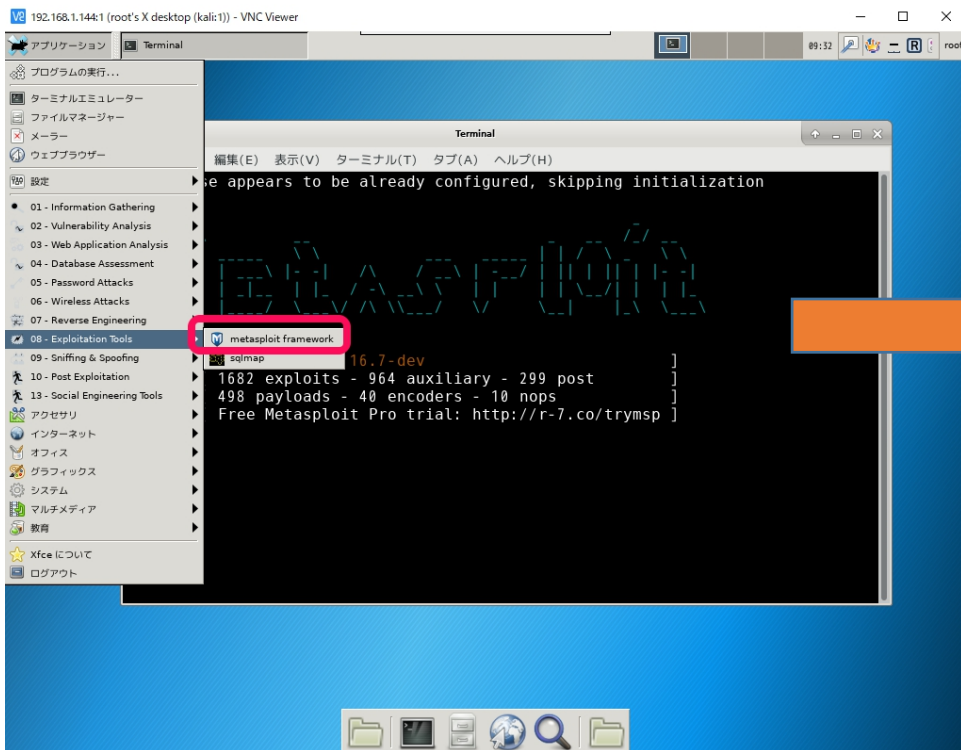
```
#sudo john --users=loginid --incremental
pass_shadow
```

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



ホワイトハッカ育成プログラム

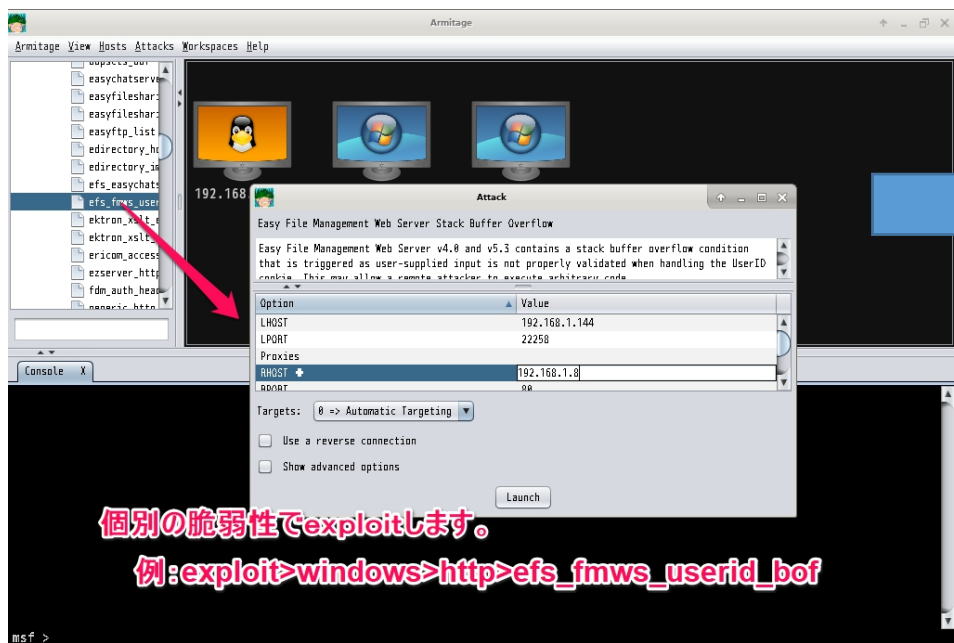
⑩. Armitage(ハッキング・ツールGUI版)

● 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。
相手のIPアドレスを入力して、launch

H)



ホワイトハッカー育成プログラム

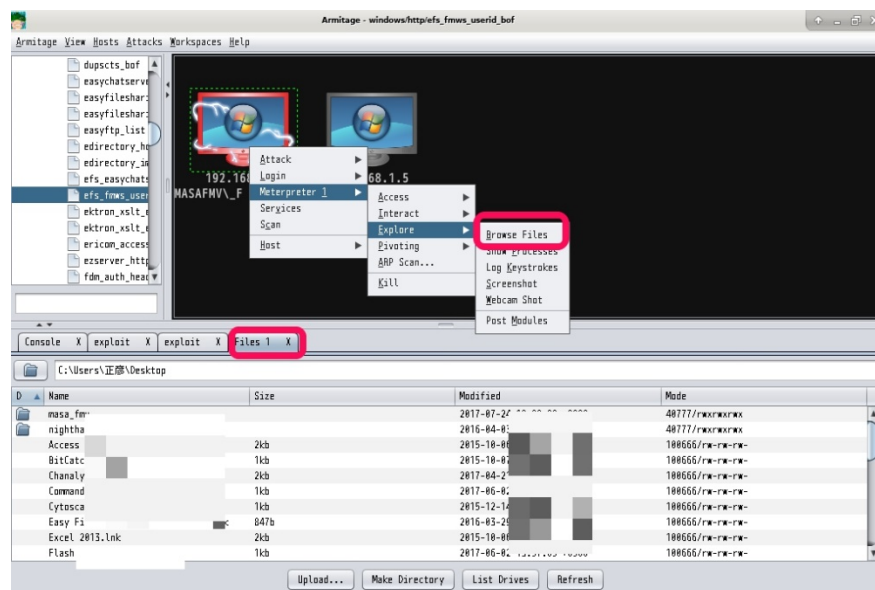
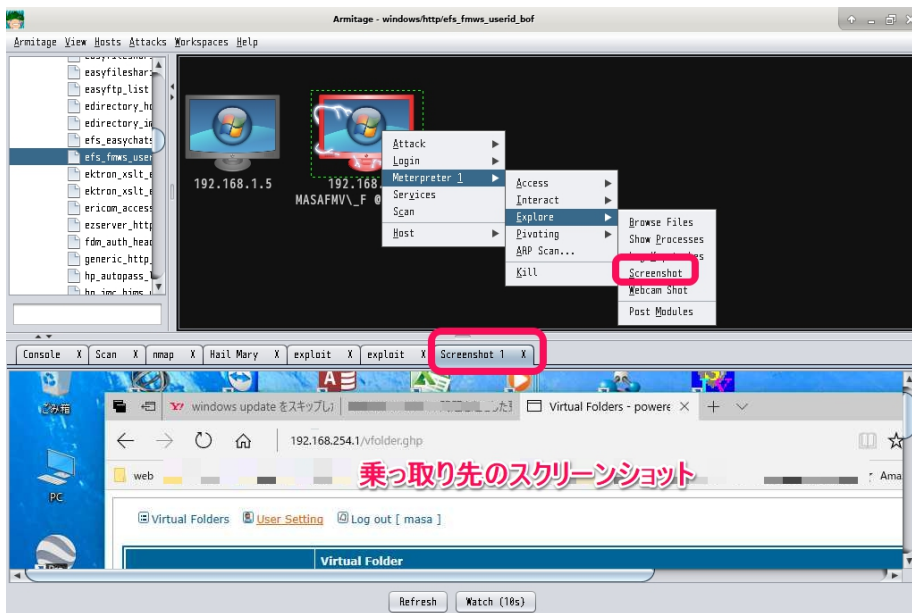
⑩. Armitage(ハッキング・ツールGUI版)

● 運用方法

1) 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>screenshot 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)

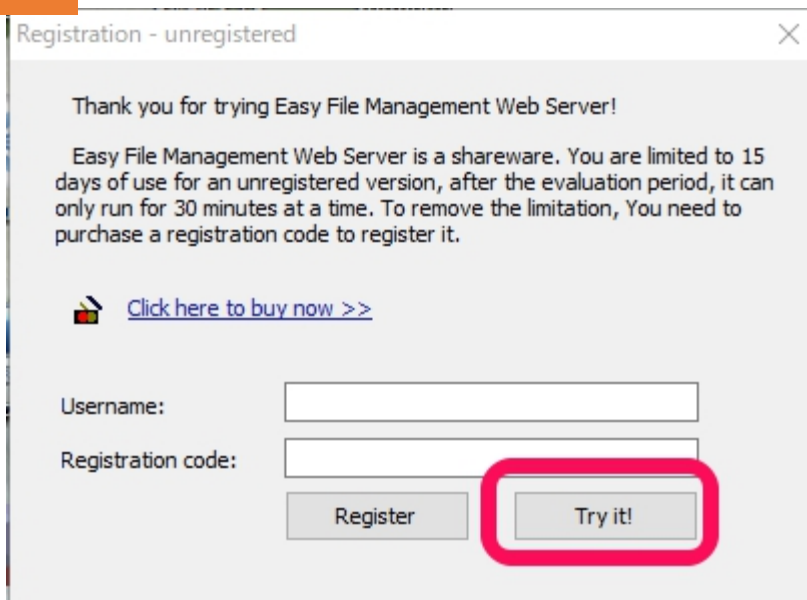
• 試験用検体設定

- 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

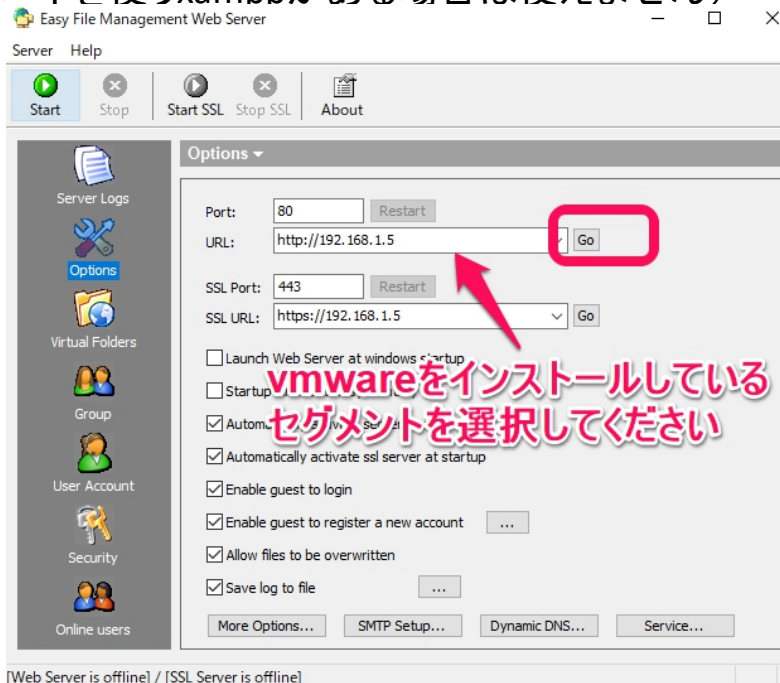
A) 試用をクリック

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

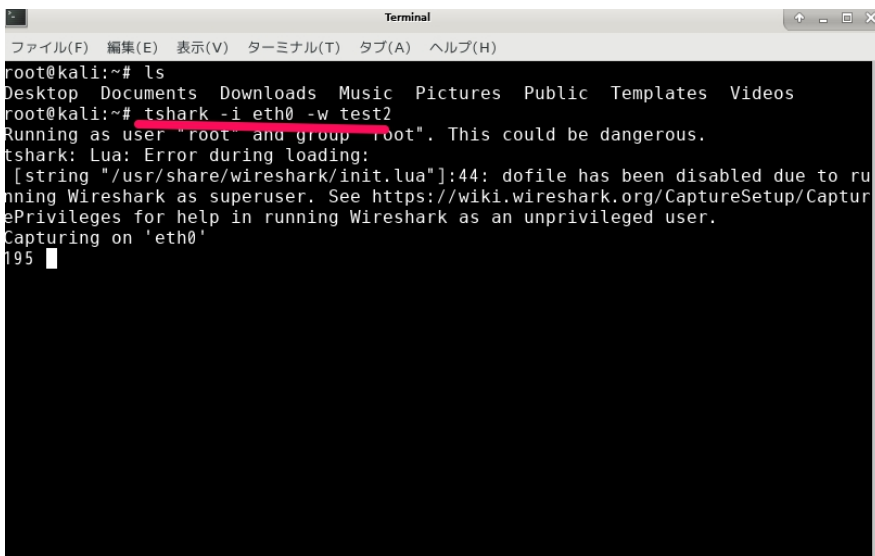
#tshark -i eth0 -w test2
ファイルを作成します。

eth0のインターフェースのデータを取得し、test2の

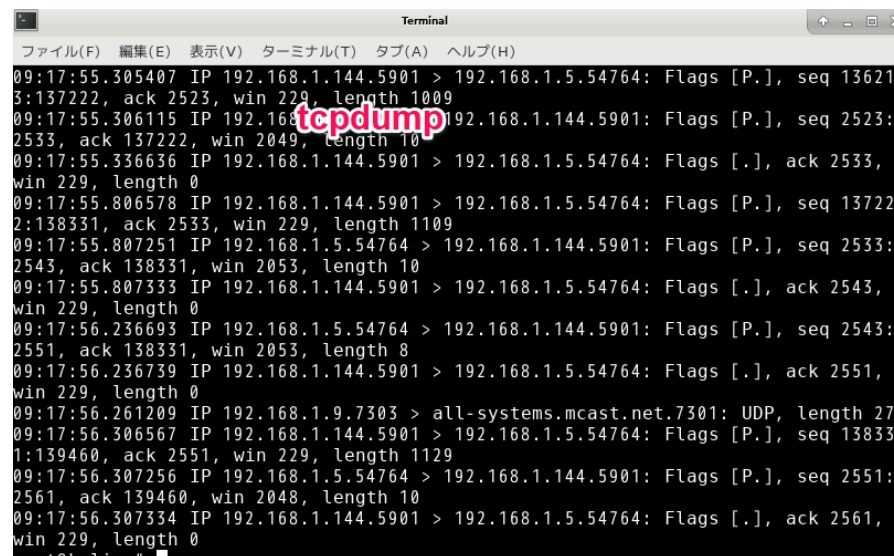
#tcpdump -r test2

test2のデータを読み出します。見づらいので他の

PCに取り出してwiresharkで見てください



```
root@kali:~# ls
Desktop Documents Downloads Music Pictures Public Templates Videos
root@kali:~# tshark -i eth0 -w test2
Running as user "root" and group "root". This could be dangerous.
tshark: Lua: Error during loading:
[string "/usr/share/wireshark/init.lua"]:44: dofile has been disabled due to ru
nning Wireshark as superuser. See https://wiki.wireshark.org/CaptureSetup/Captur
ePrivileges for help in running Wireshark as an unprivileged user.
Capturing on 'eth0'
195
```



```
09:17:55.305407 IP 192.168.1.144.5901 > 192.168.1.5.54764: Flags [P.], seq 13621
3:137222, ack 2523, win 229, length 1009
09:17:55.306115 IP 192.168.1.144.5901: Flags [P.], seq 2523:
2533, ack 137222, win 2049, length 10
09:17:55.336636 IP 192.168.1.144.5901 > 192.168.1.5.54764: Flags [.], ack 2533,
win 229, length 0
09:17:55.806578 IP 192.168.1.144.5901 > 192.168.1.5.54764: Flags [P.], seq 13722
2:138331, ack 2533, win 229, length 1109
09:17:55.807251 IP 192.168.1.5.54764 > 192.168.1.144.5901: Flags [P.], seq 2533:
2543, ack 138331, win 2053, length 10
09:17:55.807333 IP 192.168.1.144.5901 > 192.168.1.5.54764: Flags [.], ack 2543,
win 229, length 0
09:17:56.236693 IP 192.168.1.5.54764 > 192.168.1.144.5901: Flags [P.], seq 2543:
2551, ack 138331, win 2053, length 8
09:17:56.236739 IP 192.168.1.144.5901 > 192.168.1.5.54764: Flags [.], ack 2551,
win 229, length 0
09:17:56.261209 IP 192.168.1.9.7303 > all-systems.mcast.net.7301: UDP, length 27
09:17:56.306567 IP 192.168.1.144.5901 > 192.168.1.5.54764: Flags [P.], seq 13833
1:139460, ack 2551, win 229, length 1129
09:17:56.307256 IP 192.168.1.5.54764 > 192.168.1.144.5901: Flags [P.], seq 2551:
2561, ack 139460, win 2048, length 10
09:17:56.307334 IP 192.168.1.144.5901 > 192.168.1.5.54764: Flags [.], ack 2561,
win 229, length 0
root@kali:~#
```