PAKURI

Penetration test Achieve Knowledge Unite Rapid Interface

PAKURI

- Operation with Ten-key -

@Mr.Rabbit

SECCON

SECCON 2019 Akihabara
2019/12/21 - 22
YOROZU

Who am i

名前：Mr.Rabbit

資格：アーク溶接、小型移動式クレーン、玉掛け、大型自動車、OSWP、CISSP、SSCP

既往症：厨二病

趣味：サバゲー、アニメ

職歴：元サイバーディフェンス研究所研修生

What is PAKURI ?

Penetration test

Achieve

Knowledge

Unite

Rapid

Interface

What is PAKURI ?

- ペネトレーションテストに必要そうなツールを寄せ集めて、誰でも、簡単に、それっぽく実行出来る様に構成したツール

- ざっくり言うとパクってるw（権利は侵害してません）

ぱくる（異綴：パクる）

1. パクパクと食べる。大きな口を開けて食べる。
2. （俗語）隙をついて金品をかっさらう。金銭や料金を横領する。
3. （俗語）盗用する。
4. （俗語）警察などが人を捕まえ、捕縛する。

https://ja.wiktionary.org/wiki/ぱくる/

PAKURIの能力

1. 情報収集及び列挙
2. 脆弱性の分析
3. 認証試行
4. Exploit（補助）
5. 情報の可視化

PAKURI

Penetration test Achieve Knowledge Unite Rapid Interface

一般的なペネトレーションテストの流れ

No	テスト項目	説明
1	ホスト検出	ICMP応答確認を使用して、対象となるシステム上のホストを検出する
2	TCP/UDPスキャン	疑似攻撃の対象となるホストが存在しホスト上で疑似攻撃対象になるサービスが稼働していることを確認する
3	脆弱性の確認	脆弱性スキャナを利用し網羅的に脆弱性の存在を確認する
4	認証試行・アクセス権取得	推測可能なアカウント・パスワードを用いて認証試行を行い、サービスやアプリケーションの利用可否を確認する
5	既知脆弱性を利用した疑似攻撃	既知脆弱性を利用し、攻撃コードを使用して疑似攻撃を行い、実際に侵入及び情報の窃取が可能か確認する
6	影響度の確認	疑似攻撃が成功したホストの権限やファイル等を分析し他のホストへの影響度を確認する

PAKURIでやりたいこと

No	テスト項目
1	ホスト検出
2	TCP/UDPスキャン
3	脆弱性の確認
4	認証試行・アクセス権取得
5	既知脆弱性を利用した疑似攻撃
6	影響度の確認

PAKURI
Penetration test Achieve Knowledge Unite Rapid Interface

1. 情報収集及び列挙
2. 脆弱性の分析
3. 認証試行
4. Exploit（補助）
5. 情報の可視化

この範囲をサポートしたい

操作が難しいのでは？

テンキーだけで動くよ

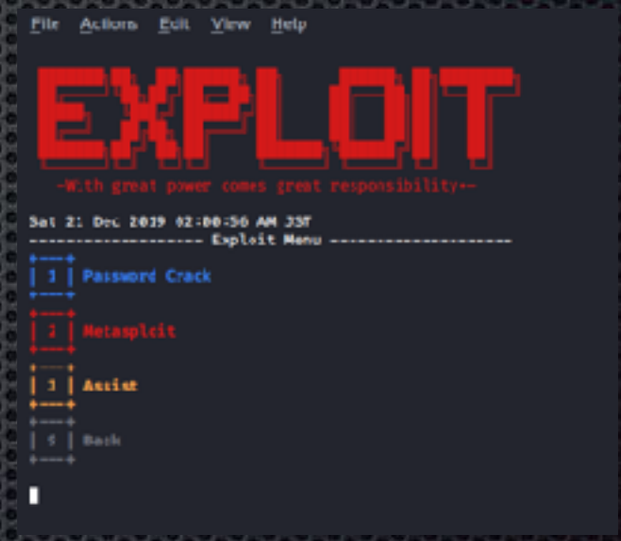
画面


File Actions Edit View Help
PAKURI
- Penetration Test Achive Knowledge Unite Rapid Interface -
inspired by CDI
v1.0.1
Author : Mr.Rabbit
Sat 21 Dec 2019 02:00:14 AM JST
Working Directory : /root/demo
Main Menu
1 Scanning
2 Exploit
3 Config
4 Assist
9 Back

1


File Actions Edit View Help
SCANNING
Scan Menu
1 Discovery Host
2 Well-known ports Scan
3 Vulnerability Scan
4 AutoReconn
5 Assist
9 Back

2


File Actions Edit View Help
EXPLOIT
-With great power comes great responsibility-
Sat 21 Dec 2019 02:00:56 AM JST
Exploit Menu
1 Password Crack
1 Metasploit
3 Assist
9 Back

3


File Actions Edit View Help
CONFIG
Sat 21 Dec 2019 02:01:10 AM JST
Config Menu
1 PostgreSQL [Running]
2 Import data into Faraday
3 Mode Switching
4 Configure Targets
9 Back

基本コマンド

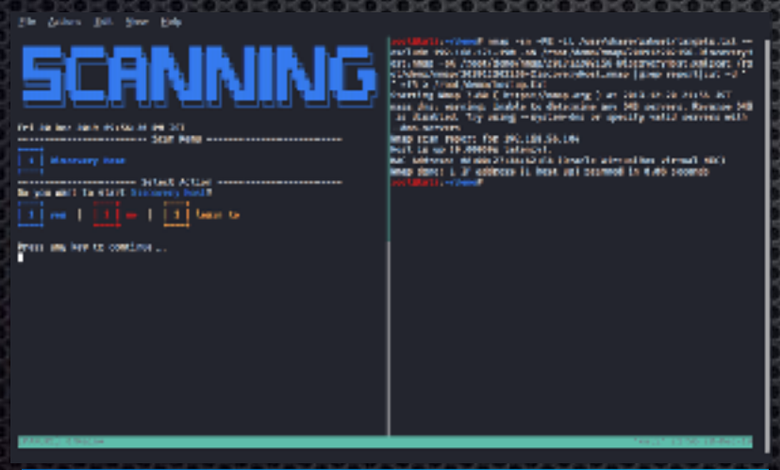
1. スキャンコマンド
2. エクスプロイトコマンド
3. コンフィグコマンド

コンボを決めて
コマンド実行！！

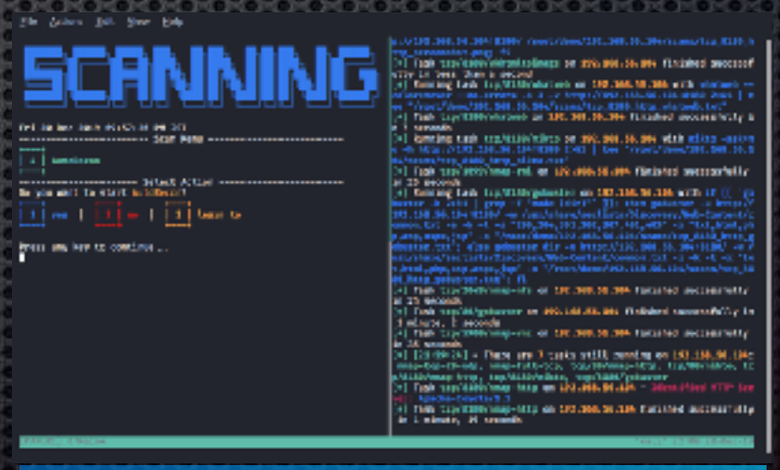
スキャンコンボ

なにをするにもまずはコレ

オススメコンボ



Discovery Host



AutoRecon

エクスプロイトコンボ

情けは無用、叩き込め！

オススメコンボ

2 — 1 — 2 Password Crack

2 — 1 — 1 Create MSF DB

3 Start Metasploit

2 Import to MSF DB

4 Check the service

Password Crack

コンフィグコンボ

成功のカギは、準備八割

オススメコンボ

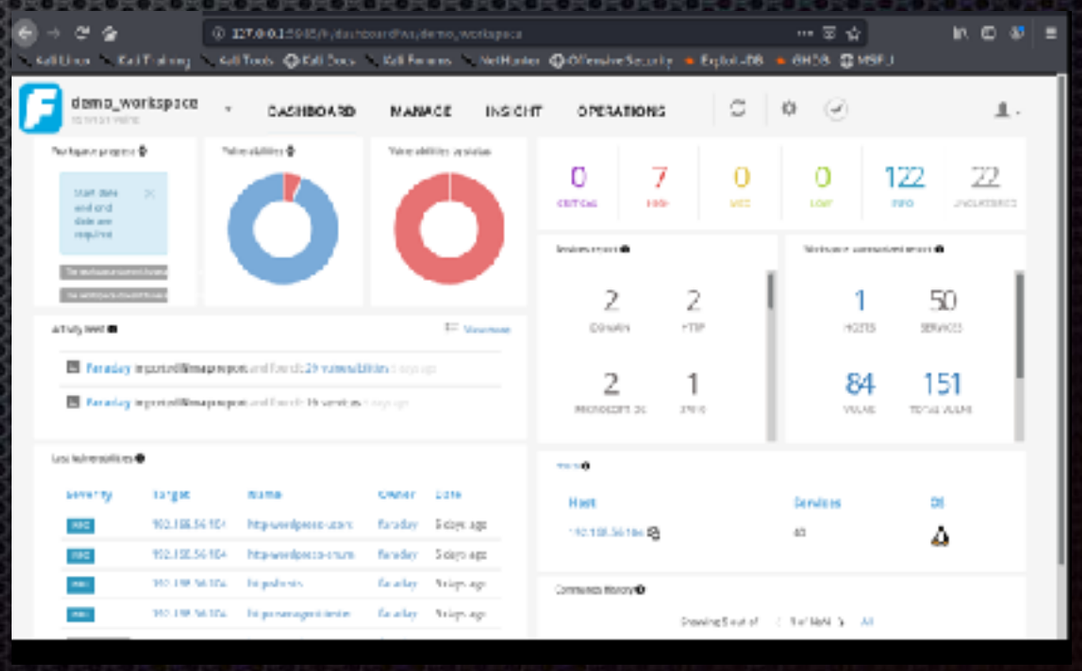
3 — 2 — 1 Import data into Faraday

3 — 1 Switch CUI mode

2 Switch GUI mode

4 Configure targets

Import data into Faraday

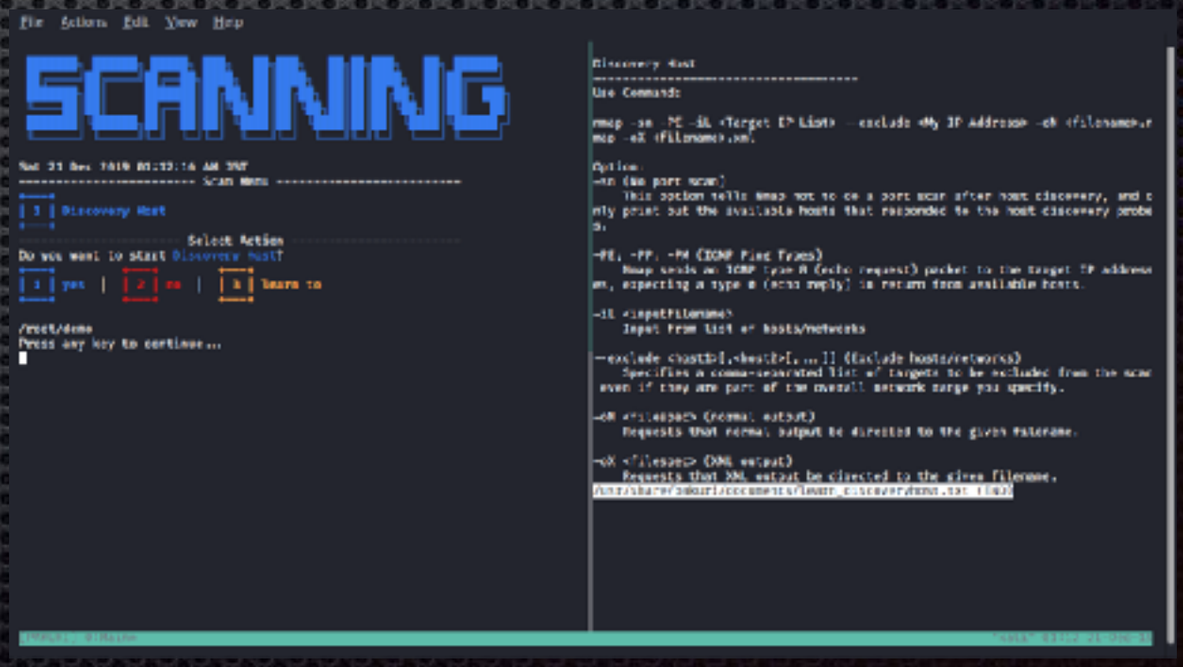


ラーニング

分からない事を知る事が一番の学び

Assist

Assistを選ぶと、各基本コマンドでの動作についての解説を表示する



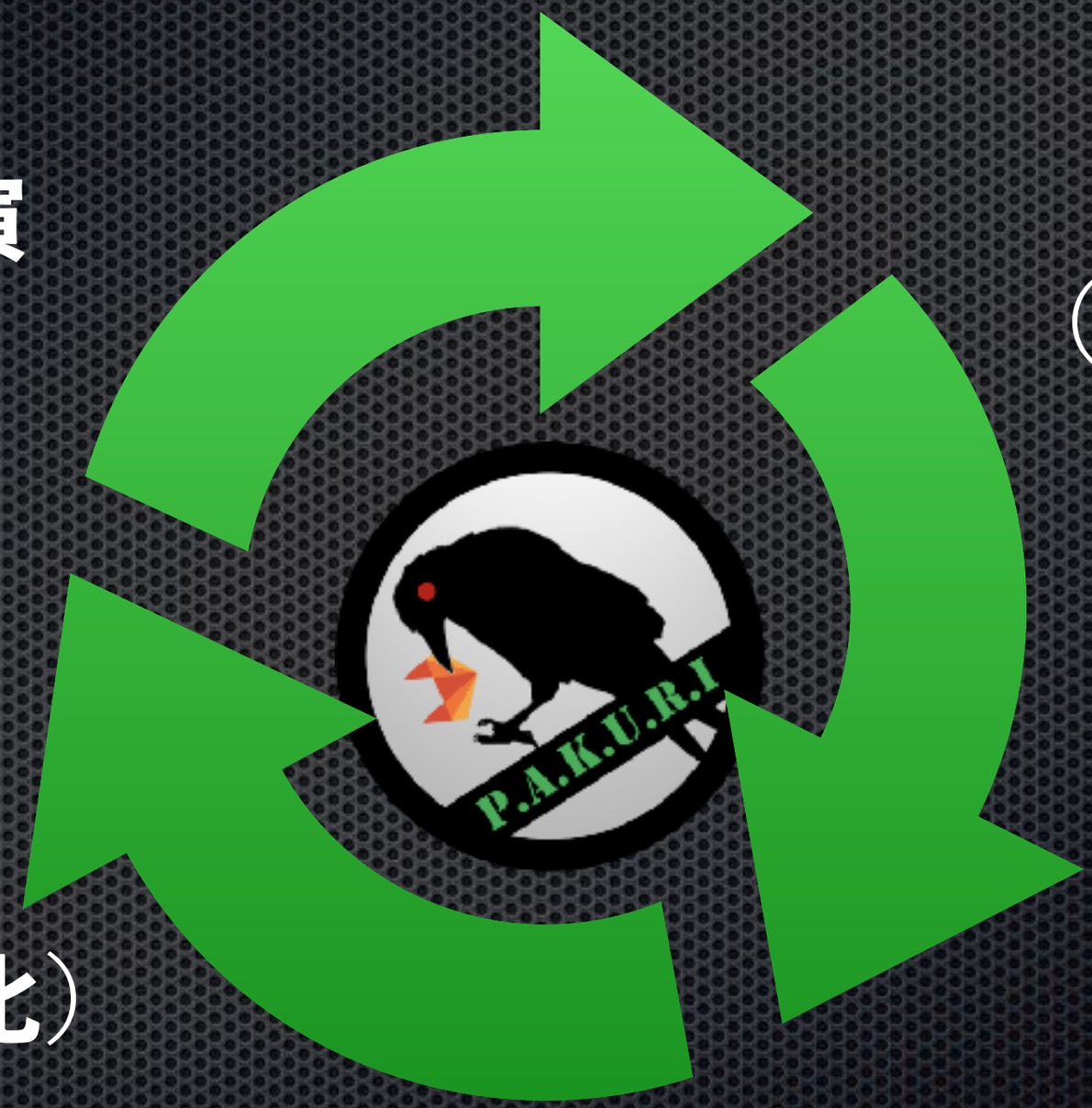
learn to

コンボの最後にlearn toを選ぶと画面右側に実行されるコマンドの説明が表示される

PAKURIを取り入れた学習サイクル

実演

解説
（ラーニング）



成功体験
（結果の可視化）

実習
（コンボ）

やってみせ、言って聞かせて、させてみせ、ほめてやらねば、人は動かじ

山本五十六

Your benefits

レッドチームの場合

1. PAKURIを使用する事で、頻繁に利用するコマンドを入力する手間が省けます。
2. 初心者のペンテスターは、PAKURIを使用して攻撃の流れを学べます。

ブルーチームの場合

1. 簡単な操作で、攻撃者の行動を模倣できます。

※あくまでも一例です

学習から実務までテンキーだけでできる！


テンキーの手
Operation with Ten-key

まとめ

ペンテスターは手を動かすことが大好きです。しかし、面倒くさい作業は好きではありません。PAKURIは、ペネトレーションテストで頻繁に使用するコマンドをテンキーの操作だけで実行します。まるで格闘ゲームをやっているような感覚でできます。

まとめ

PAKURIはペネトレーションテスターのキャリアを開始するのにも役に立てると思います。Kali-Toolsに準拠するツールを使用しているので必要以上に破壊することはしません。PAKURIを使用することで、ペネトレーションテストのフローを簡単に体験し学ぶことが出来ます。

PAKURIを使ってみて、ペネトレーションテストに興味を持ってください。

Thank you!

Please give me advice and feedback.

https://github.com/01rabbit/PAKURI

@PAKURI9
@01ra66it

pakuri.pentest@gmail.com