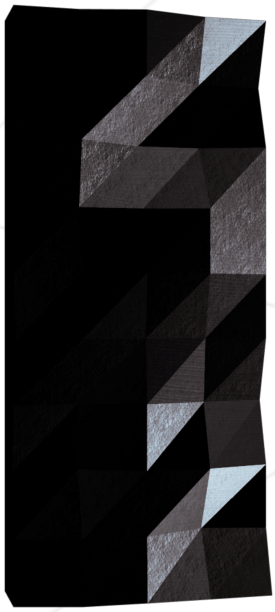


Road to Fore-Z

Summary: このドキュメントは、*Road to Fore-Z @ 42 Tokyo*の課題である。

Contents

I	**Foreword**	**2**
II	**Preparation**	**3**
III	**Mandatory Exercise 00**	**8**
IV	**Mandatory Exercise 01**	**9**
V	**Mandatory Exercise 02**	**10**
VI	**Mandatory Exercise 03**	**11**
VII	**Mandatory Exercise 04**	**12**
VIII	**Bonus Exercise 05**	**13**
IX	**Bonus Exercise 06**	**14**
X	**Bonus Exercise 07**	**15**

Chapter I

Foreword

プールで体力をつけたあなたは宇宙の旅行を経て、研究者となります。研究者へとなるための試験にてFore-Zラボへ侵入する必要があります。様々な課題を通じて培った経験を、セキュリティ分野での悪用を試みます。

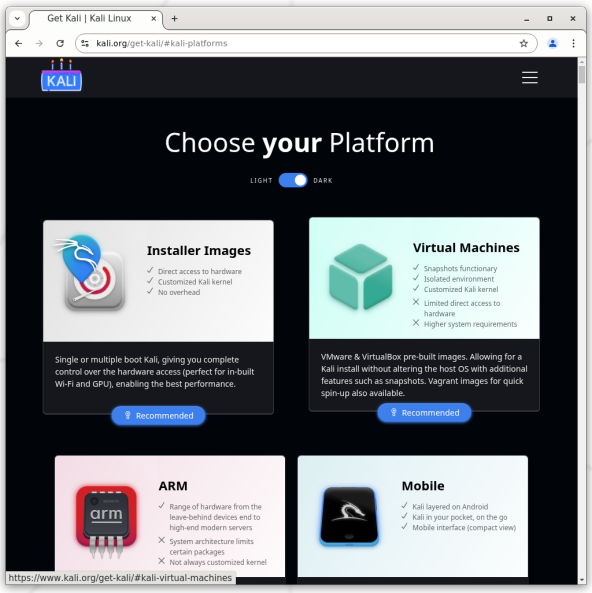
良いExploitはシンプル、かつ奇妙だ（ハッカーと画家９章より・一部改）

Chapter II

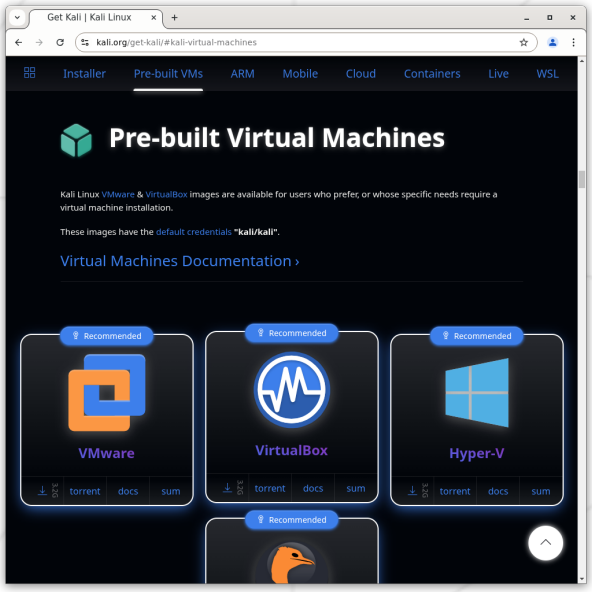
Preparation

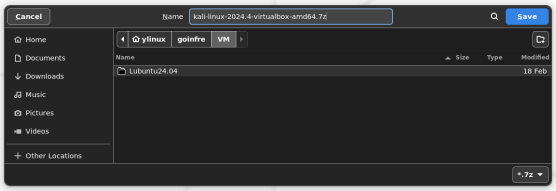
ラボを攻略するための攻撃用マシンと攻撃対象のマシンの構築を行います。

- 最初にラボを攻略するための攻撃に利用するマシンをダウンロードする必要があります。攻撃用マシンは`Kali Linux` を推奨しており、VirtualBox、VMware、 WSLでも簡単にセットアップすることが可能です。今回はVirtualBoxを利用します。
- まずは、Kali Linuxのダウンロードページにアクセスして、Virtual Machinesを選択してください。

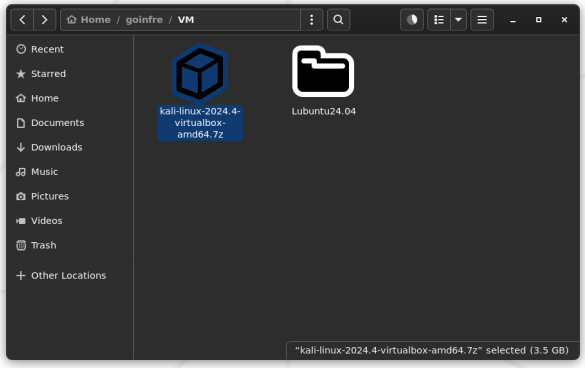


- VirtualBoxを選択し、VirtualBox用のファイルを名前を付けてgoinfre 又は sgoinfre 内に保存してください。

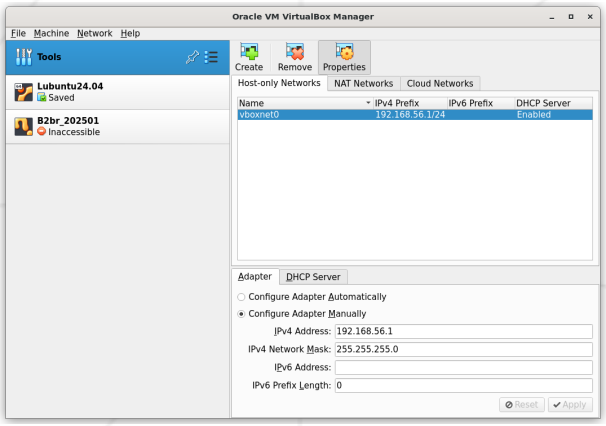




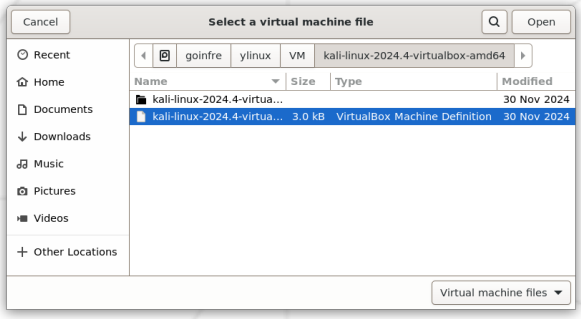
- 保存したファイルを解答してください。



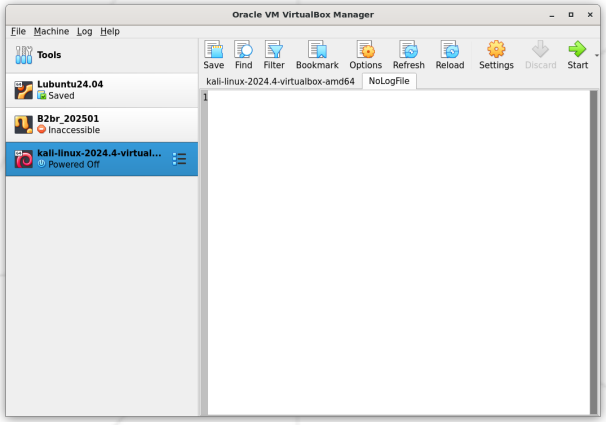
- 攻撃用マシンを構築するためにVirtualBoxを起動します。
- VirtualBoxのメニューからMachine -> Add を選択してください。



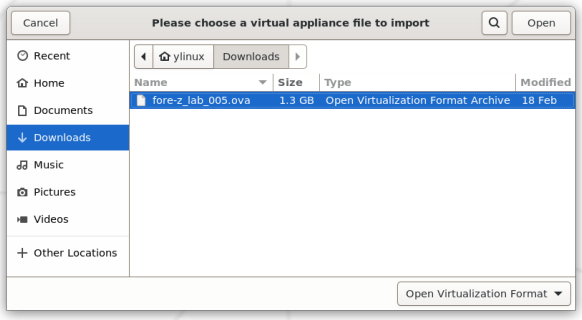
- ダウンロードして解凍したKali Linuxを選択してください。



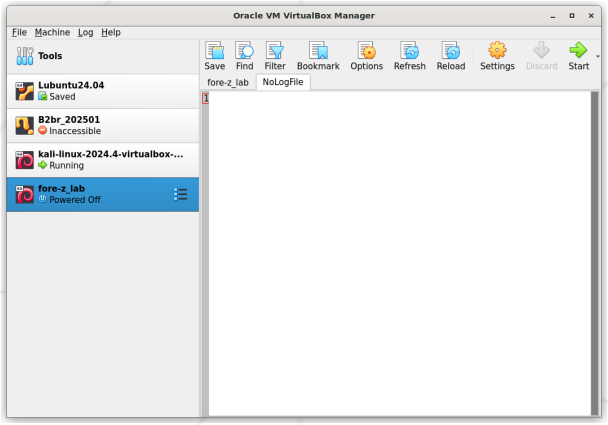
- 以下の画像のように、Kali Linuxのマシンが追加されているか確認してください。



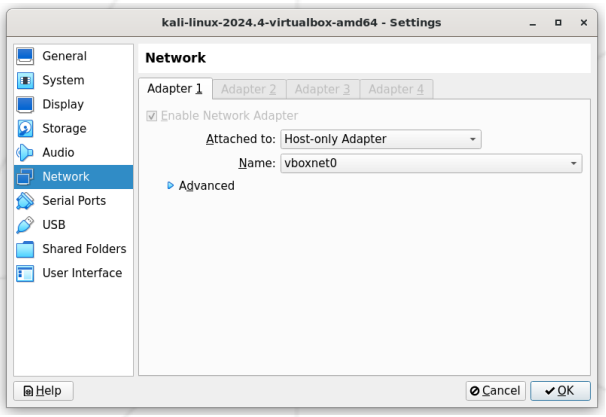
- 攻撃対象のマシンを構築するためにこちらのリンクから、ovaファイルをダウンロードしてください。
- VirtualBoxのメニューから、「File -> Import Appliance」を選択して、ダウンロードしたFore-Zの仮想マシンを選択してください。



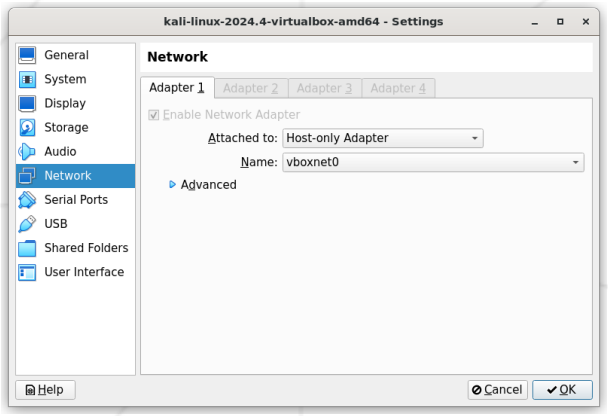
- 以下の画像のように、Fore-Zのマシンが追加されているか確認してください。



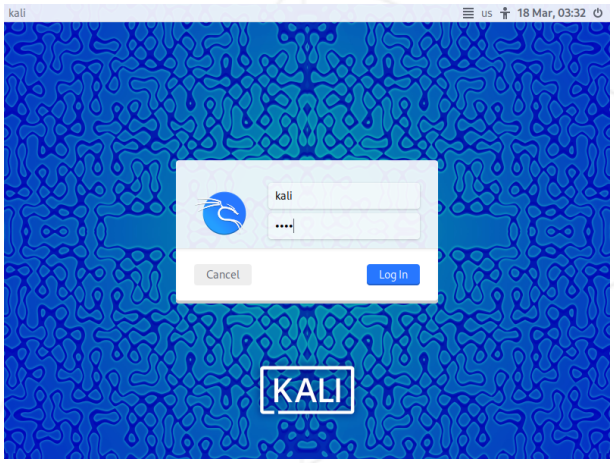
- 攻撃用マシン（kali）の設定画面を開き、ネットワークアダプタをホストオンリーアダプタに設定してください。



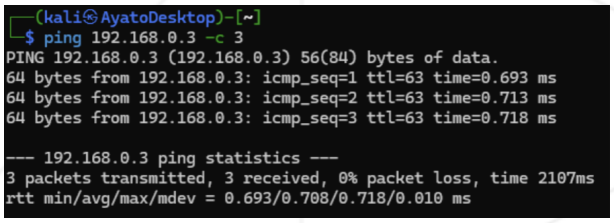
- 攻撃対象のマシン（fore-z_lab）の設定画面を開き、ネットワークアダプタをホストオンリーアダプタに設定してください。



- それぞれのマシンを起動してください。
- 攻撃用マシンに下記ログイン情報でログインしてください。
    - ユーザー名: kali
    - パスワード: kali



- 攻撃対象のマシン（fore-z_lab）に割り当てられているIPアドレスに対して、攻撃用マシン（kali）から Pingを送信してみましょう。※下のスクリーンショットのIPアドレスとは異なる可能性があります。



Chapter III

Mandatory Exercise 00

ラボの開いている 2 つのポートを列挙してください。レビューでは何番のポートが開いていたかを示す必要があります。

https://nmap.org/book/toc.html

Chapter IV

Mandatory Exercise 01

最も簡単な方法で一般ユーザーの権限でのシェルを取得してください。いくつかのブルートフォースや推測テクニックを要します。レビューでは「`cat /home/****/flag.txt`」を実行してシェルを獲得したことを示す必要があります。

https://www.kali.org/tools/hydra/
https://github.com/danielmiessler/SecLists/tree/master/Usernames

Chapter V

Mandatory Exercise 02

ラボのファイル共有に利用されているWEBポータルを悪用してWEBシェルを獲得してください。先ほどの初期アクセスを行ったシェルを利用してソースコードを確認しましょう。レビューでは「`cat /var/www/html/flag.txt`」を実行してWEBシェルを獲得したことを示す必要があります。

`https://owasp.org/www-project-top-ten/`
`https://portswigger.net/web-security/file-upload`

Chapter VI

Mandatory Exercise 03

獲得したシェルを用いて他のユーザーへログインを行います。ログインを行うと権限昇格する際に悪用が可能なバイナリが見つかります。宇宙旅行で獲得したデバッグやリバースエンジニアリングの知識が役立ちます。レビューでは「`cat /root/flag.txt`」を実行してシェルを獲得したことを示す必要があります。

Chapter VII

Mandatory Exercise 04

侵入を行った結果をレポートにまとめましょう。レポートでは以下の点に注意してください。

- 発見された脆弱性の記載：
    - 発見された脆弱性のリスト
    - 各脆弱性に対して以下の記載：
        - 概要
        - CVSSスコア
        - 脆弱性の対象
        - 脆弱性の対処法
        - 参考リンク
    - 脆弱性の再現手順：
        - ステップバイステップでの脆弱性の再現
    - スクリーンショット
    - コマンドの記載
    - 侵害ルート：
        - ステップバイステップで各ユーザー権限をどのように取得したか

Chapter VIII

Bonus Exercise 05

ダッシュボードに存在するWEBアプリの、リンクを踏んだ研究者のブラウザーで任意のJavaScriptを実行する脆弱性を発見してください。リンクを開いたときに、開いたブラウザーでポップアップが実行され、JavaScriptが実行されたことを示す必要があります。

Chapter IX

Bonus Exercise 06

問題４では権限昇格を行いました。もう１つの方法で権限昇格ができますか？

Chapter X

Bonus Exercise 07

ラボへの侵害を最速で行うためのスクリプトを作成して下さい。どのような言語を用いて作成しても問題ありません。スクリプトが実行された時、課題２～４でコマンドを実行したようにフラグを出力してください。スクリプトは以下のようなイメージで、出力に変更があっても問題ありません。