

「ハッキング・ラボのつくりかた」サーバー攻略方法

Amazonで物色しているときに書籍「ハッキング・ラボのつくりかた」が目についた。試し読みをしたところ、Linuxの基本的な説明を丁寧にしていたので購入。読み進めるにつれ、引き込まれ、思わず旧書も購入してしまった。自分用にターゲット端末の攻略のエッセンスだけを書き出す。公開することに問題があれば、指摘を願う。

構成

操作端末 : Let's note CF-T8
(Debian10,Docker:kali)
攻撃端末 : Let's note CF-T9 (Parrot)
ターゲット端末 : Let's note CF-N9(Debian12,VirtualBox7)

目次

1.機器構成

1.1 Dockerでkaliのcontainerを作成する。

ChatGPT3.5によるオプションの説明(抜粋)

操作端末側の設定[3]

DC-2の攻略手順

ファイル・ディレクトリの列挙:gobusterの実行20240507

情報収集:wigの実行20240507

ユーザーを探すnmap NSE(20240603)

参考図書・URL

[3] Dockerコンテナの中でGUIアプリケーションを起動させる | Unskilled?

1.機器構成

書籍では、Windowsを想定し、VirtualBoxを使ってハッキング・ラボを構築している。私は通常Debianを使っているので、わざわざVirtualBoxを使う必要がない。ターゲット端末は、VirtualBoxで配布されているのでそのまま構築する。

攻撃端末については、Parrotは、CF-T9にインストールしたものと、操作端末T8にDockerでkaliの環境を構築した。理由は、kaliについてDockerイメージが存在するから。

ターゲット端末は、当初W7で作成していたが、能力不足でN9に変更した。

操作端末は普段使いのT8で、ターゲット端末の準備、Parrotによるターゲット端末の攻略をssh接続で行う。

1.1 Dockerでkaliのcontainerを作成する。

kaliのcontainerでwiresharkを使いたかったので、docker runには、オプションをつけます。

```
:r !docker run --network host --cap-add NET_RAW --cap-add  
NET_ADMIN -it -e DISPLAY=$DISPLAY -v  
/tmp/.X11-unix:/tmp/.X11-unix --name kali kalilinux/kali-rolling:latest  
/bin/bash
```

あとは、exitで終了。

再スタートは、下記のコマンド。

```
:r !docker start kali  
:r !docker attach kali
```

ChatGPT3.5によるオプションの説明(抜粋)

`--cap-add NET\_RAW`と`--cap-add NET\_ADMIN`は、Dockerコンテナに特定のLinuxのcapabilities(機能)を付与するオプションです。

`NET\_RAW` capabilityは、コンテナがRaw socketsを作成する機能を付与します。Raw socketsは、データリンク層(OSIモデルでの第2層)にアクセスするためのインターフェースを提供します。これにより、コンテナ内でパケットをキャプチャしたり、生成したりすることができます。

`NET\_ADMIN` capabilityは、コンテナがネットワーク設定を変更する機能を付与します。具体的には、ルーティングテーブルの変更、ファイアウォールの設定、ネットワークデバイスの操作などが含まれます。これらのcapabilitiesをコンテナに付与することで、コンテナがネットワーク関連の操作を行うための必要な機能を持つようになります。

操作端末側の設定[3]

:r !xhost +local:

:r !xhost +local:

DC-2の攻略手順

ファイル・ディレクトリの列挙:gobusterの実行20240507

＜ChatGPT3.5説明:gobusterは、Webアプリケーションやウェブサーバーに対してディレクトリおよびファイルの検索を行うためのツールです。通常、セキュリティテストやペネトレーションテストなどのセキュリティ関連の活動で使用されます。

gobusterは、指定したURLに対して辞書攻撃を行い、存在するディレクトリやファイルを見つけることができます。これにより、攻撃者はサイト内の隠れたリソースやディレクトリ、アクセス制限が不十分なファイルなどを発見し、セキュリティ上の問題を特定することができます。end>

kaliOSで実行しようとしたが、common.txtがなかった。

なので、ParrotOSで実行

```
└─[ X ]─[yo@parrot]─[/usr/share/wordlists/dirb]
```

```
└─ $gobuster dir -u http://192.168.11.27 -w
```

```
/usr/share/wordlists/dirb/common.txt
```

```
=====
=====
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
=====
```

[+] Url: http://192.168.11.27

[+] Method: GET

[+] Threads: 10

[+] Wordlist: /usr/share/wordlists/dirb/common.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Timeout: 10s

```
=====
Starting gobuster in directory enumeration mode
=====
=====
./hta (Status: 403) [Size: 292]
./htaccess (Status: 403) [Size: 297]
./httpasswd (Status: 403) [Size: 297]
./server-status (Status: 403) [Size: 301]
./wp-admin (Status: 301) [Size: 317] [-->
http://192.168.11.27/wp-admin/]
./wp-content (Status: 301) [Size: 319] [-->
http://192.168.11.27/wp-content/]
./wp-includes (Status: 301) [Size: 320] [-->
http://192.168.11.27/wp-includes/]
./index.php (Status: 200) [Size: 53562]
./xmlrpc.php (Status: 405) [Size: 42]
Progress: 4614 / 4615 (99.98%)
=====
=====
Finished
=====
=====
```

情報収集:wigの実行20240507

<ChatGPT3.5説明: "Wig"は、Webアプリケーションに対する情報収集と攻撃サーフェスの特定を支援するためのツールです。このツールは、Webアプリケーションやその周辺のインフラストラクチャに関する情報を収集し、潜在的な脆弱性を発見するために使用されます。end>

これは、kaliOSで実行。

```
└─(root㊟T8)-[/usr/share/wordlists]
└─# wig http://192.168.11.27:80/
wig - WebApp Information Gatherer
Scanning http://192.168.11.27:80/...
```

SITE INFO

IP	Title
Unknown	DC-2 – Just another WordPress site

VERSION

Name	Versions	Type
WordPress CMS	3.8 3.8.1 3.8.2 3.8.3 3.8.4 3.8.5 3.8.6 3.8.7 3.8.8 3.9 3.9.1 3.9.2 3.9.3 3.9.4 3.9.5 3.9.6 4.0 4.0.1 4.0.2 4.0.3 4.0.4 4.0.5 4.1 4.1.1 4.1.2 4.1.3 4.1.4 4.1.5 4.2 4.2.1 4.2.2	
Apache	2.4.10	Platform
Debian	8.0	OS

INTERESTING

URL	Note	Type
/wp-login.php	Wordpress login page	
Interesting		
/readme.html	Readme file	
Interesting		

TOOLS

Name	Link	Software
wpscan	https://github.com/wpscanteam/wpscan	
WordPress CMSmap	https://github.com/Dionach/CMSmap	
WordPress		

VULNERABILITIES

Affected #Vulns

Link

WordPress 3.8 12

<http://cvedetails.com/version/162922>

WordPress 3.8.1 12

<http://cvedetails.com/version/162923>

WordPress 3.8.2 7

<http://cvedetails.com/version/176067>

WordPress 3.8.3 7

<http://cvedetails.com/version/176068>

WordPress 3.8.4 8

<http://cvedetails.com/version/176069>

WordPress 3.9 8

<http://cvedetails.com/version/176070>

WordPress 3.9.1 15

<http://cvedetails.com/version/169908>

WordPress 3.9.2 10

<http://cvedetails.com/version/176071>

WordPress 3.9.3 1

<http://cvedetails.com/version/185080>

WordPress 4.0 9

<http://cvedetails.com/version/176072>

WordPress 4.0.1 1

<http://cvedetails.com/version/185081>

WordPress 4.1 1

<http://cvedetails.com/version/185082>

WordPress 4.1.1 2

<http://cvedetails.com/version/185079>

WordPress 4.2 1

<http://cvedetails.com/version/185048>

WordPress 4.2.1 0

<http://cvedetails.com/version/184019>

WordPress 4.2.2 2

<http://cvedetails.com/version/185073>

Time: 8.9 sec Urls: 405

Fingerprints: 39241

ユーザーを探すnmap NSE(20240603)

kaliOSで実行

```
(root㊟T8)-[/usr/share/nmap/scripts]
└─# nmap -p80 --script http-wordpress-users 192.168.11.27
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 14:47
JST
Nmap scan report for dc-2 (192.168.11.27)
Host is up (0.00100s latency).
PORT      STATE SERVICE
80/tcp    open  http
| http-wordpress-users:
| Username found: admin
| Username found: tom
| Username found: jerry
|_ Search stopped at ID #25. Increase the upper limit if necessary
with 'http-wordpress-users.limit'
MAC Address: 08:00:27:3B:47:FF (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 8.49 seconds
```

以上

参考図書・URL

[1] IPUSIRON著

『ハッキング・ラボのつくりかた 完全版』翔泳社(2024/2/20)

[2] IPUSIRON著

『ハッキング・ラボのつくりかた』翔泳社(2018/12/7)

[3] [Dockerコンテナの中でGUIアプリケーションを起動させる | Unskilled?](#)

アクセス日20240417