



Tutorial - PentestGPT

Apresentação

PentestGPT é uma ferramenta para auxiliar a execução de testes de penetração, utilizando modelos de linguagem de larga escala (LLM). O objeto da solução é superar a dificuldade que modelos generalistas, como o ChatGPT, têm para manter uma compreensão integrada do cenário geral de testes.

Assim, a ferramenta garante a disponibilidade de informações de contexto necessárias para uma resposta mais precisa, além de fornecer um caminho estruturado das etapas a serem executadas para um teste de sucesso.

A solução surgiu a partir de um trabalho acadêmico envolvendo diversos pesquisadores, que pode ser consultado aqui: <https://arxiv.org/abs/2308.06782>

Instalação

Instale a versão mais recente usando o comando:

```
pip3 install git+https://github.com/GreyDGL/PentestGPT
```

Para uso da ferramenta, é necessário fornecer uma chave da API para sua conta na OpenAI.

No Linux, utilize o comando:

```
export OPENAI_KEY='<your key here>'
```

No Windows, utilize o comando:

```
set OPENAI_KEY='<your key here>'
```

Para iniciar a ferramenta, primeiro selecione o ambiente virtual onde foi feita a instalação. Em seguida, utilize o comando:

```
pentestgpt --reasoning_model=gpt-3.5-turbo-16k
```

Se desejar obter respostas mais precisas, utilize o modelo GPT-4-turbo. Porém, seu custo será superior ao modelo GPT-3.5-turbo.

Utilização

Você pode iniciar a ferramenta, informando o objetivo do teste que deseja realizar e o IP da máquina alvo. Por exemplo: “realizar um ataque à máquina <IP> para localizar o arquivo <nome_do_arquivo>

A ferramenta irá gerar uma árvore de tarefas que deverão ser executadas para atingir o objetivo solicitado.

Se precisar de mais esclarecimentos sobre as tarefas propostas, execute o comando **more**. A solução irá apresentar informações mais detalhadas sobre as ações e comandos que precisam ser executadas. Se os detalhes não forem satisfatórios, utilize a opção **brainstorm** para explorar novas possibilidades de ação. Caso precise de mais esclarecimentos, utilize o comando **discuss**.

Todos os comandos selecionados podem ser executados após confirmar a seleção usando a combinação das teclas SHIFT + seta direita.

Para sair do modo detalhado (ativado pelo comando **more**), utilize o comando **continue**.

Finalizada a execução da tarefa, execute o comando **next** e, em seguida, forneça ao PentestGPT informações que conseguir obter após terminar a tarefa. Por exemplo, se a tarefa era a realização de um port scan, informe quais as portas foram encontradas abertas e quais os serviços ativos.

Demonstração

Para demonstrar o uso da ferramenta, vamos conduzir um ataque a três dispositivos da plataforma de Hack The Box, da trilha básica de aprendizado. O objetivo será localizar o arquivo flag.txt em cada um dos dispositivos.

Será necessário utilizar um dispositivo com distribuição Linux para conduzir as tarefas do teste. Isso pode ser feito no próprio site da Hack the Box (HTB), na opção *Starting Point* -> *Pwnbox*, que disponibiliza uma instância web Linux, ou utilizando um dispositivo próprio conectado à rede da HTB por meio do aplicativo OpenVPN.

Caso opte por utilizar um dispositivo Linux próprio, gere o arquivo de configurações do OpenVPN na opção *Starting Point* -> *OpenVPN*. Importe o arquivo gerado no aplicativo OpenVPN para conectar-se à rede da HTB.

Neste tutorial, utilizaremos um dispositivo próprio, com distribuição Kali Linux, própria para execução de testes de penetração.

Para obter os IPs dos dispositivos, acesse o site <https://hackthebox.com/>, crie uma conta e depois acesse a trilha Starting Point, disponível em <https://app.hackthebox.com/starting-point>.

Dispositivo Alvo 1 – Meow

Para obter o IP do dispositivo, clique em *Meow, Spawn Machine*. Após alguns minutos, será fornecido o endereço IP correspondente.

A plataforma HTB fornece um roteiro, passo a passo, para realização do teste, que pode ser consultado na opção *Open Walkthrough*. No entanto, utilizaremos o PentestGPT para explorar as possibilidades de ações a serem executadas para cumprir nosso objetivo de localizar o arquivo *flag.txt*.

Já de posse do IP da máquina alvo e, após iniciar o PentestGPT, forneceremos a seguinte instrução: *Atacar o IP 10.129.111.181 para obter o conteúdo do arquivo flag.txt*

```
- ChatGPT Sessions Initialized.  
Please describe the penetration testing task in one line, including the target IP, task type, etc.  
> Atacar o IP 10.129.60.85 para obter o conteúdo do arquivo flag.txt
```

A solução retornará uma árvore de tarefas, similar à seguinte:

```
PentestGPT output:  
1. Reconnaissance -  
  1.1 Passive Information Gathering -  
  1.2 Active Information Gathering -  
  1.3 Identify Open Ports and Services -  
    1.3.1 Perform a full port scan -  
    1.3.2 Determine the purpose of each open port -
```

Além disso, fornecerá detalhes para execução das tarefas recomendadas, como vemos a seguir:

Realizar um port scan:

To execute task **1.3.1**, "Perform a full port scan," follow these steps:

1. Open your command-line interface (CLI).
2. Use the Nmap tool by entering the command: ``nmap -p- <target_IP>``. Replace ``<target_IP>`` with the IP address of the target system you are testing.
3. Wait for the scan to complete and review the results. The results will list all open ports on the target system.

Determinar o propósito de cada porta aberta:

For task **1.3.2**, "Determine the purpose of each open port," proceed with the following:

1. Review the list of open ports obtained from the full port scan.
2. For each open port, use Nmap's service version detection feature by entering: ``nmap -sV -p <port_number> <target_IP>``. Replace ``<port_number>`` with the specific open port number you are investigating and ``<target_IP>`` with the target system's IP address.
3. Analyze the output to determine the service and version running on each open port. This information will help you understand the potential vulnerabilities associated with each service.

Em um terminal da nossa distribuição Kali Linux, executamos o primeiro comando sugerido pelo PentestGPT. Sua execução irá demorar alguns minutos.

Caso necessite, utilize a opção **discuss** para questionar o PentestGPT sobre como reduzir o tempo de execução do port scan. Utilize perguntas como "como realizar o port scan de maneira rápida?" ou "como realizar o port scan apenas nas portas mais comuns?"

Dentre as alternativas possíveis estão o uso da flag T4, para determinar a quantidade de portas escaneadas por segundo, ou a flag F, que restringe o port scan apenas para as 100 portas mais comuns. A opção T4, no entanto, pode gerar algum alerta nos sistemas de detecção de intrusão do alvo (IDS).

Após a execução do port scan, iremos acionar o comando next e, em seguida, tool, para informar ao PentestGPT qual foi a saída obtida do nmap:

```
> next
Please choose the source of the information.
(*) tool Paste the output of the security test tool used
( ) user-comments
( ) web Paste the relevant content of a web page
( ) default Write whatever you want, the tool will handle it
Your input: (End with <shift + right-arrow>)
> PORT STATE SERVICE
- 2 - 23/tcp open telnet
```

Como resposta, o PentestGPT irá incluir novas sub-tarefas na árvore, como mostrado a seguir:

```
1.3.3 Enumerate Telnet service for version and configuration details -
1.3.4 Check for default credentials on Telnet service -
1.3.5 Attempt manual connection to Telnet service to gauge response -
```

Além disso, irá sugerir a sub-tarefa favorita para execução, fornecendo detalhes adicionais:

```
Favorable sub-task most likely to lead to successful exploit:
1.3.4 Check for default credentials on Telnet service -
□
To perform this task: Connect to the Telnet service using a Telnet client by typing `telnet 10.129.60.85 23` in the terminal, replacing "10.129.60.85" with the target IP address. Once connected, attempt to log in using common default usernames and passwords, as many systems are left with these insecure settings.
```

Após executar o comando sugerido, conseguimos acesso à tela de login da máquina alvo.

```
# telnet 10.129.60.85 23
Trying 10.129.60.85 ...
Connected to 10.129.60.85.
Escape character is '^]'.

Hack the Box

Meow login:
```

Note que a instrução anterior sugerir tentativa de login com nomes de usuário e senhas padrão. No PentestGPT, acionamos novamente a opção next -> tool, para fornecer novas informações sobre o andamento do teste e solicitar mais informações sobre essa estratégia:

```
> next
Please choose the source of the information.
(*) tool Paste the output of the security test tool used
() user-comments
() web Paste the relevant content of a web page
() default Write whatever you want, the tool will handle it
Your input: (End with <shift + right-arrow>)
> o comando telnet permitiu acessar a tela de login do dispositivo alvo. Liste quais são os usernames e pa
-> sswords comuns que podem ser testados para uma tentativa de login.
```

Como resposta, o PentestGPT sugeriu testar os seguintes usernames: admin, root ou user.

```
Favorable sub-task most likely to lead to successful exploit:
1.3.4.1 Attempt to login with common usernames and passwords -
[]
To perform this task: Use the Telnet client to connect to the target's Telnet service by entering `telnet
23` in the command line. Once at the login prompt, try a list of common default credentials, such as
"admin:admin," "root:root," or "user:user," to see if you can gain unauthorized access.
```

Após executar a tarefa, o username root permitiu o acesso ao dispositivo:

```
Meow login: root
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.4.0-77-generic x86_64)
```

De volta ao prompt de comando do PentestGPT, vamos executar o comando next -> tool, para fornecer essa atualização e solicitar novas instruções.

```
> next
Please choose the source of the information.
(*) tool Paste the output of the security test tool used
() user-comments
() web Paste the relevant content of a web page
() default Write whatever you want, the tool will handle it
Your input: (End with <shift + right-arrow>)
> o usuário root permitiu acesso ao dispositivo alvo. Forneça orientações sobre como localizar o arquivo f
-> lag.txt no dispositivo.
```

A solução, então, sugeriu o uso do comando “find / -type f -name “flag.txt” para localizar o arquivo:

```
Favorable sub-task most likely to lead to successful exploit:  
2.1.1 Locate "flag.txt" on the device -
```

```
To perform this task: Connect to the target device as the root user via the Telnet service and use the  
"find" command to search for "flag.txt" by entering `find / -type f -name "flag.txt"` in the terminal. This  
command will search the entire file system for a file named "flag.txt" and output the path to the file if  
it exists.
```

A execução do comando sugerido obteve o resultado desejado, com a localização exata do arquivo procurado:

```
root@Meow:~# find / -type f -name "flag.txt"  
/root/flag.txt
```

Teste concluído com sucesso!

Dispositivo Alvo 2 – Fawn

Para obter o IP do dispositivo, clique em *Fawn, Spawn Machine* e aguardade alguns minutos.

Em seguida, inicie o PentestGPT, e forneça a seguinte instrução: *Atacar o IP 10.129.11.83 para obter o conteúdo do arquivo flag.txt*

A ferramenta retornará novamente uma árvore de tarefas:

```
Please describe the penetration testing task in one line, including the target IP, task type, etc.  
> Atacar o IP10.129.11.83para obter o conteúdo do arquivo flag.txt  
PentestGPT output:  
1. Reconnaissance -  
  1.1 Passive Information Gathering -  
  1.2 Active Information Gathering -  
  1.3 Identify Open Ports and Services -  
    1.3.1 Perform a full port scan -  
    1.3.2 Determine the purpose of each open port -  
To execute task 1.3.1 "Perform a full port scan", please follow these steps:  
  
1. Open your terminal.  
2. Use the Nmap tool by entering the command: `nmap -p- <target_IP_address>`. Replace `<target_IP_address>`  
with the actual IP address of the target system.  
3. Wait for the command to complete and observe the output for a list of open ports.  
  
The purpose of this task is to identify all open ports on the target system, which will help in determining  
potential points of entry for further exploitation or assessment.
```

Após a execução do port scan usando o nmap, identificamos que a porta 21 está aberta com o serviço ftp. Fornecemos essa informação para o PentestGPT por meio do comando **next -> tool** e aguardamos novas instruções:

```
> next  
Please choose the source of the information.  
(*) tool Paste the output of the security test tool used  
( ) user-comments  
( ) web Paste the relevant content of a web page  
( ) default Write whatever you want, the tool will handle it  
Your input: (End with <shift + right-arrow>)  
> porta 21/tcp aberta, serviço ftp
```

Após o processamento, o PentestGPT atualiza a árvore de tarefas recomendando uma análise da porta 21/tcp. Para isso, recomenda conectar ao servidor FTP. Usaremos o comando **more** para obter mais detalhes.

```
Selected favorable sub-task for potential successful exploit:
- 1.3.2.1 Analyze port 21/tcp (FTP) -

To perform this task:
Firstly, manually connect to the FTP server using a command-line client like `ftp` or `nc` to observe the banner and determine the FTP server software and version. Secondly, research known vulnerabilities for the identified FTP server version to plan for potential exploitation.
```

A ferramenta fornece agora um passo a passo detalhado para realização da tarefa:

```
Below are the further details.
To execute task 1.3.2.1 "Analyze port 21/tcp (FTP)", please follow these steps:

1. Open your terminal.
2. Connect to the FTP server using the command: `ftp <target_IP_address>`. Replace `<target_IP_address>` with the actual IP address of the target system.
3. Observe the banner that is displayed upon connection, which often includes the FTP server software name and version.
4. Disconnect from the FTP server by typing `quit`.
5. Research known vulnerabilities for the identified FTP server software and version using online databases like CVE Details or Exploit Database.

The purpose of this task is to gather information about the FTP service running on port 21/tcp, which can be used to identify potential vulnerabilities for further exploitation.
```

Com o comando executado, identificamos a versão do ftp (vsFTPd 3.0.3) e fornecemos essa informação ao PentestGPT, solicitando mais orientações sobre como localizar o arquivo flag.txt.

```
> next
Please choose the source of the information.
(*) tool Paste the output of the security test tool used
() user-comments
() web Paste the relevant content of a web page
() default Write whatever you want, the tool will handle it
Your input: (End with <shift + right-arrow>)
> identificada versão do ftp como vsFTPd 3.0.3. Como localizar o arquivo flag.txt no dispositivo alvo usando essas informações?
```

A solução sugere 4 novas tarefas: pesquisar vulnerabilidades para essa versão do ftp, tentar um acesso anônimo, enumerar diretórios e arquivos e procurar pelo arquivo flag.txt:

```
1.3.2.1.2 Research known vulnerabilities for vsFTPd 3.0.3 -
1.3.2.1.3 Attempt anonymous access to the FTP server -
1.3.2.1.4 Try to enumerate directories and files -
1.3.2.1.5 Look for the flag.txt file -
```

Vamos executar o comando **discuss** para questionar como efetuar acesso anônimo ao servidor ftp.

```
> discuss
Please share your thoughts/questions with PentestGPT. (End with <shift + right-arrow>)
Your input: como efetuar acesso anônimo ao servidor ftp
```

Como resultado, a solução sugere uma tentativa de acesso utilizando o usuário anonymous e senha em branco.


```
Selected favorable sub-task for potential successful exploit:
- 1.3.2.1.3.1 Use FTP client to login with username 'anonymous' and empty password -

To perform this task:
Open a command-line FTP client and attempt to connect to the target FTP server using the username
'anonymous' and leaving the password field blank or using 'anonymous' as the password. If the server allows
anonymous access, check for successful login and then proceed to list and navigate through the directories
to search for sensitive files or information.
```

A recomendação foi efetiva e permitiu o acesso ao servidor ftp:

```
# ftp 10.129.11.83
Connected to 10.129.11.83.
220 (vsFTPD 3.0.3)
Name (10.129.11.83:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Vamos acionar novamente o modo **discuss**, para solicitar esclarecimentos sobre a segunda parte da recomendação, que sugere listar e navegar pelos diretórios para busca.

```
> discuss
Please share your thoughts/questions with PentestGPT. (End with <shift + right-arrow>)
Your input: após obtido acesso ao servidor ftp, como listar e navegar pelos diretórios em busca do arquivo
-> flag.txt?
```

O PentestGPT sugere, então, os comandos “ls” e “cd” para listar e mudar de diretórios. Após sua execução, já é possível identificar o arquivo “flag.txt”:

```
ftp> ls
229 Entering Extended Passive Mode (|||50456|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 32 Jun 04 2021 flag.txt
```

Teste concluído com sucesso!

Dispositivo Alvo 3 – Dancing

Para obter o IP do dispositivo, clique em *Dancing, Spawn Machine* e aguardade alguns minutos.

Em seguida, inicie o PentestGPT, e forneça a seguinte instrução: *Atacar o IP 10.129.236.122 para obter o conteúdo do arquivo flag.txt*

A ferramenta retornará novamente uma árvore de tarefas recomendando a execução de um port scan, como nos casos anteriores. Após a execução do comando, identificamos 3 portas abertas:


```

└─# nmap -F 10.129.236.122
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-10 13:02 EST
Nmap scan report for 10.129.236.122
Host is up (0.14s latency).
Not shown: 97 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.88 seconds

```

Vamos repassar essas informações ao PentestGPT e solicitar mais orientações para atingirmos nosso objetivo. Para isso, executamos os comandos next -> tool.

```

> next
Please choose the source of the information.
(*) tool Paste the output of the security test tool used
() user-comments
() web Paste the relevant content of a web page
() default Write whatever you want, the tool will handle it
Your input: (End with <shift + right-arrow>)
> as portas 135, 139 e 445 estão abertas, com os serviços msrpc, netbios-ssn e microsoft-ds. Mostre como p
-> odemos explorar essas portas para localizar o arquivo flag.txt no dispositivo alvo.

```

Como recomendação, a ferramenta sugere enumerar os compartilhamentos na porta 445 e realizar a busca pelo arquivo "flag.txt". Vamos executar o comando more, para obter mais detalhes.

```

The favorable sub-task most likely to lead to a successful exploit:
1.3.2.3.1 Enumerate shares and permissions -

To perform this task:
Use the `smbclient` tool to list shared resources on the target device's port 445. Once the shares are
listed, use the same tool or `enum4linux` to check for permissions on each share to identify where you may
have read or write access.

```

Como resposta, é apresentada uma sequência de tarefas para serem executadas:

```

Below are the further details.
To execute task 1.3.2.3.1 "Enumerate shares and permissions" on port 445, follow these steps:

1. Open your terminal or command-line interface.
2. Use the `smbclient` tool to list shares on the target machine with the command: `smbclient -L
//<target-ip> -N`
3. Take note of the shares listed by the command.
4. For each share, attempt to connect to it using: `smbclient \\\<target-ip>\\<sharename> -N`
5. Once connected, use `ls` to list files and directories within the share.
6. Use `showacls` to display permissions for each file and directory if the tool supports it.
7. Document which shares you have access to and the level of that access (read/write).

This task is crucial for identifying potentially sensitive information that is accessible through network
shares and understanding what actions an attacker could perform, such as reading sensitive files or writing
malicious files to the system.

```

Após a execução do primeiro comando, identificamos 4 compartilhamentos. Vamos tentar uma conexão com cada um deles:

```
L# smbclient -L //10.129.236.122 -N
Sharename      Type            Comment
-----
ADMIN$          Disk            Remote Admin
C$              Disk            Default share
IPC$            IPC             Remote IPC
WorkShares      Disk
```

Conseguimos acesso aos compartilhamentos IPC\$ e WorkShares. Porém, apenas esse último continha diretórios.

```
L# smbclient \\\\10.129.236.122\\WorkShares -N
Try "help" to get a list of possible commands.
smb: \> ls
.                D          0   Mon Mar 29 04:22:01 2021
..               D          0   Mon Mar 29 04:22:01 2021
Amy.J            D          0   Mon Mar 29 05:08:24 2021
James.P          D          0   Thu Jun  3 04:38:03 2021
```

Vamos retornar essa informação ao PentestGPT e solicitar novas orientações sobre como prosseguir com a busca pelo arquivo flag.txt. Para isso, vamos usar a opção discuss.

```
> discuss
Please share your findings and questions with PentestGPT.
Your input: foram identificados 2 diretórios no compartilhamento WorkShares: Amy.J e James.P. Como procede
-> r para verificar se o arquivo flag.txt está em algum desses diretórios?
```

A ferramenta apresenta, então, um esclarecimento detalhado sobre como realizar essa verificação, mostrando os comandos que devem ser executados, passo a passo:

```
Once connected, change to the `Amy.J` directory with the `cd` command:
...
cd Amy.J
...

List the contents of the `Amy.J` directory using the `ls` command to check for `flag.txt`:
...
ls
...

If `flag.txt` is not found in the `Amy.J` directory, change to the `James.P` directory:
...
cd ../James.P
...

Repeat the listing command in the `James.P` directory:
...
ls
...
```

Após execução, identificamos que o arquivo flag.txt encontra-se no diretório James.P:

```

smb: \> ls
.                               D          0 Mon Mar 29 04:22:01 2021
..                              D          0 Mon Mar 29 04:22:01 2021
Amy.J                           D          0 Mon Mar 29 05:08:24 2021
James.P                         D          0 Thu Jun  3 04:38:03 2021

5114111 blocks of size 4096. 1750435 blocks available
smb: \> cd Amy.J\
smb: \Amy.J\> ls
.                               D          0 Mon Mar 29 05:08:24 2021
..                              D          0 Mon Mar 29 05:08:24 2021
worknotes.txt                   A          94 Fri Mar 26 07:00:37 2021

5114111 blocks of size 4096. 1750435 blocks available
smb: \Amy.J\> cd ../James.P\
smb: \James.P\> ls
.                               D          0 Thu Jun  3 04:38:03 2021
..                              D          0 Thu Jun  3 04:38:03 2021
flag.txt                        A          32 Mon Mar 29 05:26:57 2021

5114111 blocks of size 4096. 1750435 blocks available

```

Teste concluído com sucesso!