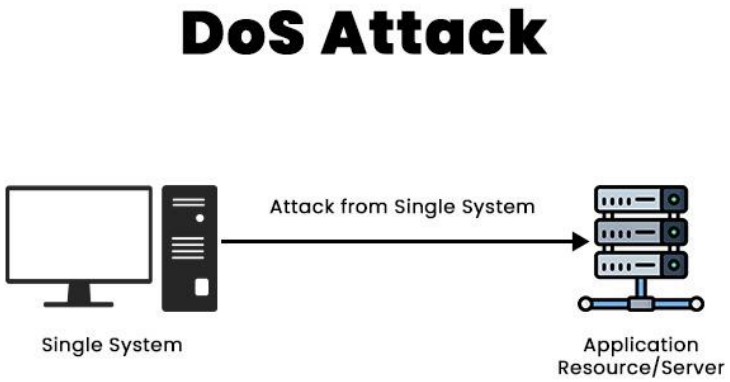
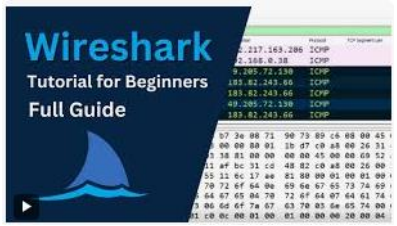
Pen Testing

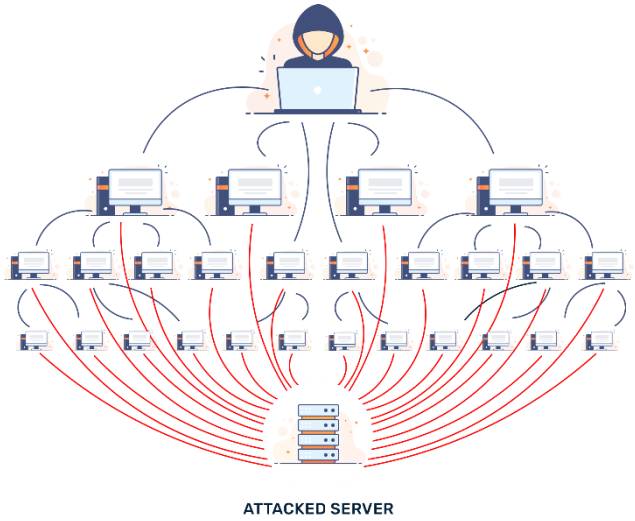
ESSAYER DE TROUVER ET D'EXPLOITER LES VULNÉRABILITÉS D'UN SYSTÈME INFORMATIQUE

DoS/DDoS

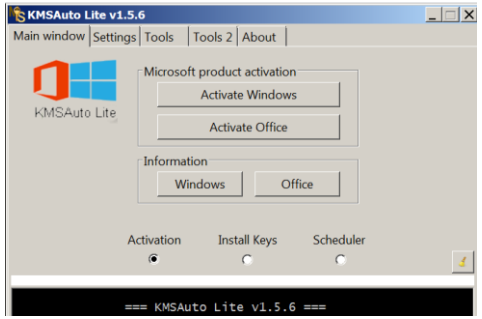


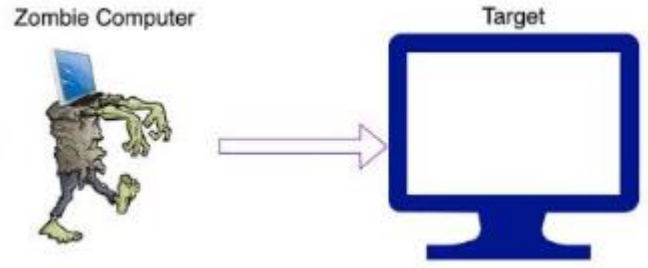
Facile à détecter





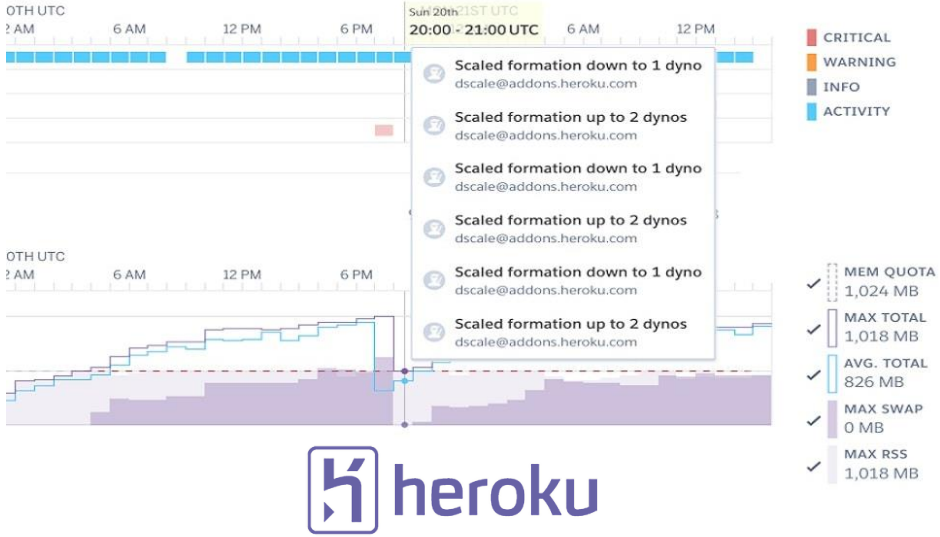
très difficile à détecter



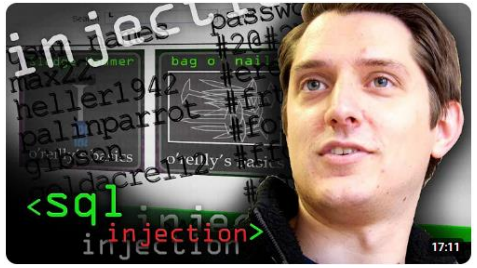


Test

de nombreux outils

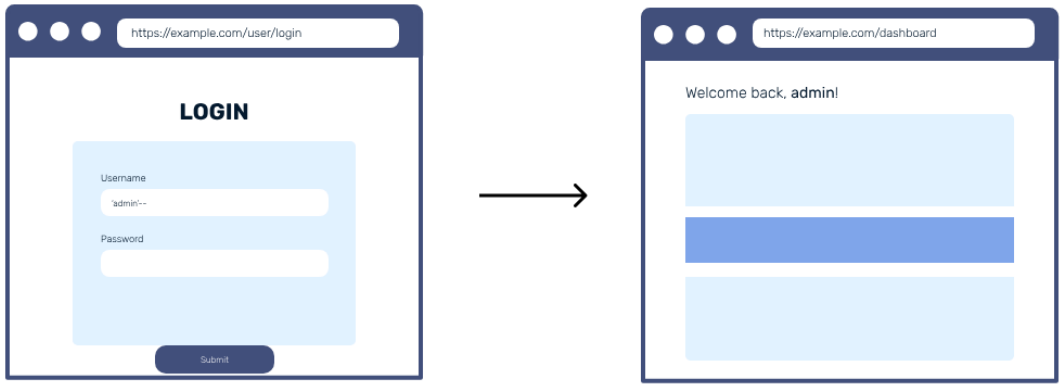


SQL injection

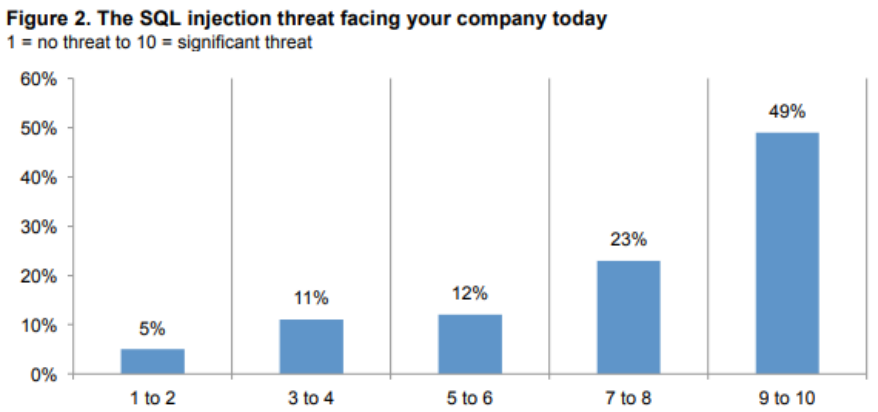


Running an SQL Injection Attack – Computerphile
https://www.youtube.com/watch?v=ciNHn38EyRc

```
query= "SELECT * FROM Users WHERE Username = " + username + " AND Password = " + password + ";"
```



Is SQL injection still a thing?



The SQL Injection Threat Study
https://www.ponemon.org/local/upload/file/DB%20Networks%20Research%20Report%20FINAL5.pdf

Tests

manually testing

```
seclist@localhost:~/scanner/sqlmap$ sudo ./sqlmap.py --update

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.0.6.65#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual
 consent is illegal. It is the end user's responsibility to obey all applicable
local, state and federal laws. Developers assume no liability and are not respon
sible for any misuse or damage caused by this program

[*] starting at 21:34:51

[21:34:51] [INFO] updating sqlmap to the latest development version from the Git
Hub repository
[21:34:51] [INFO] update in progress ....
[21:34:55] [INFO] updated to the latest revision '74d0315'

[*] shutting down at 21:34:55

seclist@localhost:~/scanner/sqlmap$ sudo ./sqlmap.py

        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.0.7.1#dev}
|_ -| . [.]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

Usage: python sqlmap.py [options]
```

MITM (man-in-the-middle)

Indicateurs d'une attaque MITM :

Connexions non chiffrées :

Trafic HTTP au lieu de HTTPS, en particulier sur des réseaux publics ou inconnus.

Ponts intermédiaires :

Le trafic semble passer par des intermédiaires inattendus (comme un proxy ou une passerelle inconnue).

Changements dans les adresses ARP :

La table ARP montre que plusieurs IP sont associées à la même adresse MAC (indication de spoofing).

Latence anormale :

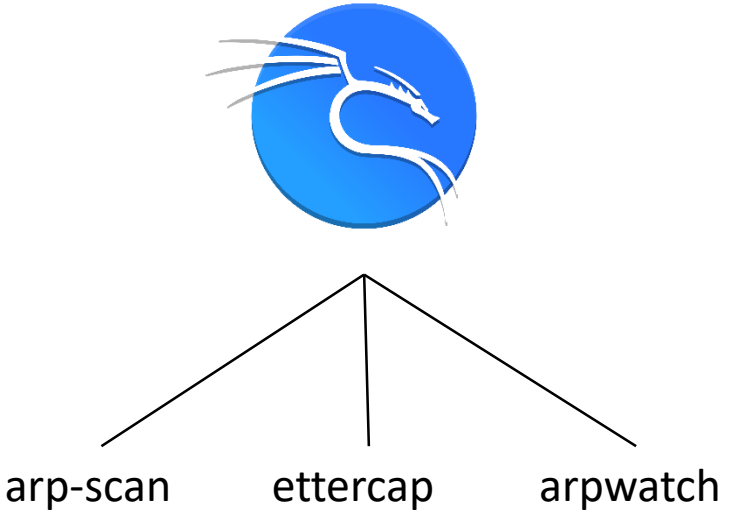
Des retards inattendus dans le trafic peuvent être un symptôme de redirection ou d'inspection.

Tests

Validation des certificats
Inspecter le certificat délivré par un serveur HTTPS pour vérifier sa validité et sa correspondance avec le domaine.

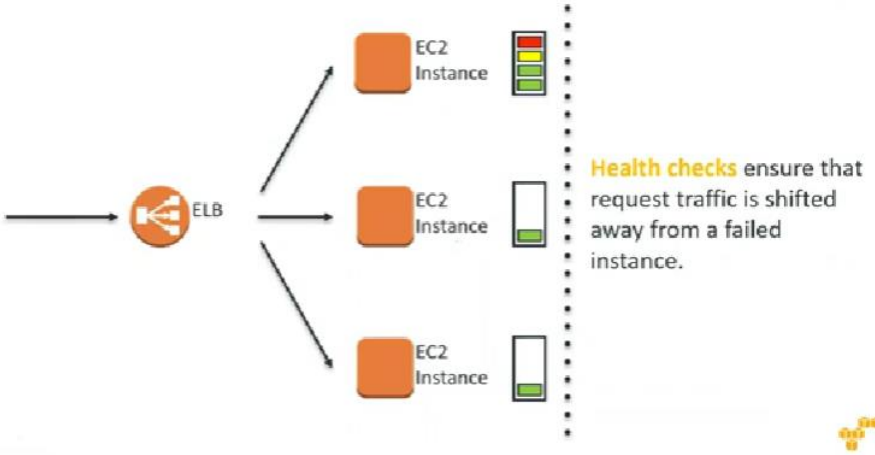
Analyse du réseau
Détection du spoofing ARP :
Détecter les changements dans la table ARP.

Tests de proxy
Analyser si un proxy intermédiaire altère le trafic :
Faux proxy pour analyser si les applications autorisent des connexions non sécurisées.

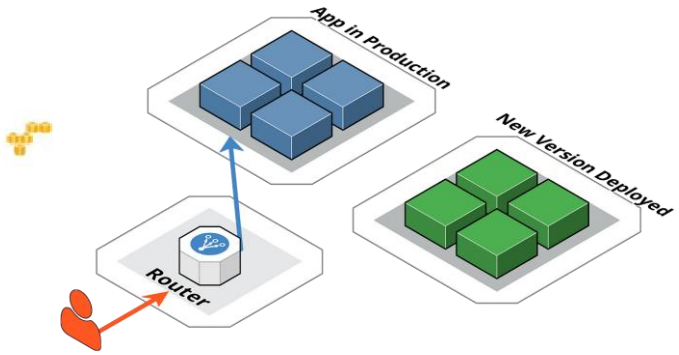


Isolement

Load Balancers with Isolated Traffic
AWS Elastic Load Balancer



Blue/Green Deployments



Canary Deployments