



# Cybersécurité

INTERVENTION CYBERSÉCURITÉ EN BTS SIO – PREMIÈRE ANNÉE

# Parcours

- ▶ Développement logiciel et outils de sécurité
- ▶ BTS SIO SLAM
- ▶ 2 mois de dev (CDD en première année)
- ▶ Root-Me
- ▶ Licence Pro ASSR (Administration et Sécurité de Systèmes et des Réseaux) (alternance)
- ▶ 2 ans de SOC (niveau 3)
- ▶ Ecole 2600 (alternance: incident response, malware analysis, gestion de crise, DevSecOps et formateur)
- ▶ CTF

# Comment sécuriser un SI ?

- ▶ Sécurité physique
- ▶ Sécurité réseau
- ▶ Sauvegarde
- ▶ PRA
- ▶ Réplication
- ▶ Antivirus/EDR/NDR/XDR
- ▶ Supervision
- ▶ Logs
- ▶ Sensibilisation cyber
- ▶ Moindre privilège
- ▶ Security by design (dev)
- ▶ Hardening
- ▶ SIEM
- ▶ SAST/DAST (par CI/CD)
- ▶ Pentest
- ▶ SOAR
- ▶ Red teaming
- ▶ Incident response (tooling / préparation)
- ▶ ...



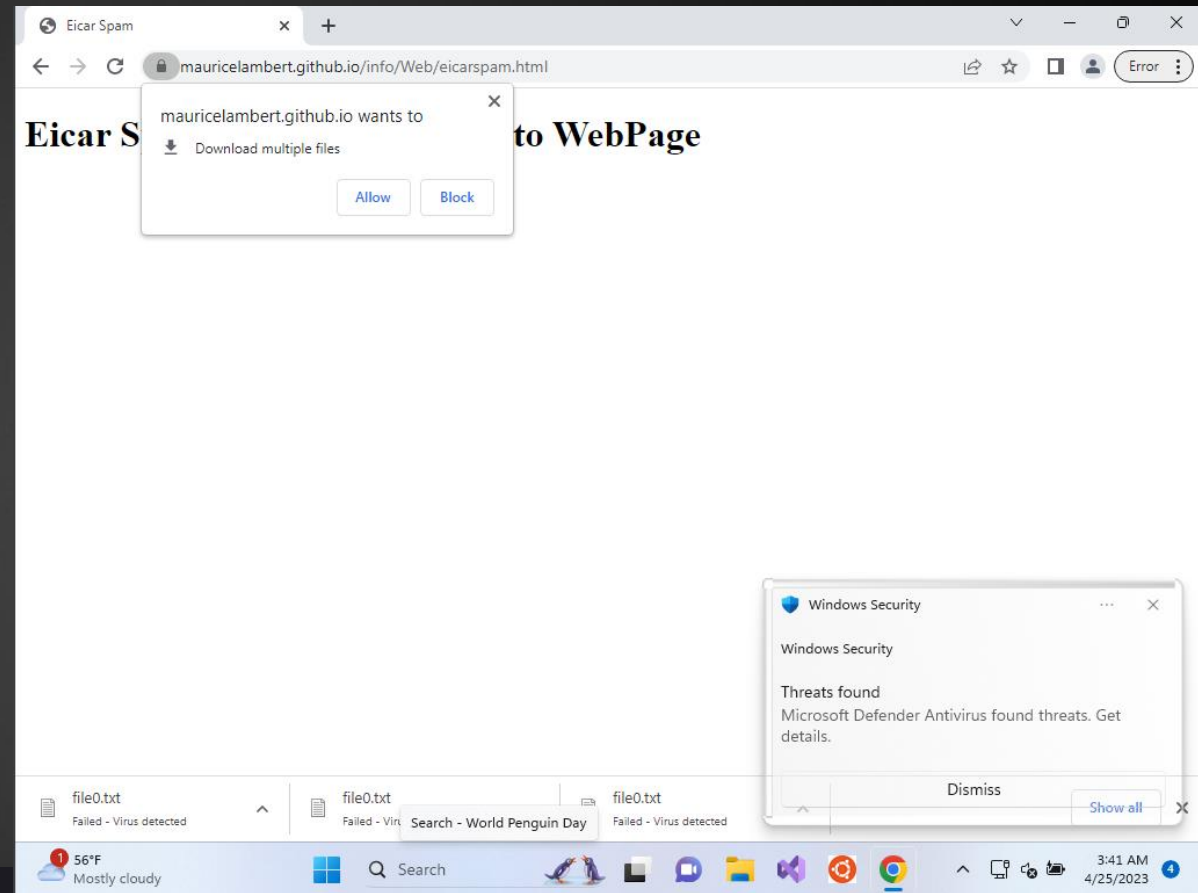
## Quel sont les points d'entrées pour les attaquants ?

- ▶ Collaborateurs
  - ▶ Malveillants
  - ▶ Qui cliquent partout
  - ▶ Installent des malwares
- ▶ DMZ - Services sur internet
- ▶ Applicatifs « client réseau » (navigateurs, ...)
- ▶ Matériels (clefs, badges, vol d'ordinateurs...)
- ▶ Réseau local (appareil personnel compromis)
- ▶ Secrets/Données publiées

# Pratique (pour le POC: pas d'exécution ni de malware, votre antivirus générera des alertes)

Site qui « vérole » automatiquement

- ▶ Cliquez sur ce [lien](#)
- ▶ Autorisez le téléchargement si nécessaire
- ▶ 300 [fichiers eicar \(test antivirus\)](#) seront téléchargés
- ▶ Pour vous protéger: bloquez le javascript (exemple: extension « noscript »)

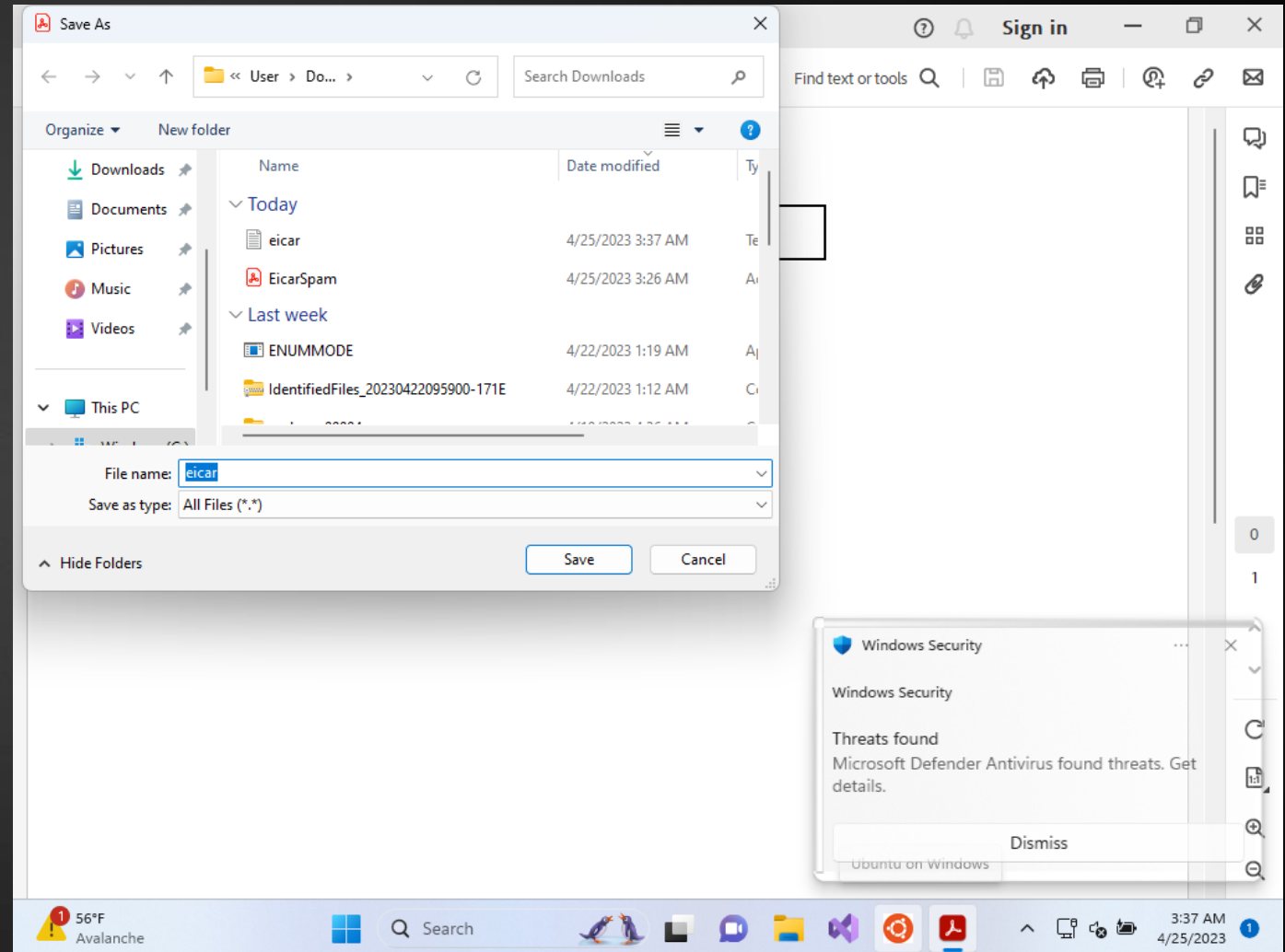


**Eicar Spam using javascript into WebPage**

# Pratique (pour le POC: pas d'exécution ni de malware, votre antivirus générera des alertes)

PDF qui « vérole » à l'ouverture

- ▶ Télécharger et ouvrir avec AdobeReader [le PDF suivant](#)
- ▶ 300 [fichiers eicar \(test antivirus\)](#) seront téléchargés
- ▶ Pour vous protéger: ne jamais ouvrir de PDF avec AdobeReader, vous pouvez les ouvrir avec Firefox (chrome non recommandé)



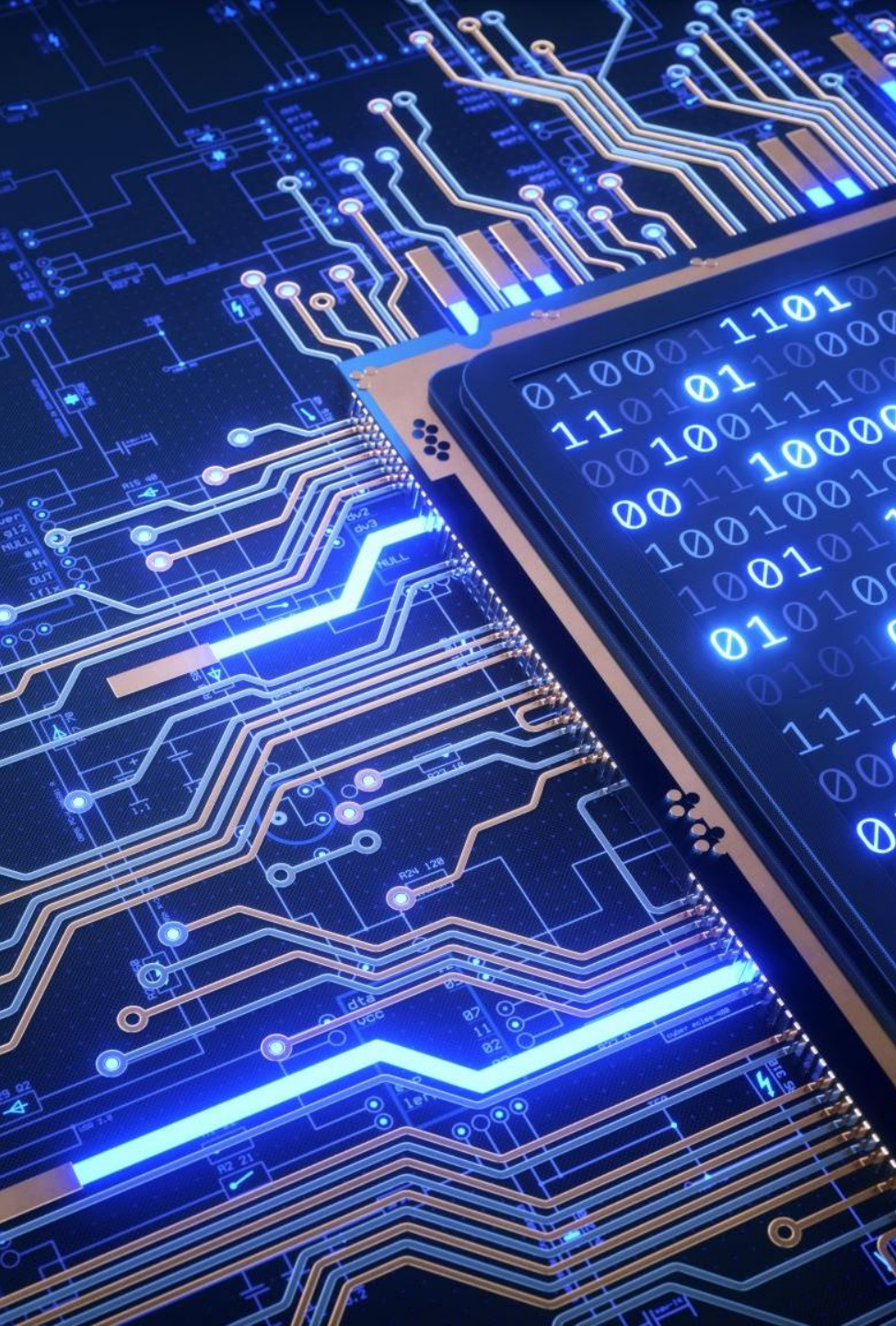
# Qu'est ce que la cybersécurité ?

- ▶ 4 principes/piliers: confidentialité, intégrité, disponibilité, traçabilité
- ▶ ChatGPT: « La cybersécurité est un ensemble de processus, de technologies et de personnes qui travaillent ensemble pour protéger les organisations, les individus et les données contre les cyberattaques et les piratages. Elle vise à protéger les ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données contre les menaces numériques. La cybersécurité est un sous-ensemble de la sécurité informatique. Elle est importante pour protéger les systèmes critiques et les informations sensibles contre les attaques numériques. »

# Qu'est ce qu'on peut faire en cybersécurité ?

- ▶ RSSI
- ▶ Officier de sécurité
- ▶ DevSecOps
- ▶ SOC
- ▶ Blue team
- ▶ Chercheur de vulnérabilité
- ▶ Purple Team
- ▶ Pentester
- ▶ Red team





# Cyber: pour les SISR (Admin) ou pour les SLAM (Dev) ?

- ▶ Ressources en dev rares et précieuses
- ▶ Salaires en dev concurrencent la cyber
- ▶ Besoin: 75% admin système/réseau et 25% dev
- ▶ Aujourd'hui 95% d'admin système/réseau pour 5% de dev
- ▶ Pas de formation cyber pour les dev



# Eternels problèmes cyber en dev

- ▶ Nerver trust inputs
  - ▶ Injections (SQL, command, code, XSS, ...)
  - ▶ Overflow (Stack Buffer Overflow...)
- ▶ Complexité des systèmes
- ▶ Pression sur le développement
- ▶ Formation des dev à la sécurité

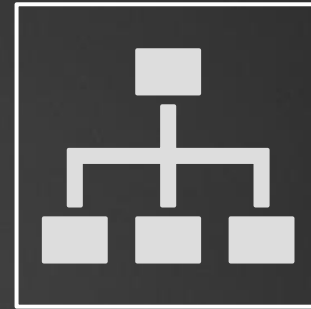
# Dev, nouveaux problèmes cyber:



## Intelligence artificielle

ChatGPT

Copilot



## Supply chain

Contributions malveillantes (politique, opportuniste, ...)

Prise de contrôle du repository

Typosquatting

Confusion de dépendances

## Pratique: demandez à ChatGPT des pages d'authentification en PHP et NodeJS

- ▶ Ouvrir [perplexity](#) et posez vos 2 questions
- ▶ J'ai eu ces résultats: [PHP auth](#) et [NodeJS auth](#)
- ▶ Multiples vulnérabilités notamment une SQL Injection et des secrets en clair

```
23 // Check if the login form has been submitted
24 if (isset($_POST['username']) && isset($_POST['password'])) {
25     $username = $_POST['username'];
26     $password = $_POST['password'];
27
28     // Validate the user's credentials
29     $sql = "SELECT * FROM users WHERE username='$username' AND password='$password'";
30     $result = mysqli_query($conn, $sql);
31
```

```
7 // Configure passport to use the local strategy for authentication
8 passport.use(new LocalStrategy(
9     function(username, password, done) {
10         // Replace this with your own authentication logic
11         if (username === 'admin' && password === 'password') {
12             return done(null, { username: 'admin' });
13         } else {
14             return done(null, false, { message: 'Incorrect username or password.' });
15         }
16     }
17 ));
```

# Pratique: POC confusion de dépendance

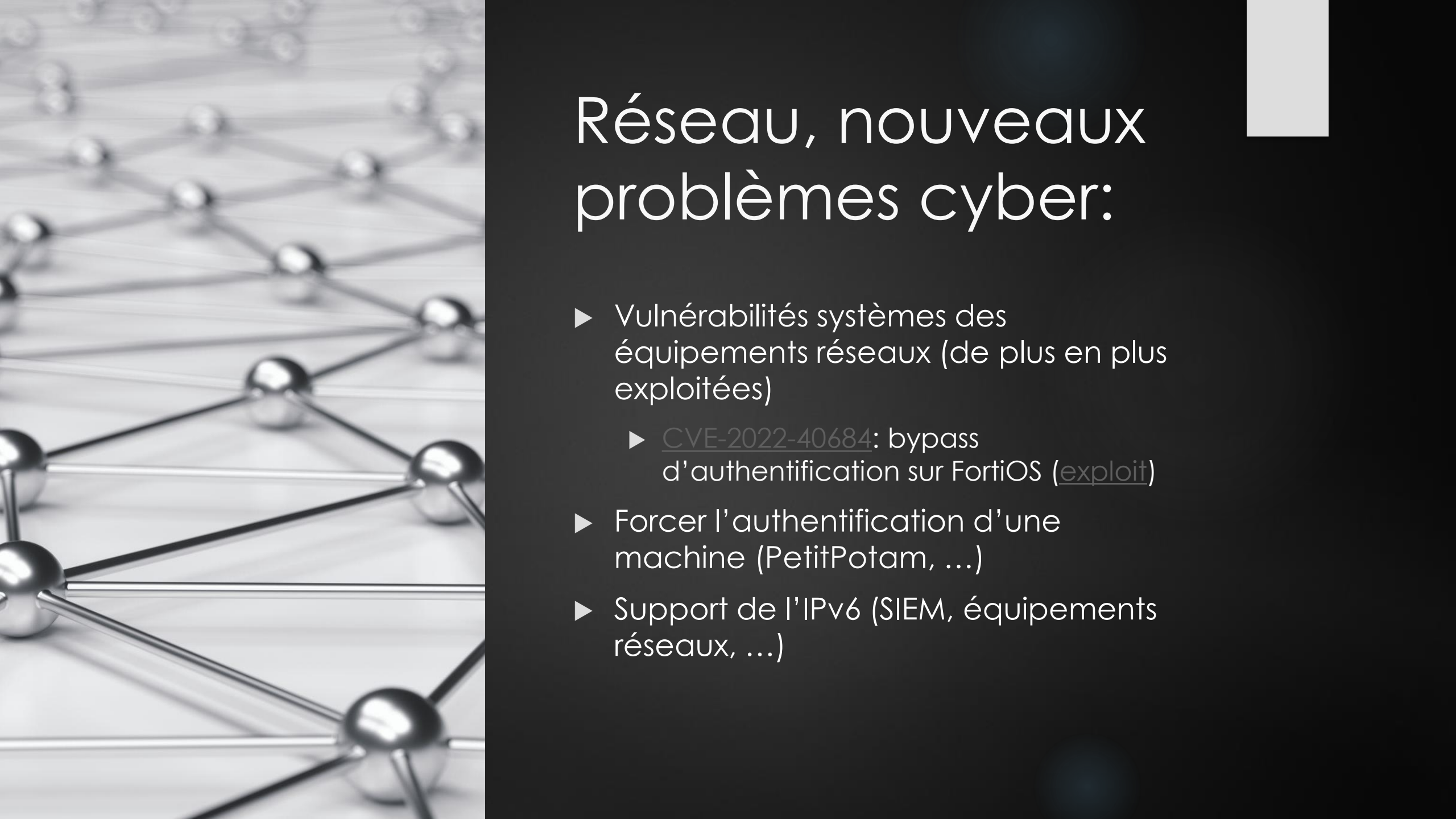
- ▶ Allez voir la version sur du repository DependencyConfusion sur [pypi](#) (version 666) puis sur [test pypi](#) (version 0.0.2)
- ▶ Installez DependencyConfusion à l'aide de pypi en spécifiant que vous voulez utiliser test pypi, avec la commande suivante:
  - ▶ `pip install --extra-index-url https://test.pypi.org/simple/ DependencyConfusion`
- ▶ Regardez la version du package installé (indiqué durant l'installation, sinon utilisez la commande: `pip freeze`)
- ▶ La version installé est la 666 et non la 0.0.2, l'attaque est réussi

```
C:\Users>pip install --extra-index-url https://test.pypi.org/simple/ DependencyConfusion
Defaulting to user installation because normal site-packages is not writeable
Looking in indexes: https://pypi.org/simple, https://test.pypi.org/simple/
Collecting DependencyConfusion
  Downloading DependencyConfusion-666.tar.gz (3.5 kB)
  Installing build dependencies ... done
  Getting requirements to build wheel ... done
  Preparing metadata (pyproject.toml) ... done
Building wheels for collected packages: DependencyConfusion
  Building wheel for DependencyConfusion (pyproject.toml) ... -
```

```
DependencyConfusion
Installation:
- DependencyConfusion (666)
You should install this module using:
pip install --extra-index-url https://test.pypi.org/simple/ DependencyConfusion
The dependency confusion attack is successful if the installed version is 666.
Otherwise if the installed version is 0.0.2 the attack is missed.
To exploit the dependency confusion attack you should use --extra-index-url instead of --index-url.
```

# Eternels problèmes cyber en réseau

- ▶ Broadcast / multicast
- ▶ MIM
- ▶ Bruteforce
- ▶ Scan de port
  - ▶ IP Sweep
- ▶ DOS
  - ▶ SynFlood / ICMP flood (Ping of death)
  - ▶ ICMP Smurf / ICMP Redirect
  - ▶ IP fragmentation attack
  - ▶ ARP spoof
  - ▶ Spanning Tree Protocol (STP) Attacks
- ▶ DNS configuration (transfert de zone)
- ▶ RFC vulnérable (pas de security by design)
- ▶ Surveillance des flux chiffrés (SSL sortant, IPv6, ...)
- ▶ Ressource pour le chiffrement (SNMP v2/v3)
- ▶ Usurpation (packet crafting, modification des routes)
- ▶ L'impact des erreurs de configuration (facebook -> BGP)
- ▶ Sniffing



# Réseau, nouveaux problèmes cyber:

- ▶ Vulnérabilités systèmes des équipements réseaux (de plus en plus exploitées)
  - ▶ [CVE-2022-40684](#): bypass d'authentification sur FortiOS ([exploit](#))
- ▶ Forcer l'authentification d'une machine (PetitPotam, ...)
- ▶ Support de l'IPv6 (SIEM, équipements réseaux, ...)

# Pratique: Hostname spoofing

- ▶ Installez [NetbiosSpoof](#) avec des droits d'admin ou root
  - ▶ `sudo python3 -m pip install NetbiosSpoof`
- ▶ Lancez NetbiosSpoof avec des droits d'admin ou root
  - ▶ `sudo python3 -m NetbiosSpoof`
- ▶ Depuis un Windows sur le même réseau faites un ping sur les noms locaux que vous voulez usurper
  - ▶ `ping -4 -n 1 facebook`
- ▶ Vous remarquerez que tous les ping partent sur la même adresse IP, celle de l'attaquant
- ▶ L'attaque est réussie

```
C:\Users>ping -n 1 -4 facebook

Pinging facebook.local [192.168.0.11] with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users>ping -n 1 -4 tralala

Pinging tralala.local [192.168.0.11] with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users>ping -n 1 -4 PocForHostnameSpoofing

Pinging PocForHostnameSpoofing.local [192.168.0.11] with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.0.11:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss)
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users>ping -n 1 -4 thatswork

Pinging thatswork.local [192.168.0.11] with 32 bytes of data:
Reply from 192.168.0.11: bytes=32 time<1ms TTL=64
```



```
(kali㉿kali)-[~]  
└─$ sudo NetworkScan -a -t 192.168.0.0/24
```

```
NetworkScanner Copyright (C) 2021, 2022 Maurice Lambert  
This program comes with ABSOLUTELY NO WARRANTY.  
This is free software, and you are welcome to redistribute  
under certain conditions.
```

```
PythonToolsKit Copyright (C) 2022, 2023 Maurice Lambert  
This program comes with ABSOLUTELY NO WARRANTY.  
This is free software, and you are welcome to redistribute  
under certain conditions.
```

```
[+] IP: '192.168.0.254' is UP and responds to ping.  
[+] IP: '192.168.0.47' is UP and responds to ping.  
[-] IP: '192.168.0.33' is DOWN  
[-] IP: '192.168.0.77' is DOWN  
[-] IP: '192.168.0.142' is DOWN  
[-] IP: '192.168.0.228' is DOWN  
[-] IP: '192.168.0.36' is DOWN  
[-] IP: '192.168.0.42' is DOWN  
[-] IP: '192.168.0.19' is DOWN  
[-] IP: '192.168.0.252' is DOWN  
[-] IP: '192.168.0.113' is DOWN  
[-] IP: '192.168.0.114' is DOWN  
[-] IP: '192.168.0.27' is DOWN  
[-] IP: '192.168.0.226' is DOWN  
[-] IP: '192.168.0.35' is DOWN  
[-] IP: '192.168.0.108' is DOWN  
[-] IP: '192.168.0.94' is DOWN  
[-] IP: '192.168.0.240' is DOWN  
[-] IP: '192.168.0.10' is DOWN  
[-] IP: '192.168.0.43' is DOWN  
[-] IP: '192.168.0.133' is DOWN  
[-] IP: '192.168.0.115' is DOWN  
[-] IP: '192.168.0.100' is DOWN  
[-] IP: '192.168.0.172' is DOWN  
[-] IP: '192.168.0.81' is DOWN  
[-] IP: '192.168.0.235' is DOWN  
[-] IP: '192.168.0.158' is DOWN
```

# Pratique: Host discovery

- ▶ Installez [NetworkScanner](#) avec la commande:  
`sudo python3 -m pip install NetworkScanner`
- ▶ Utilisez le scanner avec la commande suivante:  
`sudo NetworkScan -a -t <network/IP range>`
- ▶ Vous trouverez rapidement les adresses IP sur le réseau

# Pratique: Port scan

- ▶ Installez PortsScanner avec la commande: `python3 -m pip install PortsScanner`
- ▶ Utilisez le scanner avec la commande suivante: `sudo PortsScanner <IP address>`
- ▶ Vous trouverez rapidement les principaux ports ouverts sur la machine
- ▶ Vous pouvez utiliser d'autres scanners comme AsyncPortScanner ([SourceForge](#)) ou PowerShellAsyncPortScan. Le premier est compilé et multi-plateforme (sans aucun prérequis mais facile à détecter par un antivirus), le second est pratique sous Windows.

```
(kali㉿kali)-[~]
└─$ sudo pip install PortsScanner
[sudo] password for kali:
Collecting PortsScanner
  Downloading PortsScanner-0.0.1.tar.gz (20 kB)
  Preparing metadata (setup.py) ... done
Building wheels for collected packages: PortsScanner
  Building wheel for PortsScanner (setup.py) ... done
  Created wheel for PortsScanner: filename=PortsScanner-0.0.1-py3-
  Stored in directory: /root/.cache/pip/wheels/0e/07/77/017097f40d
Successfully built PortsScanner
Installing collected packages: PortsScanner
Successfully installed PortsScanner-0.0.1
WARNING: Running pip as the 'root' user can result in broken permi

(kali㉿kali)-[~]
└─$ sudo PortsScanner 192.168.0.47

PortsScanner Copyright (C) 2021 Maurice Lambert
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions.

open: 445 microsoft_ds microsoft_ds
open: 139 netbios_ssn netbios_ssn

(kali㉿kali)-[~]
└─$
```