



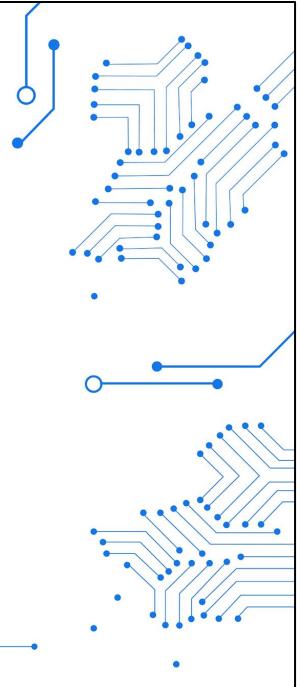
# Techniques de Hacking avancées

xxx



# Sommaire

1. Menaces sur les SI
2. Préparation et initialisation des phases à exploitation
3. Positionnement "Attaquant Externe"
4. Positionnement "Attaquant Interne"
5. Phases de Post-Exploitation
6. Bonus "autres techniques"

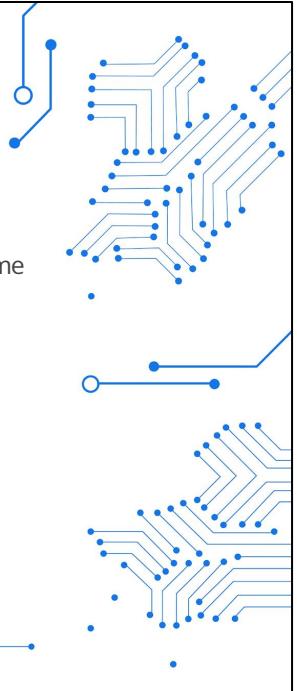


---

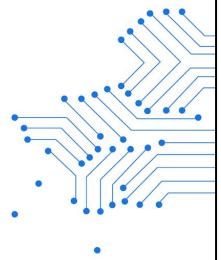
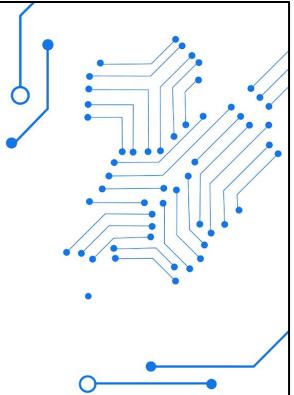
# Techniques de Hacking avancées

## Objectifs du cours

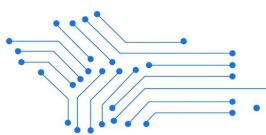
- Savoir utiliser les outils permettant l'analyse Forensic sur OS WINDOWS
- Collecter et analyser de façon méthodique des évidences lors d'un cybercrime
- Être opérationnel
- Exploitation des principaux artefacts sur Windows
- Retracer un chemin d'attaque
- Créer un rapport



---



## 1. Menaces sur les SI

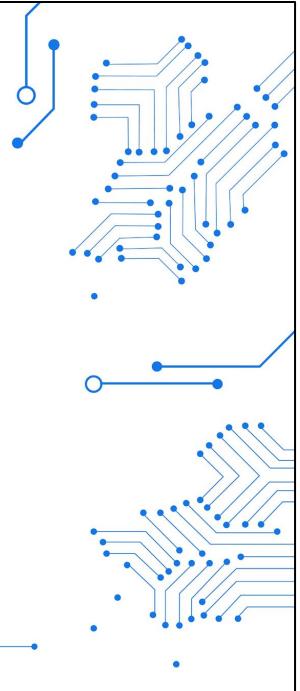


---

## 1. Menaces sur les SI

### 1) Les Modèles SI

- 2) Statistiques
- 3) Failles Connues et 0day
- 4) Étude des séquences d'exploitation



---

## Menaces sur le SI

### Les modèles SI

#### Questions

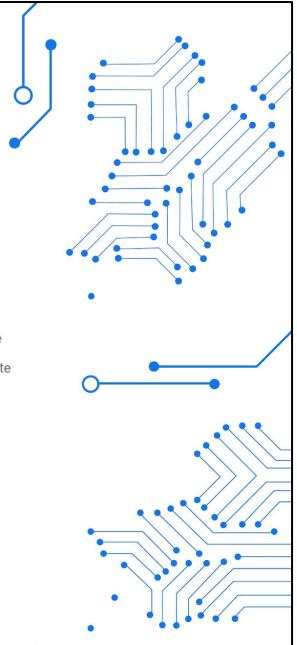
- Quel est la situation actuelle ?
- Quel sont les évolutions de nos systèmes d'information ?



---

# Menaces sur le SI

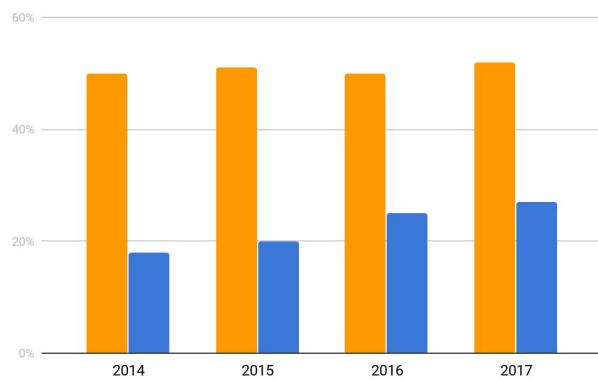
## Les modèles SI



### Cloud privé

De plus en plus d'entreprise utilise le cloud privé

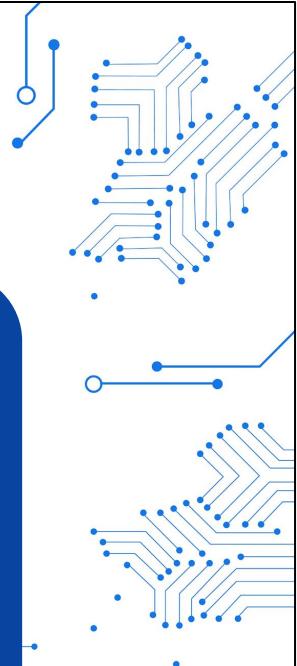
Utilisation du cloud privé



---

# Menaces sur le SI

## Les modèles SI



### C2 : Command & Control

Des services légitimes utilisés pour des activités malveillantes

Twitter

Github

Amazon

Pastebin

Yahoo

Answer

Babelfish

Dropbox

Live.com

Hotmail.com

Microsoft TechNet

Microsoft

Answers

Microsoft Social

OneDrive

Google docs

Google Code

Google Translate

Google App Script

Google Calendar

Google Plus

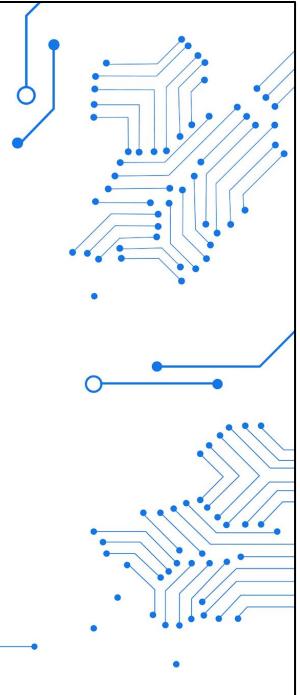
Gmail

Blogger

---

## 1. Menaces sur les SI

- 1) Les Modèles SI
- 2) Statistiques**
- 3) Failles Connues et 0day
- 4) Étude des séquences d'exploitation

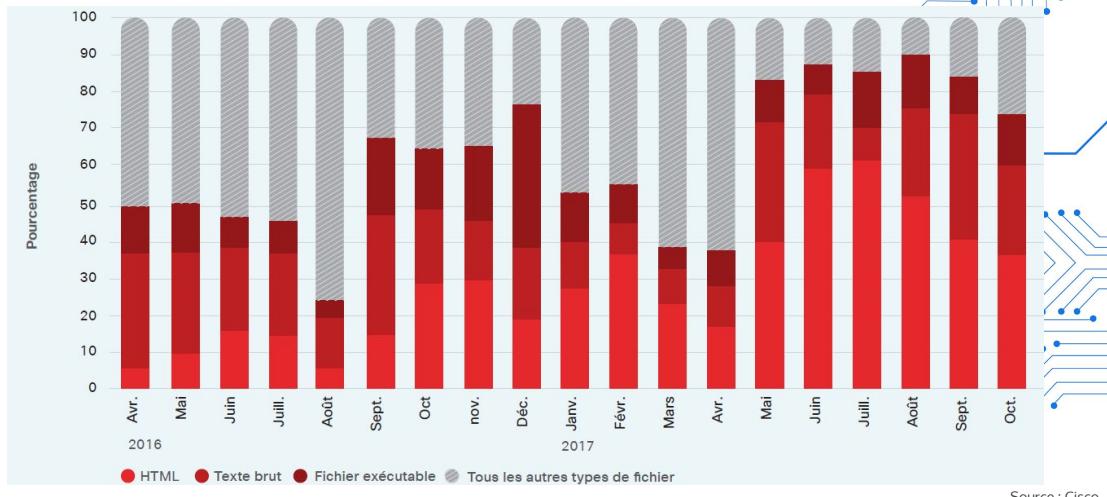


---

# Menaces sur le SI

## Statistique

### Blocage des malwares par type de contenu



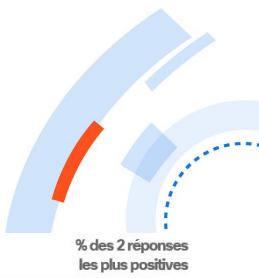
Source : Cisco

# Menaces sur le SI

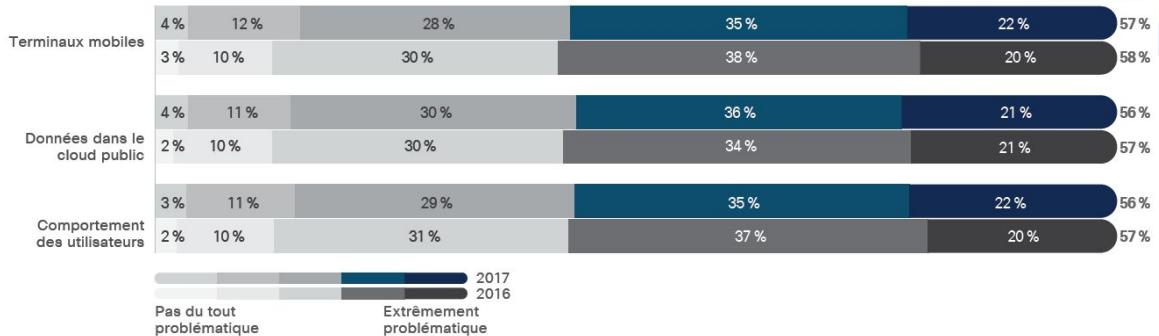
## Statistique

### Domaines les plus difficiles à défendre

Terminaux mobiles et données dans le cloud



% des 2 réponses les plus positives



Source : Cisco

---

# Menaces sur le SI

## Statistique

### Vulnérabilités / Attaques

Terminaux mobiles et données dans le cloud...

Vulnérabilités critiques				Activités d'attaque	
Mises à jour critiques Oracle, vulnérabilités OIT Plusieurs CVE	Vulnérabilités sur Open SSL Plusieurs CVE	Vulnérabilités sur Open SSL CVE-2017-3733	Vulnérabilités d'exécution du code à distance Apache Struts 2 CVE-2017-5638	Publication de Vault 7 par WikiLeaks Plusieurs CVE	Activité WannaCry MS17-010 Multiple CVEs
18 janvier	26 janvier	6 février	6 mars	7 mars	17 mai
Microsoft Windows Graphics CVE-2017-0108	Vulnérabilités du service Microsoft Windows Server Message Block pour exécuter du code arbitraire CVE-2017-0145	Vulnérabilités du protocole NTP (Network Time Protocol) Plusieurs CVE	Services IIS WebDav de Microsoft CVE-2017-7269	Campagnes internationales continues Operation Cloud Hopper	Divulgation par le Shadow Brokers Group des exploits d'Equation
14 mars	14 mars	21 mars	29 mars	6 avril	8 avril
Microsoft Office (attaque Dridex) CVE-2017-0199				Vulnérabilité du plug-in REST d'Apache Struts pour exécuter du code arbitraire pour transmettre du contenu XML CVE-2017-9805	Vulnérabilité de Microsoft .NET Framework pour exécuter du code arbitraire CVE-2017-8759
11 avril				6 septembre	12 septembre

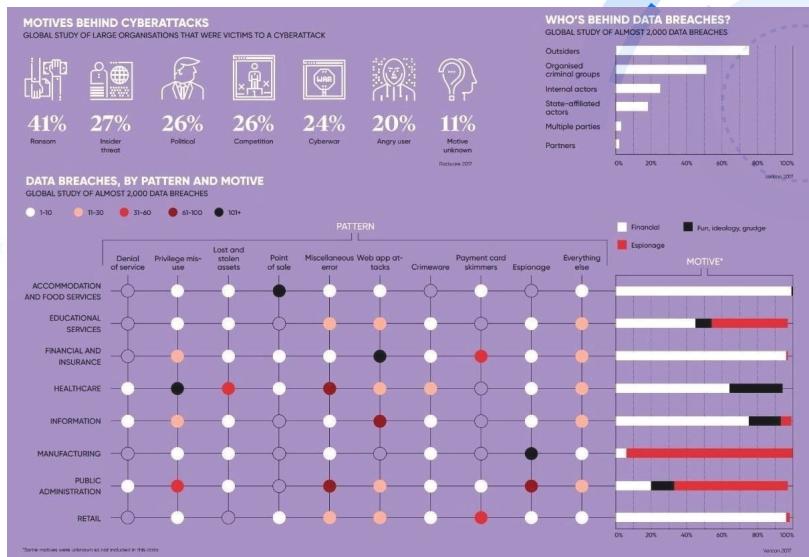
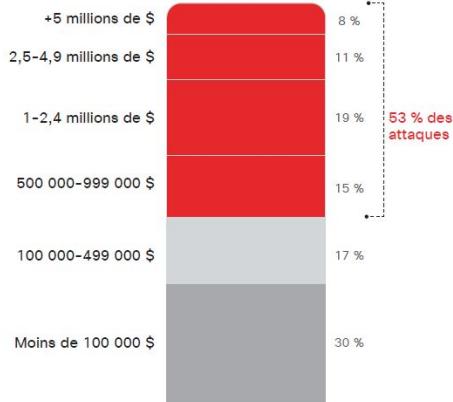
Source : Cisco

# Menaces sur le SI

## Statistique

### Motivations

Pertes pour les entreprises

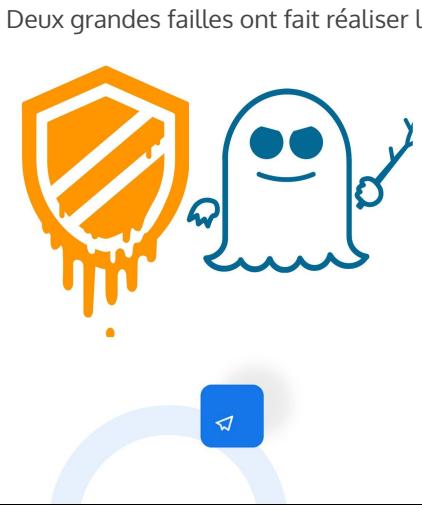


Source : Cisco

# Menaces sur le SI

## Statistique

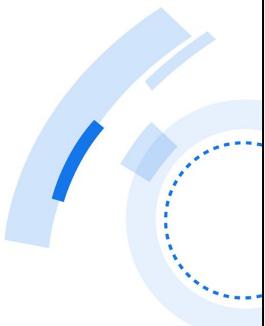
### Failles connues et 0 day



Deux grandes failles ont fait réaliser l'importance de la cyber sécurité

De nombreux sites sont disponibles pour vérifier les dernières 0 days sorties

- *DarkNet*
- *Oday.today*
- *TheRealDeal Market*
- *zerodayinitiative*



---

# Menaces sur le SI

## Statistique

### Les failles 0 days connue

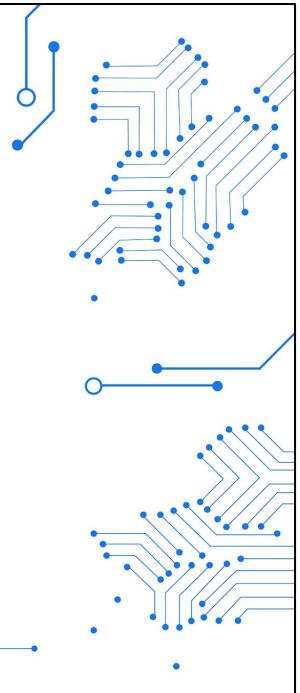
- Failles connues et célèbres
- Failles du moment



---

## 1. Menaces sur les SI

- 1) Les Modèles SI
- 2) Statistiques
- 3) Failles Connues et 0day
- 4) Étude des séquences d'exploitation**

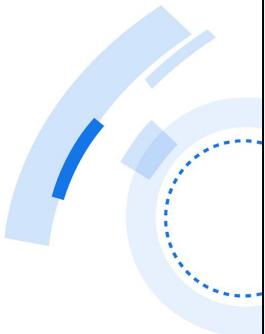


---

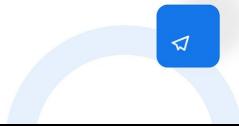
# Menaces sur le SI

## Étude des séquences d'exploitation

Rappel : Qu'est-ce qu'une séquence d'exploitation ?



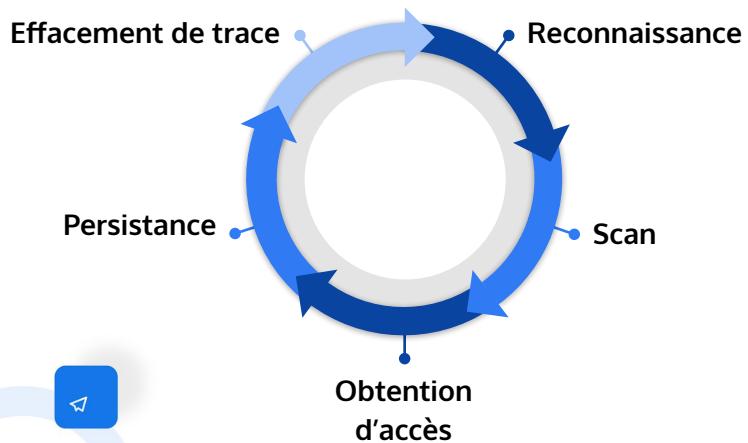
- Elles permettent à un attaquant de réussir son intrusion ainsi que de rester dans le parc informatique introduit.
- Le but est de rester le plus longtemps sans se faire remarquer.



---

# Menaces sur le SI

## Étude des séquences d'exploitation



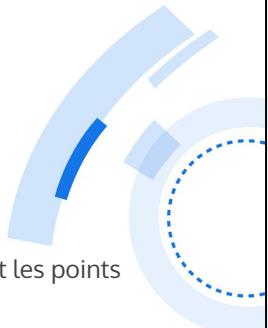
---

# Menaces sur le SI

## Étude des séquences d'exploitation

### Séquence 1 : Reconnaissance

- Cette première phase consiste en la récolte d'information sur la victime.
- Le but est de trouver les indications susceptibles de révéler les vulnérabilités et les points faibles du système.
- On y scan les pare-feu, les dispositifs de prévention des intrusions, les périmètres de sécurité (et même les comptes de médias sociaux).
  - *Dans cette phase les techniques utilisées sont l'OSINT, le scan, et le social engineering*



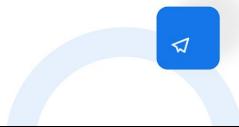
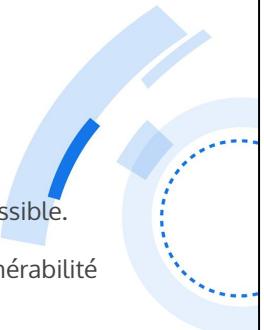
---

# Menaces sur le SI

## Étude des séquences d'exploitation

### Séquence 2 : scan et intrusion

- Cette séquence consiste à scanner la victime et obtenir le plus d'information possible.
- C'est ici que les failles de sécurité sont trouvées, ainsi que les potentiellement vulnérabilités à exploiter dans la phase suivante
  - *Dans cette phase les techniques utilisées sont du scan et du social engineering*



---

# Menaces sur le SI

## Étude des séquences d'exploitation

### Séquence 3 : Obtention d'accès et exploitation

- C'est dans cette phase que les informations récoltées lors deux premières phases servent.
- Toute les vulnérabilités sont exploitées afin d'obtenir un accès au réseau ou aux locaux de la victime.
- Les malware (y compris les ransomware, spyware et adware) peuvent être envoyés vers le système pour forcer l'entrée. C'est la phase de livraison.
  - *Dans cette phase les techniques utilisées sont toutes celles permettant l'intrusion forcée (Phishing, social engineering, exploit, site web infecté, etc)*



---

# Menaces sur le SI

## Étude des séquences d'exploitation

### Séquence 4 : Persistance

- Cette phase sert à maintenir son accès.
- S'infiltrer est une chose, réussir à garder l'accès aux données en est une autre. De multiple technologie existe pour détecter et bloquer, voir nettoyer les intrusions.
- Il est donc important de rester le plus discret possible et d'avoir les moyens de revenir si quelque chose nous fait partir du réseau.
  - *Dans cette phase les techniques utilisés sont de divulgation, de persistance, une bonne connaissance des lieux de persistance est nécessaire.*



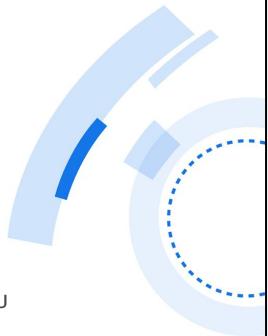
---

# Menaces sur le SI

## Étude des séquences d'exploitation

### Séquence 5 : Effacement des traces

- Cette phase consiste à rendre ses activités comme invisible.
- Nombreux système de détections sont basé sur les événements informatiques (log). Apprendre à les reconnaître et les effacer correctement est une tâche ardu mais essentiel.
- Il faut masquer la présence et les activités pour éviter toute détection et déjouer les investigations.
  - *Dans cette phase les techniques utilisées sont l'effacement de métadonnées, de timestamping, l'obfuscation, l'infection de SIEM*



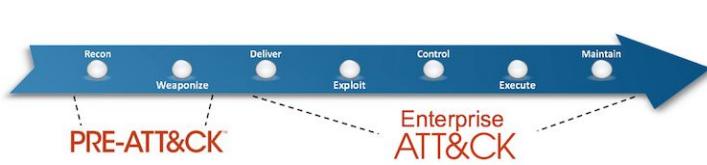
Source : <http://www.pentest-standard.org>

---

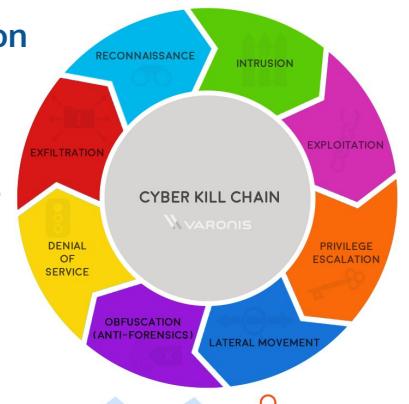
# Menaces sur le SI

## Étude des séquences d'exploitation

Les aides à la création d'une attaque



La Cyber Kill Chain, simple et efficace



Le MITRE PRE-ATT&CK et ATT&CK, détaillé et complet,  
véritable base de donnée à la création d'une attaque

Source : blog.varonis.com & attack.mitre.org

# Menaces sur le SI

## Étude des séquences d'exploitation

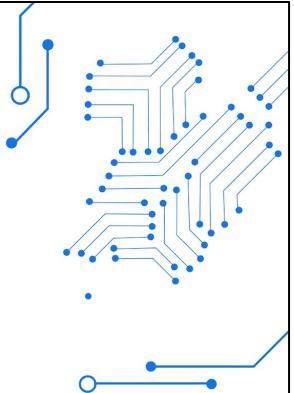


Tableau comparatif des différentes solutions

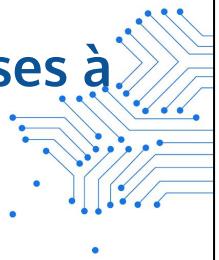
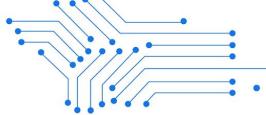
Séquences	MITRE PRE-ATT&CK et ATT&CK	Cyber Kill Chain
1 Reconnaissance	<ul style="list-style-type: none"> <li>Priority Definition Planning</li> <li>Priority Definition Direction</li> <li>Target Selection</li> </ul>	<ul style="list-style-type: none"> <li>Reconnaissance</li> </ul>
2 Scan	<ul style="list-style-type: none"> <li>Technical Weakness Identification</li> <li>People Weakness Identification</li> <li>Organizational Weakness Identification</li> <li>Adversary OPSEC</li> </ul>	<ul style="list-style-type: none"> <li>Reconnaissance</li> </ul>
3 Obtention d'accès	<ul style="list-style-type: none"> <li>Persona Development</li> <li>Build Capabilities</li> <li>Test Capabilities</li> </ul>	<ul style="list-style-type: none"> <li>Exploitation</li> <li>Escalade de privilège</li> <li>Mouvement latéral</li> <li>Déni de service</li> </ul>
4 Persistance	<ul style="list-style-type: none"> <li>Persistence</li> </ul>	
5 Effacement de trace	<ul style="list-style-type: none"> <li>Defense Evasion</li> </ul>	<ul style="list-style-type: none"> <li>Camouflage</li> </ul>

Source : blog.varonis.com & attack.mitre.org

----



## 2. Préparation et initialisation des phases à exploitation

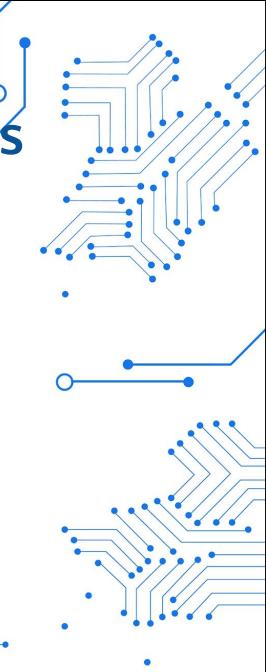


---

## 2. Préparation et initialisation des phases à exploitation

### 1) Terminologie

- 2) Présentation de différents framework et outils offensifs (Metasploit, Empire, Powershell)
- 3) Création de différents types de charges pour l'exploitation
- 4) Intégrer de nouveaux Exploits dans Metasploit
- 5) Différents types de connexions (Bind, Reverse)
- 6) Focus sur les stagers (TCP, SSH, DNS, HTTP, HTTPS)



---

# Des faiblesses à l'exploitation

## Terminologie

- **Exploit :**

Un Exploit est le Moyen par lequel un hacker ou pentester profite d'un défaut dans un système, une application ou un service, pour s'introduire dedans

- **Payload :**

Un Payload (charge utile) est le morceau du code que nous voulons que le système ciblé exécute

- **Listener :**

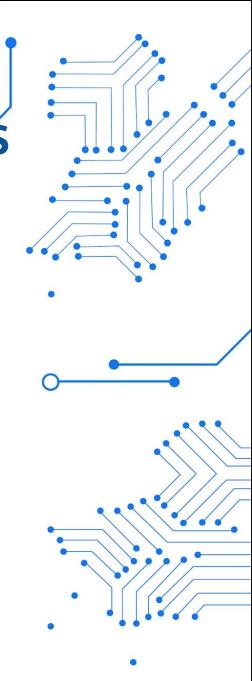
Un listener est un composant qui attend une connexion entrante sur la machine de l'attaquant



---

## 2. Préparation et initialisation des phases à exploitation

- 1) Terminologie
- 2) Présentation de différents framework et outils offensifs (Metasploit, Empire, Powershell)**
- 3) Création de différents types de charges pour l'exploitation
- 4) Intégrer de nouveaux Exploits dans Metasploit
- 5) Différents types de connexions (Bind, Reverse)
- 6) Focus sur les stagers (TCP, SSH, DNS, HTTP, HTTPS)



---

## Des faiblesses à l'exploitation

### Framework « Offensif »

- Dans le cadre de la semaine de sécurité offensive, une série d'outils sont nécessaires afin d'effectuer les opérations d'intrusion et comprendre les manipulations qui pourront être exécutées par de futurs attaquants
- Les outils sont nombreux et vous serez libre d'utiliser ceux de votre choix



## Des faiblesses à l'exploitation

### Framework « Offensif »

#### Metasploit

Metasploit Framework est un outil pour le développement et l'exécution d'Exploits (scripts permettant d'exploiter à son profit une vulnérabilité) contre une machine



## Des faiblesses à l'exploitation

### Framework « Offensif »

Empire

**Empire est un outil de post-exploitation entièrement réalisé en PowerShell et basé sur des communications cryptologiques sécurisées et une architecture flexible**

```
-----  
Empire: PowerShell post-exploitation agent | [Version]: 0.5.1-beta  
[Web]: https://www.PowerShellEmpire.com/ | [Twitter]: @harmj0y, @sixdub  
-----  
  
[EMPIRE]  
  
 91 modules currently loaded  
  1 listeners currently active  
  1 agents currently active  
  
(Empire) >
```



## Des faiblesses à l'exploitation

Powershell Only 😊

Framework « Offensif »



De plus-en-plus de nouvelles attaques utilisent PowerShell et des modules déjà présent nativement dans les systèmes Microsoft Windows, dans le but de détourner leur utilisation légitime

```
string $rawProtocolVersion = "HTTP/" + $response.ProtocolVersion
[int]$rawStatusCode = [int]$response.StatusCode
[string]$rawStatusDescription = $response.StatusDescription
$rawHeadersString = New-Object System.Text.StringBuilder
$rawHeadersCollection = $response.Headers
[int]$transferEncoding = 0
# This is used for Chunked Encoding
foreach($s in $rawHeaders)
{
    #We'll handle set-cookie and transfer-encoding later
    if($s -eq "Set-Cookie")
    {
        continue
    }
    if($s -eq "Transfer-Encoding")
    {
        $transferEncoding = 1
        continue
    }
    $rawHeadersString.AppendLine($s + ":" + $rawHeadersCollection[$s])
}
$rawHeadersString.ToString()
```



Expert(e) en Sécurité Digitale

# Des faiblesses à l'exploitation

## Framework « Offensif »

### Powershell : les bases

- **Afficher la configuration IP :**

*Get-NetIPConfiguration*

- **Lister les cartes réseau :**

*Get-NetAdapter*

- **Ping :**

*Test-NetConnection -ComputerName <computername>*

- **Tracert :**

*Test-NetConnection www.thomasmaurer.ch -TraceRoute*

- **Commandes Route :**

*Get-NetRoute -Protocol Local -DestinationPrefix <prefixip>\**

*Get-NetRoute -InterfaceAlias Wi-Fi*

*New-NetRoute -DestinationPrefix "<subnet>" -InterfaceAlias "Ethernet" -NextHop <ip>*



Expert(e) en Sécurité Digitale

# Des faiblesses à l'exploitation

## Framework « Offensif »

### Powershell : les bases



- **Nslookup :**  
*Resolve-DnsName <dnsname> -Type MX -Server <dnsserver>*
- **Netstat :**  
*Get-NetTCPConnection -State Established*
- **Scans de ports :**  
*Test-NetConnection -ComputerName <computername> -Port <port>*
- **Afficher la configuration du client SMB :**  
*Get-SmbClientConfiguration*
- **Afficher les connexions SMB :**  
*Get-SmbConnection*
- **Afficher les fichiers SMB ouverts :**  
*Get-SmbOpenFile*



---

## Des faiblesses à l'exploitation

Framework « Offensif »

Question

OS pour Pentest ?



—VS—



Expert(e) en Sécurité Digitale

## Des faiblesses à l'exploitation

L'offensive dans la pratique  
Metasploit pour l'exploitation



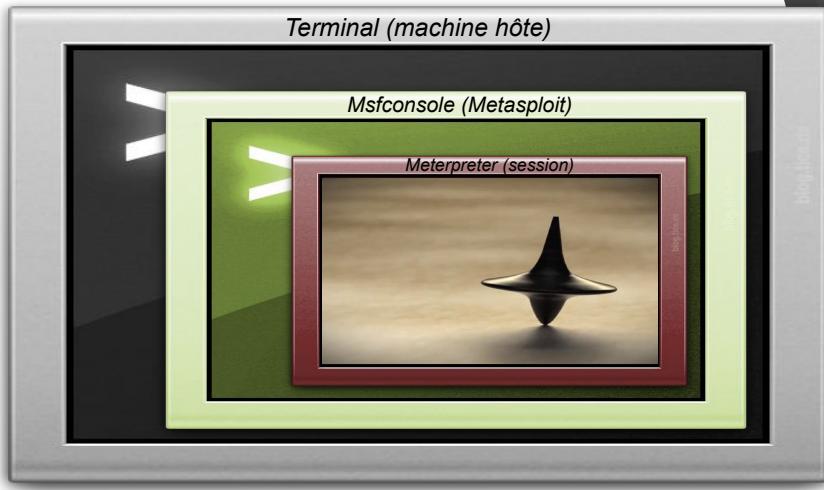
- Une fois les vulnérabilités identifiées, plusieurs possibilités s'offrent à vous quant à la manière de les exploiter
- Le Framework « Metasploit » permet comme vu précédemment une interaction assez forte avec les scanners de vulnérabilités, cependant toutes les vulnérabilités ne seront pas forcément exposées (erreur de conception d'infrastructure, etc...)



# Des faiblesses à l'exploitation

## L'offensive dans la pratique

Metasploit pour l'exploitation

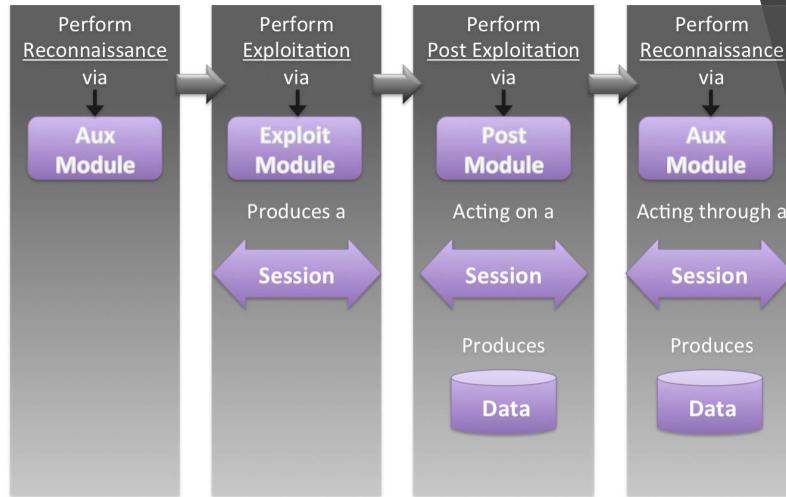


**ESD**

Expert(e) en Sécurité Digitale

## Des faiblesses à l'exploitation

### L'offensive dans la pratique Metasploit pour l'exploitation

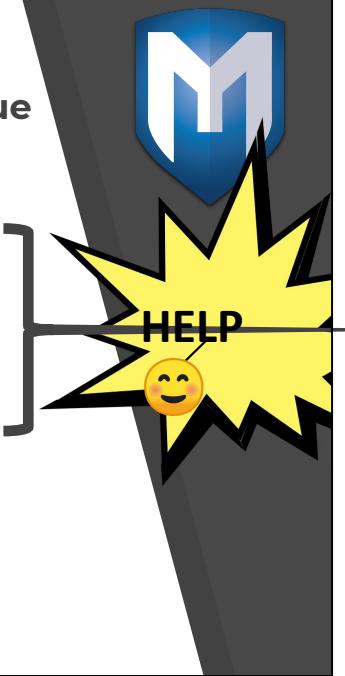


## Des faiblesses à l'exploitation

### L'offensive dans la pratique

Metasploit : commandes de base

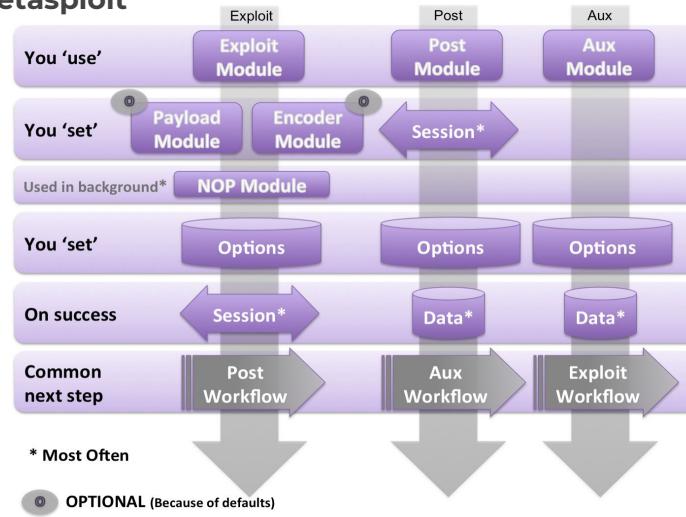
- **Use** : Sélectionner un module particulier
- **Set** : assigner une valeur à un objet du module
- **Show** : voir la liste de tous les modules/exploits/auxiliaires
- **Exploit** : lancer un exploit
- **Back** : revenir en arrière
- **Search** : permet de trouver un exploit/auxiliaire en particulier
- **Check** : vérifier si les cibles sont vulnérables à l'exploit chargé
- **Sessions** : Permet de lister ou établir une connexion avec les sessions actives



## Des faiblesses à l'exploitation

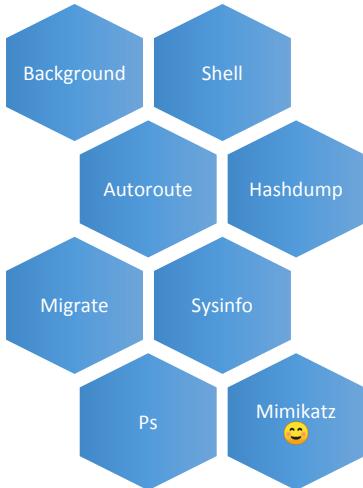
### Comprendre Metasploit

### L'offensive dans la pratique

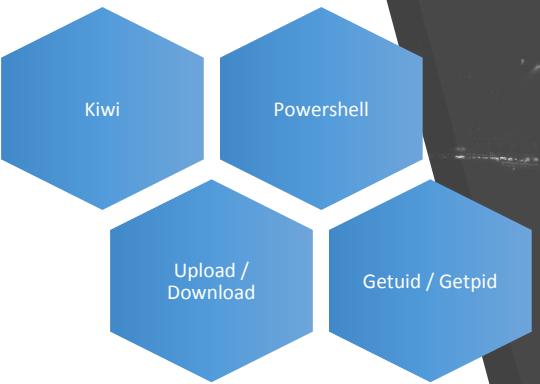


## Des faiblesses à l'exploitation

“Meterpreter”



## L'offensive dans la pratique

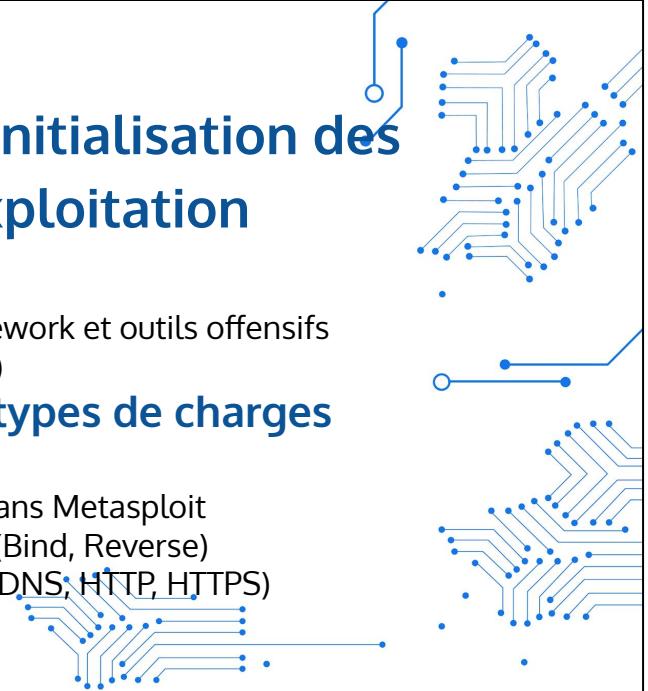


## 2. Préparation et initialisation des phases à exploitation

- 1) Terminologie
- 2) Présentation de différents framework et outils offensifs (Metasploit, Empire, Powershell)

### 3) Crédit de différents types de charges pour l'exploitation

- 4) Intégrer de nouveaux Exploits dans Metasploit
- 5) Différents types de connexions (Bind, Reverse)
- 6) Focus sur les stagers (TCP, SSH, DNS, HTTP, HTTPS)



---

# Des faiblesses à l'exploitation

## L'offensive dans la pratique

### Les utilitaires Metasploit

- Anciennement, Metasploit comprenait MSFPAYLOAD & MSFENCODE pour générer une grande variété de payloads et les chiffrer avec un grand nombre de méthodes d'encodage
- Depuis peu MSFVENOM est venu fusionner ces 2 solutions permettant de faire l'ensemble du travail avec un seul et même script

```
The usage of msfvenom is fairly straight forward:  
01. fahrenheit:msf3_banned$ ./msfvenom -h  
02. Usage: ./msfvenom [options] <var=val>  
03.  
04. Options:  
05.   -p, --payload  [payload]      Payload to use. Specify a '--' or stdio to use custom payloads  
06.   -l, --list     [module_type]  List a module type example: payloads, encoders, nops, all  
07.   -n, --nopsled  [length]       Prepend a nopsled of [length] size on to the payload  
08.   -f, --format   [format]      Format to output results in: raw, ruby, rb, perl, pl, c, js_be, js_le, java, dll, exe, exe-small, elf, macho, vba, vbs, loop-vbs, asp, war  
09.   -e, --encoder  [encoder]    The encoder to use  
10.   -a, --arch    [architecture] The architecture to use  
11.   --platform  [platform]    The platform of the payload  
12.   -s, --space   [length]      The maximum size of the resulting payload  
13.   -b, --bad-chars [list]      The list of characters to avoid example: '\x00\xff'  
14.   -i, --iterations [count]  The number of times to encode the payload  
15.   -x, --template  [path]     Specify a custom executable file to use as a template  
16.   -k, --keep      Preserve the template behavior and inject the payload as a new thread  
17.   -h, --help      Show this message
```



Expert(e) en Sécurité Digitale



# Des faiblesses à l'exploitation

## MSFVENOM

```
msf > msfvenom
[*] exec: msfvenom root 1039 Jun 29 19:30 41224.rb
[*] exec: msfvenom root 4096 May 15 13:35 MS17-010-master
Error: No options
Usage: ./msfvenom [options] <var=val>
Also a replacement for msfpayload and msfencode.
Usage: /usr/bin/msfvenom [options] <var=val>

Options:
  -p, --payload      <payload>    Payload to use. Specify a '--' or stdin to
o use custom payloads
  -l, --list          <main>       List the payload's standard options
  -e, --encoder      <encoder>    The encoder to use
  -a, --arch          <arch>       The architecture to use
  -i, --iterations   <length>     Prepend a nopsled of [length] size on to
the payload
  -f, --format        <format>     Output format (use --help-formats for a
list)
  --help-formats     <main>       List available formats
  -e, --encoder      <encoder>    The encoder to use
  -a, --arch          <arch>       The architecture to use
  -i, --iterations   <length>     List module type. Options are: payload
  -p, --platform     <platform>   The platform of the payload
  --help-platforms   <main>       List available platforms
  -s, --space         <length>     The maximum size of the resulting payload
```

- **-p** désigne la charge que nous voulons utiliser
- **-e** désigne l'encodeur que nous voulons utiliser
- **-i** désigne le nombre d'itérations avec lesquelles coder la charge-a désigne l'architecture que nous voulons utiliser (par défaut x86)
- **-s** désigne la taille maximale de la charge utile
- **-x** désigne un fichier exécutable personnalisé à utiliser comme modèle



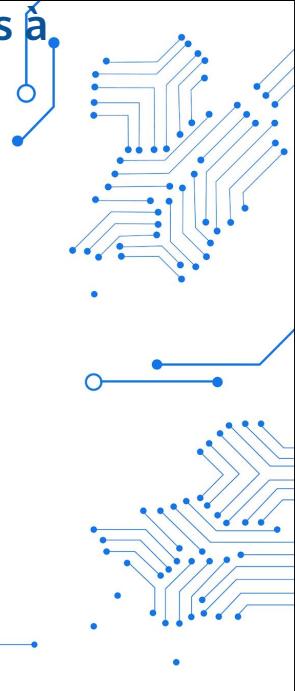
Expert(e) en Sécurité Digitale

## 2. Préparation et initialisation des phases à exploitation

- 1) Terminologie
- 2) Présentation de différents framework et outils offensifs (Metasploit, Empire, Powershell)
- 3) Création de différents types de charges pour l'exploitation
- 4) Intégrer de nouveaux Exploits dans Metasploit**
- 5) Différents types de connexions (Bind, Reverse)
- 6) Focus sur les stagers (TCP, SSH, DNS, HTTP, HTTPS)



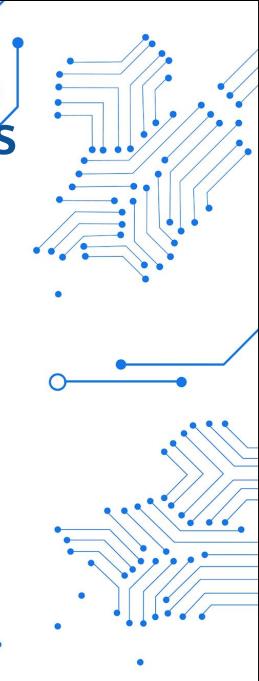
---



Exemple d'utilisation : extraction du processus lsass

## 2. Préparation et initialisation des phases à exploitation

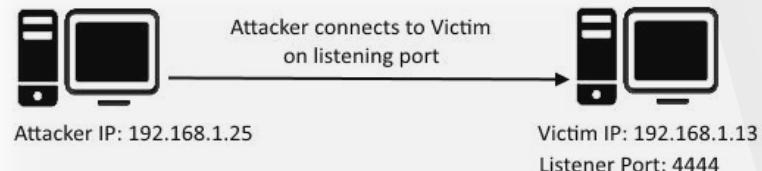
- 1) Terminologie
- 2) Présentation de différents framework et outils offensifs (Metasploit, Empire, Powershell)
- 3) Création de différents types de charges pour l'exploitation
- 4) Intégrer de nouveaux Exploits dans Metasploit
- 5) Différents types de connexions (Bind, Reverse)**
- 6) Focus sur les stagers (TCP, SSH, DNS, HTTP, HTTPS)



---

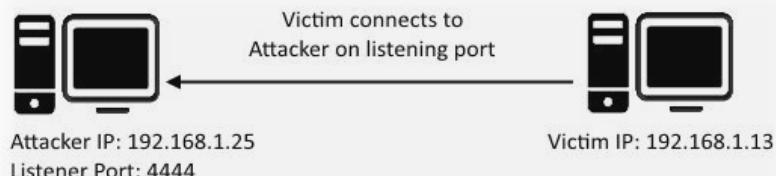
# Des faiblesses à l'exploitation

## Terminologie



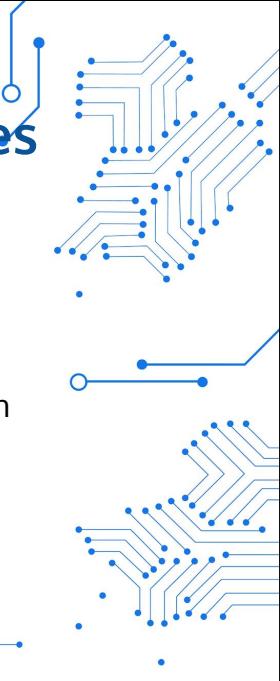
### Types de Shells

#### Reverse / Bind

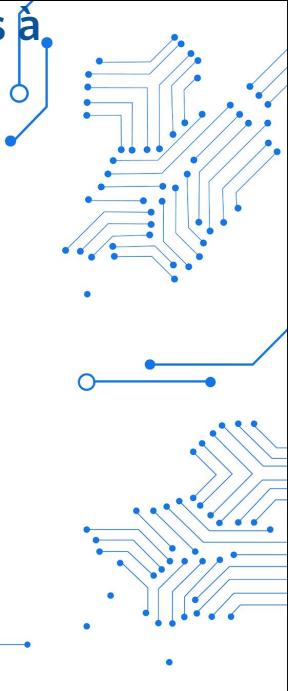


## 2. Préparation et initialisation des phases à exploitation

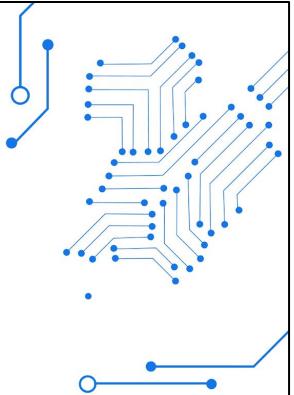
- 1) Terminologie
- 2) Présentation de différents framework et outils offensifs (Metasploit, Empire, Powershell)
- 3) Création de différents types de charges pour l'exploitation
- 4) Intégrer de nouveaux Exploits dans Metasploit
- 5) Différents types de connexions (Bind, Reverse)
- 6) Focus sur les stagers (TCP, SSH, DNS, HTTP, HTTPS)**



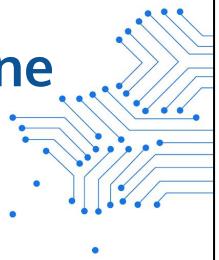
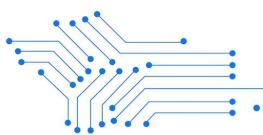
---



Exemple d'utilisation : extraction du processus lsass



### 3. Positionnement - Attaquant Externe

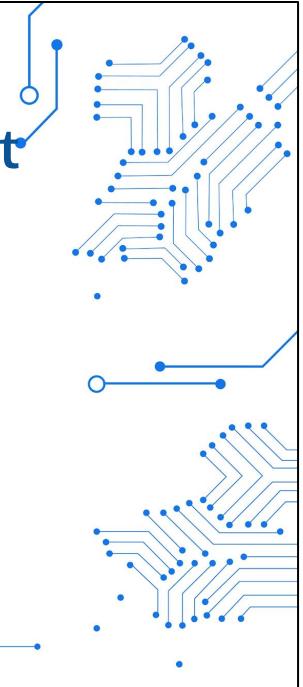


---

### 3. Positionnement - Attaquant Externe

#### 1) Introduction sur les attaques externes

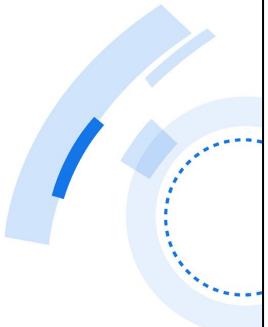
- 2) Social Engineering
- 3) Fichier malicieux
- 4) Recherche d'identifiants sur les bases de "Leak"
- 5) Les attaques Cloud
- 6) Étude et exploitation réseaux Wi-Fi environnant



---

# Positionnement - Attaquant Externe

## Introduction sur les attaques externe



- Une attaque externe est effectuée lorsque l'accès au réseau interne ou aux locaux interne n'est pas disponible.
- Il est possible d'obtenir des informations publiques comme privées.
- Ce n'est pas parce qu'il n'y a pas d'accès interne qu'il n'est pas possible d'obtenir des informations confidentielles.



La rubber ducky, toujours aussi efficace pour les attaques externes

---

# Introduction sur les attaques externes

## Introduction sur les attaques externe

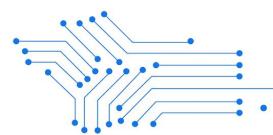
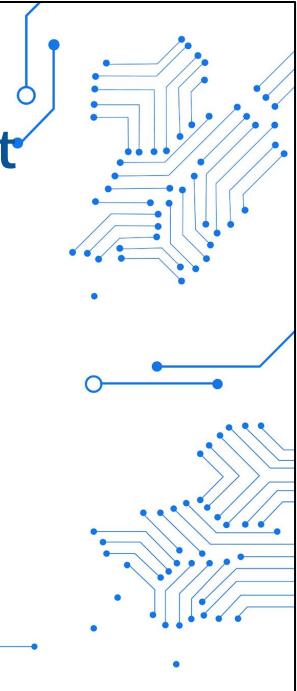
### Les informations intéressantes

01	Profils	<ul style="list-style-type: none"><li>• Employés faillible</li><li>• Employés mécontent</li><li>• Ancien employés ayant gardé des accès</li></ul>
02	Informations sur la victime	<ul style="list-style-type: none"><li>• Réputation numérique</li><li>• Adresses mails</li><li>• Informations DNS</li></ul>
03	Erreurs de configuration	<ul style="list-style-type: none"><li>• Données accessibles publiquement</li><li>• Services publics avec des identifiants par défaut</li></ul>
04	Accès interne	<ul style="list-style-type: none"><li>• Parc informatique</li><li>• Locaux privé</li></ul>
05	Failles	<ul style="list-style-type: none"><li>• Humaines</li><li>• Technologiques</li><li>• Physiques</li></ul>

---

### 3. Positionnement - Attaquant Externe

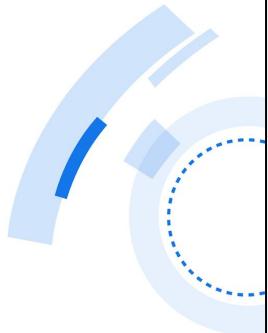
- 1) Introduction sur les attaques externes
- 2) Social Engineering**
- 3) Fichier malicieux (Macros Office, PDF, HTML, APK)
- 4) Recherche d'identifiants sur les bases de "Leak"
- 5) Les attaques Cloud (Office 365, Azure, AWS)
- 6) Étude et exploitation réseaux Wi-Fi environnant



---

# Social Engineering

## Technique de phishing



### Le harponnage sentimental

- La compassion est un des sentiments les plus simples à exploiter.
- Qui n'aiderait pas quelqu'un dans le besoin ou quelqu'un de malade ? Imaginez qu'en plus cette personne soit quelqu'un de **proche** ?
  - **Une attaque alliant sentiment et usurpation d'identité est très efficace**

 @outlook.com>  
Ven 19/07/2019 12:50  
Vous ↗

Merci pour ta réponse cela me soulage de te parler, excuse-moi de t'importuner avec mes affaires personnelles, mais actuellement pour des raisons de santé, je ne peux me déplacer car j'ai récemment été diagnostiquée d'un cancer de la prostate.

Tu es l'unique personne que j'en ai informé à ce jour et je tiens à ce que ceci reste confidentiel.  
Au sujet du service dont j'ai besoin vu que je ne peux pas me déplacer, je souhaite que tu fasses une démarche pour moi il me faut urgentement recharger ma carte prépayée.

↪ ⏪ → ...

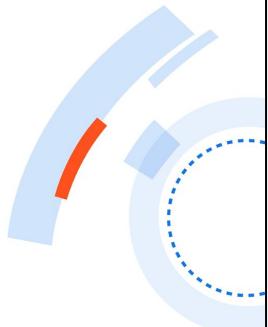
----

# Social Engineering

## Technique de phishing

### La pression

- Une des attaques ayant amassé le plus d'argent ces dernières années joue sur la **pression**.



#### L'attaque au président :

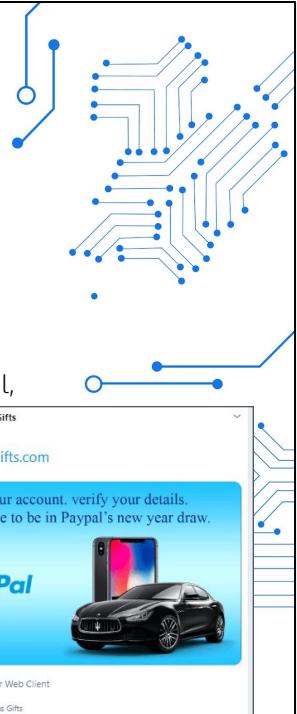
- appelez une entreprise en se faisant passer pour une autorité supérieur (DG, DAF, Actionnaire, etc)
- Mettez une forte pression très rapidement afin que l'interlocuteur ne prenne pas le temps de vérifier ou d'effectuer les procédures ("Je suis avec un client actuellement", "Vous refusez mes ordres ?", "Il me faut absolument cette information tout de suite")



---

# Social Engineering

## Technique de phishing



### La bonne occasion

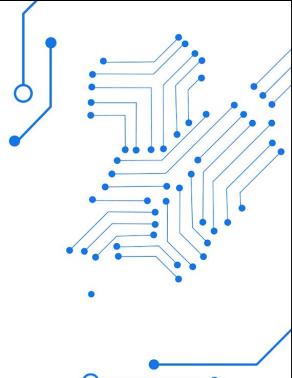
- Une technique encore très efficace consiste à proposer une **offre alléchante** afin que l'on clique ou que l'on effectue une suite d'action qui permet de voler de l'argent, obtenir l'accès à un réseau, avoir plus d'information sur la personne.
- C'est une technique qui peut passer par plein de support, E-mail, pub, oral, réseaux sociaux, etc
- **La force de cette technique réside dans l'adaptation au moment**  
*(Exemple : Sortie du nouvel Iphone = Proposer un Iphone gratuit ou en avant-première)*



----

# Social Engineering

## Technique de phishing



### Attaques ciblées

- La technique la plus efficace reste la ciblée.
- Elle consiste à créer une campagne de phishing avec des **informations précises** sur la victime (Nom, prénom, âge, fonction, évènement passé, anecdote uniquement connu de la victime).
- Exemple typique d'un mail de phishing ciblé.
- On y retrouve :
  - *Le nom et prénom de la victime*
  - *Une information personnelle*
  - *Une offre alléchante*
  - *Un lien cliquable*

Proposition après tes études de maquillage Boîte de réception ✎

**Antoine Dès Lunès** <adunes@cinemakeup.com>

À moi ✉ 17:52 (il y a 0 minute) ⭐ ➔

Bonjour Astrid Berthelot,

J'ai vu ton travail de maquilleuse sur Instagram, je trouve ça très impressionnant !

Et j'aimerais t'addrer dans ta carrière car je pense que tu peux vraiment aller très loin.

Je pourrai t'offrir une offre d'emploi après la fin de tes études dans mon entreprise de maquillage pour des production cinéma. C'est une occasion pour toi de faire tes preuves et pour nous de recruter une des artistes les plus doué de sa promotion.

Que pense-tu de notre offre ? Si elle t'intéresse, je te laisse déposer ton CV ainsi que ton book sur ce lien : <https://www.cinemakeup.com/candidat&q=Eb5ea078GfFe>

Cordialement,

Antoine dès Lunès,  
Direction des Ressources Humaines  
Ciné Maquillage

MERCII BEAUCOUP ! Merci. Je vous remercie pour votre proposition.

----

# Social Engineering

## Clone de page d'authentification



### En quoi ça consiste ?

- Une des techniques courante consiste à envoyer un lien cliquable redirigeant vers une fausse page d'authentification
  - Le but est que la victime rentre ses identifiants**

A screenshot of a web browser showing a cloned Instagram login page. The URL in the address bar is 'gadwat.com/?j3wf//INCuqV4albsB8U6/inst/en/?i=1265352'. The page itself is a copy of the official Instagram login interface, featuring fields for 'Phone number, username, or email' and 'Password', and a 'Log in' button. Below these are links for 'Forgot password?' and 'Don't have an account? Sign up'. At the bottom, there are download links for the App Store, Google Play, and Microsoft.

Page de connexion Instagram malicieuse

A screenshot of a web browser showing the official Instagram login page at 'https://www.instagram.com/accounts/login/?hl=en'. The layout is identical to the fake version, with fields for 'Phone number, username, or email' and 'Password', and a 'Log in' button. Below are 'Forgot password?' and 'Sign up' links. At the bottom, there are download links for the App Store, Google Play, and Microsoft.

Page de connexion Instagram légitime

----

# Social Engineering

## Clone de page d'authentification

Plusieurs technique possible - La redirection

- Afin de rester le plus discret possible, il faut chercher à faire croire que le vol d'identifiant n'est pas eue lieu.

- Pour ceci, une fois que les identifiant ont été entrés, il faut rediriger la connexion vers le site légitime.

- ***La première technique consiste à rediriger les identifiants vers le site légitime afin de la connexion***



---

# Social Engineering

## Clone de page d'authentification

Plusieurs technique possible - L'erreur

- La seconde technique consiste à rediriger la victime sur la page d'erreur de connexion du site légitime afin de lui faire entrée une deuxième fois ses identifiants.
- Cette technique permet de ne pas diffuser les identifiants sur internet. Très utile lorsque l'attaquant à un accès interne.*
- Cela permet ne pas alerter les potentiels pare-feu, IDS/IPS ou Proxy qui surveillent les communications vers l'extérieur.*



Instagram

Phone number, username, or email

Password

Forgot password?

Log In

OR

Log in with Facebook

Sorry, your password was incorrect. Please double-check your password.

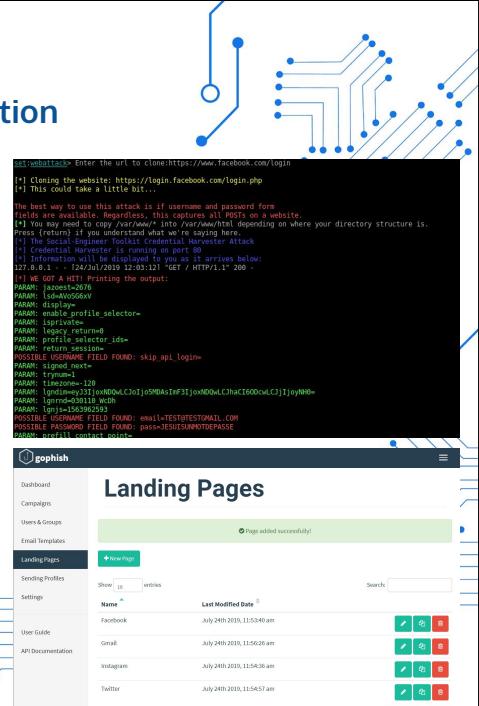
---

# Social Engineering

## Clone de page d'authentification

### Quelque outils

- SeToolkit
  - Outils spécialisé dans le Social Engineering.
- Gophish
  - Framework de phishing spécialisé dans les campagnes de phishing



The image consists of two screenshots. The top screenshot shows terminal output for a credential harvester attack on Facebook. It includes command-line usage, a warning about capturing all POSTs, and a log of a successful login attempt. The bottom screenshot shows the Gophish application's 'Landing Pages' section, displaying a list of cloned landing pages for various platforms like Facebook, Gmail, Instagram, and Twitter.

Name	Last Modified Date
Facebook	July 24th 2019, 11:52:40 am
Gmail	July 24th 2019, 11:56:26 am
Instagram	July 24th 2019, 11:56:36 am
Twitter	July 24th 2019, 11:56:57 am

### SeToolkit

Il est possible de cloner des pages via "Social Engineering attack/Website attack vector/Credential harvester attack/Site cloner"

{1 - 2 - 3 - 2}

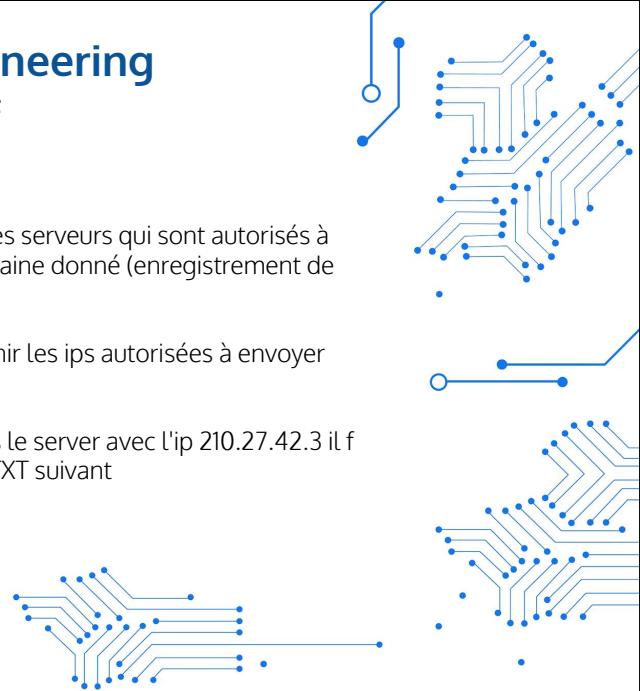
### Gophish

Il est possible de cloner des pages via l'option "Landing pages"

### Qu'est-ce que c'est ?

- C'est une norme qui permet d'identifier les serveurs qui sont autorisés à envoyer des emails pour un nom de domaine donné (enregistrement de type txt:spf au sein des DNS).
  - Cet enregistrement permet de définir les ips autorisées à envoyer des emails avec votre domaine.
- Par exemple si on envoit les email depuis le server avec l'ip 210.27.42.3 il faudra configurer l'enregistrement TXT suivant

**v=spf1 a mx ip4:210.27.42.3 ~all**



Source : www.grafikart.fr

### Exemple d'argument :

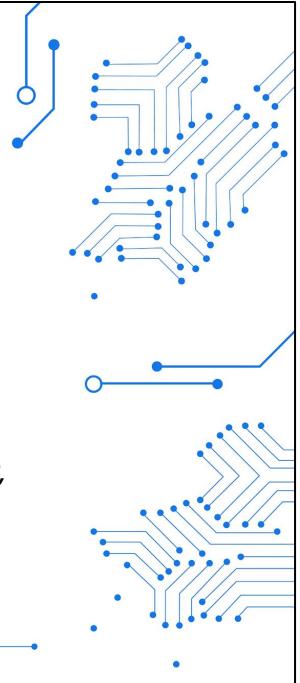
- **a** indique les noms de domaines autorisé à envoyer les emails de ce domaine (vide = domaine en cours)
- **mx** permet d'indiquer les serveurs mx autorisés à envoyer les emails de ce domaine (vide = domaine en cours)
- **ip4** permet de préciser les ip (format v4) autorisé à envoyer les emails de ce domaine
- **include** peut être utilisé pour copier le spf d'un autre domaine (par exemple include:un\_autre\_domaine.fr)

# Social Engineering

## SPF

### En quoi c'est faillible ?

- Le phishing utilisent souvent des adresses et domaines falsifiés pour envoyer des mails.
- Si le domaine à une bonne réputation en matière d'envoi, un spammeur peut tenter d'envoyer des courriers électroniques de ce domaine afin de s'affranchir de sa réputation auprès des FAI
- ***Le SPF étant optionnel, peu d'entreprise l'ont mis en place. En 2018, 40% des entreprises ont le SPF d'activé***



# Social Engineering

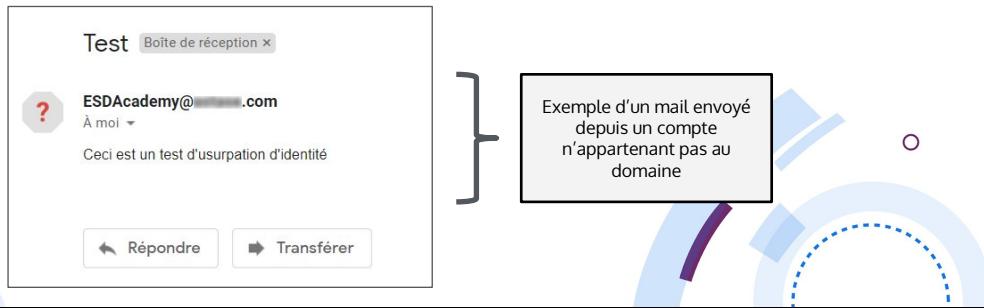
## SPF

### Les 3 cas les plus communs

- Le SPF n'est pas activé

Test	Result
! SPF Record Published	No SPF Record found
✓ DNS Record Published	DNS Record found

- *Risques : Usurpation d'identité, vol de réputation numérique*



# Social Engineering

## SPF

### Les 3 cas les plus communs

- Le SPF est activé et bien configuré

spf:_spf.google.com		Find Problems	Solve Email Delivery Problems	
Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	_netblocks.google.com	Pass	The specified domain is searched for an 'allow'.
+	include	_netblocks2.google.com	Pass	The specified domain is searched for an 'allow'.
+	include	_netblocks3.google.com	Pass	The specified domain is searched for an 'allow'.
-	all		SoftFail	Always matches. It goes at the end of your record.

- Risques : Aucun risque d'attaque via le SPF



Un mail qui tente d'usurper l'identité sur un domaine avec un SPF bien configuré sera directement taggé comme "Indésirable"

Si le SPF est configuré avec un ~all (SoftFail), le mail sera taggé "indésirable"

Si le SPF est configuré avec un -all (HardFail) le mail sera jeté

# Social Engineering

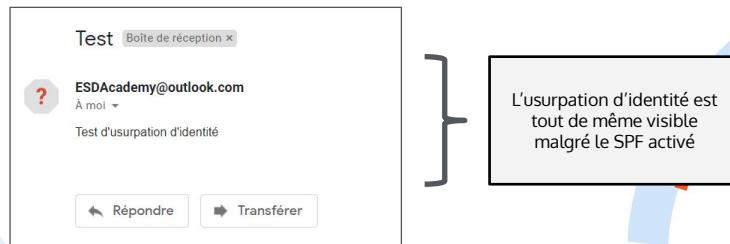
## SPF

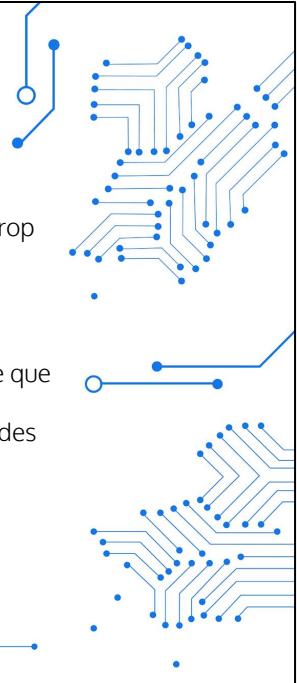
### Les 3 cas les plus communs

- Le SPF est activé mais mal configuré

spf.outlook.com   Solve Email Delivery Problems					
Prefix	Type	Value	PrefixDesc	Description	
v	version	spf1	Pass	The SPF record version	
+	include	spf-a.outlook.com	Pass	The specified domain is searched for an 'allow'.	
+	include	spf-b.outlook.com	Pass	The specified domain is searched for an 'allow'.	
+	ip4	157.55.9.128/25	Pass	Match if IP is in the given range	
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.	
+	include	spf-a.hotmail.com	Pass	The specified domain is searched for an 'allow'.	
+	include	_spf.ssg.b.microsoft.com	Pass	The specified domain is searched for an 'allow'.	
-	include	_spf.ssg.c.microsoft.com	Pass	The specified domain is searched for an 'allow'.	
-	all		SoftFail	Always matches. It goes at the end of your record.	

- Risques : Usurpation d'identité, vol de réputation numérique





### Exemple de mauvaise configuration

- Les mauvaises configurations du SPF viennent souvent du champ d'autorisation trop large
  - Les arguments potentiellement faillibles :
- **ip4** : Une erreur de saisie du CIDR peut autoriser une plage d'IP bien plus grande que voulue (Exemple : /2 à la place de /20)
- **include** : En incluant les autorisations SPF d'un autre domaine, il est possible qu'un des serveurs soit trop ouvert ou que leur configuration SPF soit mal faite ou erronée.
- **?all** : Ce paramètre indique que d'autres serveurs peuvent faire des envois.
- **exist** : Mal configuré il permet d'autoriser tout envoi sous le nom de domaine
- **+all** : Ce paramètre indique que tout est autorisé.
- **ptr** : Cet argument autorise tous les sous domaines

<https://www.socketlabs.com/blog/best-practices-sender-policy-framework-spf/>

## Pour aller plus loin

- L'e-mail étant un protocole ayant besoin d'être patché par construction, plusieurs sécurités se sont rajouté au fil du temps.
- **DKIM :**
  - Avec les infrastructures mutualisés, plusieurs personnes peuvent se trouver sur une même IP. Le DKIM ajoute un principe de clé asymétrique pour s'assurer que le mail est bien intégré et que l'expéditeur à l'autorisation d'envoyer des mails à ce serveur.
- *Les conséquences d'un DKIM inactif sont une usurpation d'identité possible malgré un SPF bien configuré.*
- *Le SPF et le DKIM sont deux protocoles qui vont de paire. L'un est rarement activé sans l'autre mais cela peut arriver.*



[https://www.youtube.com/watch?v=\\_6GwqzuYGus](https://www.youtube.com/watch?v=_6GwqzuYGus)

<https://blog.devensys.com/ameliorer-la-securite-des-emails/>

DKIM s'implémente directement dans le domaine de messagerie comme une paire de clé asymétrique.

La signature se trouve dans l'entête du mail

ex :

*DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;  
t=1476054397;  
s=m1; d=e.renpath.com; i=@e.renpath.com;  
h=Date:From:To:Subject:MIME-Version:Content-Type;  
bh=Rm+zVdTj9mQiUHxMpu+O9d9OuV3cOTuaNWHONtEXYo0=;  
b=oGVqGJKcS8KZ+YR8+AKzGKg2t1qpwKFXpg6jO3eU/MvQnl9hRpn9NYSR1v  
V20MSYvJP9ZBiG7hftTHxYUwrP/Ur4Gt4a6bzt6Q6KETOiUrksD1Jnvwt7YG/cw  
GqGfjfmuYU +/fk3oboothCsnvOl79hHrR8q/a0eCLnkL5BC7L1g=*

1 - Générer une paire de clé

2 - Placer un TXT sur son domaine avec la clé publique

3 - Générer et sauver la signature

# Social Engineering

## SPF

### Pour aller plus loin

- Suite à la sortie du DKIM et du SPF, il a été trouvé une nouvelle faille qui consiste à forger un mail en changeant le champ "from" pour se faire passer pour légitime. Un protocole a donc été inventé pour patcher les deux protocoles
  - **DMARC :**
    - Son principe est de s'assurer que le champ "from" et le champ "mailfrom" soit alignés. S'ils ne le sont pas, DMARC va vérifier le DKIM et SPF des deux contenus.
    - Le DMARC permet aussi de choisir où placer les mails frauduleux. Quarantaine ou suppression.
-  - ***Les conséquences d'un DMARC inactif sont une usurpation d'identité possible malgré un SPF ou un DKIM bien configuré.***



Un DMARC est un txt au format v=DMARCv1; <ARGUMENTS>

exemple :

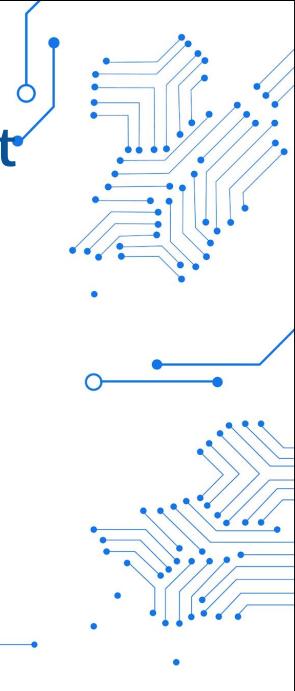
v=DMARC1; p=none; fo=1;

rua=mailto:dmarc\_agg@auth.returnpath.net,mailto:dmarc\_aggdata@exampledestination.com;

ruf=mailto:dmarc\_afrr@auth.returnpath.net,mailto:dmarc\_forensic@exampledestination.com

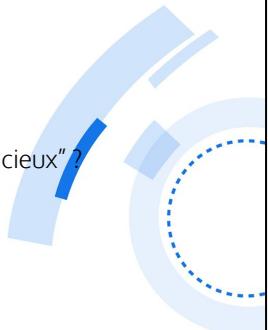
## 3. Positionnement - Attaquant Externe

- 1) Introduction sur les attaques externes
- 2) Social Engineering
- 3) Fichier malicieux**
- 4) Recherche d'identifiants sur les bases de "Leak"
- 5) Les attaques Cloud (Office 365, Azure, AWS)
- 6) Étude et exploitation réseaux Wi-Fi environnant



# Fichier malicieux

## Introduction



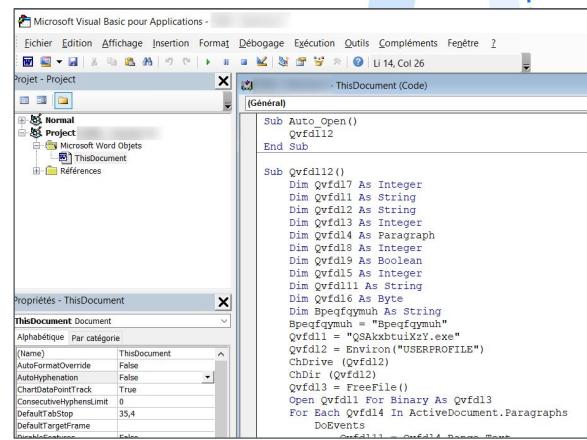
- A quoi serve les fichiers malicieux ?
    - obtenir un accès
    - collecter des identifiants, mot de passe
  - Dans quel contexte les utiliser ?
    - Dans le cadre d'un phishing
    - Attaque de social engineering
  - Qu'est-ce qu'un "fichier malicieux" ?
    - *Fichier macro*
    - *pdf*
    - *apk*
    - *hta*
    - *ps1*
    - *py*
    - *exe*
- ***Ce n'est pas car l'extension est connue qu'elle n'est pas exploitable, bien au contraire.***



# Fichier malicieux

## Macros office

- C'est l'extension la plus courante lors d'une attaque.
- Elle à l'avantage d'être :
  - Simple à mettre en place
  - Exécutable facilement par tous
  - Rapide et discrète
  - Codage simple (vba)
  - Pack office très implanté dans les entreprises
- Et à très peu de désavantage :
  - Nécessite le pack office
  - Requiert une action utilisateur
  - AMSI



The screenshot shows the Microsoft Visual Basic pour Applications interface. On the left, the Project Explorer shows a 'Project' node with 'Normal Project' expanded, containing 'Microsoft Word Objects' and 'ThisDocument'. The Properties window on the left displays settings for 'ThisDocument' such as 'AutoFormatOverride' set to 'False' and 'ConsecutiveHyphenLimit' set to '0'. The main code editor window contains the following VBA code:

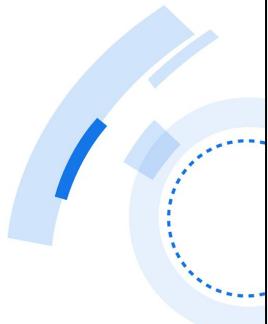
```

Sub Auto_Open()
    Qvfd112
End Sub

Sub Qvfd112()
    Dim Qvfd17 As Integer
    Dim Qvfd18 As String
    Dim Qvfd19 As Long
    Dim Qvfd13 As Integer
    Dim Qvfd14 As Paragraph
    Dim Qvfd18 As Integer
    Dim Qvfd19 As Boolean
    Dim Qvfd15 As Integer
    Dim Qvfd11 As String
    Dim Qvfd16 As Byte
    Dim Bpeqfymuh As String
    Bpeqfymuh = "Bpeqfymuh"
    Qvfd11 = "Q3AkxbtuiXzV.exe"
    Qvfd12 = Execution("USERPROFILE")
    Chdir (Qvfd12)
    Qvfd13 = FreeFile()
    Open Qvfd11 For Binary As Qvfd13
    For Each Qvfd14 In ActiveDocument.Paragraphs
        DoEvents
        Qvfd11 = Qvfd14.Range.Text
    Next Qvfd14
End Sub

```

## Fichier malicieux pdf



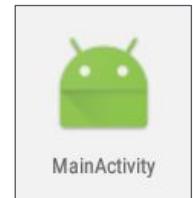
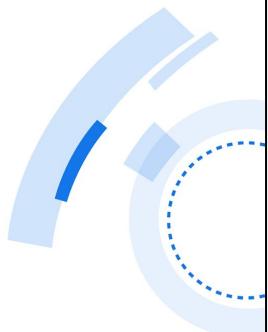
- Ce format est aussi très utilisé aussi
- Il a l'avantage d'être :
  - Facilement à mettre en place (msfvenom)
  - Discret
  - Rapide
  - Facilement exécutable par l'utilisateur
- En contrepartie :
  - Il faut que le lecteur soit dans une version faillible
  - Que la charge soit adapté à cette version du lecteur pdf



	AcroRd32.exe	2076	33.66	Adobe Reader 8.0	Adobe Systems Incorporated
	calc.exe	2108	1.90	Application Calculatrice de ...	Microsoft Corporation

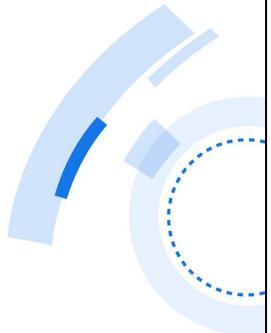
## Fichier malicieux apk

- Les fichiers apk sont utilisé pour installer des applications sous android.
- C'est aussi un format de fichier assez intéressant car :
  - Facile à créer (Framework disponible)
  - Relativement discret (< android 4.0)
  - Peut obtenir des droits très élevé facilement
  - Téléphonie mobile très utilisé en entreprise
  - BYOD courant
  - Facile à mettre en ligne (25€ la création de compte développeur play store)
- En contrepartie :
  - L'utilisateur doit être un minimum technicien pour installer un apk
  - Le google play store de plus en plus alerte aux applications frauduleuse



25€ la création de compte développeur play store VS 80€/an pour le apple store

## Fichier malicieux hta



- C'est l'extension
- Elles sont peu utilisé mais encore très efficace de nos jours pour :
  - Facile à mettre en place
  - Exécution simple
  - Permet de contourner un filtrage par liste blanche
- En contrepartie :
  - Il faut une action de la part d'un utilisateur
  - Rendre un hta FUD requiert de compétences de développement un peu plus poussé



- ***Cette extension est excellente utilisée avec une attaque ARP pour rediriger un flux (ettercap)***



## Fichier malicieux ps1



- Les scripts ps1 sont une des extensions les plus puissantes pour générer des applications malveillantes car ils utilisent PowerShell
- Cela à l'avantage de :
  - être nativement adapté aux plateformes microsoft
  - Relativement facile à écrire
  - Avoir la puissance du framework .NET
- En contrepartie :
  - Très surveillé par les systèmes microsoft
  - Exécution de code en mémoire



## Fichier malicieux py

- Les extensions .py proviennent de script exécutable Python
- Cet extension a l'avantage de :
  - Être légère
  - Avoir la puissance du langage Python
  - Être multi-plateforme
- En contrepartie :
  - L'environnement à besoin d'être installé ou empaqueté avec le code
  - Il faut savoir coder en Python
  - Un utilisateur lambda ne saura pas le lancer

