COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Journées de Concertations sur l'Adhésion de la République Islamique de Mauritanie à la Convention de Budapest sur la Cybercriminalité/Conseil de l'Europe

Les Attaques et les Crimes Cybernétiques

Didi Ould Mohamed Lemine
Ingénieur Principal en systèmes et réseaux ,
CCNA R&S, CCNP R&S, prep. CEH
dmlemine@yahoo.fr

Prepared By:
Name
Title
Date

clause de non responsabilité

Toutes les informations citées dans cette présentation sont destinées à développer l'attitude de défense contre les Hackers et aider à prévenir les attaques de pirates. J’insiste que cette information ne doit pas être utilisée pour provoquer directement ou indirectement tout type de dommage.

Prepared By:
Name
Title
Date

Sommaire

- ✓Quelques Statistiques sur les Attaques et les Crimes Cybernétiques
- ✓ Terminologies
- ✓ Méthodologie d'une intrusion
- ✓Hacking Windows Server 2008
- ✓Recommandations

Prepared By:
Name
Title
Date

Bulletin de Kaspersky sur la sécurité en 2014. Principales statistiques pour 2014

Toutes les données statistiques citées dans ce rapport ont été obtenues à l'aide du réseau antivirus distribué Kaspersky Security Network (KSN) suite au fonctionnement de divers composants chargés de la protection contre les malwares. Ces données proviennent des utilisateurs du KSN qui ont marqué leur accord pour l'utilisation des données. Des millions d'utilisateurs de logiciels de Kaspersky Lab répartis dans 213 pays et territoires participent à cet échange global d'informations sur l'activité des malwares.

Les données présentées couvrent la période allant de novembre 2013 à octobre 2014.

Chiffres de l'année

✓ D'après les données de KSN, les solutions de Kaspersky Lab ont bloqué 6 167 233 068 d'attaques contre les ordinateurs et les périphériques nomades des utilisateurs en 2014.

✓Le nombre de tentatives d'infection bloquées sur la plate-forme Mac OS X est égal, quant à lui, à 3 693 936.

✓1 363 549 attaques contre des appareils Android ont été repoussées.

✓Les solutions de Kaspersky Lab ont repoussé 1 432 660 467 attaques depuis des ressources Internet situées dans différents pays.

✓44% des attaques Internet bloquées par nos produits ont été organisées à l'aide de ressources Internet malveillantes situées aux **Etats-Unis et en Allemagne.**

✓Au cours de l'année, 38,3 % des ordinateurs des utilisateurs ont été exposés au moins une fois à une attaque via Internet.

✓Des tentatives d'exécution de malwares bancaires ont été repoussées sur les ordinateurs de 1 910 520 utilisateurs.

✓Notre antivirus Internet a détecté 123 054 503 objets malveillants uniques (scripts, codes d'exploitation, fichiers exécutables, etc.).

✓Notre antivirus fichiers a détecté 1 849 949 malwares et autres programmes potentiellement indésirables sur les ordinateurs des utilisateurs.

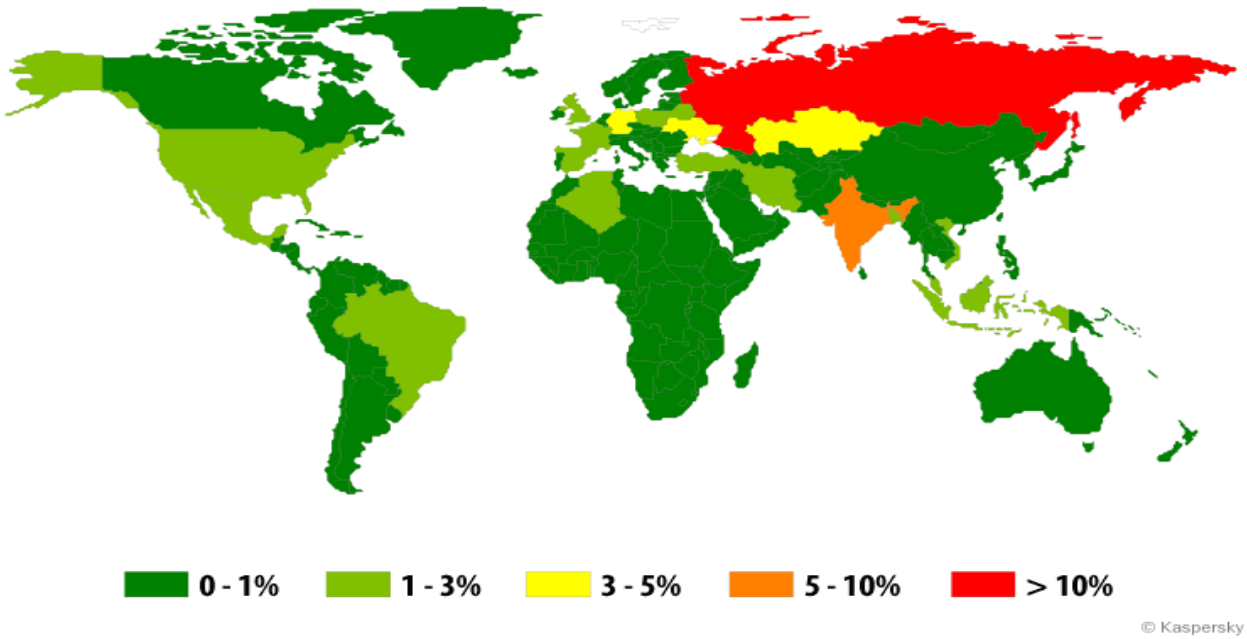
Menaces sur les appareils mobiles

Voici le résultat des détections au cours de la période couverte par le rapport :

- 4 643 582 paquets d'installation malveillants
- 295 539 nouveaux malwares pour appareils nomades
- 12 100 Trojans bancaires pour appareils nomades

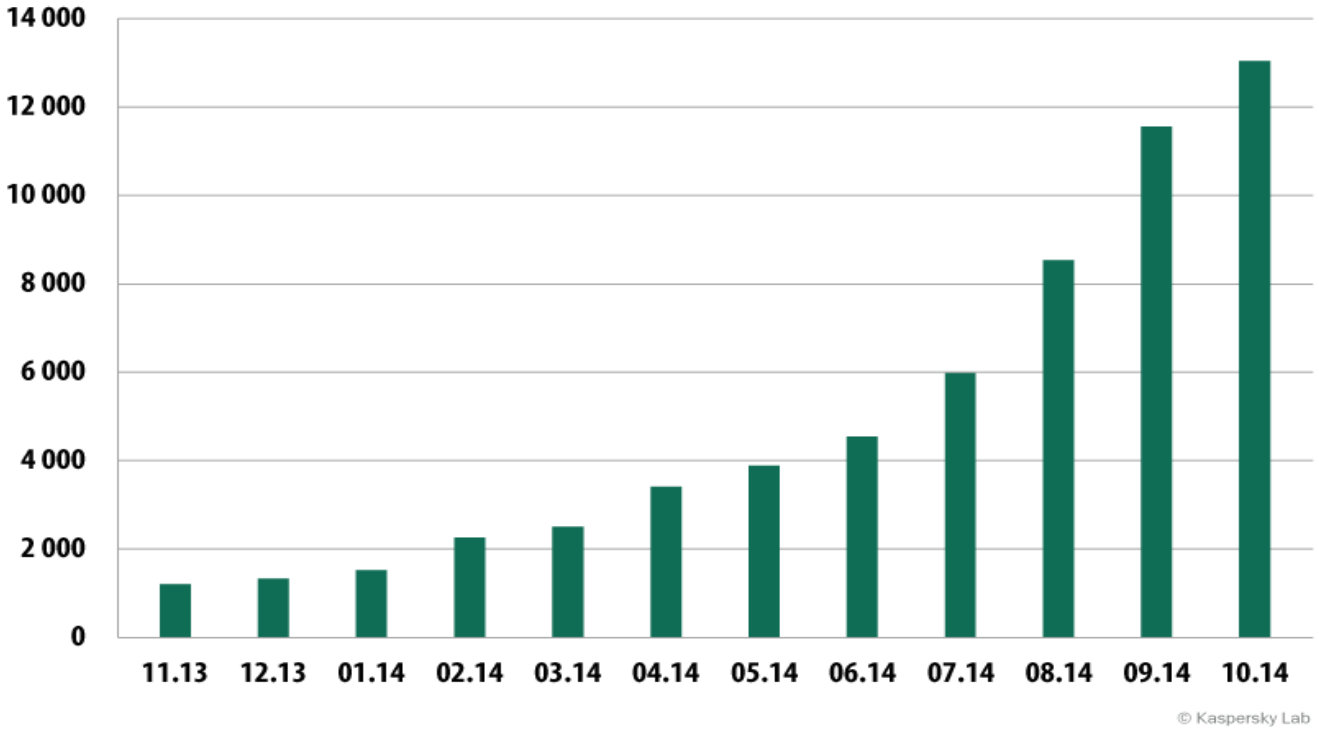
Autrement dit, le nombre d'attaques contre les appareils Android a été multiplié **par 4**.

Répartition géographique des menaces pour appareils mobiles



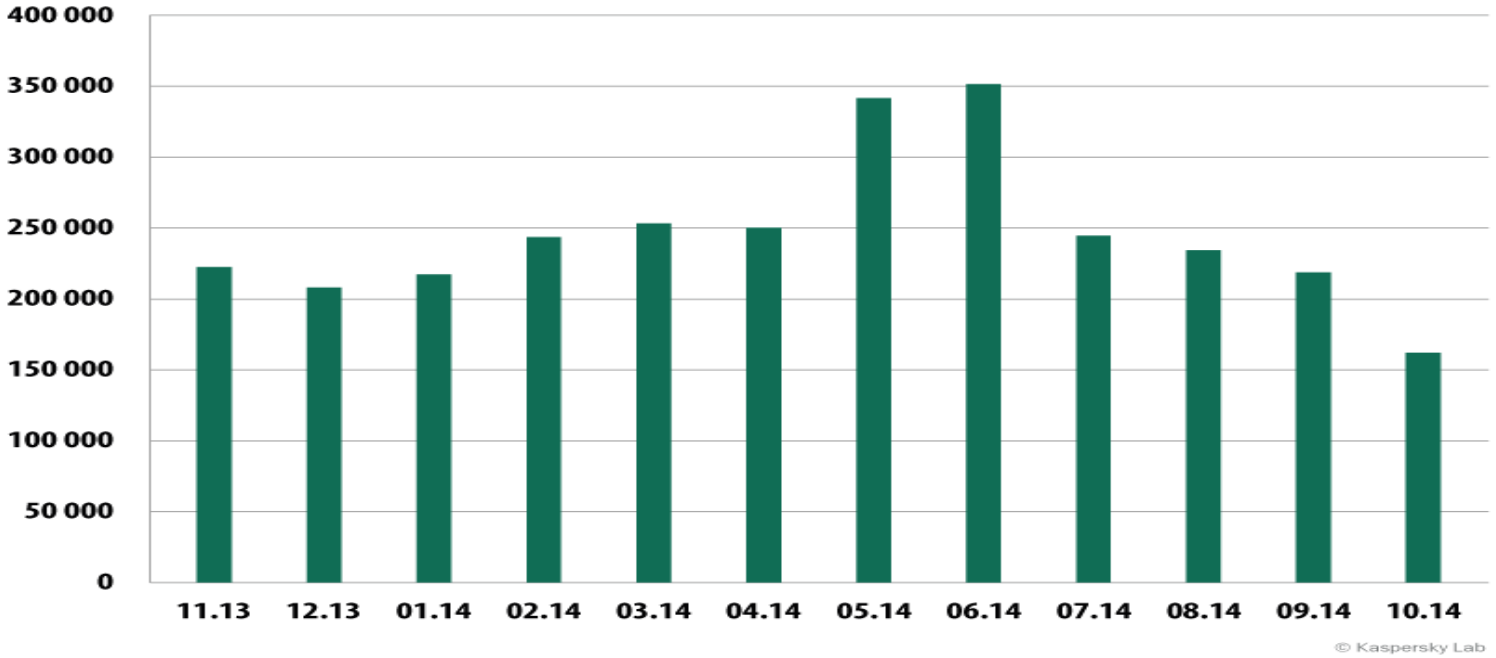
Trojan-bankers pour appareils mobiles

Au cours de la période couverte par le rapport, nous avons découvert 12 000 Trojan-Bankers pour appareils mobiles, soit 9 fois plus qu'en 2013.

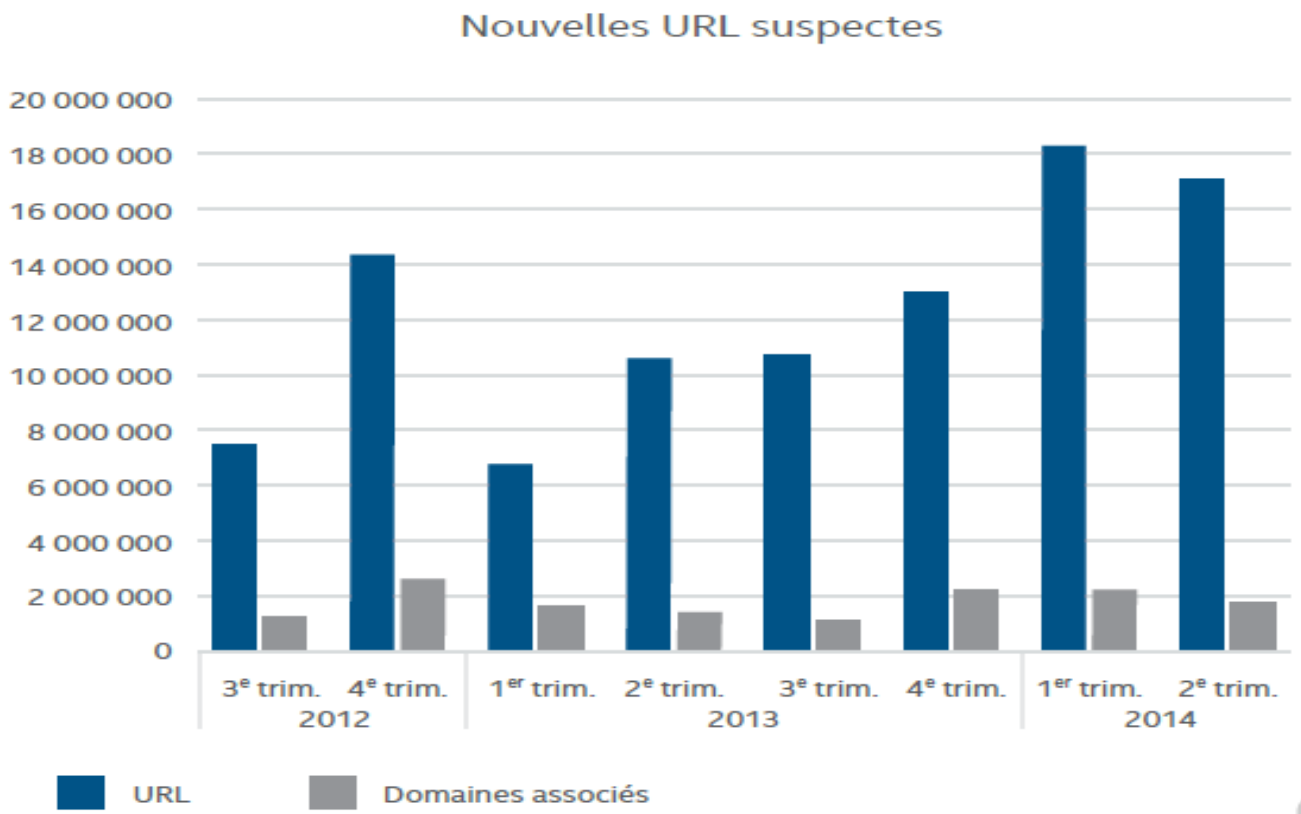


Menaces en ligne dans le secteur bancaire

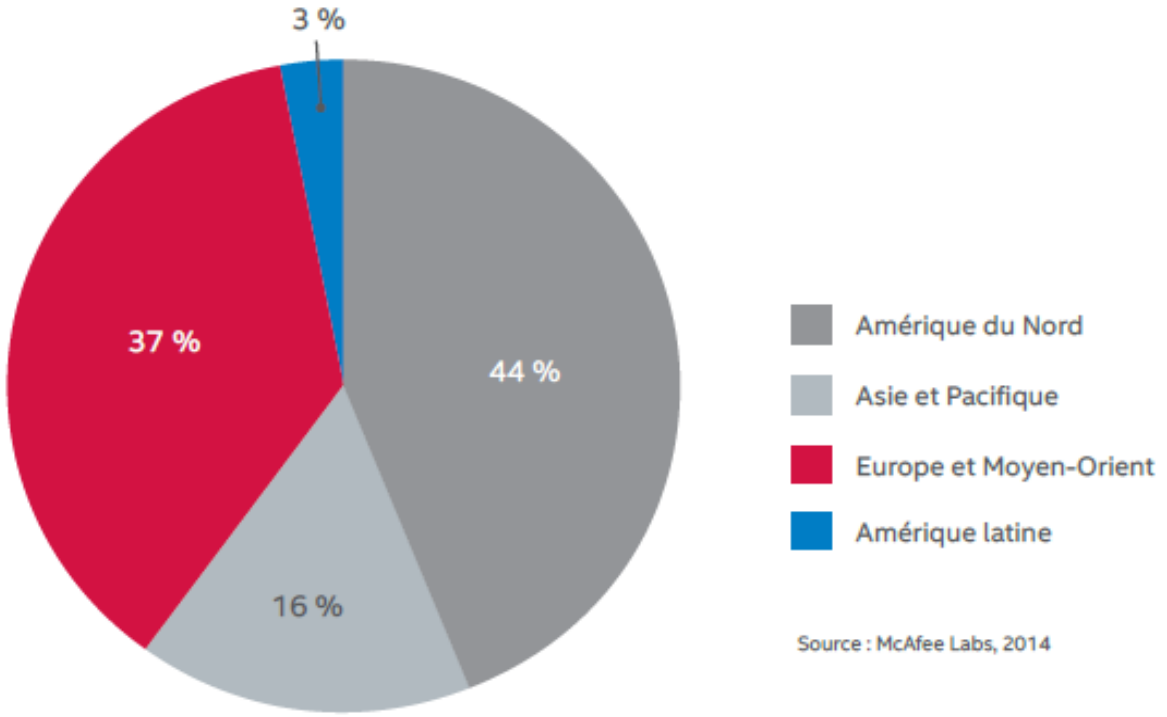
Au cours de la période couverte par le rapport, les solutions de Kaspersky Lab ont déjoué des tentatives d'exécution de malwares conçus pour voler l'argent via les systèmes de banques électroniques sur les ordinateurs de **1 910 520** utilisateurs.



Menaces Internet

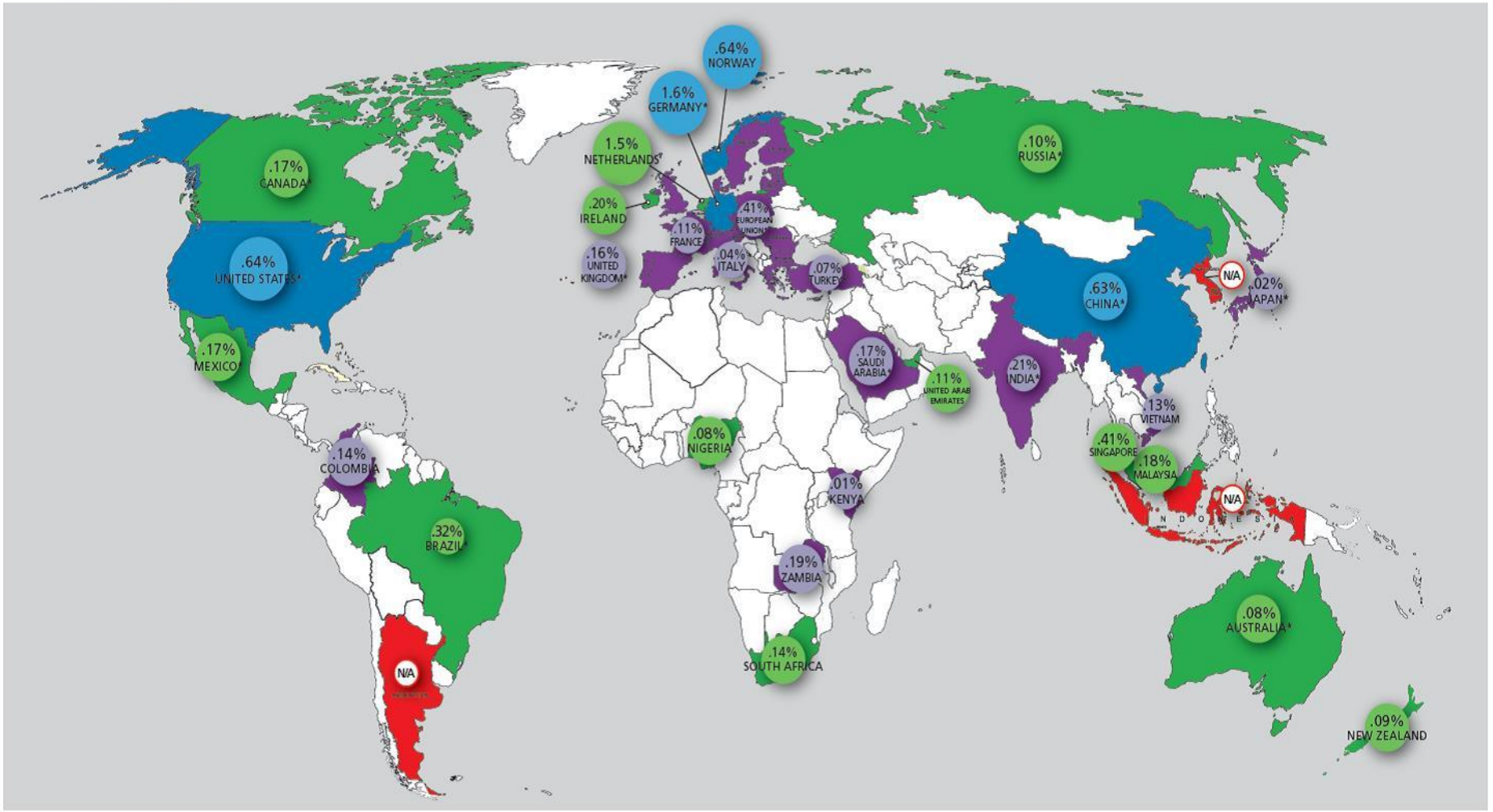


Emplacement des serveurs hébergeant du contenu suspect



McAfee
An Intel Company

CYBERCRIME LOSS AS A PERCENT OF GDP (GROSS DOMESTIC PRODUCT)



Confidence Ranking: Countries Current Tracking of Cybercrime within Their Borders.

- % High Confidence Level
- % Low Confidence Level
- * G-20 Countries
- % Medium Confidence Level
- N/A - Countries currently not measuring cybercrime loss

$445 BILLION
The annual estimated cost to the global economy from cyber crime

200,000+
Jobs lost in the U.S

150,000+
Estimated in Europe

61100info_csis-econ-cybercrime_0514_fnl_ETMG

Le Monde dans lequel on vit

- Nous sommes face non seulement à une augmentation de la quantité, mais surtout de l'**importance des données**.
- Avec le développement d'Internet, chacun a accès au réseau où de plus en plus d'informations **circulent**.
  Exemple:
  les entreprises communiquent et diffusent des informations, que ce soit dans leurs liens avec leurs fournisseurs ou leurs partenaires ou en interne, dans les relations entre les employés eux-mêmes.
- Le transport des données en dehors du domicile d'un particulier ou d'une entreprise mérite que l'on s'interroge sur la **sécurité** des transmissions pour ne pas compromettre un système d'information.

Qu'est-ce que la sécurité?

- **Définition de base** : La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles.
- Sécurité = "Safety"
  Protection de systèmes informatiques contre les accidents dus à l'environnement, les défauts du système.
- Sécurité = "Security "
  Protection des systèmes informatiques contre des actions malveillantes intentionnelles.
- Note : Une vulnérabilité (ou faille) est une faiblesse dans un système informatique.

http://www.securityfocus.com

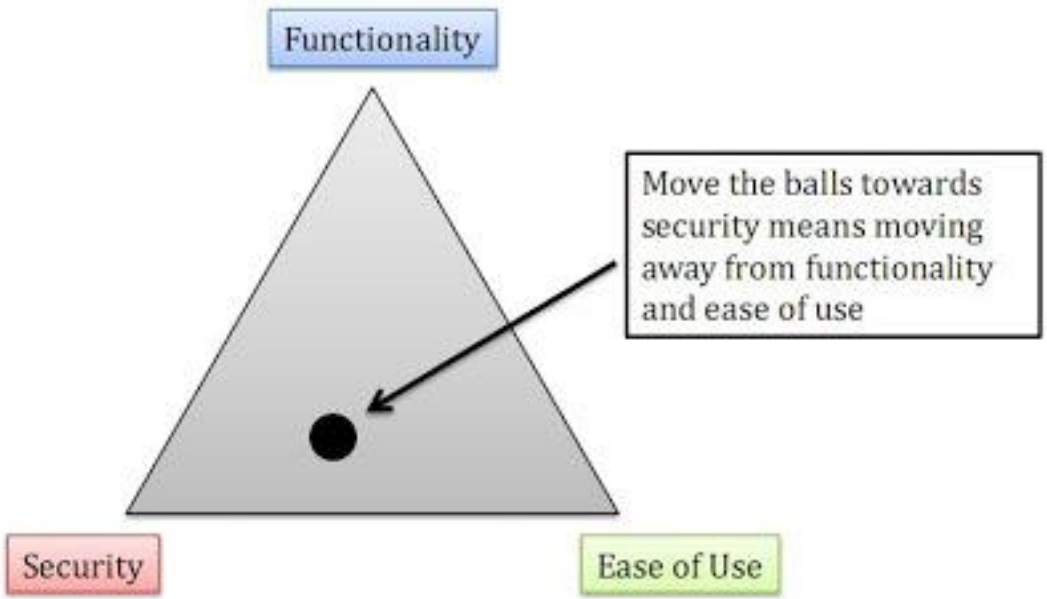
http://nvd.nist.gov

http://securitytracker.com

.

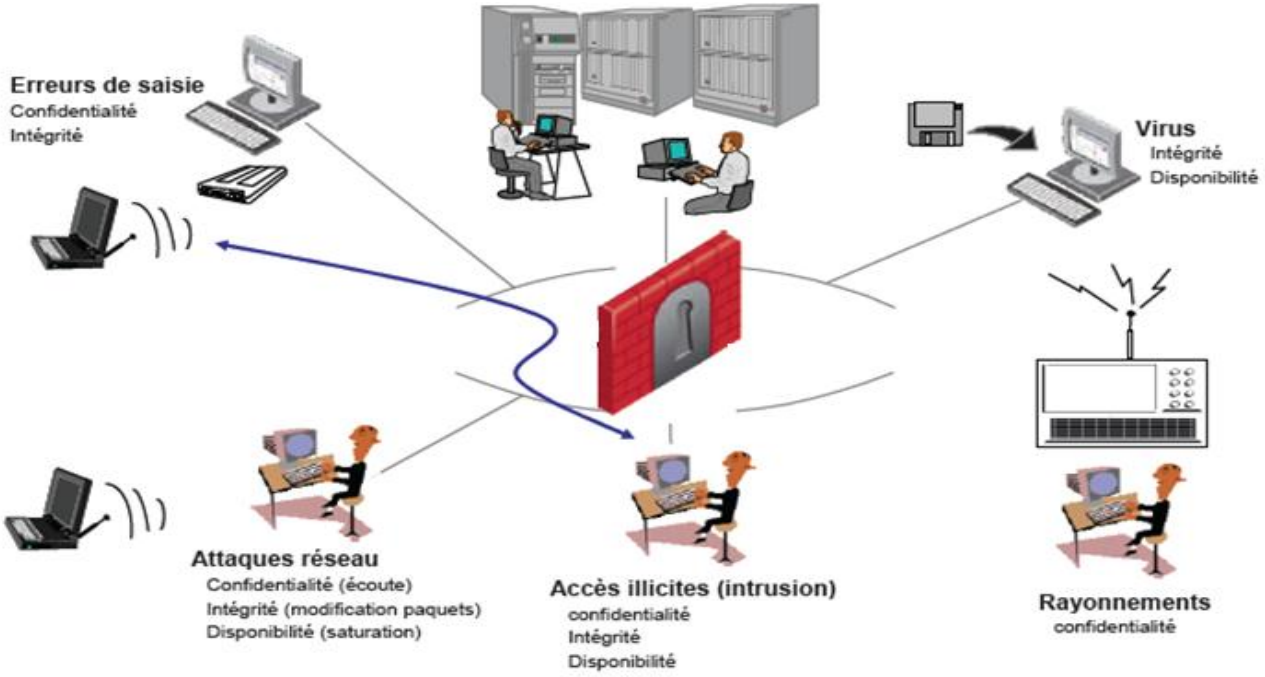
Terminologies

Triangle de la Sécurité, Performance et Simplicité d'utilisation



Les attaques

- Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une **attaque**.
- Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système.



Les attaques

Les motivations des attaques peuvent être de différentes sortes :

- obtenir un accès au système ;
- voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- avoir des informations personnelles sur un utilisateur ;
- récupérer des données bancaires ;
- s'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- troubler le bon fonctionnement d'un service ;
- utiliser le système de l'utilisateur comme “rebond” pour une attaque ;
- utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée

Les pirates

Hacker/pirate

- Le terme "**hacker**" est souvent utilisé pour désigner un **pirate** informatique.
- A l'origine ce nom désignait les programmeurs expérimentés.
- Il servit au cours des années 70 à décrire les révolutionnaires de l'informatique, qui pour la plupart sont devenus les fondateurs des plus grandes entreprises informatiques.
- C'est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéos, en désamorçant les protections de ces derniers, puis en en revendant des copies.
- Aujourd'hui ce mot est souvent utilisé à tort pour désigner les personnes s'introduisant dans les systèmes informatiques.

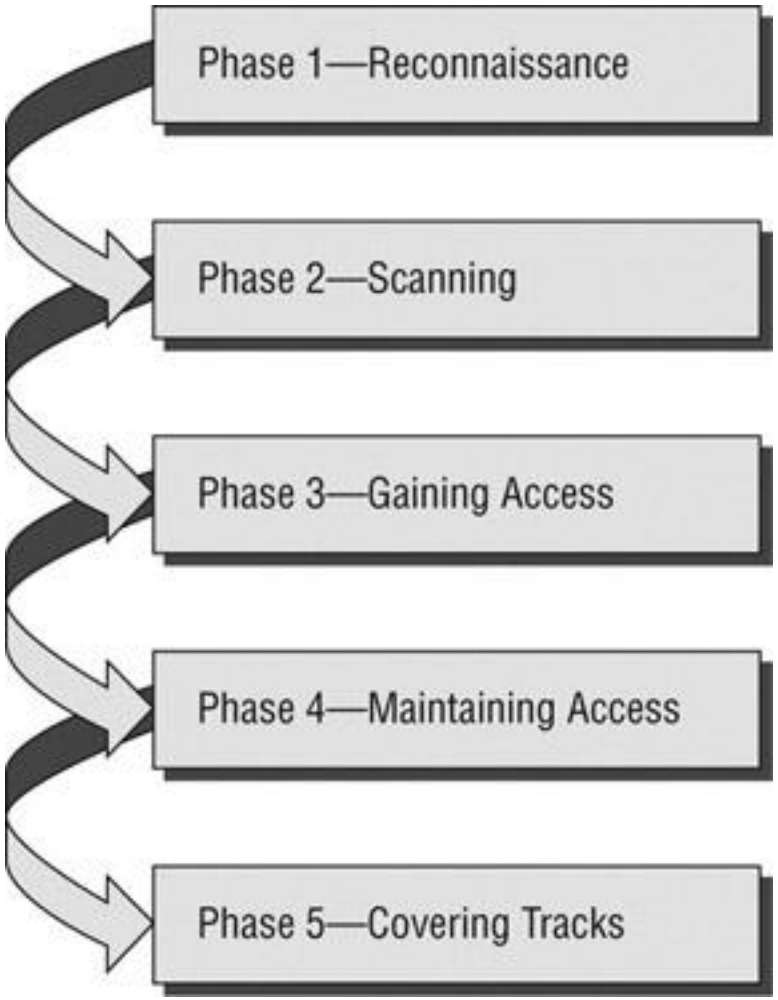
Les pirates

Les différents types de pirates

En réalité il existe de nombreux types d' attaquants catégorisés selon leur expérience et selon leurs motivations :

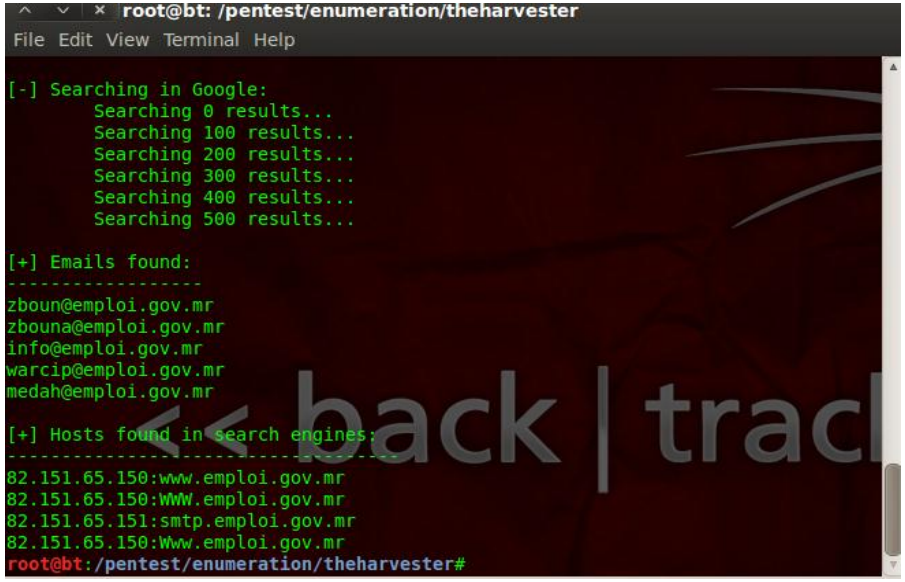
- Les "**white hat hackers**", hackers au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui; Le courrier électronique est un des meilleurs exemples;
- **Les** "**black hat hackers**", plus couramment appelés pirates, c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans un but nuisible ;
- Les "**hacktivistes**" (cybermilitant ou cyberrésistant), sont des hackers dont la motivation est principalement idéologique.

Méthodologie d'une intrusion

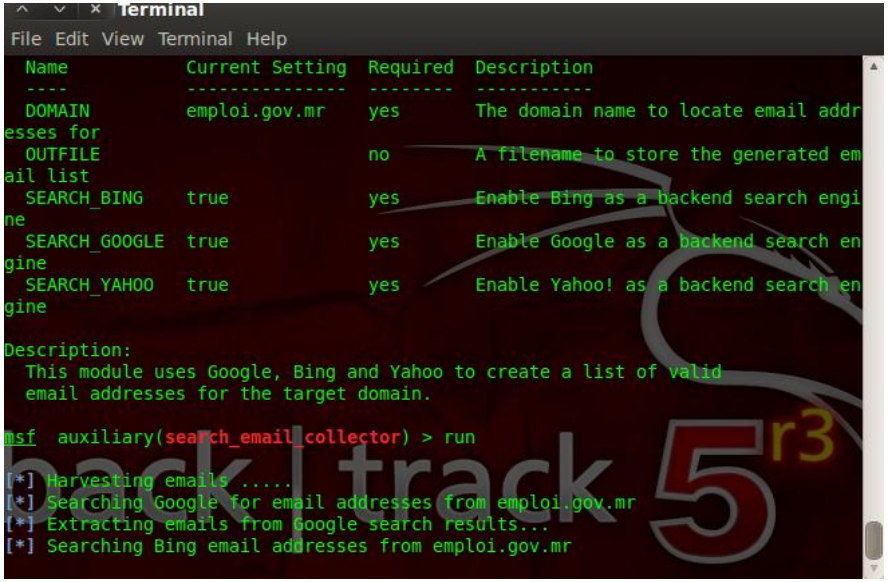


Enumeration des Emails

- theHarvester



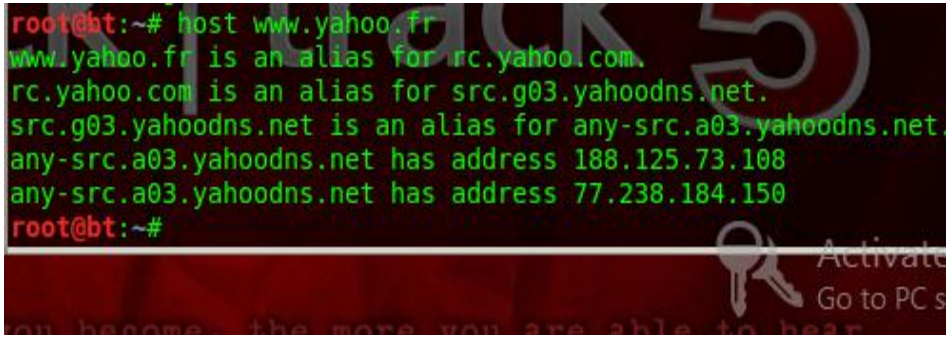
- Collecting emails using Metasploit



Reconnaissance

Comprendre le Footprinting d'un Serveur Web

- Trouver l'adresse IP d'un Serveur: ping, host
- Localiser l'adresse IP: http://www.iplocation.net/
- Trouver le type de serveur web: **Outil**: whatweb

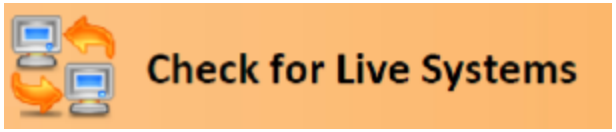


- Trouver les sites Web héberger sur le méme serveur

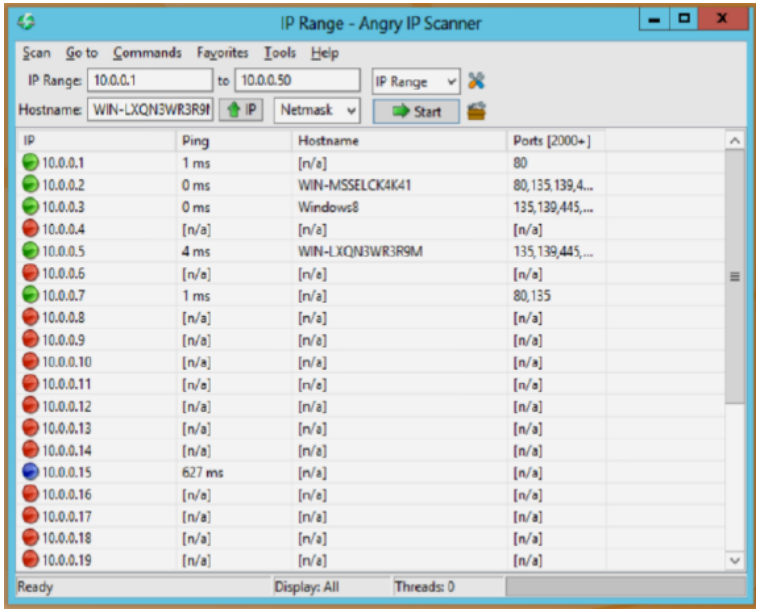
Méthodologie de Balayage (Scanning)

Check for Live Systems	Scan for Vulnerability
Check for Open Ports	Draw Network Diagrams
Scanning Beyond IDS	Prepare Proxies
Banner Grabbing	Attack

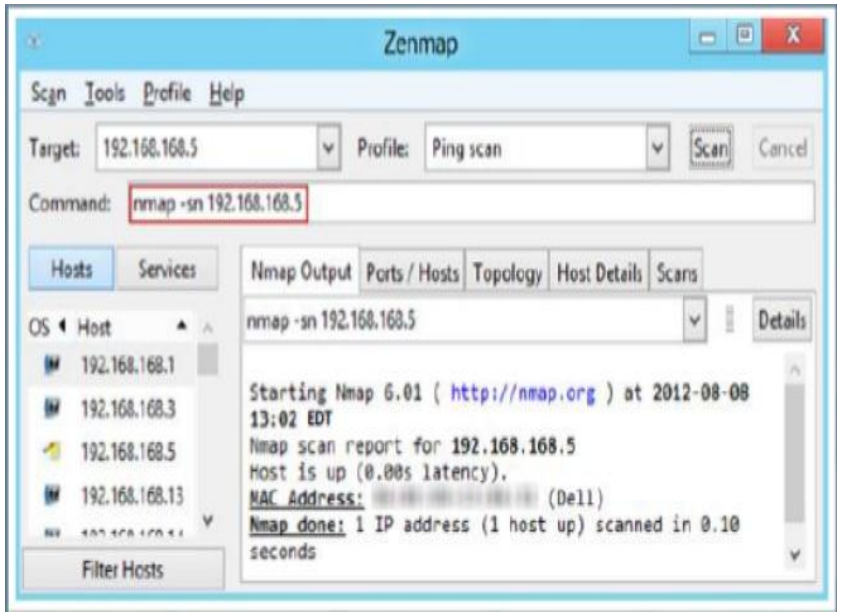
Méthodologie de Balayage (Scanning)



Angry IP Scanner



Zenmap



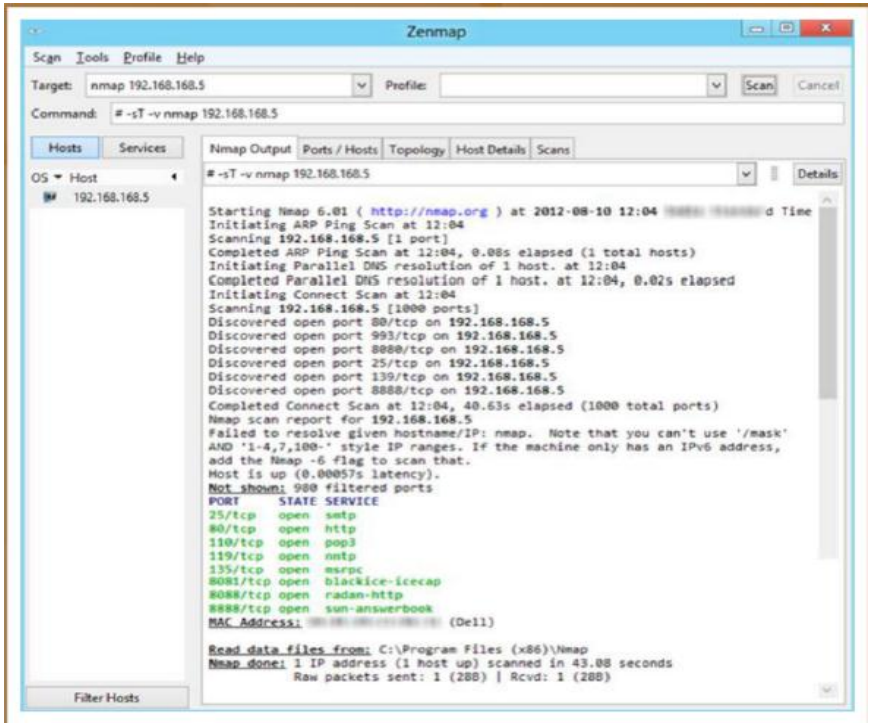
Méthodologie de Balayage (Scanning)

Check for Open Ports

Hping3

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# hping3 -A 10.0.0.2 -p 80
HPING 10.0.0.2 (eth1 10.0.0.2): A set, 40 headers + 0 data byte
s
len=40 ip=10.0.0.2 ttl=128 DF id=26085 sport=80 flags=R seq=0 w
in=0 rtt=1.3 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26086 sport=80 flags=R seq=1 w
in=0 rtt=0.8 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26087 sport=80 flags=R seq=2 w
in=0 rtt=1.0 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26088 sport=80 flags=R seq=3 w
in=0 rtt=0.9 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26089 sport=80 flags=R seq=4 w
in=0 rtt=0.9 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26090 sport=80 flags=R seq=5 w
in=0 rtt=0.5 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26091 sport=80 flags=R seq=6 w
in=0 rtt=0.7 ms
len=40 ip=10.0.0.2 ttl=128 DF id=26092 sport=80 flags=R seq=7 w
in=0 rtt=0.8 ms
```

Zenmap



Méthodologie de Balayage (Scanning)

Banner Grabbing

Active Banner Grabbing

- Specially crafted packets are sent to remote OS and the response is noted
- The responses are then compared with a database to determine the OS
- Response from different OSes varies due to differences in TCP/IP stack implementation

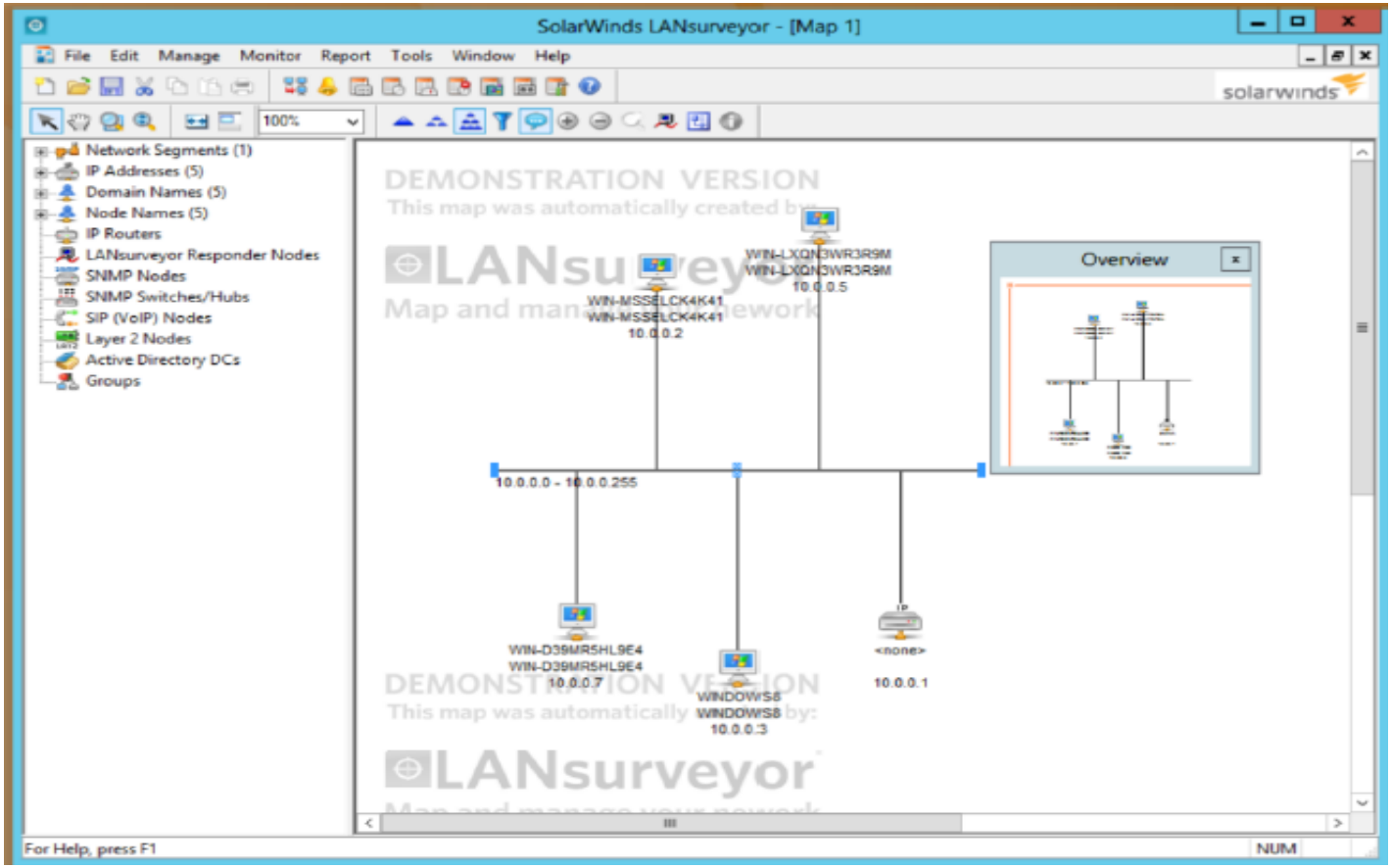
Passive Banner Grabbing

- Banner grabbing from error messages:
  Error messages provide information such as type of server, type of OS, and SSL tool used by the target remote system
- Sniffing the network traffic:
  Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system
- Banner grabbing from page extensions:
  Looking for an extension in the URL may assist in determining the application version
  Example: .aspx => IIS server and Windows platform

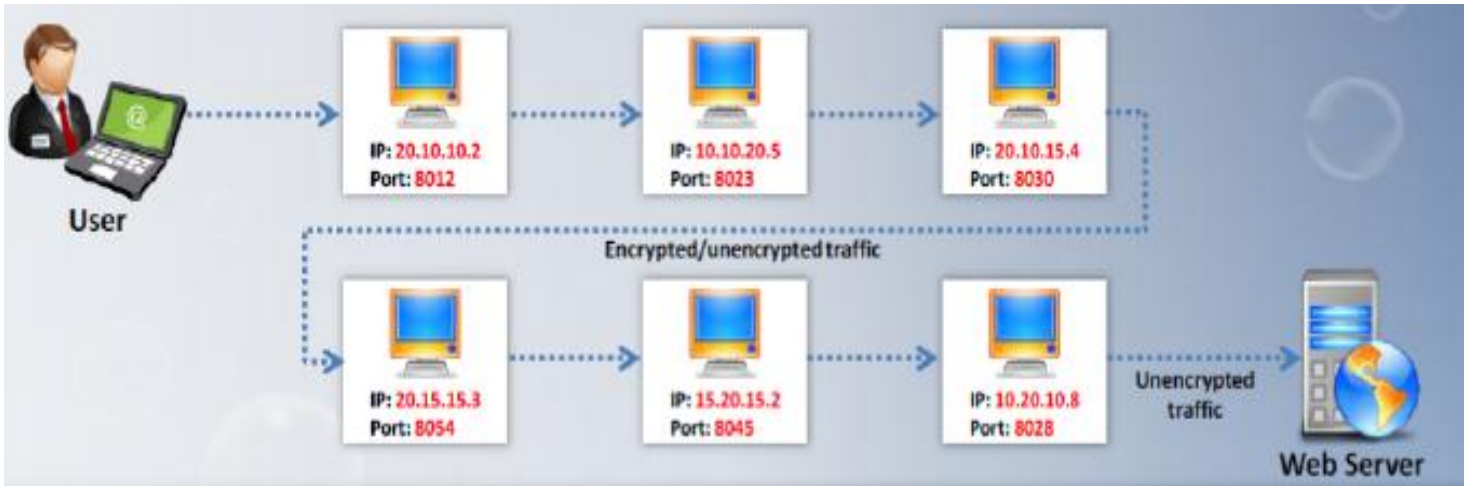
Méthodologie de Balayage (Scanning)

Autres outils : Nessus, GFI LanGuard, Acunetix(Web app vuln)

Méthodologie de Balayage (Scanning)

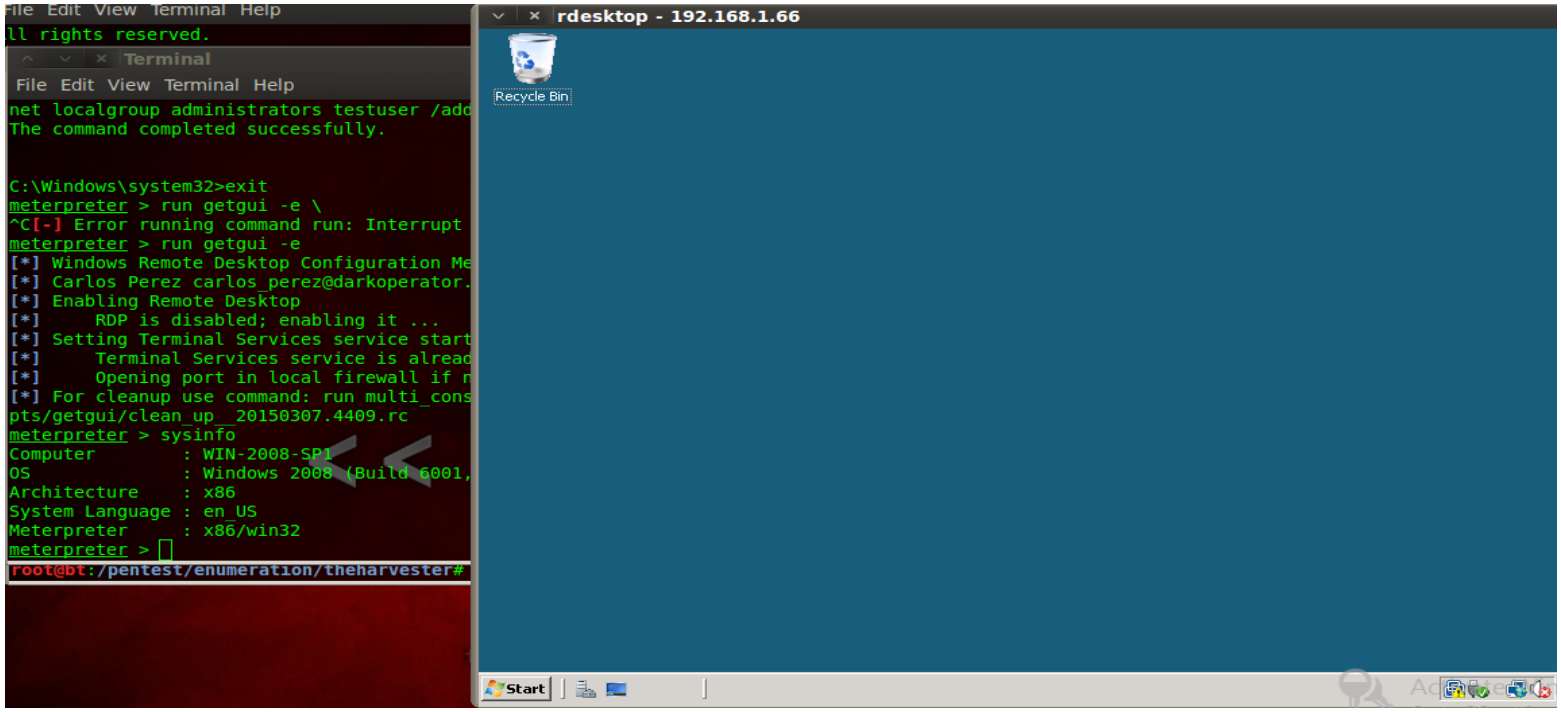


Méthodologie de Balayage (Scanning)



Exemple de PenTest: Windows Server 2008

Si vous utilisez Windows serveur 2008 SP1/SP2 par exemple vous êtes obligés d'etre conscient d'une vulnérabilité dans le service SMB2: Server Message Block version 2(pour le partage de ressources).
Pour faire le PenTest utiliser l'exploit
exploit/windows/smb/ms09_050_smb2_negotiate_func_index
PAYLOAD:windows/meterpreter/reverse_tcp



Recommandations

1. « Patcher » votre système
2. Installer un antivirus avec Internet Security
3. Ne pas ouvrir d'email ou de pièces jointes de messages suspects (de Source inconnue)
4. Ne pas partager l'accès à son ordinateur
5. Protéger votre ordinateur contre les intrusions
6. Ne pas visiter les sites web douteux
7. Utiliser des mots de passe difficiles à deviner.
8. Sauvegarder régulièrement les données importantes
9. Ne pas laisser son poste connecté au réseau (et surtout à l'Internet), sans contrôle
10. Avoir la bonne réaction

Je vous remercie