Hackfest 2013 War Game

Highlights & How to

Prices - War Game

- 1st place (territory points)
  - Soviet Union
  - 9x100$
  - 1 Offensive Security CTP
- 2nd place (territory points)
  - European Union
  - 10x No Starch books
- Best Free Thinker
  - NO! (Bryon Hart)
  - Voucher code for Offensive Security Wireless Attacks v.3.0 + Certification

Side note

- Middle East got third place, they were the stealthiest team.

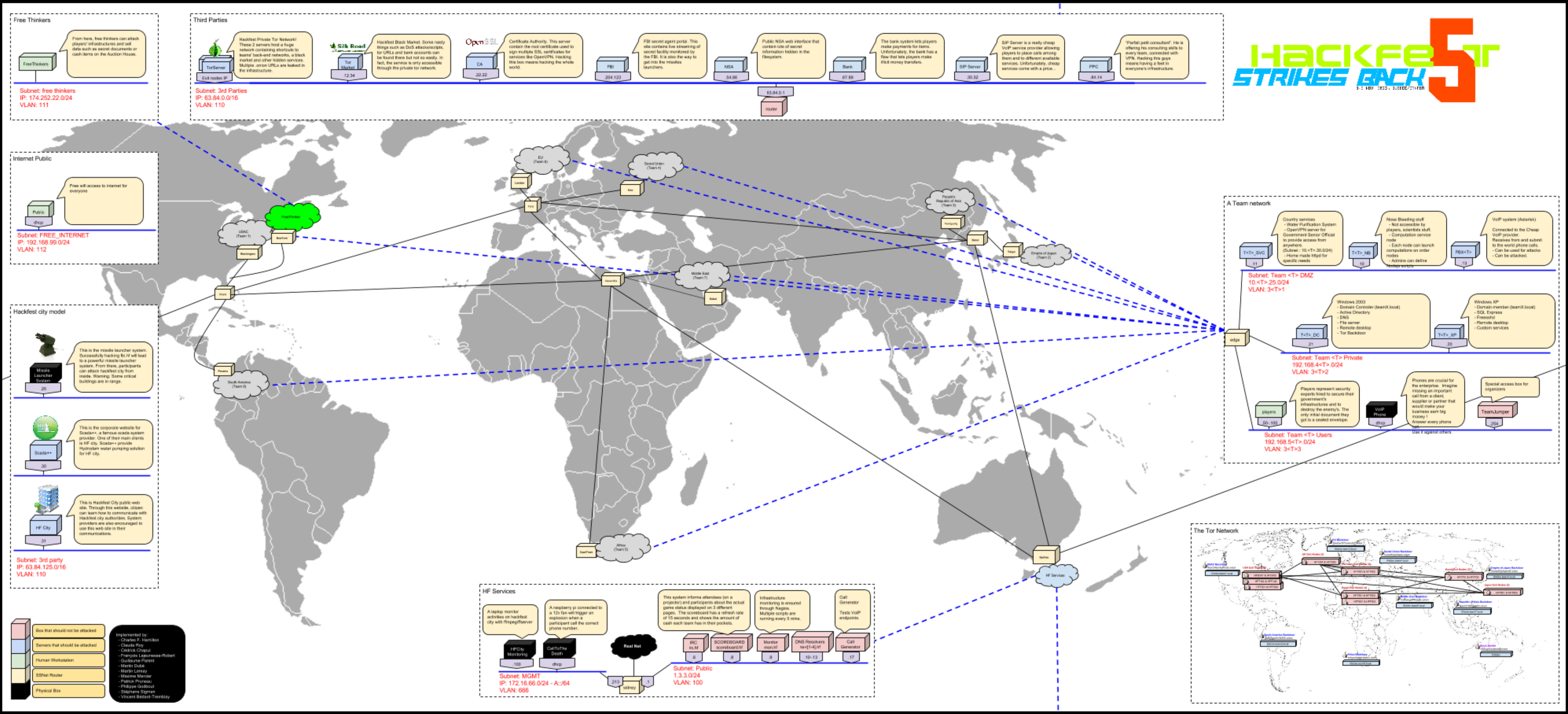
2013 War Game Highlights

- Hackfest city got pwned
- FTP server username/password bruteforce was hard (wtf?)
- No territory flag until leaks? (Cmon guys ;))
- Challenge was harder than last year
- People were tired answering the phone
-

2013 War Game FAILS

- FBI FAIL !
- Monitoring frontend not matching the backend
- Computation service UI not supporting google Chrome
- One of our server died 1 hour before start…
- Some bitches loved to unplug cables

World Map



Free Thinkers

FreeThinkers

From here, free thinkers can attack players' infrastructures and sell data such as secret documents or cash items on the Auction House.

Subnet: free thinkers
IP: 174.252.22.0/24
VLAN: 111

Third Parties

TorServer
Exit nodes IP

Hackfest Private Tor Network! These 2 servers host a huge network containing shortcuts to teams' back-end networks, a black market and other hidden services. Multiple .onion URLs are leaked in the infrastructure.

Silk Road
Tor Market
.12.34

Hackfest Black Market. Some nasty things such as DoS attacks/scripts, tor URLs and bank accounts can be found there but not so easily. In fact, the service is only accessible through the private tor network.

OpenSSL
CA
.22.22

Certificate Authority. This server contain the root certificate used to sign multiple SSL certificates for services like OpenVPN. Hacking this box means hacking the whole world.

FBI
.204.123

FBI secret agent portal. This site contains live streaming of secret facility monitored by the FBI. It is also the way to get into the missiles launchers.

NSA
.54.86

Public NSA web interface that contain lots of secret information hidden in the filesystem.

Bank
.67.89

The bank system lets players make payments for items. Unfortunately, the bank has a flaw that lets players make illicit money transfers.

SIP Server
.30.32

SIP Server is a really cheap VoIP service provider allowing players to place calls among them and to different available services. Unfortunately, cheap services come with a price...

PPC
.84.14

"Parfait petit consultant". He is offering his consulting skills to every team, connected with VPN. Hacking this guys means having a feet in everyone's infrastructure.

63.84.0.1
router

Subnet: 3rd Parties
IP: 63.84.0.0/16
VLAN: 110

Internet Public

Public
dhcp

Free wifi access to internet for everyone

Subnet: FREE_INTERNET
IP: 192.168.99.0/24
VLAN: 112

Hackfest city model

Missile Launcher System
25

This is the missile launcher system. Successfully hacking fbi.hf will lead to a powerful missile launcher system. From there, participants can attack hackfest city from inside. Warning: Some critical buildings are in range.

Scada++
30

This is the corporate website for Scada++, a famous scada system provider. One of their main clients is HF city. Scada++ provide Hydrodam water pumping solution for HF city.

HF City
31

This is Hackfest City public web site. Through this website, citizen can learn how to communicate with Hackfest city authorities. System providers are also encouraged to use this web site in their communications.

Subnet: 3rd party
IP: 63.84.125.0/16
VLAN: 110

🟥	Box that should not be attacked
🟦	Servers that should be attacked
🟩	Human Workstation
🟨	SSNet Router
⬛	Physical Box

Implemented by:
- Charles F. Hamilton
- Claude Roy
- Cédrick Chaput
- François Lajeunesse-Robert
- Guillaume Parent
- Martin Dubé
- Martin Lemay
- Maxime Mercier
- Patrick Pruneau
- Philippe Godbout
- Stéphane Sigmen
- Vincent Bédard-Tremblay

A Team network

T<T>_SVC
.11

Country services
- Water Purification System
- OpenVPN server for Government Senior Official to provide access from anywhere.
(Subnet : 10.<T>.30.0/24)
- Home made httpd for specific needs

T<T>_NB
.10

Nose Bleeding stuff
- Not accessible by players, scientists stuff.
- Computation service node
- Each node can launch computations on order nodes
- Admins can define Nodejs scripts

PBX<T>
.13

VoIP system (Asterisk)

Connected to the Cheap VoIP provider.
Receives from and submit to the world phone calls.
- Can be used for attacks
- Can be attacked.

Subnet: Team <T> DMZ
10.<T>.25.0/24
VLAN: 3<T>1

edge

T<T>_DC
.21

Windows 2003
- Domain Controler (teamX.local)
- Active Directory
- DNS
- File server
- Remote desktop
- Tor Backdoor

T<T>_XP
.20

Windows XP
- Domain member (teamX.local)
- SQL Express
- Freesshd
- Remote desktop
- Custom services

Subnet: Team <T> Private
192.168.4<T>.0/24
VLAN: 3<T>2

players
.50-.100

Players represent security experts hired to secure their government's infrastructures and to destroy the enemy's. The only initial document they got is a sealed envelope.

VoIP Phone
dhcp

Phones are crucial for the enterprise. Imagine missing an important call from a client, supplier or partner that would make your business earn big money !
Answer every phone call.
Use it against others.

TeamJumper
.254

Special access box for organizers

Subnet: Team <T> Users
192.168.5<T>.0/24
VLAN: 3<T>3

The Tor Network

HF Services

HFCity Monitoring
.100

A laptop monitor activities on hackfest city with ffmpeg/ffserver

CallToThe Death
dhcp

A raspberry pi connected to a 12v fan will trigger an explosion when a participant call the correct phone number.

Subnet: MGMT
IP: 172.16.66.0/24 - A::/64
VLAN: 666

Real Net
213
sidney
.1

IRC
irc.hf
.6

SCOREBOARD
scoreboard.hf
.8

This system informs attendees (on a projector) and participants about the actual game status displayed on 3 different pages. The scoreboard has a refresh rate of 15 seconds and shows the amount of cash each team has in their pockets.

Monitor
mon.hf
.9

Infrastructure monitoring is ensured through Nagios. Multiple scripts are running every 5 mins.

DNS Resolvers
ns-r[1-4].hf
.10-.13

Call Generator
.17

Call Generator

Tests VoIP endpoints.

Subnet: Public
1.3.3.0/24
VLAN: 100

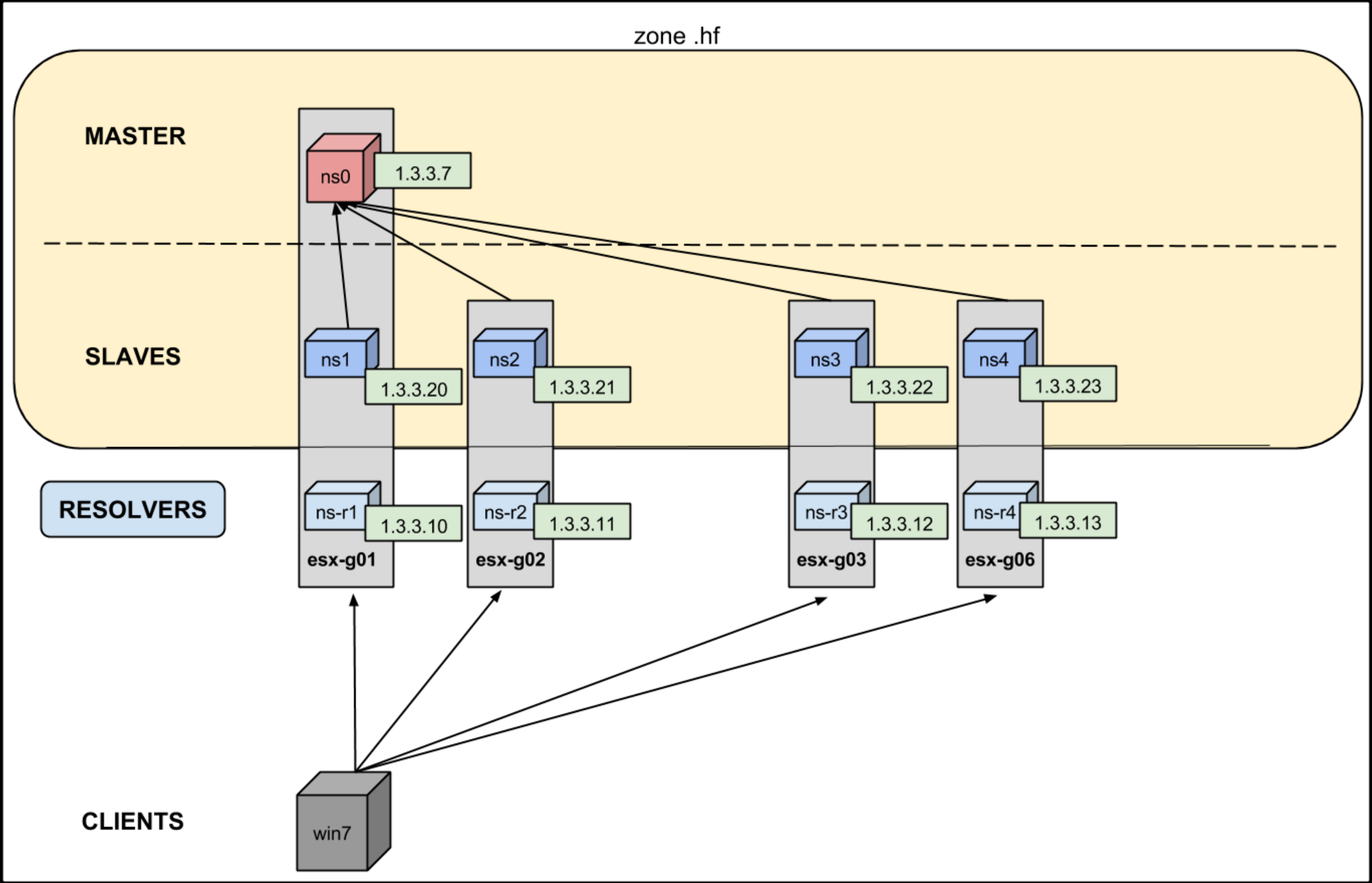
Hackfest War Game Numbers

- 90 virtual machines
- 6 physical hosts
- 47 vlans
- DNS servers: 1 master, 4 slaves, 4 resolvers
- WorkHours = 12 * RND(100, 300);
- WorkHours = between 1200 to 3600 hours
  - There’s no way to know for sure…
- 12 extremely dedicated team members!
- Total of 239 flags!

Hackfest War Game Numbers (2)

- VOIP
  - A total of 437/740 calls were answered ! Others just failed…
  - 2 teams made a call with a spoofed callerID

Core Infra - DNS Architecture



Teams Infra

- Frontend
    - OpenVPN (Let players access other teams’ network)
    - Water purification system
    - Computation service (Make it yourself exploits)
        -
    - VoIP services

Teams Infra

- Backend
  - Windows XP
  - Windows 2k3 (Domain Controller)
  - Real life weaknesses
    - SAM cracking
    - Weak passwords
    - In-memory cleartext passwords
    - Pass the hash
    - Weak custom services
    - Password reutilization
    - Autologon config
  - Freesshd service vuln
  - SQL priv escalation

Third Parties

- TOR
  - 18 TOR nodes (18 relays, 18 exit nodes, 4 directory)
  - 2 VMs (redundancy)
  - 9 chroot configs per server
  - Hidden services, tor backdoor, black market… ;)
  - Real geolocation information for the TOR map
  - Automated private TOR network deployment
    - This means that we have a full private TOR network deployed and working in less than 2 minutes =)

Third Parties

- PPC (Parfait Petit Consultant)
    - International consultant connected to every team
    - Hack this guy, hack the world!

Third Parties

- http://fbi.hf (Fake, self hosted)
- http://nsa.hf (Fake, self hosted)
- http://bank.hf
- blackmarket.hf (436iuq5zqrtqwbbj.onion)

Model

- Missiles launchers
  - Aim and shoot (Raspberry PI GIOS pins)
- Remotely detonated bomb
  - Call the right number to trigger the explosion
- Oil refinery
  - Fire at the refinery
- Hydro electric dam
  - Reverse the picture and do some social engineering to flood the city

CyberWarfare Team

- Cédrik Chaput :
  - Implication : Monitoring & SSnet
- Charles F Hamilton :
  - Implication : Bank, NSA, FBI, Water purification
- Claude Roy :
  - Implication : Networking
- Guillaume Parent :
  - Implication : Networking, DNS, IRC

CyberWarfare Team

- François Lajeunesse-Robert
  - Implication : Computation service/Nose Bleeding
- Martin Dubé :
  - Implication : Team leader / M.I.A. dad
- Martin Lemay :
  - Implication : VOIP
- Maxime Mercier :
  - Implication : Model

CyberWarfare Team

- Patrick Pruneau :
  - Implication: CA, Open VPN track
- Philippe Godbout :
  - Implication: Scoreboard, Hydro Dam
- Stéphane Sigmen :
  - Implication: Tor, Virtualization, Windows backend

Special thanks

Model: SMI

Lock Pick & Bunker: PRO-CLEF
CONSEILLER EN SÉCURITÉ
RBQ 3100-3189-12

In Game IPS: CGI