

# HACKFEST STRIKES BACK

B-9 NOV 0813 - BUEBEE/CNNHUB

### Free Thinkers

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: 63.84.0.0/16  
VLAN: 110

**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, for 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 contains the root certificate used to sign multiple SSL certificates for services like OpenVPN. Hacking this box means hacking the whole world.

**FBI secret agent portal.**  
204.123  
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

### Internet Public

Free wifi access to internet for everyone

Subnet: FREE\_INTERNET  
IP: 192.168.99.0/24  
VLAN: 112

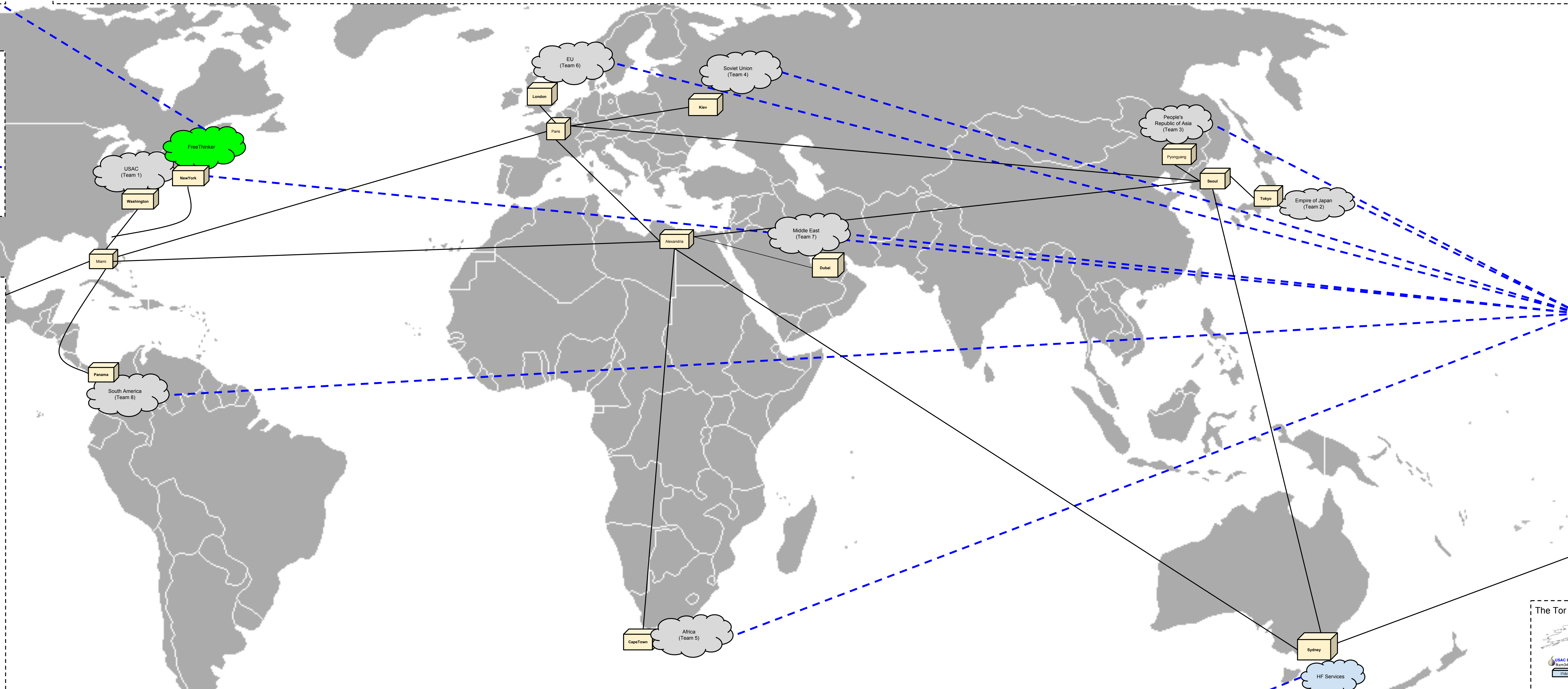
### Hackfest city model

**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



### A Team network

**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

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

**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

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

**Windows XP**  
- Domain member (teamX.local)  
- SQL Express  
- FreeSSH  
- 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**  
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  
Use it against others.

**Special access box for organizers**  
TeamJumper  
254

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

**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 Sigman  
- Vincent Bédard-Tremblay

### HF Services

A laptop monitor activities on hackfest city with ffmpeg/server

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

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.

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

Call Generator  
Tests VoIP endpoints.

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

Subnet: Public  
1.3.3.0/24  
VLAN: 100

