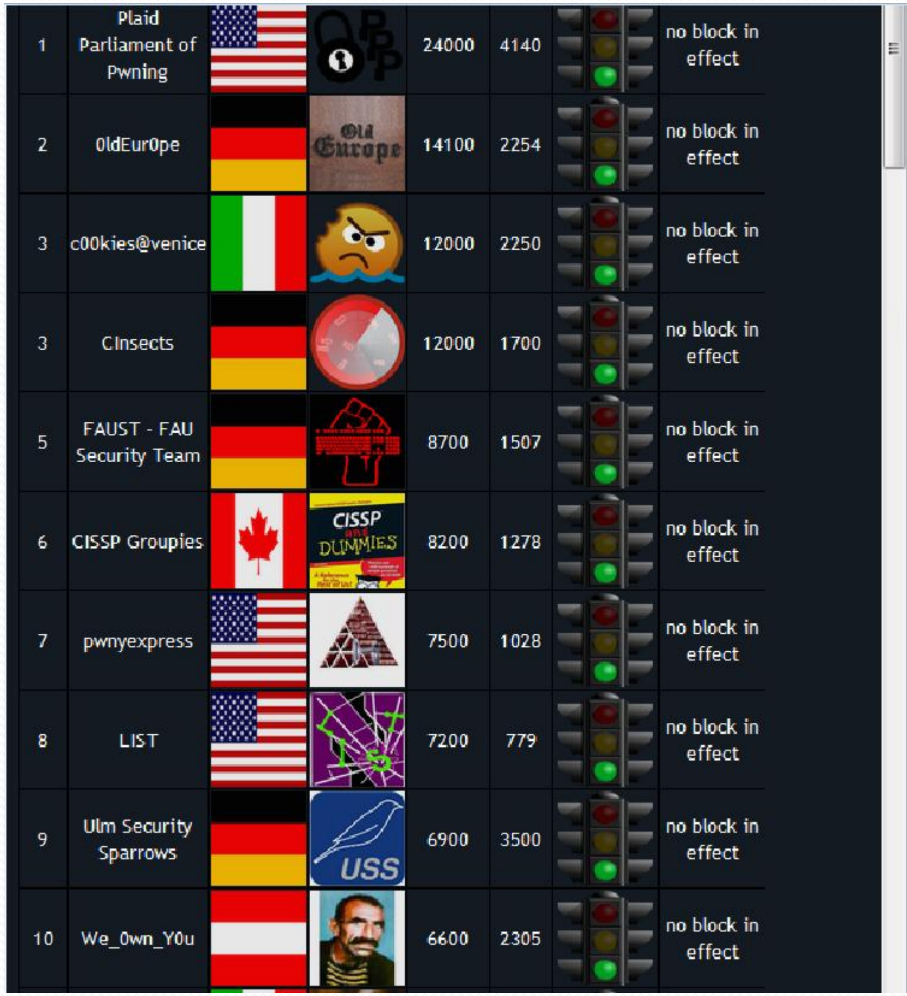
Capturing the Flag – Kicking Butt and Taking Names

Michael Kunz, Tory Cullen, Adam Gehringer

Why are we here?



1	Plaid Parliament of Pwning		PPP	24000	4140	●	no block in effect
2	OldEur0pe		Old Europe	14100	2254	●	no block in effect
3	c00kies@venice			12000	2250	●	no block in effect
3	CInsects			12000	1700	●	no block in effect
5	FAUST - FAU Security Team			8700	1507	●	no block in effect
6	CISSP Groupies		CISSP for DUMMIES	8200	1278	●	no block in effect
7	pwnyexpress			7500	1028	●	no block in effect
8	LIST			7200	779	●	no block in effect
9	Ulm Security Sparrows		USS	6900	3500	●	no block in effect
10	We_0wn_Y0u			6600	2305	●	no block in effect

What is the iCTF?

- “The UCSB International Capture The Flag (also known as the iCTF) is a distributed, wide-area security exercise, whose goal is to test the security skills of the participants. The iCTF contest is organized by Prof. Giovanni Vigna of the Department of Computer Science at UCSB, and is held once a year."
- “The Capture The Flag contest is multi-site, multi-team hacking contest in which a number of teams compete independently against each other.”

http://ictf.cs.ucsb.edu/index.php

Some iCTF History

- Started in 2003 with 14 U.S. Universities
- In 2004 it was opened internationally
- In 2005 it evolved into an intercontinental exercise
- This year 73 Teams competed from 16 countries
- There were a total of 898 participants
- "The **largest** live security exercise ever performed on the Internet."

http://ictf.cs.ucsb.edu/index.php

How was the competition setup in prior years? (2003-2007)

- Each team was provided with a pre-distributed Virtual Machine, with multiple services, multiple vulnerabilities, weak configurations, and deliberate security flaws.
- These Virtual Machines connected to a single VPN located at the UCSB.
- Offensive and Defensive Scoring
- Challenge Puzzles – Various computer related questions spanning multiple domains with a single answer. Multiple guesses allowed.

How was the competition setup in prior years? (2003-2007) (Part 2)

- **Defense:** There was a "ScoreBot" that periodically verified the required services were running on everyone's Virtual Server, which served to prevent users from just taking the Virtual Server Offline.
- Your job was to keep the machine "up" and to protect files on your server called "flags".
- **Offense:** Attack someone else's server and retrieve their "flags" to gain points.
- Free-For-All scenario

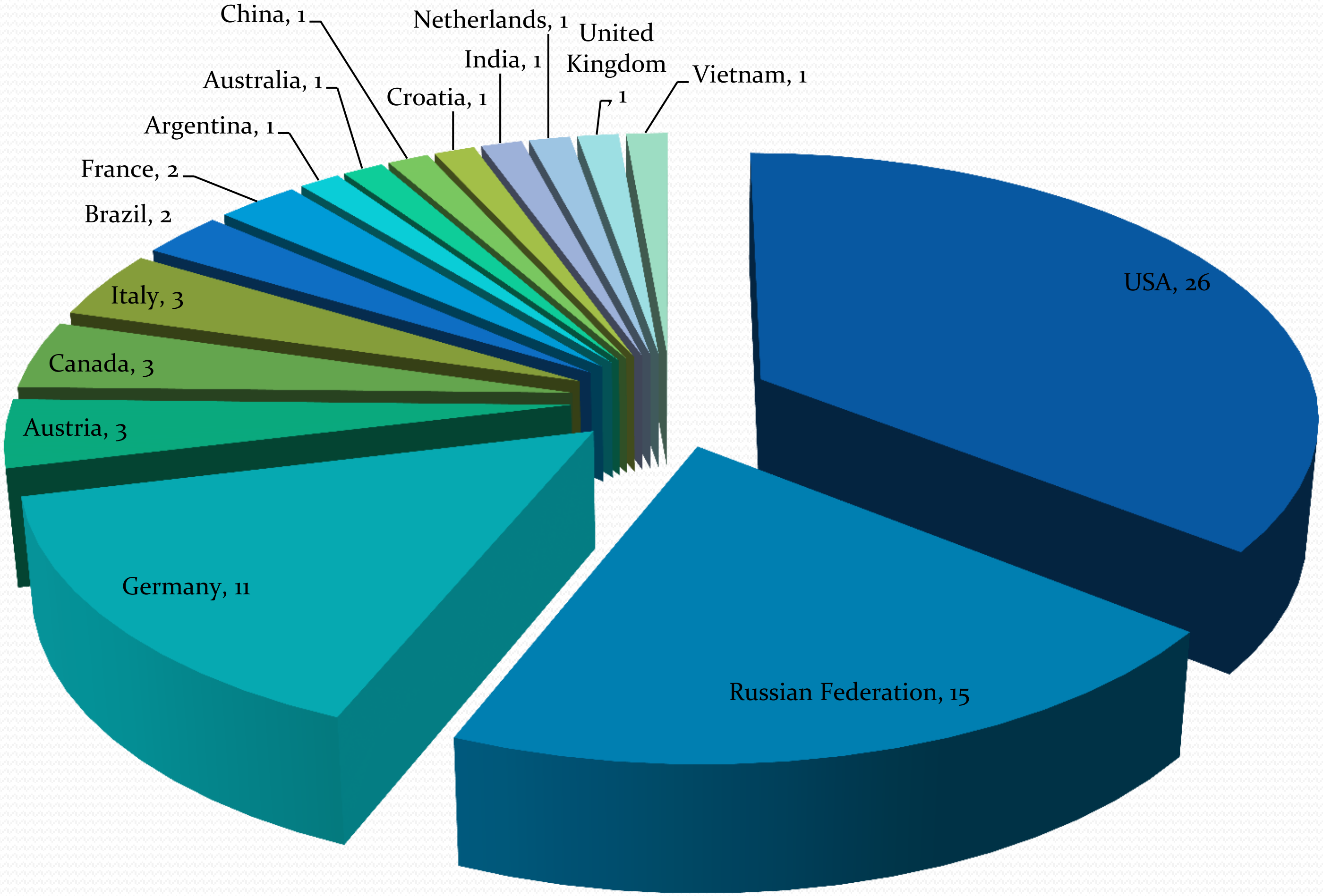
How is the competition setup in recent years?

- Virtual Machines are no longer pre-distributed.
- Vulnerable Servers are hosted on UCSB's VPN.
- No more Defensive Scoring
- Additional points awarded for discovering unlisted servers and services
- Participants are tasked with retrieving "flags" from the servers hosted at UCSB.
- Challenge Puzzles still exist
- Intrusion Detection Systems were implemented to deduct points for noisy network scans or attacks. (High Type II Error Rate and has been known to not always work right.)

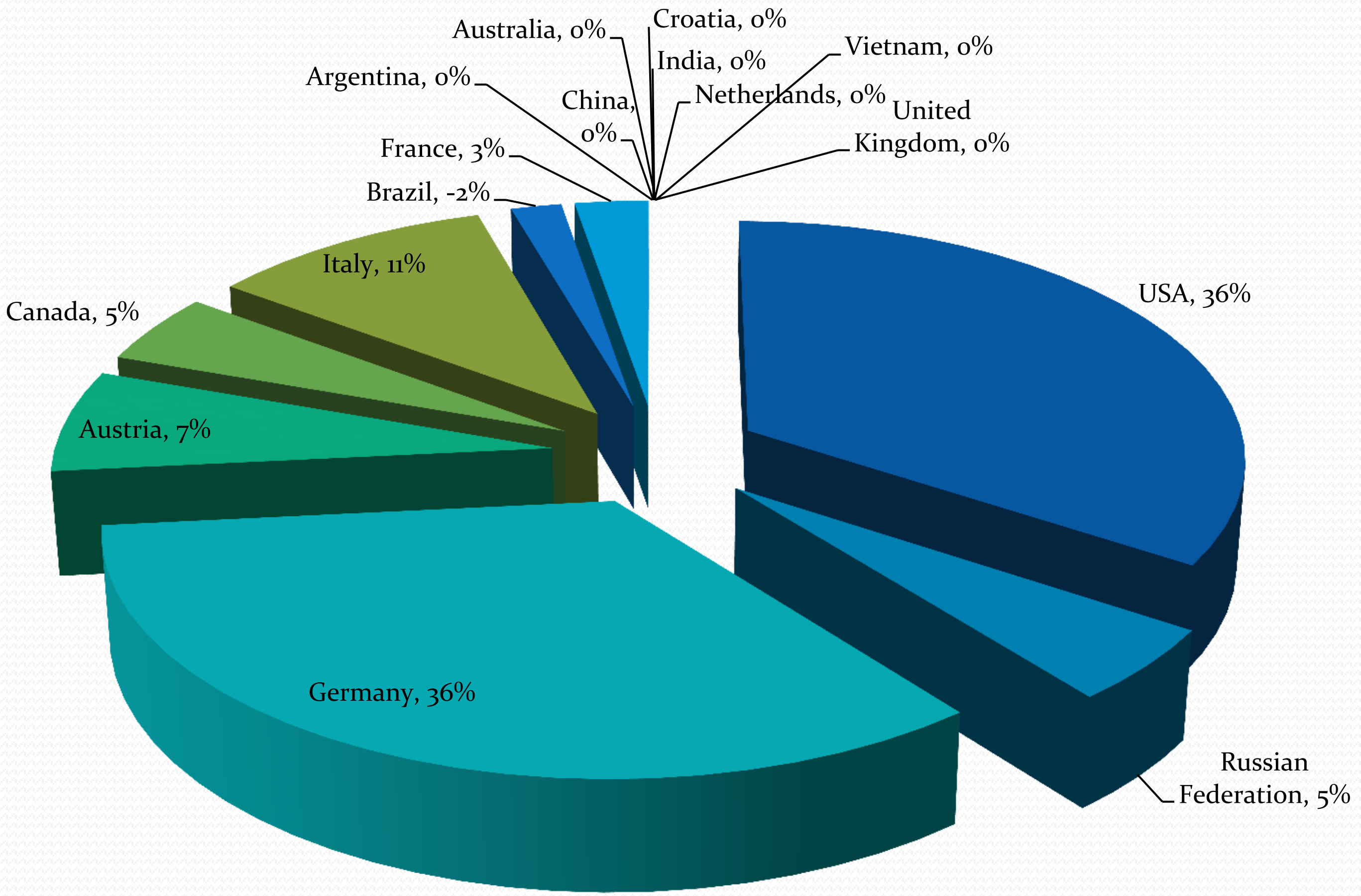
Some interesting facts

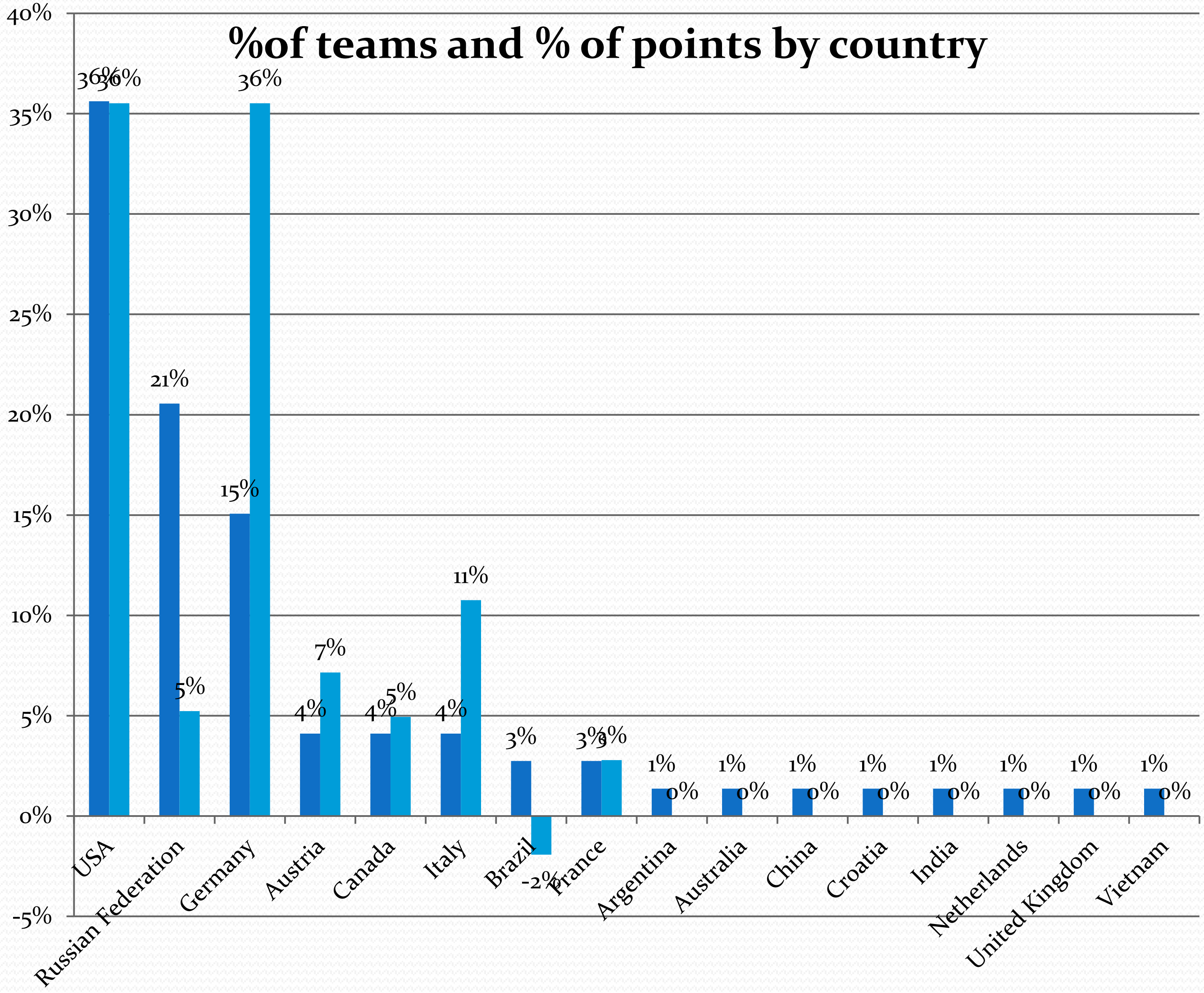
- In 2009 51% of the Teams were US Based, however we only accounted for 31% of the total points.
- In 2009 we (NUCIA) only placed 33 out of 56
- In 2009, Very few teams scored offensive points due to fake Virtual Machines being deployed and very difficult tasks to exploit vulnerabilities in client side browsers.
- In 2010 36% of the Teams were US Based, and we accounted for 34% of the total points.

# of teams by Country



% of points by Country





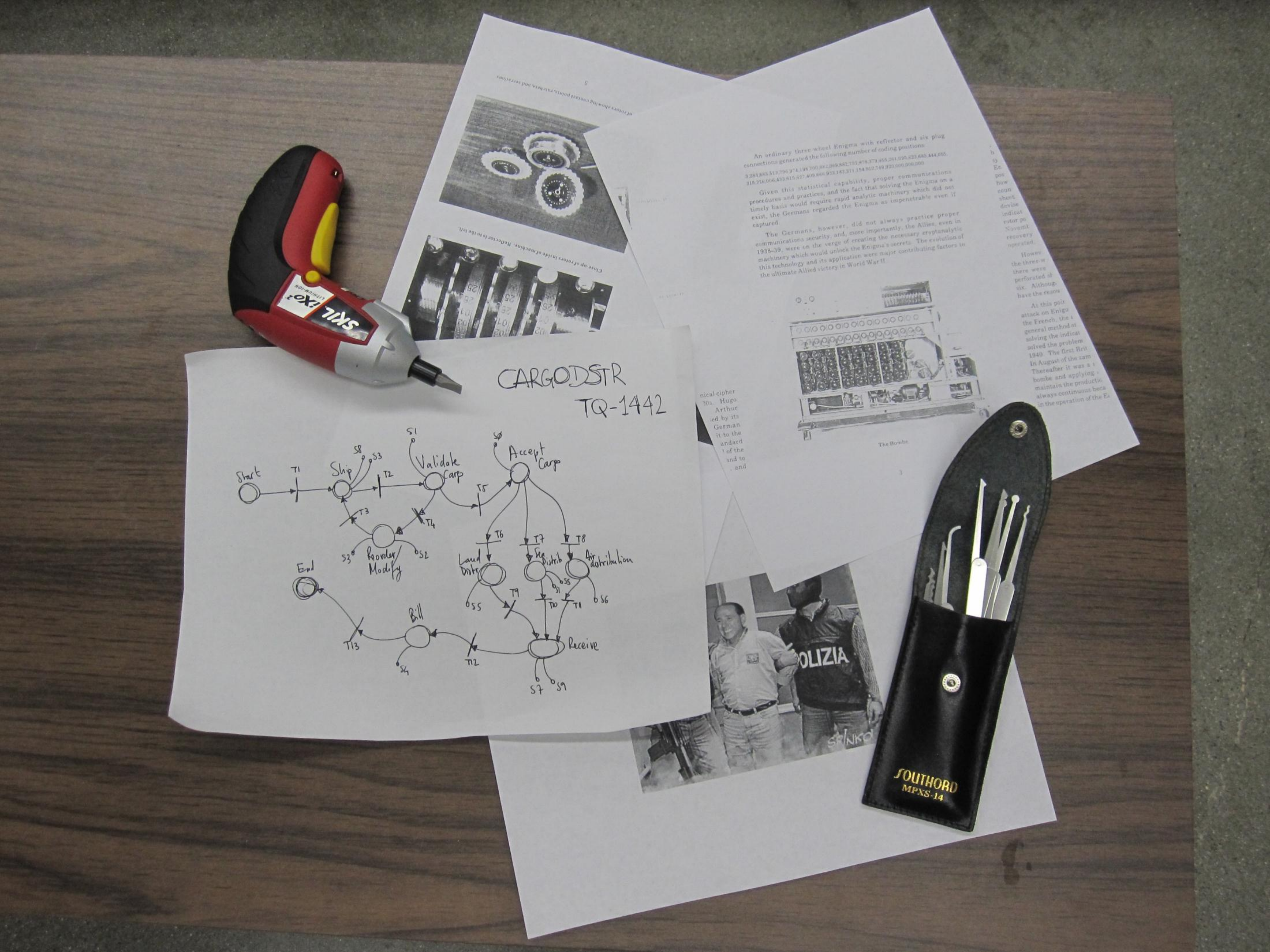
%of teams and % of points by country

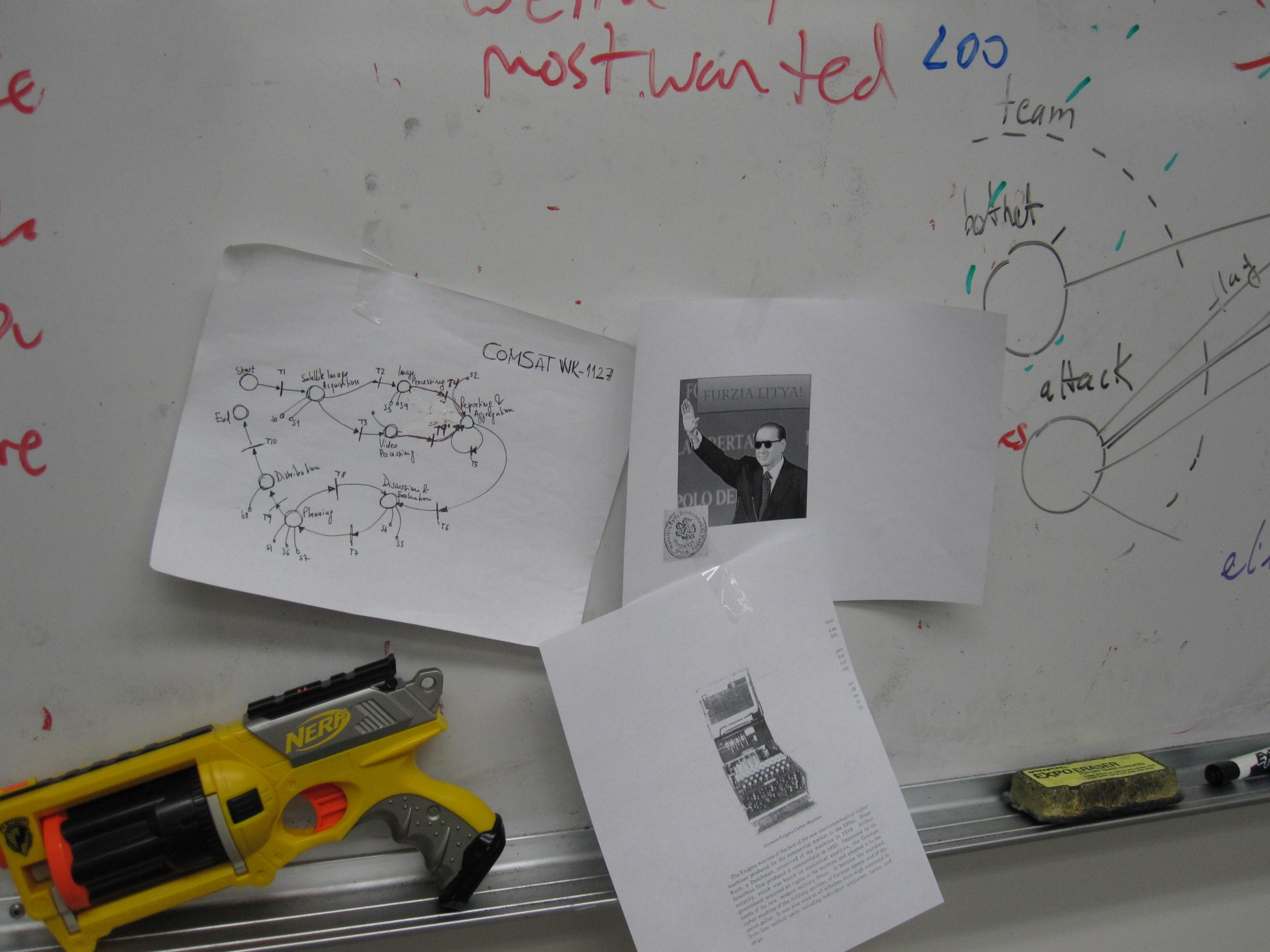
Preparing for the 2010 iCTF

- <Intentionally Left Blank>

THE 2010 iCTF SCENARIO: MISSION AWARENESS IN STATE-SPONSORED CYBERWAR

- Friday, December 3rd, 2010 from 10AM to 7PM CST
- The fake country “Litya” a play on “Italy” is a major center for illegal activities of all kinds.
- The Lityian dictator Lisvoy Bironulesk has pioneered and emplaced a botnet in every country to support Litya’s economy.
- The international community discovers this and collectively attempts to hack them and prevent this corruption.
- International spies have collected information about the Botnet and have released four pictures.

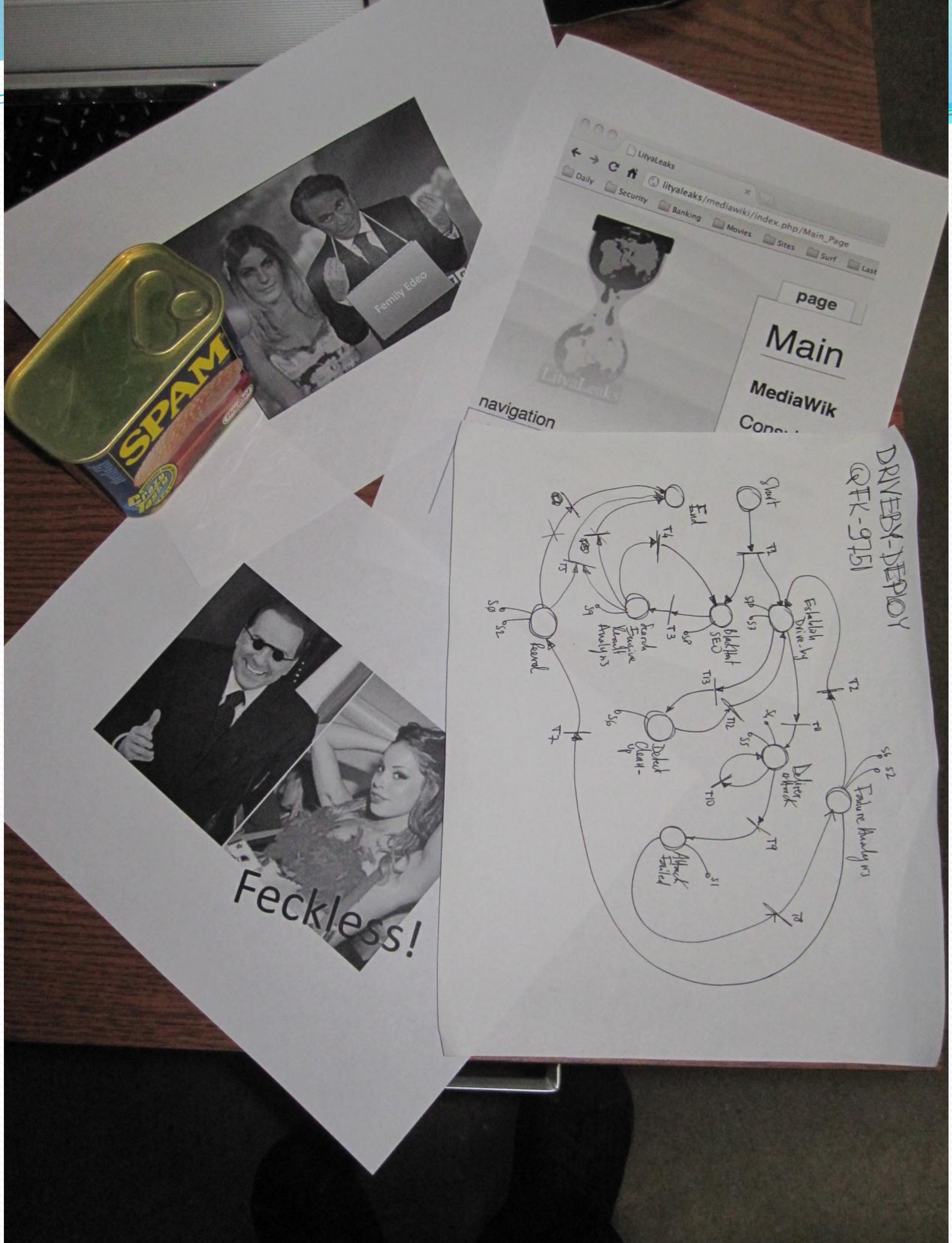

CARGODSTR
TQ-1442
Start
T1
Ship
S8
S3
T2
S1
Validate Carp
S0
Accept Carp
T5
T3
T4
Reorder/ Modify
S3
S2
T6
T7
T8
Land Distr
Sea Distrib
Air distribution
S5
S1
S6
S5
T9
T10
T11
End
Bill
T13
T12
Receive
S4
S7
S9
SKIL
iXO
POLIZIA
SOUTHORD
MPXS-14
The Bombe

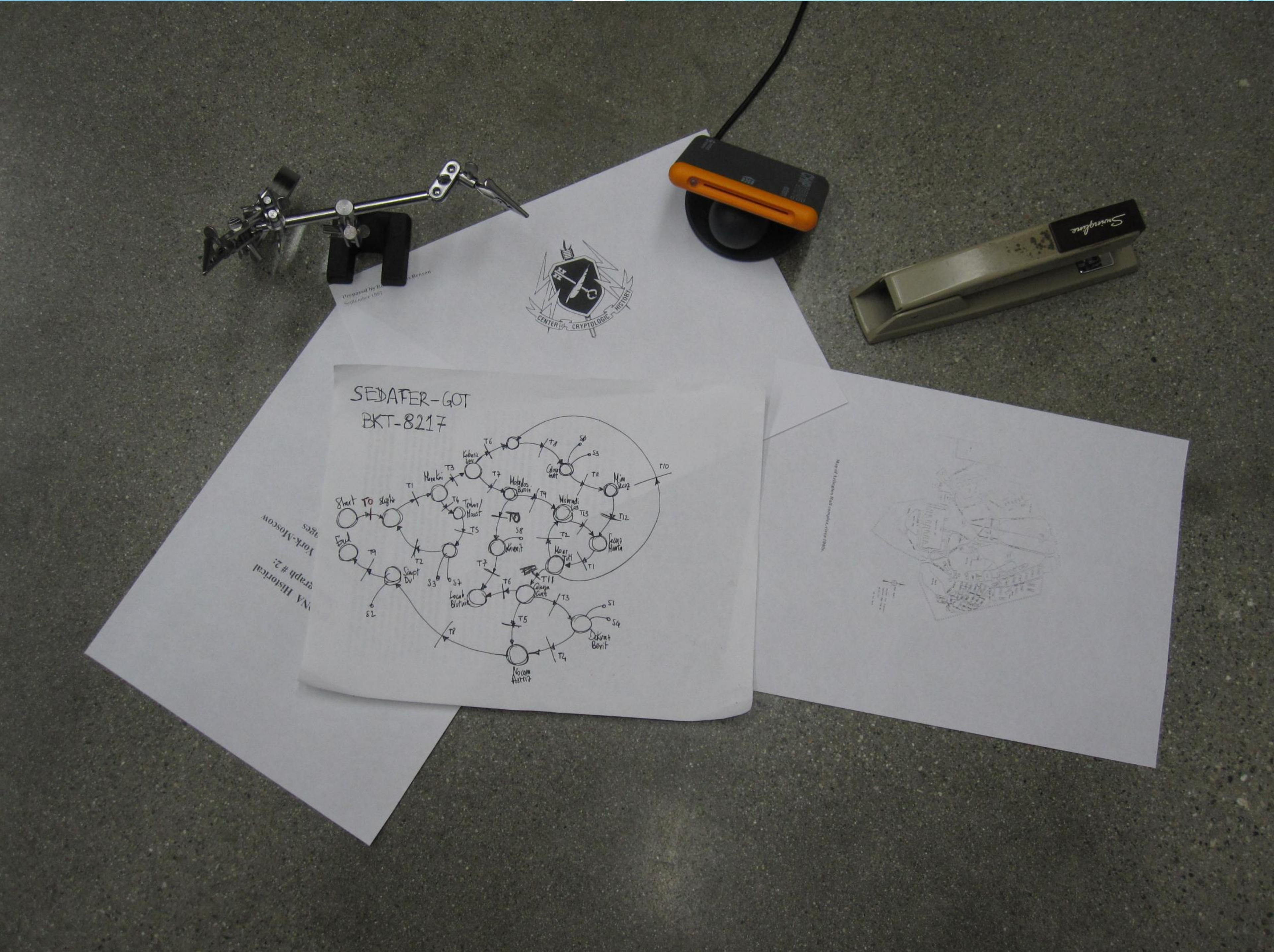


German Enigma Cipher Machine

The Enigma was one of the best of the new electromechanical cipher machines produced for the commercial market in the 1920s. Hugo Koch, a Dutchman, conceived of the machine in 1919. Arthur Scherbius first produced it commercially in 1923. Impressed by its security, which was based on statistical analysis, the German government acquired all rights to the machine and adapted it to the needs of its new, modern military forces. It became the standard cipher machine of the military services, of German agents and of the secret police. It was also used at all echelons from high command to front-line tactical units including individual airplanes, tanks, and ships.

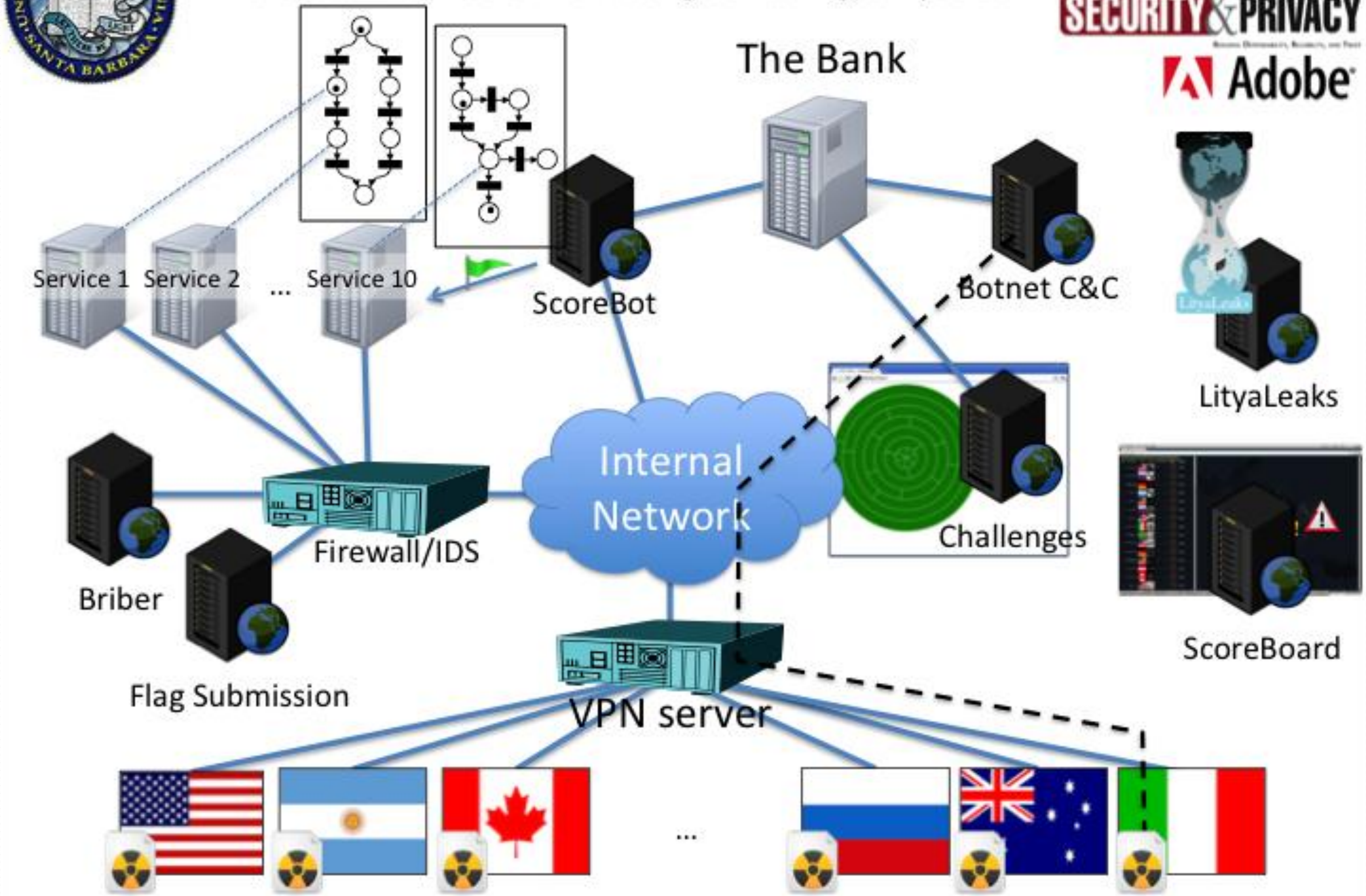
2


Femily Edeo
SPAM
LityaLeaks
Daily
Security
Banking
Movies
Sites
Surf
Last
lityaleaks/mediawiki/index.php/Main_Page
page
Main
MediaWik
Cons
navigation
LityaLeaks
Feckless!
DRIVEBY-DEPLOY
@FK-9751
Start
End
T1
T2
T3
T4
T5
T7
T8
T9
T10
T11
T12
T13
Establish Drive-by
BlackHat SEO
Search Engine Result Analysis
Reord
Detect Clean-up
Deliver attack
Attack Failed
Failure Analysis
S0
S1
S2
S3
S4
S5
S6
S8
S9


SEDAFER-GOT
BKT-8217
Start
T0
End
T9
Simpt Dv
S2
T1
Marakni
T3
Koberiz Jev
T6
T8
S0
S3
Clouthut
T11
Mim Secnz
T10
T7
Motados Buroli
T9
Nobradi Los
T13
T12
Secuz Hiarta
T4
Trohar/ Moast
T5
T2
S3
S7
T0
S8
Kavenit
T2
Moar TrH
T1
T7
T6
Locat Blutnik
T11
Canaya Cvets
T3
S1
S4
Dekrat Berit
T5
T4
T8
Nocom Astriz
CENTER CRYPTOLOGIC HISTORY
Prepared by R[illegible] Benson
September 1997
NA Historical
graph # 2:
York-Moscow
ages

72 teams from 16 countries, 900 students playing live: the UCSB iCTF is the world's largest hacking competition!

1st Prize: $1,000
Sponsored by

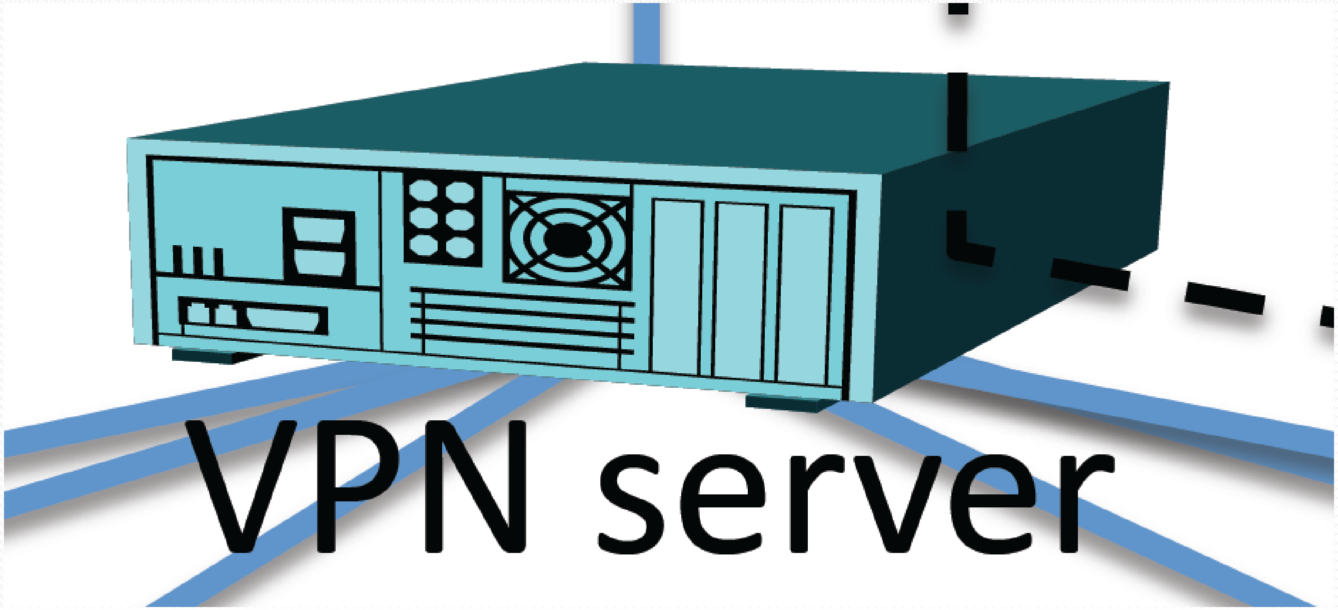


Critical Servers

- VPN Server
- ChallengeBoard
- ScoreBoard
- LityaLeaks
- Botnet C&C
- The Bank
- ScoreBot
- Firewall/IDS
- Briber
- Flag Submission
- IRC Server

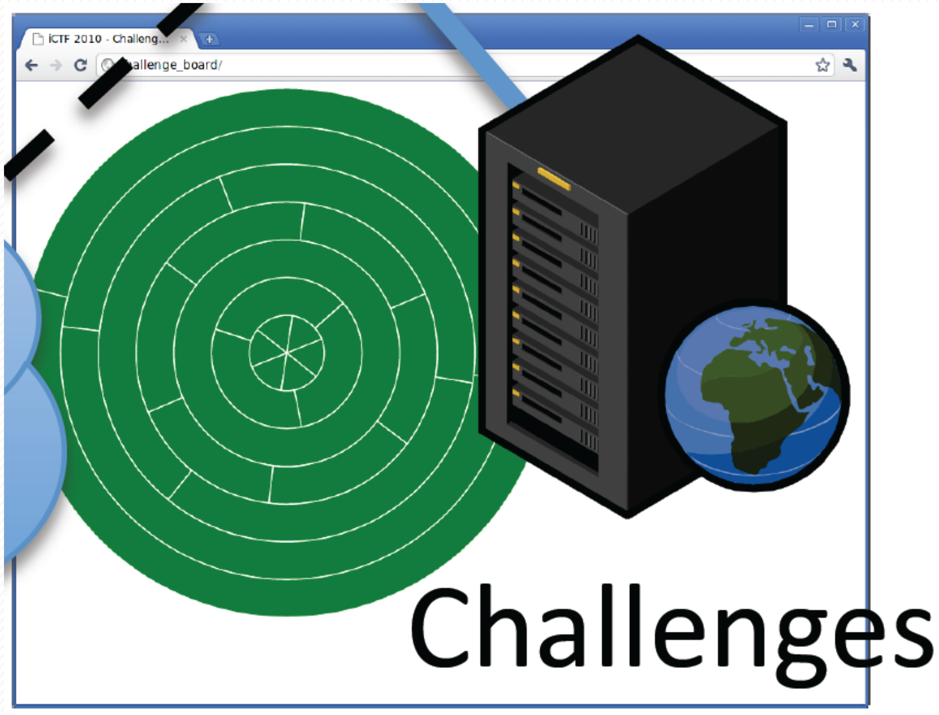
VPN Server

- Allows for a safe and secure environment so that the competition can be held.



Challenge Board

- Listed puzzles required to acquire money to participate in the botnet to score points.



Types of Challenge Board Questions

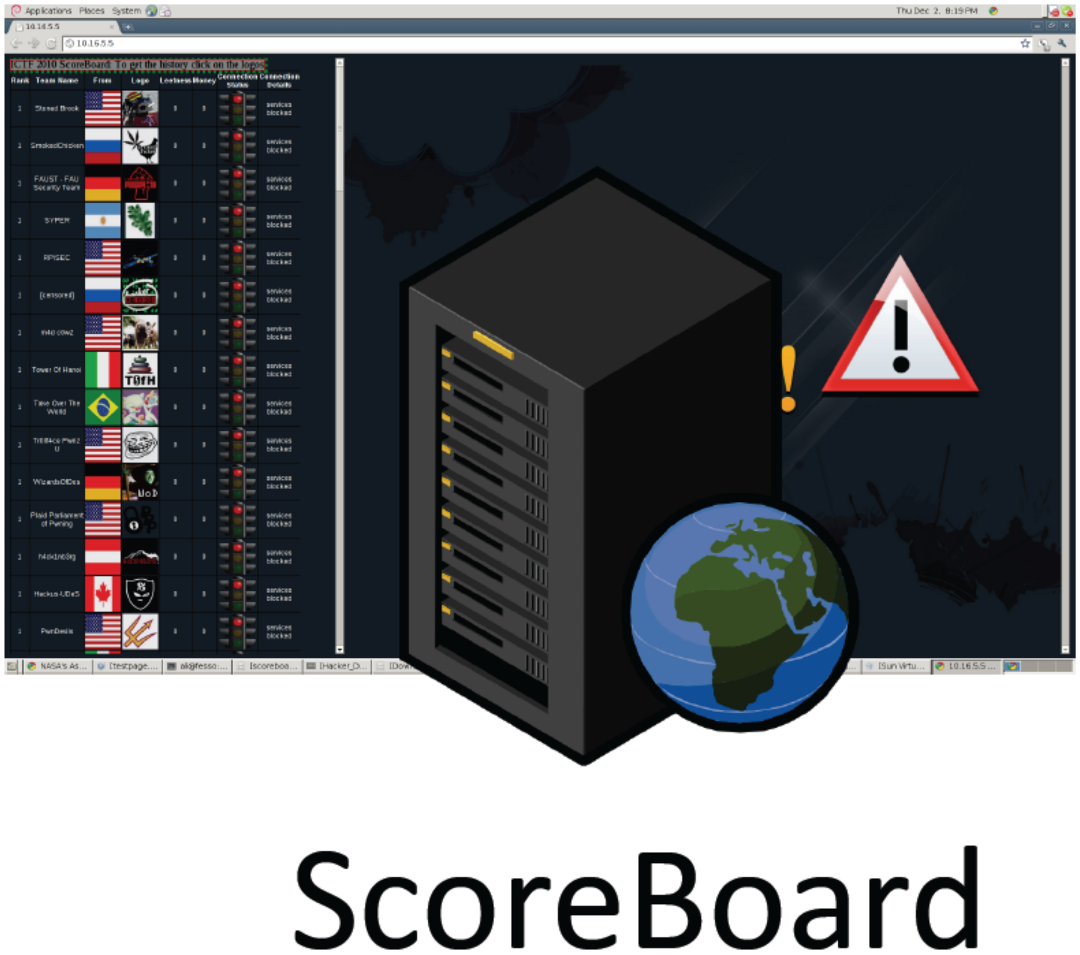
- Fully Encrypted Questions
- Wireshark pcap dumps, Your task was to extract the files and determine passwords.
- Identify people in ‘Swirled’ Pictures
- Bruteforce Archive Passwords
- Understand common cryptographic and mathematical functions
- Locate hidden file streams
- Hidden messages in pictures
- Decoding phone DTMF sounds
- Code in various languages
- Use tools such Ollydbg and IDA Pro to dissect EXE’s
- Convert and open obscure picture formats

Knowledge Required for the Challenge Boards

- US Culture was fairly helpful. (References to American culture were common place.)
- Programming and Scripting was thoroughly tested
- Cryptography
- Packet Analysis
- Image Manipulation
- Google Magic

ScoreBoard

- Keeps track of each teams Money, Points Earned, and Botnet Connection Status.
- Was hacked by two teams
- Their modifications were discarded

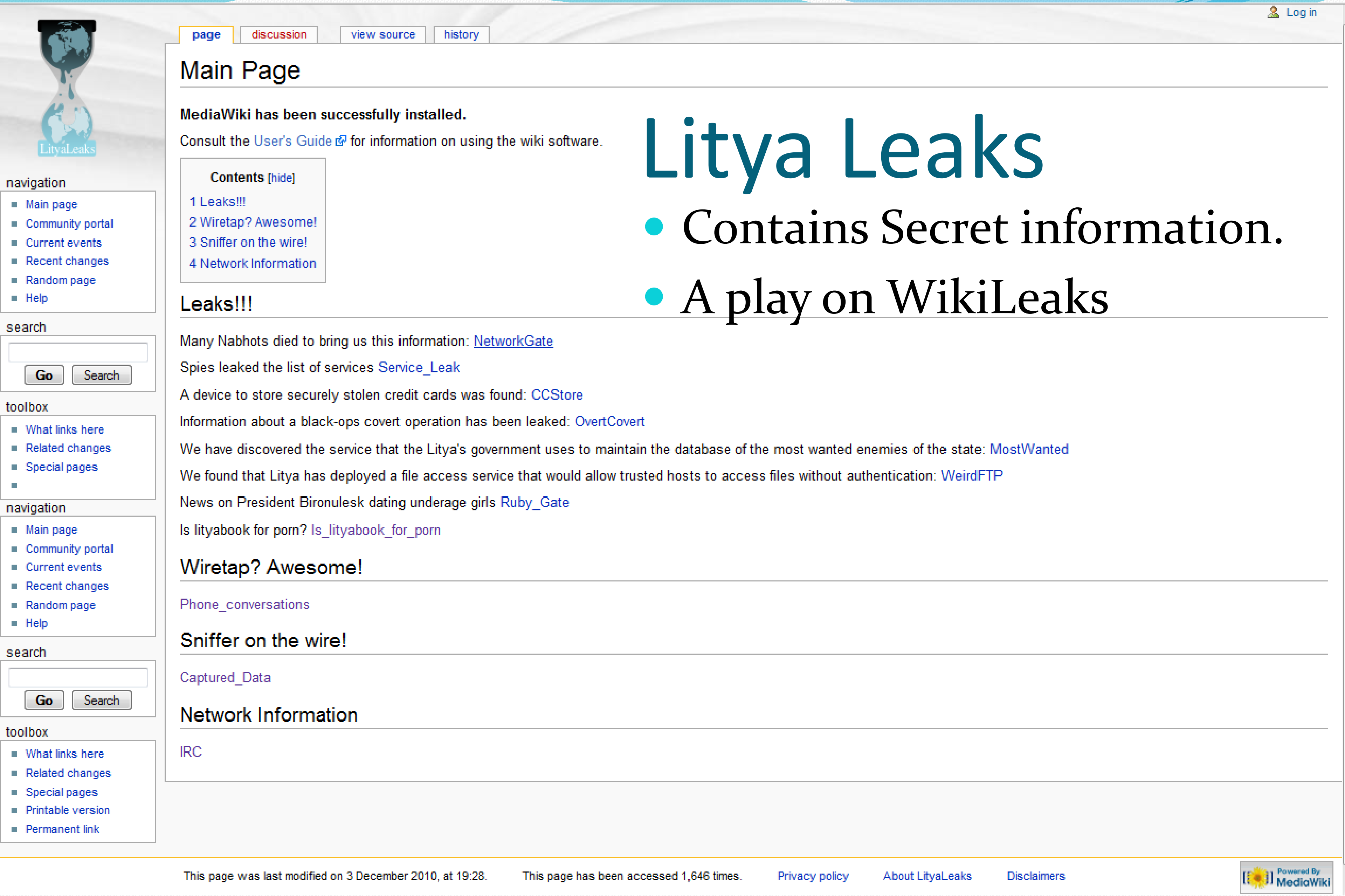


ICTF 2010 ScoreBoard: To get the history click on the logos

Rank	Team Name	From	Logo	Leetness	Money	Connection Status	Connection Details
1	Stoned Brook			0	0		services blocked
1	SmokedChicken			0	0		services blocked
1	FAUST - FAU Security Team			0	0		services blocked
1	SYPER			0	0		services blocked
1	RPISEC			0	0		services blocked
1	[censored]			0	0		services blocked
1	m4d c0w2			0	0		services blocked
1	Tower Of Hanoi			0	0		services blocked
1	Take Over The World			0	0		services blocked
1	Tr0ll4ce Pwn2 U			0	0		services blocked
1	WizardsOfDos			0	0		services blocked
1	Plaid Parliament of Pwning			0	0		services blocked
1	h4ck1nb3rg			0	0		services blocked
1	Hackus-UDe5			0	0		services blocked
1	PwnDevils			0	0		services blocked

Litya Leaks

- Contains Secret information.
- A play on WikiLeaks



Main Page

MediaWiki has been successfully installed.

Consult the User's Guide for information on using the wiki software.

Contents [hide]

1 Leaks!!!
2 Wiretap? Awesome!
3 Sniffer on the wire!
4 Network Information

Leaks!!!

Many Nabhots died to bring us this information: NetworkGate

Spies leaked the list of services Service_Leak

A device to store securely stolen credit cards was found: CCStore

Information about a black-ops covert operation has been leaked: OvertCovert

We have discovered the service that the Litya's government uses to maintain the database of the most wanted enemies of the state: MostWanted

We found that Litya has deployed a file access service that would allow trusted hosts to access files without authentication: WeirdFTP

News on President Bironulesk dating underage girls Ruby_Gate

Is lityabook for porn? Is_lityabook_for_porn

Wiretap? Awesome!

Phone_conversations

Sniffer on the wire!

Captured_Data

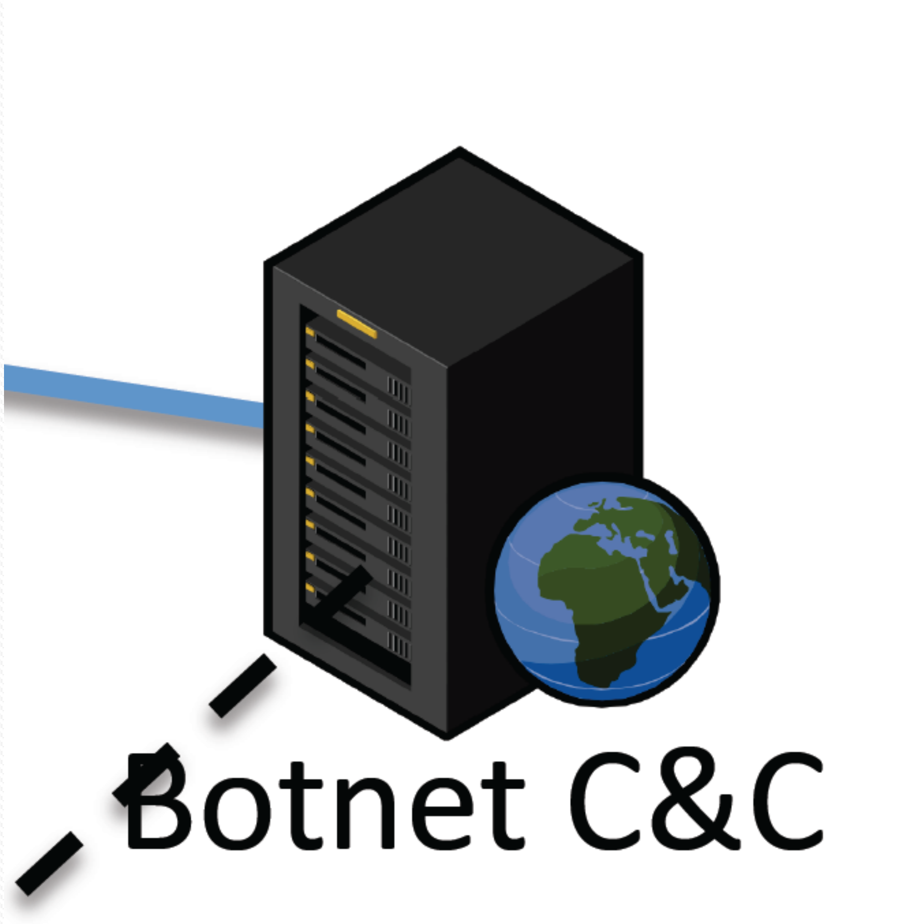
Network Information

IRC

This page was last modified on 3 December 2010, at 19:28. This page has been accessed 1,646 times. Privacy policy About LityaLeaks Disclaimers

Botnet C&C

- Gradually drains money from people connected to the Botnet.

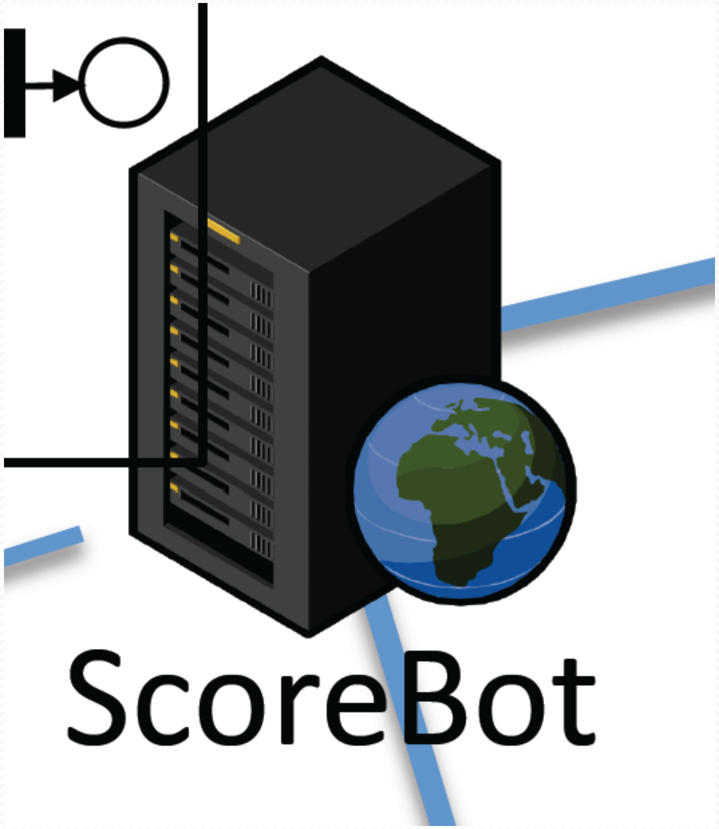


The Bank

- Provides a web interface to buy time on the Botnet.

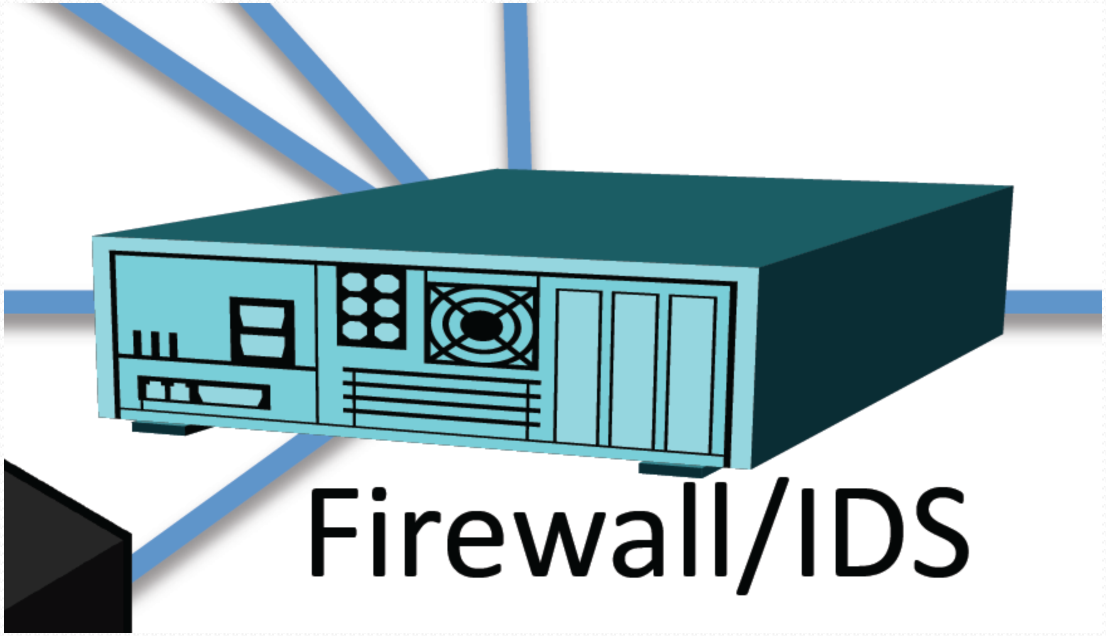
ScoreBot

- Adds points to the ScoreBoard server.



Firewall/IDS

- Deducts points for abusive traffic.
- Issues temporary and permanent bans

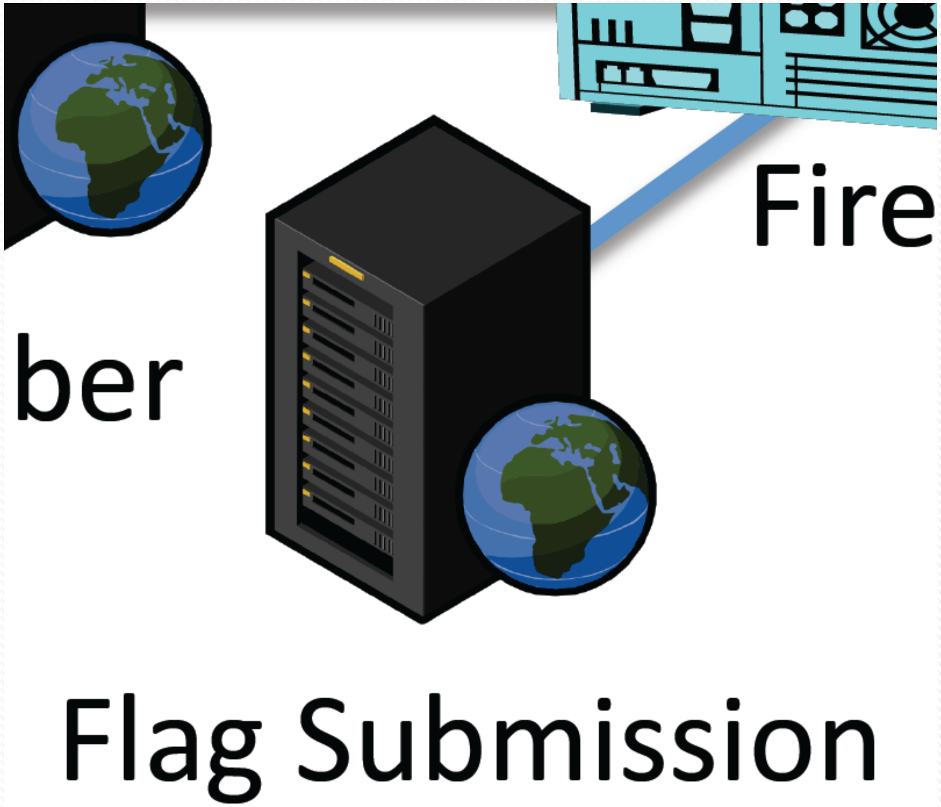


Briber

- Provides an interface to bribe corrupt Lityan Government officials to lower firewalls.

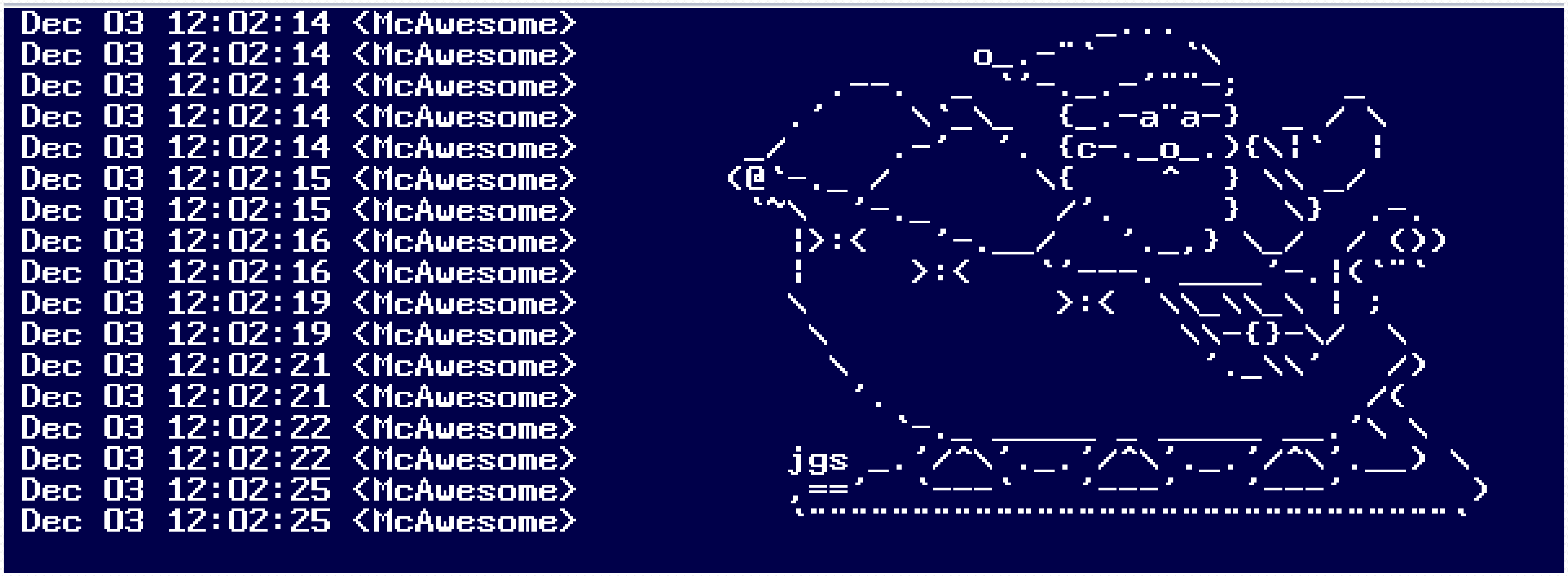
Flag Submission

- Provides an interface to submit successfully stolen flags and to gain points.



IRC Server

- Used to communicate between all participants and UCSB officials.



```
Dec 03 12:02:14 <McAwesome>                         _...
Dec 03 12:02:14 <McAwesome>                   o_.-"`    `\
Dec 03 12:02:14 <McAwesome>            .--.  _ `'-._.-'""-;     _
Dec 03 12:02:14 <McAwesome>          .'    \`_\_  {_.-a"a-}  _ / \
Dec 03 12:02:14 <McAwesome>        _/     .-'  '. {c-._o_.){\|`  |
Dec 03 12:02:15 <McAwesome>       (@`-._ /       \{    ^  } \\ _/
Dec 03 12:02:15 <McAwesome>        `~\  '-._      /'.     }  \}  .-.
Dec 03 12:02:16 <McAwesome>          |>:<   '-.__/   '._,} \_/  / ())
Dec 03 12:02:16 <McAwesome>          |     >:<   `'---. ____'-.|(`"`
Dec 03 12:02:19 <McAwesome>          \            >:<  \\_\\_\ | ;
Dec 03 12:02:19 <McAwesome>           \                 \\-{}-\/  \
Dec 03 12:02:21 <McAwesome>            \                 '._\\'   /)
Dec 03 12:02:21 <McAwesome>             '.                       /(
Dec 03 12:02:22 <McAwesome>               `-._ _____ _ _____ __.'\ \
Dec 03 12:02:22 <McAwesome>          jgs _.'/^\'._.'/^\'._.'/^\'.__) \
Dec 03 12:02:25 <McAwesome>          ,=='  `___`   ,___'   ,___'      )
Dec 03 12:02:25 <McAwesome>          `""""""""""""""""""""""""""""""",
```

Non Critical Servers

- LityaBook
- LityaHot
- PerlCGI
- BinCGI
- Applet
- Idreamofjeannie
- Mostwanted
- Overtcovert
- weirdtcp

Offensive Actions

- Find servers
- Exploit services
- Find information about the actions of the Lityan Government.
- Solve Puzzle Challenges to acquire money to participate in the Botnet that supports the Lityan economy and hack them.
- Bribe corrupt officials of the Lityan Government to lower firewall restrictions allowing you to score points when you submit flags.

Defensive Actions

- Secure your botnetted server by changing the default password.
- A few teams did not do this, and it is not against the rules to attack them.
- You can lose points if you submit flags at the incorrect time.

Starting the Day off Right

mtn DEW

Back Up My PC
APC

In the Beginning (N00bz G4l0r3)

- People brought in their desktops and laptops from home, imaged the STEAL computers with fresh soon to be infected installations of Windows.
- Newbies as far as the eye can see (Only two team members had competed previously)
- Rough Start (People had to connect to the network, connect to the IRC server, Deal with DNS server issues, and Connect to the Challenge Server all while trying to figure out the main goals of the game.)

Mid-Way (Divide and Conquer)

- File Getters
- 2-4 Attackers
- Coordination and Puzzle Solving
- What Goes up, Must come down
  - The high number of teams created heavy traffic loads causing the connectivity to the critical servers to be sporadic.

A Demonstration of a Moderately difficult Challenge Question

- You are provided with a file called Aliens.tgz
- And the question asks "What was the aliens message as they traveled the earth?“
- 1. Open with 7zip
- 2. Script the extraction
- 3. Find the final file
- 4. Stalk the file creator
- 5. Discover the filenames are actually flickr photo id numbers
- 6. Collect GPS Coordinates
- 7. Map the coordinates

How we gained Offensive points

- Steve Left…
- We telneted into the ‘MostWanted’ Server (A SQL Lite Database that stores a picture of a person in a table with a matching name.
- A python socket was established and SQL injection code was sent across to retrieve the file secret.txt which contained a flag which was then used to gain points by bribing the officials and sending the flag to the right server at the right time according to the leaked map in one of the four original pictures.
- Methods to automate the process were not attempted for fear of losing points.

Various Hazards to competing in the iCTF.

- Starvation (JJ Came to the Rescue)
- Over Caffeination (Monster, Mountain Dew, Coffee)
- Carpal tunnel
- Confusion leading to onset headaches
- Information Overload
- Exposure to boot camp style motivational speeches
- Excessive High Fiving
- Near-guaranteed infection of computers connected to the VPN. (Our shared USB drive and File Share to transfer tools for hacking became infected.)

Final Thoughts

- 2nd out of 26 US teams
- 7th out of 73 world teams
- Scored 4% of total points
  - Compare 14% CMU
- 12% of US points
  - Compare 39% CMU
- Being more prepared for the competition would have helped considerably.

Special Thanks

- University of California Santa Barbara
- NUCIA Faculty and Staff
- University of Nebraska
- Steve Nugen
- Robin Gandhi
- Lucas Wentz
- Bill Mahoney
- Aaron Keck
- Derek Pecka
- And anyone else we may have forgotten.

Questions?

Contact Information

- Michael Kunz – mtkunz@unomaha.edu
- Tory Cullen – tjcullen@unomaha.edu
- Adam Gehringer - ajgehringer@unomaha.edu

Resumes Available