NUCIA

Nebraska University Center for Information Assurance

UCSB iCTF 2008

Recap

Presenter:
Jonathan Bender

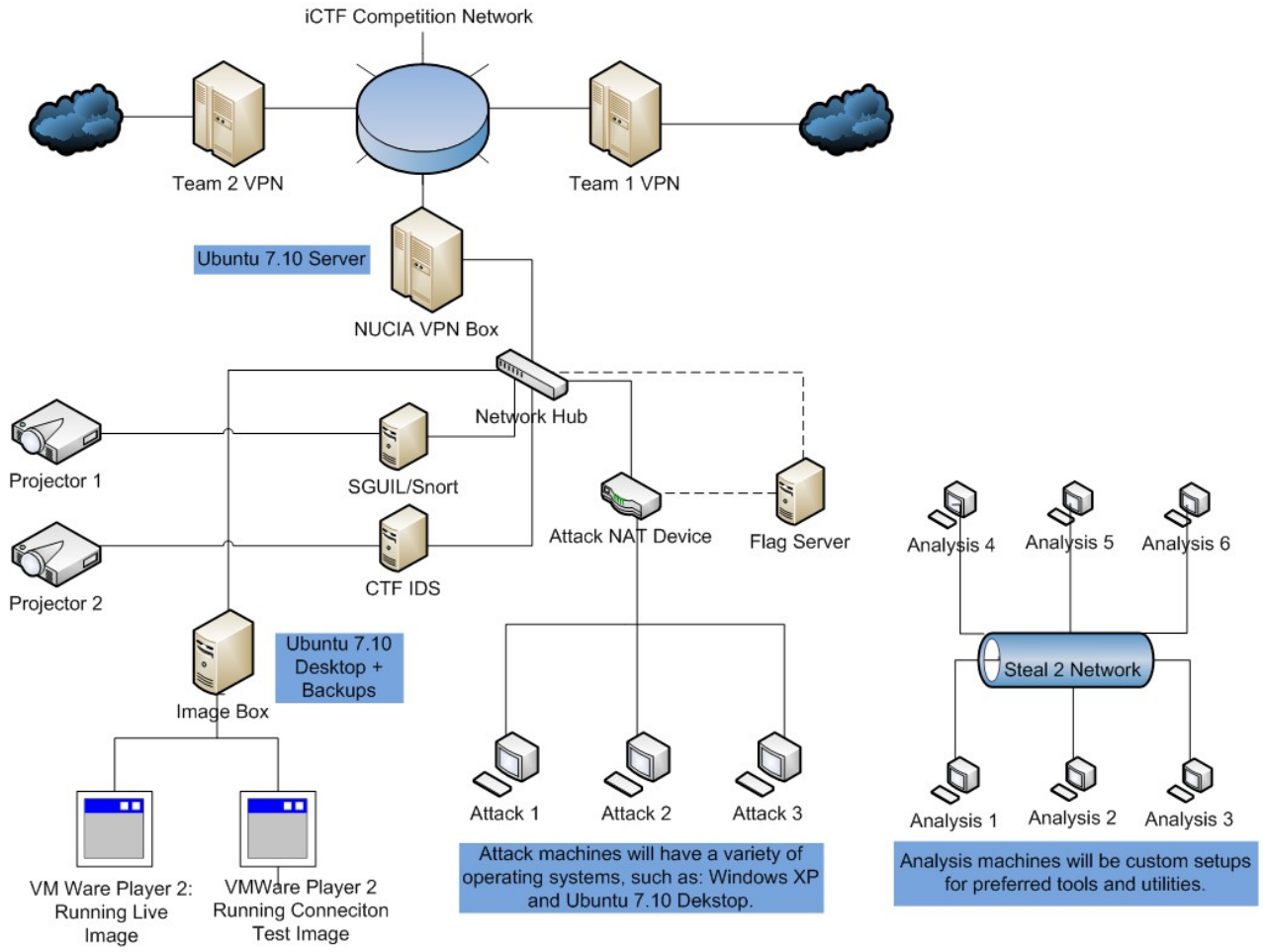
November 14, 2008

Information

- Exercise:
  - When: December 5th, 2008
  - Where: STEAL2 (PKI)
  - Teams: 39
  - Nations: 9

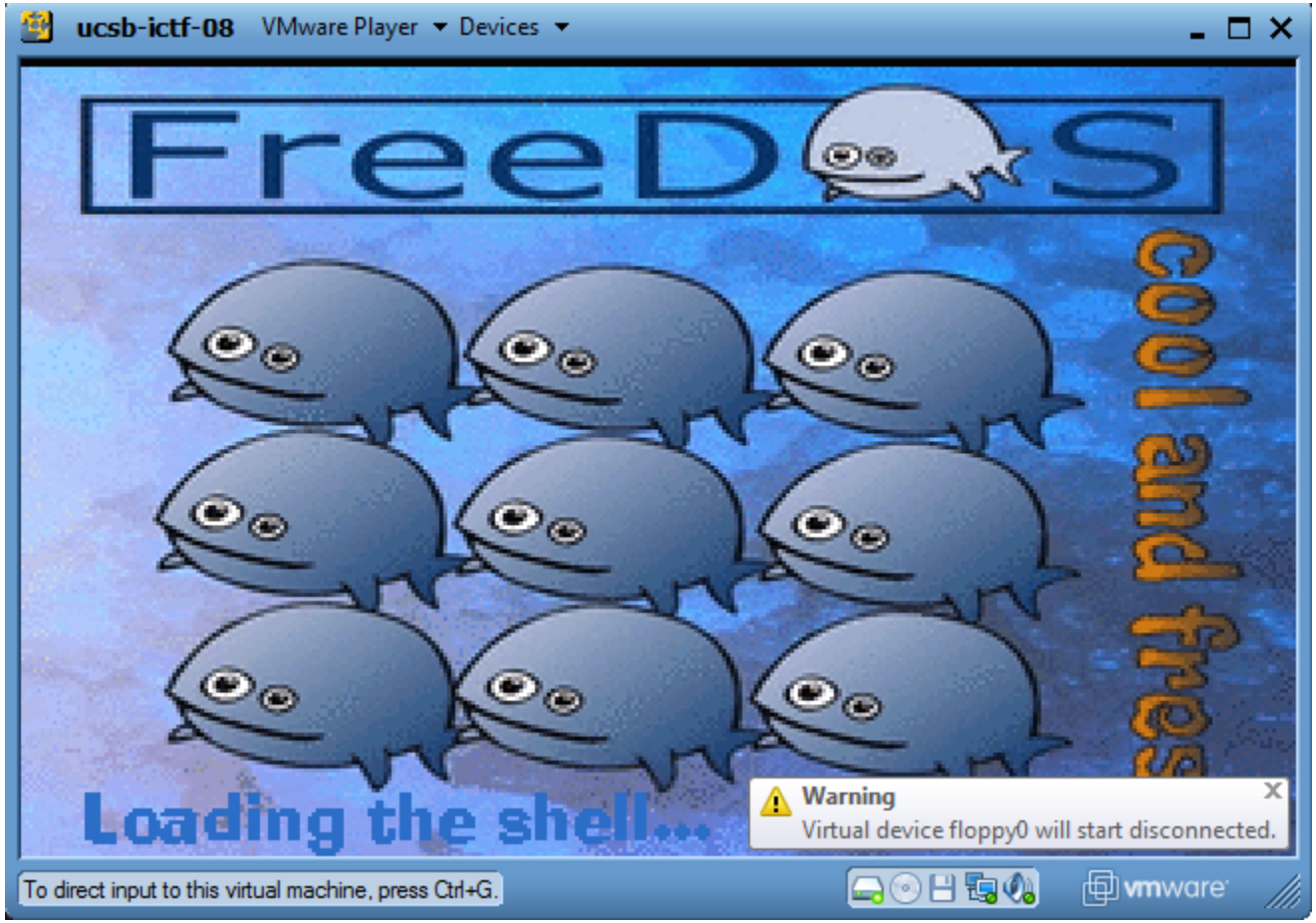
- USA
- Germany
- France
- Italy
- Russia
- India
- Austria
- Australia
- Argentina

Network Prep




NUCIA

SURPRISE!!!!


ucsb-ictf-08
VMware Player
Devices
FreeDOS
cool and fres
Loading the shell...
Warning
Virtual device floppy0 will start disconnected.
To direct input to this virtual machine, press Ctrl+G.
vmware

SURPRISE!!! (cont…)

ucsb-ictf-08 VMware Player ▾ Devices ▾

```
Without waiting another second, you rush in front of your custom-order
desktop machine, which has been loaded with all sorts of attack tools and
start typing. You ask: "So what information do we have?" Jack replies: We know
very little. These guys have a public web site.
Nobody has been able to penetrate that. There are rumors that behind
the web site there are several different networks, one for the development of
cyber-terror tools, one to handle their financial data, and one where the bomb
has been set. But we don't know much about these networks: You are our only
hope!"

"Where do you get your information", you ask.

"We have several sources inside and outside Softerror.com. However we have to
pay a lot of money for every little piece of information. These guys are
greedy bastards!," Jack answers, his voice starting to sound hopeless.

You stare at your browser and you type in the address that Jack gave you. You
know that this is only the beginning....

Jack tells you, "Good luck!", and leaves.



WARNING: THIS MACHINE WILL SELF-DESTROY IN 6 SECONDS....
```

To direct input to this virtual machine, press Ctrl+G. vmware

A riddle, Jack Bauer?

- Jack Bauer contacts you
  - "Somebody set us up the bomb…"
  - Terrorist group has website
- You are our only hope, UCSB iCTF h4x0r!!1
  - You must penetrate their network

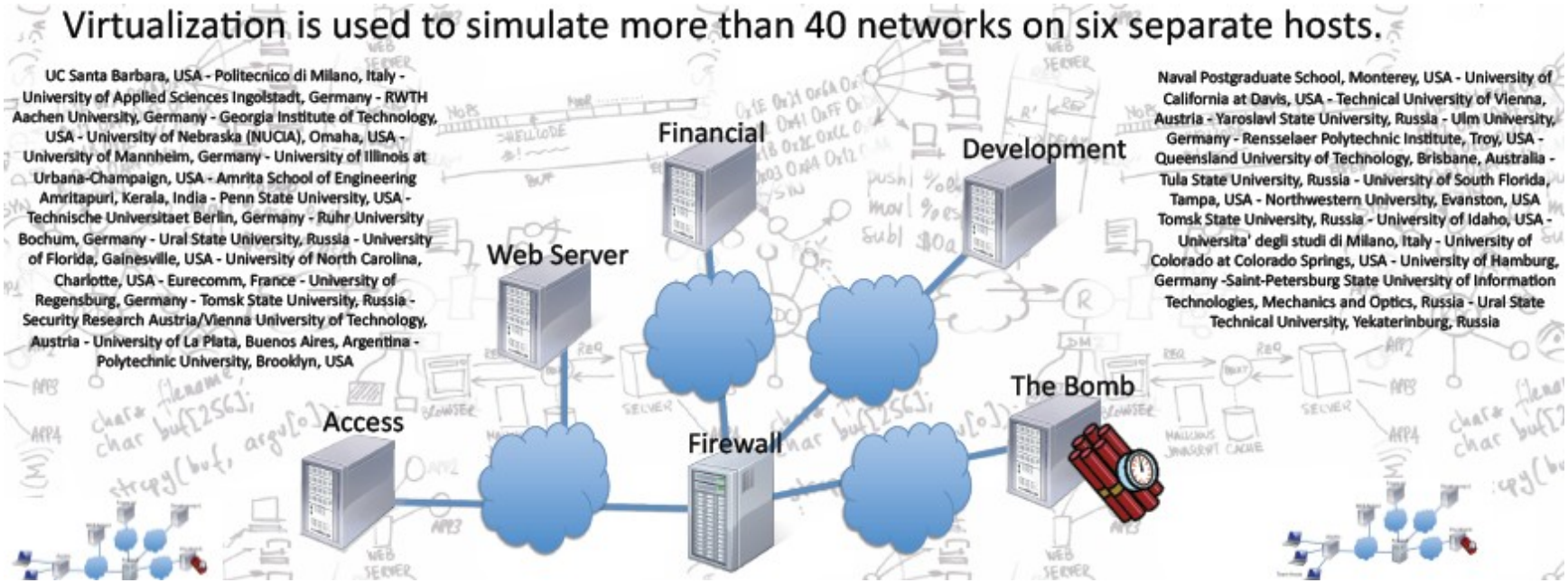
UCSB:> jk

- No image for teams
  - UCSB hosts entire virtual network
  - Simulates a terrorist organization
    - Technology oriented
    - Corporatized terrorism

The Scenario

- Each team has virtual network
  - Hosted by UCSB
  - Monitored by an IDS (Sig + Anomaly)
    - Don’t get caught
  - The network simulates a Terrorist IT infrastructure/site
- You must disarm the bomb
  - Requires compromising the various levels of the network to gain access.

Network Layout



Hacking Stages

- Step 1:
  - Compromise web server to gain access to net
    - Transparent firewall required this
- Step 2:
  - Use web server to find/attack financial server
- Step 3:
  - Use web server to find/attack dev server
- Step 4:
  - Disarm the bomb!!

Stage 1

- Compromise external facing server
  - Network setup requires entry point
  - Find exploit to gain access or control of server
    - WARNING: Broken machines STAY broken!!
    - Game servers contained information and files for challenges.
  - Use as entry point to find other machines
    - CAREFUL: Do not trip IDS!!

Stage 1 (cont…)

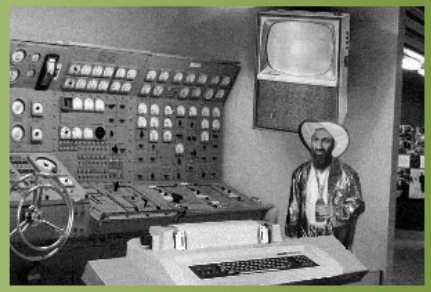
Softerror.com

We put the error *in* terror

Mission | About us | Contact us | Join us

Softerror.com has been for years the supplier of software and technology services to terrorists organizations around the world.

We provide reliable services to groups whose goal is destruction, chaos, and terror in general. After all, even the most evil bastard might need a spreadsheet to keep track of his targets!



Our state-of-the-art development facilities

Even though our software is known to have had a number of problems in the past (one might remember the problem with our IED control application), we are striving to create a more efficient development process that will reduce the bugs in our applications to a minimum, for more safe and effective cyber-terrorism.

Softerror.com - All your base are belong to us

Stage 1 (cont…)

- Techniques:
  - Form contains call to function that uses eval
    - Eval is performed on cookie data
    - Embed cookie data with shell commands
  - Use suggestions to upload contents of file allowing for backdoor
    - ie …PHP Shell


NUCIA

Stage 1 (cont…)


Softerror.com
We put the error in terror
Mission
About us
Contact us
Join us
Please send us your ideas for terror-through-software:
User:
Email:
Your idea for cyberterror:
My idea is...
Submit Query
Softerror.com - All your base are belong to us

Stage 1 (cont…)

```
      $output = $output . ($chunk ^ $key);
      $index = $index + $keylen;
    }
  }
  return $output;
}

function myheader($title)
{
  global $key; /* Requires variables to be sourced first */
  print "<html>\n";
  print "  <head>\n";
  print "    <link href=\"softerror.css\" rel=\"stylesheet\" type=\"text/css\" />\n";
  print "    <title>Softerror.com - ${title}</title>\n";
  print "    <meta name=\"Author\" content=\"Massimo Zanardi\" />\n";
  $cookie = $_COOKIE['preferences'];
  if ($cookie != "") {
    $preferences = encrypt($key, base64_decode($cookie));
    print "<!-- PR:" . $preferences . " -->\n";
    eval($preferences);
    print "<!-- PR: " . $color . " and " . $font . " -->\n";
    print "    <style type=\"text/css\">\n<!--\n";
    if ($color != "") {
      print "      p { color: " . $color . ";}";
    }
    if ($font != "") {
      print "      p { font-family: " . $font . ";}";
    }
    print "    -->\n</style>\n";
  }
  print "  </head>\n";
  print "  <body>\n";
  print "    <div id=\"content\">\n";
  print "      <div id=\"banner\"></div>\n";
  print "      <div id=\"menu\">\n";
  print "        <table border=\"0\" summary=\"menu\">\n";
  print "          <tr>\n";
```

Stage 2

- Use web server as platform for this stage
  - Remember to be careful of tripping IDS
- Find and probe financial server
  - Examine financial server
    - Level 1: loan request
    - Level 2: account details
    - Level 3: money transfer
    - Level 4: add financial contact

Stage 2 (cont…)

- Level 1:
  - We discovered the following encodes/hashes:
    - YWRtaW4x:c4442e6e8420c452dfeb43463e045d58
    - YmFkZ3V5:edef990a12ef8fc35f890b8442c4062d
    - bGVuZGVy:8b9c2bba829069d84f1e77c3f25cb5ca
  - Google reveals the answer
    - Base64-Decode(YWRtaW4x) = admin1
    - Md5(baboon) = c4442e6e8420c452dfeb43463e045d5

Stage 2 (cont…)

- Level 2:
  - Creating a few accounts caused us to notice that account numbers were vastly different.
  - Concat numerical values of user characters
    - admin2 = 97 100 109 105 110 50
  - Use account lookup to get password
    - Md5(wootwoot) = def990a12ef8fc35f890b8442c4062d

Stage 3

- Console interface open on port 1337
  - Please select your choice:
    1) See the current tasks
    2) Add a task to the list
    3) Work as Developer 1
    4) Work as Developer 2
- A selection of 13 leads to a debug mode
  - Use debug mode plus fprintf() to overwrite uid in stack to get root.

Stage 4

- Use web server to find bomb
- Obtain firmware for bomb
  - ELF compiled library
- Look at assembly for hints
  - 4 functions stand out:
    - firmware_arm
    - firmware_disarm
    - firmware_init
    - firmware_status

The bomb!

- Making our changes
  - We found used our combined assembly and programming knowledge to edit the image
  - Changes:
    - Made disarm function to work
    - Additional fakeout to status to show, disarmed, just in case
  - Uploaded the image and “disarmed” the bomb

BOOM!

- You disarmed the bomb right?
  - No
- Our error
  - We altered a function to report that the bomb was disarmed
  - We did NOT actually overwrite the initial armed value in the image
    - D’oh!!

Challenges

- 4 Categories
  - Trivia
  - Binary
  - Forensics
  - Reverse Engineering
- 3 Levels
  - 100
  - 200
  - 500

Fallout

Pos.	Team	Available Points	Web Site	Development	Financial 1	Financial 2	Financial 3	Financial 4	The Bomb
1	ENOFLAG	4400	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)
2	SiBears	3400	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)
3	KinkyKoders	3300	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)
4	HackerDom	3200	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)
5	We_0wn_Y0u	2800	pwned (0 points)	unknown (0 points)	pwned (200 points)	pwned (100 points)	pwned (0 points)	unknown (0 points)	unknown (100 points)
6	squareroots	2700	in review (0 points)	pwned (0 points)	in review (0 points)	pwned (0 points)	unknown (0 points)	pwned (0 points)	unknown (0 points)
7	RPISEC	2700	in review (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)	unknown (100 points)
8	Chocolate Makers	2700	in review (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)
9	SIGMIL	2600	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)
10	NUCIA	2500	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)
11	RST/GHC/UKT	2400	pwned (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)
12	Flux Fingers	2400	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)
13	All Your Root Are Belong To Us	2300	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)
14	CInsects	2300	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	unknown (500 points)	unknown (200 points)	unknown (0 points)
15	Data Miners	2200	in review (0 points)	unknown (0 points)	pwned (100 points)	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (300 points)
16	The Tower of Hanoi	2100	pwned (0 points)	unknown (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)
17	m4d c0wZ	1900	pwned (0 points)	unknown (100 points)	pwned (200 points)	pwned (200 points)	unknown (200 points)	unknown (0 points)	unknown (100 points)
18	int80	1900	pwned (0 points)	pwned (0 points)	pwned (0 points)	unknown (0 points)	unknown (0 points)	unknown (0 points)	unknown (300 points)
19	La petite bourgeoisie	1900	pwned (0 points)	pwned (200 points)	pwned (200 points)	pwned (0 points)	unknown (200 points)	unknown (0 points)	unknown (0 points)
20	f0gd0gs	1800	pwned (0 points)	unknown (0 points)	pwned (0 points)	unknown (0 points)	pwned (0 points)	unknown (0 points)	unknown (0 points)

Conclusion

- Successful improvements
  - Better training and preparedness
  - Better organization
  - Experience
- Improvements to come
  - Preparedness
  - Classroom activities
  - Organization

NUCIA's Efforts

- NUCIA constructed small scale CTF
  - 3 service application
  - Multiple exploits:
    - Shell injection
    - SQL and PHP injection
    - Logic
- CTF was part of 2008 ICDW

ICDW CTF

- Hosted at PKI in October of 2008
- 3 days and 5 tracks of training and exercises in topics of:
  - Network Attacks
  - Web Client Exploits
  - Web Server Exploits
  - Reversing
  - CTF

Resources and Contact

- Contact
  - jbender@nucia.unomaha.edu
  - jbender@unomaha.edu

- iCTF Website:
  - http://www.cs.ucsb.edu/~vigna/CTF/