UNIVERSITY OF NEBRASKA AT OMAHA

COMPETITIVE HACKING: NULLIFY’S ORIGINS

Nick Beede – Senior IA Major

Tory Cullen – Potentially Graduated CS & IA Major *

Michael Kunz – Potentially Graduated IA Major *

Justin Roberts – Potentially Graduated IA Major *

* -- Currently awaiting final grades from Mr. Steve Nugen

OVERVIEW

NULLify Founding
CTF Competitions
NUCIA
CSAW CTF
RWTHCTF
ICTF
ISU CDC
IFSF CTF
Plaid CTF
Future Goals

NULLIFY

NULLIFY FOUNDING – BEGINNING AT DEFCON 19

DEFCON

- Las Vegas, NV
- Place for security-minded people to share experiences and learn
- Pink mohawks and gadgets galore
- Presentations from experts in the security world
- Feeling of belonging to a community

A LITTLE INSPIRATION FROM DEFCON19

- Beat to 1337: Create a successful university cyber defense organization
  - By Mike Arpaia & Ted Reed
- Provided inspiration to create a student led computer security organization

NULLIFY FOUNDING – CAPTURE THE FLAG COMPETITIONS

CAPTURE THE FLAG (CTF) COMPETITIONS

- Hosts: various universities and organizations
- Usually last 24-48 hours, non-stop
- As few as 8 and as many as 204 teams
- Two Genres
  - Attack/Defend
  - Challenge-Based

KEY PERFORMANCE INDICATORS

- Number of active members
- Participation in CTF Competitions
- Placement in CTF Competitions
- Extra curricular activities

NEBRASKA UNIVERSITY CENTER FOR INFORMATION ASSURANCE (NUCIA)

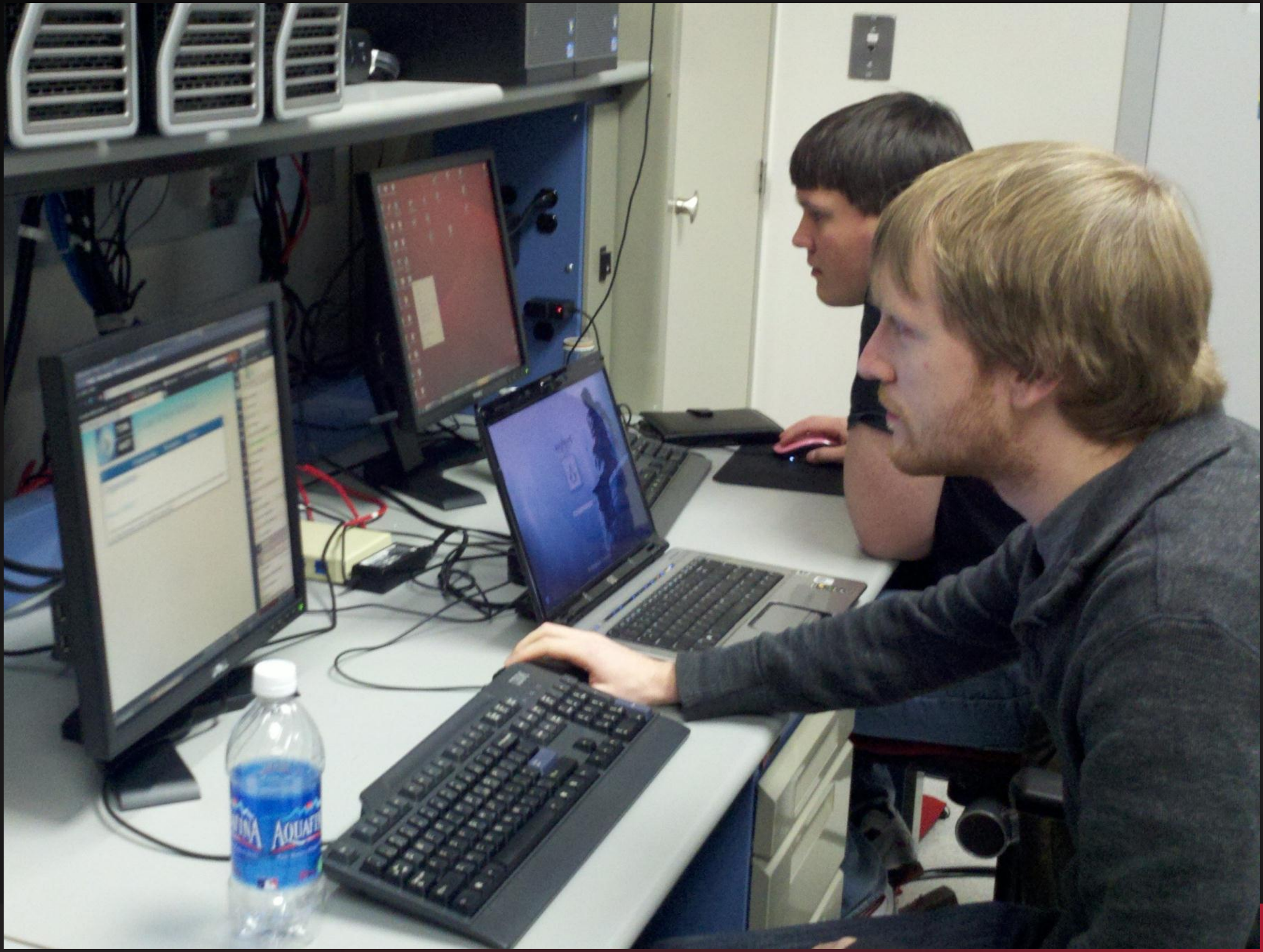
- NSA National Center of Academic Excellence in Information Assurance Education
- Bachelor’s Degree in Information Assurance is available
- Master’s Degree in Information Assurance is available beginning in Fall 2012

STUDENT TECHNOLOGY EDUCATION AND ANALYSIS LABS (STEAL)

- 3 physical labs, one virtual
- Isolated from the Internet and no writeable media may connect to the network
- Students are able to image computers with any environment needed for experimentation and learning
    - Dedicated CTF image for competitions

SAMSUNG

DROP PINGS, NOT BOMBS
versity of Nebraska at Omaha



CSAW VIII

- Hosted by Polytechnic Institute of New York University (NYU-Poly)
- Placed 9th out of 207 teams
- Qualified for Final Round in New York City

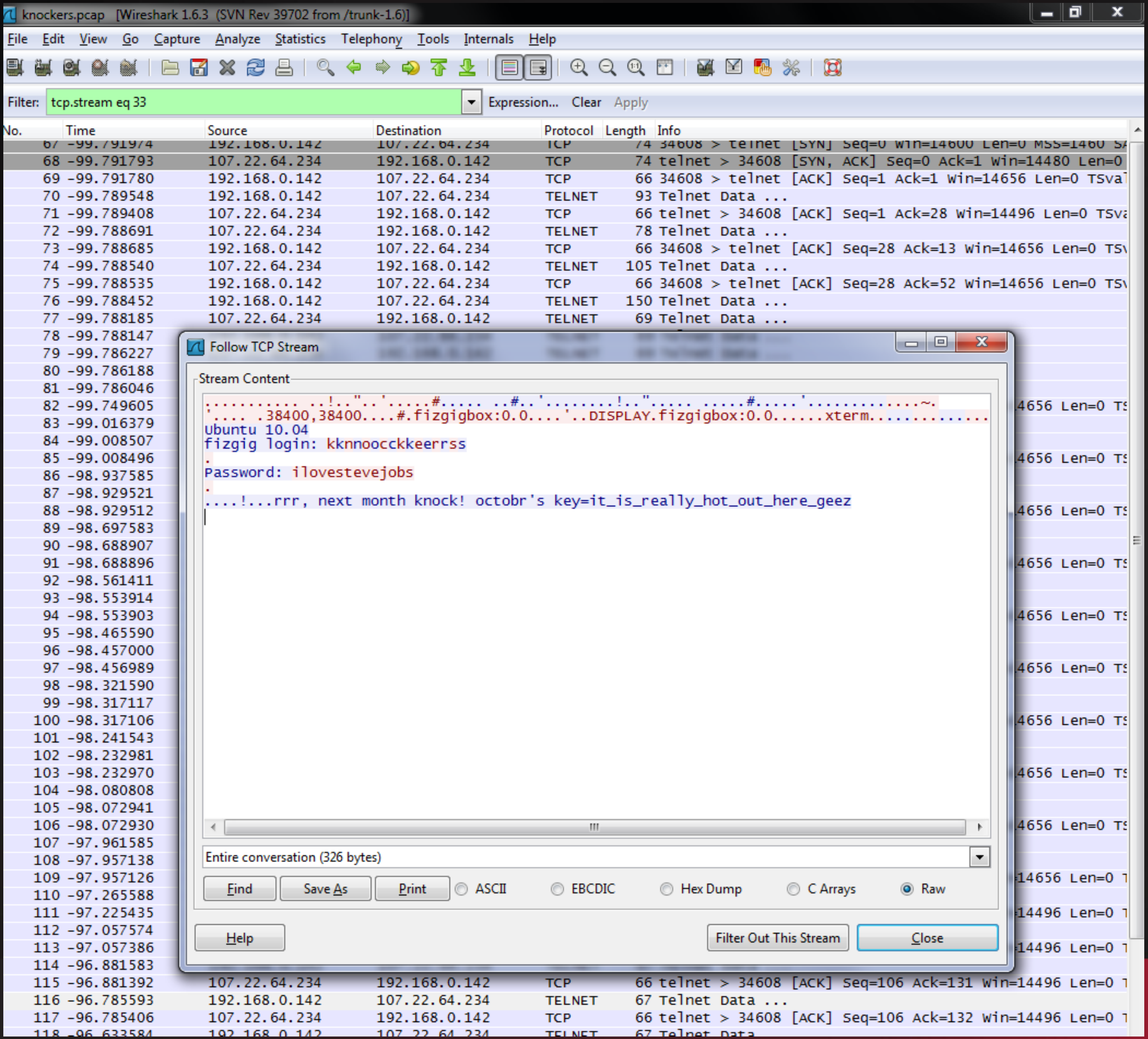
SCENARIO OVERVIEW

Challenge Based:

- Reverse Engineering
- Web Exploitation
- Forensics
- Networking
- Cryptography

CHALLENGE EXAMPLE

- “Knockers”
  - Port knocking challenge
  - Several red herrings
  - “It’s a trap!”



knockers.pcap [Wireshark 1.6.3 (SVN Rev 39702 from /trunk-1.6)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: tcp.stream eq 33

Expression... Clear Apply

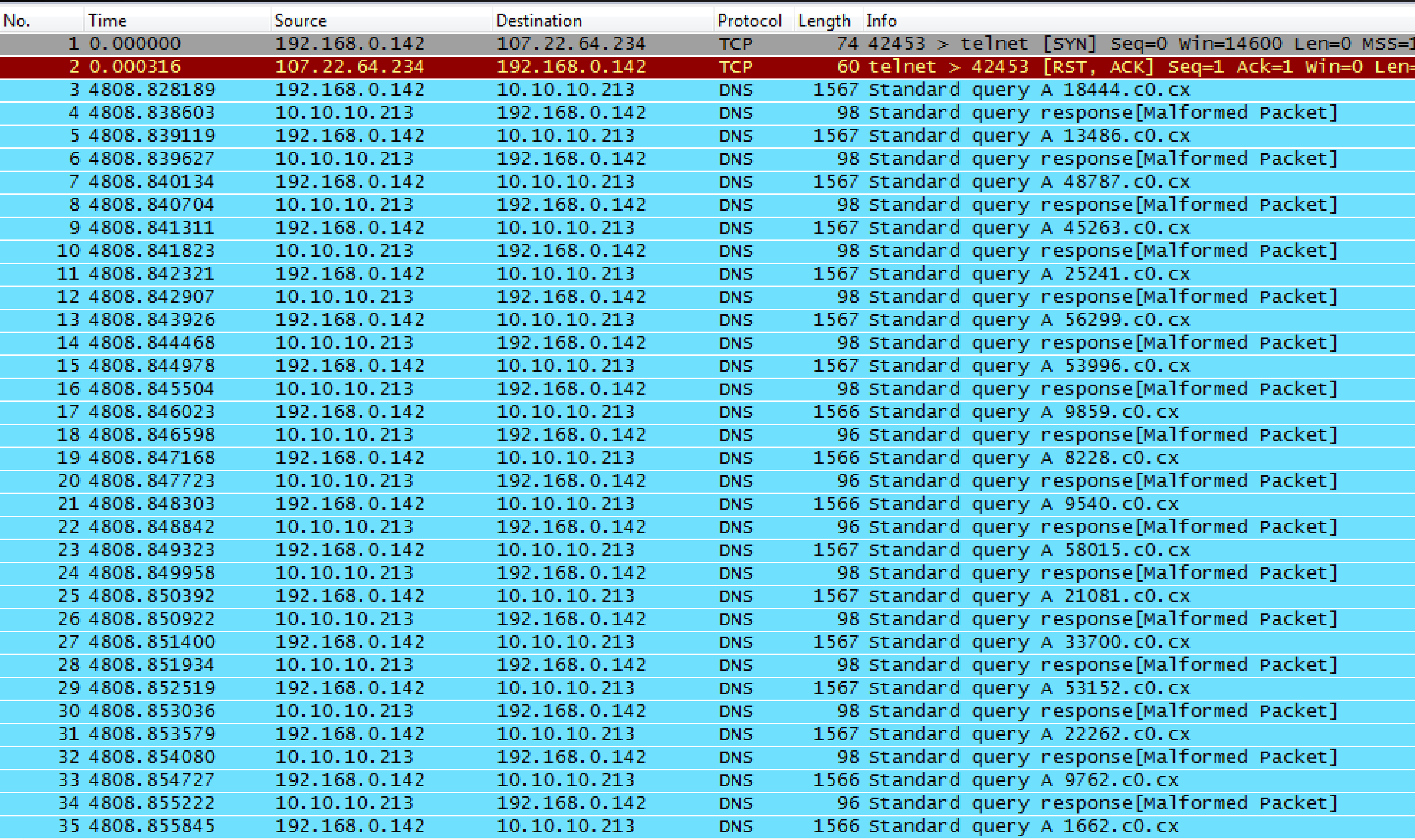
```
No.  Time        Source          Destination     Protocol Length Info
 67 -99.791974  192.168.0.142   107.22.64.234   TCP       74 34608 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1460 SA
 68 -99.791793  107.22.64.234   192.168.0.142   TCP       74 telnet > 34608 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0
 69 -99.791780  192.168.0.142   107.22.64.234   TCP       66 34608 > telnet [ACK] Seq=1 Ack=1 Win=14656 Len=0 TSval
 70 -99.789548  192.168.0.142   107.22.64.234   TELNET    93 Telnet Data ...
 71 -99.789408  107.22.64.234   192.168.0.142   TCP       66 telnet > 34608 [ACK] Seq=1 Ack=28 Win=14496 Len=0 TSva
 72 -99.788691  107.22.64.234   192.168.0.142   TELNET    78 Telnet Data ...
 73 -99.788685  192.168.0.142   107.22.64.234   TCP       66 34608 > telnet [ACK] Seq=28 Ack=13 Win=14656 Len=0 TSv
 74 -99.788540  107.22.64.234   192.168.0.142   TELNET   105 Telnet Data ...
 75 -99.788535  192.168.0.142   107.22.64.234   TCP       66 34608 > telnet [ACK] Seq=28 Ack=52 Win=14656 Len=0 TSv
 76 -99.788452  192.168.0.142   107.22.64.234   TELNET   150 Telnet Data ...
 77 -99.788185  107.22.64.234   192.168.0.142   TELNET    69 Telnet Data ...
 78 -99.788147
 79 -99.786227
 80 -99.786188
 81 -99.786046
 82 -99.749605                                                  4656 Len=0 TS
 83 -99.016379
 84 -99.008507
 85 -99.008496                                                  4656 Len=0 TS
 86 -98.937585
 87 -98.929521
 88 -98.929512                                                  4656 Len=0 TS
 89 -98.697583
 90 -98.688907
 91 -98.688896                                                  4656 Len=0 TS
 92 -98.561411
 93 -98.553914
 94 -98.553903                                                  4656 Len=0 TS
 95 -98.465590
 96 -98.457000
 97 -98.456989                                                  4656 Len=0 TS
 98 -98.321590
 99 -98.317117
100 -98.317106                                                  4656 Len=0 TS
101 -98.241543
102 -98.232981
103 -98.232970                                                  4656 Len=0 TS
104 -98.080808
105 -98.072941
106 -98.072930                                                  4656 Len=0 TS
107 -97.961585
108 -97.957138
109 -97.957126                                                  14656 Len=0 T
110 -97.265588
111 -97.225435                                                  14496 Len=0 T
112 -97.057574
113 -97.057386                                                  14496 Len=0 T
114 -96.881583
115 -96.881392  107.22.64.234   192.168.0.142   TCP       66 telnet > 34608 [ACK] Seq=106 Ack=131 Win=14496 Len=0 T
116 -96.785593  192.168.0.142   107.22.64.234   TELNET    67 Telnet Data ...
117 -96.785406  107.22.64.234   192.168.0.142   TCP       66 telnet > 34608 [ACK] Seq=106 Ack=132 Win=14496 Len=0 T
118 -96.633584  192.168.0.142   107.22.64.234   TELNET    67 Telnet Data
```

Follow TCP Stream

Stream Content

```
........... ..!.."..'.....#..... ..#..'........!.."..... .....#.....'..............~.
'.... .38400,38400....#.fizgigbox:0.0....'..DISPLAY.fizgigbox:0.0......xterm.............
Ubuntu 10.04
fizgig login: kknnoocckkeerrss
.
Password: ilovestevejobs
.
....!...rrr, next month knock! octobr's key=it_is_really_hot_out_here_geez
```

Entire conversation (326 bytes)



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.0.142	107.22.64.234	TCP	74	42453 > telnet [SYN] Seq=0 Win=14600 Len=0 MSS=1
2	0.000316	107.22.64.234	192.168.0.142	TCP	60	telnet > 42453 [RST, ACK] Seq=1 Ack=1 Win=0 Len=
3	4808.828189	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 18444.c0.cx
4	4808.838603	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
5	4808.839119	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 13486.c0.cx
6	4808.839627	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
7	4808.840134	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 48787.c0.cx
8	4808.840704	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
9	4808.841311	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 45263.c0.cx
10	4808.841823	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
11	4808.842321	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 25241.c0.cx
12	4808.842907	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
13	4808.843926	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 56299.c0.cx
14	4808.844468	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
15	4808.844978	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 53996.c0.cx
16	4808.845504	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
17	4808.846023	192.168.0.142	10.10.10.213	DNS	1566	Standard query A 9859.c0.cx
18	4808.846598	10.10.10.213	192.168.0.142	DNS	96	Standard query response[Malformed Packet]
19	4808.847168	192.168.0.142	10.10.10.213	DNS	1566	Standard query A 8228.c0.cx
20	4808.847723	10.10.10.213	192.168.0.142	DNS	96	Standard query response[Malformed Packet]
21	4808.848303	192.168.0.142	10.10.10.213	DNS	1566	Standard query A 9540.c0.cx
22	4808.848842	10.10.10.213	192.168.0.142	DNS	96	Standard query response[Malformed Packet]
23	4808.849323	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 58015.c0.cx
24	4808.849958	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
25	4808.850392	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 21081.c0.cx
26	4808.850922	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
27	4808.851400	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 33700.c0.cx
28	4808.851934	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
29	4808.852519	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 53152.c0.cx
30	4808.853036	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
31	4808.853579	192.168.0.142	10.10.10.213	DNS	1567	Standard query A 22262.c0.cx
32	4808.854080	10.10.10.213	192.168.0.142	DNS	98	Standard query response[Malformed Packet]
33	4808.854727	192.168.0.142	10.10.10.213	DNS	1566	Standard query A 9762.c0.cx
34	4808.855222	10.10.10.213	192.168.0.142	DNS	96	Standard query response[Malformed Packet]
35	4808.855845	192.168.0.142	10.10.10.213	DNS	1566	Standard query A 1662.c0.cx

REFLECTION

- Proved NULLify is able to compete on a national scale.
- Other schools do not have facilities like the STEAL Labs available at UNO

RWTHCTF

- Hosted by Aachen University and 0ldEur0pe CTF team (First time hosting!)
- Placed 36th out of 77 teams
- Scenario: Stop the Missile Crisis

SCENARIO OVERVIEW

- Challenge based
  - Total of four questions
  - Answer each question to move onto the next challenge
- To stop the missile from launching all challenges had to be completed along with remotely moving a robot to hit the stop button

REFLECTION

- First CTF hosted by Aachen University and 0ldEur0pe
- Only two teams ended up completing more than one challenge
- Winning team called the hosts for a walkthrough of the challenges

ICTF

- Hosted by University of California Santa Barbara (UCSB)
- Placed 48th out of 87 total teams
- Scenario: Money Laundering

SCENARIO OVERVIEW

- Challenge and service based
  - Challenges were completed to acquire dirty money
  - Services were exploited to launder money and score points
- Cut, Payoff, Risk
  - Two minute rounds were used where the risk, payoff, and cut fluctuate

REFLECTION

- While we succeeded on the challenge portion of the competition, we have found that we need to work on the service based attacks
- Lack of organization for a large number of people proved to be cumbersome

NATIONAL CYBER DEFENSE COMPETITION

- Iowa State University IA Center
- Live CTF with vulnerable servers
    - Secure System Administration
- Finished 7th out of 8 teams

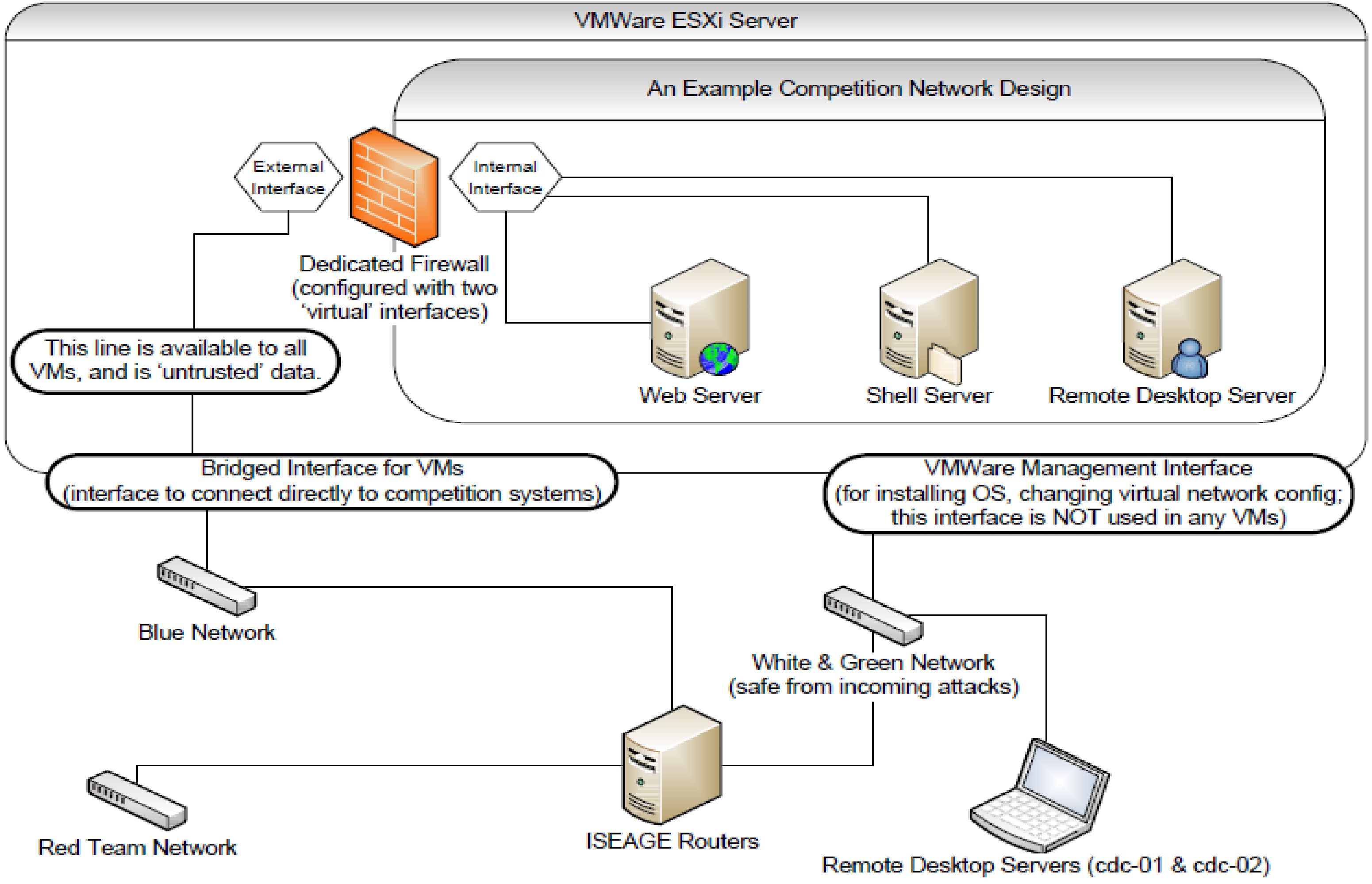
ISEAGE
Internet-Scale Event and Attack Generation Environment

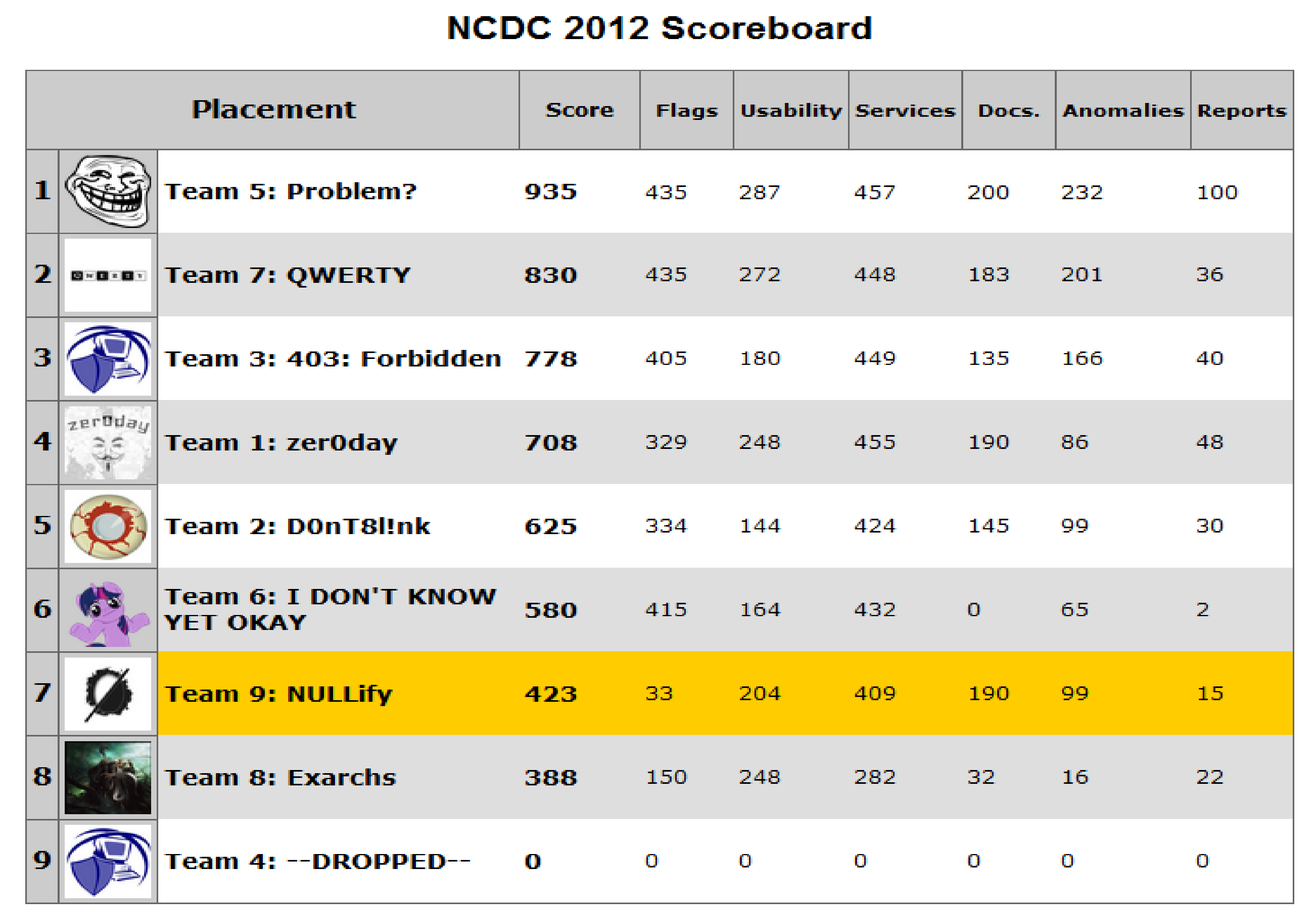
IOWA STATE UNIVERSITY
INFORMATION ASSURANCE CENTER

SCENARIO OVERVIEW

- New System Administrator for the Cynical Dentist Collation (CDC)
- Secure several highly unsecured servers
- Protect your flags from the attacking red team
- Complete challenges, documentation, and anomalies

CDC Network Topology with VMWare ESXi Virtualization


VMWare ESXi Server
An Example Competition Network Design
External Interface
Internal Interface
Dedicated Firewall (configured with two 'virtual' interfaces)
This line is available to all VMs, and is 'untrusted' data.
Web Server
Shell Server
Remote Desktop Server
Bridged Interface for VMs (interface to connect directly to competition systems)
VMWare Management Interface (for installing OS, changing virtual network config; this interface is NOT used in any VMs)
Blue Network
White & Green Network (safe from incoming attacks)
Red Team Network
ISEAGE Routers
Remote Desktop Servers (cdc-01 & cdc-02)



NCDC 2012 Scoreboard

Placement		Score	Flags	Usability	Services	Docs.	Anomalies	Reports
1	Team 5: Problem?	935	435	287	457	200	232	100
2	Team 7: QWERTY	830	435	272	448	183	201	36
3	Team 3: 403: Forbidden	778	405	180	449	135	166	40
4	Team 1: zer0day	708	329	248	455	190	86	48
5	Team 2: D0nT8l!nk	625	334	144	424	145	99	30
6	Team 6: I DON'T KNOW YET OKAY	580	415	164	432	0	65	2
7	Team 9: NULLify	423	33	204	409	190	99	15
8	Team 8: Exarchs	388	150	248	282	32	16	22
9	Team 4: --DROPPED--	0	0	0	0	0	0	0

POINTS OF INTEREST

- Unique CTF with services and vulnerable servers
- Nuclear fallout event
- Network modification challenges on the fly
- Only team to never previously compete

REFLECTION

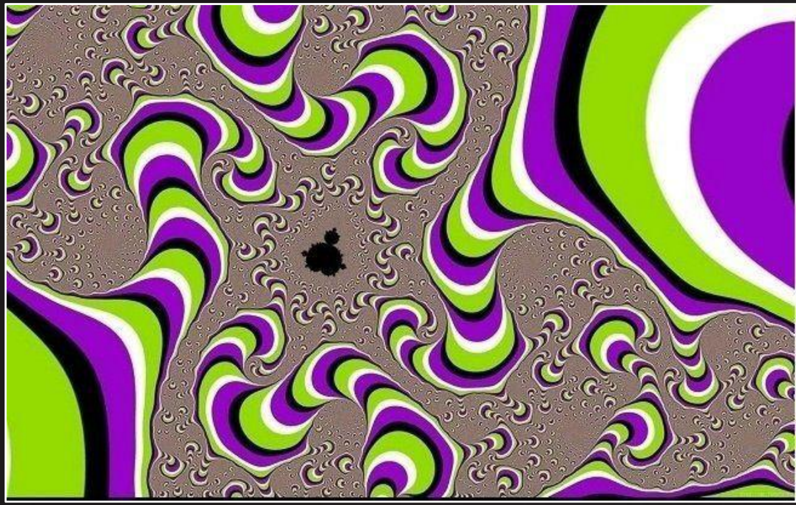
- Time taken to prepare our network for the event
- Penetration test our network before hand
- Gained real world experience in securing networks from hackers
- And last but not least...

Pizza and Wings!!!

IFSF CTF

- Hosted by forbiddenBITS
  - From Tunisia
- Challenge-based
- NULLify placed 21st of 90 scoring teams worldwide
  - 4th among U.S. teams

CHALLENGE EXAMPLE



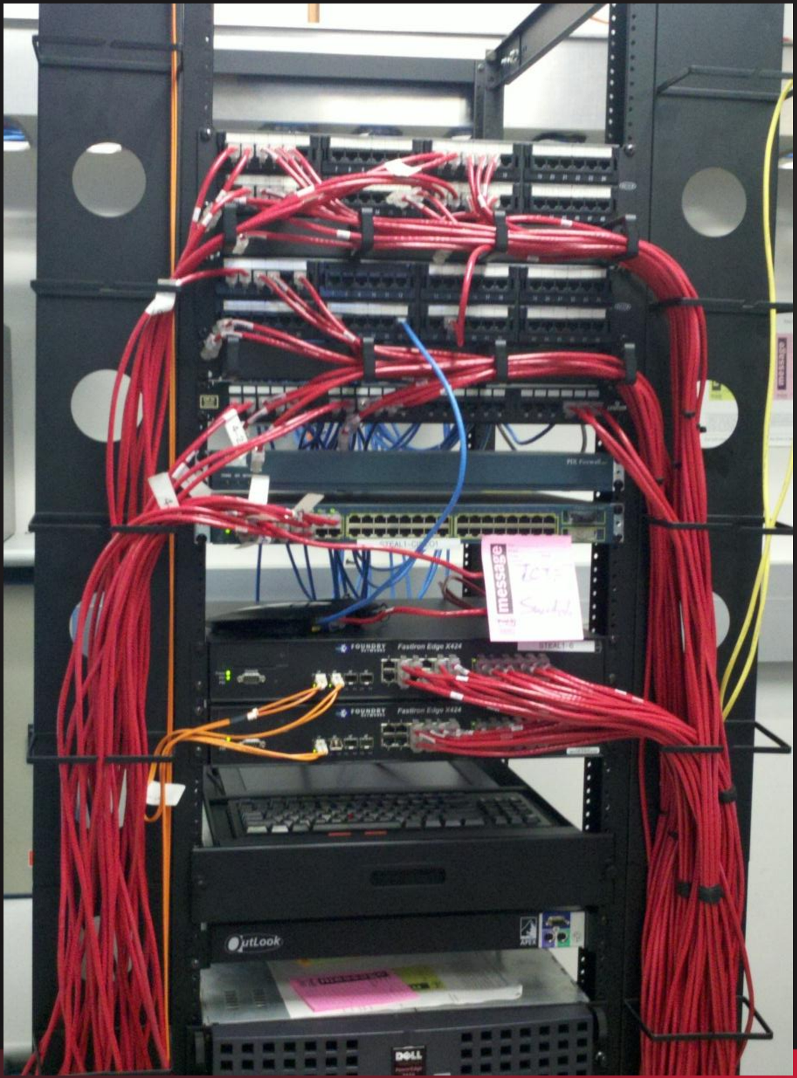
- “Hidden Files”
  - Notice the small black strip at the bottom
  - Stegdetect detected an appended file (Turns out to be a zip)
  - Included a password protected file
  - A simple password cracker determined the password was “pass”

SCENARIO OVERVIEW

- Challenge Based
    - DOS application reverse engineering
    - Esoteric programming languages
    - Cryptography
    - Networking

STEAL -1

- Temporarily reconfigured for going to battle on IFSF CTF servers
- The real STEAL network was still isolated from the Internet



REFLECTIONS

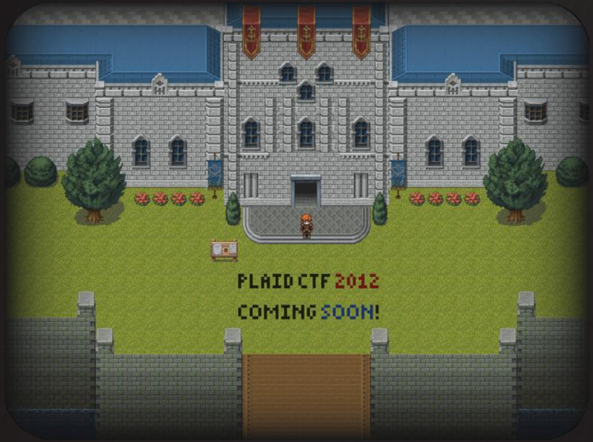
- ‘ is different than `
- Timestamps from other countries may be in a different format than those from the United States
- Two to three people working on a challenge is plenty

PLAID CTF

- Hosted by Plaid Parliament of Pwning (PPP)
  - CTF team from Carnegie Mellon University
- Challenge based
- NULLify placed 35th of 243 scoring teams
  - 12th place among U.S. teams

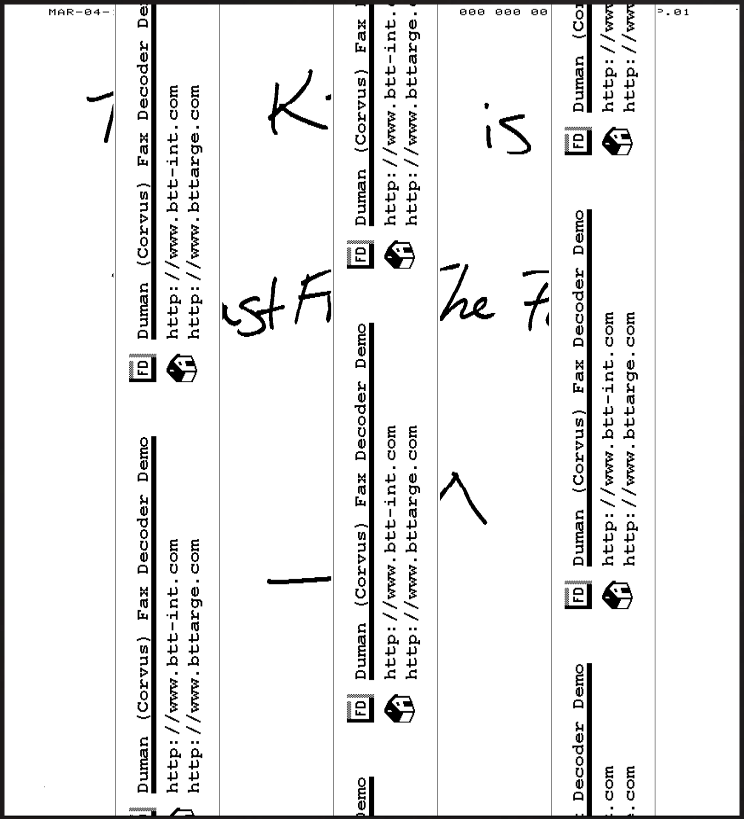
SCENARIO OVERVIEW

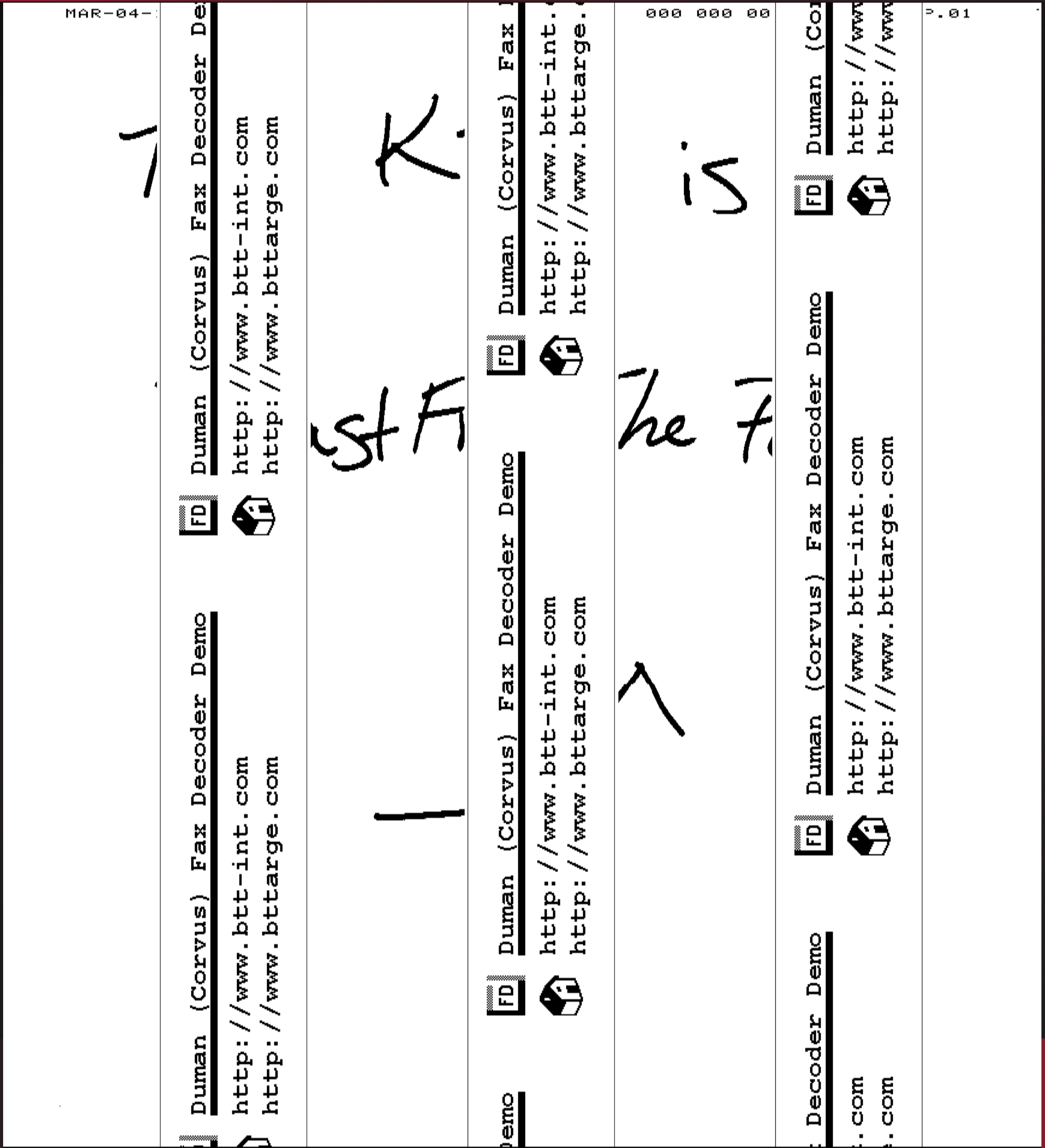
- Challenge Based
  - Instead of a typical web page with challenges listed, contestants were required to playa custom RPG for the CTF based on RPG JS
  - Challenges were more difficult than previous CTFs



CHALLENGE EXAMPLE

- “80’s Thinking”
  - Audio file of a fax wiretap
  - We had to find a way to decode the transmission
  - Key:???


MAR-04-
Duman (Corvus) Fax Decoder Demo
http://www.btt-int.com
http://www.bttarge.com
FD
K
is
st F
he F



MAR-04-

T

Duman (Corvus) Fax Decoder De
http://www.btt-int.com
http://www.bttarge.com

Duman (Corvus) Fax Decoder Demo
http://www.btt-int.com
http://www.bttarge.com

K:

st Fi

Duman (Corvus) Fax
http://www.btt-int.
http://www.bttarge.

Duman (Corvus) Fax Decoder Demo
http://www.btt-int.com
http://www.bttarge.com

emo

000 000 00

is

The F

Duman (Co
http://www
http://www

Duman (Corvus) Fax Decoder Demo
http://www.btt-int.com
http://www.bttarge.com

Decoder Demo
.com
.com

P.01

ANSWER

“BlastFromThePast^_^”

REFLECTIONS

- The RPG element was innovative albeit time consuming to list challenges
- Organizing, and competing in a CTF the weekend before finals week is difficult

FUTURE GOALS

- Continue to expand NULLify
- Continue to compete in CTF competitions
- Compete in CTF qualification rounds for DEFCON

FUTURE GOALS

- Encourage members to study and train for certifications
- Travel to DEFCON 20

CONCLUSION

- Membership has grown from just a few to over ten active members meeting at least once a week
- The number of CTF competitions has increased from one per year, to six this year
- NULLify has competed very well on the national and international level

RESOURCES

- https://csawctf.poly.edu/
- http://ctf.forbiddenbits.net/
- http://ctf.itsec.rwth-aachen.de/
- https://www.iac.iastate.edu/wiki/Cyber_Defense_Competitions
- http://ictf.cs.ucsb.edu/
- http://ppp.cylab.cmu.edu/wordpress/
- http://rocktheflag.net
- http://utdcsg.org/

QUESTIONS?

UNIVERSITY OF Nebraska Omaha

http://w ww.unonullify.com
https://www.facebook.com/groups/UNOnullify