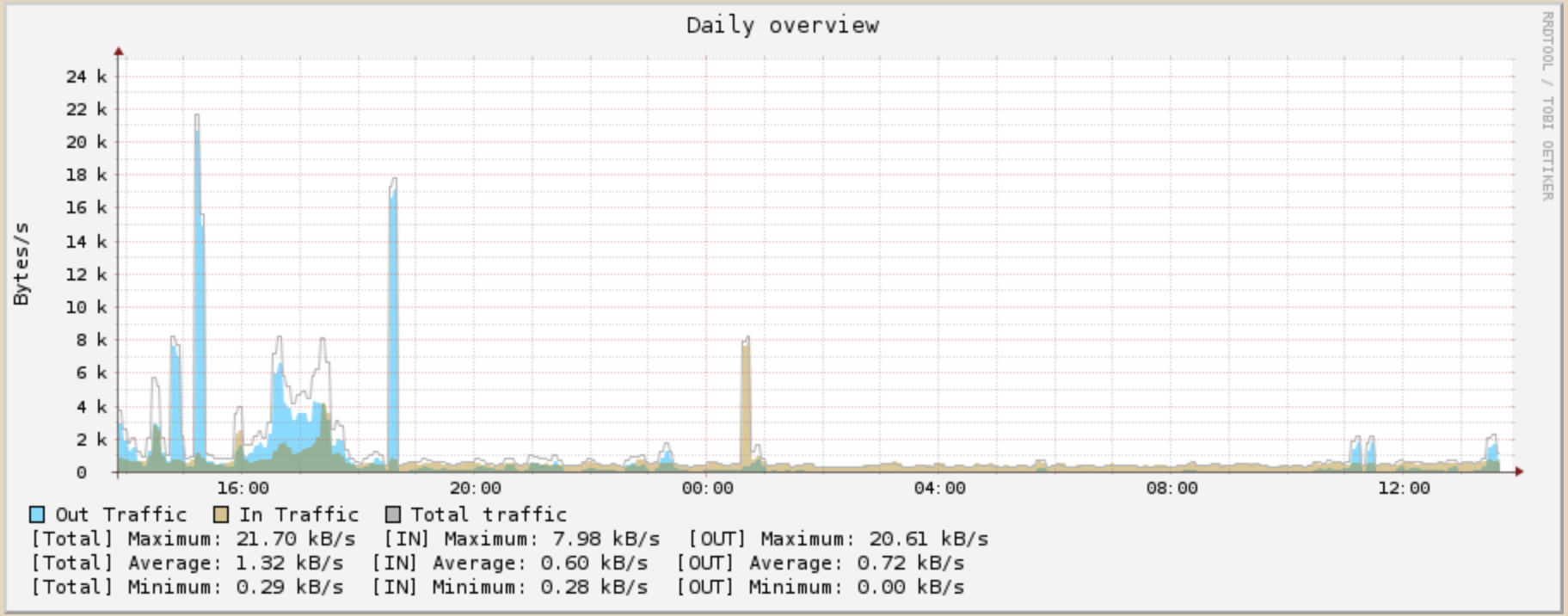
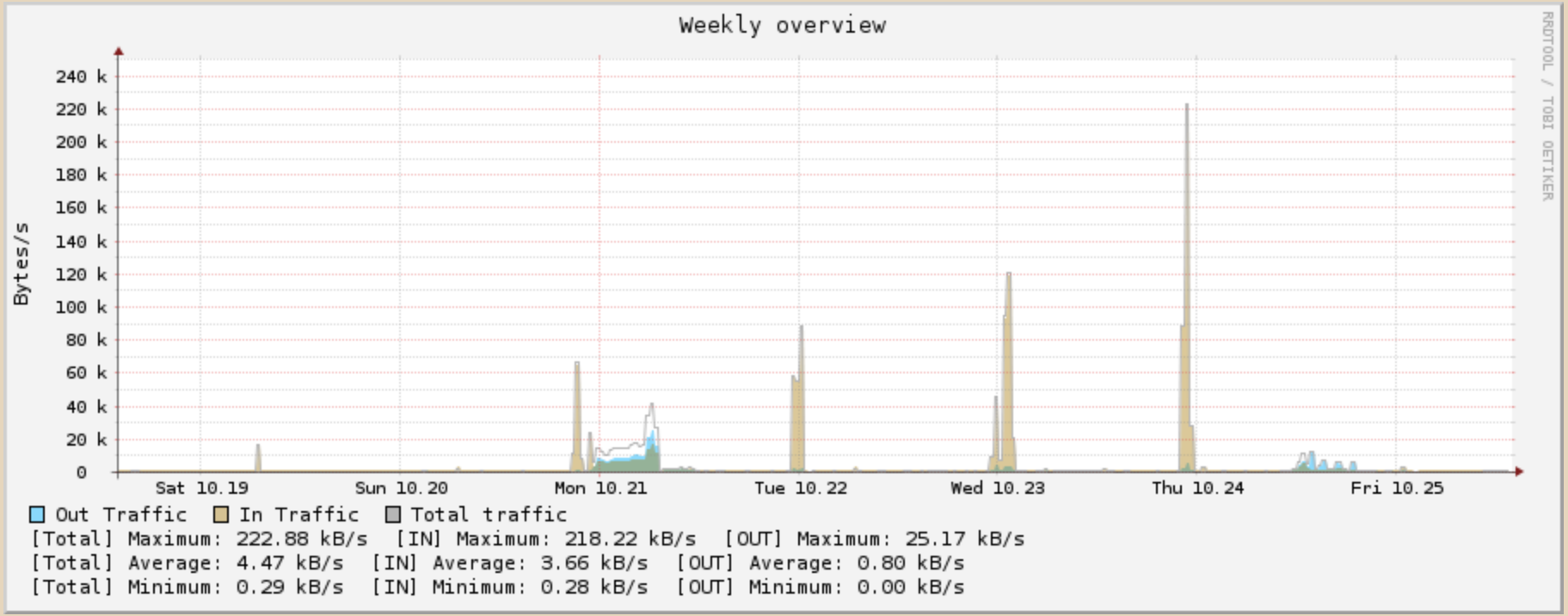
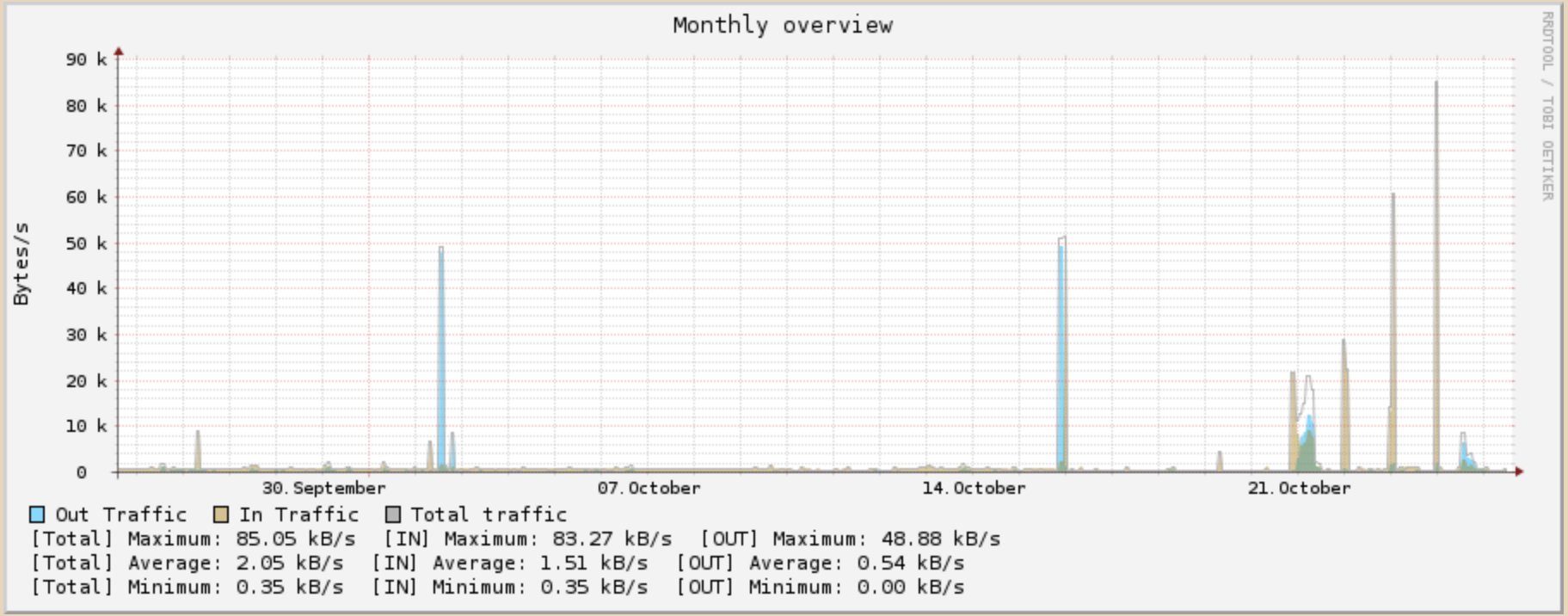
# 2013 Capture The Flags Post-Mortum

Ming Chow
COMP 116: Introduction to Computer Security
Thursday, October 31, 2013

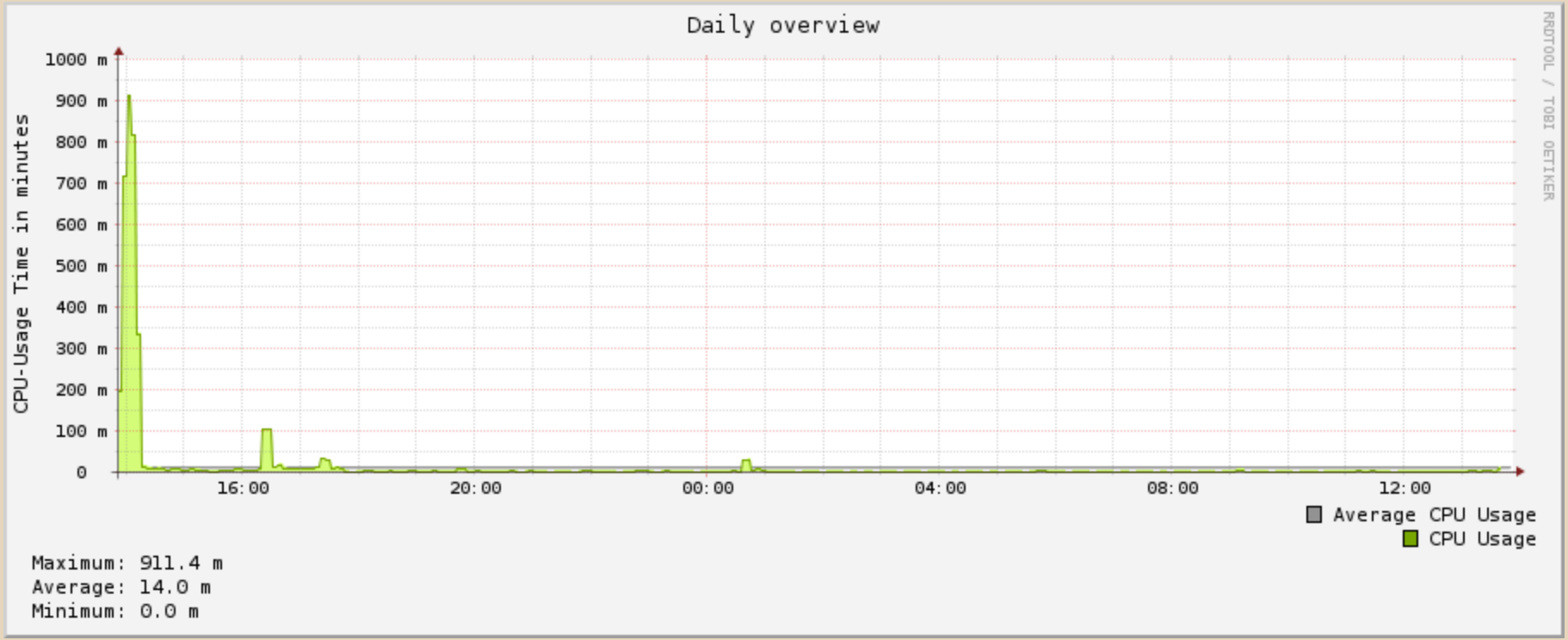
~1 GB traffic (bandwidth) sent to 67.23.79.113

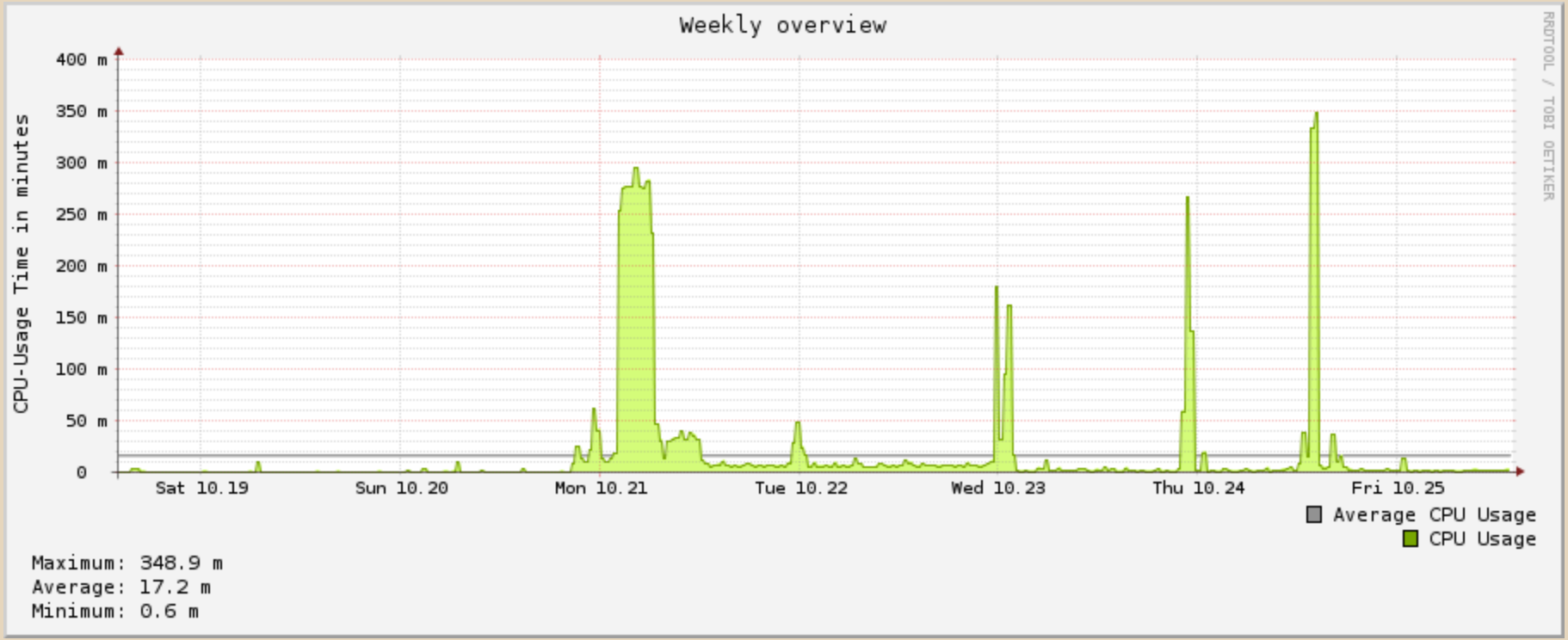

Daily overview
RRDTOOL / TOBI OETIKER
Bytes/s
24 k
22 k
20 k
18 k
16 k
14 k
12 k
10 k
8 k
6 k
4 k
2 k
0
16:00
20:00
00:00
04:00
08:00
12:00
Out Traffic
In Traffic
Total traffic
[Total] Maximum: 21.70 kB/s [IN] Maximum: 7.98 kB/s [OUT] Maximum: 20.61 kB/s
[Total] Average: 1.32 kB/s [IN] Average: 0.60 kB/s [OUT] Average: 0.72 kB/s
[Total] Minimum: 0.29 kB/s [IN] Minimum: 0.28 kB/s [OUT] Minimum: 0.00 kB/s


Weekly overview
RRDTOOL / TOBI OETIKER
Bytes/s
240 k
220 k
200 k
180 k
160 k
140 k
120 k
100 k
80 k
60 k
40 k
20 k
0
Sat 10.19
Sun 10.20
Mon 10.21
Tue 10.22
Wed 10.23
Thu 10.24
Fri 10.25
Out Traffic
In Traffic
Total traffic
[Total] Maximum: 222.88 kB/s [IN] Maximum: 218.22 kB/s [OUT] Maximum: 25.17 kB/s
[Total] Average: 4.47 kB/s [IN] Average: 3.66 kB/s [OUT] Average: 0.80 kB/s
[Total] Minimum: 0.29 kB/s [IN] Minimum: 0.28 kB/s [OUT] Minimum: 0.00 kB/s


Monthly overview
RRDTOOL / TOBI OETIKER
Bytes/s
90 k
80 k
70 k
60 k
50 k
40 k
30 k
20 k
10 k
0
30. September
07. October
14. October
21. October
Out Traffic
In Traffic
Total traffic
[Total] Maximum: 85.05 kB/s [IN] Maximum: 83.27 kB/s [OUT] Maximum: 48.88 kB/s
[Total] Average: 2.05 kB/s [IN] Average: 1.51 kB/s [OUT] Average: 0.54 kB/s
[Total] Minimum: 0.35 kB/s [IN] Minimum: 0.35 kB/s [OUT] Minimum: 0.00 kB/s

# CPU usage…


Daily overview
CPU-Usage Time in minutes
1000 m
900 m
800 m
700 m
600 m
500 m
400 m
300 m
200 m
100 m
0
16:00
20:00
00:00
04:00
08:00
12:00
Average CPU Usage
CPU Usage
Maximum: 911.4 m
Average: 14.0 m
Minimum: 0.0 m
RRDTOOL / TOBI OETIKER


Weekly overview
CPU-Usage Time in minutes
400 m
350 m
300 m
250 m
200 m
150 m
100 m
50 m
0
Sat 10.19
Sun 10.20
Mon 10.21
Tue 10.22
Wed 10.23
Thu 10.24
Fri 10.25
Average CPU Usage
CPU Usage
Maximum: 348.9 m
Average: 17.2 m
Minimum: 0.6 m
RRDTOOL / TOBI OETIKER

# A team managed to lose points

# Someone figured out that the flags (keys) were SHA-1 hashes of U2 song titles

# The Flags

1. key{18e9d8d92b4c6342ffd51de9934b69223c312b51} => Sunday Bloody Sunday
2. key{dc76ee78430d2982026f8364dbccb5755f6d5561} => Where The Streets Have No Name
3. key{b220a91e7eab10fde8677c149829fee7ef6b6758} => Bullet The Blue Sky
4. key{ee16dd465865e2233c2e715f11ef3caf4ac79c03} => I Still Haven't Found What I'm Looking For
5. key{2645e286540c44f4bac5f648dfe301c81dcfbff7} => Get On Your Boots
6. key{8aace50bc0675c767c949fea6ae483a5212a739d} => Angel Of Harlem
7. key{d21f5c37658648250bfbb22824a337174ced3161} => The Incredible Fire
8. key{04e3895d689bbbe88f80021e3a8428eb3b626b6f} => Sometimes You Can't Make It On Your Own

# Nick Andre did a lot of damage

The username:password of the CTF VM now available for download is defcon:ming@ling (long story)

# A look back at each of the challenges and the big idea behind each flag

The entire game (source code) has been released to GitHub: https://github.com/mchow01/Security/tree/master/ctf-f2013

# There is so much more security #fail in this game beyond the challenges...