The Security Gap

Philip Young
aka Soldier of Fortran
@mainframed767

#SHAREorg

SHARE is an independent volunteer-run information technology association that provides **education**, professional **networking** and industry **influence**.

SHARE in Seattle 2015

DISCLAIMER

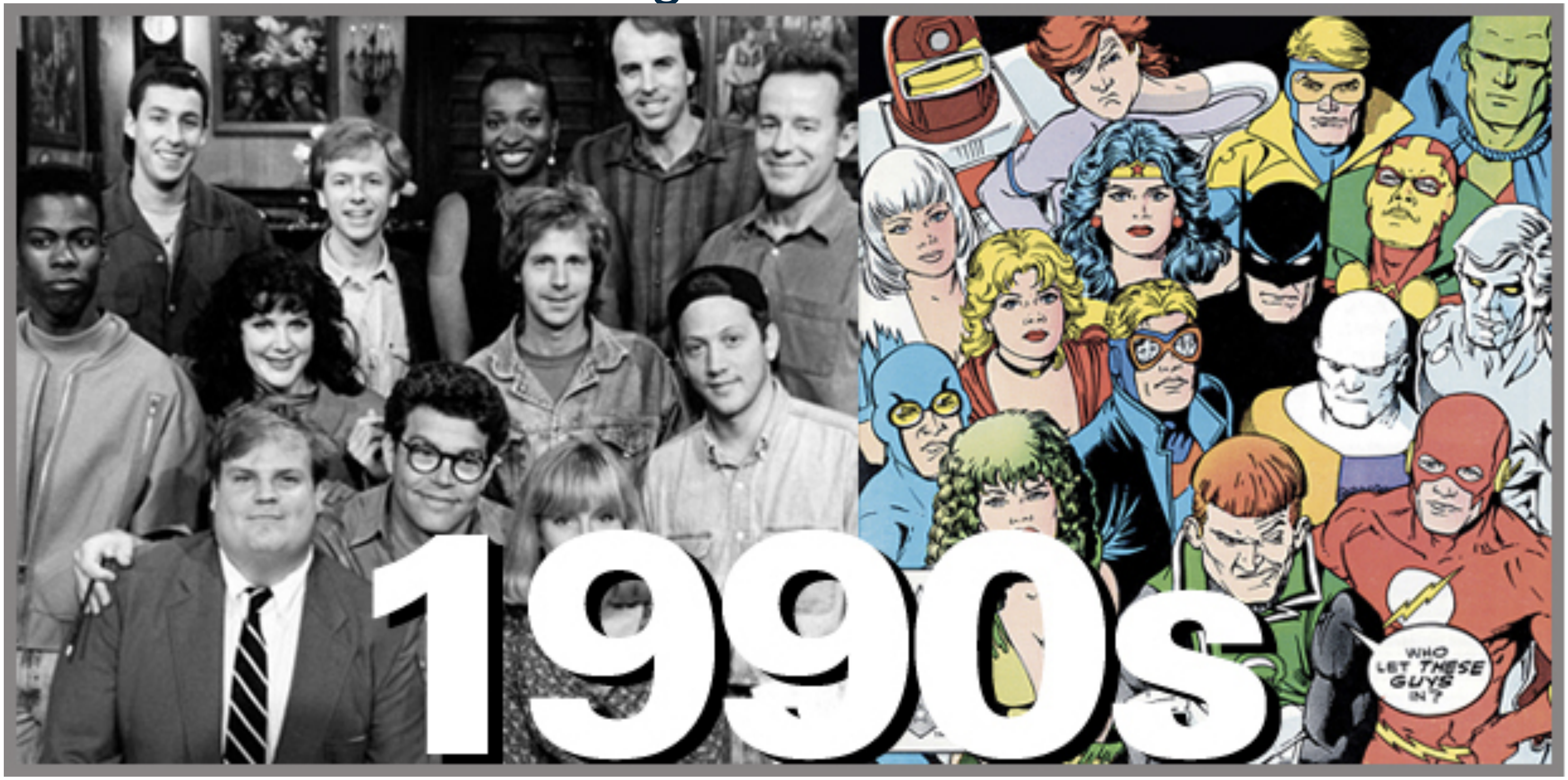
All research was done under personal time. I am not here in the name of, or on behalf of, my employer.

Any views expressed in this talk are my own and not those of my employer.

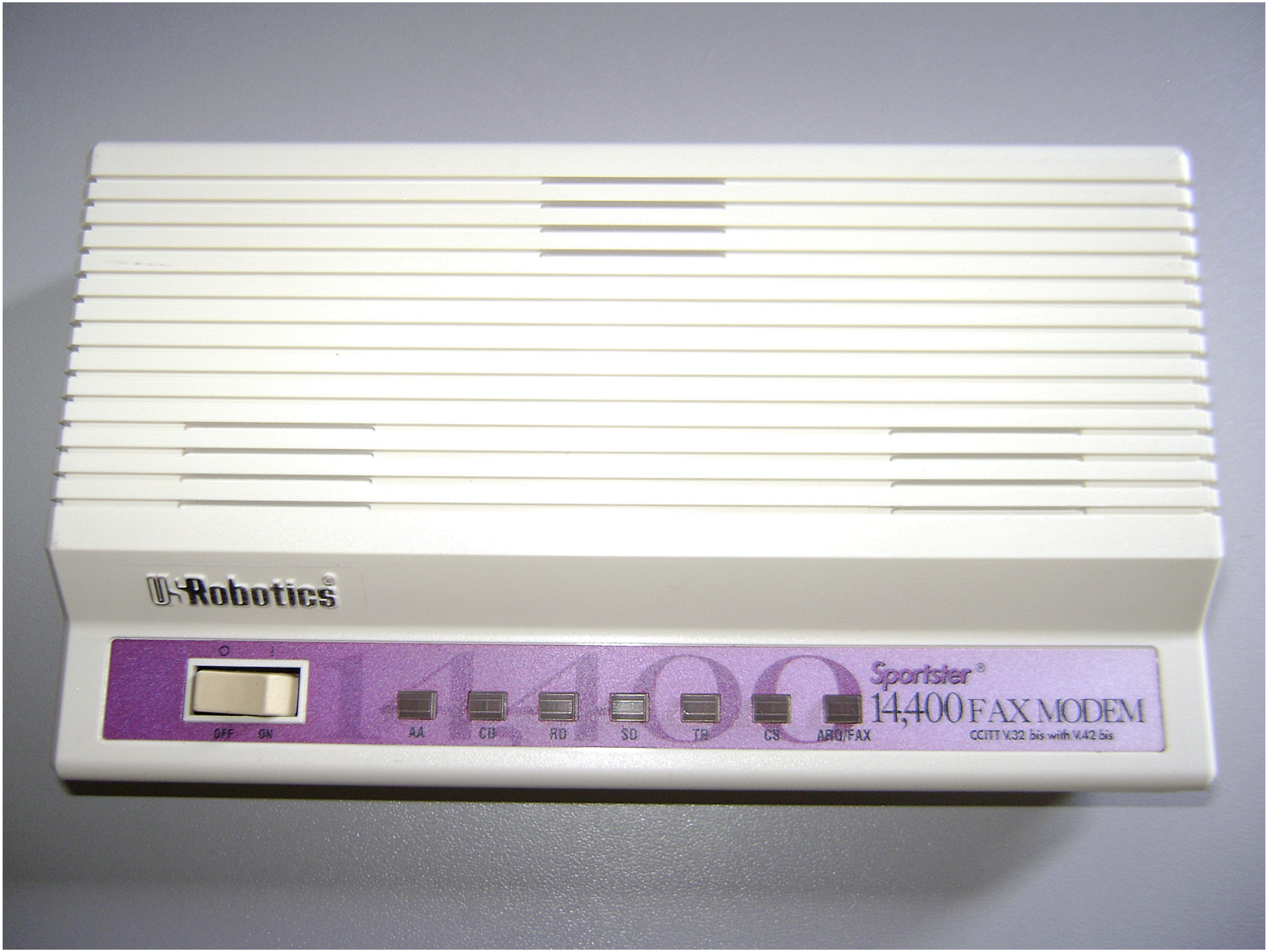
This talk discusses work performed in my spare using personal equipment and resources.

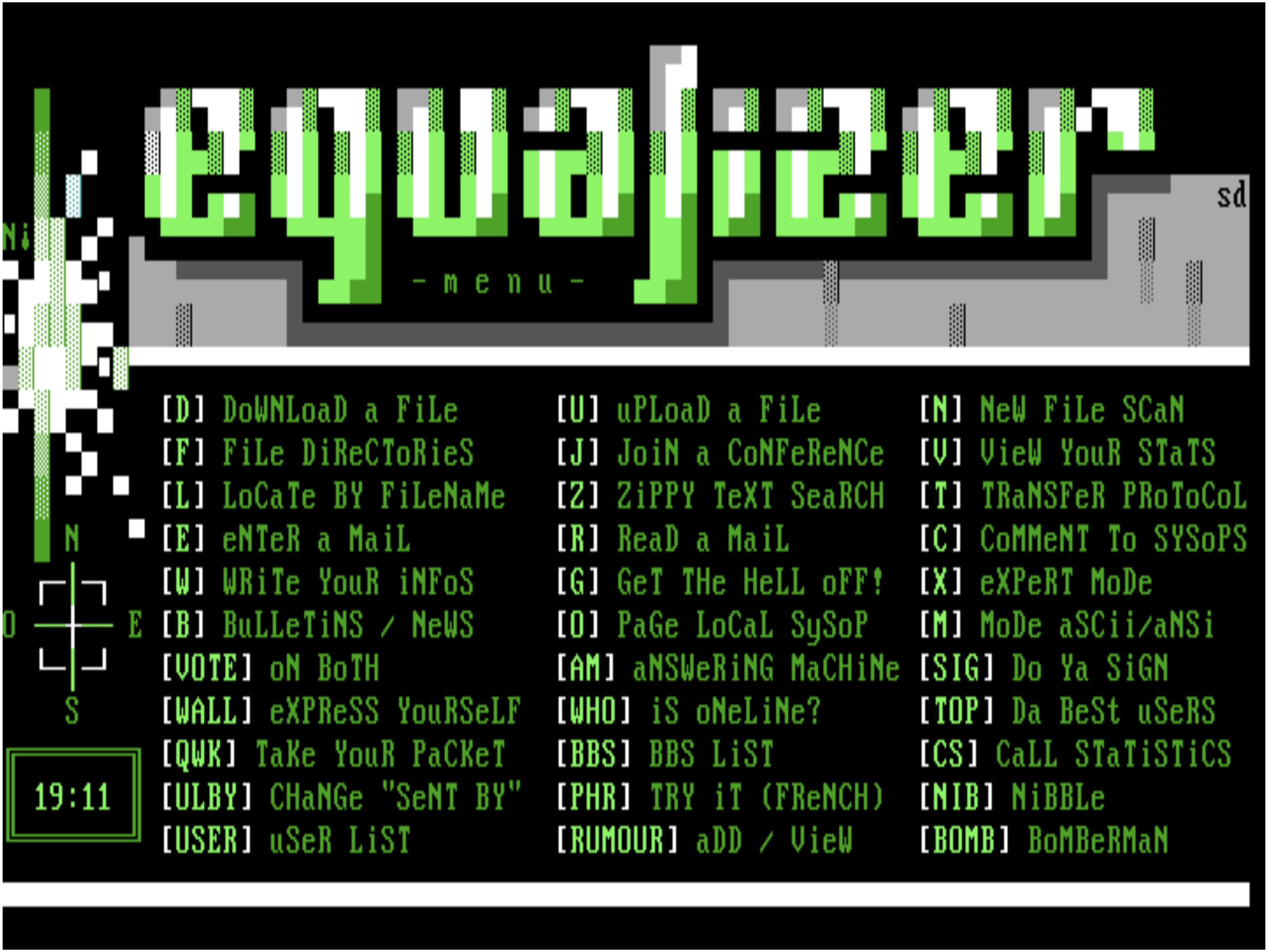
My Story

- Started a ***LONG*** time ago……



Ok, not ***THAT*** long ago


USRobotics®
O I
OFF ON
1400
AA
CD
RD
SD
TR
CS
ARQ/FAX
Sportster®
14,400 FAX MODEM
CCITT V.32 bis with V.42 bis



```
[D] DoWNLoaD a FiLe          [U] uPLoaD a FiLe              [N] NeW FiLe SCaN
[F] FiLe DiReCToRieS         [J] JoiN a CoNFeReNCe          [V] VieW YouR STaTS
[L] LoCaTe BY FiLeNaMe       [Z] ZiPPY TeXT SeaRCH          [T] TRaNSFeR PRoToCoL
[E] eNTeR a MaiL             [R] ReaD a MaiL                [C] CoMMeNT To SYSoPS
[W] WRiTe YouR iNFoS         [G] GeT THe HeLL oFF!          [X] eXPeRT MoDe
[B] BuLLeTiNS / NeWS         [O] PaGe LoCaL SySoP           [M] MoDe aSCii/aNSi
[VOTE] oN BoTH               [AM] aNSWeRiNG MaCHiNe         [SIG] Do Ya SiGN
[WALL] eXPReSS YouRSeLF      [WHO] iS oNeLiNe?              [TOP] Da BeSt uSeRS
[QWK] TaKe YouR PaCKeT       [BBS] BBS LiST                 [CS] CaLL STaTiSTiCS
[ULBY] CHaNGe "SeNT BY"      [PHR] TRY iT (FReNCH)          [NIB] NiBBLe
[USER] uSeR LiST             [RUMOUR] aDD / VieW            [BOMB] BoMBeRMaN
```

19:11

DATAPAC INTERNATIONAL ACCESS PROCEDURES

Datapac International provides outgoing and incoming access to 6 U.S. based Networks and to over 100 packet-switched networks around the world. To successfully complete such calls, Datapac has implemented the International CCITT X.75 procedures and X.121 International numbering plan. Thus, the Datapac user originating an international call must use the following format:

```
                                              (1) (DNIC) (FOREIGN ADDRESS)
                                               :     :           :
      One defines the Datapac International.:     :           :
      Prefix.                                     :           :
                                                  :           :
      Packet networks are identified by a ........:           :
      four digit number called a DNIC                         :
      (data network identification code)                      :
                                                              :
      The foreign national address is ........................:
      expressed as an eight to ten digit
      address.
```

Here is a list of useful DNIC's if you get the urge to scan "other" networks.

```
    Sprintnet          3110
```

Let’s fast forward

- Joined Ernst & Young in 2005
  - Young
  - bright eyed
  - Naïve
- Bounced around consulting firms for a bit
- Joined Visa in 2009
  - 2009-2013: Internal Audit
  - 2013-2014: Information Security
- Currently: Large Financial Institution
  - Joined Cyber Security Red Team

@ Visa

- Tasked on multiple mainframe reviews
- Started doing personal research
- Thought to myself:

"I can't be the only one thinking like this, maybe other people would be interested"

Speaking Out

Mainframed

The Forgotten Fortress

Phil Young - Soldier of Fortr

Mainframed:

The Secrets Inside that Black Box

ice-9406

MAINFRAMES

"What the F$#K is That About?"

SoLdIeR Of FoRtRaN @MAINFRAMED767

-py_

Legacy 0-Day

How Hackers Breached the Logica Mainframe

black hat USA 2013

Mainframes: The past will come back to haunt you

By: Philip "Soldier of Fortran" Young

FROM ROOT TO SPECIAL

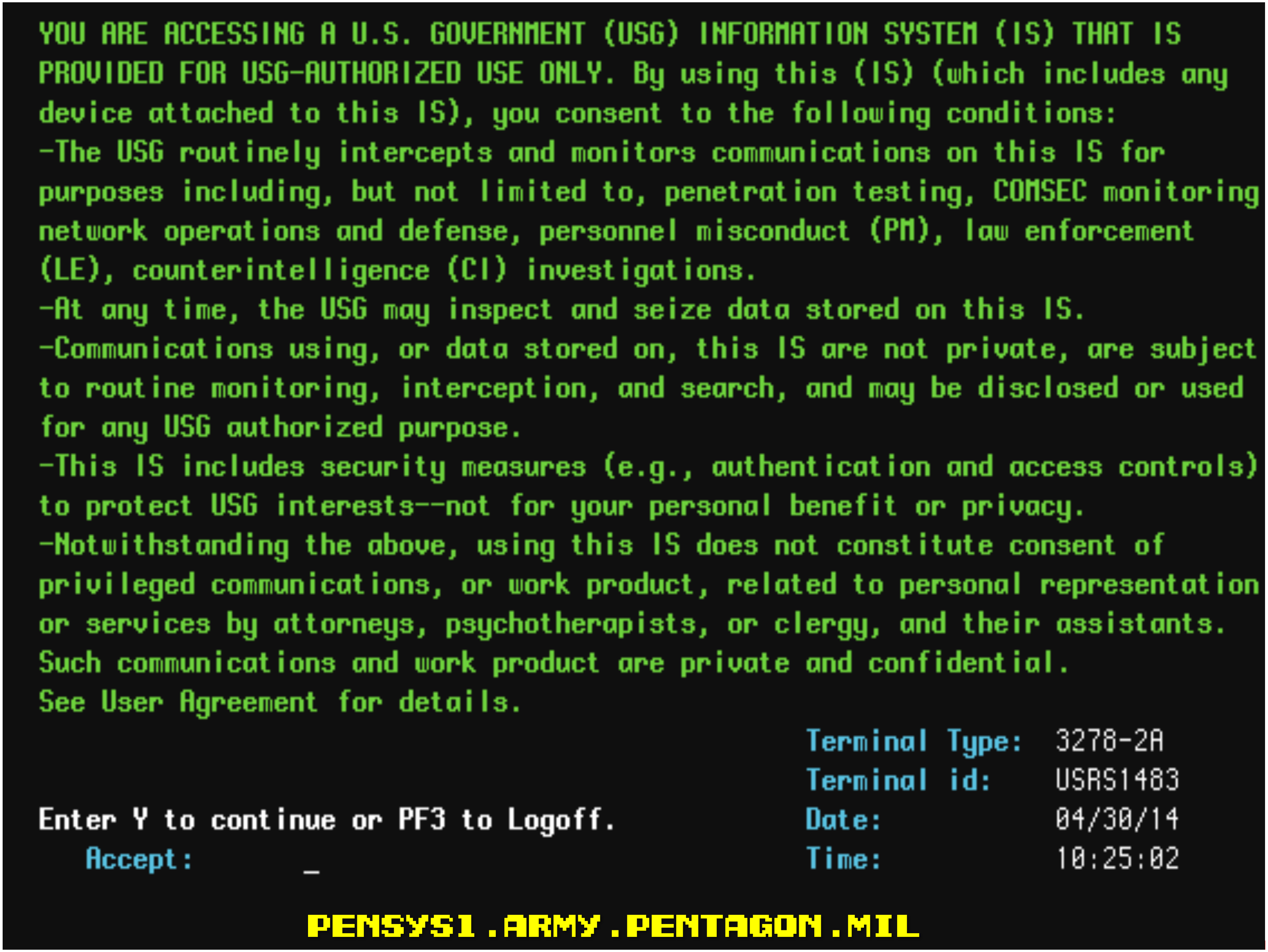
PWNING IBM MAINFRAMES

Soldier of Fortran @mainframed767

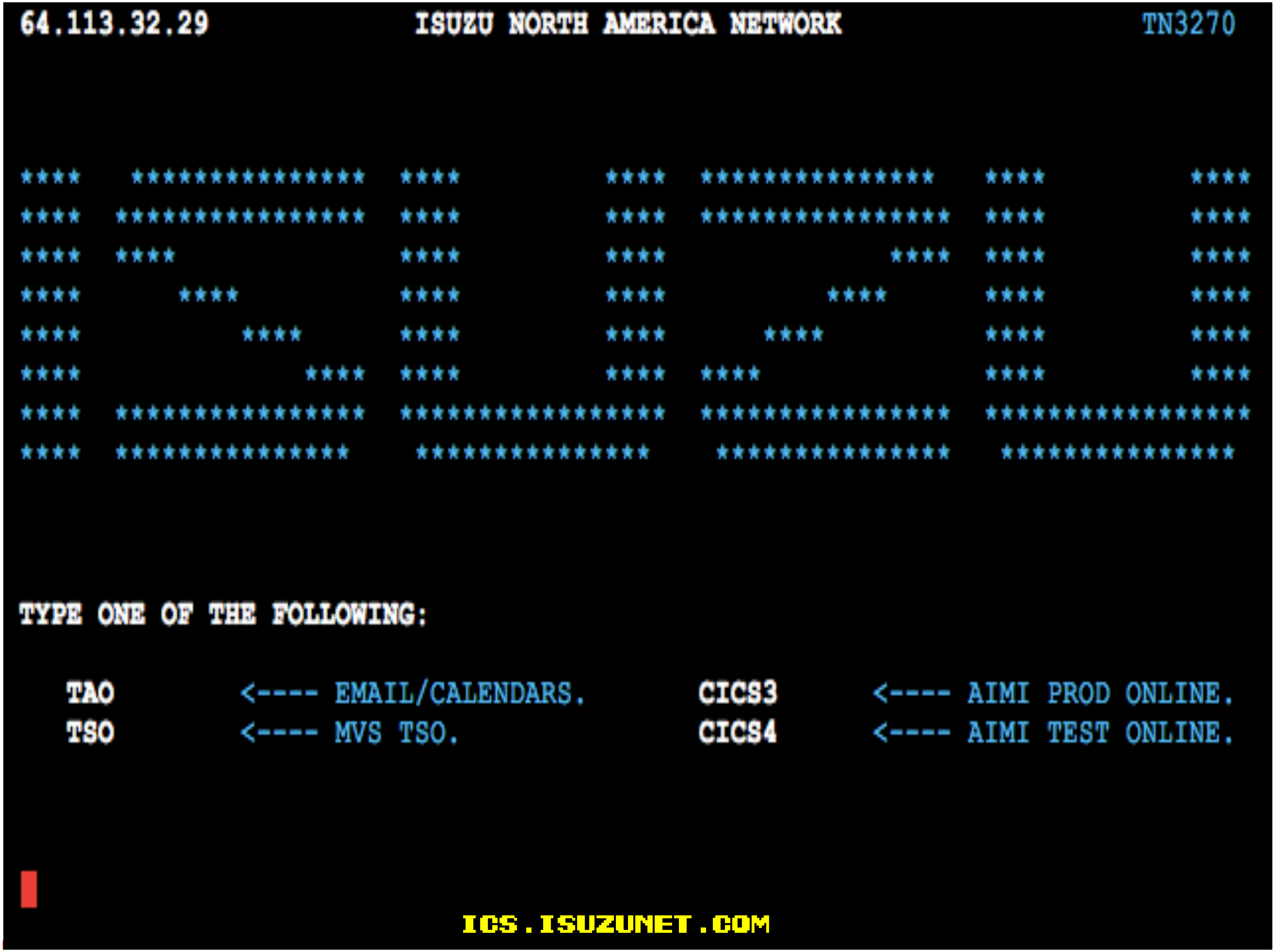
Internet Mainframes Project

- Early 2014 scanned entire internet
  - Thanks to help from friends
- Supplemented with tools like Shodan/GoogleFu
- Found 332
- MFScreen.py:
  - Python script
  - Connected to mainframe over TOR
  - Takes a screenshot

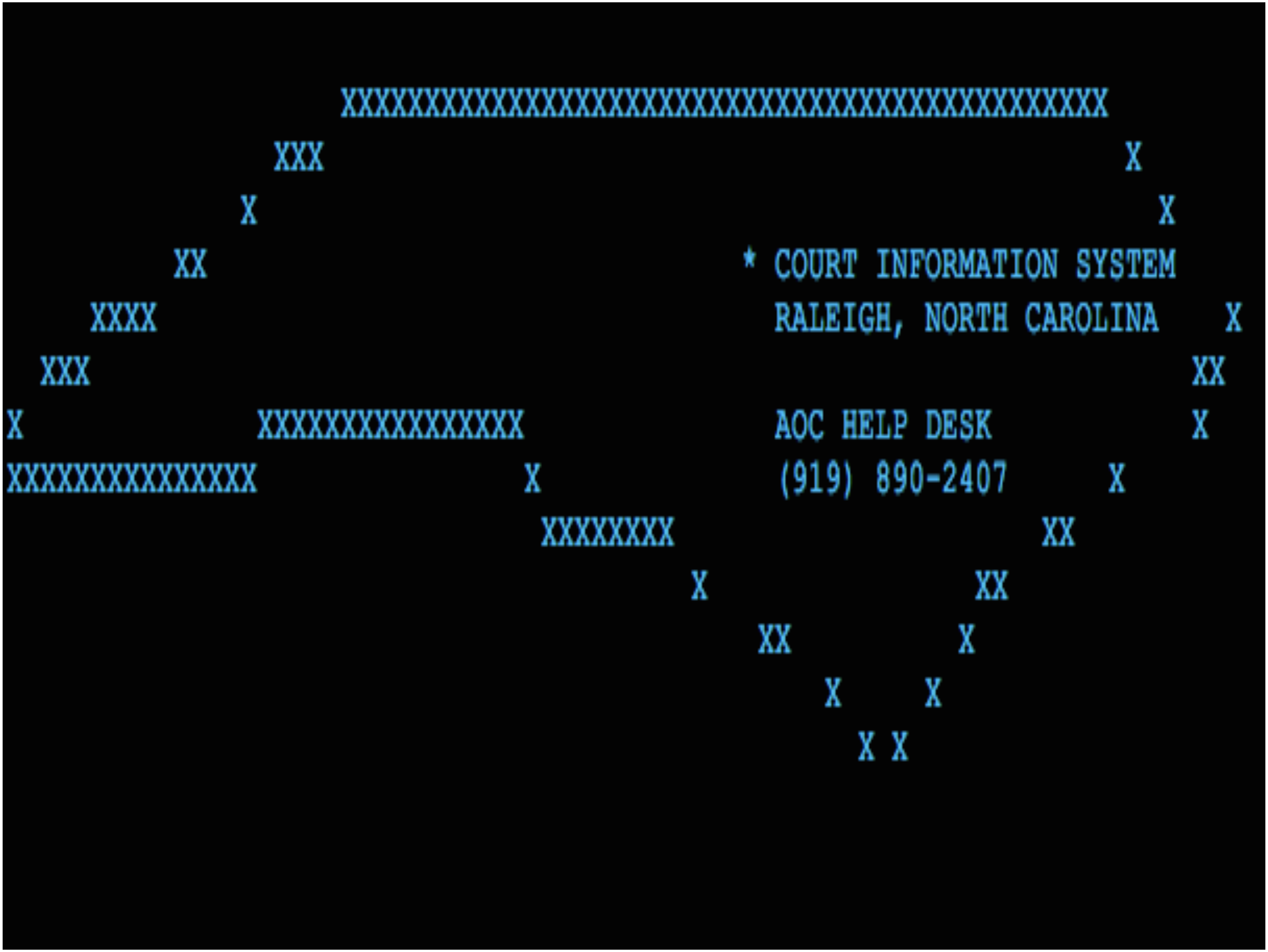
Some personal favorites:



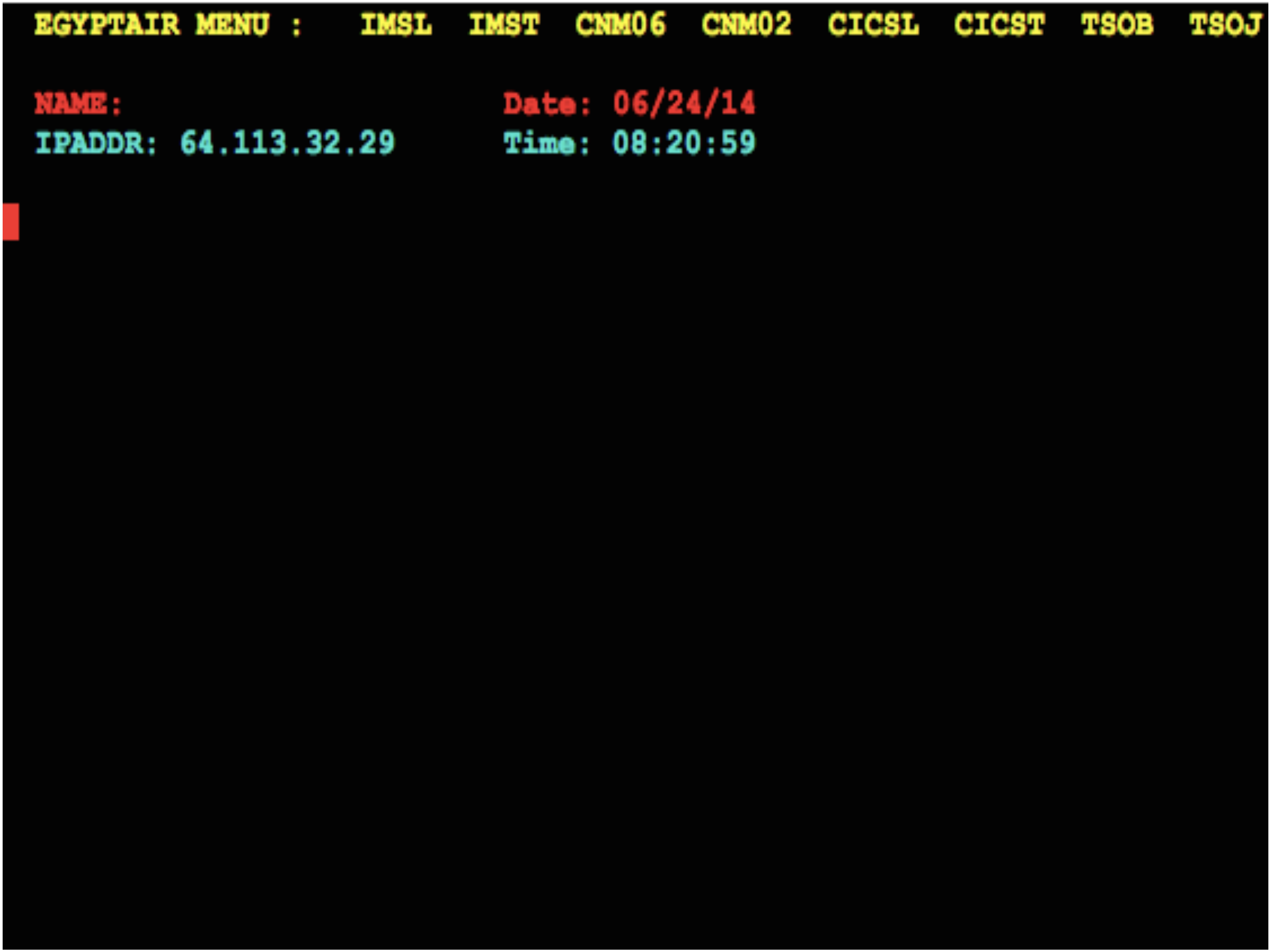
```
YOU ARE ACCESSING A U.S. GOVERNMENT (USG) INFORMATION SYSTEM (IS) THAT IS
PROVIDED FOR USG-AUTHORIZED USE ONLY. By using this (IS) (which includes any
device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC monitoring
network operations and defense, personnel misconduct (PM), law enforcement
(LE), counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be disclosed or used
for any USG authorized purpose.
-This IS includes security measures (e.g., authentication and access controls)
to protect USG interests--not for your personal benefit or privacy.
-Notwithstanding the above, using this IS does not constitute consent of
privileged communications, or work product, related to personal representation
or services by attorneys, psychotherapists, or clergy, and their assistants.
Such communications and work product are private and confidential.
See User Agreement for details.
                                                        Terminal Type:   3278-2A
                                                        Terminal id:     USRS1483
Enter Y to continue or PF3 to Logoff.                   Date:            04/30/14
   Accept:      _                                       Time:            10:25:02

                   PENSYS1.ARMY.PENTAGON.MIL
```



```
64.113.32.29             ISUZU NORTH AMERICA NETWORK                   TN3270



****   ***************  ****         ****  ***************   ****         ****
****  ****************  ****         ****  ****************  ****         ****
****  ****              ****         ****              ****  ****         ****
****      ****          ****         ****          ****      ****         ****
****          ****      ****         ****      ****          ****         ****
****              ****  ****         ****  ****              ****         ****
****  ****************  *****************  ****************  *****************
****  ***************    ***************    ***************   ***************



TYPE ONE OF THE FOLLOWING:

   TAO        <---- EMAIL/CALENDARS.       CICS3      <---- AIMI PROD ONLINE.
   TSO        <---- MVS TSO.               CICS4      <---- AIMI TEST ONLINE.



                            ICS.ISUZUNET.COM
```



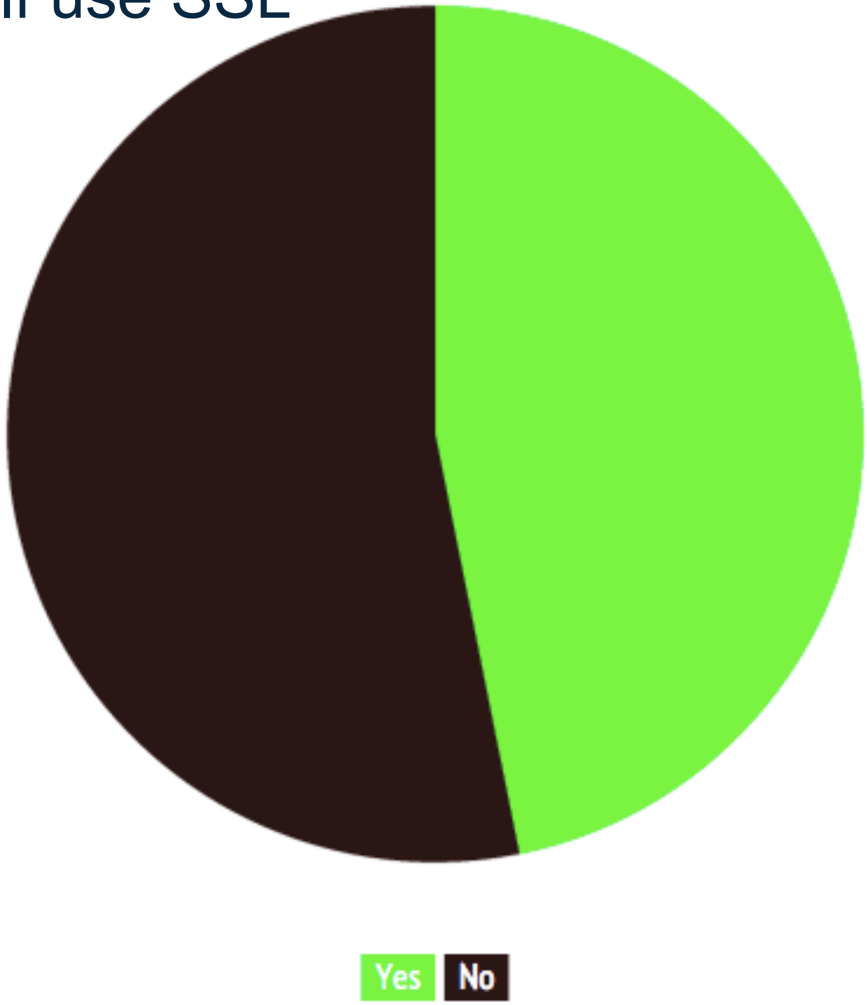
```
                    XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
                XXX                                                X
              X                                                      X
          XX                                * COURT INFORMATION SYSTEM
     XXXX                                     RALEIGH, NORTH CAROLINA    X
  XXX                                                                  XX
X              XXXXXXXXXXXXXXXX               AOC HELP DESK            X
XXXXXXXXXXXXXXX                X              (919) 890-2407      X
                                XXXXXXXX                      XX
                                         X                XX
                                             XX          X
                                                 X     X
                                                   X X
```



```
EGYPTAIR MENU :   IMSL  IMST  CNM06  CNM02  CICSL  CICST  TSOB  TSOJ

NAME:                        Date: 06/24/14
IPADDR: 64.113.32.29         Time: 08:20:59
```

Interesting Factoid

- Only about half use SSL



https://infogr.am/unencrypted_mainframes

Current Landscape

Current Testing

- Vulnerability Scanning
  - Using automated tools to scan a machine for known weaknesses
  - Usually detects lack of patches or configuration issues
- Penetration Testing
  - Black Box: No information known
  - White Box: Attacker has system information
  - Purpose: Identify potential security weaknesses

Penetration Testing

- Rarely performed on mainframes or mainframe applications
- Lack of skillsets and information
- Lack of demand from enterprise
- Concern for system outtages and downtime
- Mainframe organization political power

Vulnerability Scanning

- You’re being force to do it
- Standard processes being forced to fit
- Example: Qualys
  - Standard vulnerability scanning tool
  - Used all over the world
  - Supports both authenticated and unauthenticated scans

Completely useless outside of common issues

Why?

- Qualys doesn't support z/OS
- IBM (and Vendors) don't publicly release security vulnerabilities

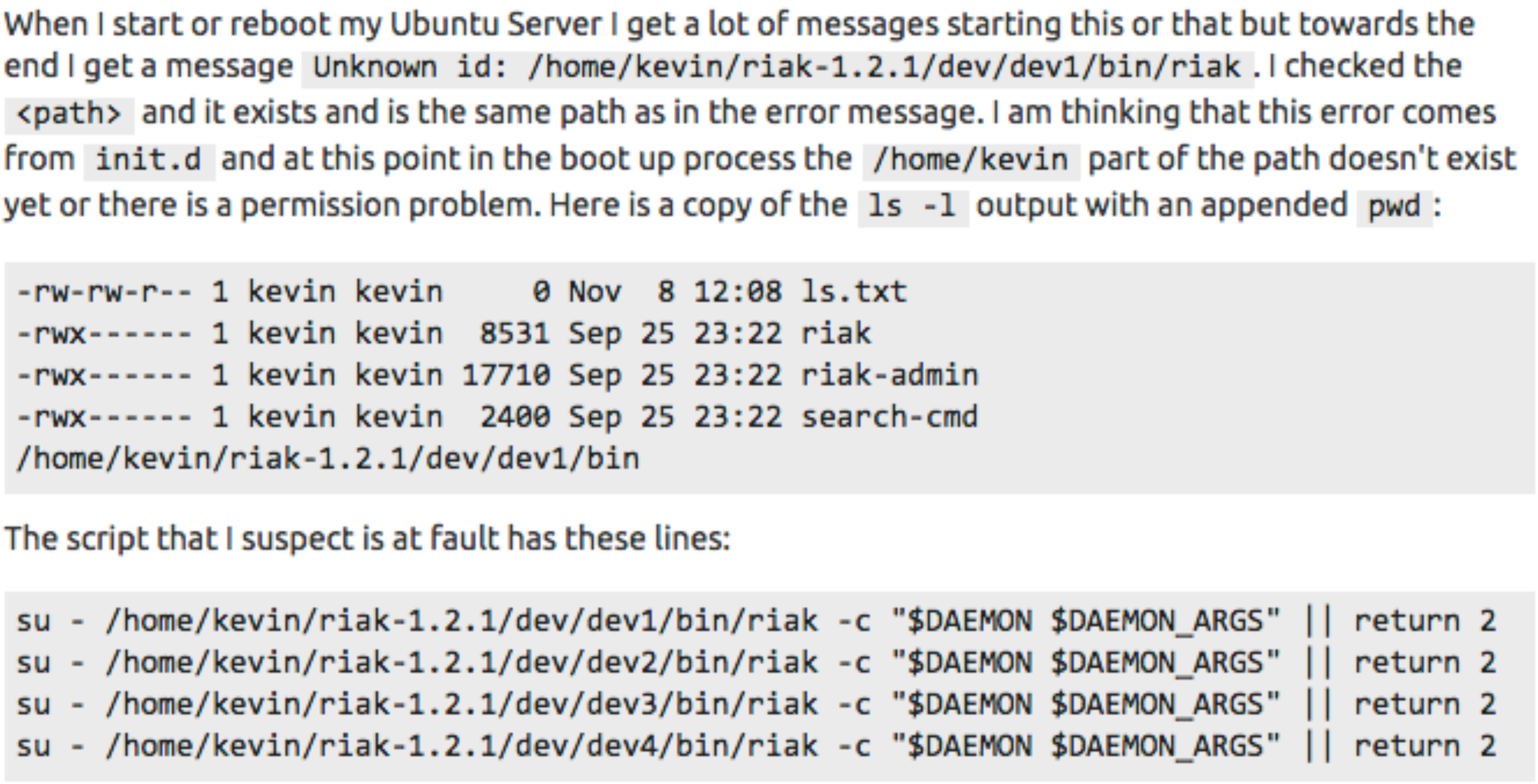
Resulting in:

- Compliance scans only catching small issues
  - E.G. Older version of apache
- False sense of security
- Appeasing PCI gods

The Community

- Really hard to break in to
- Pay to participate model
- Closed off and silo’d
- Compare to open source community:

Opensource Community



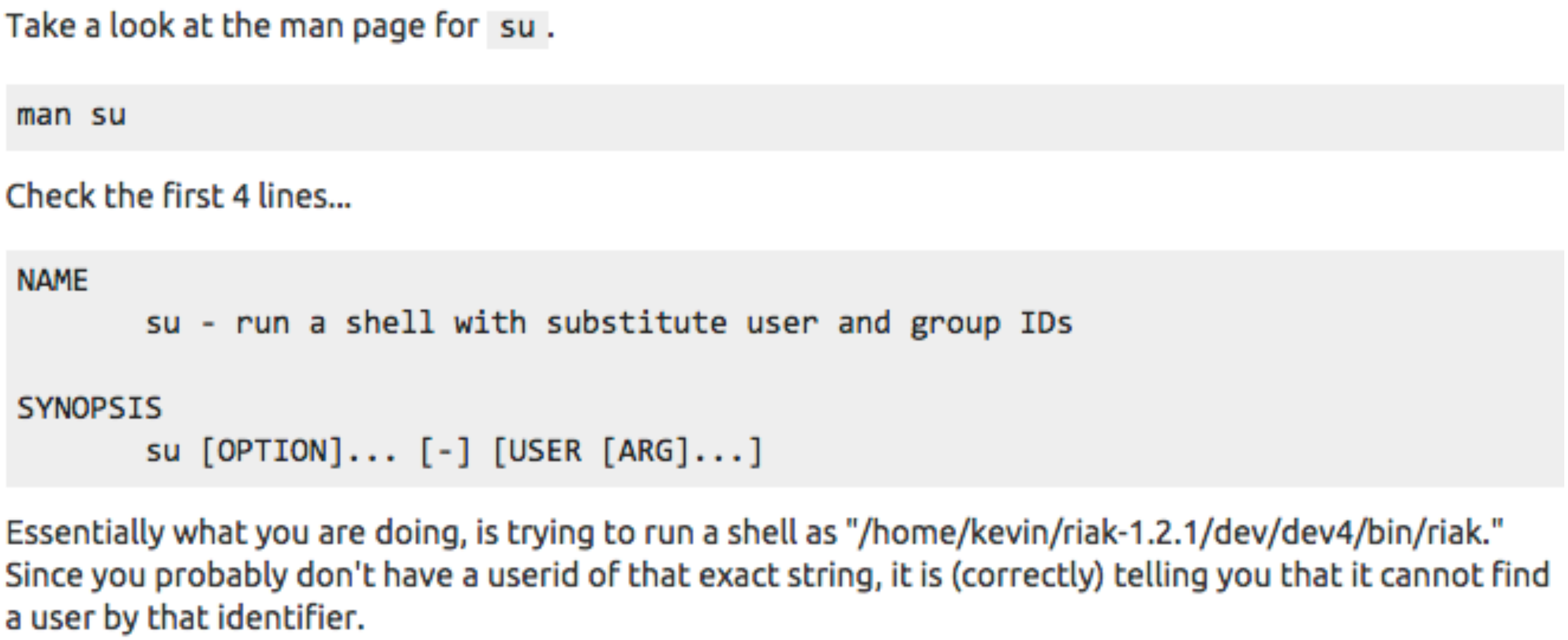
When I start or reboot my Ubuntu Server I get a lot of messages starting this or that but towards the end I get a message `Unknown id: /home/kevin/riak-1.2.1/dev/dev1/bin/riak`. I checked the `<path>` and it exists and is the same path as in the error message. I am thinking that this error comes from `init.d` and at this point in the boot up process the `/home/kevin` part of the path doesn't exist yet or there is a permission problem. Here is a copy of the `ls -l` output with an appended `pwd`:

```
-rw-rw-r-- 1 kevin kevin     0 Nov  8 12:08 ls.txt
-rwx------ 1 kevin kevin  8531 Sep 25 23:22 riak
-rwx------ 1 kevin kevin 17710 Sep 25 23:22 riak-admin
-rwx------ 1 kevin kevin  2400 Sep 25 23:22 search-cmd
/home/kevin/riak-1.2.1/dev/dev1/bin
```

The script that I suspect is at fault has these lines:

```
su - /home/kevin/riak-1.2.1/dev/dev1/bin/riak -c "$DAEMON $DAEMON_ARGS" || return 2
su - /home/kevin/riak-1.2.1/dev/dev2/bin/riak -c "$DAEMON $DAEMON_ARGS" || return 2
su - /home/kevin/riak-1.2.1/dev/dev3/bin/riak -c "$DAEMON $DAEMON_ARGS" || return 2
su - /home/kevin/riak-1.2.1/dev/dev4/bin/riak -c "$DAEMON $DAEMON_ARGS" || return 2
```

Opensource Community



Take a look at the man page for `su`.

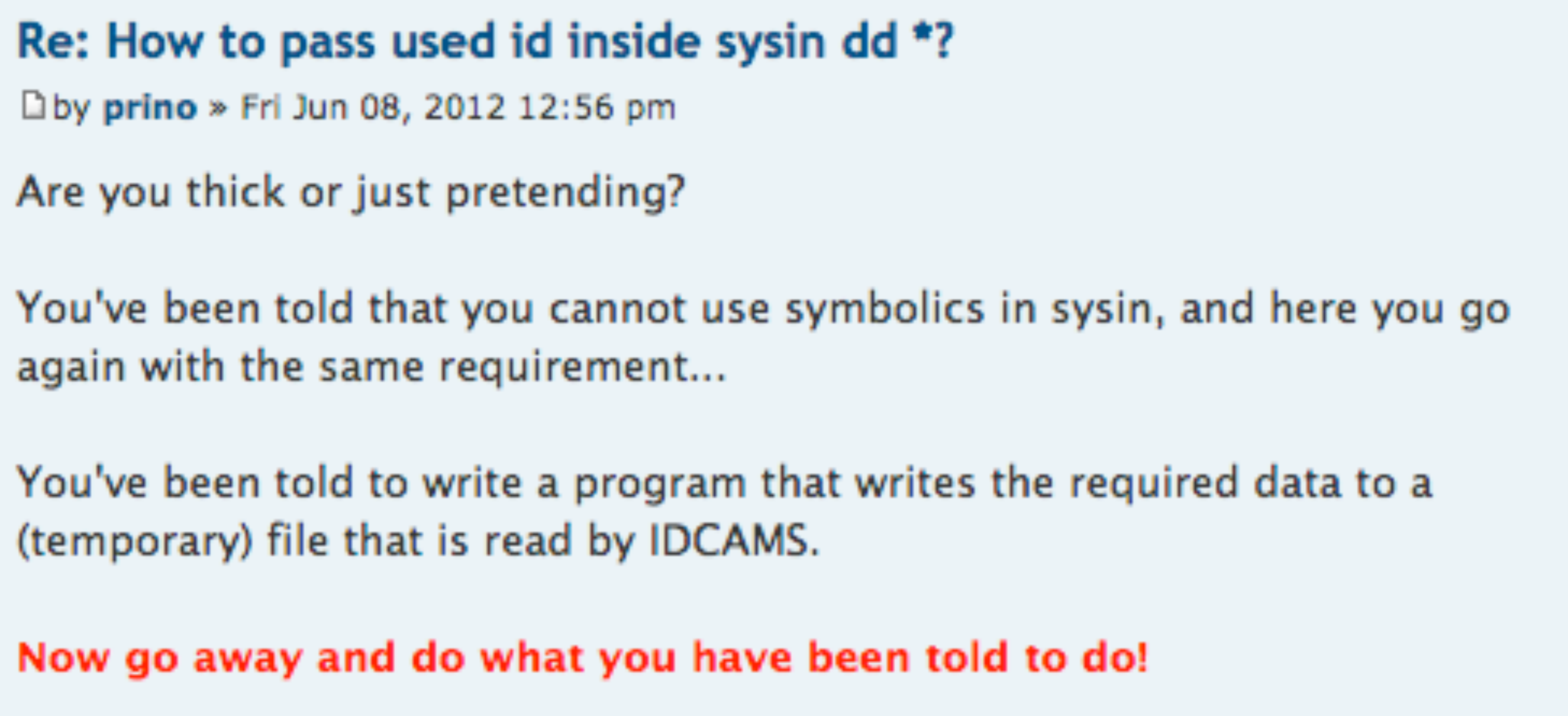
```
man su
```

Check the first 4 lines...

```
NAME
       su - run a shell with substitute user and group IDs

SYNOPSIS
       su [OPTION]... [-] [USER [ARG]...]
```

Essentially what you are doing, is trying to run a shell as "/home/kevin/riak-1.2.1/dev/dev4/bin/riak." Since you probably don't have a userid of that exact string, it is (correctly) telling you that it cannot find a user by that identifier.

z/OS “Community”



Re: How to pass used id inside sysin dd *?

by **prino** » Fri Jun 08, 2012 12:56 pm

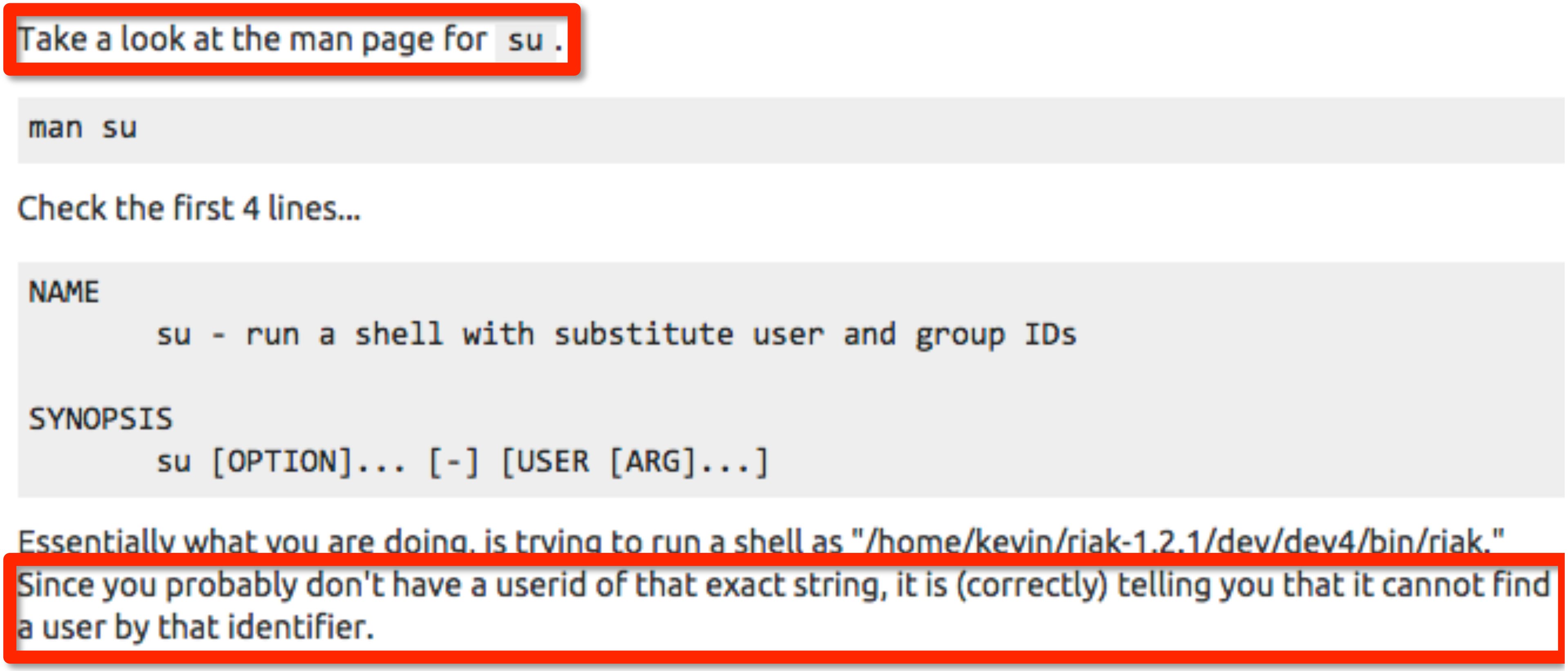
Are you thick or just pretending?

You've been told that you cannot use symbolics in sysin, and here you go again with the same requirement...

You've been told to write a program that writes the required data to a (temporary) file that is read by IDCAMS.

Now go away and do what you have been told to do!

Opensource Community



Take a look at the man page for `su`.

```
man su
```

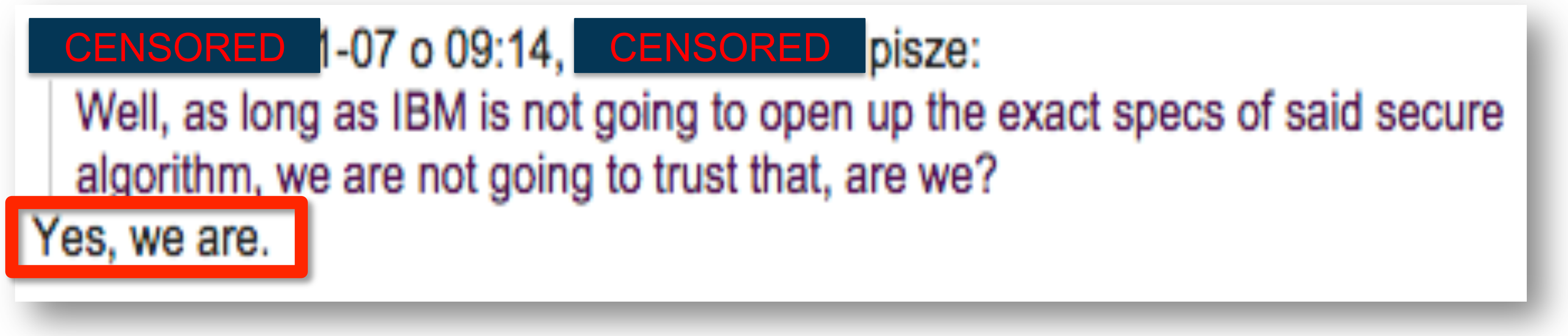
Check the first 4 lines...

```
NAME
       su - run a shell with substitute user and group IDs

SYNOPSIS
       su [OPTION]... [-] [USER [ARG]...]
```

Essentially what you are doing, is trying to run a shell as "/home/kevin/riak-1.2.1/dev/dev4/bin/riak." Since you probably don't have a userid of that exact string, it is (correctly) telling you that it cannot find a user by that identifier.

Vendor Trust

- A lot of trust is placed on operating system and software vendors (when it comes to security)
- Example:



CENSORED -07 o 09:14, CENSORED pisze:

> Well, as long as IBM is not going to open up the exact specs of said secure algorithm, we are not going to trust that, are we?

Yes, we are.

The Hackers are Coming

When I started - 2012

- Prior to 2012:
  - Some forum posts
  - No public discussion
  - No tools support
  - Complete misunderstanding

Trouble for asking simple question!

2012 – It's starting

- Gave first public talk
- Asked simple question on offline cracking tool mailing list
  - John the Ripper
- With significant help from Nigel Pentland and Dhiru Kolia added support for RACF
- Started Mainframe Security Blog:
  - mainframed767.tumblr.com

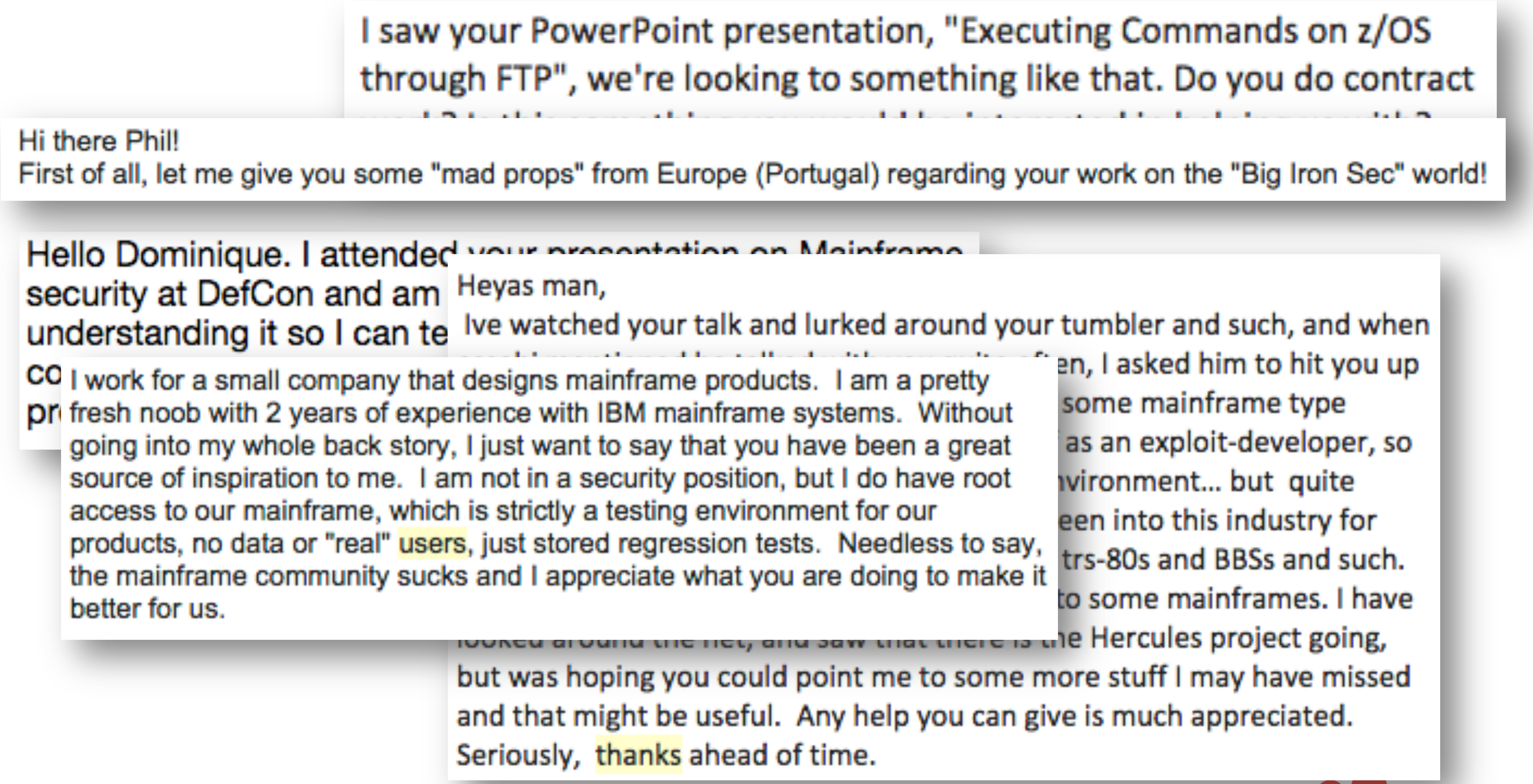
Not a single email

2013 & 2014 – Years of Talks

- Gave 10 talks in 2013/2014
  - 8 in US
  - 1 in Sweden
  - 1 in Hungary

- Created new tools, or added support for mainframe applications
  - Man in the Middle TSO connections
  - Enumerate user IDs
  - OMVS Privilege Escalation
  - Netcat + ebcdic

Interest in the Community



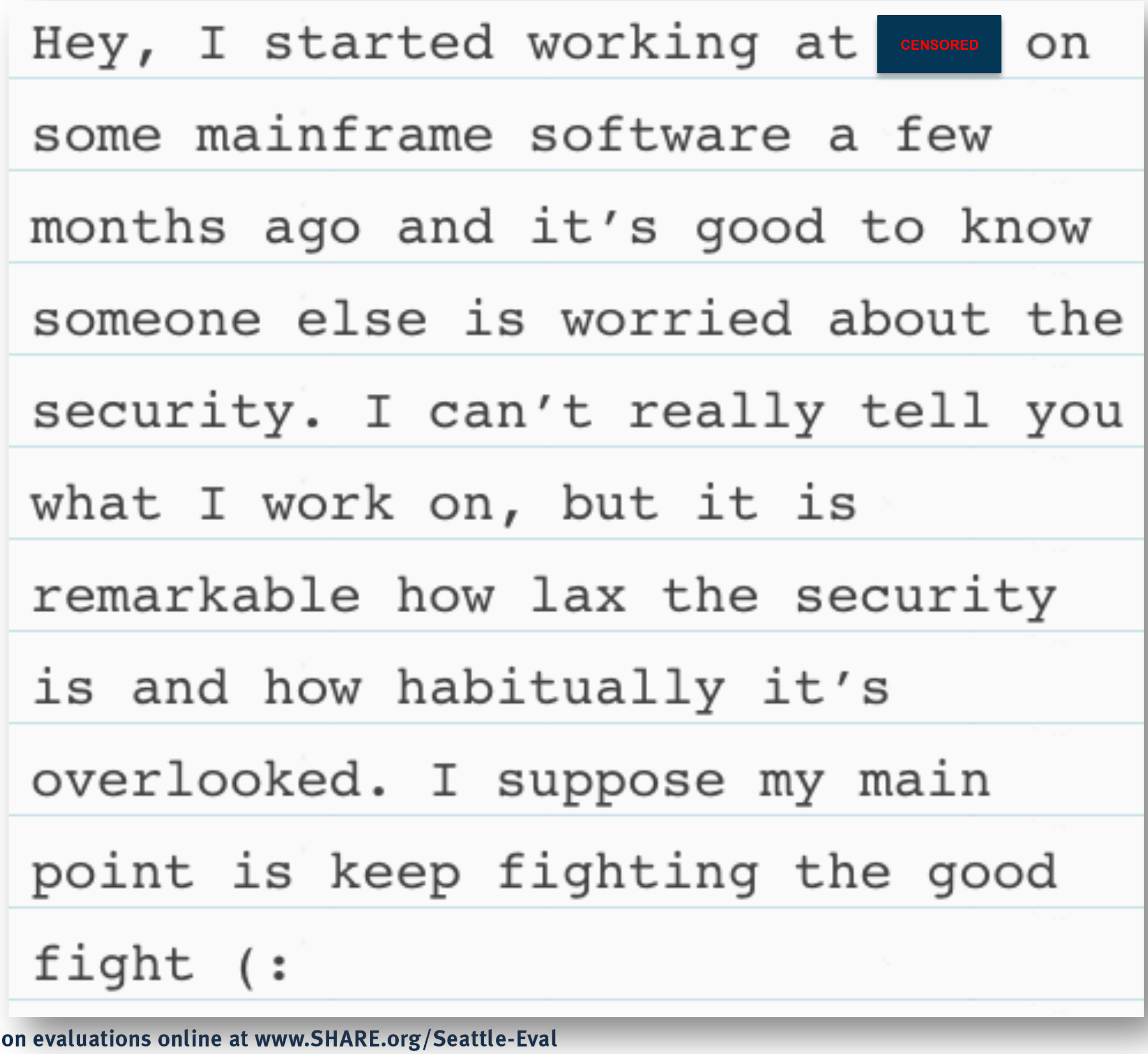
I saw your PowerPoint presentation, "Executing Commands on z/OS through FTP", we're looking to something like that. Do you do contract

Hi there Phil!
First of all, let me give you some "mad props" from Europe (Portugal) regarding your work on the "Big Iron Sec" world!

Hello Dominique. I attended
security at DefCon and am
understanding it so I can te
co
pr

I work for a small company that designs mainframe products. I am a pretty fresh noob with 2 years of experience with IBM mainframe systems. Without going into my whole back story, I just want to say that you have been a great source of inspiration to me. I am not in a security position, but I do have root access to our mainframe, which is strictly a testing environment for our products, no data or "real" users, just stored regression tests. Needless to say, the mainframe community sucks and I appreciate what you are doing to make it better for us.

Heyas man,
Ive watched your talk and lurked around your tumbler and such, and when
en, I asked him to hit you up
some mainframe type
as an exploit-developer, so
nvironment... but quite
een into this industry for
trs-80s and BBSs and such.
to some mainframes. I have
e Hercules project going,
but was hoping you could point me to some more stuff I may have missed
and that might be useful. Any help you can give is much appreciated.
Seriously, thanks ahead of time.



Hey, I started working at CENSORED on some mainframe software a few months ago and it's good to know someone else is worried about the security. I can't really tell you what I work on, but it is remarkable how lax the security is and how habitually it's overlooked. I suppose my main point is keep fighting the good fight (:

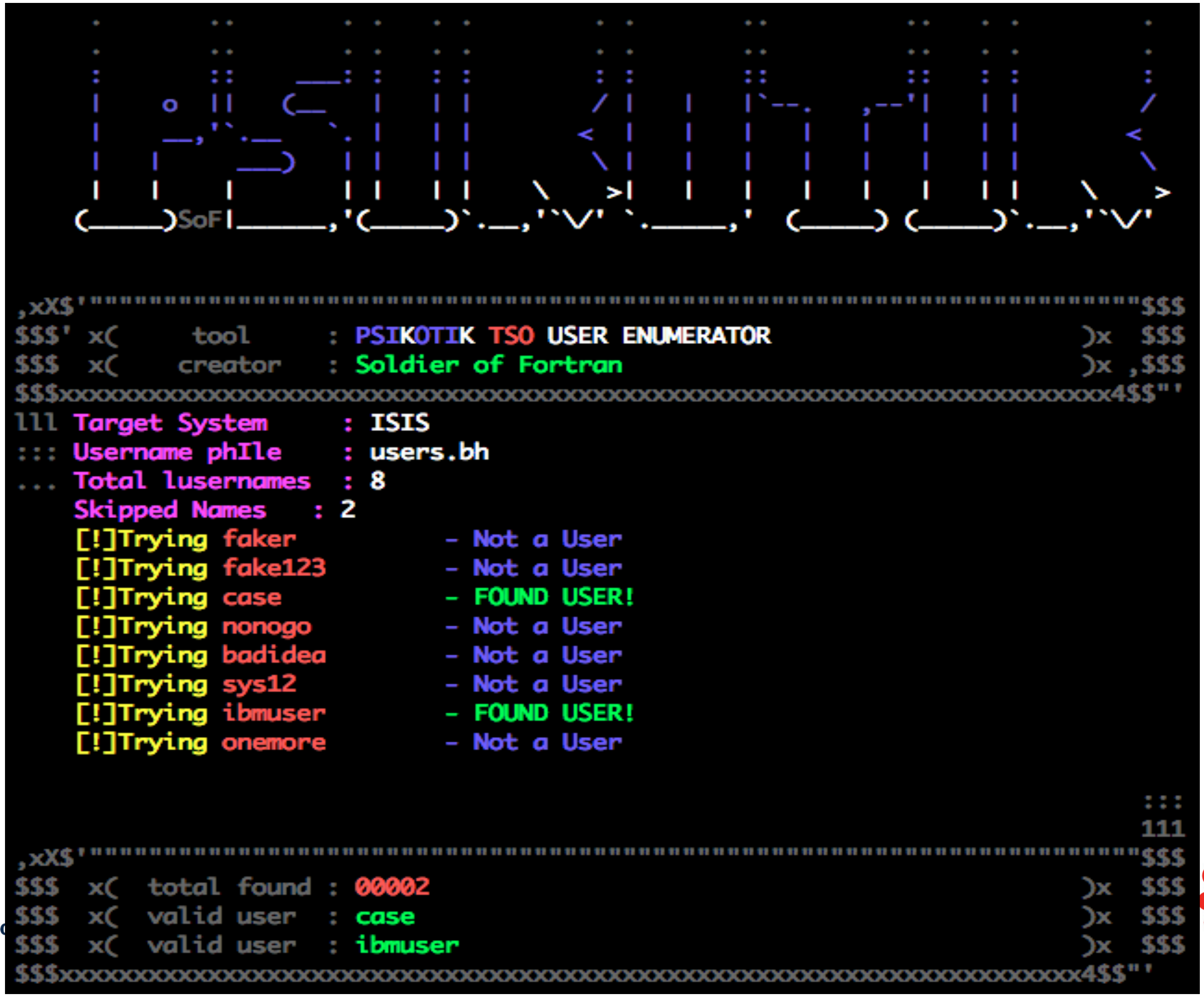
Then There Were Two

- Dominic White
- Gave a talk at Hack in the Box and DerbyCon in 2014
- Discussed vulnerabilities at TN3270 level
- Developed two applications:
  - Big Iron Reconnaissance and Pwnage
  - Mainframe Brute

Talk available online:

https://www.youtube.com/watch?v=3HFiv7NvWrM

User Enumeration

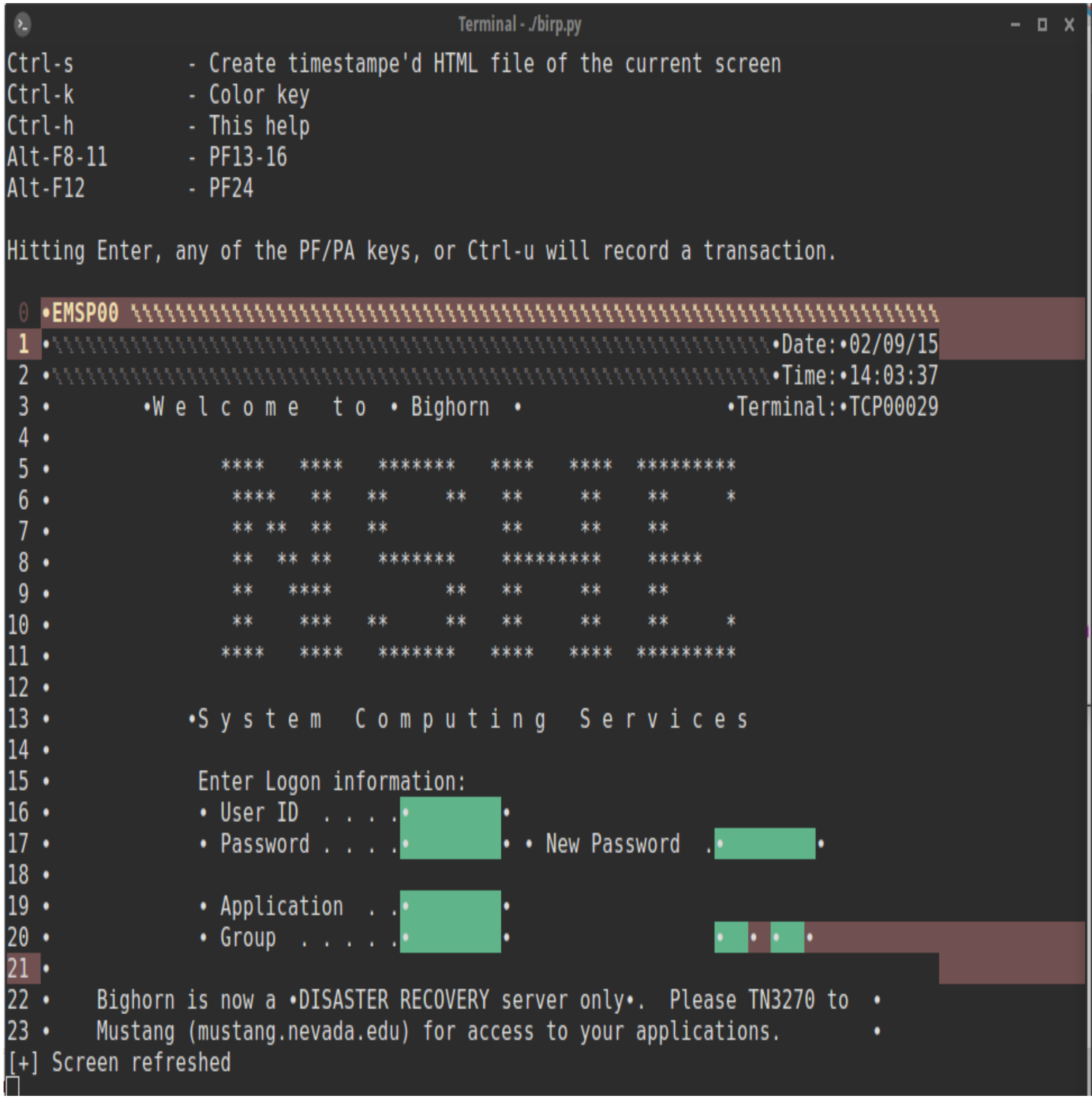


```
(____)SoF|

,xX$'"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""$$$
$$$' x(     tool      : PSIKOTIK TSO USER ENUMERATOR              )x  $$$
$$$  x(    creator    : Soldier of Fortran                        )x ,$$$
$$$xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4$$"'
lll Target System      : ISIS
::: Username phIle     : users.bh
... Total lusernames   : 8
    Skipped Names    : 2
    [!]Trying faker           - Not a User
    [!]Trying fake123         - Not a User
    [!]Trying case            - FOUND USER!
    [!]Trying nonogo          - Not a User
    [!]Trying badidea         - Not a User
    [!]Trying sys12           - Not a User
    [!]Trying ibmuser         - FOUND USER!
    [!]Trying onemore         - Not a User


                                                                      :::
                                                                      lll
,xX$'"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""$$$
$$$  x(  total found : 00002                                      )x  $$$
$$$  x(  valid user  : case                                       )x  $$$
$$$  x(  valid user  : ibmuser                                    )x  $$$
$$$xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4$$"'
```

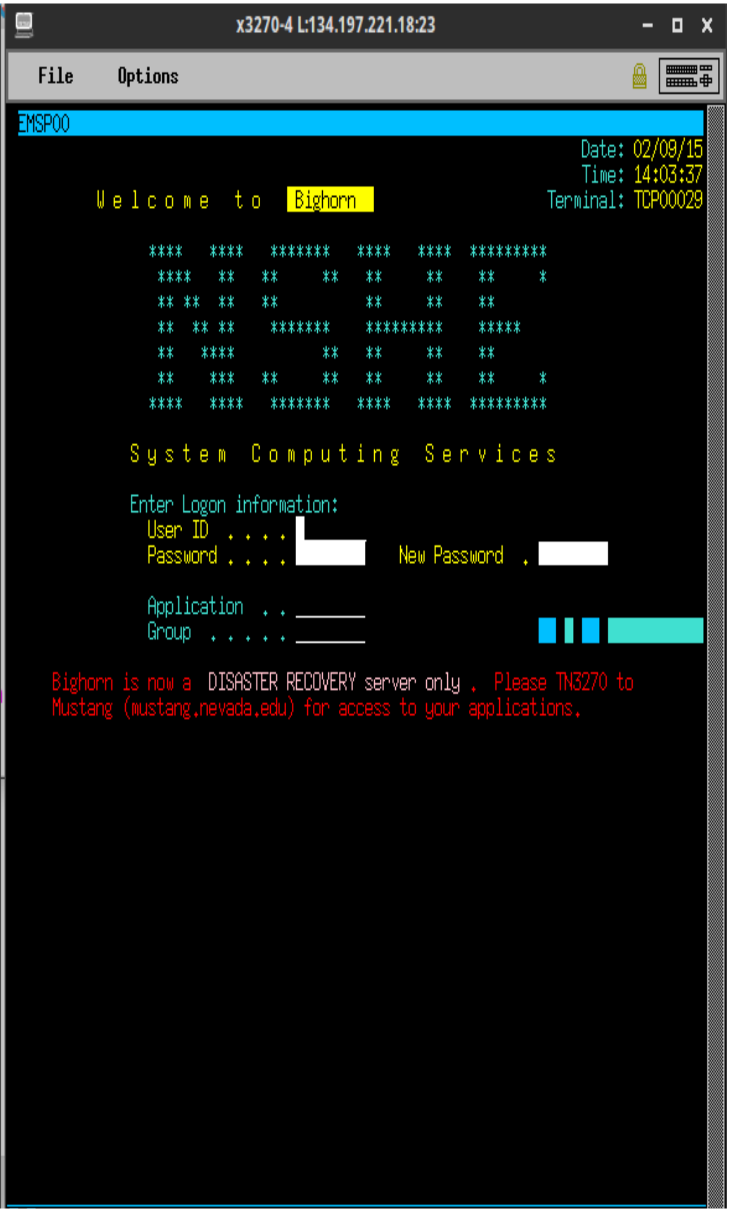
REXX SetUID Exploit

```
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
```

BIRP

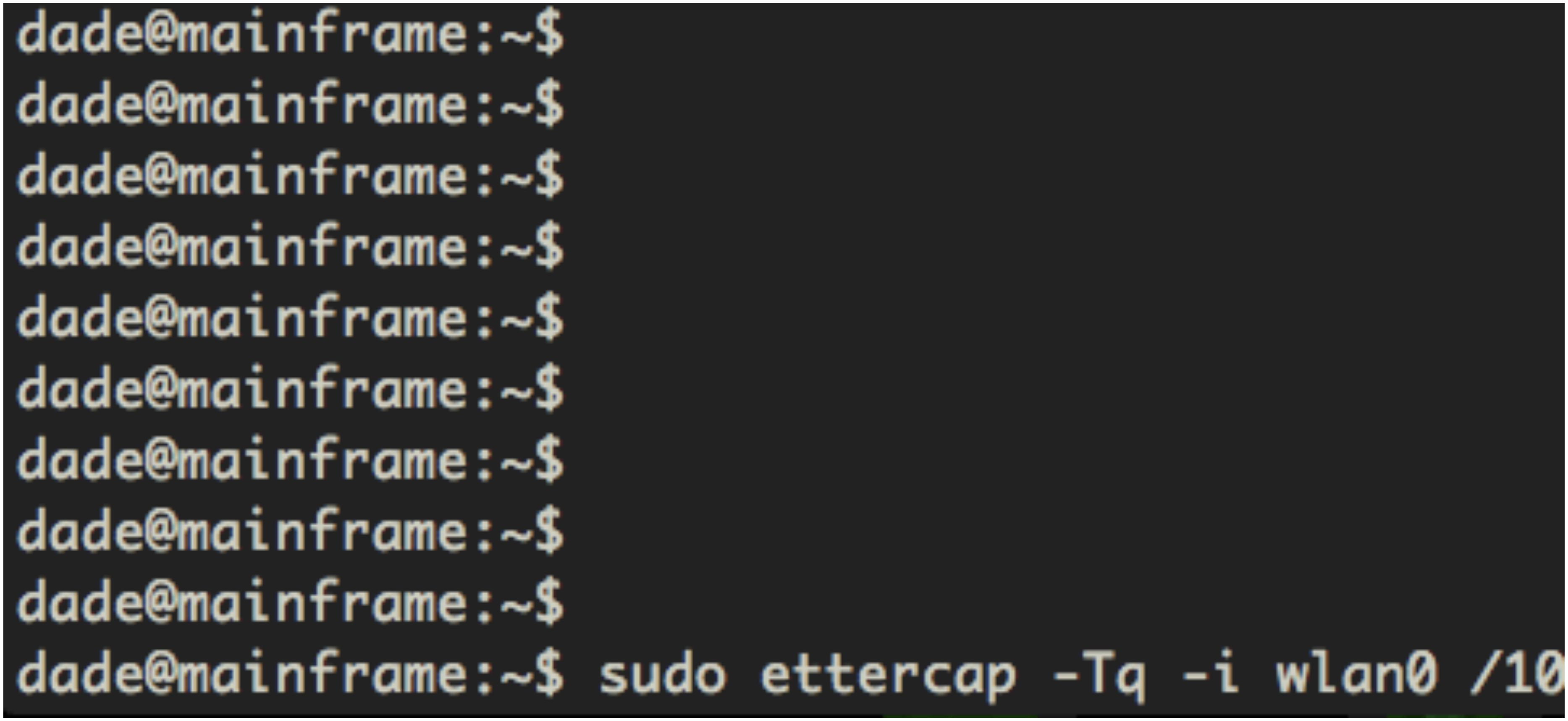


```
Ctrl-s        - Create timestampe'd HTML file of the current screen
Ctrl-k        - Color key
Ctrl-h        - This help
Alt-F8-11     - PF13-16
Alt-F12       - PF24

Hitting Enter, any of the PF/PA keys, or Ctrl-u will record a transaction.

 0 •EMSP00 \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
 1 •\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\•Date:•02/09/15
 2 •\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\•Time:•14:03:37
 3 •       •W e l c o m e   t o  • Bighorn  •               •Terminal:•TCP00029
 4 •
 5 •              ****   ****   *******   ****   ****  *********
 6 •               ****   **   **     **   **     **    **     *
 7 •               ** **  **   **          **     **    **
 8 •               **  ** **    *******    *********    *****
 9 •               **   ****          **   **     **    **
10 •               **    ***   **     **   **     **    **     *
11 •              ****   ****   *******   ****   ****  *********
12 •
13 •          •S y s t e m   C o m p u t i n g   S e r v i c e s
14 •
15 •           Enter Logon information:
16 •           • User ID  . . . .•        •
17 •           • Password . . . .•        • • New Password  .•        •
18 •
19 •           • Application  . .•        •
20 •           • Group  . . . . .•        •                     • •  • •
21 •
22 •    Bighorn is now a •DISASTER RECOVERY server only•.  Please TN3270 to  •
23 •    Mustang (mustang.nevada.edu) for access to your applications.        •
[+] Screen refreshed
```



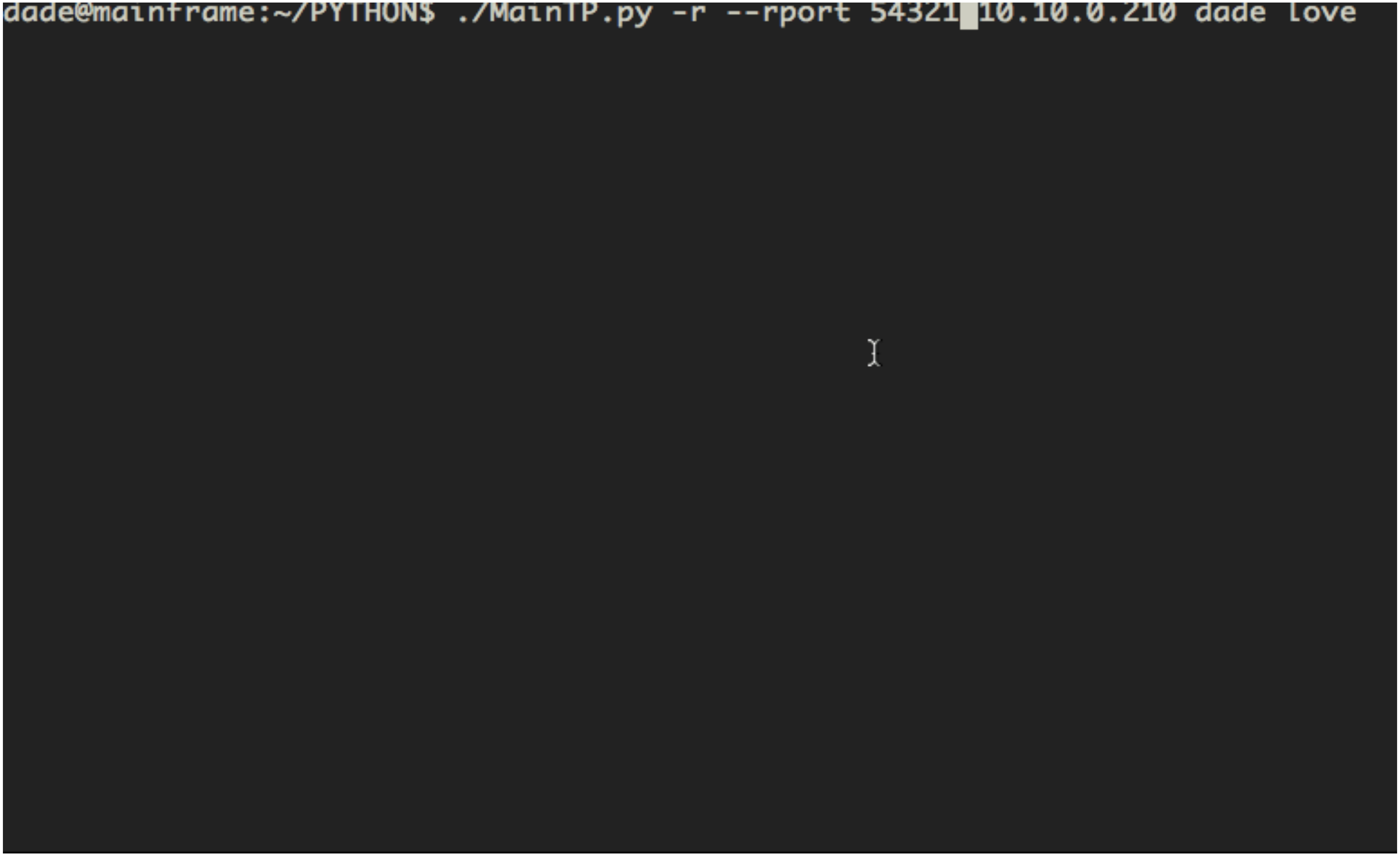
```
EMSP00
                                                              Date: 02/09/15
                                                              Time: 14:03:37
       W e l c o m e   t o   Bighorn                      Terminal: TCP00029

              ****   ****   *******   ****   ****  *********
               ****   **   **     **   **     **    **     *
               ** **  **   **          **     **    **
               **  ** **    *******    *********    *****
               **   ****          **   **     **    **
               **    ***   **     **   **     **    **     *
              ****   ****   *******   ****   ****  *********

          S y s t e m   C o m p u t i n g   S e r v i c e s

          Enter Logon information:
            User ID  . . . .
            Password . . . .           New Password  .

            Application  . .
            Group  . . . . .

    Bighorn is now a  DISASTER RECOVERY server only .  Please TN3270 to
    Mustang (mustang.nevada.edu) for access to your applications.
```

MitM TSO Credential Stealing

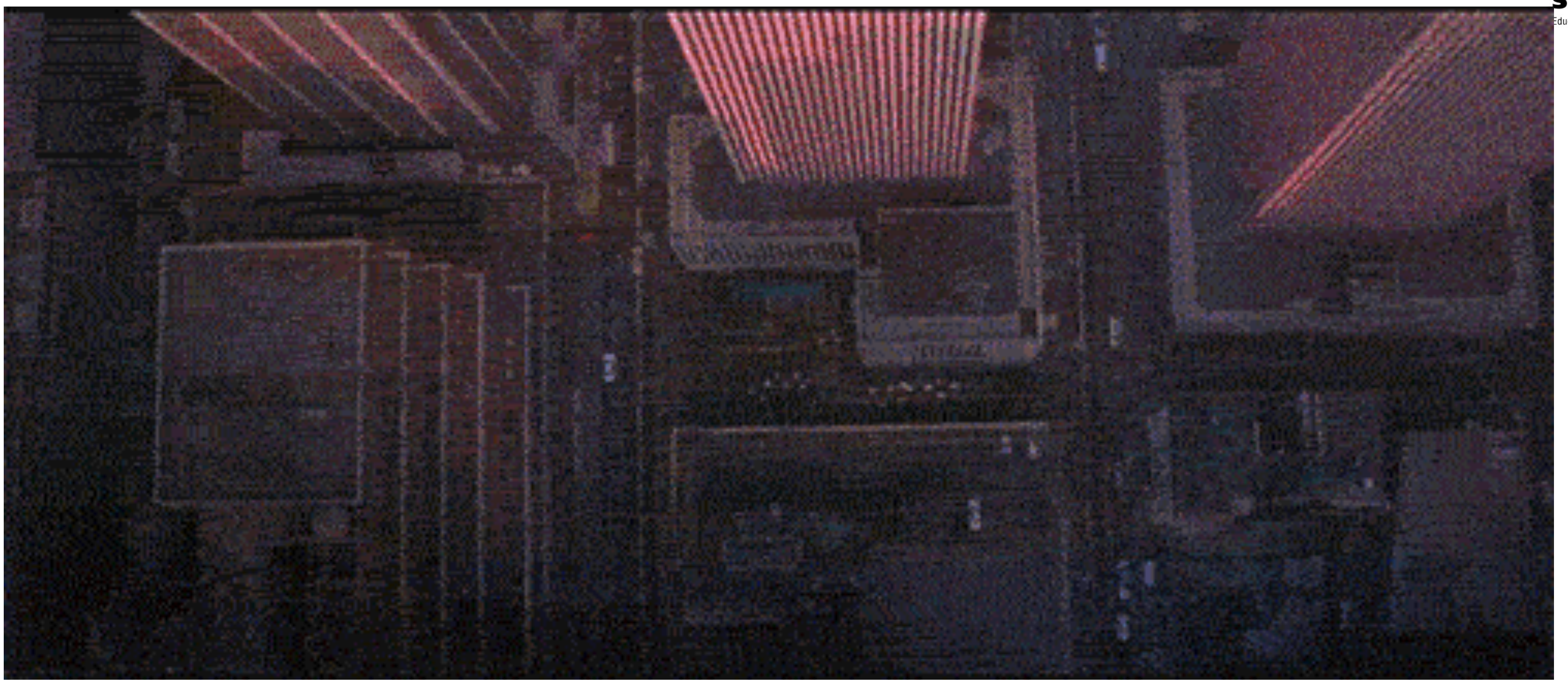


```
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$ sudo ettercap -Tq -i wlan0 /10
```

MainTP – FTP + JCL + REXX + C =



```
dade@mainframe:~/PYTHON$ ./MainTP.py -r --rport 54321 10.10.0.210 dade love
```



Logica and Nordea Breach

Pirate Bay co-founder charged with hacking IBM mainframes, stealing money

Loek Essers
@loekessers

Apr 16, 2013 9:05 AM

Pirate Bay co-founder Gottfrid Svartholm Warg was charged with hacking the IBM mainframe of Logica, a Swedish IT firm that provided tax services to the Swedish government, and the IBM mainframe of the Swedish Nordea bank, the Swedish public prosecutor said on Tuesday.

"This is the biggest investigation into data intrusion ever performed in Sweden," said public prosecutor Henrik Olin.

Besides Svartholm Warg, the prosecution charged three other Swedish citizens.

Two of them live in Malmö and provided accounts for money transfers while one other—who lives in the middle of Sweder—was charged with mainframe hacking, Olin said.

The third man and Svartholm Warg were also charged with hacking into the Bisnode webservice system that is part of Logica's mainframe environment, Olin added.

2012

- Anakata:
  - Created PirateBay
  - Was sued by Swedish RIAA
  - Fled to Cambodia
- Cambodian Hackers
  - Break in to neighbors wifi
  - Target Swedish RIAA lawyer
  - steal her credentials for a Swedish government application

Anakata discovers this application runs on z/OS

Next Steps

- Installs Hercules
  - Hercules is a zSeries CPU emulator
  - Allows you to run z/OS on commodity hardware
  - Check out Tur(n)key MVS for public domain OS
  - Also runs z/OS
- Obtains z/OS R1V9
- Develops two zero day attacks, multiple backdoors, code, etc

Zero Days

- CVE-2012-5951
  - Local Privilege Escalation
  - Uses REXX and spawn function
  - Exploits SetUID files to get UID 0 in OMVS
  - Script: kuku.rx
- CVE-2012-5955
  - CGI-BIN parser flaw*
  - Passing ‘;’ to parser allowed command execution
  - Script: UTCam.sh

All scripts available at: https://github.com/mainframed/logica

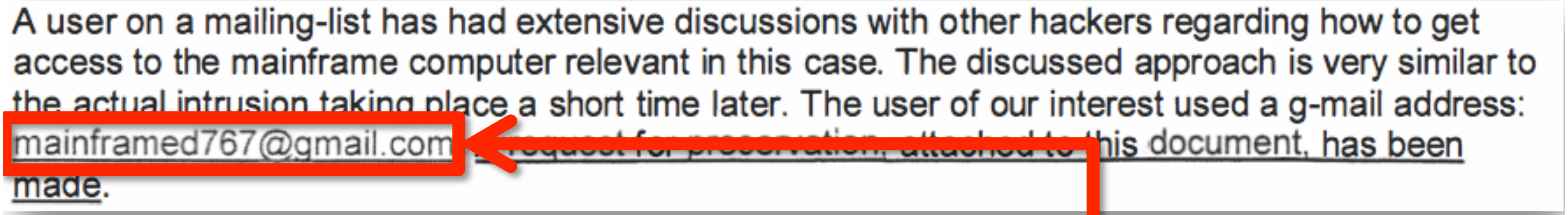
* This is just a guess. IBM doesn’t share details

Backdoors

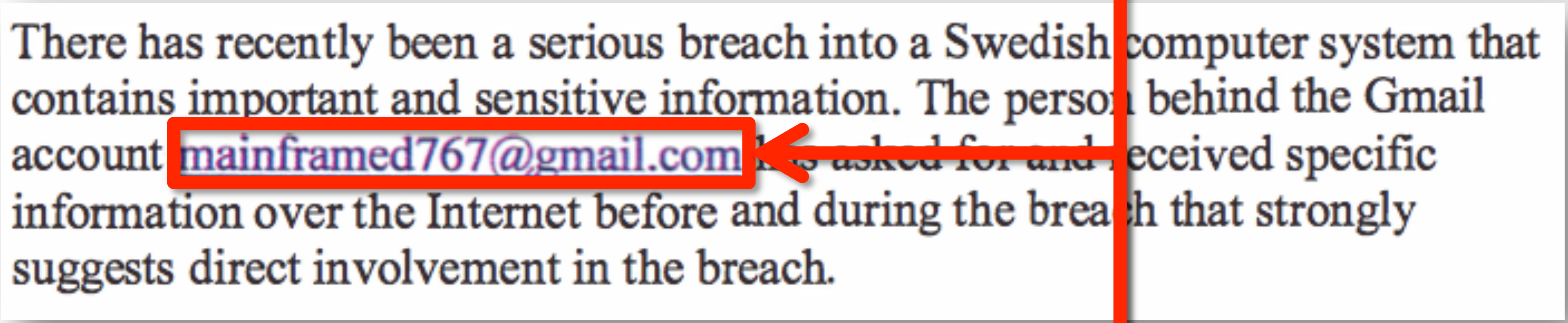
- 8 C programs to execute a root shell were uploaded:
  - asd, be, err, d044, qwe, daf1367, daf1473 and e90opc, a.env
- a.env was reworked and eventually became CSQXDISP
  - A program calling home on port 443
  - A custom interpreter phoning home
- INETD was changed (root shell on port 443)
- SSH keys added
- Custom assembly to disable RACF (Tfy.source.backdoor)

All scripts available at: https://github.com/mainframed/logica

I’m in Trouble



A user on a mailing-list has had extensive discussions with other hackers regarding how to get access to the mainframe computer relevant in this case. The discussed approach is very similar to the actual intrusion taking place a short time later. The user of our interest used a g-mail address: mainframed767@gmail.com A request for preservation, attached to this document, has been made.



There has recently been a serious breach into a Swedish computer system that contains important and sensitive information. The person behind the Gmail account mainframed767@gmail.com has asked for and received specific information over the Internet before and during the breach that strongly suggests direct involvement in the breach.

That’s me!

More Information

- Read the detailed investigation
  - Most of it is in Swedish
- Read the (few) news articles
- Buy me a beer

OR

Come see my hour long talk just about the breach!

Embrace the Community

Nothing to be Afraid Of

- Hacker isn't a bad word

- Not all Hackers are Bad
  - not all 14,000 people at DEFCON are evil, just some
- It's already started
  - You invited me here!
- Demand in the hacker community
- Change their opinion of you

Where to Start?

- It starts with you
- Invite the 'Hackers' in
  - No, not really, just your internal security people
  - Show them the ways
  - Be patient
  - Answer questions

- Learn from them!

Work With Us, Not Against

- Mainframes aren’t going anywhere
  - Neither is security
- Want to make them as secure as possible
- View security as a partner
- Security experts will eventually poke around, either by
  - audit mandate
  - Executive Management concerns
  - Red Team exercises

Might as well be at the table

The Future

- Capture the Flag Events
  - Contests with vulnerable systems
- Pwn 2 Own participation
  - Application compete to prove they can’t be hacked
- CDCC Participation
  - Next generation of system administrators compete to keep ‘hackers’ out
- Open sharing of known vulnerabilities
  - Better integration with tools and general openess of the platform