Gibson 101

QUICK INTRODUCTION TO HACKING MAINFRAMES IN 2020

Thanks

- You awesome people for being here
- Phil (Soldier of Fortran - @mainframed767)
- Chad (@bigendiansmalls)
- Ayoub (@ayoul3__)
- Many other mainframe security researchers

Ref: https://rlv.zcache.com/funny_japanese_akita_with_cute_smile_thank_you_card-r7c85cc2bcb8f48a5b29047d2781ed5f4_xvuat_8byvr_324.jpg

About Me

- Organizer – BSides Singapore
- Principal Security Consultant at SEC Consult – Singapore
- Do the H4kS on daily basis – Web, Mobile apps & Infra mainly
- 7+ years in Information Security
- Author of XVWA – WebAppSec learning app
- Interested in Windows Exploit development, SDR & Mainframes
- Licensed Scuba/Sky diver
- Travels in free time (https://www.aroundtheglobe.life/)
- Tweet me ***@samanl33t***

What to expect …

- Basic Idea of Mainframe systems
- Lots of new words and terminologies
- Probable overflow of Information in 1 hour.
- Attack kill-chain for Mainframes
- Demos (Yes!)
- (Hopefully) a trigger for curiosity about mainframes

What is a Mainframe?

This..

Ref: https://www.dailyhostnews.com/wp-content/uploads/2018/04/derver-1050x600.jpg

What is a Mainframe

And this..

Ref: https://upload.wikimedia.org/wikipedia/commons/thumb/f/fc/Glowing_IBM_z13_and_clock_-_cropped.JPG/1200px-Glowing_IBM_z13_and_clock_-_cropped.JPG

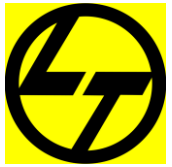
What is a Mainframe?

- Mainly Z/OS or IBM system Z
- Not AS400 (System i)
- Widely used Business critical system – Banks, Insurance, Airlines..
- Not Legacy – IBMZ15 released few months ago.
- Available since 1950s
- Handles millions of Input/output per second.
- God of backwards compatibility
- Built for RAS (Reliability, Availability, Serviceability)
- Supports many languages – HLASM, COBOL, C, Java, JCL, REXX, CLIST, Python etc.

z15 Specs

- 190 processors – 12 core, 5.2 GHz each
- 40 TB of RAM
- Dedicated processors for managing I/O
- Dedicated processors for Encryption/Decryption

Why is this relevant?



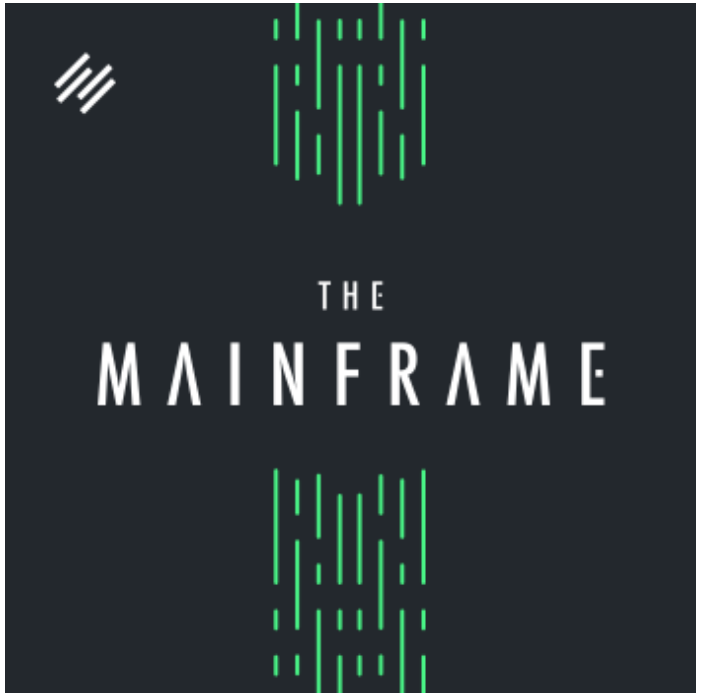

Ref: http://ibmmainframes.com/references/a41.html

z/OS Terminal

```
Enterprise Computing                          Local IP Address = 106.204.196.217
Enterprise Thinking                             http://mtm2019.mybluemix.net

              December 31, 2019 was last day of Master the Mainframe contest

                                //  OOOOOOO  SSSSSSS
                               //  OO    OO SS
                        zzzzzz //  OO    OO SS
                          zz  //  OO    OO   SSSS
                        zz   //  OO    OO       SS
                      zz    //  OO    OO       SS
                    zzzzzz //   OOOOOOO  SSSSSSS

                     IBM Z, The Next Generation

                  z/OS Runs the Economy of the World


 ===> Enter "logon" followed by the TSO userid. Example "logon userid" or
 ===> Enter TSO
```

Talking Mainframe..

- LPARS – Logical Partitions (Hosts/Servers)
- VTAM – Virtual Telecommunications Access method
- DASD – Direct Access Storage Devices (Basically hard drives)
- Storage – Memory
- TSO – Time Sharing Option (z/OS Shell)
- IPL – Initial Program Load – Booting the mainframe
- Sysprog – System Programs, Operators – Console Operators
- MVS, OS390 – Old names for Z/OS



https://rainmaker.fm/wp-content/uploads/2015/06/themainframe2-350x350.png

Talking Mainframe – Files/Folders

- Called Datasets
- Starts with High Level Qualifier (HLQ)

  For example : "**NULLCHD**" in "**NULLCHD**.TEST.FILE"
- Two types:
  - Sequential Datasets

    Use . ("DOT") naming convention

    Example : **NULLCHD**.TEST.FILE , where NULLCHD is HLQ, TEST is like a folder and FILE is the file.
  - Partitioned Datasets

    Also called Libraries, Libs

    Example : NULLCHD.TEST(FILE), where NULLCHD is HLQ, TEST is the Library and FILE is the member of library
- Files are called "members of a dataset" in case of PDS

Connecting to z/OS system

- TN3270 protocol
- Basically Telnet on weed
- Uses EBCDIC (Not ASCII)
- Clear-text
- TN3270 over SSL is also used (port 992)
- Emulators:
  - X3270
  - W3270 (Windows)
  - C3270
- VTAM : The first screen you see when you connect over TN3270

https://upload.wikimedia.org/wikipedia/commons/a/a8/IBM-3279.jpg

Time Sharing Option (TSO)

- Command prompt for Z/OS

```
READY
_
```

- Not so user friendly
- Accepts commands like:
  - ping
  - netstat home
  - Listuser (LU)

Time Sharing Option (TSO)

```
 READY
LU
 USER=Z53859  NAME=UNKNOWN  OWNER=SYS1      CREATED=19.334
  DEFAULT-GROUP=STUDENT4 PASSDATE=20.002 PASS-INTERVAL=180 PHRASEDATE=N/A
  ATTRIBUTES=NONE
  REVOKE DATE=NONE   RESUME DATE=NONE
  LAST-ACCESS=20.018/03:12:44
  CLASS AUTHORIZATIONS=NONE
  NO-INSTALLATION-DATA
  NO-MODEL-NAME
  LOGON ALLOWED   (DAYS)          (TIME)
  ---------------------------------------------
  ANYDAY                          ANYTIME
   GROUP=STUDENT4  AUTH=USE      CONNECT-OWNER=SYS1      CONNECT-DATE=19.334
     CONNECTS=    02  UACC=NONE     LAST-CONNECT=20.018/03:12:44
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
 SECURITY-LABEL=NONE SPECIFIED
 READY
ping google.com
 Unknown host 'GOOGLE.COM'
 READY
netstat home
 MVS TCP/IP NETSTAT CS V2R3       TCPIP Name: TCPIP           09:13:28
 Home address list:
 LinkName:    OSDL
   Address:   192.86.32.91
     Flags:   Primary
 LinkName:    LOOPBACK
   Address:   127.0.0.1
     Flags:
 IntfName:    LOOPBACK6
   Address:   ::1
     Type:    Loopback
     Flags:
 READY
```

Interactive System Productivity Facility (ISPF)

- GUI for Z/OS
- User friendly

```
   Menu   Utilities   Compilers   Options   Status   Help
 ------------------------------------------------------------------------
                              ISPF Primary Option Menu
 Option ===> _                                                          
                                                          More:      +
 0   Settings        Terminal and user parameters
 1   View            Display source data or listings
 2   Edit            Create or change source data
 3   Utilities       Perform utility functions
 4   Foreground      Interactive language processing
 5   Batch           Submit job for language processing
 6   Command         Enter TSO or Workstation commands
 7   Dialog Test     Perform dialog testing
 8   LM Facility     Library administrator functions
 9   IBM Products    IBM program development products
 10  SCLM            SW Configuration Library Manager
 11  Workplace       ISPF Object/Action Workplace

                     ------ Other Install Products ------
 FA  IDI             Fault Analyzer 13.1.0
  D  Debug Tool   Debug Tool Utility V14.1
 SD  SDSF            System Display and Search Facility
 IP  IPCS            Inter Problem Control Facility
 IS  ISMF            Inter Storage Management Facility
 SM  SMP/E           SMP/E and CBIPO Dialogs
 HC  HCD             HW Configuration Definition Dialog
  R  RACF            Resource Access Control Facility
  S  DFSORT          Data Facility Sort
 OE  OEDIT           OpenEdition MVS Edit files
 OB  OBROWSE         OpenEdition MVS Browse files
 OS  OSHELL          OpenEdition MVS ISPF Shell
 BR  READ            BookManager READ/MVS
 BB  BUILD           BookManager BUILD/MVS
 BI  READ INDEX      BookManager Index Utility
 DA  DXT ADMIN       Invoke DXT Administrative Dialogs
 DE  DXT END USER    Invoke DXT End User Dialogs
 DU  MVS/DITTO       MVS/DITTO Utility
 IN  INSPECT         INSPECT for C/370 and PL/I
 D2  DB2I            Perform DB2 Interactive functions
 PM  DB2PM           DATABASE 2 Performance Monitor
 MQ  MQ              MQ 9.0.1 operations and control panels
  F1=Help       F2=Split      F3=Exit       F7=Backward   F8=F
 F10=Actions   F12=Cancel
```

Unix on Mainframe – USS/OMVS

- Unix System Services (USS)
- Implements TCP/IP stack
- Used in almost all Z/OS systems today
- Webserver, FTP, SSH etc. configured and works from here.
- Supports a lot of standard Unix commands
- Comes with Z/OS specific UNIX commands

Unix on Mainframe – USS/OMVS

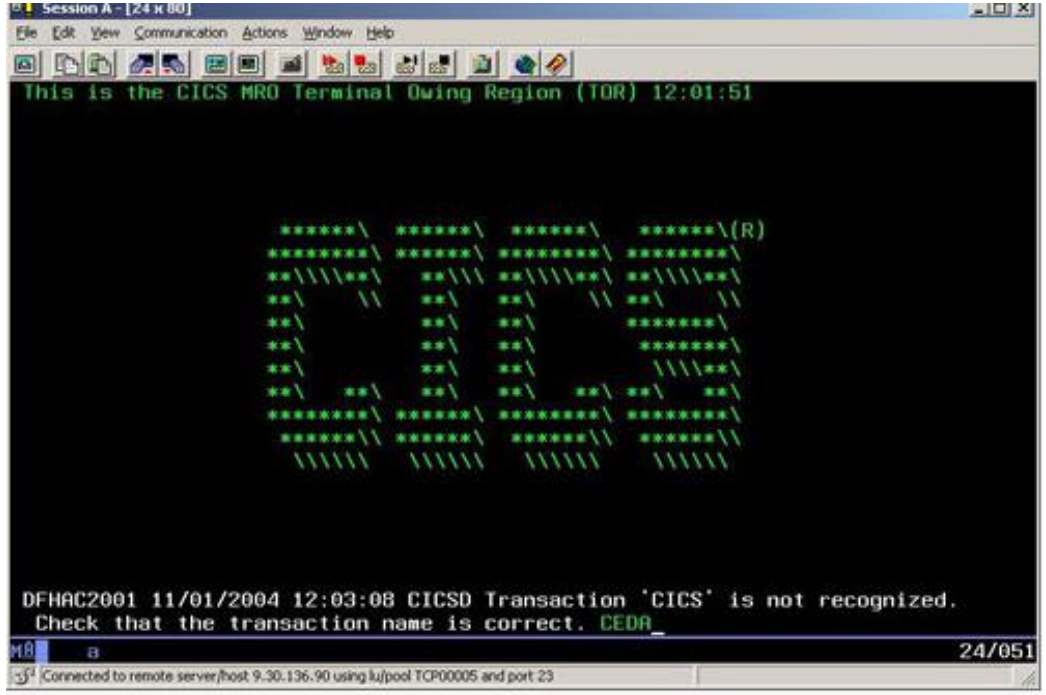
```
IBM
Licensed Material - Property of IBM
5650-ZOS Copyright IBM Corp. 1993, 2017
(C) Copyright Mortice Kern Systems, Inc., 1985, 1996.
(C) Copyright Software Development Group, University of Waterloo, 1989.

U.S. Government Users Restricted Rights -
Use,duplication or disclosure restricted by
GSA ADP Schedule Contract with IBM Corp.

IBM is a registered trademark of the IBM Corp.

id
/z/z53859 > uid=1008245(Z53859) gid=990008(STUDENT4)
/z/z53859 > uname -a
OS/390 S0W1 26.00 04 3906
/z/z53859 >

 ===> _
                                                                  RUNNING
ESC=¢    1=Help      2=SubCmd    3=HlpRetrn  4=Top       5=Bottom    6=TSO
         7=BackScr   8=Scroll    9=NextSess 10=Refresh  11=FwdRetr  12=Retrieve
```

Other interfaces

- FTP
- SSH
- Telnet – Normal telnet
- NJE – Network Job Entries
- Connect:Direct (C:D)
- Message Queues (MQs)
- Etc..

Mainframe Applications

- Applications for Transaction management
- CICS – Customer Information Control System
  - Most common today
- IMS – Information Management System
- Trust on the Client-side.
- Batch processing
- Out of scope for this talk



Ref: https://www.ibm.com/ibm/history/ibm100/images/icp/T891660T84208Q97/us__en_us__ibm100__cics__application_screen__620x350.jpg

Demo 1 – Mainframe (z/OS) Interface

Ref: https://imgc.allpostersimages.com/images/P-473-488-90/65/6599/39P2100Z/posters/mick-stevens-we-met-20-years-ago-when-tom-hacked-into-my-mainframe-cartoon.jpg

Z/OS Security Architecture

- By design – a Strong Security Architecture.
- Strong segregation for each program running on the system
- This segregation prevents programs interfering with other programs as well as the Operating System.
- Unless system is modified to set such privileges for a program (**privileged programs**)
- **Privileged programs** can bypass ALL security controls.

z/OS Security Controls

Two Types:

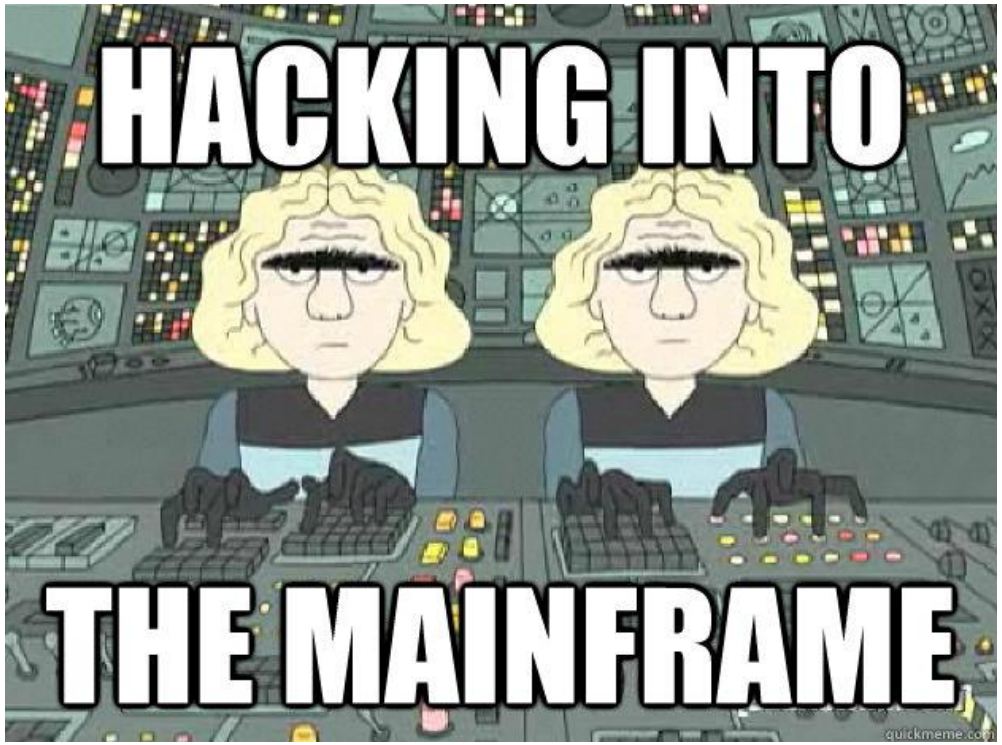
- **Hardware based security controls**
  - Supervisor State – Restricts privileged hardware instructions
  - Protect Keys – Restricts memory a program can update
  - Address Spaces – Restricts memory a program can read
- **Software based security controls:**
  - RACF (IBM)
  - ACF/2 (CA)
  - TopSecret (CA)

Purpose of software-based controls is to check what a user is authorized to access and do.

Resource Access Control Facility (RACF)

- Makes about 75% of the market
- Almost everything is controlled via RACF
- Stores everything in a RACF DB
    - Password hashes as well
- Users and other resources are assigned attributes defining their privilege level:
    - Super User access is called "SPECIAL" (SPECIAL Attribute)
- Default passwords are 6/8 characters (all CAPS, 3 special characters)
- Default User - IBMUSER/SYS1
    - Usually disabled
- Allows: WARNING Mode & SURROGATE Profiles

Hacking/Pentesting Mainframes



Ref: http://www.quickmeme.com/img/9e/9e8b15a7bd7ba7c33486602aaee307be487ac260811100613ee3535ca0aa0bb1.jpg

Hacking/Pentesting Mainframes

Common Scope:

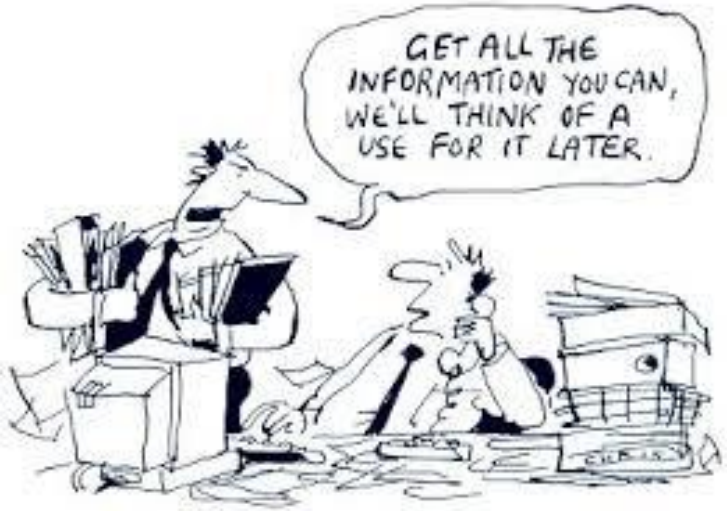
- Z/OS system - which includes complete OS,RACF, TSO etc.
- Mainframe Applications – CICS, IMS etc.

Approach:

Initial recon > Gaining Access > Local Recon > Privilege Escalation

Hacking Mainframes – Initial Recon

- Nmap Scanning
  - Open Ports/Running Services
  - NMAP scripts to enumerate following information (by Phil Young)
    - VTAM (APPLIDs)
    - Logical Units (LUs)
    - TSO User Ids
    - CICS transactions
  - Look for:
    - Telnet 3270 - Port 23/992 (and variants)
    - FTP - Port 21 (and variants)
    - NJE Services
    - MQ and Connect:Direct Services – 1414 & 1363,1364.



Hacking Mainframes – Gaining Access

- Default Accounts - IBMUSER/SYS1
  - most likely disabled
- Bruteforcing TSO user accounts
  - Accounts might get locked after 3 attempts
  - Applies to TSO, FTP, SSH etc.
- Steal credentials
  - MiTM
  - Phishing (SETn3270)
- Using FTP
  - Uploading the JCL and executing it to get reverse shell
  - Manually
  - Metasploit
  - TSh0cker

```
------------------------------- TSO/E LOGON ---------
IKJ56420I Userid NULLUSR not authorized to use TSO

  Enter LOGON parameters below:

 *Userid    ===> NULLUSR

  Password  ===>
```

Hacking Mainframes – Gaining Access

- Using Credentials
  - Most likely provided for Grey box pentest
- CICS Applications
  - This is usually when the CICS applications are in scope.
  - Some sensitive transactions are accessible without authentication.
  - Tools/Scripts:
    - CICSPwn
    - BRIDA
- Other Usual Ways
  - Webservers
  - DB2
  - Other vulnerable network services

Ref: https://nmap.org/movies/matrix/access_granted.jpg

Hacking Mainframes – Local Recon

- Check for your current user's security (RACF) attribute
- If you're already "SPECIAL" or "OPERATOR", you have access to everything.
- Look for following:
  - Basic System information – version info, security software used (RACF/AFC2 etc.) etc.
  - Interesting files with configuration of other services (MQ, C:D Netmap files etc.)
  - SURROGATE Users
  - Users with access to USS etc.
- REXX ENUM Script: https://github.com/mainframed/Enumeration

Hacking Mainframes – Local Recon

- Manual Way (commands/utils)
  - IPLINFO
  - SHOWZOS
  - TASID
- Using SEARCH command
  - List of APF Authorized Libraries
  - List of SVCs (Supervisor Calls)
  - Running JOBs
- Enumeration in USS/OMVS
  - Check for 'a' attribute (APF authorized Libraries)
  - Usual unix enumeration - crontabs, config files, webserver folders, files,

Hacking Mainframes – Privilege Escalation

- RACF
  - Cracking Passwords
  - SURROGATE Profiles
    - submit Job as SURROGATE user (using JCL)
- Unix Privilege Escalation
  - BPX.SUPERUSER?
    - Permissions on su to root without password
  - BPX.FILEATTR.APF
    - Create APF Auth files (+a)
  - SUPERUSER.FILESYS.MOUNT
    - Mount malicious filesystem with SPF/SETUID
  - UID = 0 is NOT gaining SPECIAL on z/OS

Hacking Mainframes – Privilege Escalation

- APF Auth libraries:
  - If you have UPDATE access on any of APF libraries, you can do whatever you want.
- SVC (Supervisor Calls)
- Tools/Scripts -
  - ELV.APF (By Ayoub) - https://github.com/ayoul3/Privesc
  - Metasploit (apf_privesc_jcl)
    - Mount malicious filesystem with SPF/SETUID

Demo 2 – From nothing to SPECIAL

Challenges

- Challenges:
  - A common belief - “Our Mainframe is Secure because it’s not accessible from over the internet”
  - Every organization will have their own mainframe configuration (and it varies a lot)
  - Highly protected systems in an organization.
    - Making them hard to get information about.
    - Mainframe teams are usually the only people in an organization who knows about these system.
  - Everything is documented, but too many documents

On the other hand:

- Modern mainframers are super helpful and are security aware.
- The Security community has started to gain interest in mainframes recently

Where to go from here?

- Start exploring z/OS mainframes:
  - Master the Mainframe contest by IBM (https://masterthemainframe.com/)
  - Your company's mainframes are the easiest and hardest to explore.
  - Setup local lab with Hercules & Turnkey
  - zD&T – if you can afford.
- Develop more resources and tools to aid in mainframe security research.
- Connect:Direct is unexplored as of now.

Overwhelmed?

Awesome Mainframe Hacking Resources :
https://github.com/samanL33T/Awesome-Mainframe-Hacking

Twitter: @samanl33t

Email: saman.j.l33t@gmail.com

Ref: http://www.quickmeme.com/img/31/3182781d07db4c2024894ca56ac3dfaeaed9d7c657139cc3499c662644f18c0e.jpg