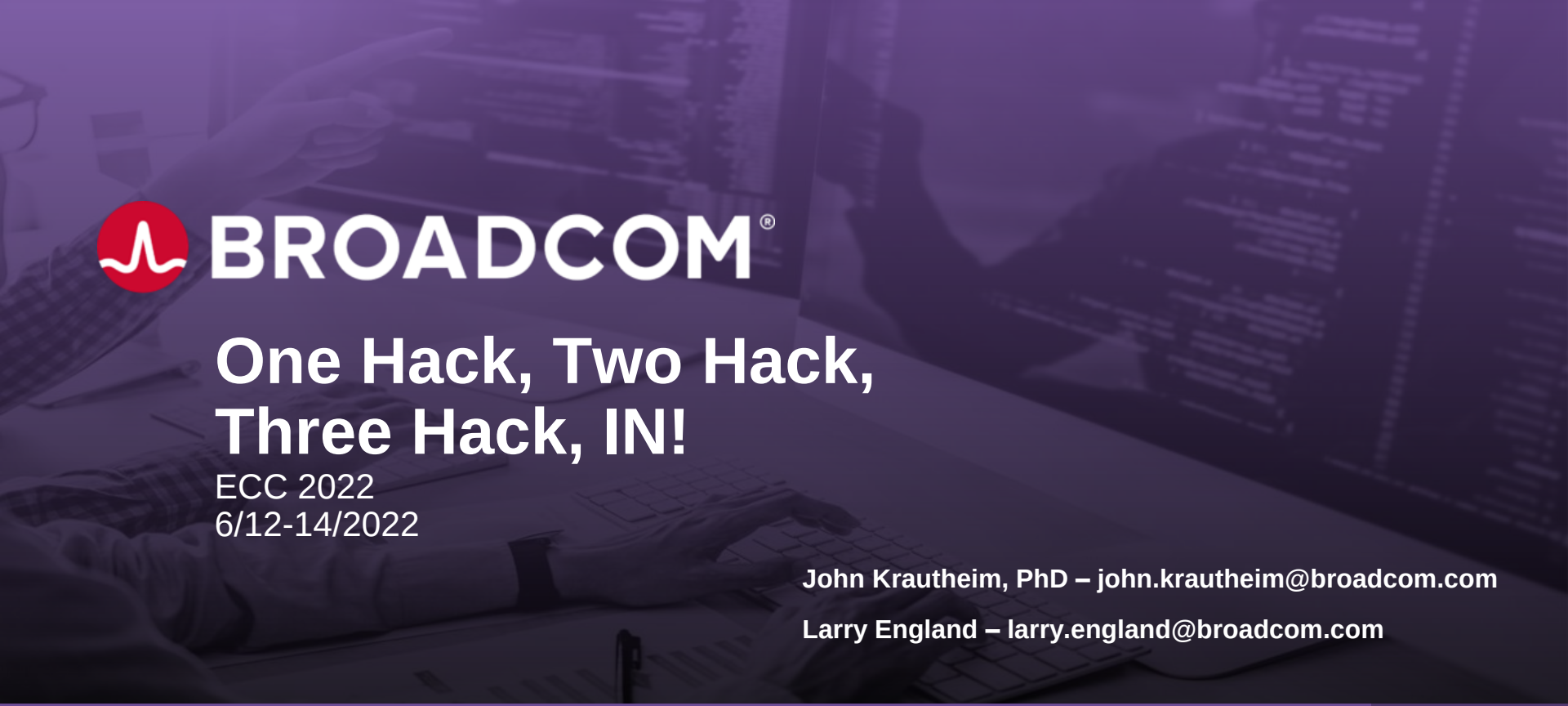


One Hack, Two Hack, Three Hack, IN!

ECC 2022
6/12-14/2022

John Krautheim, PhD – john.krautheim@broadcom.com

Larry England – larry.england@broadcom.com

Disclaimer

Don’t believe everything you read.

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Who are the Presenters? Who are these guys anyway?

John Krautheim, PhD, CISSP-ISSEP

Broadcom Software Engineer

20 years experience in Computer Security

Enjoys cycling and camping

Is an audiophile on the cheap

Larry England

Broadcom Software Engineer with experience across many technologies

Enjoys hiking, trail running (ultras), biking, xcountry skiing, photography, music

Very amatuer piano player

Participant in the witness protection program

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

A lil’ story - an anatomy of a breach!

Step 1) Harvested userids via ‘leaked’ information via enumeration

Step 2) Access to the mainframe via ftp, ssh, tn3270 given a single credential

Step 3) Still restricted access, looked thru log files (firewall, ftp, webserver, etc)

Step 4) Thousands of attempts over time using discovered ids with elevated privileges finally found the way into z/OS with elevated privileges

- able now to upload attack tools
- non-standard networking to offload information - camouflaged network traffic looked ‘normal’
- moved data to multiple relaying servers - to isolate the ultimate endpoint and lower the visibility
- Installed a number of ‘backdoors’ into the system

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

A lil’ story - an anatomy of a breach!

Step 1) Harvested userids via ‘leaked’ information via enumeration

Step 2) Access to the mainframe via ftp, ssh, tn3270 given a single credential

Step 3) Still restricted access, loc ebserver, etc)

Step 4) Thousands of attempts o h elevated privileges finally found the way in

- able now to upload attack t
- non-standard networking to ed network traffic looked ‘normal’
- moved data to multiple rela ate endpoint and lower the visibility
- Installed a number of ‘back

Info from “**Report on the IT security incident of 2012**” - computer forensic investigation of Logica breach.

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Agenda - Topics

Why worry about the Mainframe

Pentesting on Mainframe

Why it’s different / Why it’s similar

Pentesting System vs Pentesting Product

Unique things about mainframe

Skills required

Tools for mainframe penetration testing

Demo - if the demo-gods are willing

What should you do?

Questions and answers

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

What is “Penetration Testing”?

What is it? Find the most likely places where an attacker/hacker can gain unauthorized control or unauthorized access to system and/or data – then take proactive steps to reduce/remove the vulnerability.

It may provide the necessary proof of compliance in some situations (PCI-DSS, HIPAA, SOX, GDPR, etc)

Characteristics of pen testing:

- Model the activities of real-world attackers
- Find vulnerabilities in target systems likely to be found by real-world attackers
- Exploit found vulnerabilities under controlled circumstances
- Determine and document risk and potential business impact in a safe fashion according to agreed upon rules of engagement
- Help an organization prioritize resources to improve its security stance

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Isn’t vulnerability scanning enough?

A **Vulnerability Scan** looks for known vulnerabilities in your system or product - sometimes at the source code or at the binaries looking for well-known patterns

Penetration Testing is intended to exploit weaknesses in the application architecture, system configuration, network configuration acting as a malicious attacker.

These two activities compliment each other and *both* should be employed! Some industries mandate both activities to be carried out by an enterprise.

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

How does one measure a lock's effectiveness?

Time to breach - "An expert can crack a 3-digit padlock in less that 40 minutes while the same expert would need at least 4 hours to crack a 4-digit padlock."

Please note: Hackers don't play by the rules - "An intruder doesn't care if s/he breaks a window to enter a house."

The underlying assumption is all locks can be broken. It's a matter of time!

Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Pen testing a system vs Pen testing a product

Pen testing a system

- Freedom to move laterally from one place to another
- Ability to leverage multiple vulnerabilities across multiple software stacks (Stuxnet leveraged 4 zero-day vulnerabilities to gain access)

Pen Testing a product

- Focus on exposed interfaces, user input, product configuration
- Authentication
- Data stores and access

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

What’s the difference between Pen Testing a system vs a product?

Scope - System Test

- gaining system access (general user) – considered “easy”
- accumulate system information over time
- varies significantly from one system to another
- Able to ‘move laterally’ across multiple products taking advantage of small vulnerabilities or ‘leaked’ information

Scope - Product Pen test

- focus on APIs, avenues of access, discrete level of access (user vs admin, for ex), elevated privileges
- Need to focus on configuration/install options
- Baked in security vs adding security icing

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Is the mainframe impenetrable?

- **Yes!** If unplugged
- See this BlackHat Conference Video

- Has the mainframe been hacked? Yes! See this – and more!
  - SHARE blog series - Mainframe Hacker
  - PCWorld article - Pirate Bay cofounder caught
  - Broadcom Blog Post - 3 Mainframe Myths

- Is there a **false sense of security** based upon its reputation? z/OS is the most "secure" platform … or is it the most "Securable" platform?
  - … but there are rules/guidelines to ensure it retains its high level of security

- Complacency - Are **enterprises keeping pace with security** on the mainframe?
  - https://www.darkreading.com/vulnerabilities-threats/the-mainframe-is-seeing-a-resurgence-is-security-keeping-pace-
  - (internal link) Share presentation - Anatomy of a Hack
  - Is Mainframe Security Keeping Pace?

Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

What's different about z/OS? What's the same as the 'others'?

z/OS is a unique operating system integrated with the underlying hardware and a unique character encoding (EBCDIC). While different, it has a number of characteristics and tools that are found on 'other' systems such as Linux and Windows.

Different:

Operating Systems

Network Interfaces - OSA

Specialized interfaces - 3270

Storage - datasets

Centralized

Logical partitioning

Stack management

Programming Languages

- Cobol, PL/I, HLASM

Same:

Common Libraries

Common Protocols

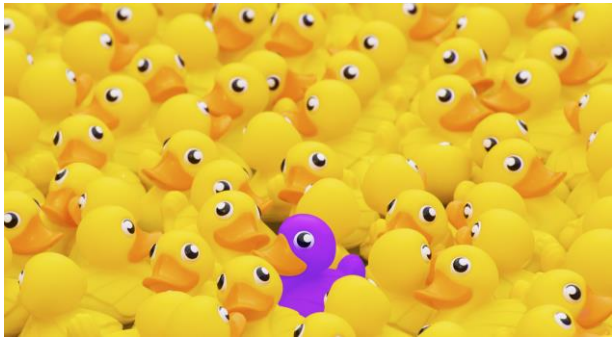
- FTP, Telnet, SSH

High Level Programming languages

- Java, Kotlin, C/C++

Containers and Microservices

Distributed applications



Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

What technologies/skills are unique to z/OS? The same?

- What's different?
  - Access - multiple, unique roads into the mainframe (like 3270, SNA/networking, network job entry)
  - Character encoding - EBCDIC vs ASCII/UTF8
  - Scripting languages (Rexx, Clists, JCL)
  - Command and command structures (TSO, JES, JES, VTAM, CICS, IMS, DB2, IDMS, …)
  - Transaction processing (CICS, IMS, IDMS)
  - Batch processing (JCL)
  - File systems and access methods (PDS, PDS/e, VSAM, etc)
  - ESMs (RACF, TSS, ACF2) - hardware enforced memory access, APF authorized datasets, prob/sup state
    - Supervisor state / system protection key (0-7)
    - Problem program state / user key (8-15)
  - SW-managed, stack oriented architecture vs Hardware managed stack
  - Pervasive encryption
- What's the same?
  - access (ftp, ssh, TCPIP, etc)
  - commands (Unix/Posix)
  - Transaction processing (Websphere, Tomcat)
  - scripting (Ansible, shell scripting)
  - file system (USS filesystem - recursive directory structure)

Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Are there tools for hackers (and pen testers) for z/OS?

In a word – YES! Many! We'll have a look at a few.

The Evil Mainframe - Phil Young, Chad Rikansrud

Attribution goes to them!

Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

What are the Tools for hackers on z/OS?

nmap - Network Mapper

ncat - network utility which reads/writes data across networks from the command line

SET'n'3270 - Man in the Middle tn3270 proxy

CICS stuff!

Note: CICS security not turned on by default - CEMT, CEDA, CECI

CICSpwn - tool to pentest CICS Transaction servers on z/OS

cics-info, cics-enum - CICS transactions ID

SOCKET command

USS Extended attribute (+a) on executable makes it seem to be loaded from APF auth library

tn3270-screen - Reading TN3270 screens

vtam-enum - Appl ID enumerations

enum - enumeration os z/OS artifacts using REXX

John the Ripper - password cracker! supports RACF database! (8 char limit, no special chars!!)

metasploit - a library of routines (exploits!)

zACS - IBM's z/OS Authorized Code Scanner

Kali Linux - Platform for advanced penetration testing and security auditing

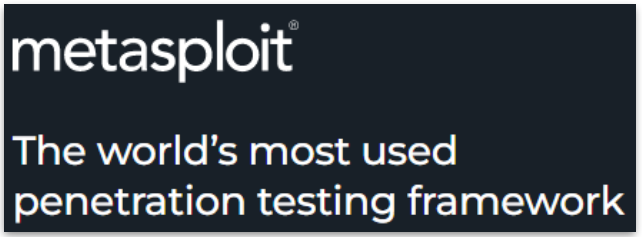
Wireshark - protocol analyzer - let's you see what's happening on your network!

Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

Automation - Metasploit - does it support z/OS?

- **Metasploit**
  - public open source framework for known exploits used to test for known vulnerabilities
  - Chad Rikensrud (of Evil Mainframe fame) added support for zArch in 2016
  - Can be authenticated - using real credentials
  - Non-authenticated - binary exploits (buffer overflow)
  - Other
    - scanning, brute forcing, emulation (ftp, http, smb)
  - See this and that

- apf_privesc_jcl
  - Must have UPDATE access to an APF lib
  - Uses FTP
- Adds **SYSTEM SPECIAL** and **BPX.SUPERUSER** to user profile
- This privesc only works with z/OS systems using RACF, no other ESM is supported
- See also other metasploit mainframe scripts



Copyright © 2022 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries.

So what did we touch upon?

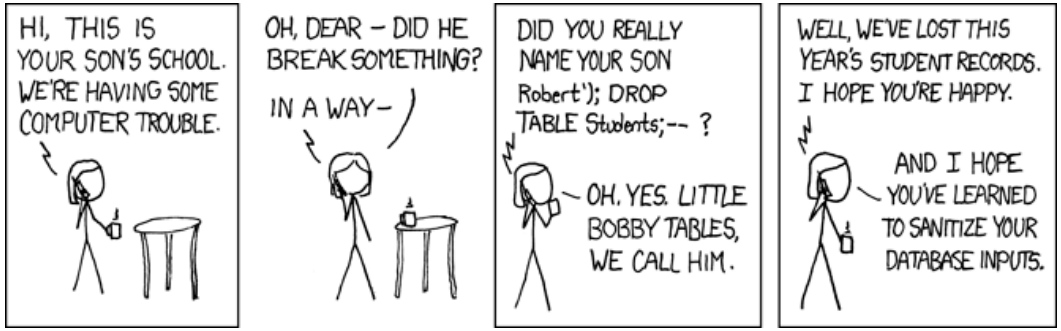
We looked at

- what is pen testing and various aspects
- Is the mainframe secure or securable?
- Where can I find some info about tools & techniques applicable to z/OS?

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

OK! So what now? What do I do?

- The mainframe can be hacked. You must be constantly **diligent** to ensure that it is secure.
- **Trust but verify!** Be afraid. Be very afraid.
- Look at tools (like Security Insights) to help identify risks and potential threats
- **Constantly evaluate the system** - keep up-to-date, enforce the policies in place for user management (constantly prune!)
- Evaluate the “Evil Mainframe” Course? (editorial note: very very very interesting!)
- **Keep up to date with security vulnerabilities** and exploits
- <what else can you do to sleep better at night?/>



Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

BROADCOM

Questions?

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

BROADCOM

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

BROADCOM

Backup Slides

Copyright © 2022 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Platform differences - sweeping generalities

Distributed platforms (x86, Linux, Unix)	Mainframe – z/OS
Virtualization, ephemeral instances are rapid to produce and dispose	Virtualized, ephemeral mainframes are not in widespread use
Platform standardization – each instance of a server is identical.	Each instance of z/OS is unique (snowflake!)
One set of servers is used for a given application	z/OS hosts multiple applications simultaneously (on-line, batch, etc)
Data on a given server is dedicated for a specific application	Data on a given server supports multiple applications
Freedom to experiment – given the ability to have virtual, ephemeral instances	z/OS is tightly controlled and changes are highly scrutinized
Applications are typically built with more modern architectures creating sets of services	Applications are monolithic (big balls of mud) and evolving to sets of services
Multiple servers needed for development, test and production	Dev, test, production are isolated via LPARs
Highly interconnected with a network of servers	Highly interconnected with a network of servers
Scaling is typically horizontally	Scaling is both vertical and horizontal

Copy