Chad Rikansrud
Mark Wilson

BMC Mainframe Services

1

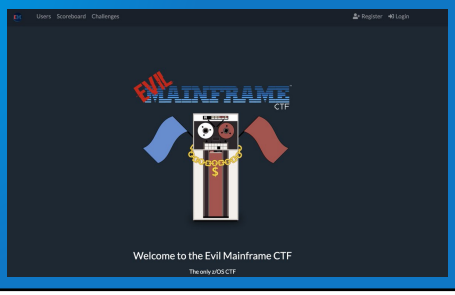
Introductions

- **Chad Rikansrud**
  - Director N.A. Mainframe Services
  - Mainframer for about 15 years
  - Prior led teams for large financial services org
  - Hacker
  - Speaker (DEF CON, blackhat, RSA, SHARE, etc.)
  - Technical background mainly UINX, network, reverse engineering
- **Mark Wilson**
  - Senior Director Mainframe Services
  - Been a Mainframe since May 1980
  - Operator > Senior Operator > Shift Leader > Ops Analyst > Systems Programmer > Consultant
  - Mainframe Security Specialist; especially Penetration Testing and Security Assessments
  - Passion for fast things (Motorcycles & Cars)
  - Real Football!
  - Scuba Diving

2

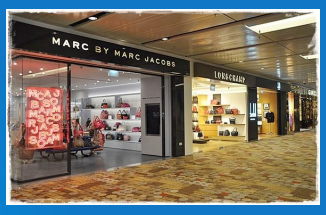
What is EM?

- **Why is it called "Evil Mainframe"?**
- **The Class**
  - This first of its kind mainframe hacking class teaches you the techniques you need to conduct mainframe penetration tests. Using a live z/OS mainframe you'll get the ability to put the classroom teachings in to practice
  - Three main sections
    - Techniques
    - Hands On
    - CTF



3

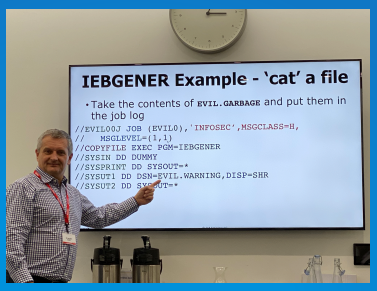
Where have we been?

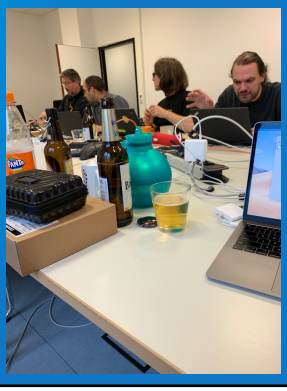


- **Places Visited**
  - London, Copenhagen, Singapore, Amsterdam, Frankfurt, Sydney & most of the USA!
- **Comments from our wives**
  - You two spend more time with each other than you do us!
  - There was a price to be paid!

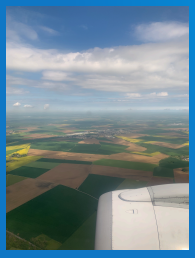
4

The Fun Part





No I Said the Fun Part!!



What did we learn

- Next generation of MF security folks might not be traditional Mainframers!
- Why?
- Role of the traditional Mainframer (training, knowledge xfer and yes, some of you will do this role too (we had some Mainframers in our classes that were sharp! – eg. Copenhagen))

Questions, Questions, Questions!!

- Asking questions no one asks in SHARE & GSE, etc
- And ultimately led to this one question

The Question

Can USS/OMVS Superuser be used as the basis for z/OS system takeover?

Discussion of the question

- Could USS/OMVS Superuser be used to compromise a mainframe z/OS system?
- Our collective view at the times was NO!
- But it can do APF right?
  - No; Superuser does not grant the authority to switch from problem State to Supervisor State
- What can it do?
  - Well it can Mount and Unmount Filesystems

So the gloves were off and off we went to see what we could do

What did we learn?

- Editing z/OS aggregate directly – Worked!
- Still had a problem in that we still needed to mount it
- What about UNIXPRIV superuser.filesys.mount / usermount?
- Hold on a minute.. Do we have something here?
- We now have Carry-in exploits!

DEMO TIME

13

Questions?

14


bmc
Customer
Experience
CONFIDENTIAL INTERNAL ONLY © Copyright 2020 BMC Software, Inc.
15