Course Name
Evil Mainframe Penetration Testing

Course Description

Have you ever been mid pentest with mainframe credentials and thought ‘now what?’ Or were you ever asked to do a mainframe pentest and didn’t even know where to start? Maybe you’re a sysprog and think your systems are impenetrable. No matter your background this course is for you!

This course provides training on mainframe penetration testing using the most recent and up to date attack vectors. Walking through techniques for gaining system access, performing end-to-end penetration tests, and teaching you to ‘own’ the mainframe.

After a quick overview of how z/OS works and how to translate from Windows/Linux to “z/OS” the instructors will lead students through multiple real world scenarios and labs against a real live target mainframe brought on site for the training. The areas explored in this course include VTAM, CICS, TSO, Unix and Web. Students will be given access to this mainframe environment for the duration of the course where they will learn to navigate the operating system, learn some of the misconfiguration targets and privilege escalation techniques. They will get introduced to the open source tools and libraries available for all the steps of a penetration test including Nmap, python, kali, and metasploit as well as being able to write their own tools on the mainframe using REXX, JCL, C and CLISTs.

The majority of the course will be spent performing instructor led hands on mainframe testing with tools provided by the instructors. Goals for each segment will be laid out with appropriate time afforded to students to allow them the ability to gain a deep understanding of how a mainframe pentest could and should be performed. Exercises will be based on real world attack scenarios.

While this class is outlined as a beginner class to mainframe hacking the attendee should have knowledge of IT security, penetration testing and very basic Python.

Course Outline

Day One: Mainframe Basics, User Interaction, Scripting, Network Protocols & Security

- About us and the course
- Mainframes: A *brief* History
- z/OS Basics
    - TSO
    - Unix
    - JCL
    - REXX
- **LAB**: Creating a folder on a mainframe. Copy/Pasting to that folder. Writing JCL, submitting the job and viewing the output.
- Patching
- System Startup Understanding the boot process
- Storage (Memory)
- Security: How security it is handled on mainframes and what to look for
- **LAB**: RACF commands, accessing dataset in warning mode. Submitting JCL with ‘SURROGAT’ authority
- Writing *real* JCL
    - IKJEFT01
    - BPXBATCH
    - IXRJCL
- Writing REXX
    - Simple
- Writing CLISTs

- Writing and compiling C with JCL
- **LAB**: Write REXX script to create a reverse shell. Compile C program to create reverse shell.
- Writing HLASM
- CICS: Understanding how CICS works and used in the enterprise
- **LAB:** Connecting to CICS, accessing a transaction and gathering information
- TN3270: How the major mainframe protocol works and how to use it to our advantage
- **LAB:** Using TN3270 python script to hack poorly coded TN3270 apps

Day Two: Let's Hack a Mainframe

- Reconnaissance
    - OSINT and the Mainframe
    - Using Nmaps *new* tn3270 library
    - Writing your own Nmap scripts to target mainframe applications
    - **LAB**: Using Nmap enumerate LU names, VTAM Application IDs, CICS transactions.
- System Interaction/Shells
    - Breaking in through TSO, CICS, Web
    - Using Python for infil/exfil
    - Using x3270 & s3270 scripting
    - **LAB**: Using Python and Tn3270 to automate
    - CICS Security Bypass
    - Using CICS to get a shell
    - **LAB**: CICSPwn reverse shell
    - FTP and JCL
    - **LAB**: Using FTP and JCL to run a job & get a shell.
    - Automating it all with metasploit

- System Enumeration
    - Gathering system information
    - Living off the land (showzos/iplinfo/tasid)
    - SuperC
    - Memory storage locations
    - Enum (rexx script)
    - SETRCVT (rexx script)
    - **LAB**: Identify all APF authorized libraries
- Offline Cracking
    - How passwords are stored
    - Where they are stored
    - Understanding the hashing algorithm
    - Cracking the passwords with John/Hashcat
- Privilege Escalation
    - JCL
    - Warnmode
    - BPX.Superuser
    - SURROGAT authority
    - Search/SuperC
    - APF Authorized
    - **LAB**: Using ELV.APF (rexx script) to escalate privileges
- Review
    - Cover any questions/remaining items
- CTF
    - The last hour+ is a mainframe CTF which uses everything learned in the class to ‘own’ a mainframe.
    - Students attack the in-house mainframe to gain points. First team to get the highest wins!

Requirements

Students must bring their own laptop to class. This device should be capable of running VMware player/Fusion or Virtualbox. A virtual machine image will be provided prior to class.

If students wish to build their own here's the required software:

- Linux (Ubuntu, CentOS, Arch)
- Nmap – current SVN version
- Metasploit – Current nightly
- X3270 Compiled from source
- BIRP - with x3270 patches installed
- SSH Client
- Python 2.7+
- Git client (to install tools discussed in the class, the virtual image has these tools pre-installed)

Trainer Names:

Philip "Soldier of FORTRAN" Young

Chad "Big Endian Smalls" Rikansrud

Trainer Bios

Philip Young

Philip Young, aka Soldier of FORTRAN, is a leading expert in all things mainframe hacking. Having spoken and taught at conferences around the world, including DEFCON, RSA, BlackHat and keynoting at both SHARE and GSE Europe, he has established himself as the thought leader in mainframe penetration testing. Since 2013 Philip has released tools to aid in the testing of mainframe security and contributed to

multiple opensource projects including Nmap, allowing those with little mainframe capabilities the chance to test their mainframes. In addition to speaking, he has built mainframe security programs for multiple Fortune 100 organizations starting from the ground up to creating a repeatable testing program using both vendor and public toolsets. His hope is that through raising awareness about mainframe security more organizations will take their risk profile seriously.

Chad Rikansrud

Chad Rikansrud, aka Big Endian Smalls, is the Director of North American Operations for RSM Partners (www.rsmpartners.com) - a world leader in IBM mainframe security consulting services. Chad is a nationally recognized security industry speaker, with appearances at: DEF CON, RSA2017, SHARE, and other regional conferences. Most of Chad's 20-year career has been in technology leadership for the financial services industry where he has held various senior leadership positions, including worldwide datacenter operations, infrastructure and recovery responsibility, as well as enterprise-wide system z storage.