Evil Mainframe Hacking Mini

Course Description

Come live your cyberpunk dreams! Mainframes are the workhorse behind almost every fortune 500. It's probably time you learned how to hack one. This workshop provides a one of a kind experience, allowing you to get hands on mainframe hacking experience with multiple labs. This workshop lays the groundwork for mainframe penetration testing. Walkinging you through techniques for gaining system access, performing end-to-end penetration tests, and teaching you to 'own' the mainframe.

After a brief 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 workshop. The areas explored include VTAM, CICS, TSO, and Unix. Students will be given access to a mainframe environment for the duration of the course where they will learn to navigate the operating system, learn some easy wins, 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, and JCL.

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

Part 1: Mainframe Basics

- z/OS Basics
  - TSO
  - Unix
  - JCL
  - REXX
  - RACF
- **LAB**: Creating a folder on a mainframe. Copy/Pasting to that folder. Writing JCL, submitting the job and viewing the output.
- Security Control on the mainframe
  - 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

- Using/Writting *real* JCL
  - IKJEFT01
  - BPXBATCH
- Using/Writing REXX
- Writing and compiling C with JCL
- **LAB**: Reverse Shells

Part 2: 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**: Information Gathering...
- System Interaction/Shells
  - Breaking in through TSO, CICS, Web
  - Using x3270 & s3270 scripting
  - 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
  - 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

```
//*--------------------------------------
//OUT1 OUTPUT DEST=EVILNODE,
//            MAILTO=henri@evilmainframe.com
//*--------------------------------------
```

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
- X3270
- SSH Client
- Python 2.7+
- Git client (to install tools discussed in the class, the virtual image has these tools pre-installed)