Red Team Village Workshop Abstract

Title: Hunting & Exploiting DLL Sideloads

Summary: This workshop will go through the process of manually identifying applications that can be vulnerable to DLL Sideloading and exploiting them. Attendees will learn how to use Promon to find applications that can be vulnerable to DLL sideloading, identify the correct DLL functions to proxy using CFF Explorer, and write a basic DLL to run shellcode.

Bios:

Matthew Nickerson CRTO, OSCP – Offensive Security Consultant @ Layer 8 Security

Nick Swink OSCP, PNPT – Offensive Security Consultant @ Layer 8 Security