STUDENT PREPARATIONS
Penetration Testing in Hostile Environments: Client and Tester Security

Dear Student,

Thank you for signing up for our *Penetration Testing in Hostile Environments* workshop! This document presents information that will be useful to you in preparation for our DEF CON 26 workshop.

A student who wishes only to partake in the lecture and discussion portions of the workshop and observe demonstrations is welcome to attend and will gather some value from the session. For practitioners that engage hands-on in offense-oriented operations and want to gain the most information and experience possible from the workshop, I encourage you to be ready to follow along with exercises with your own computer.

If you'd like to be placed on an email list for the class to receive additional materials ahead of class, email me at wesley.mcgrew@hornecyber.com . All materials will be provided on-site on USB as well. Feel free to email me with any questions you might have as well!

Laptop

To participate in hands-on exercises, you should bring a laptop meeting the following specifications:

- RAM
  - For Linux host operating systems, 8GB of RAM should be sufficient
  - For Windows host operating systems, 16GB of RAM is recommended, as a portion of your RAM will be reserved by Docker in a Hyper-V VM (when using the Windows Docker installer), or by a Linux VM you manage yourself for Docker.
- Storage
  - After everything is installed and configured, having 30GB of drive space free will ensure that you have enough breathing room to work during the workshop. Likely we will need much less
- Docker
  - A working Docker installation is required, to the point of being able to successfully execute "docker run hello-world" and see some reassuring output.
  - We'll have a little "Intro to Docker" time for those of you unfamiliar with it, but
- The ability to sniff networks in monitor mode is useful for one part of an exercise, though if you don't have the hardware for it on-hand, it's not worth the purchase for that moment alone.
- Administrative Privileges
- A lack of sensitive data – I would encourage you not to bring your firm's darkest secrets with you on any sort of work travel.

Materials

All slides and materials necessary to complete the exercises (such as Docker containers) will be provided to you on a USB drive. The whitepaper that this workshop revolves around is included in this zip file as well. You may want to review the material before the conference.

Prerequisite Knowledge

To get the most out of this class, students should have the ability to read/follow code in many programming languages (C/C++, Python, PHP, etc.). Students should also be familiar with navigation and use of the Linux command line. Experience with penetration testing will be useful, but those new to penetration testing should not be discouraged. The entire point is to pick up good operational security habits.

Your Instructors

Wesley McGrew

I'll be your point of contact for any questions or discussion before or after the workshop. Feel free to contact me for questions, or simply to introduce yourself, at any time via email or twitter:

- wesley.mcgrew@hornecyber.com
- @McGrewSecurity

I will be presenting talks on penetration testing multi-container applications at Black Hat USA and DEF CON 26, if you'd like to check them out. The DEF CON talk will be earlier in the day on the day of the workshop:

- https://www.blackhat.com/us-18/briefings/schedule/index.html#an-attacker-looks-at-docker-approaching-multi-container-applications-9975
- https://www.defcon.org/html/defcon-26/dc-26-speakers.html#McGrew

My Bio:

Wesley McGrew oversees and participates in penetration testing in his role as Director of Cyber Operations for HORNE Cyber Solutions. He has presented on topics of penetration testing, vulnerabilities, and malware analysis at DEF CON and Black Hat USA. He teaches a self-designed course on reverse engineering to students at Mississippi State University, using real-world, high-profile malware samples. Wesley graduated from Mississippi State University's Department of Computer Science and Engineering and previously worked at the Distributed Analytics and Security Institute. He holds a Ph.D. in computer science for his research in vulnerability analysis of SCADA HMI systems.

Kendall Blaylock

Kendall serves as Director of Cyber Intelligence for HORNE Cyber, where his specialty is digital forensics and incident response. Prior to his role at HORNE Cyber, Kendall co-founded the National Forensics Training Center where he served as lead instructor providing training to law enforcement and U.S. military veterans in a wide range of digital forensic skills.