**Description**

PowerShell has surpassed the administrative use that it was originally developed for. It now additionally serves as a capability that enables threat hunters and incident responders to illuminate malicious activity and respond to such threats. It also enables pentesters and malicious actors to gain and maintain access as well as proliferate throughout a network without bringing any additional toolkits. In most cases, the two additional uses often are not detected or known by the admins or the opposite side. We will dive into and demo a number of methods in which both sides are using or could use PowerShell to achieve their overall objectives.

***The Evolution of PowerShell: Red and Blue Team Tactics Workshop* is the best way to get hands-on experience and exposure to real-world uses.** You will learn:

* Core aspects of the language to get started with; one would call it a primer
* Defensive hunting techniques for use locally or across an Enterprise
* Triage forensics capabilities to highlight potential abuse
* Detection methods of adversarial lifecycle stages of intrusion
* Reconnaissance tactics for information gathering
* Exfiltration techniques and additional toolset uploading
* Persistence mechanisms for assured execution
* Tips and tricks including other uses for the language and shortfalls

**PowerShell is an extremely powerful language that has proven useful for all aspects of blue and red team activities. Walking away, you will be better postured to identify these tactics or use them for specific purposes without adding anything additional to the network.**

**Workshop Format**

**This workshop is delivered live in Huntsville from 9:00 AM to 4:00 PM**. You will participate in demonstrations and hands-on activities that help you become more comfortable with PowerShell and various use-cases.

The workshop is being held the day before [BSides](http://www.securitybsides.com/w/page/135708132/BSides%20Greenville%202020" \t "_blank) Huntsville. If you're coming to town for the conference, consider coming a day early for the workshop.

**About the Instructor**

Fernando Tomlinson has 18 years in cybersecurity and system administration within the Department of Defense. He currently serves as the Technical Director of a Cyber Operations Center. Previously he has led multi-level Digital Forensics and Incident Response (DFIR) and threat hunting teams. He is also a collegiate cybersecurity Adjunct Professor who enjoys contributing to the community through his blog at https://cyberfibers.com and projects at https://github.com/wiredpulse. He is the developer of PoSh Hunter (https://posh-hunter.com) and co-developer of Under the Wire (https://underthewire.tech), which both are interactive PowerShell educational platforms. Additionally, he is a consultant with Reliable Cyber Solutions (https://rcybersolutions.com), a company focused on cybersecurity training and certification.

**FAQ**

**What do I get?**

* One day of classroom instruction with Fernando Tomlinson
* A collection of PowerShell code for the labs

**I’ve coded in PowerShell; will I still learn anything in the workshop?**

Absolutely! With the versatile and agile the language is, the possible uses are endless. Additionally, many of the lab exercises in the workshop are unique. You will be exposed to content that isn’t available in a book.

**Will I be lost if I haven’t used PowerShell before?**

Not at all! The workshop doesn't assume you’ve used the language before. Additionally, majority of the code that we will be using will be given to you so you are able to follow along.

**What hardware is required for the workshop?**

None! A system will be provided for attendees.

**What do I need to bring to the workshop?**

You should plan to bring:

* A ticket for the event (if supplied)
* An open mind