ISSA DELAWARE VALLEY

Quarterly Meeting
June 1, 2018

8:00 – 8:45	Registration and Continental Breakfast
8:45 – 8:55	Introduction - Opening remarks from Mark Hufe, Wilmington Univ
9:00 – 10:00	"Intro to Web Security Dojo" *David Rhoades, Maven Security* *<See requirements below if you want to actively participate>*
10:00 – 11:00	The modern approach to security architecture *Lee Gitzes, Sr. Client Solutions Architect, Optiv*
11:00 – 11:15	Break
11:15 – 12:00	Impact of the SEC Cyber Disclosure Rules *Muazzam Malik - Managing Director, Protiviti*
12:00 – 1:00	Lunch
1:00 – 1:30	GDPR – May has come, What now? *Scott Laliberte – Global Cyber Security Leader, Protiviti*
1:30 – 2:30	APT Communication: Domain Fronting...the Death of Reputation Filtering - *John Baek, FusionX/ OWASP*
2:30 - 2:45	Break
2:45 – 3:30	Defending the End Point *Kevin Thompson - Reliaquest*
3:30 – 4:00	Birds of a Feather Discussions – Topics TBD

Abstracts (if available)

Title: Web Security Dojo – Your own personal web app fight club

Format: Presentation with demos and optional follow-along exercises
Length: 60 minutes

Web Security Dojo is a free open-source training environment for learning and practicing web app security testing. It is ideal for self-paced learning and skill assessment, as well as training classes and conferences since it does not require a network to function. Web Security Dojo contains tools, targets, and documentation pre-installed within a single virtual machine image suitable for Virtual Box or VMware.

This presentation will introduce the audience to the Web Security Dojo, and demonstrate how to get up and running in a few easy steps. Participants are encouraged to follow along as the Web Security Dojo is put through its paces locating and exploiting cross-site scripting (XSS) and SQL injection flaws. The flaws and their potential impacts will be explained (and demonstrated) for those not familiar with web app security.

* Set up and use the Web Security Dojo

* Understand two common web flaws, SQL injection and Cross Site Scripting (XSS)

* Locate and exploit XSS and SQL injection using commonly available free tools.

Anyone wishing to follow-along during the presentation should bring a laptop computer so that they can run the Web Security Dojo virtual machine. Student system requirements are simple:

- any operating system that can run the latest stable version of VirtualBox (free from http://www.virtualbox.org/). Currently supported operating systems included Windows, Mac, and Linux. VMWare also works, but you will be shunned like a leper if you have technical issues following along.
- 5 GB of free HD storage
- 2 GB of RAM (more is better)
- wifi networking capability (optional)

Before the presentation please:

1) **Install** the latest stable version of VirtualBox. Optionally you may also install the latest version of "Oracle VM VirtualBox Extension Pack". Both are free and found here: http://www.virtualbox.org/wiki/Downloads
2) **Download** the Web Security Dojo from here: http://bit.ly/webdojo
   This is a virtual machine image (.OVA file).

3) **(Optional but recommended) Importing** and starting this image will be covered during the presentation, but it is best if you try ahead of time in case there are some conflicts with your setup (such as virtualization capabilities disabled in your BIOS). To try the import process simply double click the OVA file. That starts the import process in VirtualBox. Accept the default settings (unless you're sure you know what you are doing). The import process takes about 2 to 5 minutes.

Title: APT Communication: Domain Fronting…the Death of Reputation Filtering

Abstract: Advanced Persistent Threats (APTs) utilize complex methods in all areas of their operation in order to not get detected or caught. One important piece of the operation is communication. APT29, also known as CozyBear, believed to be tied to Russian intelligence, used domain fronting in at least one of its campaign. Its use is becoming popularized in communications that attempt to evade the traditional controls like reputation filtering. We will review in this talk what domain fronting is, show some cool demos, and what kind of defense can help organizations to detect such attempts.

Title: GDPR – May has come, What now?

Abstract: GDPR protects European data subject information, but also places strict requirements on companies that handle this data. The May deadline has passed and regulation is in effect. How will the regulation affect your ability to conduct business with customers and partners? Are you ready to respond to requests and demands from data subjects? We will review in this talk the GDPR requirements, how they may affect your business and what you should do next.