ISC2DE MINUTES 8/13/20

Meeting date and time

- Thursday August 13 10:00 am
- Opened at 10 by Mac

Attendees

Names copied from Zoom windows:

- Mac McKosky
- Jim Chilcutt
- Ray Pompon
- Matthew Ng
- Brian Arcidiacono
- Tom Rainer
- Elayne Starkey
- Jason Wright
- Thomas Glenn
- Chuck Obst
- Sander Vinberg
- Priscilla Vega

Treasurer report

- Presented by Matthew Ng
- Opening balance $1247.42
- Closing Balance $1422. 53
- Dues are $25 per year
  - Mail to Matthew
  - Address: 602 Olde Field Drive, Magnolia, DE 19962
  - Make checks payable to ISC2 Delaware Chapter
- 2020 dues are now due
- Web site payment due in January
- No online payment of dues available at current time
- Motion by Mac to approve Treasurer report
- Seconded by Ray
- Unanimous approval

Last meeting minutes

- Motion made by Mac to skip reading of minutes and accept as posted on web site
- Seconded by Ray
- Accepted unanimously

Membership report

- 12 people on the Zoom meeting
- Members should submit their own CPE credits for the time being
    - Correct process is being investigated

Next meeting location

- Meetings occur on the second Thursday of the second month of each quarter
- Format and location will be announced based on conditions at the time of the next meeting

Old business

- Discussion of our table adventures at Secure Delaware
- Attempts to get a non-profit table at Secure Delaware
- Question,
    - What kind of people are needed for cyber security?
- Senior people are very expensive

New items

- Secure Delaware will be virtual this year
- Discussion on what is cyber security
    - Multi discipline
    - Needs to be communicated to non-technical people
        - i.e. managers
    - Hard to define because skills cover such a broad spectrum
- Where is the industry headed?
- Need people who can translate to non-technical people
- Need discipline not specific fixes
    - Need people who can think and make decisions
- If a company hired you, what is the first thing you would do
    - Suggestion, see if head of cybersecurity can unilaterally shut down everything
    - The suggestion is a test to see how much authority the head of security has in the organization

Presentation topic

- Sander Vinberg – Threat Research Evangelist, F5 Labs
- 2020 Application Protection Report – API's and Making Sense of the Moment
    - https://www.f5.com/labs/articles/threat-intelligence/2020-apr-vol1-apis-architecture
- What are APIs

    - A piece of code to allow software to talk to software
- API can look like a web page or a component
- API incidents are rising
    - Results compiled from open source reports
    - Biggest category
        - Complete lack of authentication
        - Authentication in front of an API
    - Bad authentication
    - Bad authorization after authentication
    - Immaturity in authentication and authorization
- Bulk of issues coming from the tech companies
- No pattern of evolution over time
- APIs use the web to work
    - Hard to draw boundaries around apps
    - Where does one end and the other start
    - Apps are developed making assumptions where data comes from
        - A web user interface for example
    - APIs allow you to incorporate code you did not write into code you did write
- Recommendations
    - Specific controls already exist
    - Cannot really address all content delivery scenarios
- Feedback
    - Info security people do not have the authority to stop deployment of an app that may have security issues

Additional topics

- No additional topics

Meeting ended

- Meeting adjourned at 10:30

PRESENTATION ABSTRACT: THE WEB SECURITY DOJO

TITLE: WEB SECURITY DOJO – YOUR OWN PERSONAL WEB APP FIGHT CLUB

Format: Presentation with demos and optional follow-on exercises

Length: 45-60 minutes (flexible)

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 https://www.virtualbox.org/). Currently supported operating systems included Windows, Mac, and Linux. **VMWare also works.**

- 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