ISC2DE MINUTES 5/14/20

Meeting date and time

- Thursday May 14th 10:00 am

Attendees

Names copied from Zoom windows:

- Mac McKosky
- Jim Chilcutt
- Ray Pompon
- Jason Wright
- Jim Reed
- Brian Arcidiacono
- Matthew Ng
- David Rhoades guest presenter
- Brendan Davis
- Maurice Black
- Ron Teixeira
- Craig Morea
- Larry Merin

Last meeting minutes

- Presented by Jim Chilcutt
- Motion to approve by Mac
- Seconded by Ray
- Approve by all

Treasurer report

- Presented by Matthew Ng
- Opening balance $1247.30
- Closing Balance $1247.42 close
- Motion to approve by Mac
- Second by Ray
- Approved by all
- 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

Membership report

- No update
- 11 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 about who is paying for web site
    - Inigo used to settle the payment for the web site with a credit card but he has moved to Norway
    - Matthew and Mac will investigate
    - When does web site expire? Next renewal date 2021/01/10; Current plan is $17.99 a year

- We are still investigating table at Secure Delaware through OWASP or any other non-profit
    - Suggestions for alternatives are:
        - HTCIA High Technology Crime Investigation Association
        - High tech training for investigators
        - ISSA
        - ISACA

New items

Cyber-attacks spiking?

- Ray has heard that but has seen no evidence of it.
- Discussion of media reviews of hacking and who is doing them

Discussion of the evolution of cybercrime task forces

Most current cybercrime now seems to be phishing and coronavirus scams

Question on whether or not Facebook has authority to police content?

- Do media organizations have responsibility to fact check information
- What are responsibilities of Facebook, Twitter, Instagram etc.

Presentation Topic

- 45 minutes planned
- Abstract attached below
    - Double click to read
- Maven Security Consulting

- Presenter David Rhoades, President Maven Security Consulting – www.mavensecurity.com
  - David.rhoades@mavensecurity.com
- Web Security Dojo
  - A web site providing a preinstalled virtual environment for practicing pen testing techniques
- Some links from the presentation:
  - Dojo.mavensecurity.com
  - Sourceforge.net/p/websecurity.com
  - Websecuritydojo.sourceforge.io
  - Sourceforge.net/p/websecuritydojo/code/ci/master/tree/changes
    - Ubuntu distribution
- Uses VirtualBox from Oracle for virtual machine setups. Its free

Additional topics

- Useful web sites:
  - www.issa-dv.org
  - owasp.org Delaware chapter
  - meetup.com
  - cyber.fastrack.org

Meeting ended

- Meeting adjourned at 11:35

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