**Speakers**

*Thursday – April 23, 2015*

**9 am Jon Schipp/Wayland Morgan**

**Presentation:** ISLET (Isolated, Scalable, & Lightweight Environment for Training)

**Abstract:**  ISLET (Isolated, Scalable, & Lightweight Environment for Training)
is a system that streamlines Linux based software training for IT events. It minimizes the participation barrier to that of an SSH client. It uses Linux containers to provide students with isolated environments from which they can perform work. ISLET is used at the University of Illinois at Urbana-Champaign to teach digital forensics tools and by the Bro Project to teach Bro, among other use cases. This talk will discuss ISLET, the problems it solves, a technical overview of Linux containers, and includes a live demonstration of standing up a brand new ISLET system in under 10 minutes.

Bio: **Jon Schipp** is on the security operations team at the NCSA, and an IT consultant. He is the author of ISLET and a contributor to many Free and Open Source Projects including The Netsniff-NG Toolkit, SecurityOnion, and the Bro Project. Founder of the Open Network Security Monitoring Group (OpenNSM), a weekly research and user DFIR/NSM group without borders, along with multiple LUG's, and the Southern Indiana Computer Klub (SICKbits). Jon has had the pleasure of speaking at many conferences including Derbycon, Hack3rCon, AIDE, BroCon, MOSSCon, and more. He enjoys death metal, intellectual history, and recreational volleyball. More info at [http://jonschipp.com](http://jonschipp.com/%22%20%5Ct%20%22_blank)

**Wayland Morgan** is an IT Security Analyst at the University of Illinois at Urbana-Champaign where he is the team lead for Digital Forensics, Incident Response, and eDiscovery at the University's Office of Privacy and Information Assurance. Wayland began his Information Security career as a vulnerability analyst for a Fortune 200 energy company and since has led several high profile intrusion cases in a heterogeneous R1 research environment. In addition to a bachelors degree in Management Information Systems, Wayland holds several industry recognized certifications such as GCIH, GCFE, GCFA, CISSP, CISA, and ITIL.

**10 am - Bill Gardner/Kim DeTardo-Bora/Amanda Richards**

**Presentation:** Examining Hacktivism: Crime and Punishment in the Digital Age

**Abstract:** Little to no research has been conducted about how the Computer Fraud and Abuse Act of 1986 (18 U.S.C. § 1030) has been used to charge those who have committed computer crimes, especially among the hacktivist group, Anonymous. This presentation will cover the results of our study, which examined seven “operations” (i.e., Chanology (2008), Operation Payback (2010), Operation Paypal (2010), HBGary Federal (2010), Op Sony (2011), Stratfor (2011), and Operation Last Resort (2012-2013), and each of the members of Anonymous who were charged with this federal statute.

Bio: **Kimberly A. DeTardo-Bora** is a Professor of Criminal Justice and Criminology at Marshall University where she serves as both undergraduate and graduate program director. She obtained her Ph.D. in Criminology from Indiana University of Pennsylvania in 2003. Her most recent endeavor has been exploring the world of “hacktivists.” In Fall 2014, she presented a paper titled, “Peering into Hacktivism: The Search for a Criminological Lens” with co-authors Bill Gardner and Amanda Richards. Besides a book titled, *West Virginia’s Criminal Justice System*published with co-authors Dhruba Bora and Samuel Dameron, Dr. DeTardo-Bora’s research has been published in scholarly venues such as *Action Research*, *Corrections Compendium, Security Journal, and Women and Criminal Justice.*

**Bill Gardner** is an Assistant Professor at Marshall University, where he teaches in the Digital Forensic and Information Assurance Program. He is also President and Principal Security Consultant at BlackRock Consulting, and the Information Security Chair at the Appalachian Institute of Digital Evidence. Prior to joining the faculty at Marshall, Bill co-founded the 304Geek and Hack3rCon. Bill is the coauthor of "Building an Information Security Awareness Program: Defending Against Social Engineering and Technical Threats" with Valerie Thomas, which was published in August.

**Amanda Richards** is a graduate student in the Criminal Justice and Criminology Program at Marshall University.

**11 am - Adrian Crenshaw**

**Presentation:** Intro to Darknets: Tor and I2P

**Abstract:** This class introduces students to the I2P and Tor Darknets. We cover setting up Tor & I2P, the basics of use, and how to make hidden services. We also go over case examples like Eldo Kim Harvard & the Harvard Bomb Threat, Hector Xavier Monsegur (Sabu)/Jeremy Hammond (sup\_g) & LulzSec, Freedom Hosting & Eric Eoin Marques and finally Ross William Ulbricht/“Dread Pirate Roberts” of the SilkRoad, to explain how people have been caught and how it could have been avoided.

Bio: **Adrian Crenshaw** has worked in the IT security industry for the last twelve years. He runs the information security website Irongeek.com, which specializes in videos and articles that illustrate how to use various pen-testing and security tools. Adrian is one of the founders of DerbyCon, a large-scale hacker conference located in Louisville Kentucky. Adrian frequently presents at a number of large and small INFOSEC conferences, and contributes to a number of open-source projects.

You can follow Adrian on Twitter: @irongeek\_adc

**Noon – Lunch**

**1 pm – Tess Schrodinger**

**Presentation:**Quantum Computing 01100101

**Abstract:** We have all probably heard at one point or another that quantum computing would render current encryption standards as we know them obsolete.  Intrigued by this assertion, I set about to understand why. This presentation will cover the very basics of classical versus quantum physics to include key concepts in the field, a “not too technical” introduction to quantum computing, an explanation of quantum key cryptography, a comparison of quantum computers versus various types of cryptography (such as lattice and AES), post quantum cryptography, and those currently trying to hack and secure systems in a quantum environment.

Bio: **Tess** **Schrodinger** is a security engineer with Digital Cloak who almost got her undergrad degree in physics.  She began her college experience as a physics major but veered off into forensic science, lollygagged in law enforcement for a spell, and then made the transition into “national security”. She has now come full circle, marrying her years of security experience with her original passion for science and technology.

**2 pm – Aeadan Somerville/Shawn Jordan**

**Presentation:** Introducing Network Scout: Defending the Soft Center of Your Network

Abstract: Everyone is watching the edge of their network. We have installed firewalls, IDS, IPS, and other defensive technologies at the network edge. Network-Scout moves these technologies inside your network to monitor for malicious activities that gets by traditional network perimeter defenses. Network-Scout is a distributed IDS, IPS, and Honeypot that is built on a Raspberry Pi using off-the-shelve technologies for under $150 per device.

Bios: **Shawn Jordan** and **Aedan Somerville** are seniors at Marshall University. They are currently majoring in Digital Forensics and Information Assurance. Shawn Jordan runs a small home inspection company, leads a small college church group, and is conducting forensic research. Aedan Somerville works part time at a local restaurant and is president of the Marshall CCDC team.

**3 pm – 5 pm– Jeremy Druin - Mutillidae (two hour presentation)**

**Presentation:** Web Pentesting with Mutillidae

Abstract: Mutillidae is a free, open source web application provided to allow security enthusiest to pen-test and hack a web application. Mutillidae can be installed on Linux, Windows XP, and Windows 7 using XAMMP making it easy for users who do not want to install or administrate their own webserver. It is already installed on Samurai WTF. Simply replace existing version with latest on Samurai. Mutillidae contains dozens of vulnerabilities and hints to help the user exploit them; providing an easy-to-use web hacking environment deliberately designed to be used as a hack-lab for security enthusiast, classroom labs, and vulnerability assessment tool targets. Mutillidae has been used in graduate security courses, in corporate web sec training courses, and as an "assess the assessor" target for vulnerability software.

Mutillidae has been tested/attacked with Cenzic Hailstorm ARC, W3AF, SQLMAP, Samurai WTF, Backtrack, HP Web Inspect, Burp-Suite, NetSparker Community Edition, and other tools. If you would like to practice pen-testing/hacking a web application by exploiting cross-site scripting, sql injection, response-splitting, html injection, javascript injection, clickjacking, cross frame scripting, forms-caching, authentication bypass, or many other vulnerabilities, then Mutillidae is for you.

The current version of Mutillidae, code named "NOWASP Mutillidae 2.x", was developed by Jeremy Druin aka webpwnized. Mutillidae 2.x is based on Adrian "Irongeek" Crenshaw's Mutillidae project that is now refered to as Mutillidae 1.x or Mutillidae classic. Mutillidae 1.x is still available on Sourceforge along side the current project.

Bio: **Jeremy Druin** GISF, GSEC, GPEN, GXPN, GWAPT, GMOB, Sec+ Email: jeremy@ellipsisinfosec.com Twitter: @webpwnized Jeremy works as a internal pen-tester, application security consultant, and defect-remediation expert for a multi-national transportation logistic company. Jeremy is also the owner of Ellipsis Information Security assisting the community with these security services. Additionally Jeremy develops the open-source Mutillidae 2.x training environment and teaches on security topics. As a Director of Education for the Kentucky ISSA chapter, Jeremy presents on web application pentesting and remediation along with operating the "webpwnized" YouTube video channel. Jeremy has a Bachelors in Computer Science from Indiana University and is a GIAC-certified Web Application, Mobile and Network Pen-Tester.

*Friday – April 24, 2015*

**9 am – Tom Moore**

**Presentation:** TBA

**Abstract:** TBA

Bio: (c0ncealed) **Tom Moore** is a Penetration Tester and former Red Team member for a Fortune 50 organization. He has an extensive background in network administration and web development. He is a graduate of Marshall University, member of 304Geeks, and the Security Awareness Training Framework project. He is an unremitting g33k, husband, father, and Christian. He enjoys his 2nd amendment, outdoor primitive recreation, photography, gaming, lock picking, and inserting random single quotes where they don’t belong.”

Twiter: @c0ncealed’s

**10 am - Elliott Cutright**

**Presentation:** OWASP Applied

Abstract:  A look at real world web application flaws and what can be gained from their exploitation. We will look beyond alert('xss') and ' or 1=1-- on a variety of popular web application platforms using real world code and examples.

Bio: **Elliott Cutright** is a Senior Red Team analyst with a large US corporation based in the Richmond Virginia area. Specialized in Linux post exploitation, web applications and password cracking. He can be found tweeting about his favorite hipster beer @nullthreat.

**11 am – Brian Martin**

**Presentation:** The Future of Digital Forensics: Rust Never Sleeps

**Abstract:** Forensics is a volatile field, and electronic forensics is the most volatile aspect due to the rapid advancement of commercial technology.  We’ve gone from a local problem of passed paper notes cribbed in code, to a global front of high end encryption passed in white spaces, games, and images.  As practitioners, we’ve had to adapt to every new tech trend that came along and the future is not slowing down.  Where is it going and what can we do to prepare?  In this talk, Brian Martin of Digital Trust discusses trends, likely futures, and practitioner and market responses.

Bio: **Brian Martin, CISSP, CHFI, BS** is a computer security expert and electronic evidence specialist with Digital Trust® in Allentown, PA. Digital Trust assists clients and legal agencies with electronic evidence, digital forensics, and security consulting.

Noon – Lunch

**1 pm – Frank Hackett**

**Presentation:** TBA

**Abstract:** TBA

**Bio: TBD**

**2 pm – Dave Kennedy (Keynote)**

**Presentation:** TBA

**Abstract:** TBA

Bio: **David Kennedy** is the founder and CEO of TrustedSec and Co-Founder and CTO of Binary Defense Systems (BDS).  Kennedy is a co-author of the book “Metasploit: The Penetration Testers Guide,” the creator of the Social-Engineer Toolkit (SET), and the creator of Artillery. Kennedy has presented on a number of occasions at Black Hat, Defcon, ShmooCon, BSIDES, Infosec World, Notacon, AIDE, ISACA, ISSA, Infragard, Infosec Summit, and a number of other security-related conferences. Kennedy has been interviewed by several news organizations including CNN, Fox News, and BBC World News. Kennedy is one of the co-authors of the Penetration Testing Execution Standard (PTES); a framework designed to fix the penetration testing industry. Kennedy is the co-founder of DerbyCon, a large-scale conference in Louisville Kentucky. Prior to the private sector, Kennedy worked for the three letter agencies and deployed to Iraq twice for intelligence related missions.

**Twitter:** @HackingDave

**3 pm – Jayson Street (Keynote)**

**Presentation:** BREAKING in BAD (I’m the one who doesn’t knock)

**Abstract:** I’m come to realize that while I’m may not do a lot of social engineering engagements I do a quite a few weird ones. I also seem to have three main roles I play (all adorably) to try to get into my target. I thought it would be cool to share at least a story from each one of these roles. Some have pictures, some with just witty comments. Though all three will come more importantly with ways that would have stopped me from being successful. The goal is not to show how ‘L337’ I am or these attacks are! Far from it this talk is to show how EASY these attacks were done and how every single attack has one common thread connecting all of them! Though you’ll have to see my talk to find out what that is! ;-)

Bio: **Jayson E. Street** is an author of “Dissecting the hack: The F0rb1dd3n Network” from Syngress. Also creator of http://dissectingthehack.com He has also spoken at DEFCON, DerbyCon, UCON and at several other ‘CONs and colleges on a variety of Information Security subjects. His life story can be found on Google under “Jayson E. Street” \*He is a highly carbonated speaker who has partaken of Pizza from Beijing to Brazil.

**Twitter:** @jaysonsteet