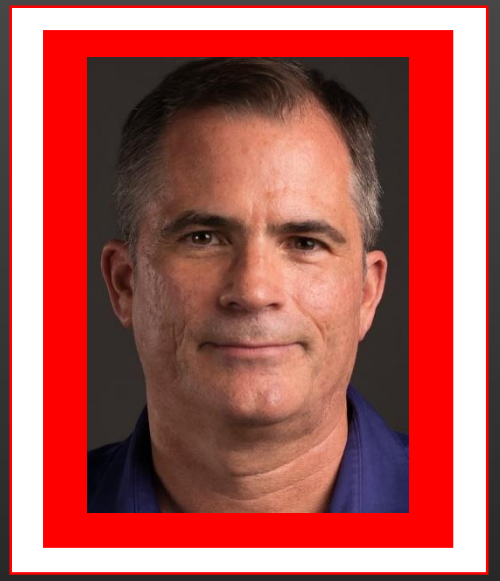
22nd CISSE Colloquium

Practical Hands-On Training and Foundation Skills in IT Curriculums

Kevin Cardwell, MSSE

EC-COUNCIL | ACADEMIA
PREPARING THE NEXT GENERATION OF CYBER SECURITY EXPERTS

Kevin Cardwell, MSSE



- Master of Science in Software Engineering
- Adjunct Faculty
  - UMUC – 18 years
  - UCLA Extension – 5 years
- EC-Council University(ECCU) Advisory Board
- 25 Years in IT Security Consulting
- 30 Years in Curriculum Development
- Author
  - EC-Council Center for Advanced Security Training (CAST)
  - EC-Council Licensed Penetration Testing(LPT) - Advanced Penetration Testing Course
  - Over 7 Other Additional Publications

EC-COUNCIL | ACADEMIA
PREPARING THE NEXT GENERATION OF CYBER SECURITY EXPERTS

Agenda

1) Discussing Cybersecurity Training Observations

2) Exploring Requirements for Foundational Skills

3) Introducing the Mobile Security Toolkit, STORM

4) Identifying Examples of STORM Usage

5) Assessing Deployment Options for a Mobile Security Toolkit Network

Cybersecurity Training Observations

- It is critical that hands-on training be part of any Cybersecurity training program
- Theory based training is not effective for enforcing the skills needed to perform at a high level in Cybersecurity
- The practice of participating in a Capture-the-Flag(CTF) competition has become popular, and while a vehicle for skills development, it has to meet the realistic requirements, part of which includes…
  - The Network representative of an actual network

    (Many of the CTF exercises are on a flat and not a layered network)
  - The interface is accurate

    (Many of the CTF exercises are "gamified" and more video game than realistic)

CTF Research

- Effectiveness of Cybersecurity Competitions

- Ronald S. Cheung, Joseph Paul Cohen, Henry Z. Lo, Fabio Elia, Veronica Carrillo-Marquez *Department of Computer Science University of Massachusetts Boston* *CLICK HERE TO ACCESS*

- Using CTFs for an Undergraduate Cyber Education

- Martin Carlisle, Michael Chiaramonte, and David Caswell *Department of Computer Science United States Air Force Academy* *CLICK HERE TO ACCESS*

EC-COUNCIL | ACADEMIA
PREPARING THE NEXT GENERATION OF CYBER SECURITY EXPERTS

Effectiveness of Cybersecurity Competitions

- Pique's student interest in Cybersecurity
- Effectiveness of this approach in producing high quality cybersecurity professionals is limited
- Knowledge barrier needed to compete in these competitions is extremely high
- Students have to be proficient in numerous topics
- Majority of CS majors feel that they do not possess the right skill set

Using CTFs for an Undergraduate Cyber Education

- Immensely beneficial experience gained from red-blue team exercises is the interplay between offensive operations and defensive operations
- Tough challenges and team based activities allow students to collaborate and teach each other
- CTF approach is highly effective at encouraging student learning of Cybersecurity
- A willingness for more self-directed learning

EC-COUNCIL | ACADEMIA
PREPARING THE NEXT GENERATION OF CYBER SECURITY EXPERTS

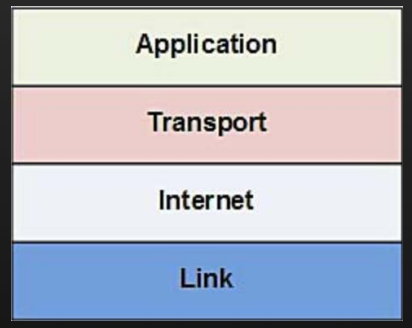
Job Skills

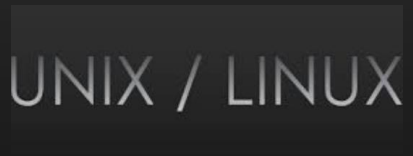
- Does the curriculum produce skilled students
- The NICE initiative was created for this
- Reality
  - *Many of the programs fall short at delivering job skill specific training*

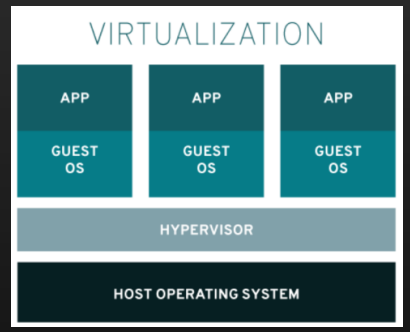
  - Focus is more on the application layer and the different tools than it is on the foundational skills

Foundational Skills

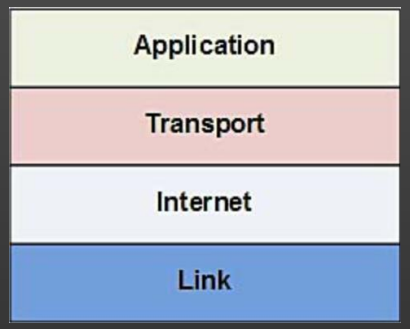
- A lack of focus at the building blocks of security
- Three main areas to develop
  - TCP/IP
  - Unix/Linux
  - Virtualization







TCP/IP

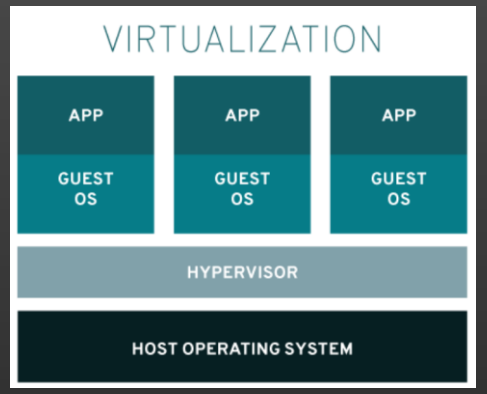


- The backbone of the Internet
- Everything takes place at the packet level unless we are isolated to the host machine
- Job skills need to be to the level of understanding the communication and transport of the network traffic
  - Flags of TCP
  - Components of normal traffic and attack traffic
  - Reading of protocol headers
  - Perform protocol analysis

Unix/Linux

- Virtually all of the open source tools come out with a *nix platform
- Takes approximately 6 months to port to Windows, and not necessarily stable
- All students who are “Windows” centric are behind the curve
- Provides the capability to teach the low level functionality of exploitation

Virtualization



- An area that is often overlooked
- Required to effectively build a range environment
- Most curriculums teach how to use ranges, but not build them
- We need to teach our students how to build their own ranges
  - This provides the best experience and skills for working in cyber security
  - When a student builds a range virtually they will acquire
    - Knowledge of routing and methods of controlling traffic
    - Multihomed methods of emulating true enterprise architectures

Recommendation

- Build Cybersecurity curriculums that focus on the foundational skills
- Enhance programs with these skills, so that they are practiced at every level
- Repetition is required and essential
- Foundational skills are perishable
- Place more focus on knowledge building on layer 2-4 of the network
- Require curriculums to train students to build their own cyber ranges

EC-COUNCIL | ACADEMIA
PREPARING THE NEXT GENERATION OF CYBER SECURITY EXPERTS

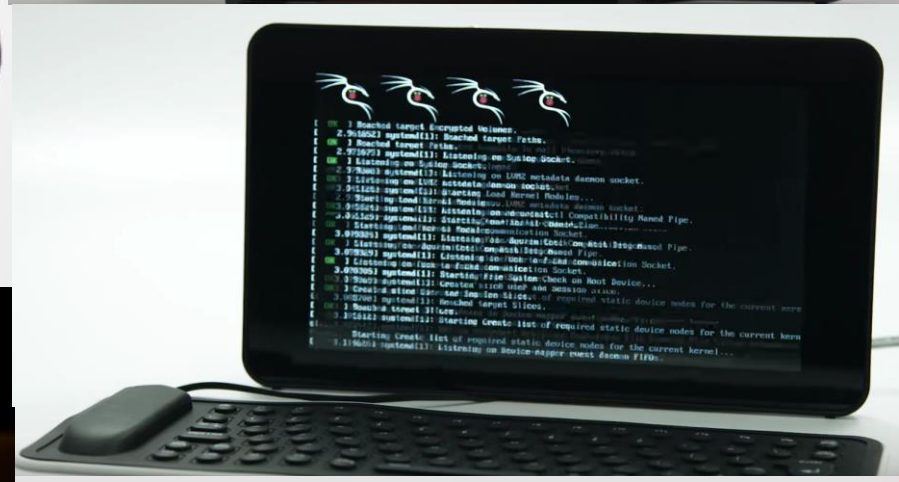
EC-Council

STORM

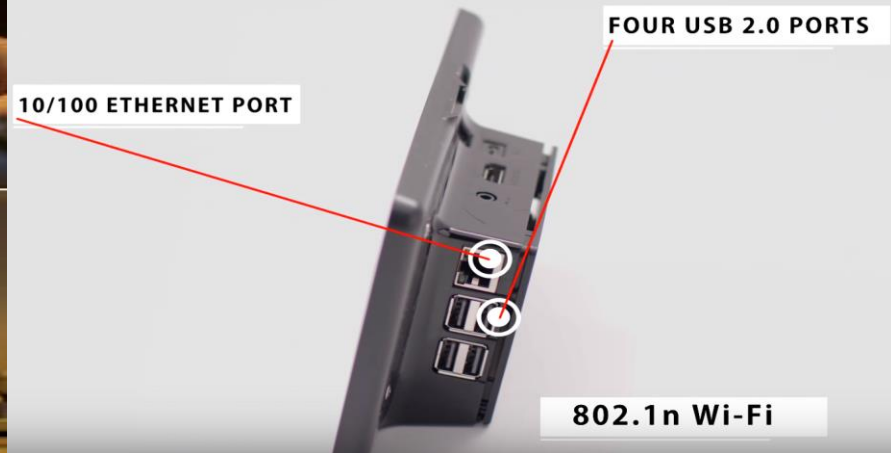
Mobile Security Tool Kit

ETHICAL HACKING WORKSHOP

[CLICK HERE TO SEE A VIDEO OVERVIEW]

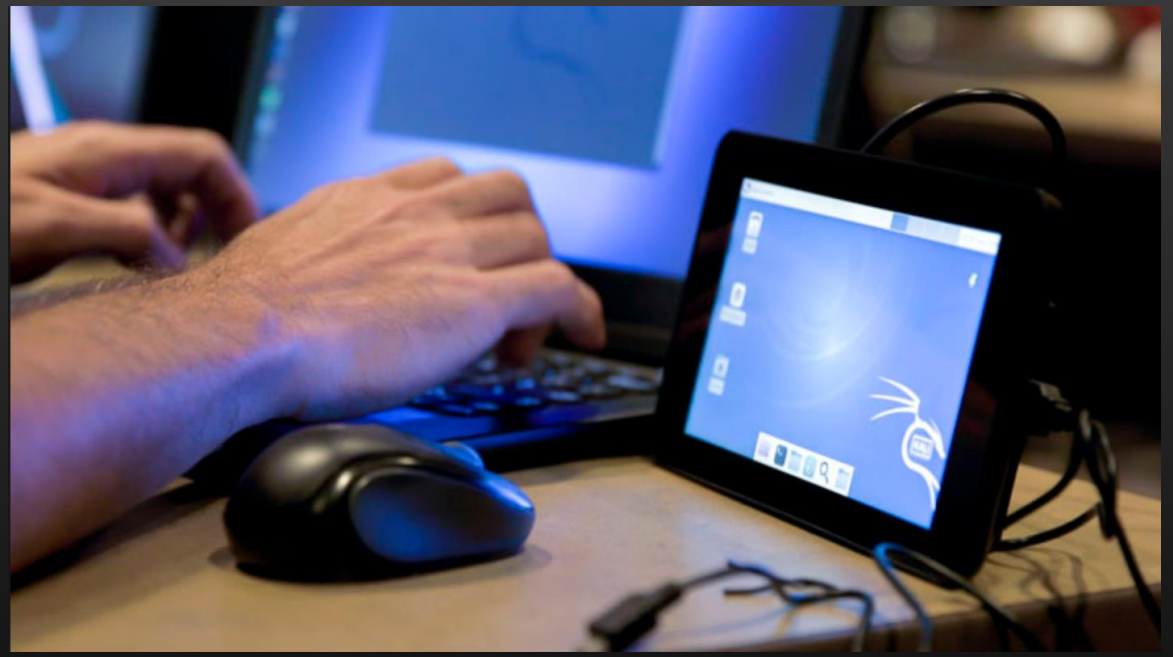


Click Here to see our full Mobile Security Workshop List



STORM Specifications

- 64 Bit – Quad Core Mobile System with Case
- 1 GB RAM
- 7 inch Touch Screen Display
- 64 GB MicroSD – Preloaded w/Custom Linux Hacking OS
- 100Mb Ethernet Port
- 4 USB Ports
- 802.11n Wireless
- Bluetooth 4.1



STORM G-Force 10 Expansion Pack Specifications

- JBtek Raspberry Pi Micro USB Cable ON/Off Switch
- 20000mAh, 4 Port Power Supply
- Software Defined Radio
- Super Mini Wired Keyboard
- HooTOo Wireless Travel Router
- TP-Link N150 Wireless High Gain USB Adapter
- USB Powered 10/100 5-Port Switch
- Raspberry Pi 3 Power Supply

STORM Image

- Custom Linux distribution
- Loaded with tools
- Portal for updates
  - We provide the latest working images
  - Saves you the challenge of keeping the updates and tools working
    - ARM images are not the most stable
- Support available
- Lifetime updates

Why the STORM was Created

- Too many struggle with getting their tools and attack platform setup
- Once setup, another challenge is getting the tools working
- At updates, the tools often break
- Numerous students come to classes with company provided laptops
  - Have endpoint protections
  - Cannot access the network configurations
  - Makes virtual machines difficult to setup
- Provides a working and portable platform for attack or defenses
  - Hack from the palm of your hand

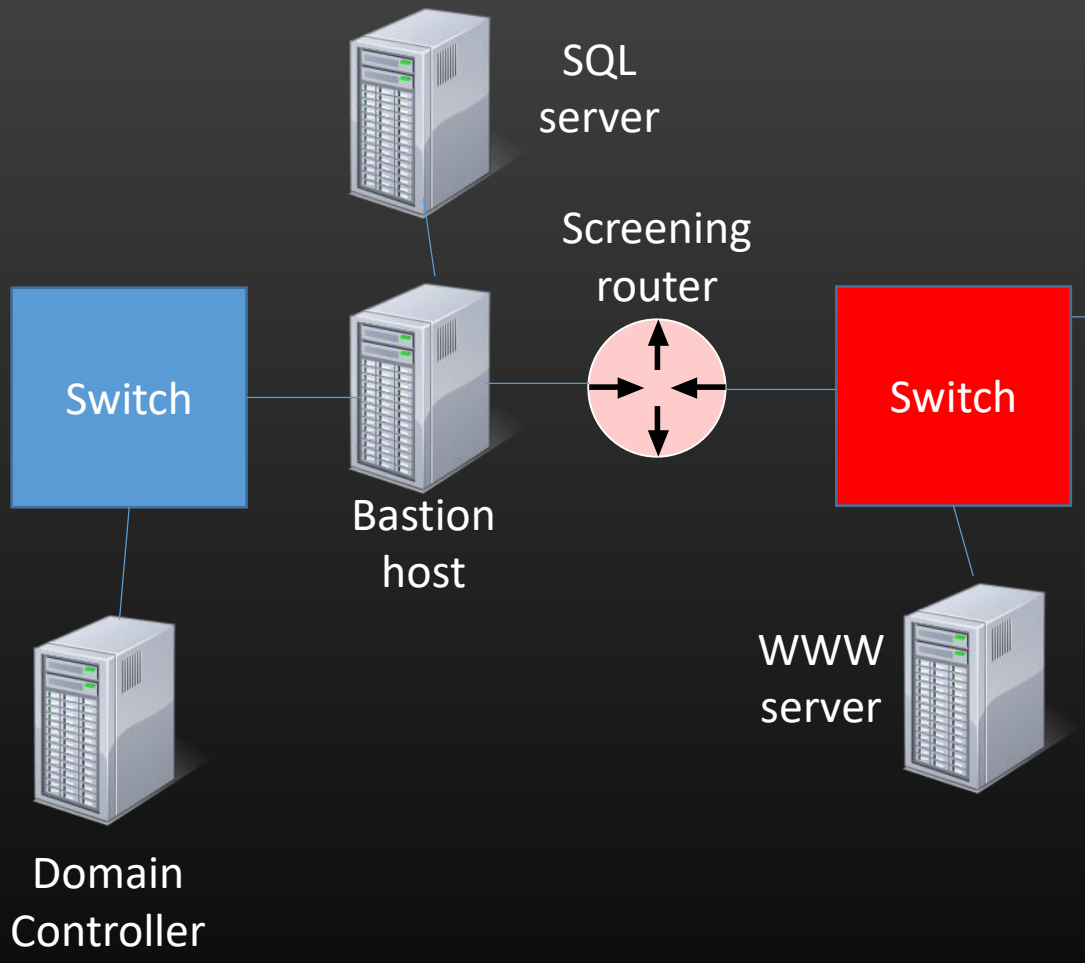
Examples of Storm Usage

- Use a virtual bridge
  - Connect your Storm device to your laptop/machine
  - Run virtual software
  - Create a switch and bridge it to your Storm device
- Isolate the Storm
  - With the bridge
  - Use wireless to wired routing
- Configure secure remote access, send a Storm device to your client and connect from the Internet
  - Do your assessments from your back yard ☺
  - No airport security checks!

Storm in the Curriculum

- Provides the students a working attack platform loaded with tools
- In the early stages of development the students can focus on practicing the processes of hacking and defense
- At the intermediate level the Storm can be used as a bridge device
- At an advanced level the Storm can be used for hardware as well as software customization

Mobile Testing Lab



Mobile Testing Lab in the Curriculum

Entry level

- Provide the machines for the architecture
- Have the students practice the process and methodology
- Explore the different layers of routing traffic

Intermediate level

- Have the students build the network machines and architecture
- Configure basic traffic rules through the perimeter filters

Advanced level

- Add more machines to the architecture and create advanced rule sets
- Create SQL applications and test them
- Hardening the machines in the net

Conclusion

- ✓Discussed Cybersecurity training observations
- ✓Explored requirements for foundational skills
- ✓Introduced the Mobile Security Toolkit STORM
- ✓Identified examples of STORM usage
- ✓Assessed deployment options for a Mobile Testing Lab

Thank you to all of the participants that registered for the Mobile Security Tool Kit class held at CISSE 2018!

Questions?