Experiential Learning Via Cyber Ranges

National Institute of Standards and Technology (NIST)
Federal Information Systems Security Educators’ Association (FISSEA)
Awareness – Training – Education

Center for Security Studies
Funding provided by CAE Cybersecurity Grant Program - S-004-2017 CAE Cybersecurity (CAE-C) “Investment in Expansion of CAE-C Education Programs”
Dr. Loyce Best Pailen, Principal Investigator
Questions to Explore

1. How do we increase the pipeline of cybersecurity talent?

2. How does experiential learning via Cyber Ranges support this objective?

3. How is the Cyber Range industry developing and who are the players?
Increasing the Supply of Cyber Talent

Cybersecurity Ventures predicts 3.5 million unfilled cybersecurity positions by 2021
NICE Cybersecurity Workforce Framework

- Analyze
- Collect and Operate
- Investigate
- Operate and Maintain
- Oversee and Govern
- Protect and Defend
  - Defense Analysis
  - Defense Infrastructure Support
  - Incident Response
  - * Vulnerability Assessment & Mgmt
- Securely Provision

<table>
<thead>
<tr>
<th>Vulnerability Assessment &amp; Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>A0001</strong>: Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.</td>
</tr>
<tr>
<td><strong>A0044</strong>: Ability to apply programming language structures (e.g., source code review) and logic.</td>
</tr>
<tr>
<td><strong>A0120</strong>: Ability to share meaningful insights about the context of an organization’s threat environment that improve its risk management posture.</td>
</tr>
<tr>
<td><strong>A0123</strong>: Ability to apply cybersecurity and privacy principles to organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).</td>
</tr>
</tbody>
</table>

KP Professional Maturity Model

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>A0001</td>
<td>50-75</td>
<td>75-100</td>
<td>100-125</td>
</tr>
<tr>
<td>A0044</td>
<td>50-75</td>
<td>75-100</td>
<td>100-125</td>
</tr>
<tr>
<td>A0120</td>
<td>50-75</td>
<td>75-100</td>
<td>100-125</td>
</tr>
<tr>
<td>A0123</td>
<td>50-75</td>
<td>75-100</td>
<td>100-125</td>
</tr>
</tbody>
</table>
Cyber Ranges & Experiential Learning

Cyber ranges are interactive, simulated representations of an organization’s local network, system, tools, and applications that are connected to a simulated Internet level environment. - NIST
Why Use A Cyber Range?

• Provide Performance Based Learning And Assessment
• Provide a Simulated Environment Where Teams Can Work Together
• Provide Real-Time Feedback
• Simulate On-the-Job Experience
• Provide an Environment Where New Ideas Can be Tested

Experiential Learning via Cyber Range

- Red teams attempt cyber attacks against an enterprise’s security posture
- Green teams are legitimate users connected with various devices (wireless and/or wired)
- Blue teams defend an enterprise’s use of information systems by maintaining its security posture
- White teams create the situations under which the teams compete and monitor results
Congratulations! You are now responsible for rhinoribbons.org, here are your credentials: admin:Rhinos

**Machines in the network:**

- **External:**
  - Web: www.rhinoribbons.org - 185.110.107.59
  - Mail: mail.rhinoribbons.org - 185.110.107.131

- **Internal:**
  - Database: db.rhinoribbons.org - 10.0.0.15
  - File server: fileserver.rhinoribbons.org - 10.0.0.39

- **Border:**
  - Firewall: fw.rhinoribbons.org - 185.110.106.2, 10.0.0.1, 185.110.107.1

There is a backup of the website in root's home directory on www.rhinoribbons.org
You should complete the following before the close of business today:

1. Setup your email client and check it often. There may be important emails that you will need to attend to.
2. Ensure the firewall is properly configured such that only absolutely required traffic can get from the DMZ to the LAN.
3. Ensure all external servers are safe from SSH brute force attacks. Policy change is at your discretion.
4. Inspect your network for any additional flaws or poor security practices and take appropriate action or report your findings.

Configuring your email client:

1. Open Thunderbird and press "Skip this and use my existing email"
2. Enter your name: email: admin@rhinoribbons.org; password: Rhinos
3. Use mail.rhinoribbons.org for both the incoming and outgoing server hostname and choose re-test.

Open Cyber Challenge Platform: https://opencyberchallenge.net/
Experiential Learning: Capture the Flag (CTF)

- Teams compete for flags that hold point value placed on network
- Teams can be co-located (separate rooms) or Virtual
- Attack – Defend
  - Red Team Vs. Blue Team
- Jeopardy Style
  - Red Team vs. Red Team
  - Blue Team vs. Blue Team
- Resources
  - Open Web Application Security Project (OWASP)
  - National Cyber League (NCL)
  - International Capture The Flag (ICTF)
  - CTFTime.org
Sample Learning Path

**Intern (Aware)**
- Module 1: * Basic Learning Skills
- Module 2: * IT Basics
  * Modeled on Comp TIA A+ Program

**Apprentice (Novice)**
- Module 3: * Workstations/Servers/Networks
- Module 4: * Networks / System Admin
- Module 5: * Admin/IT Security/Cyber

**Professional (Intermediate)**
- Module 6: * Security Ops/Cyber Review / Tools
- Module 7: * Hands on Cyber Range
  * Practice Handling Real World Threats

Baltimore Cyber Range (https://www.baltimorecyberange.com/)
Cyber Range Industry Profile

Military/Government, Academia and the Private Sector are all engaged in building cyber ranges with significantly different scale and capabilities
Cyber Range Industry Profile

Military / Government
- National Cyber Range (NCR)
- DoD Cyber Security Range (CSR)

Private Sector
- Metova (CENTS/SLAM-R)
- IBM (X-Force)
- Raytheon (CODE)
- Financial Sector Information Sharing and Analysis Council (FS-ISAC)

Academia
- AR: University of Central Arkansas ([https://uca.edu/cnsm/2017/10/05/cyber-range-announcement/] )
- AZ: Grand Canyon University ([https://www.azcwr.org/] )
- FL: University of West Florida ([https://floridacyberrange.org/] )
- GA: Augusta University ([http://cyber.augusta.edu/georgia/] )
- MI: Wayne State/Oakland University ([https://www.merit.edu/cyberrange/] )
- VA: Regent University ([https://www.regent.edu/institutes/cybersecurity/cyber-range/home.cfm] )
- VA: Virginia Tech ([https://virginiacyberrange.org/] )
## Who is Using Cyber Ranges?

<table>
<thead>
<tr>
<th>Who</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professionals</td>
<td>Professionals from diverse groups such as information technology, cybersecurity, law enforcement, incident handlers, continuity of operations, and others use cyber ranges to improve individual and team knowledge and capabilities.</td>
</tr>
<tr>
<td>Students</td>
<td>Students can use cyber ranges to apply knowledge in a simulated network environment, develop cyber skills, work as teams to solve cyber problems, and prepare for cyber credentialing examinations.</td>
</tr>
<tr>
<td>Educators</td>
<td>Educators can use cyber ranges as a classroom aide or instruct or assess students virtually.</td>
</tr>
<tr>
<td>Organizations</td>
<td>Organizations can use cyber ranges to evaluate their cyber capability, test new procedures, train their team on new organizational and technical environments and protocols before they are introduced into the organizational environment and expand personnel abilities.</td>
</tr>
</tbody>
</table>

Jim Smith III
CADF Fellow
Adjunct Professor, UMUC
CEO, Kinetic Potential Scholars
Jim.Smith@faculty.umuc.edu
301.883.8256