

# **Standing up a Cyber Range Capability in Michigan**

Centre for Secure Computing (CSC), De Montfort University  
Partnered with the Michigan Cyber Security Center (MCC)

## Background of the Problem

- America's Cyber-Infrastructure is under attack
- Those attacks come in the form of break-in's, denials of service, eavesdropping, man-in-the-middle, data modifications and any other exploit that the human imagination can develop
- Any of these exploits can be run on any network at any time and the incidence of all of these types of attacks is growing

## Background of the Problem

- For instance – according to the Computer Security Institute's (CSI) most current annual survey
  - 90 percent of respondents detected computer security breaches
  - 80 percent reported financial losses due to security breaches
  - 44 percent quantified their financial losses, reporting a total of US \$455,848,000 in losses
  - 74 percent of respondents reported their Internet connection as a frequent point of attack
  - 33 percent reported their internal systems as a frequent point of attack
  - 34 percent of respondents reported these intrusions to law enforcement

## Background

- 40 percent of respondents detected a system breach from the outside
- 40 percent detected a denial of service attack
- 78 percent detected employee abuse of Internet access privileges
- 85 percent detected computer viruses
- 38 percent were aware of unauthorized access or misuse of their Web sites
- 39 percent of those who reported attacks reported 10 or more incidents
- 70 percent of those attacked reported vandalism
- 55 percent reported theft of transaction information
- 6 percent reported financial fraud
- Information theft and financial fraud contributed to the most serious financial losses

## What is a Cyber Range?

- A cyber range is like having the entire Internet in a bottle
- It is essentially a virtual environment on a massive scale
- Such a capability has heretofore been impossible to achieve using current virtualization techniques
- That is because we do not have the computing horsepower needed to generate and support an environment of the necessary size

## What is a Cyber Range?

- A Cyber-Range capability offers a practical and controlled setting where attack scenarios and security responses can be evaluated in real-world conditions and recorded and analyzed to improve the overall resilience of target networks
  - This massive increase in scale offers the capacity to emulate any host domain and an infinite variety of endpoints.
  - Those virtual elements can then be subjected to countless simulated external or internal cyber exploits.
  - In that respect, it allows an organization to test very large-scale cyber security solutions without impacting operations.

## What Does a Cyber Range Allow You To Do?

- The best way to fully understand the weakness present in a network is to attack a network. This is called “penetration testing” or “ethical hacking”
- **Aim:** to attack the corporate infrastructure and attempt to breach any network borders.
- **Problem:** these types of tests are basically destructive events that could compromise network stability and even cause service failure.
- **Dilemma:** potentially harming the organization’s network in order to better understand how to prevent harm to it

## What Does a Cyber Range Allow You To Do?

- A cyber-range removes that paradox
- The Cyber Range (CR) provides a unique testing environment that allows large and small scale networks to be simulated using a mixture of virtual and physical devices.
- Once a network has been placed onto the Cyber-Range, it can be attacked and defended without having to place the organization's actual networks at risk.

## **What Does a Cyber Range Allow You To Do?**

- The Cyber-Range's simulations can also be used to test hardware, software, and to help prepare for any large network upgrades or to diagnose network problems.
- As an interactive environment, the Cyber-Range is an ideal place to train and educate network responders and infrastructure design teams to be more secure and efficient.

## What Does a Cyber Range Allow You To Do?

- The best way to understand the term “range” is to think of a military rifle range where people can practice to become expert in the use of a weapon
- The difference between a cyber-range and a rifle-range is that the rifle range just has cardboard soldiers.
- With a cyber range you have a simulated battlefield with a simulated airspace, maritime and even outer space if you want it
  - filled with friends and foe that you can interact with and who shoot at you (both the friends and the foes).
- In the UK, they do military exercises on Salisbury Plain. The cyber range is similar except it is inside a bunch of computers.

# Overview

- Users can easily create and tear-down entire network environments in order to test the performance of new hardware and software.
- Users can create their own custom environments.
  - These custom environments can be stored within User Profiles for later use.
  - Pre-configured environments can be modified to suit exact requirements.
  - Environments are configured in the current Cyber-Range using a simple web interface or API, communicating using XML over HTTPS.

## General Capabilities and Services of the Cyber-Range

- Networks can be deployed onto the Cyber Range with full functionality, to enable field testing of cutting edge cyber tools.
- The Cyber Range can be made available to remote clients, in order to provide services to a very wide-area audience.
- In addition, the current participating organizations offer:
  - Operational support for the range
  - Research and development environments for field testing the latest cyber-defense tools
  - Education and training environments to ensure the next generation of cyber warriors

## Enhanced Opportunities

- Cyber range operators can enhance their situational awareness capabilities by learning about how to do things such as:
  - Identifying and responding to threats
  - Performing network forensics triage activities
  - Doing trouble ticketing and DIN deployments
  - Practicing incident response and other real-time security operations.

## Enhanced Opportunities

- People can be trained in a realistic cyber attack environment.
  - The IT Department may know how to patch boxes and recover from malware outbreaks, but have they tried their skills and procedures while under a simulated attack from organized crime gangs
  - In a single day, IT workers can experience—in a cyber paintball exercise—how they match up to the challenge of the best of the best.
  - The debrief after use of the range shows the IT workers what was going on, what they did and guides them toward best practice.
  - It is a lesson they are not likely to forget.

## Enhanced Opportunities

- Cyber range operators can enhance their tests and simulation capabilities by inserting customized or proprietary hardware and software into the Cyber Range and then utilizing the Range to allow clients to do their own testing.
- Academia and industry can test full-scale, revolutionary research in the Cyber Range's simulated real world environment and obtain immediate feedback.

## Enhanced Opportunities

- Processes for incident response, new security utilities, and procedures can be tested in the cyber range to ensure they can withstand the rigors of a full-on attack.
- By simulating an organization's IT infrastructure and placing it under attack, realistic testing can be done and provide a greater sense of confidence that the solution works.
  - And if it does not, at least you found out before it went live.
- There is no current way of testing infrastructure in its operational environment without a cyber range unless you are prepared to attack your production network.

## Why This Cyber Range is the Right One

- Our Cyber-Range does not use a purely virtualized environment with VMware virtual machines connected through standard IPv4 /24 networks using Active Directory
- We can simulate any network and we can connect any set of parts together.
  - For example, we can use the hardware of the cyber range efficiently to sketch out the vast areas that don't require much fidelity using modified honeynets to simulate large parts of the internet.
  - Parts that do need to be more realistic can be run as virtual machines, but we use a variety of different virtualization techniques and make them play nicely together.
  - **And** For those parts where virtualization is still not realistic enough, we can insert real, physical networks, real switches and routers and real endpoint devices (SCADA devices, cash machines, physical servers, laptops, etc.), and the physical and virtual components work seamlessly together.

## Current Development Work

- Current development work focuses on augmenting the Cyber Range by integrating various APIs to provide a holistic picture of real-time Internet environments.
  - A real-time dashboard based around Pharos will be one of the first of these APIs integrations
- Other areas of development include the development of massive-scale mobile computing simulations in order to better understand what the addition of that new capability represents for modern networks
- Finally, direct applications in the military and law enforcement are being developed and tested on the range in order to determine their feasibility and effectiveness in practice

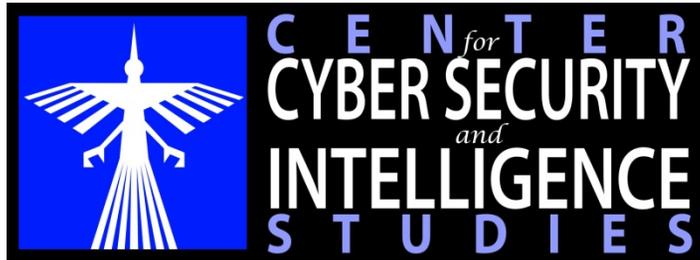
## Finally - Who Are We?

- The Centre for Secure Computing (CSC) at DeMontfort University is a multi-disciplinary group of academics and industry experts who focus on a wide variety of computer forensics and security issues
- The prospective Michigan Cyber Range (MCR) is partnered with the CSC
- The MCR will have an active role in research and development efforts, coordination of cyber security activities, and the provision of active lab resources for research of threats and creation of responses.

# What's in it for the State

- The Michigan Cyber-Range will facilitate:
  - The development of an elite cyber workforce;
  - Targeted training and education programs; and
  - Creation of distinct opportunities for traditional students and displaced technical workers.
- Benefits of the Michigan Cyber Range include:
  - Critical infrastructure and key resource protection from cyber attacks
  - A collaborative environment between the public and private sectors
  - Secure network for cyber security testing
  - Enhanced research and development to respond effectively to existing challenges
  - Innovative and dominant defenses against cyber attacks, to include the Defense Industrial Base

# Thank you for your Attention



Dan Shoemaker PhD,  
Professor and Senior Research Scientist  
Center for Cybersecurity and Intelligence Studies  
University of Detroit Mercy

[Dan.shoemaker@att.net](mailto:Dan.shoemaker@att.net)