
MARYLAND
CYBER CHALLENGE
2014 Overview
leidos
UMBC
StaySafeOnline.org
National Cyber Security Alliance
CYBER MARYLAND
Epicenter for Information Security & Innovation
TECHCOUNCILOFMD
MdBio | MdTech

Why Participate?

- Explore: Discover the world of cybersecurity
- Encourage: Motivate participants towards cybersecurity careers
- Educate: Learn and improve cybersecurity skills
- Enhance: Teamwork, collaboration, critical thinking
- Enrich: Compete for scholarships and/or cash prizes
- Enjoy: A fun challenge

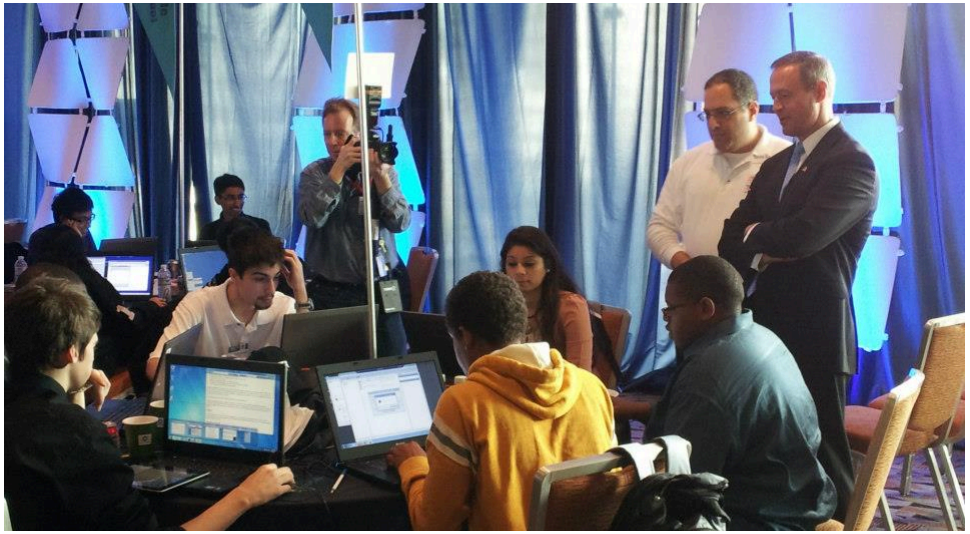
Contestant Requirements:

Basic understanding of Windows/Unix and the Internet
Willingness to Learn
Work as a Team
Desire to Have Fun

Background

- Over 700 Competitors and 115 teams over the past 3 years
- 3 Divisions
  - High School
  - College
  - Professional
- Team Sizes of 3-6 members
- Over $250,000 in student prizes awarded to date
- Internships offered to student winners and runners-up
- Trophies, cash, and/or professional development prizes for professional team winner
- Competition finals run alongside 2 day conference
- Open to teams **Nationwide!**

MARYLAND
CYBER CHALLENGE



Building a Team

- You can represent your organization or create a team with members from various organizations and companies
- Individual names will not be publicized nor will your company name (unless it's part of your team name)
- Your team name **will** be publicized.
- Only first and second place winners will be made public
- Team rankings will be given only to teams and not released publically
- Pictures will be taken at the event for use to market the event in the future
- **Register soon!** Team rosters will be locked on September 9th
- Identify your captain. This is the main communication point throughout the event.

Challenge Timeline

- **Registration Closed – September 9, 2014**
- **Practice Round #1 (unscored)**
  - Windows – August 12, 2014
  - Linux – August 18, 2014
  - Forensics – August 20, 2014
- **Practice Round #2 (unscored)**
  - Windows – August 25, 2014
  - Linux – August 27, 2014
- **Qualification Round 1 (Scored) - September 13-15, 2014**
  - System Hardening for all competitors
- **Qualification Round #2 (Scored) – September 21-23, 2014**
  - System Hardening for High School (different target)
  - Forensics for College & Professionals
- **Finals @ Baltimore Convention Center**
  - October 29 for College & Professionals
  - October 30 for High School

Online

Challenge Game Types

- System Hardening (Practice/Qualifications)

  Analyze Windows & Linux systems for vulnerabilities or potential vulnerabilities and secure systems that are vulnerable

- Forensics (College and Professional)

  Finding and reporting evidence of intrusions, discovery of malware, analysis of payloads, log analysis, network analysis, and tracking of attackers on images either of computer systems or USB drives. The more details reported to the White Team, the more points earned.

- Defense/CND (High School)

  Defending a network being attacked by a live Red Team, while maintaining critical services and securing hosts, detecting and mitigating Red Team activity and other misuse, and communicating findings.

- Attack/Defend – Capture the Flag (College and Professional)

  Compromise and control targets, maintain control of targets, and secure your own targets against other teams' attacks. The longer a team holds a target and maintains its critical services (i.e., 'Capture and Defend'), the more points earned.

Key Skills for Success

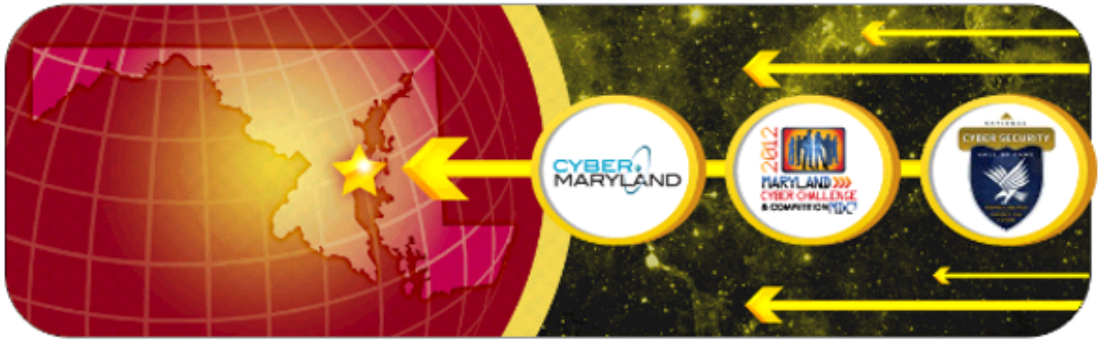
- System Hardening
  - Windows & Linux System Administration knowledge
- Forensics
  - Disk image analysis
  - File carving
  - Log file analysis
  - Network traffic (Packet Capture) analysis
- Attack/Defend – Capture the Flag
  - Windows & Linux System Administration
  - Log File Analysis
  - Incident Response & Handling
  - Intrusion Detection
- Teamwork, Organization, & Good communications skills are essential!

Helpful Hint

- During each round, you can download and 'work on' as many VMs as you wish to make effective use of your team's time. However, only **one** VM may connect into CyberNEXS to represent your team for scoring purposes.
- Multiple logins from the same team may result in disqualification.

Cyber Maryland Conference

- October 29-30, 2014 @ Baltimore Convention Center
  - Runs simultaneously with the Maryland Cyber Challenge
  - Access included in your Challenge registration
- Two Days of technical and non-technical conference sessions appealing to a wide range of audiences, industries, and expertise
- Exhibitor Fair
- Employer & Professional Networking Opportunities



Cyber Operations Key Skills

- Maintain critical services even during moments of intrusion and misuse
- Identify vulnerabilities and lock down systems (computers, network and security devices)
- Recognize and respond to hacker and computer misuse activity (Monitor and Forensics)
- Collect and Analyze Forensics Data
- Penetration Testing
- Communicate Effectively

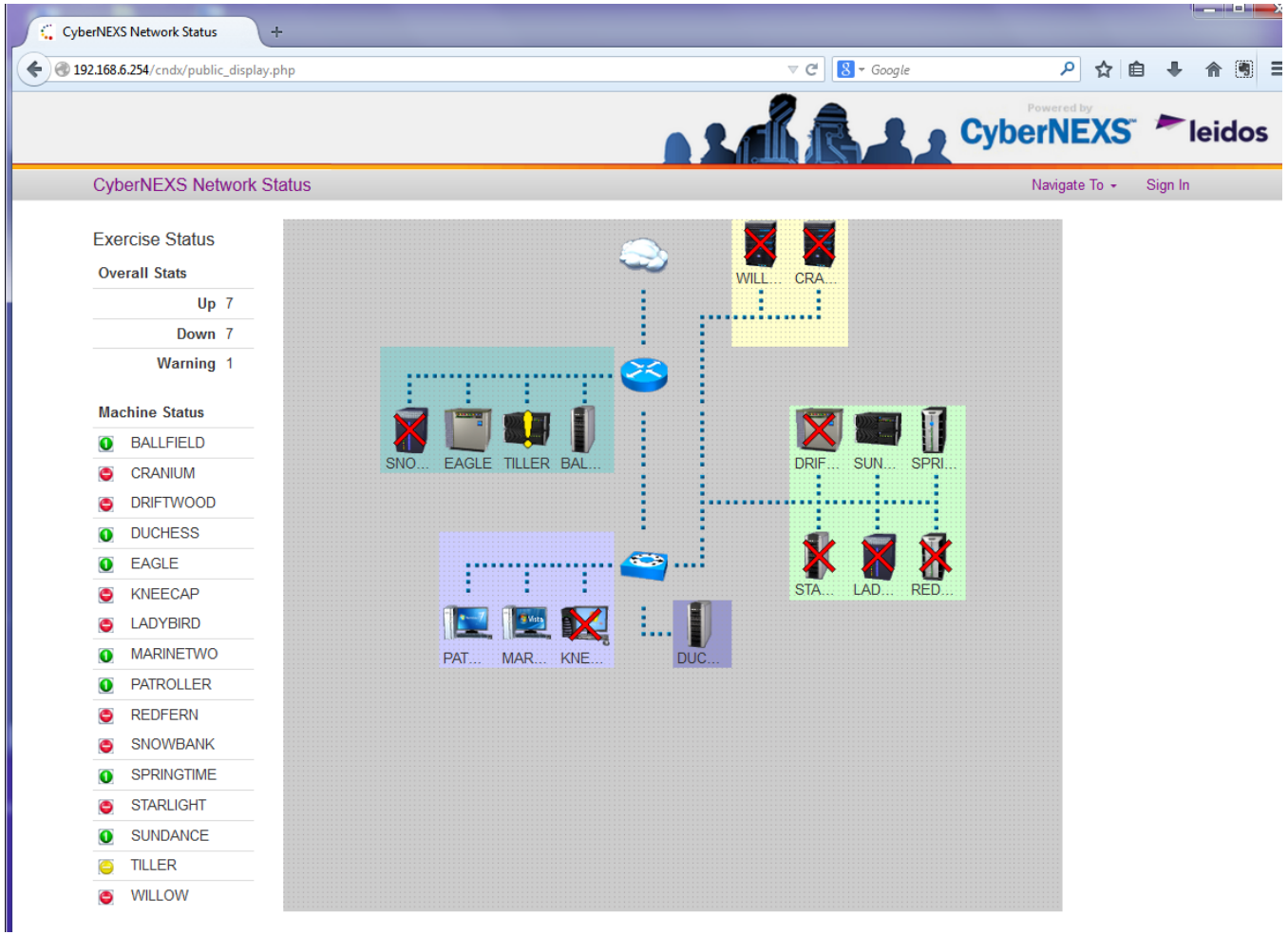
Realistically Train as you expect to Operate

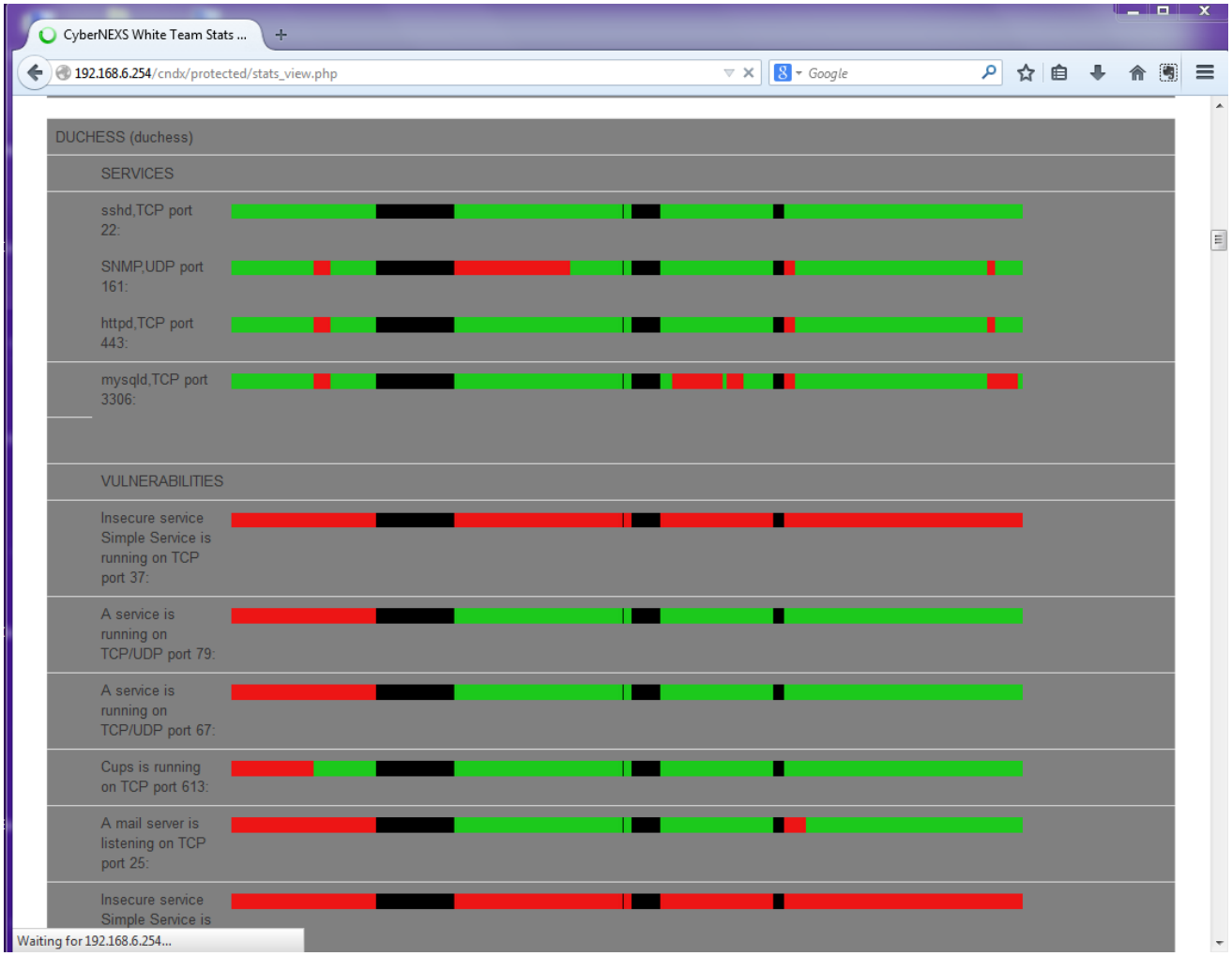
CyberNEXS: The Environment

leidos

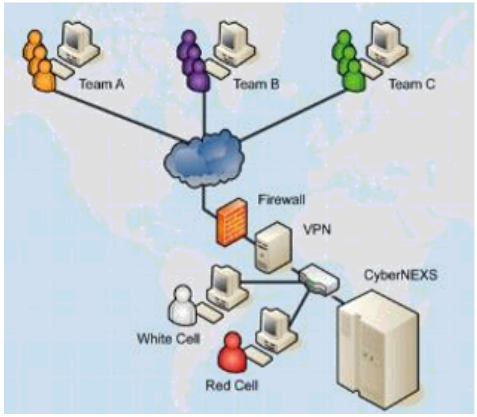
- Instruct – Classroom Instruction
  - Learning of facts
  - Question and answers
  - Instructor demonstrations
- Exercise – Live Lab
  - Reinforcement of learning
  - Student hands-on
  - Trail and error with real-time feedback
- **Compete – Game**
  - **Measure individual or team**
  - **Learn new techniques from others**
  - **Fun; stimulus to learn more**
- Certify – Demonstrate Practical Knowledge
  - Final verification of level of capability
  - Certified under pressure

MARYLAND CYBER CHALLENGE




CyberNEXS White Team Stats ...
192.168.6.254/cndx/protected/stats_view.php
Google
DUCHESS (duchess)
SERVICES
sshd,TCP port 22:
SNMP,UDP port 161:
httpd,TCP port 443:
mysqld,TCP port 3306:
VULNERABILITIES
Insecure service Simple Service is running on TCP port 37:
A service is running on TCP/UDP port 79:
A service is running on TCP/UDP port 67:
Cups is running on TCP port 613:
A mail server is listening on TCP port 25:
Insecure service Simple Service is
Waiting for 192.168.6.254...

Qualification Round 1



Contestant Computer Requirements

- 2GB RAM
- 20GB Disk Space
- VMware Player (free)
- Internet Connectivity Requirements
  - 64Kbps up/down link
  - No latency requirements

Characteristics

- For all Divisions
- 6 **contiguous** hours once connected to complete the round
- Prior to the round, contestant downloads VM target to their own machine.
- Decryption key sent ~15 minutes prior to the start of the round
- Following system registration instructions is crucial!
- Contestant maintains critical services on own machine & conducts system hardening
- Agent sends status to CyberNEXS Global Services which returns score to Contestant's Status Page

Qualification Round 2
High School

Contestant Computer Requirements

- 2GB RAM
- 20GB Disk Space
- VMware Player (free)
- Internet Connectivity Requirements
  - 64Kbps up/down link
  - No latency requirements

Characteristics

- 6 **contiguous** hours once connected to complete the round
- Before the round, contestant downloads VM target to their own machine
- Decryption key sent ~15 minutes prior to the start of the round
- Following system registration instructions is crucial!
- Contestant maintains critical services on own machine & conducts hardening.
- Agent sends status to CyberNEXS Global Services which returns score to Contestant's Status Page

Qualification Round 2
College & Professional

Contestant Computer Requirements

- 2GB RAM
- 20GB Disk Space
- VMware Player (free)
- Internet Connectivity Requirements
  - 64Kbps up/down link
  - No latency requirements

Characteristics

- 6 **contiguous** hours to complete during the round once connected
- Prior to the round, contestant downloads VM target and instructions to their own machine.
- Decryption key sent ~15 minutes prior to the start of the round
- Following system registration instructions is crucial!
- Contestants conduct forensics analysis and report their findings to the White Team.
- Agent sends status to CyberNEXS Global Services which returns score to Contestant's Status Page

Finals (in-person)
High School

- Teams log into their own CyberNEXS network
- Contestants harden systems in their network, maintain critical services and fill out trouble tickets, while Red Team attacks their network
- Contestant Computers will be supplied
- Understanding of Remote Desktop (Windows) and ssh (Linux) software is required along with system admin & security skills.
- No electronic media/devices
- Books & paper notes OK
- No staged internet sites or outside tools
- No coaching

Finals
College and Professional

- Teams log into their own CyberNEXS network
- Contestants identify and compromise targets, then plant flags
- Contestants harden systems in their network, maintain critical services and protect their systems (and those they 'own' by planting flags) while other teams try to attack
- Contestant Computers will be supplied
- Understanding of Remote Desktop (Windows) and ssh (Linux) software is required, along with system admin & security skills.
- No electronic media/devices
- Books & paper notes OK
- No staged internet sites or outside tools
- No coaching

Points of Contact

Competition Director: Dr. Richard Forno (UMBC)

Richard.forno@umbc.edu

Competition Questions & GamePlay:

Richard.forno@umbc.edu

Competition Technical Support:

cybernexs@leidos.com

CyberNEXS Program Manager: Susan Crowe

Susan.m.crowe@leidos.com

MDC3 Event Publicity: Devaney & Associates

410-296-0200

www.marylandcyberchallenge.com