Clearing the Tall Poles

12 Week High School Cyber Defense eLearning Pilot

Duke Ayers, CyberNEXS Program Manager

June 2012

SAIC
From Science to Solutions

Cyber Security Training: Awareness vs. STEM

Awareness – Learning to protect one self

STEM* – Learning to protect others and entry into the professional workforce

**Science, Technology, Engineering & Mathematics*

Keys Points to Remember

1. First Time Event
2. Using real Windows systems with real-time feedback
3. The Students will gain knowledge
4. The Teachers/Mentors are not being graded
5. Overall results will be anonymous in Final Report
6. Teacher/Mentor feedback is crucial
7. Kids will have fun with practical exercise

STEM Shortfalls

- **Curriculum**
  - Classroom Instruction
  - Practical Lab
  - Exercise/Competition
  - Certification Standard

- **Technology**
  - Live, real-world training system, available via internet
  - Self-contained for student experimentation and live exploits
  - Highly scalable to train large numbers
  - Highly configurable for immediate and constant reuse
  - Exercise complexity to fit level of student

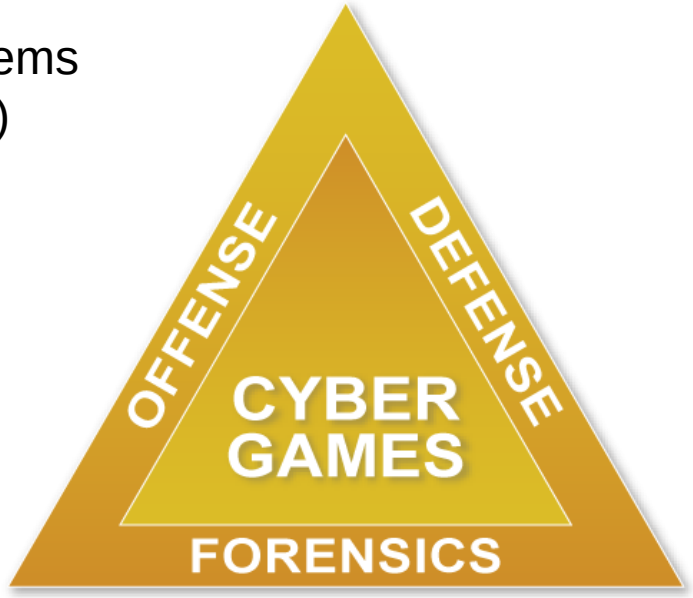
- **Tools**
  - Teacher's Guide
  - Student's Manual
  - Automated lab processes
  - Real-time feedback and displays to show status, trends and scores

- **Trainers**
  - Qualified local educator
  - Volunteer on-site mentors
  - Train-the-trainer support
  - Help Desk
  - On-line training tools

Cyber Operations Key Skills

Realistically Train as you expect to Operate

1. Maintain critical services even during moments of intrusion and misuse
2. Identify vulnerabilities and lock down systems (computers, network and security devices)
3. Recognize and respond to hacker and computer misuse activity (Monitor and Forensics)
4. Collect & Analyze Forensics Data
5. Penetration Testing
6. Communicate effectively



Cyber Security Training Life Cycle

Instruct – Classroom Instruction

- Learning of facts
- Question and answers
- Instructor Demonstrations

Exercise – Live Lab

- Reinforcement of learning
- Student Hands-on
- Trial-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

- Performance-based test
- Final verification of level of capability
- Certified under pressure

CyberNEXS™™ is part of the SAIC System Administrator Security Training Curriculum CNSS 4013 Certification

Purpose of the Pilot

1. Demonstrate the scalability and effectiveness of training using an internet-based trainer across multiple time zones
2. Empower local educator through Train-the-Trainer and on-line tools
3. Weekly measurement of student and instructor progress throughout Pilot
4. Gather student and instructor feedback
5. Produce Final Report

Bottom-Line Requirements

- Classroom – Empower Local Educator
- Student Convenience:
  - Distance Learning (virtual)
  - 7X24
- Real-World, Live Systems
- Instruction and Practice
- Timely feedback
- Fun

Internet-based HS Curriculum Pilot

Week of	Monday	Tuesday	Wednesday	Thursday	Friday
	1-2 weeks prior to commencement of Pilot		SAIC provides 2 hour pre-Pilot training to teachers via internet		
19-Sep-11	Each student takes the 2-Hr on-line Entrance Exam monitored by Teacher (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 1) to Schools via Internet
26-Sep-11	Teachers deliver Module 1 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 2) to Schools via Internet
3-Oct-11	Teachers deliver Module 2 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 3) to Schools via Internet
10-Oct-11	Teachers deliver Module 3 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 4) to Schools via Internet
17-Oct-11	Teachers deliver Module 4 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 5) to Schools via Internet
24-Oct-11	Teachers deliver Module 5 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 6) to Schools via Internet
31-Oct-11	Teachers deliver Module 6 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 7) to Schools via Internet
7-Nov-11	Teachers deliver Module 7 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 8) to Schools via Internet
14-Nov-11	Teachers deliver Module 8 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 9) to Schools via Internet
21-Nov-11	Teachers deliver Module 9 instruction to Students, who then exercise on-line (Mon-Thurs)				SAIC provides 2 hour train-the-trainer instruction (Module 10) to Schools via Internet
28-Nov-11	Teachers deliver Module 10 instruction to Students, who then exercise on-line (Mon-Thurs)				Teacher deliver individual feedback to SAIC for the Final Pilot Report
5-Dec-11	Each student takes the 2-Hr on-line Exit Exam monitored by Teacher (Mon-Thurs)				

SAIC From Science to Solutions

25 Schools participated

1. Global Institute for Cybersecurity & Research (GISCR), Florida
2. Arts and Technology Centre, Manitoba, Canada
3. LA Unified School District
4. State of Hawaii
5. Huntsville, AL

Teacher/Mentor Tools

1. Curriculum
   - Presentation Slides with Speaker's Notes
   - Practical Lab Slides
     - Objectives
     - Activities
     - Quiz(s)
2. Train-the-Trainer Videos
3. CyberNEXS™ on-line Training Environment
4. Manuals
   - Introductory Letter
   - User's Guide
   - Teacher/Mentor Guide
   - Security Concerns and Technical Considerations
5. Views of Scores
6. Other tools: www.saic.com/cybernexs

12 Week, 10 Module High School Pilot Curriculum

I. Overview, Entrance exam
II. Windows Basics , Qualify statement (include computer component definition)
III. Windows Networking
IV. Accounts Basics
V. Threats and Vulnerabilities
VI. Threats and Vulnerabilities /Patching
VII. DNS, Routes, Workgroups/Domain/
VIII. Services/DR/shadow copies
IX. Authentication/Access Controls/basic crypto
X. Servers -File Server
XI. Locking down Servers with utilities -add on utilities
XII. Review, re-take Entrance exam

Measures of Effectiveness

Quantitative

1. Difference between Entrance and Exit Assessments
2. Trend of Student Weekly Scores
3. Numerical Results of Instructor Surveys
4. Module scores as a whole
5. Numbers of Registrations per week

Qualitative

1. Did you learn something?
2. Did you find the instruction material of value?
3. Did you find the Labs to be of value?
4. Did you have fun?

Mid-Term Results

Over the first five modules, we have documented the following statistics:

- 52 Teachers/Regional Directors registered for individual accounts to view the real-time lab progress of their respective student population.
- Upwards of 140 students from 31 schools participated in the weekly labs.
- Week 1 Entrance Exam results for 212 participants:
  - Low score = zero; high = 77%; Ave = 27.6%; Median = 16.6%
  - Half the participants scored no higher than 11%
- During weeks 2-5, the quiz results were quite encouraging. Each week, there was an average of 105 students participating; the overall average score was 81%, 82%, 85%, 77%, respectively.

Weekly Downloads

- Week 4: Accounts Basics (October 7, 2011)
  Lesson 4:
  - Lesson 4 Presentation (.avi movie format) 124 MB
  - Lesson 4 Presentation (.mp4 movie format) 29 MB
  - Lesson 4 Presentation (Windows Media Player format) 28 MB
  - Lesson 4 Presentation (.PPT format) ** no audio **
  - Lesson 4 Online Presentation

  Lab 4:
  - Lab 4 Presentation (.PPT format)
- Week 5: Threats and Vulnerabilities (October 14, 2011)
  Lesson 5:
  - Lesson 5 Presentation (.avi movie format) 777 MB
  - Lesson 5 Presentation (Windows Media Player format) 46 MB
  - Lesson 5 Presentation (.PPT format) ** no audio **
  - Lesson 5 Online Presentation

  Lab 5:
  - Lab 5 Presentation (.PPT format)

Teacher Input

Some observations and comments, Deborah Kula, Sacred Hearts Academy
Dec. 2011

First and foremost, we are extremely appreciative for the opportunity to participate in this program. I remained amazed at the volume and quality of the content and presentations and labs and quizzes and the thought that has gone into organizing and structuring the program. It is wonderful that this opportunity is being afforded to high school students. The experience has definitely had a positive impact on my students.

I really appreciated the technical and moral support offered along the way. Your positive energy helped us through the maze.

The biggest challenge for us was the length of each lesson. Our consensus is that shorter lessons with additional lab opportunities would be more effective. While we could pause the video and discuss or research a topic further, we did not attempt the lab exercises until the entire lesson had been covered.

A direct result of the students participating in this program has been increased interest in campus and other students asking if they can take the course next year.

Aloha,
Deborah

Weekly Quiz Results by Region & Module

On Average, 90 students participated weekly

	Windows Basics	Windows Networking	Accounts Basics	Threats & Vuls	Threats & Vuls - Patching	DNS, Routes, Workgroups	Services, DR, shadow copies	Auth/Access, crypto	Servers-File server	Hardening Servers	
Region One	82	92	89	86	97	50	96	83	94	81	85.0
Region Two	80	78	84	71	82	59	82	88	97	78	79.9
Region Three	83	85	87	77	90	76	89	90	100	85	86.2
Region Four	85	79	83	79	86	57	80	90	96	79	81.4
Region Five	76	84	87	73	85	74	89	78	83	88	81.7
	81.2	83.6	86	77.2	88	63.2	87.2	85.8	94	82.2	**82.8**

10 Week Score Average for all Exercises = 82.8%
Regional Averages ranged from 79.9 – 85%

SAIC From Science to Solutions

Student Feedback

Student 1

The CyberNEXS Pilot program was extremely helpful in preparing for the CyberPatriot competition as well as learning basic security. They covered general policies for security as well as very specific ways to make your computer more secure. The quizes were helpful in recalling the important points of the lessons covered and the labs allowed us to practice and experience the material hands on. The only thing that I think could use improvement would be possibly breaking up the lessons with the different parts of the lab because it is sometimes a lot of information to digest. Covering one topic at a time then learning how to do it in the lab would be easier to understand and remember.

Student 4

The lessons were very informational. However, I believe that shorter lessons would be better. Many people get tired after listening to one person talk for quite a long time. The powerpoints were informational as well, but they were very long and it took time to get through the entire powerpoint. **The labs, on the other hand, was interesting. It taught me new things about computers and security. It was also a good experience to do apply everything I have learned to secure the image.** The quizzes that were incorporated within the lab is good because it causes me to think and remember what I have learned from the lesson. While doing some of the quizzes, I had to research some information, which allowed me to memorize it better for future references.

Lessons Learned

Negative:

- Curriculum pace was overly aggressive; lectures were too long
- Difficult coordinating meeting times when considered extra-curricula
- Download of large images required too much time
- Few used images outside the classroom
- Declining numbers
- Some indicated lack of resources (internet, computers, etc.)

Positive:

- Students grasped the instruction material
- Videos proved effective supplanting need for train-the-trainer sessions
- Overall weekly exercise scores averaged 82.8%; least was 79.9%
- Normalized Entrance/Exit exams demonstrated significant gain of knowledge
- All MOEs measured with majority of results as positive
- Good feedback; both surveys and personal notes reflect positive experience
- Right mix of content

On-Line Survey Results

1. How many students in your class? *136 total; 2-45 range; 13.6 mean; 7.5 median*
2. What days/time of day do you provide student instruction? *No pattern*
3. How much time are the students spending reviewing the lesson and working on the labs? *1-6 hrs range; 3.3 hrs mean*
4. Do you have all the tools you need to conduct the class? *10 yes; 1 no*
5. What were the biggest hurdles you had to overcome?
   - *Large downloads*
   - *Resource limitations (internet and computers)*
   - *Coordination of meeting times*
6. What method of instruction do you primarily use? *8 both; 3 various*
7. Do your students take the weekly on-line quizzes? *Most say yes*
8. Do your students work on the VMware images form outside of school? *4 yes; 7 no*
9. Are the students interested and engaged with the CyberNEXS™ Pilot Program? Are they having fun? *9 yes; 1 no; 1 no comment*

On-Line Survey Results (continued)

10. Are the students gaining knowledge? *10 yes; 1 not much*
11. What do you think of the videos? *8 positive; 2 negative; 1 not noted*
12. How many times do you watch the videos per week? *Average 1-2 times per week*
13. What video format works best for you? *2 streamed from site; others mix wmv and avi*
14. Do you attend the weekly on-line train-the-trainer sessions? If not, why? *4 attended; most had scheduling conflicts*
15. If you do attend the sessions, does it help you with your instruction? *Most who attended found it positive*
16. What do you think of the content of the course? *8 right mix; 2 too hard; 1 not technical*
17. How would you grade the CyberNEXS™ Pilot (1-10)? Average 7.7; Media 8
18. Other comments? *Lectures too long*

STEM Outreach

CyberNEXS: INSTRUCT, EXERCISE, COMPETE, CERTIFY

CyberPatriot: National High School Cyber Defense Competition

MARYLAND CYBER CHALLENGE & CONFERENCE MDC3

Utah Cyber Defense Challenge & Symposium

SAN DIEGO MAYOR'S CYBER CUP

GLOBAL CYBERLYMPICS

WOUNDED WARRIOR PROJECT

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

USCC US CYBER CHALLENGE

CYBER SECURITY CHALLENGE.ORG.UK

CyberNEXS™ Experience

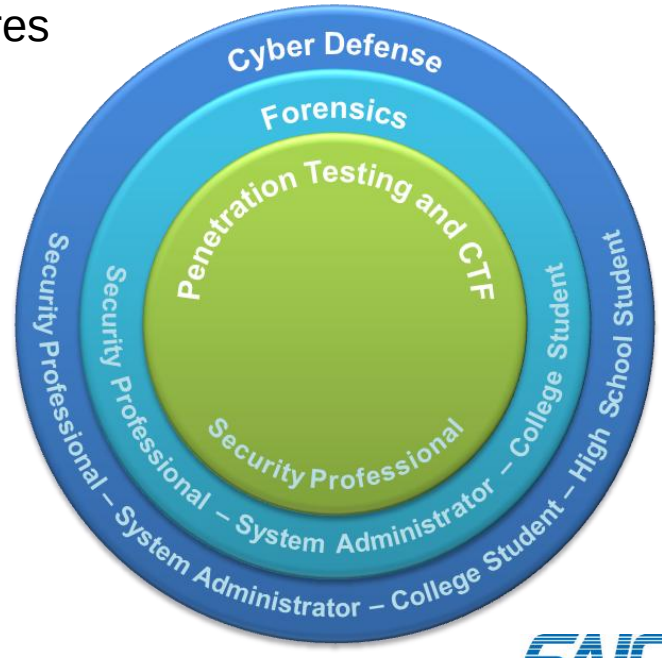
- Competed 7 years DefCon CTF (2 time winner)
- 100+ Training and Competition Events
- Mid-High School
  - AFA National High School Cyber Defense Competition: Cyber Patriot I,II,III, & IV
  - NDIA Cyber Challenge
  - San Diego Mayor's Cyber Cup I, II
  - State of Maine HS Cyber Defense Challenge I - II
  - Thomas Jefferson HS tjSTARS
- Collegiate
  - Mid-West Regional Cyber Defense Competition
  - Mid-Atlantic Regional Cyber Defense Competition
  - Navy Post-Graduate School
  - National Collegiate Cyber Defense Competition
- Adult
  - EUCOM, Joint and Coalition Forces
  - University of California
  - Sempra
  - Canadian Forces School of Communications and Electronics
  - NCIS, FIWC, JITC/ACOMS, JITC, TRANSCOM
  - Naval Supply CISO, 23rd IOS/AFIWC, FBI RCFL, NMCI Det
  - FIRST – Singapore, ToorCon, HTCIA, ISSA
- License Sales
  - 711th USAF Human Performance Wing
  - 175th USAF Network Warfare Squadron
  - 177th USAF Information Aggressor Squadron
  - University of Maryland University College

Energy | Environment | National Security | Health | Critical Infrastructure

SAIC From Science to Solutions

Cyber Security Trainer Requirements

- Self-contained; never touches operational environment
- Emulates student's operational environment using standard Windows®, UNIX®, network management interface and network/security devices
- Realistic, live environment with real-time, automated, quantitative scoring
- Complexity to the student level (middle school to professional)
- Outbrief capability showing status, trends and scores
- Ability to rerun same scenario
- Available anytime-anywhere
- Scale to large numbers
- Automation for ease of use
- Used in every phase of the Life Cycle
- Cost Effective



Windows is a registered trademark of Microsoft Corporation in the U.S. and/or other countries.
UNIX is a registered trademark of x/Open Company in the U.S. and/or other countries.
VLAN = virtual large area network
IDS = Intrusion Detection System
VMware is a registered trademark of VMware, Inc. in the U.S. and/or other countries.

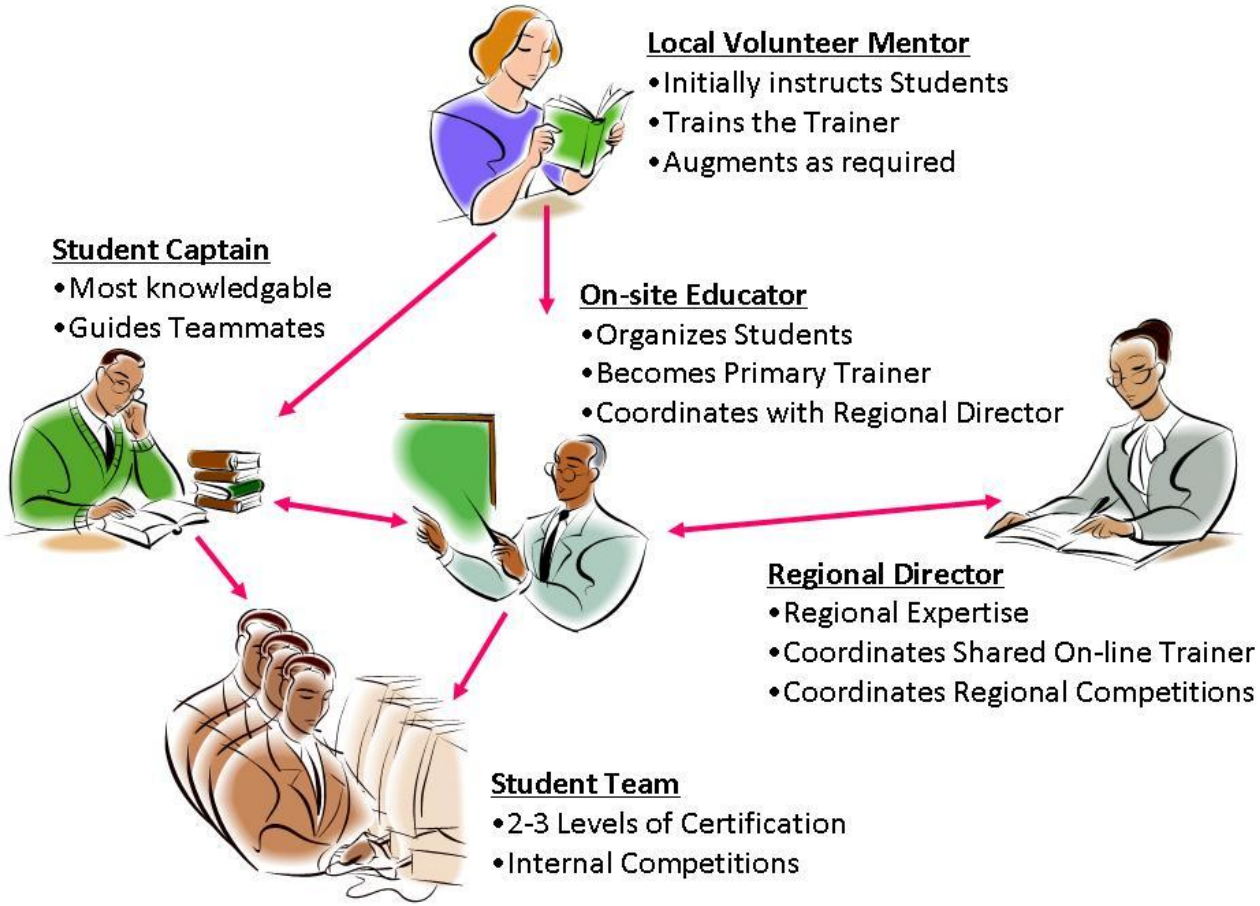
Preparation for the Pilot

1. Establish MOU between SAIC and the major organizational groups (named later)
2. Organizations identify schools/clubs to participate
3. Organizations identify local educator/mentor for each school/club to deliver training and guide students for on-line exercising
4. Local educators identify computer and internet resources sufficient for use by students
5. Local educator identify student leader to aid in mentoring of teammates
6. SAIC provides on-line training for the local educators
   - Overview of Curriculum contents
   - Use of on-line training system

Conduct of the 12 Week Pilot

1. Pilot starts week of 19 Sep; ends week of 5 Dec.
2. 1st and 12th week will be exams to first baseline knowledge and then determine degree of learning
3. Weeks 2-11 will be conducted as follows:
    1. SAIC provide on-line presentation of the next week's instruction to mentors/teachers on Fridays: 11:00 AM -1:00 PM Pacific
    2. Monday-Thursday each week:
        1. Mentor/teacher provides classroom instruction for approx. 1.5 hours
        2. Students conduct hand's-on exercising

Sample Organization



Local Volunteer Mentor
- Initially instructs Students
- Trains the Trainer
- Augments as required

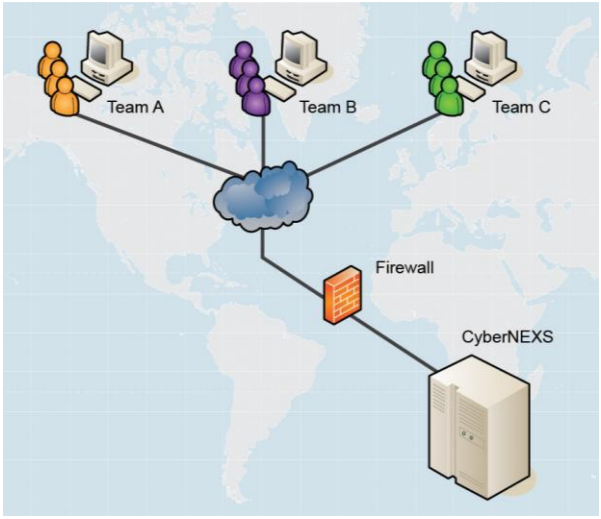
Student Captain
- Most knowledgable
- Guides Teammates

On-site Educator
- Organizes Students
- Becomes Primary Trainer
- Coordinates with Regional Director

Regional Director
- Regional Expertise
- Coordinates Shared On-line Trainer
- Coordinates Regional Competitions

Student Team
- 2-3 Levels of Certification
- Internal Competitions

Distributed Game (CND Lite)

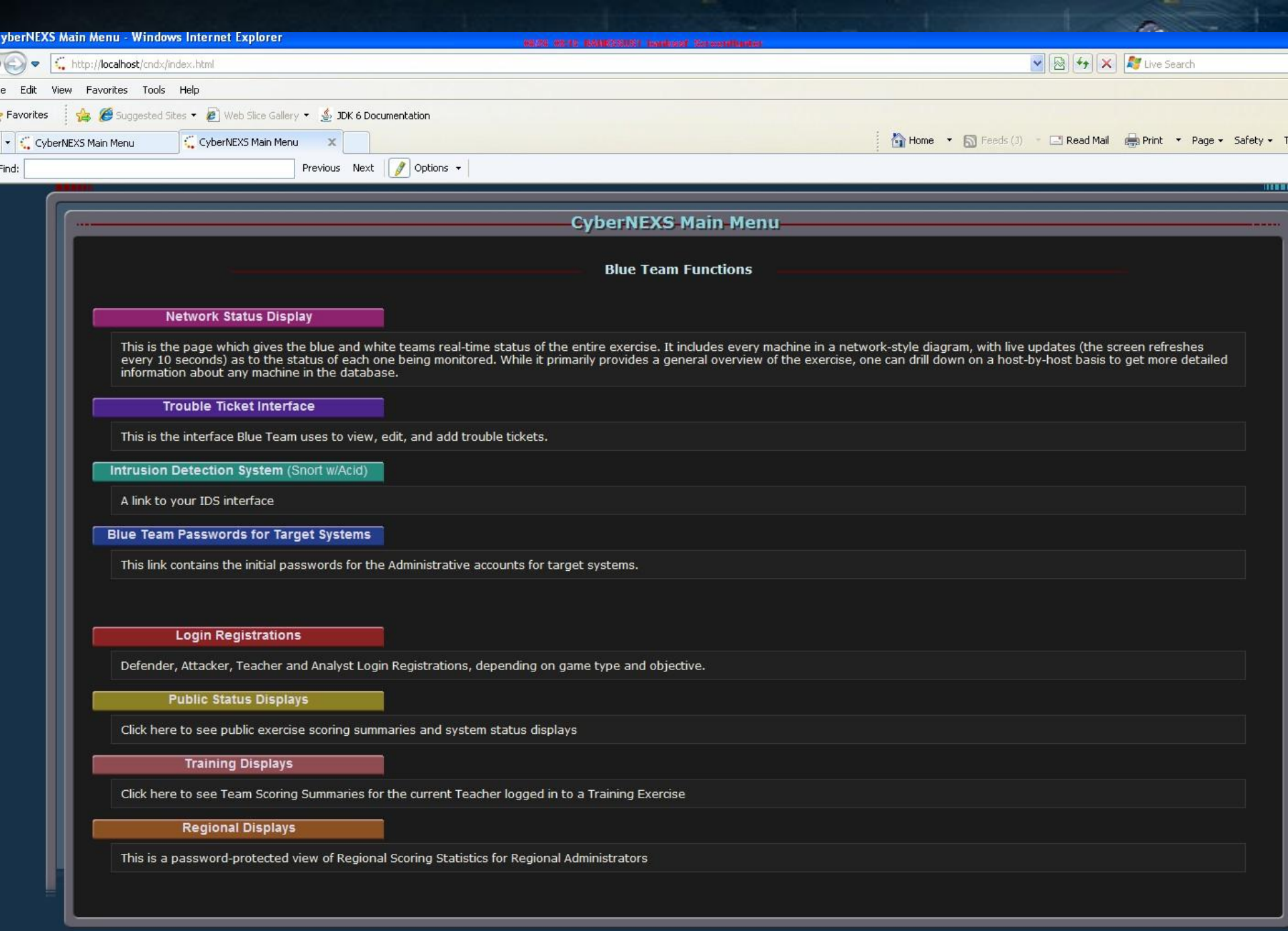


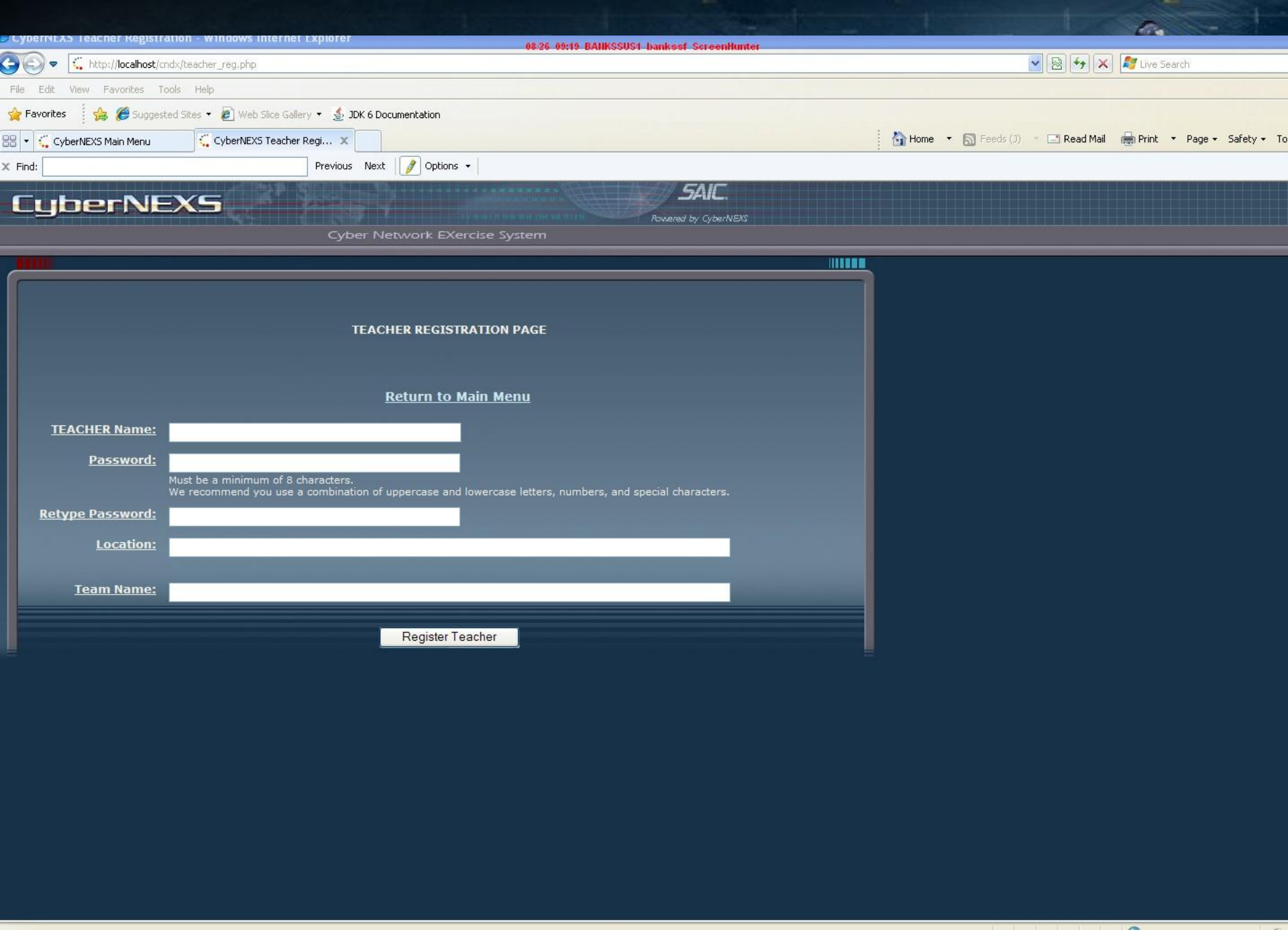
Characteristics

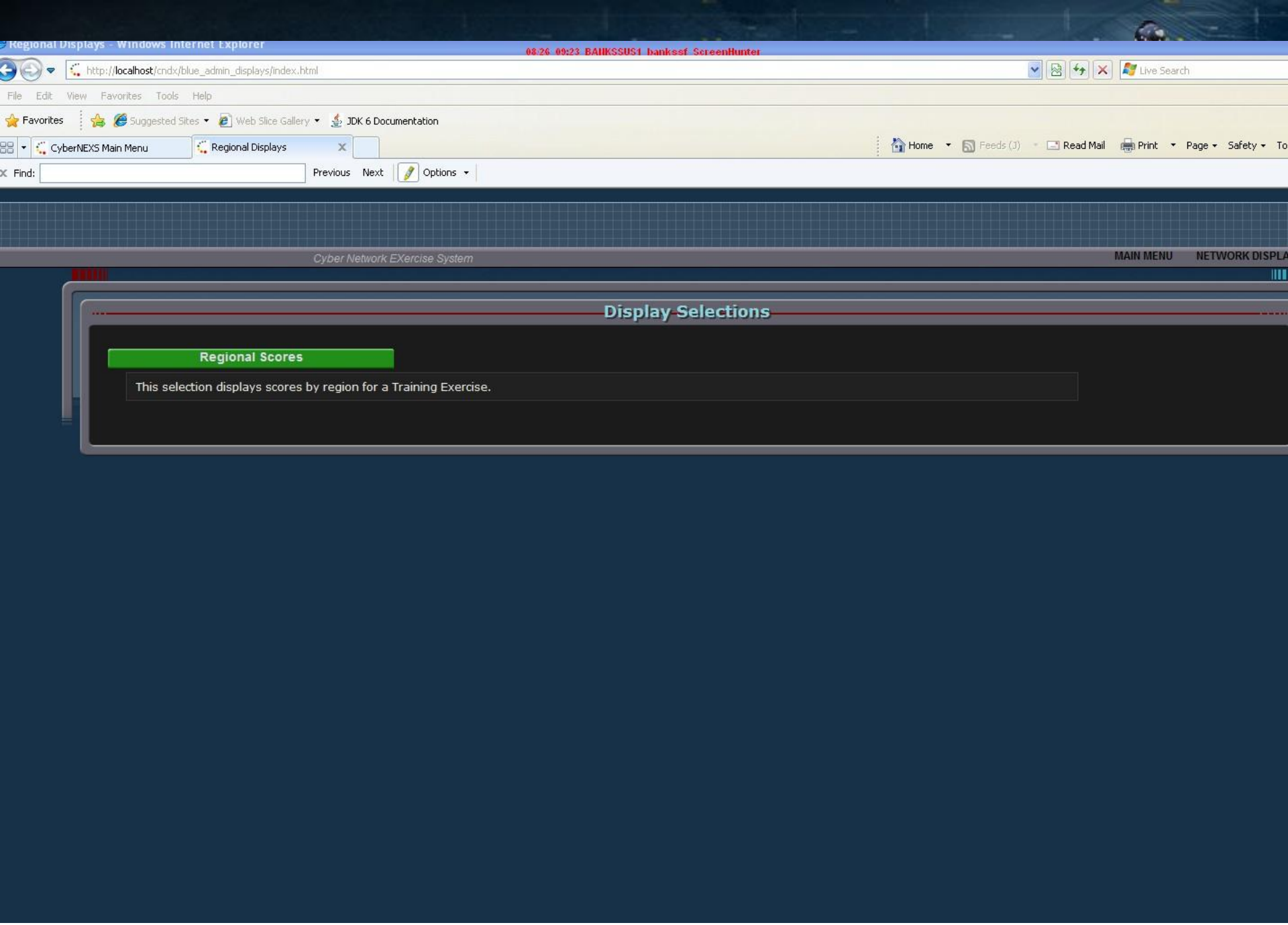
- Contestant downloads and hardens target on own machine
- Contestant maintains critical services on own machine
- Agent sends status to CyberNEXS™ Global Services which returns score to Contestant's Status Page
- No attacks nor trouble ticket activity performed (no red/white team required)
- Highly scalable

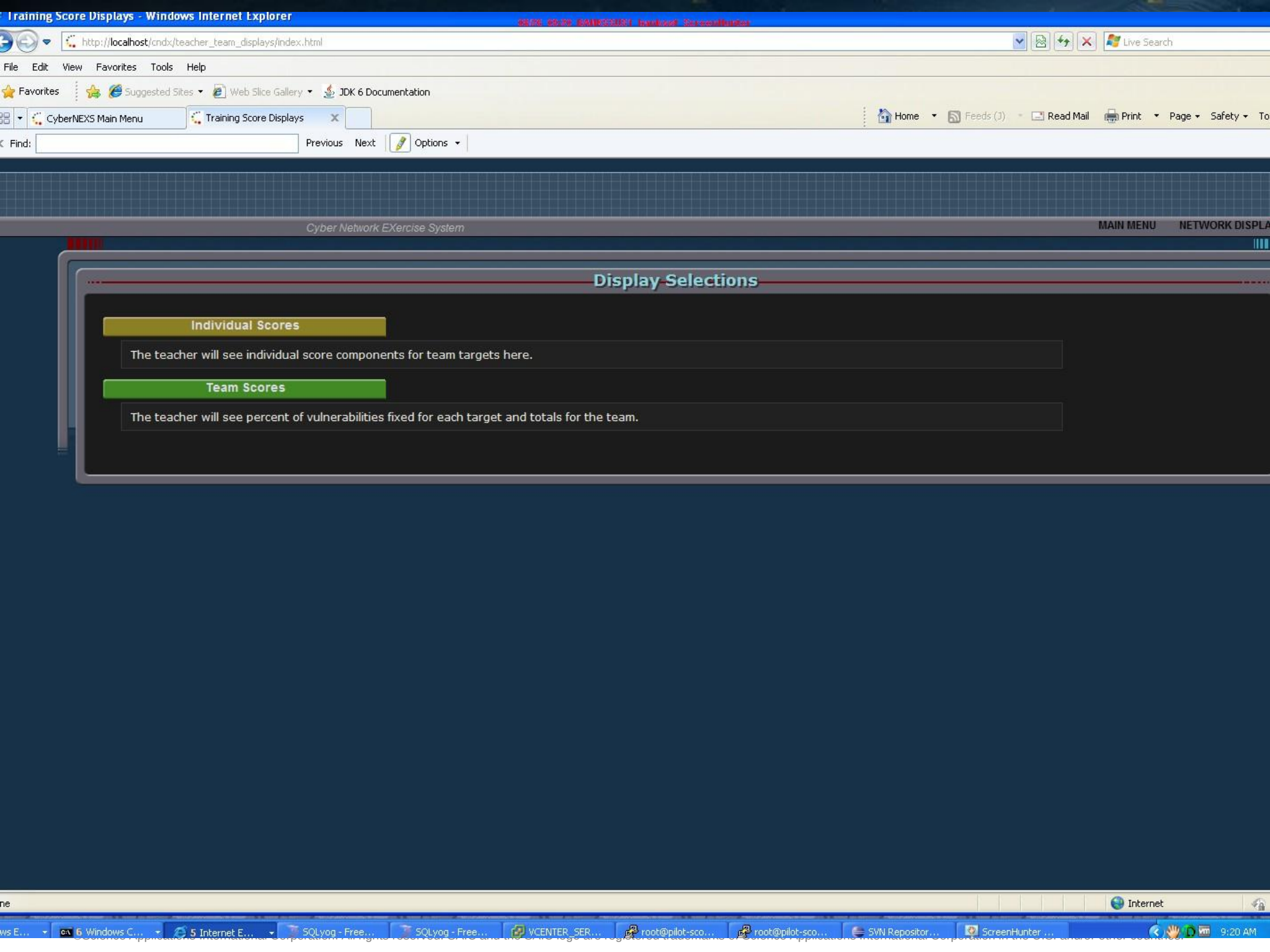
Lessons Learned

- Contestant's computer requires 2GB RAM & 20 GB Disk Space
- Contestant's internet connectivity requires 64Kbps up/down link, with no latency requirements
- Minimal software requirements, but must use versions prescribed
- Load balancing technology required for larger scales
- Invaluable technique for large scale, routine exercises and competitions








Training Score Displays - Windows Internet Explorer
http://localhost/cndx/teacher_team_displays/index.html
Live Search
File Edit View Favorites Tools Help
Favorites
Suggested Sites
Web Slice Gallery
JDK 6 Documentation
CyberNEXS Main Menu
Training Score Displays
Home
Feeds (J)
Read Mail
Print
Page
Safety
Find:
Previous
Next
Options
Cyber Network EXercise System
MAIN MENU
NETWORK DISPLA
Display Selections
Individual Scores
The teacher will see individual score components for team targets here.
Team Scores
The teacher will see percent of vulnerabilities fixed for each target and totals for the team.
Internet
9:20 AM