Providing "real-world" experiences to Cyber Security Students

The Problem

- Education and certification are often insufficient for students seeking work in the field after graduation as the majority of cyber security positions require some experience.
- Traditional internship opportunities are not feasible for many cyber security students – especially those in community college programs

Possible Solutions

- Capstone projects that allow student teams to perform security assessments/follow-up hardening activities for businesses

NVCC – ITN 293 - Capstone

- Semester-long team project, assessing security posture for a college partner business
  - Students sign NDAs
  - Students run Nessus scans (both internal and external), do wireless scans with NetStumbler
  - Limited social engineering activities performed (dumpster diving)
  - Findings and recommendations are presented in front of the client and a Board

NVCC – Community PC Cleanup

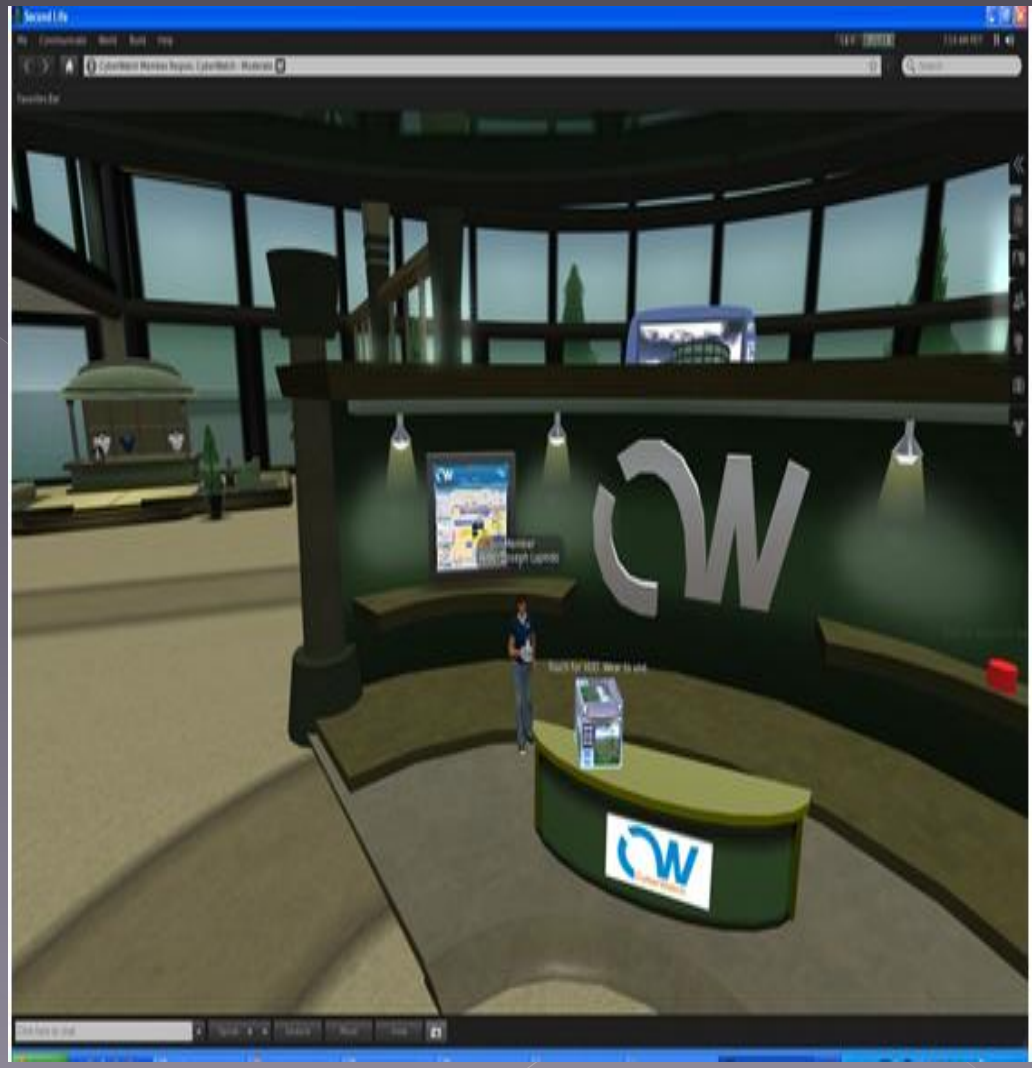
- Advertise for local residents to bring PCs into NVCC to have students clean them up from viruses and spyware
- Done in conjunction with A+ classes to also provide troubleshooting (hard disk defragmentation) services.

Proposed Expansion

- Develop student-led Security Center
- Provide security assessment and hardening services for small businesses and non-profit organizations
- Students develop security documentation (Incident Response, Contingency Plans, System Security Plans, etc.)
- Funding to support background checks
- Coordination with Legal offices a must

Cyber Watch Second Life Resources

- Cyber Watch Second Life Island - simulated security assessments (exercises relative to CNSS 4012 and, eventually, 4013)



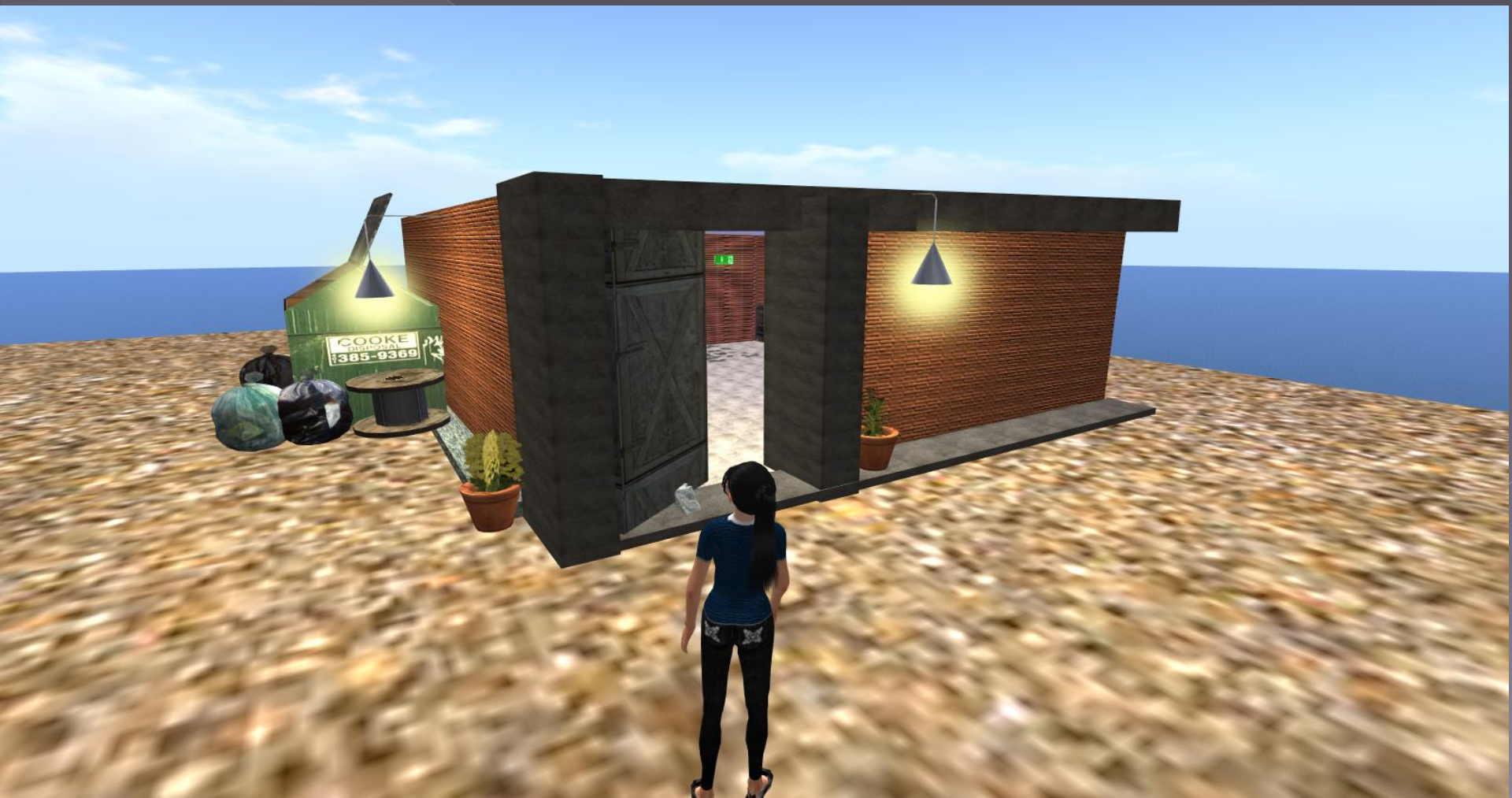
Audit Instrument

Exercise 1 VoIP Audit

Scenario: You are a security analyst and have been asked to perform a security audit for a University that has just installed a VoIP that will eventually replace the existing PBX. Since there are several team members, you have been provided only a small segment of items to check out. Using the audit checklist provided below, and the DISA VoIP Checklist, visit the facility in Second Life and complete the audit report, provided below, with your findings. Write up your findings, with your recommendations, in a report for the system owner.

ID	Description/Default Findings	Status (Open, Not a Finding, Not Applicable, Not Reviewed)	Reviewer Comments:
V0008225	**Description:** The IAO will ensure all critical VoIP network and server components are located in a secured area. Controlling physical access to the VoIP network and server components is critical to assuring the reliability of the voice network and service delivery. Documenting or logging physical access to the VoIP network and server components is critical to determine accountability for auditing purposes. **Default Findings:** The following VoIP components are installed in an area that does not have adequate physical security controls applied: List components and locations that are not physically secure (except end instruments): VoIP system servers and/or network components are installed in a locked room, closet, or cabinet, but the distribution of keys to access the equipment is NOT limited, controlled, or documented. A physical access log is not maintained. **Checks:** During a walk through inspection, visually confirm that VoIP network and server components are installed in secured areas to include locked rooms, closets, and/or cabinets. Interview the IAO to determine how the distribution of keys to access the equipment is limited, controlled, and documented. Additionally determine if access control procedures/documentation are/is being used and review the access logs for compliance.		
V0008222	**Description:** LAN Not Enclave and Network STIG compliant. The VoIP system is not compliant with overall network security architecture and appropriate enclave security requirements. The IAO will ensure that the network supporting IPT implementations is configured to comply with the Network Infrastructure and Enclave STIGs, most importantly, packet filtering and monitoring. **Default Findings:** The VoIP system is not compliant with overall network security architecture.		

The Sandbox



Dumpster Diving

Data Center

Data Center


Professor Garnet
Sit Here
Notecard: Firewall Configuration
Description:
Firewall Configuration Information
IP Address: 10.15.116.2
Subnet Mask: 255.255.255.0
Default Gateway: 10.15.116.1
DHCP Server: 10.15.116.3
DNS Servers: 164.25.101.9
164.25.101.10
#access-list 100 extended deny tcp 10.15.0.0 255.255.0
host 10.15.116.15 eq 69
#access-list 100 extended deny tcp 10.15.0.0 255.255.0
host 10.15.116.15 eq 161
#access-list 100 extended deny tcp 10.15.0.0 255.255.0
host 10.15.116.15 eq 162
#access-list 100 extended deny tcp 10.15.0.0 255.255.0
host 10.15.116.15 eq 389
#access-list 100 extended permit tcp 10.15.116.8
host 10.15.116.15 eq 3389
#access-list 100 extended deny tcp 10.15.0.0 255.255.0
host 10.15.116.15 eq 123
Save

Classroom Space

Public Auditorium/Brown Bags

Meeting Space

Planned

- Develop a simulated Security Operations Center (SOC) with sanitized data feeds to train on Incident Response/Signature Analysis
- Integrate classrooms with CyberWatch's Virtual Lab environments for a one-stop training shop

Contact

- Use of the site is free to CyberWatch members, including the sandbox, however registration is required

Contact:

Margaret Leary
mleary@nvcc.edu

Questions