



ISC 互联网安全大会



360 互联网安全中心



SEED Labs: 为计算机安全教育开发的动手实验

杜文亮 教授, 雪城大学 (Syracuse University)

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
(原“中国互联网安全大会”)

《荀子·儒效》

不闻不若闻之，闻之不若见之，
见之不若知之，知之不若行之。
学至于行之而止矣。

I hear and I forget.
I see and I remember.
I do and I understand.

安全教育的状况（2001）

- 重理论，少实验
- 简单的 buffer overflow attack: 半个学期
- 设计一个好的实验很花时间
- 好的实验设计缺乏
- 已有的设计可采纳性很低
- 实验平台一家一个样

其它课程有不少好的实验：操作系统，网络，编译原理

历经16年的研发和测试



SEED Labs: (SEcurity EDucation)

<http://www.cis.syr.edu/~wedu/seed>

- 经费：130万美元（3个NSF项目）
- 35个实验
- 400多页教师手册
- 1本教科书
- 60多个国家约800所高校和高中使用
- 8期培训班
- 不少公司用作内部培训和招聘考题
- NSF给美国国会报告中的模范项目之一

2002年设计的初衷

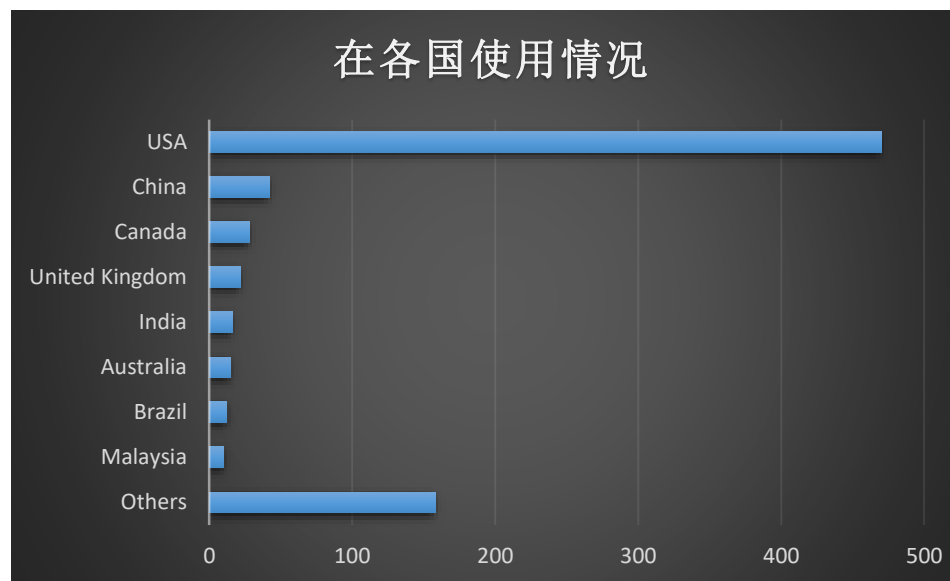
- 开发一系列的动手实验
- 面向计算机安全教育
- 覆盖范围广
- 注重安全的基础和原理，不是产品
- 容易被他人采用
- 搭建实验环境：成本低
- 实验的使用：开源，免费

在世界范围的采用情况

大约800 所学校 (65个国家)



在各国使用情况



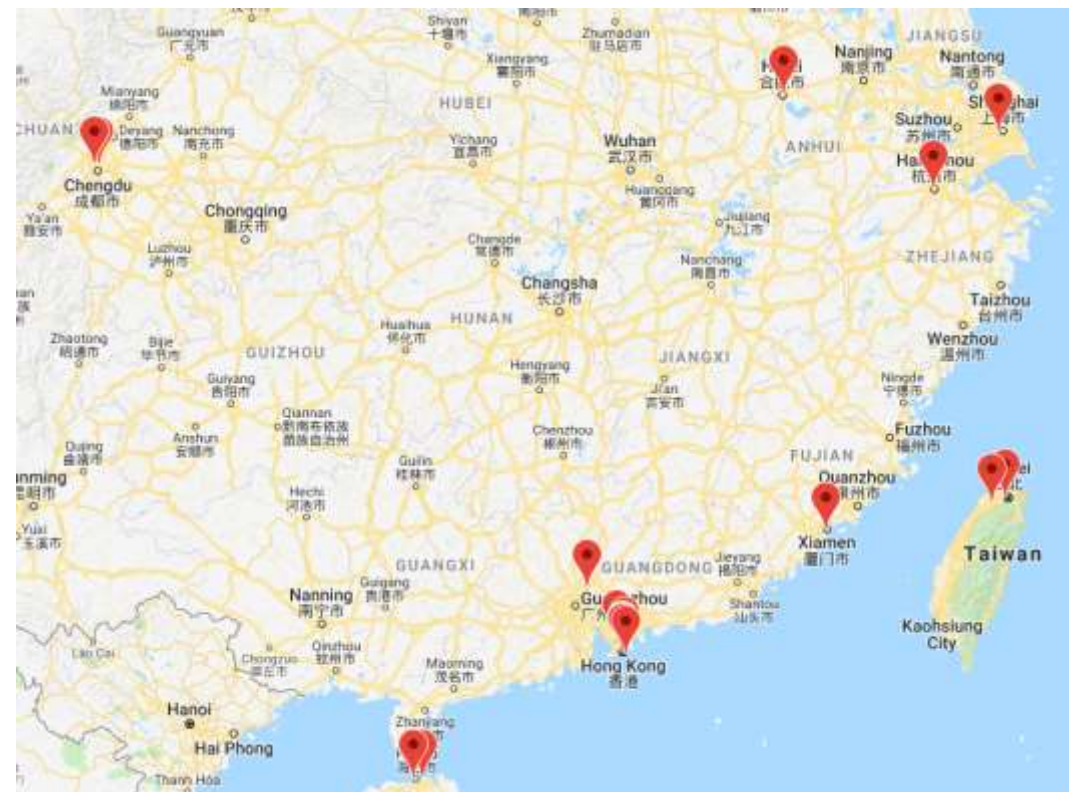
在中国的使用情况



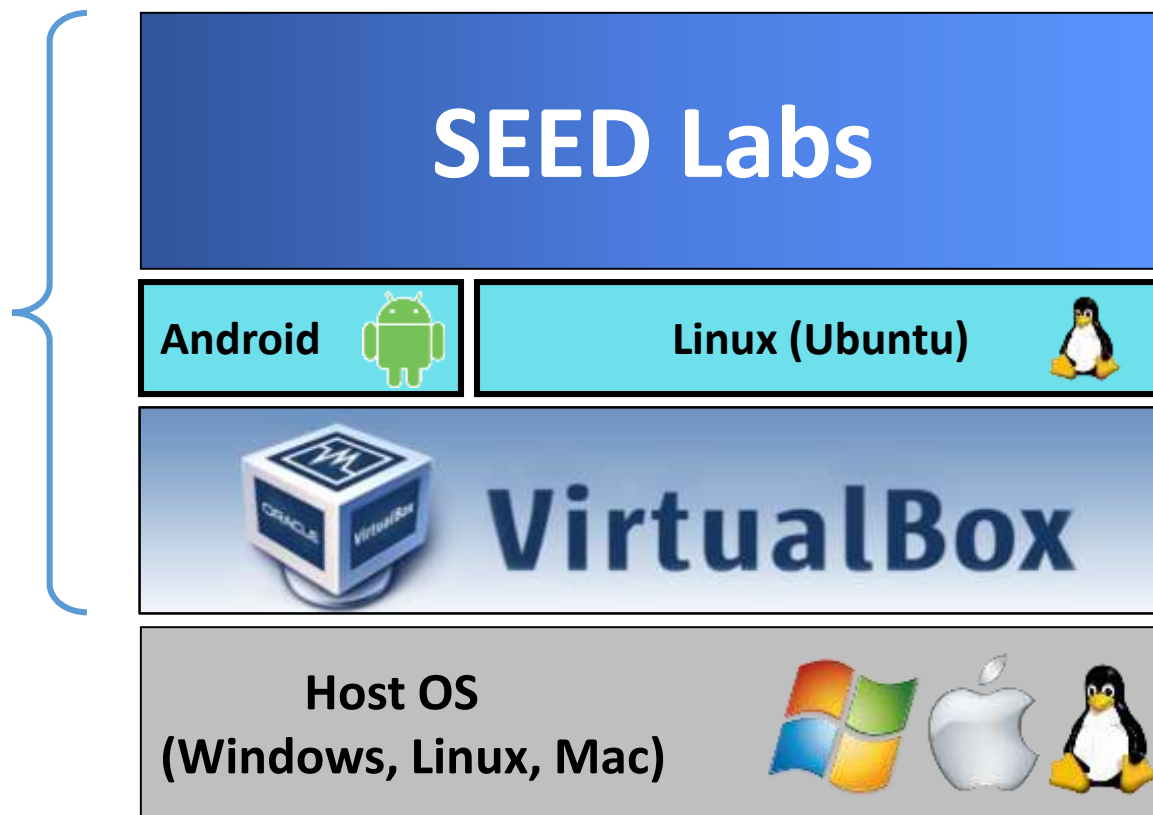
ISC 互联网安全大会



360 互联网安全中心



开源
免费



虚拟机映像

Ubuntu09.11



Ubuntu11.04



Ubuntu12.04



Ubuntu16.04

Android 5.1



Android 7.1

如何使用实验环境



学生的个人计算机



云



公用机房

实验分成六类

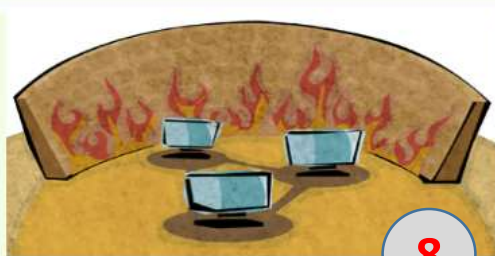
网站: <http://www.cis.syr.edu/~wedu/seed/>



7

Software Security Labs

These labs cover some of the most common vulnerabilities in general software. The labs show students how attacks work in exploiting these vulnerabilities.



8

Network Security Labs

These labs cover topics on network security, ranging from attacks on TCP/IP and DNS to various network security technologies (Firewall, VPN, and IPsec).



3

Web Security Labs

These labs cover some of the most common vulnerabilities in web applications. The labs show students how attacks work in exploiting these vulnerabilities.



2

System Security Labs

These labs cover the security mechanisms in operating system, mostly focusing on access control mechanisms in Linux.



5

Cryptography Labs


These labs cover three essential concepts in cryptography, including secret-key encryption, one-way hash function, and public-key encryption and PKI.



2

Mobile Security Labs

These labs focus on the smartphone security, covering the most common vulnerabilities and attacks on mobile devices. An Android VM is provided for these labs.




Ubuntu 16.04

Home → SEED Labs → Network Security Labs

Network Security Labs

AttackExplorationImplementation




Packet Sniffing and Spoofing Lab

Sniffing packets sent over the local network and spoofing various types of packets.

Exploration

Easy

Hard




TCP/IP Attack Lab

Launching attacks to exploit the vulnerabilities of the TCP/IP protocol, including session hijacking, SYN flooding, TCP reset attacks, etc.

Attack

Easy

Hard




Heartbleed Attack Lab (Ubuntu 12.04 VM only)

Using the heartbleed attack to steal secrets from a remote server.

Attack

Easy

Hard




Local DNS Attack Lab

Using several methods to conduct DNS pharming attacks on computers in a LAN environment.

Attack

Easy

Hard




Remote DNS Attack Lab

Using the Kaminsky method to launch DNS cache poisoning attacks on remote DNS servers.

Attack

Easy

Hard



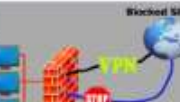
Firewall Exploration Lab

Writing a simple packet-filter firewall; playing with Linux's built-in firewall software and web-proxy firewall; experimenting with ways to evade firewalls.

Exploration

Easy

Hard




Firewall Evasion Lab

Implement a simple vpn program (client/server), and use it to bypass firewalls.

Exploration

Easy

Hard



Virtual Private Network (VPN) Lab

Design and implement a transport-layer VPN system for Linux, using the TUN/TAP technologies. This project requires at least a month of time to finish, so it is good for final project.

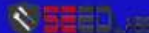
Implementation

Easy

Hard

TCP/IP Attack Lab

SEED Lab: A Hands-on Lab for Security Education



Overview



The learning objective of this lab is for students to gain first-hand experience on vulnerabilities, as well as on attacks against these vulnerabilities. Wise people learn from mistakes. In security education, we study mistakes that lead to software vulnerabilities. Studying mistakes from the past not only help students understand why systems are vulnerable, why a "seemly-benign" mistake can turn into a disaster, and why many security mechanisms are needed. More importantly, it also helps students learn the common patterns of

vulnerabilities, so they can avoid making similar mistakes in the future. Moreover, using vulnerabilities as case studies, students can learn the principles of secure design, secure programming, and security testing.

The vulnerabilities in the TCP/IP protocols represent a special genre of vulnerabilities in protocol designs and implementations; they provide an invaluable lesson as to why security should be designed in from the beginning, rather than being added as an afterthought. Moreover, studying these vulnerabilities help students understand the challenges of network security and why many network security measures are needed.

Lab Tasks (Description)

- **VM version:** This lab has been tested on our pre-built SEEDubuntu16.04 VM.

Recommended Time: 2 weeks

Suggested Reading

- **SEED Book:** Wenliang Du, *Computer Security: A Hands-on Approach* (Chapter 13).
- *Netwox/Netwag Guides*, by Sridhar Iyer.
- Comer's book: Chapter 13.
- *Slipping in the Window: TCP Reset attacks*, by Paul A. Watson.
- *Strange Attractors and TCP/IP Sequence Number Analysis* by Zalewski.
- *ICMP attacks against TCP*, by Gont, F.

SEED Project

- [Home Page](#)

SEED Labs – TCP/IP Attack Lab

1

TCP/IP Attack Lab

Copyright © 2018 Wenliang Du, Syracuse University.

The development of this document was partially funded by the National Science Foundation under Award No. 1303306 and 1718086. This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. A human-readable summary of (and not a substitute for) the license is the following: You are free to copy and redistribute the material in any medium or format. You must give appropriate credit. If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original. You may not use the material for commercial purposes.

1 Lab Overview

The learning objective of this lab is for students to gain first-hand experience on vulnerabilities, as well as on attacks against these vulnerabilities. Wise people learn from mistakes. In security education, we study mistakes that lead to software vulnerabilities. Studying mistakes from the past not only help students understand why systems are vulnerable, why a seemly-benign mistake can turn into a disaster, and why many security mechanisms are needed. More importantly, it also helps students learn the common patterns of vulnerabilities, so they can avoid making similar mistakes in the future. Moreover, using vulnerabilities as case studies, students can learn the principles of secure design, secure programming, and security testing.

The vulnerabilities in the TCP/IP protocols represent a special genre of vulnerabilities in protocol designs and implementations; they provide an invaluable lesson as to why security should be designed in from the beginning, rather than being added as an afterthought. Moreover, studying these vulnerabilities help students understand the challenges of network security and why many network security measures are needed. In this lab, students need to conduct several attacks on the TCP protocol. This lab covers the following topics:

- TCP SYN flood attack, and SYN cookies
- TCP reset attack
- TCP session hijacking attack
- Reverse shell

Readings and related topics. Detailed coverage of TCP attacks can be found in Chapter 13 of the SEED book, *Computer Security: A Hands-on Approach*, by Wenliang Du.

Lab environment. This lab has been tested on our pre-built Ubuntu 16.04 VM, which can be downloaded from the SEED website.

- 经典漏洞和攻击

- 软件: Buffer overflow, return-to-libc, format string, race condition
- 网络:
 - ARP cache poisoning
 - TCP: SYN flooding, TCP Reset, Hijacking (Mitnick)
 - DNS cache poisoning (Kaminsky)
 - Packet Sniffing/Spoofing
 - Evade firewall (翻墙)
- Web : XSS (Samy Worm), CSRF, SQL Injection
- 密码 : MD5 collision, IV, Man-in-the-Middle
- 手机 : Repackaging, Rooting



把新的攻击变成实验



- Meltdown Attack Lab (2018)
- Spectre Attack Lab (2018)
- Hash Collision Attack Lab (2018)
- Dirty COW Attack Lab (2016)
- Shellshock Attack Lab (2014)
- Heartbleed Attack Lab (2014)

- 注重防守机制
 - 密码应用
 - 防火墙
 - VPN
 - SSL/TLS Protocol
 - 操作系统，网络，浏览器的安全机制
- 简化复杂的机制
 - 解剖一个真正的系统
 - 抛弃或简化不重要的部分
 - 围绕重要部分设计实验
 - 替换，改动，观察
- 对编程要求不高

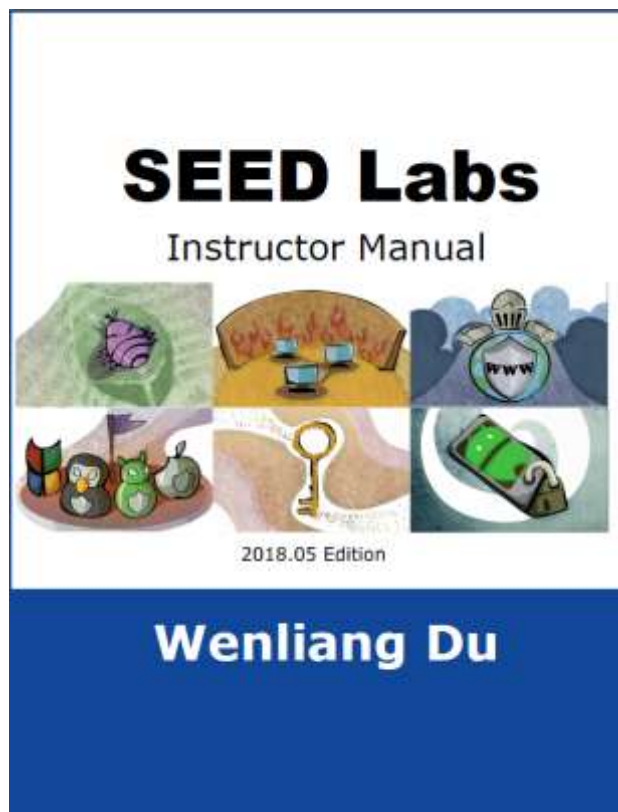


“The best way to learn something is build one yourself”:
学一样东西最好的方法是亲手把它做出来

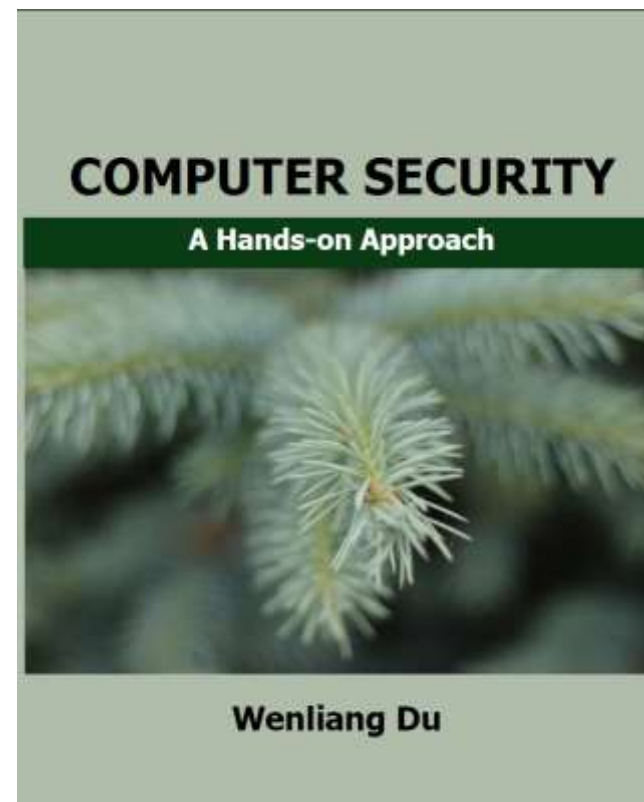
- 强调对综合能力的培养
 - 攻击，风险分析，防守
 - 培养安全编程的习惯
- 设计和实现一个简化的安全系统或机制
 - Mini-firewall
 - Mini-VPN
 - Role-based Access Control
 - Encrypted File System
 - SSL/TLS Protocol
- 对编程要求高



教师手册 (wedu@syr.edu)



教科书 <https://www.handsonsecurity.net/>



教师培训（美国自然科学基金资助）

人才培养模式：Train the Trainer: 培训教师

2015: 60位教师

2016: 70位教师

2017: 70位教师

2018: 80位教师



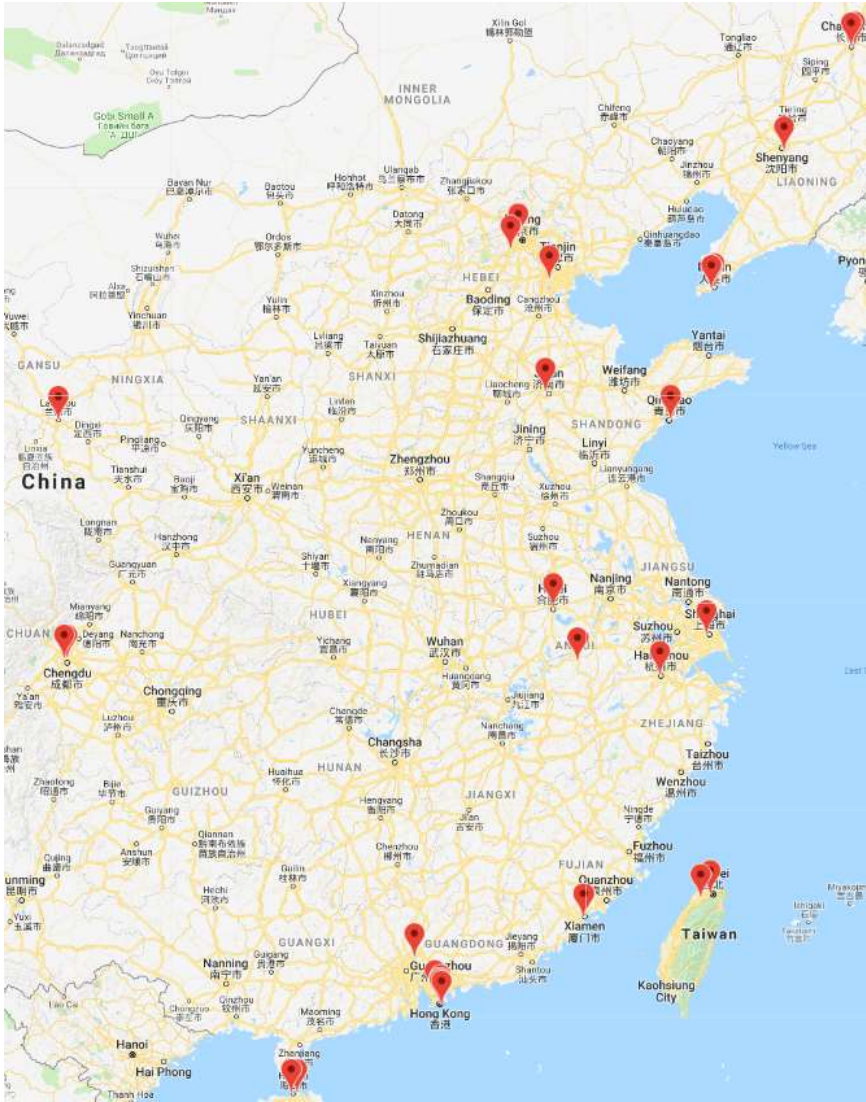
美国和中国使用对比



ISC 互联网安全大会



360 互联网安全中心



未来五年打算: 推广

- 促进SEED Labs在中国和其他国家的使用
 - 中国
 - 欧洲国家
 - 沙特
 - 印度
- “Train the Trainer”: 培训教师
- 公益性为主
 - 教师免费
 - 国家有关部门资助
 - 公司赞助



- 新的实验
 - 区块链教学和实验平台 (Coursechain)
 - 缩微“景区”：DNS In a Box, BGP In a Box
- CTF 版本 (Capture-The-Flag)
 - 把SEED Labs改成CTF竞赛 (课堂上)
 - 攻击类
- 非计算机专业版本
 - IT 专业, 信息管理
 - 面向高中生



ISC 互联网安全大会



360互联网安全中心

谢谢!

ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing · China

(原“中国互联网安全大会”)

Labs: <http://www.cis.syr.edu/~wedu/seed/>

Book: <https://handsonsecurity.net>

Email: wedu@syr.edu