Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

SmartStep

CCNA
Cyber Security Operations

Fachkursleitung:
Peter Infanger
Dozent Informatik

Mail: peter.infanger@hslu.ch

Agenda

1. Cybersecurity and NetAcad
2. Learning Pathways
3. Curriculum & Details
4. Schedule

Cybersecurity Opportunities

Cybercrime Costs

Cybersecurity Ventures: Cybersecurity Market Research- Top 15 statistics for 2017

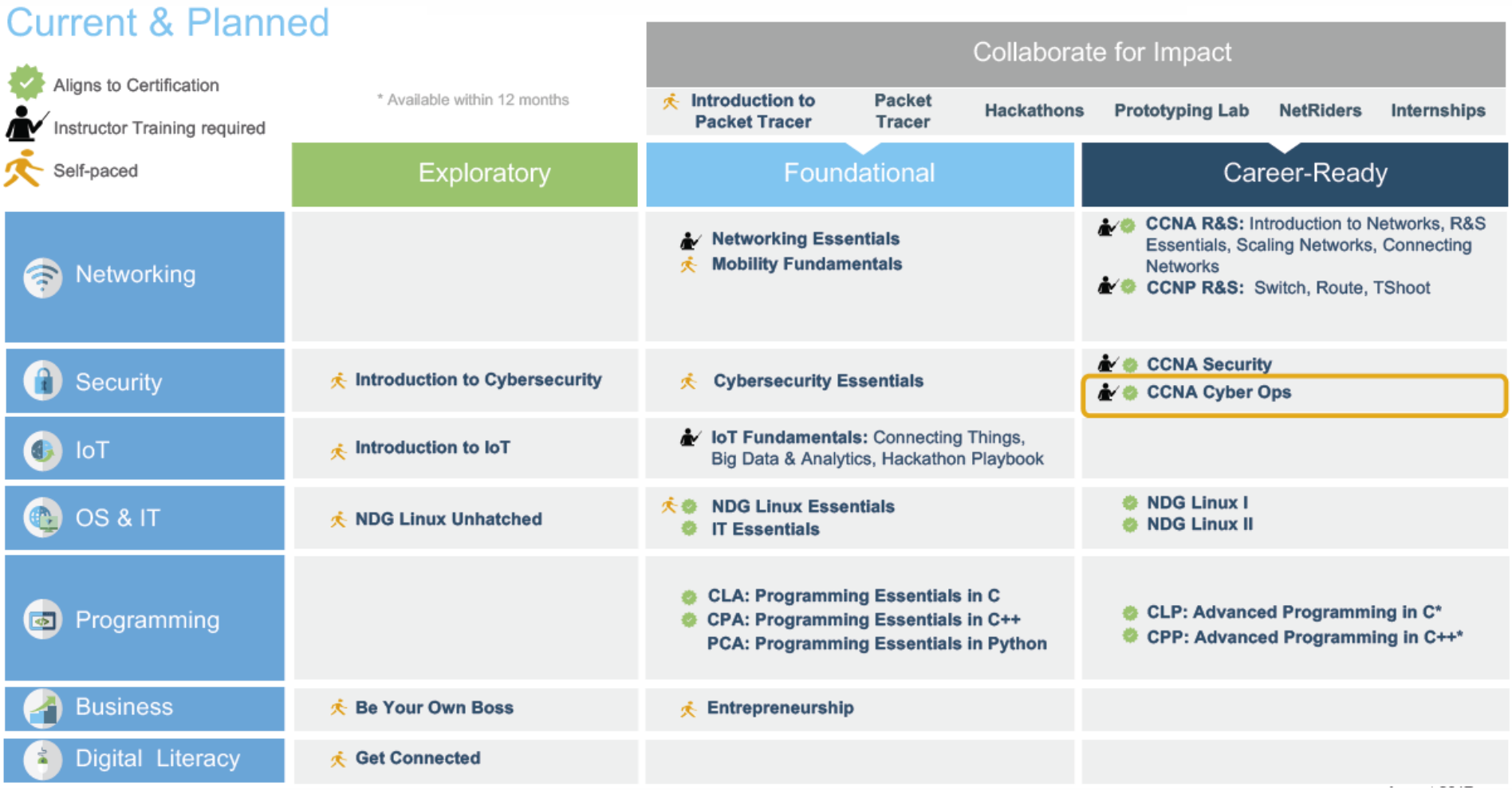
Security Spending

Cybersecurity Ventures: Cybersecurity Market Research- Top 15 statistics for 2017

Unprecedented Opportunity

Cybersecurity Ventures: Cybersecurity Market Research- Top 15 statistics for 2017

Networking Academy Learning Portfolio



CCNA Cybersecurity Operations Curriculum

Overview

CCNA Cyber Ops introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems.

Career Prep

The skills developed in the curriculum prepares students for a career in the rapidly growing area of cybersecurity operations working in or with a security operations center (SOC) in entry-level job roles such as:

- Security SOC Analyst
- Incident Responder

Learning Components

- 13 chapters of interactive content, quizzes, and chapter exams
- Labs, and hands-on labs using virtual machine environment (PC required, no other equipment required)
- Cisco® Packet Tracer activities (PT 7.0)
- Certification practice exams, practice final, final exam and skills-based assessment

Features

Target Audience: Students enrolled in technology degree programs at institutions of higher education and IT professionals who wants to pursue a career in Security Operations.

Prerequisites: None

Languages: English

Course Delivery: Instructor-led

Estimated Time to Complete: 70 hours

CCNA Cyber Sec Ops Value Proposition

- Gain understanding and handson experience on how to detect and respond to security incidents
- Understand how organizations deal with cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and related issues
- Gain job-ready practical skills for in-demand job roles in cybersecurity operations
- Prepare for industry recognize CCNA Cybersecurity Operations certification

CCNA Cyber Ops Recommended Pathways

Recommended Entry Knowledge

Recommended pre-requisite knowledge :

- PC and Internet navigation skills
- Basic Windows and Linux system concepts
- Basic Networking concepts
- Binary and Hexadecimal understanding
- Awareness of basic programming concepts
- Awareness of basic SQL queries
- Familiarity with Cisco Packet Tracer, a network simulation application.

Note:

While not mandatory, taking one or more of the following Networking Academy courses enhances and maximizes student learning:

IT & OS (one or more of the following
- IT Essentials
- NDG Linux Essentials

Networking (one or more of the following)
- Networking Essentials
- CCNA R&S: Introduction to Networks

Security
- Introduction to Cybersecurity
- Cybersecurity Essentials

Packet Tracer
- Introduction to Packet Tracer

CCNA Cyber Ops contains optional refresher material for the above skills within the instructional flow

Course Structure

Chapter	Title	Theme
1	Cybersecurity and the Security Operations Center	Introduction
2	Windows Operating System	OS Fundamentals
3	Linux Operating System	
4	Network Protocols and Services	Networking Fundamentals
5	Network Infrastructure	
6	Principles of Network Security	Cybersecurity Fundamentals
7	Network Attacks: A Deeper Look	
8	Protecting the Network	
9	Cryptography and the Public Key Infrastructure	
10	Endpoint Security and Analysis	
11	Security Monitoring	Cybersecurity Operations
12	Intrusion Data Analysis	
13	Incident Response and Handling	

CCNA Cyber Sec Ops Equipment

Equipment Requirements

Curriculum requirements: 1 student Personal Computer (Desktop/Notebook) per student (recommended), at most 2 students per PC

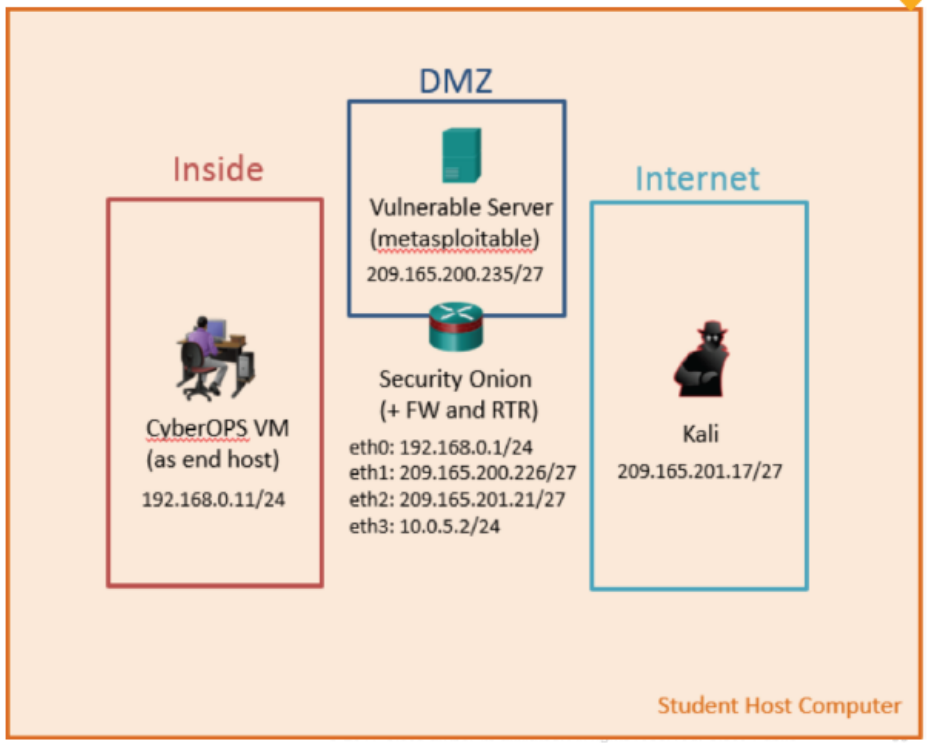
Platform	Description
Desktop PC	• OS: Windows 7, 8, or 10, MAC OSX • Processor: 64-bit processor with Virtualization Support , see https://www.computerhope.com/issues/ch001121.htm to determine if computer has a 64-bit processor • Memory: 8 gigabyte (GB) RAM (standard) or 4 GB (alternate option) • Display Adapter: PCI, PCIe (recommended), or AGP video card (DirectX 9 graphics device with WDDM driver) • Disk: 45 GB hard drive. See table in the next slide for details. • Network: 1 Ethernet Card or 1 Wireless Ethernet Card
Web Browser	The most recent version of Microsoft Internet Explorer, Google Chrome, or Mozilla Firefox with the most recent versions of Java and Flash Player installed.
Oracle VirtualBox	The latest version. http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
Windows Experience Index (WEI)	6.5 (recommended)
Packet Tracer	Minimum version 7.0 or later

CCNA Cyber Sec Ops Equipment

Equipment Requirements

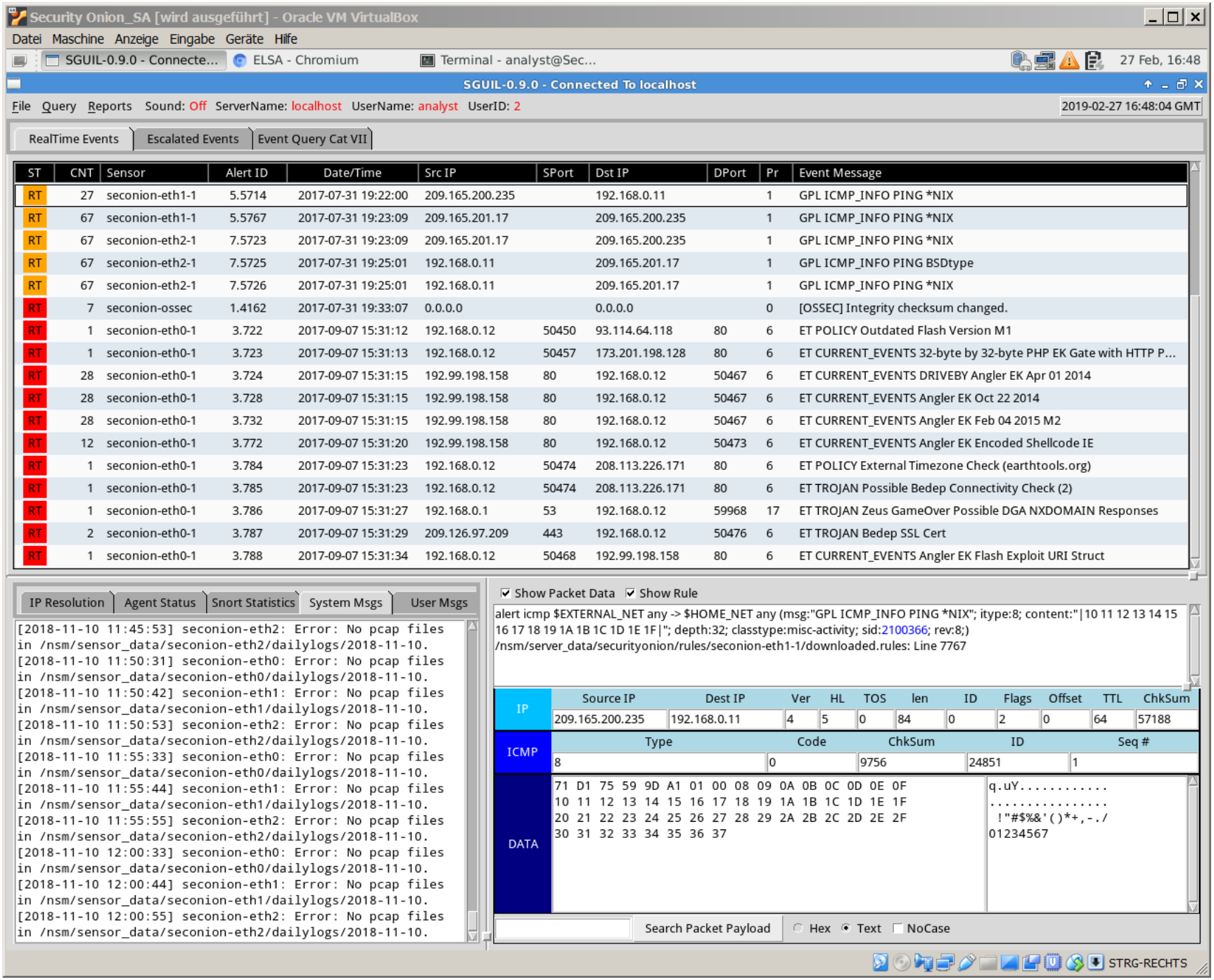
Virtual Machine Name	Disk Space	RAM
CyberOps Workstation VM	7 GB	1 GB
Kali Linux VM	10 GB	1 GB
MetaSploitable VM	8 GB	512 MB
Security Onion VM	10 GB	4 GB
Security Onion VM*	10 GB	3 GB

* Chapter 12 labs provide an option of using only one Alternative Security Onion VM

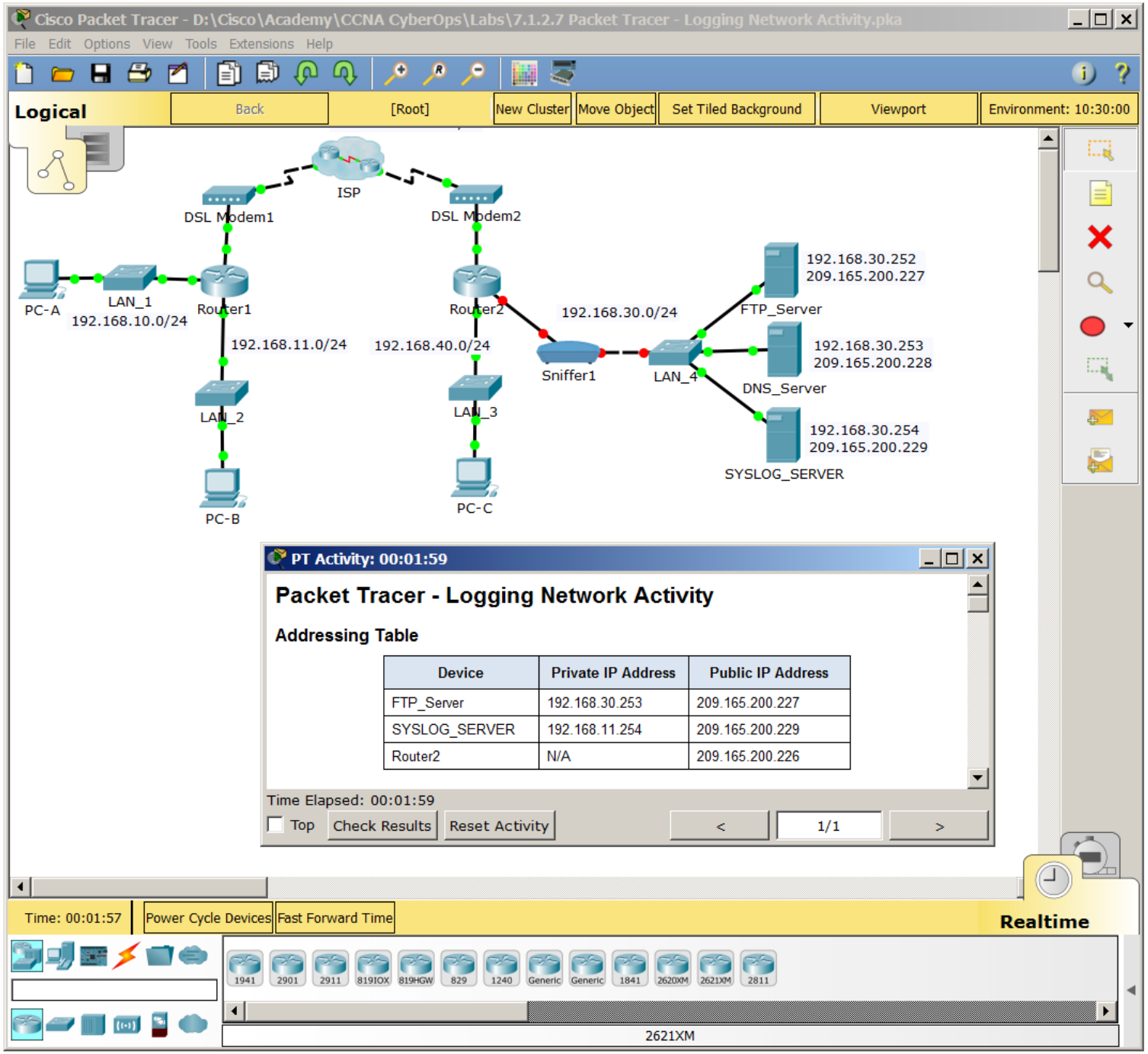


Lab Setup

Security Onion: a Network Security Manager



Packet Tracer Simulator



Timeline

Fachkurs / SmartStep
CCNA Cyber Security Operations (CySecOp)

https://www.hslu.ch/de-ch/informatik/weiterbildung/networking-and-innovative-technologies/fk-ccna-cysecop/

Start:
Donnerstag. 9. Mai – 27. Juni 2019 jeweils 16:00 – 20:50
7 Kontaktstudienblöcke + 1 praktischer Abschlusstest (4h)

Kosten: Fr. 3950.-

Einbettung

Teil eines Grösseren:

CAS Cyber Security Defence & Response

Ausschreibung startet anfangs März
(https://www.hslu.ch/de-ch/informatik/weiterbildung/)

mit Start im Herbst 2019 (Sept./Okt.)

Fragen und Kommentare

Backup Slides

CCNA Cyber Sec Ops Course Outline

Chapter	Chapter Titles	Summary Description
1	Cybersecurity and the Security Operations Center	Understand the who, what, and why of cyberattacks. Different people commit cybercrime for different reasons. Security Operations Centers work to combat cybercrime.
2	Windows Operating System	Understand basic concepts of Windows, including how the operating system works and the tools used to secure Windows endpoints.
3	Linux Operating System	Perform basic Linux operations, administrative and security-related tasks.
4	Network Protocols and Services	Explain how networks normally behave using the TCP/IP suite of protocols, and associated services that enable tasks on computer networks.

CCNA Cyber Sec Ops Course Outline

Chapter	Chapter Titles	Summary Description
5	Network Infrastructure	Explain the basic operation of network infrastructures, including wired and wireless networks, network security, and network designs.
6	Principles of Network Security	Use the variety of tools and methods that threat actors use to launch network attacks.
7	Network Attacks: A Deeper Look	Understand the importance of traffic monitoring and how it is conducted. Classify vulnerabilities of network protocols and services including IP, TCP, UDP, ARP, DNS, DHCP, HTTP, and email.
8	Protecting the Network	Explain the approaches to network security defense, access control methods, and the various sources cybersecurity analysts rely on for threat intelligence.

CCNA Cyber Sec Ops Course Outline

Chapter	Chapter Titles	Summary Description
9	Cryptography and the Public Key Infrastructure	Explain the impact of cryptography on network security monitoring.
10	Endpoint Security and Analysis	Explain how to investigate endpoint vulnerabilities and attacks.
11	Security Monitoring	Explain security technologies and log files used in security monitoring.
12	Intrusion Data Analysis	Understand how network security alerts are reported, evaluated, analyzed, escalated, and preserved as evidence.
13	Incident Response and Handling	Apply incident response and handling models and procedures including the Cyber Kill Chain, the Diamond Model, the VERIS schema and National Institute of Standards and Technologies (NIST) guidelines for the structure of Computer Security Incident Response Teams (CSIRTs) and processes for handling an incident.