

How can students develop real Cybersecurity skills?

Jelena Revzina





- IT Security
- Virtualization
- Data Storage
- Data centers

www.ipro.lv

Cisco Networking Academy

Platform evolution

Delivered online through netacad.com, a global cloud-based learning and collaboration platform.

Since 1997

9.26 million students



In FY18

180 countries

11,400 academies

24,700 instructors

1.87 million learners

28% female learners

\$320 million in-kind contributions from Cisco



By 2020

2 million students enrolled annually*

Learning portfolio updates





Seven new courses and workshops including a new security portfolio, CyberOps, emerging technologies.

Talent Bridge Matching Engine


Digital platform automates connections of Networking Academy students to jobs with Cisco and its channel partners.










The Networking Academy Learning Portfolio

Current

-  Aligns to Certification
-  Instructor Training required
-  Self-paced
-  ASC Alignment required

Collaborate for Impact

-  Introduction to Packet Tracer
- Packet Tracer
- Hackathons
- Prototyping Lab
- Internships

	Exploratory	Foundational	Career-Ready
Networking		<ul style="list-style-type: none">  Networking Essentials  Mobility Fundamentals  Emerging Tech Workshop: Network Programmability Using Cisco APIC-EM 	<ul style="list-style-type: none">    CCNA R&S: Introduction to Networks, R&S Essentials, Scaling Networks, Connecting Networks    CCNP R&S: Switch, Route, Tshoot
Security	<ul style="list-style-type: none">  Introduction to Cybersecurity 	<ul style="list-style-type: none">  Cybersecurity Essentials 	<ul style="list-style-type: none">    CCNA Security    CCNA Cybersecurity Operations
IoT & Analytics	<ul style="list-style-type: none">  Introduction to IoT 	<ul style="list-style-type: none">   IoT Fundamentals: Connecting Things, IoT Security, Big Data & Analytics, Hackathon Playbook 	
OS & IT	<ul style="list-style-type: none">  NDG Linux Unhatched 	<ul style="list-style-type: none">    NDG Linux Essentials    IT Essentials 	<ul style="list-style-type: none">  NDG Linux I  NDG Linux II
Programming		<ul style="list-style-type: none">  CLA: Programming Essentials in C  CPA: Programming Essentials in C++   PCAP: Programming Essentials in Python  Emerging Tech Workshop: Experimenting with REST APIs using Webex Teams 	<ul style="list-style-type: none">  CLP: Advanced Programming in C  CPP: Advanced Programming in C
Business	<ul style="list-style-type: none">  Be Your Own Boss 	<ul style="list-style-type: none">  Entrepreneurship 	

Reduce PI image an

Why, and who, and how, to teach cybersecurity...



Cybersecurity Statistics in 2019

- It takes half a year to detect a data breach.
- 43% of all cyber attacks are aimed at small businesses
- 91% of attacks launch with a phishing email.
- A business falls victim to a ransomware attack every 14 seconds
- 38% of malicious attachments are masked as one Microsoft Office type of file or another.
- Cybercriminals managed to exploit the credit cards of 48% of Americans back in 2016.
- The global cost of online crime is expected to reach \$6 trillion by 2021.



Cybercrime damages will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015. Costs include destruction of data, stolen money, and more.



The world will spend \$1 trillion cumulatively from 2017-2021 on products and services to combat cybercrime.

Jobs Critical for Digital Transformation

Analytics and Business Process

Collecting and analyzing data; creating efficient business processes, and improving product design

Application Development and Support

Designing, testing, and managing applications for (IoT) platforms & controllers, protocols and end device software

Infrastructure and Operations

Building, monitoring and maintaining infrastructure (network, compute, storage); integration with control systems and other enterprise applications, and device management

Digital Security and Privacy

Securing (IoT) infrastructure, networks, applications, and devices

General IT/Horizontal

Securing environments, creating strategy, and ensuring usability

66 million FTEs worldwide will be driving digital transformation in 2023

Source: Cisco IoT/Digital Jobs, Gartner 2018



3X

Cybersecurity jobs are growing **THREE TIMES FASTER** than IT jobs in general.

53%

53% of employers currently take longer than **SIX MONTHS** to find qualified cybersecurity professionals.

3M

There will be a global shortage of **3 MILLION** cybersecurity professionals by 2021.

84%

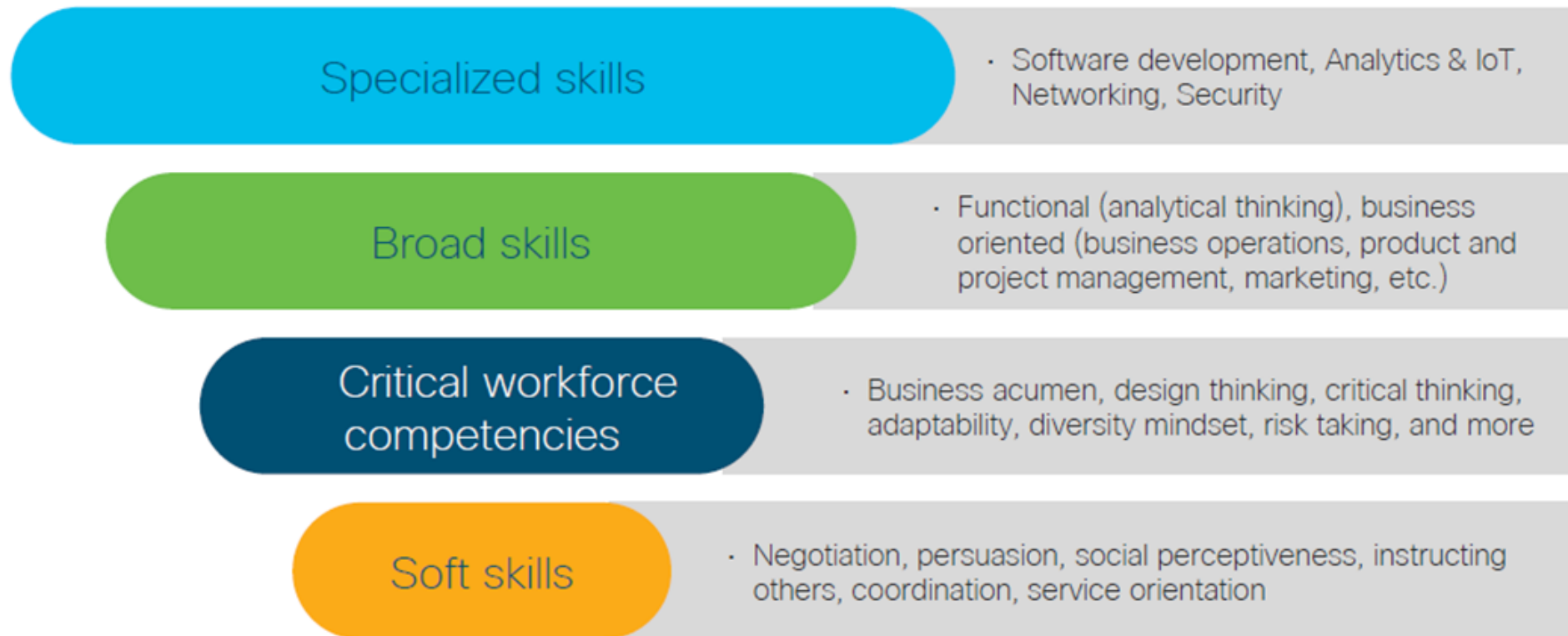
84% of organizations believe that **50% or fewer** applicants for open security jobs are qualified.

Source: ISACA Cybersecurity Skills Gap 2016, US Information Systems Audit and Controls Association, Cybersecurity Business Report

Who



Skills Required for a Digital Workforce



How

- The field of cybersecurity grew out of information technology, cybersecurity education is evolving as an offshoot of the computer science field.
- The current state of cybersecurity course offerings as an underdeveloped computer science footnote is allowing the skills gap to grow.
- To change this, higher education has to address the theoretical and hands-on skills students need to do their jobs post-graduation.

Challenges

- Cybersecurity is a broad field with many different facets.
- Each student should check the different options and possibilities to find the role and field that best suits their interests.
- For these reasons it is difficult to provide specific guidance that fits reverse engineers and developers, as well as data analysts.



Cybersecurity Framework



Teaching approaches

- Problem-based learning
- Case Studies
- Hackathons
- Cooperation and Mentoring



Case Study

Crybaby businessman-Case Study

Objectives

The objective of this exercise is to investigate a security incident related with an attack that targeted a business man. At the end of the investigation you should write and report that explains how the attack

Cybersecurity Operations

Case Study: The inexperienced analyst

Objectives

You are currently working at Organization "X" SOC as an analyst. During one of your night shift, you notice a non-specific alert from a generic IDS while the snort-based IDS was offline. You decide to investigate further so to establish whether the alert indicates malicious traffic, or it is a false positive.

Your task is to determine the line of events that led to the alert.

Resources

For the task assigned, you are provided with the pcap file which captured the network that caused the alert; you should analyse it with Wireshark. You can also replay the traffic in order to generate the alert(s) on the snort-based IDS.

Tools to use:

- Wireshark;
- Sguil;
- VirusTotal (optional);
- Google (optional).

Task 1: Setup and configuration

(pcap) that has the details of series events that happened
ing the following tools, provided as part of the Security Onion

Project 2: Metasploit



Table of Contents

1. Introduction: What is Metasploit?
2. Basic Concepts and Knowledge Requirements
 - 2.1 Knowledge Requirements
 - 2.2 Basic Concepts
 - 2.2.1 Hypervisors
 - 2.2.2 Kali Linux
 - 2.2.3 Metasploitable
 - 2.2.4 Exploit
 - 2.2.5 Payload
 - 2.3 Basic Metasploit Methodology
3. Lab Exercise
 - 3.1 Scenario Description
 - 3.2 Getting Started: Installation of the Virtual Machine
 - 3.3 Gaining access to the target using the CVE 2004-2687 exploit
 - 3.4 Gaining root privileges
4. Questions to think about and reflect on
5. References

NetworkMiner

A Network Forensic Analysis Tool

Project 2 – Topic 7

Introduction

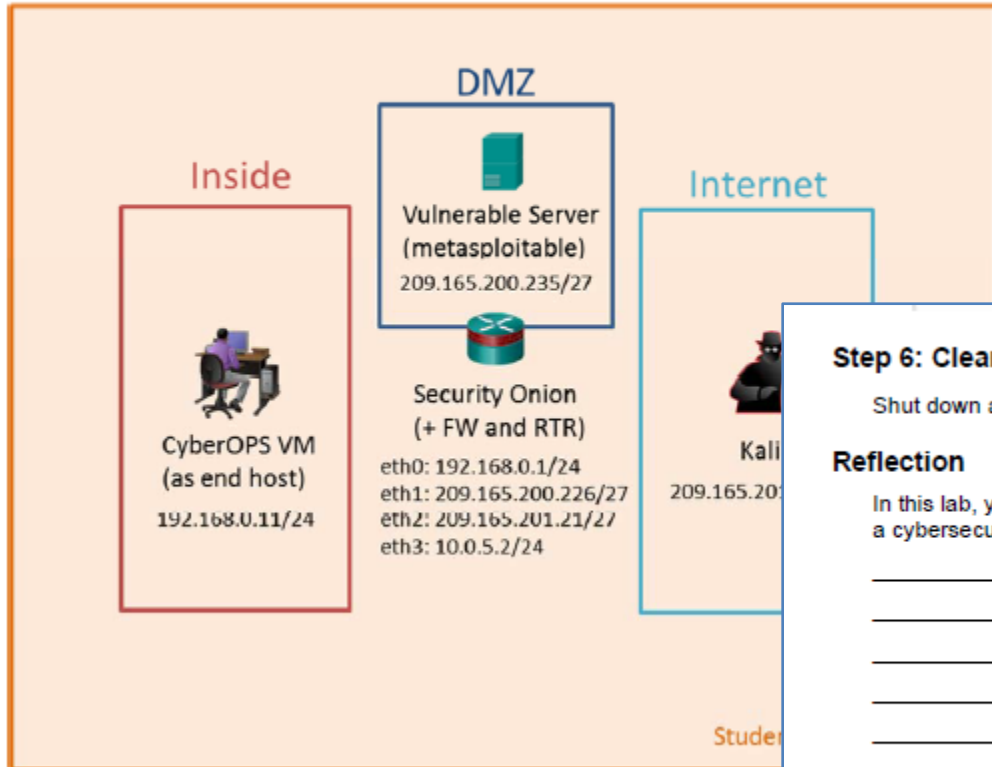
In this report we had to identify and analyze a PCAP file of an attack and to find and export files and objects that can be used as evidence for further investigation. And finally we explained how the attack happened and which machines were involved.

NetworkMiner is an open source Network Forensic Analysis Tool (NFAT) that can work in different Operating Systems such as Windows, Linux, Mac OS X and FreeBSD. NetworkMiner can parse PCAP files for off-line analysis and to regenerate/reassemble transmitted files and certificates from PCAP files. It can also be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports etc. without putting any traffic on the network.

Hands-on Lab Example

Lab – Isolated Compromised Host Using 5-Tuple

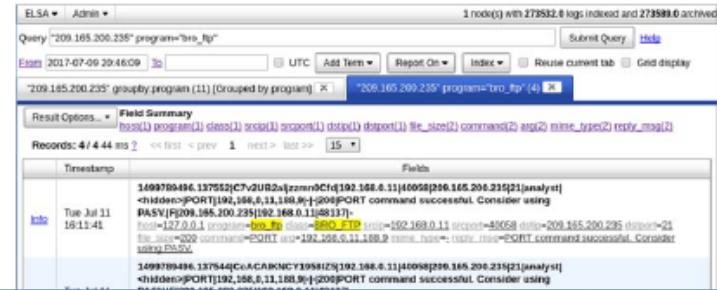
Topology



- d. You can also right-click the Alert ID and select Wireshark to review and save the pcap file and TCP stream.

Step 5: Use ELSA to view exfiltrated data.

- a. To use ELSA for more information about the same alert as above, right-click either the source or destination IP address and select ELSA IP Lookup > DstIP.
- b. Click bro_ftp to view ELSA logs that are related to FTP.



Step 6: Clean up

Shut down all VMs when finished.

Reflection

In this lab, you have used a vulnerability to gain access to unauthorized information and reviewed the logs as a cybersecurity analyst. Now summarize your findings.

Web pentests

<https://portswigger.net/burp>



```
URI proxyUri;
try {
    proxyUri = new URIBuilder(uri)
        .setHost(backendURL.getHost())
        .setPort(backendURL.getPort())
        .setScheme(backendURL.getScheme())
        .build();
} catch (URISyntaxException e) {
    Util.sendError(ctx, 400, INVALID_REQUEST_URI);
}
return;
```

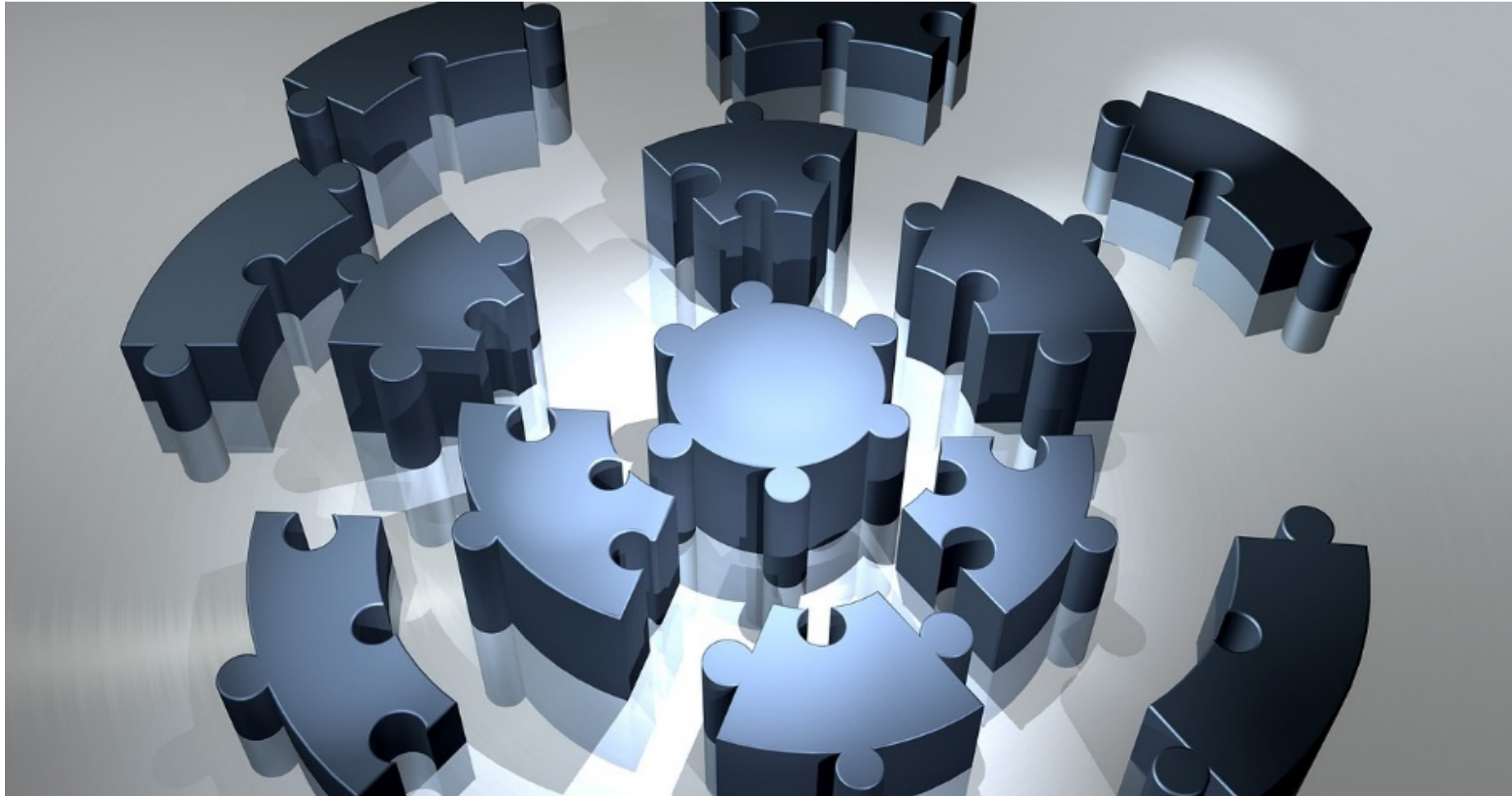
18.10.2019
CYBERCHESS 2019

Damn Vulnerable Web Application (DVWA)



<http://www.dvwa.co.uk/>

Collaboration



Hackathons

Organized in the Helsinki Area, Finland, Junction is a meeting place for thousands of developers, designers, and entrepreneurs. A weekend-long experience, gathering tech enthusiasts from all over the world to create with the latest technology in a unique environment and atmosphere.

Hack the Future

Tracks

Here are the Tracks for Junction 2019.

SECURE THE FUTURE	DATA ECONOMICS
GAME JAM	HEALTHTECH
SUSTAINABILITY	INTELLIGENT INFRASTRUCTURE
DIGITAL RETAIL	CYBERSECURITY
FUTURE CITIES	MOBILITY



Mentor's role by Katy Dickinson

Mentors advise and inspire.

In short, practical terms:

1. Mentor make introductions – to people, to programs or companies.
2. Mentor give recommendations to best resources – reading, classes, experiences.
3. Mentor give feedback for the mentee to consider.



Mentoring vs. Coaching vs. Sponsorship

	Power	Topic	Duration	Boundaries	Reward
Sponsor	Hierarchical or positional authority	Succession planning, leadership building	Long-Term: many years	Part of regular work	Career direction, protection during growth
Coach	Special knowledge	Transfer of specific information, tools	Short-Term: class or program duration	School or training program's scope and management	Student: passing a test Coach: payment
Mentor	Wisdom authority	Career or personal growth	Mid-Term: 6 to 12 months	Mentoring program's scope and management	Mutual learning, recommendations , feedback

Based on 2014 work by Everwise, licensed under a Creative Commons Attribution-ShareAlike 4.0 International License:
<https://creativecommons.org/licenses/by-sa/4.0/>

jelena.revzina@ipro.lv

- IT Security Expert r at iPro company www.ipro.lv
- Cisco Networking Academy instructor (CCNA, CCNA Security, Cybersecurity CyberOps) at Transport and Telecommunication Institute www.tsi.lv
- Cisco Networking Academy Recognitions:
 - Instructor Excellence Expert - 2012, 2013, 2015
 - Cisco Women in Networking (in Europe) - 2012
 - 10 Years of Service - 2016



Thank you!

References

1. Cisco Networking Academy www.netacad.com
2. Cisco DevNet <https://developer.cisco.com/>
3. Scapy Documentation <http://scapy.readthedocs.io/>
4. OWASP Homepage <https://www.owasp.org/>
6. Hackers Online Club <https://www.hackersonlineclub.com/network-hacking/>
7. Vulnerability Assessment, Penetration testing framework
<http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>
8. Katy Dickinson <http://www.mentoringstandard.com/>