

CCNA Cybersecurity Operations

- Workshop: Netzwerk ganz praktisch

18. Nationaler Akademietag in Hamburg

Almut Leykauff-Bothe, MMBbS Hannover
Stefan Krieger BBS Rotenburg

04. Mai 2019

: reserved. Cisco Confidential

Worum gehts

-  Kahoot!
-  Security courses
-  CCNA Cyber Ops Kursdesign
-  Erfahrungsaustausch
-  Cisco CyberOps Skills Challenge Game



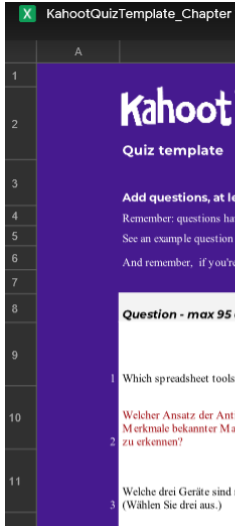
Kahoot!

Aufgabe 10

Erstellen eines gemeinsamen KahootQuiz zum Chapter 10.

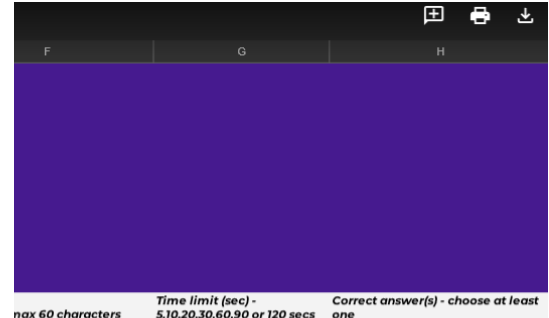
Erarbeiten Sie in zufälligen Gruppen Antworten zu vorgegeben Fragen aus den Abschnitten:

Gruppe	Curriculum	Kahoot Fragenzeile
1	10.1.1 Antimalware Protection	2- 5
2	10.1.2 Host-Based Intrusion Protection	6 - 9
3	10.1.3 Application Security	10 - 13
4	10.2.1 Network and Server Profiling	14 - 17
5	10.2.2 Common Vulnerability Scoring System (CVSS)	18 - 21
6	10.2.4 Secure Device Management	22 - 25



Google Sheets CyberOpsChapter10 Block ROT

Für Teilnehmer/innen verborgen



Join with the Kahoot! app or at kahoot.it with Game PIN:

160685

0 Players



Kahoot!



Grundlagen der Cybersicherheit

Leykauff

Created 11 months ago • 5 plays



Visible to only you

Play

Challenge

<https://create.kahoot.it/create - /edit/cc6e7d64-7600-4850-8e05-3d0e0ce2ce2b/done>



Security courses

Instructor-led, Online self-paced

Introduction to Cybersecurity

The introductory course for those who want to explore the world of cybersecurity.


Beginning



[Learn More](#)

Instructor-led, Online self-paced

Cybersecurity Essentials

For those planning to study for CCNA Routing & Switching or CCNA Security certifications.


Intermediate



[Learn More](#)

Instructor-led

CCNA Cybersecurity Operations

Develop the know-how to monitor, detect and respond to cybersecurity threats.


Advanced



[Learn More](#)

Instructor-led

CCNA Security

Develop the skills needed to design and support the integrity of network devices.


Advanced



[Learn More](#)

Introduction to Cybersecurity



Einführung in die Cybersicherheit

Kursübersicht

Der Kurs untersucht Cyber-Trends, Bedrohungen und die Sicherheit im Cyberspace, um den Schutz von persönlichen Daten und Unternehmensdaten zu gewährleisten.

MMBbS Kurs

MMBbS – Einführung in die Cybersicherheit
- SJ 2018/2019

[Link zur Selbstbeschreibung](#)



Features

Zielgruppe : Alle SchülerInnen der MMBbS

Voraussetzungen : Keine

Sprache : Deutsch, Englisch

Kosten : Keine

Kursart : Selbststudium

Geschätzter Zeitaufwand : 15 Stunden

Course Structure: Introduction to Cybersecurity

	Chapters	Labs (selected)	Other
1	The Need for Cybersecurity	Compare Data vs Hash	No PT labs
2	Attacks, Concepts and Techniques		Some videos
3	Protecting Your Data and Privacy	Creating strong passwords, Backing up your data	
4	Protecting the Organization		
5	Will Your Future Be in Cybersecurity?		

Labs



Control Panel Home

- Create a system image
- Create a system repair disc

Back up or restore your files

Backup

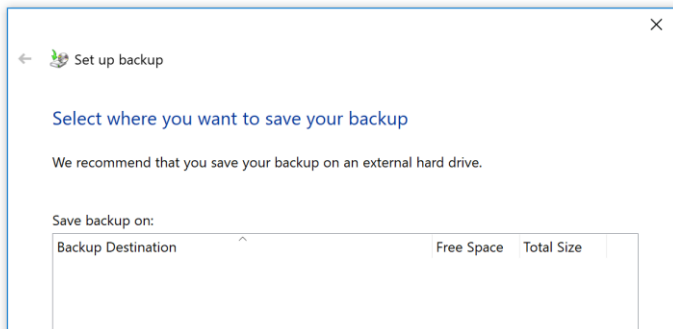
Windows Backup has not been set up.

[Set up backup](#)

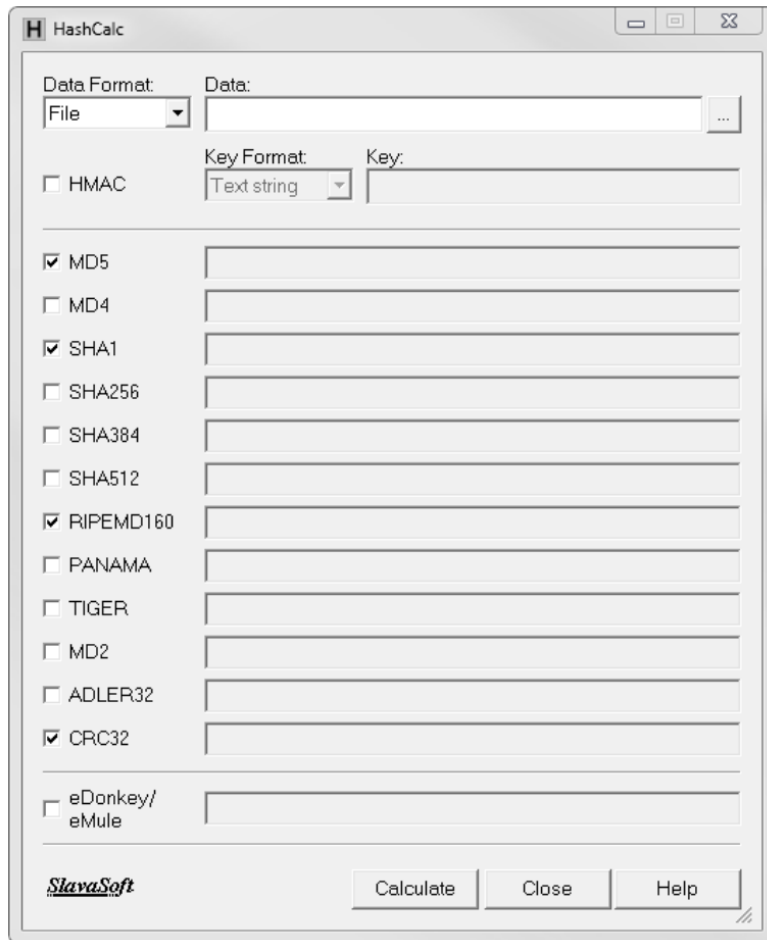
Restore

Windows could not find a backup for this computer.

[Select another backup to restore files from](#)



See also
Security and Maintenance
File History



What's in it for me?

Upon completion of this course student is able to:

- Stop sticking his password to a monitor
- Think about password management
- Think before sharing any information
- Implement backup before Data is lost
- Be a Cybersecurity ambassador



Aktionsplan für Introduction to Cybersecurity

- Erstellen einer Self-Enroll-Seite mit dem Logo der Schule. Veröffentlichung und Verbreitung des Links
- Mails, Aushänge, News, Infos auf Webseite

MMBBS – CYBERSECURITY SUMMER SCHOOL 2018

Herzlich Willkommen zu unseren Kursen zur Selbstschreibung. Aus dem Cisco Networking Academy Kurs Portfolio bietet die MMBbS ab jetzt für alle Schüler Kurse zur Selbstschreibung an.

Einführungskurse:

MMBBS - Intro to Packet Tracer - SJ 2018/19

MMBBS - NDG Linux Unhatched - SJ 2018/19

MMBBS - Introduction to Cybersecurity - SJ 2018/19

MMBBS - Introduction to IoT - SJ 2018/19



MMBBS - Introduction to Cybersecurity - SJ 2018/19

Multi-Media Berufsbildende Schulen Hannover

Multi-Media Berufsbildende Schulen
Regionales Bildungszentrum für die Medien- und
IT-Berufsausbildung in der Region Hannover

Multi
Cisco
Networking
Academy

Multi Media
Berufsbildende Schulen

Course Details

MMBBS - Introduction to Cybersecurity - SJ 2018/19
Introduction to Cybersecurity (German v2.01)
8 July 2018 - 9 July 2019
Joachim Kemmlies, Almut Leykauff-Bothe

Enroll Now

leykauff.bothe@mmbbbs.de

Submit

Description

Willkommen zur "Einführung in den Kurs zur Cybericherheit!"

Die Gefahr durch gezielte Angriffe auf zentrale Computersysteme und weltweit zeitgleich gebündelte Attacken auf Netzwerke nehmen zu. Finden Sie heraus, wer die Cyber-Angreifer sind und welche Ziele ihre Manipulationen haben!

Lernen Sie die wichtigsten Begriffe und die verschiedenen Arten von Malware und Cyberangriffen kennen kennen. Erfahren Sie, wie sich Unternehmen vor diesen Angriffen schützen. Werden Sie sich der Bedeutung des sicheren Online-Verhaltens, der potenziellen Folgen von Cyberangriffen und der möglichen Karrierechancen im Bereich „Cybericherheit“ stärker bewusst.

Dieser deutschsprachige Kurs der Cisco Networking Academy umfasst rund 15 Stunden Online-Lerninhalte. Zusätzlich gibt es Quizze, Übungen und Packet Tracer-Simulationen, die zur Vertiefung des neu gewonnenen Wissens genutzt werden können.

Die Teilnahme ist kostenfrei nach Anmeldung unter „Sign up now“ auf der rechten Seite und Aktivierung ihrer Anmeldung durch Bestätigung des Anmelde-links, welchen Sie per E-mail erhalten.

[Link zur Selbstschreibung](#)



Umsetzung Introduction to Cybersecurity an den BBS ROW

- Der Kurs wird genutzt zu Beginn des 2. Ausbildungsjahrs der Informationstechnischen Assistenten, als Crashkurs vorm vierwöchigen Praktikum
- Niveau angemessen für diese Schulform
- Schnelldurchlauf bei der Zielgruppe möglich, pro chapter ca. 45-90 min (ohne Übungen)
- nur wenige Labs (Hash-Calc, sichere Passwörter, Backup)



Vorteile Introduction to Cybersec

- Kurs eignet sich als Einstieg ins LF 5
- gute Vorbereitung fürs Praktikum
(Wiederholung für die fitten Schüler, solide Basis für die weniger fitten...)
- dieser Kurs geht nicht in die Tiefe, recht kurzweilig
- Labs könnten ausgebaut werden



Cybersecurity Essentials



Grundlagen der Cybersicherheit

Kursübersicht

Der Kurs umfasst grundlegendes Wissen und grundlegende Fähigkeiten für alle Bereiche der Cybersicherheit, einschließlich Informationssicherheit, Systemsicherheit, Netzwerksicherheit, Ethik und Gesetze sowie Verteidigungs- und Entschärfungstechniken, die zum Schutz von Unternehmen eingesetzt werden.

MMBbS Kurs

MMBbS - Cybersecurity Essentials
- SJ 2018/2019

[Link zur Selbsteinschreibung](#)



Features

Zielgruppe : SchülerInnen der Berufsschulen MMBbS

Voraussetzungen : Einführung in die Cybersicherheit

Sprache : Deutsch, Englisch

Kosten : Keine

Kursart : Selbststudium

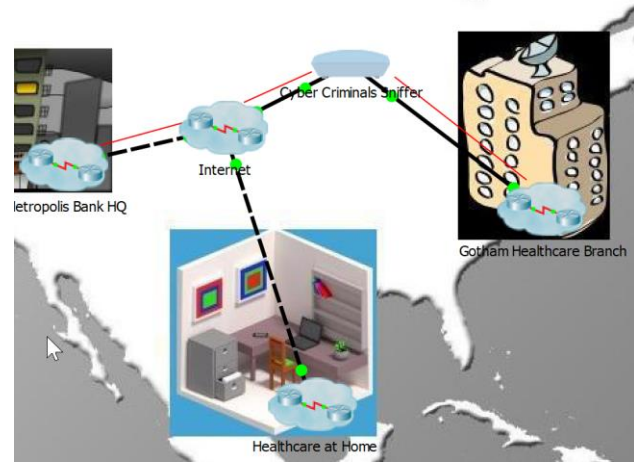
Geschätzter Zeitaufwand : 30 Stunden

Empfohlener nächster Kurs : CCNA R&S Introduction to Networks

Course Structure: Cybersecurity Essentials

	Chapters	Labs (selected)	Other
1	Cybersecurity – A World of Experts and Criminals	Threat Identification	10+ PT Labs
2	The Cybersecurity Cube	Exploring AAA	No Videos
3	Cybersecurity Threats, Vulnerabilities and Attacks	Detecting Threats and Vulnerabilities	
4	The Art of Protecting Secrets	Using Steganography	
5	The Art of Ensuring Integrity	Password Cracking in Linux, Remote access	
6	The Five Nines Concept		
7	Protecting a Cybersecurity Domain	Hardening a Linux System	
8	Becoming a Cybersecurity Specialist		

Labs



[+] Users, Groups and Authentication

```
- Search administrator accounts [ OK ]
- Checking for non-unique UIDs [ OK ]
- Checking consistency of group files (grpck) [ OK ]
- Checking non unique group ID's [ OK ]
- Checking non unique group names [ OK ]
- Checking password file consistency [ OK ]
- Query system users (non daemons) [ DONE ]
- Checking NIS+ authentication support [ NOT ENABLED ]
- Checking NIS authentication support [ NOT ENABLED ]
- Checking sudoers file [ FOUND ]
  - Check sudoers file permissions [ OK ]
- Checking PAM password strength tools [ SUGGESTION ]
- Checking PAM configuration files (pam.conf) [ FOUND ]
- Checking PAM configuration files (pam.d) [ FOUND ]
- Checking PAM modules [ FOUND ]
- Checking LDAP module in PAM [ NOT FOUND ]
- Checking accounts without expire date [ OK ]
- Checking accounts without password [ OK ]
- Checking user password aging (minimum) [ DISABLED ]
- Checking user password aging (maximum) [ DISABLED ]
- Checking expired passwords [ OK ]
```

```
cisco@ubuntu: ~/Downloads/john-1.8.0/run
cisco@ubuntu:~/Downloads/john-1.8.0/run$ ./john --wordlist=password.lst
mypass2
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3)
[?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password1 (Eric)
12345 (Bob)
123456 (Alice)
password (cisco)
password (Eve)
5g 0:00:00:08 31% 0.5561g/s 106.7p/s 160.1c/s 160.1c/s meggie..seattle
5g 0:00:00:11 42% 0.4500g/s 120.9p/s 164.1c/s 164.1c/s deede..grizzly
5g 0:00:00:13 53% 0.3782g/s 130.7p/s 167.0c/s 167.0c/s rockie..surfing
5g 0:00:00:18 83% 0.2714g/s 151.1p/s 177.1c/s 177.1c/s Johnson..buzz
5g 0:00:00:22 100% 0.2267g/s 160.8p/s 182.5c/s 182.5c/s !@#%..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
cisco@ubuntu:~/Downloads/john-1.8.0/run$
```

Equipment

Lab PC Hardware Requirements

- Computer with a minimum of 2 GB of RAM and 8 GB of free disk space, 1 Virtual Machine used
- High speed Internet access to download Oracle VirtualBox and the virtual machine image file
- Packet Tracer

Aktionsplan für Cybersecurity Essentials

- Erstellen einer Self-Enroll-Seite mit dem Logo der Schule. Veröffentlichung und Verbreitung des Links
- Mails, Aushänge, News, Infos auf Webseite

MMBBS – CYBERSECURITY SUMMER SCHOOL 2018

Herzlich Willkommen zu unseren Kursen zur Selbststeinschreibung. Aus dem Cisco Networking Academy Kurs Portfolio bietet die MMBbS ab jetzt für alle Schüler Kurse zur Selbststeinschreibung an.

Einführungskurse:

MMBBS - Intro to Packet Tracer - SJ 2018/19

MMBBS - NDG Linux Unhatched - SJ 2018/19

MMBBS - Introduction to Cybersecurity - SJ 2018/19

MMBBS - Introduction to IoT - SJ 2018/19



MMBBS - Cybersecurity Essentials - SJ 2018/19

Multi-Media Berufsbildende Schulen Hannover

Multi-Media Berufsbildende Schulen
Regionales Bildungszentrum für die Medien- und
IT-Berufsausbildung in der Region Hannover



Course Details

MMBBS - Cybersecurity Essentials - SJ 2018/19
Cybersecurity Essentials (German v1.0)
8 July 2018 - 9 July 2019
Joachim Kemmies, Almut Leykauff-Bothe

Description

Herzlich Willkommen zu „CyberSecurity Essentials“!

Durch den Kurs „Cybersecurity Essentials“ entwickeln Sie ein grundlegendes Verständnis für Cybersicherheit und wie diese mit Informations- und Netzwerksicherheit in Beziehung steht. Die charakteristischen Merkmale von Cyberkriminellen werden analysiert und deren Taktiken beleuchtet. Darüber hinaus stellt der Kurs die Technologien, Ansätze und Verfahren vor, mit denen Cybersicherheitsexperten Cyber-Kriminalität bekämpfen.

Der **englischsprachige Kurs** der Cisco Networking Academy umfasst rund 30 Stunden Online-Lerninhalte. Zusätzlich gibt es interaktive Übungen, die das erworbene Wissen unterstützen, Videos, Spiele und Quizze sowie simulationsbasierte Lernaktivitäten mit PacketTracer, um die Lösung komplexer Probleme zu trainieren.

Die **Teilnahme ist kostenfrei** nach Anmeldung unter „Sign up now“ auf der rechten Seite und Aktivierung Ihrer Anmeldung durch Bestätigung des AnmeldeLinks, welchen Sie per E-mail erhalten.

Enroll Now

leykauff-bothe@mmbbs.de

Submit

[Link zur Selbststeinschreibung](#)



Lernsituation an der MMBbS

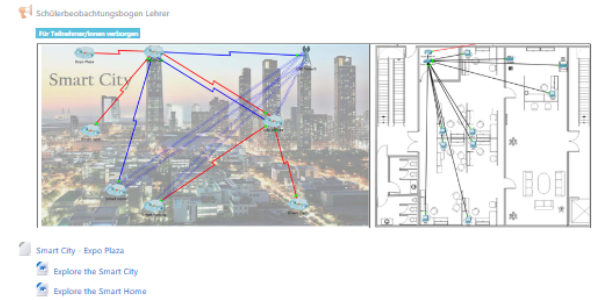
LF7: Vernetzte IT-Systeme 2.AJ - LB - SJ 18-19

Grundlagen der Cybersicherheit

Lernsituation 7.19

Grundlagen der Cybersicherheit

Konzepte und praktische Umsetzungen für Cybersicherheit, einschließlich Informationssicherheit, Systemsicherheit, Netzwerksicherheit, Ethik und Gesetze sowie Verteidigungs- und Entschärfungstechniken, die zum Schutz von Unternehmen eingesetzt werden.



Netzwerkgrundlagen Einführung Teil 1

Fig. 1: Einführung/Übersicht über

Lernsituation 7.8

CCNA Routing and Switching: Introduction to Networks

Chapter 7: IP Addressing

Chapter 8: Subnetting IP Networks

Chapter 10: Application Layer

Netzwerkgrundlagen Einführung Teil 2

Fig. 1: Einführung/Übersicht über

Lernsituation 7.9

CCNA Routing and Switching: Introduction to Networks

Chapter 5: Ethernet

Chapter 6: Network Layer

Chapter 9: Transport Layer

Windows Server 2016 - Konzeption, Installation und Konfiguration

Lernsituation 7.18

Windows Server 2016

Aufbau und Verwaltung eines Netzwerks

Windows Server 2016 installieren, Einführung in Active Directory; Domänencontroller installieren und neue Domänen erstellen; DNS und Namensauflösung; Active Directory Konten verwalten; Gruppen, Dateidienste einrichten; Drucker verwalten; Benutzerprofile verwalten; Server überwachen; Software Updates mit WSUS.

Grundlagen der Cybersicherheit

Lernsituation 7.19

Grundlagen der Cybersicherheit

Konzepte und praktische Umsetzungen für Cybersicherheit, einschließlich Informationssicherheit, Systemsicherheit, Netzwerksicherheit, Ethik und Gesetze sowie Verteidigungs- und Entschärfungstechniken.

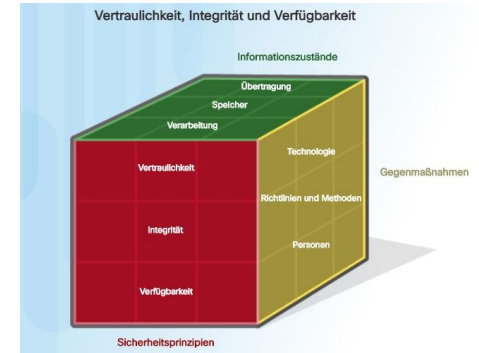
Umsetzung Cybersecurity Essentials an den BBS ROW

- deutlich umfangreicher als Introd. to Cybersec
- deutlich höheres Niveau, für Informations-technische Assistenten zunächst nicht geeignet
- ABER: als Abschluss am Jahresende für diese Schulform sehr gut geeignet
- es gibt geringe Doppelungen mit dem Intro-Kurs – aber durch den langen Zeitraum zwischen den beiden Kursen fällt das gar nicht so auf...



Vorteile Cybersecurity Essentials

- kompakte und spannende LABs
- sehr viele der behandelten Themen aus LF 5 werden aufgegriffen und erweitert:
Serverfunktionen, Linux, Absicherung eines Geräts, VPN-Tunnel anwenden, Verschlüsselung, Hash-Verfahren, uvm.
- der Kurs passt am Ende des Jahres sehr gut vom Niveau her zu dieser Schulform



CCNA Security



CCNA Security 2.0 Course Outline

Course Chapters and Goals

Chapter 1	Modern Network Security Threats Goal: Explain security threats in modern network infrastructures and how to mitigate them.
Chapter 2	Securing Network Devices Goal: Secure Cisco routers.
Chapter 3	Authentication, Authorization and Accounting Goal: Implement AAA on Cisco routers using local router database and server-based ACS or Identity Service Engine (ISE).
Chapter 4	Implementing Firewall Technologies Goal: Implement firewall technologies to secure network perimeter.
Chapter 5	Implementing Intrusion Prevention Goal: Implement IPS to mitigate attacks on networks.
Chapter 6	Securing the Local Area Network Goal: Secure endpoints and mitigate common Layer 2 attacks.
Chapter 7	Cryptographic Systems Goal: Secure communications to ensure integrity, authenticity and confidentiality.
Chapter 8	Implementing Virtual Private Networks Goal: Implement secure Virtual Private Networks.
Chapter 9	Implementing the Cisco Adaptive Security Appliance (ASA) Goal: Implement an ASA firewall configuration using the CLI.
Chapter 10	Advanced Cisco Adaptive Security Appliance (ASA) Goal: Implement an ASA firewall configuration and VPNs using ASDM.
Chapter 11	Managing a Secure Network Goal: Test network security and create a technical security policy.

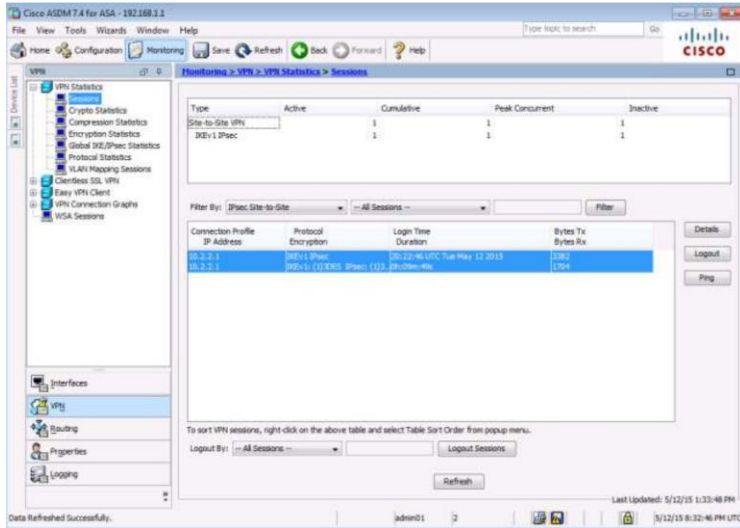
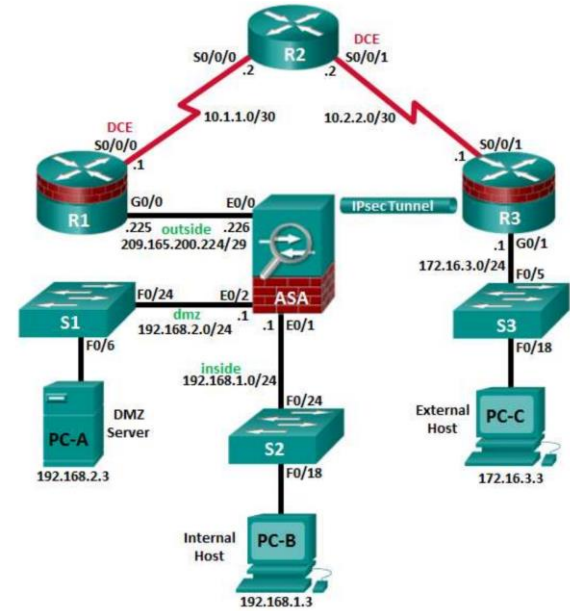
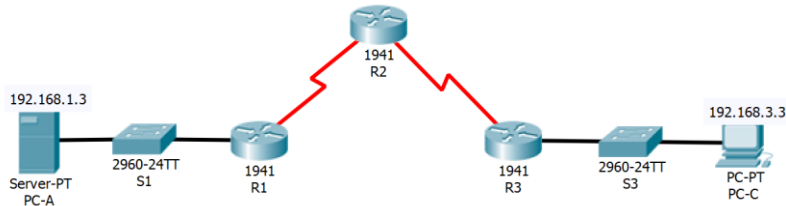
CCNA Security 2.0 Key Competencies

Upon completion of this course, students will be able to:

- Describe security threats facing **modern network infrastructures**
- Secure **Cisco routers and switches**
- Describe **AAA** functionalities and implement AAA on Cisco routers using local router database and server-based **ACS** or **ISE**
- Mitigate threats to networks using **ACLs and stateful firewalls**
- **Implement IPS and IDS** to secure networks against evolving attacks
- Mitigate threats to email, web based and endpoints attacks and common Layer 2 attacks
- Secure communications to ensure integrity, authenticity and confidentiality
- Describe the purpose of VPNs, and **implement** Remote Access and **Site-to-Site VPNs**
- Secure networks using **Cisco ASA**



Labs



```
R1(config)# crypto isakmp policy 10
R1(config-isakmp)# hash sha
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 14
R1(config-isakmp)# lifetime 3600
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# end
```

Equipment

Qty	Product Number	Description
3	ISR4221-SEC/K9	Cisco ISR 4221 SEC Bundle with Security License (SL-4220-SEC-K9)
	Or ISR4321-SEC/K9	Cisco ISR 4321 Sec bundle w/SEC license
	Or ISR4331-SEC/K9	Cisco ISR 4331 Sec bundle w/SEC license
3	NIM-2T=	2-Port Serial WAN Interface card
3	CAB-SS-V35MT=	V.35 Cable, DTE Male to Smart Serial, 10 Feet
3	CAB-SS-V35FC=	V.35 Cable, DCE Female to Smart Serial, 10 Feet
3	WS-C2960+24TC-L	Catalyst 2960 Plus 24 10/100 + 2T/SFP LAN Base
1	ASA5506-K9	ASA 5506-X with FirePOWER services, 8GE, AC, 3DES/AES
	ACS-4220-RM-19=	19 inch rack mount kit for Cisco ISR 4220

What's in it for me?

CCNA Security enables students:

- Understand core security concepts and how to develop and **implement** security policies to mitigate risks
- **Configure, monitor, and troubleshoot** network security
- Prepare for the Cisco CCNA Security **Certification** exam
- Develop themselves as network and security engineer



CCNA Security an der MMBbS

WFK: CCNA Security

Kursangebot Schuljahr 2018/2019 für das
3. Ausbildungsjahr

CCNA Security

Kurszeiten: **Donnerstags** von 15:20 – 20:30
01.11., 08.11., 15.11., 22.11., 29.11., 06.12.,
13.12.2018 und 10.01.2019

CCNA Security Career Ready



Kursübersicht

Das CCNA Security-Curriculum behandelt die wichtigsten Sicherheitstechnologien sowie die Installation, Fehlerbehebung und Überwachung von Netzwerkgeräten, die die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Geräten gewährleisten.

MMBbS Kurs

FISI16_Do –
CCNA Security



[Link zu den
Kurszeiten](#)



Features

Zielgruppe : FachinformatikerInnen Systemintegration der MMBbS

Voraussetzungen : CCNA R&S: ITN and RSE (CCENT)

Sprache : Englisch

Kosten : 130 €

Kursart : Präsenzkurs, Instruktor geführt

Geschätzter Zeitaufwand : 70 Stunden

Empfohlener nächster Kurs : CCNA Cybersecurity Operations





CCNA Cyber Ops Kursdesign

Course Structure: CCNA Cyber Ops

Chapter	Title	Theme	Student Profile
1	Cybersecurity and the Security Operations Center	Introduction	
2	Windows Operating System	OS Fundamentals	Students with ITE, Linux Essentials knowledge
3	Linux Operating System		
4	Network Protocols and Services	Networking Fundamentals	Students with CCNA R&S (ITN) knowledge
5	Network Infrastructure		
6	Principles of Network Security	Cybersecurity Fundamentals	Students with Cybersecurity Essentials and CCNA Security knowledge
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 Ops

Course Design

- Easy-to-navigate graphical user interface
- 13 chapters, modifiable chapter quizzes and chapter exams
- 13 terms & concepts practice quizlets
- 13 chapters containing accessible text and media text
- 54 interactive activities
- 45 hands-on labs (27 labs use VM)
- 5 Cisco Packet Tracer activities, require PT 7.x or above
- 1 skills-based assessment
- 2 certification practice exams
 - 1x 210-250 SECFND
 - 1x 210-255 SECOPS
- 1 practice final exam and final exam
- Accessibility compliant to WCAG 2.0 AA level
- Certificate of Completion, Letter of Merit
- Certification voucher



CCNA Cyber Ops

Equipment Requirements

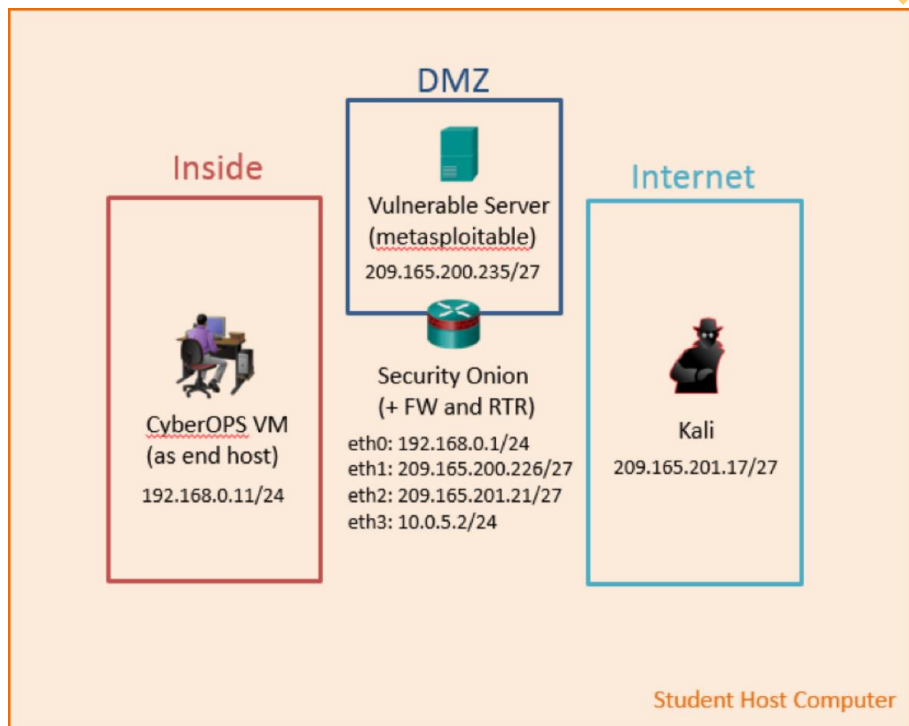
Curriculum requirements: 1 student PC per student (recommended), at most 2 students per PC

Platform	Description
Computer	<ul style="list-style-type: none">• OS: Any• Processor: Intel Core i7 4600U 2.7GHz (with Virtualization Support)• Memory: 8 gigabyte (GB) RAM (standard) or 4 GB RAM (alternative option)• Display Adapter: PCI, <u>PCIe</u> (recommended), or AGP video card (DirectX 9 graphics device with WDDM driver)• Disk: 45 GB hard drive (minimum). 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 <u>VirtualBox</u>	The latest version
Windows Experience Index (WEI)	6.5 (recommended)
Packet Tracer	Min. Version 7.0

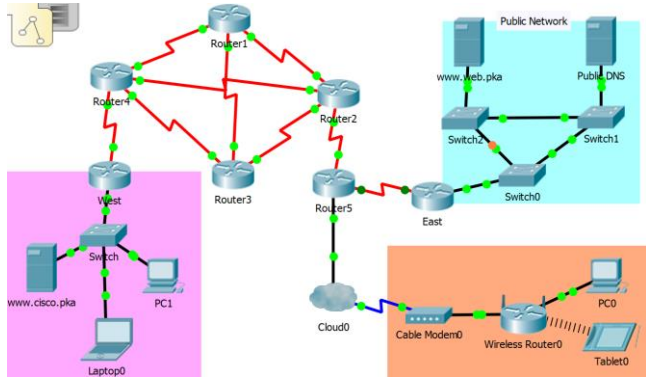
CCNA Cyber Ops

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 (standard)



Labs



httpdump.pcap [Wireshark 2.2.3]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
124	10.252422	10.0.2.15	65.61.137.117	HTTP	514	[TCP Previous segment not captured]
138	10.332405	65.61.137.117	10.0.2.15	HTTP	761	HTTP/1.1 200 OK (text/html)
181	13.298897	10.0.2.15	65.61.137.117	HTTP	675	POST /bank/login.aspx HTTP/1.1
185	13.472733	65.61.137.117	10.0.2.15	HTTP	611	HTTP/1.1 302 Found (text/html)
187	13.476894	10.0.2.15	65.61.137.117	HTTP	579	GET /bank/main.aspx HTTP/1.1
195	13.603919	65.61.137.117	10.0.2.15	HTTP	171	HTTP/1.1 200 OK (text/html)

In the lower window, the message is displayed. Expand the **HTML Form URL Encoded: application-www-form-urlencoded** section.

▶ Frame 181: 675 bytes on wire (5400 bits), 675 bytes captured (5400 bits)

▶ Ethernet II, Src: PcsSystem_21:f3:5c (08:00:27:21:f3:5c), Dst: RealtekU_12:35:02 (52:54:00:12:35:02)

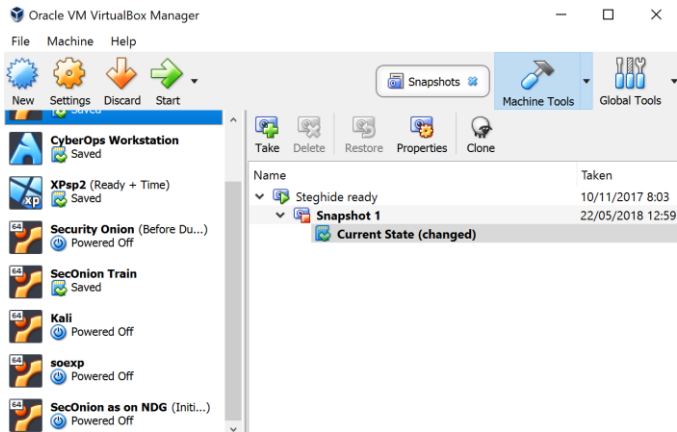
▶ Internet Protocol Version 4, Src: 10.0.2.15, Dst: 65.61.137.117

▶ Transmission Control Protocol, Src Port: 58652, Dst Port: 80, Seq: 462, Ack: 8988, Len: 621

▶ Hypertext Transfer Protocol

▶ HTML Form URL Encoded: application-www-form-urlencoded

Labs



ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	73	seconion-...	3.57	2017-07-25 14:39:20	192.168.0.11		192.168.0.11
RT	73	seconion-...	3.58	2017-07-25 14:39:20	192.168.0.11		192.168.0.11
RT	27	seconion-...	5.5713	2017-07-31 19:22:00	209.165.200.235		192.168.0.11
RT	27	seconion-...	5.5714	2017-07-31 19:22:00	209.165.200.235		192.168.0.11
RT	76	seconion-...	5.5767	2017-07-31 19:23:09	209.165.201.17		209.165.201.17
RT	76	seconion-...	5.5723	2017-07-31 19:23:09	209.165.201.17		209.165.201.17
RT	67	seconion-...	7.5725	2017-07-31 19:25:01	192.168.0.11		209.165.201.17
RT	67	seconion-...	7.5726	2017-07-31 19:25:01	192.168.0.11		209.165.201.17
RT	5	seconion-...	1.4162	2017-07-31 19:33:07	0.0.0.0		0.0.0.0
RT	1	seconion-...	3.722	2017-09-07 15:31:12	192.168.0.12	50450	93.114.4.114
RT	1	seconion-...	3.723	2017-09-07 15:31:13	192.168.0.12	50457	173.201.1.1
RT	28	seconion-...	3.724	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.11
RT	28	seconion-...	3.725	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.11
RT	28	seconion-...	3.732	2017-09-07 15:31:15	192.99.198.158	80	192.168.0.11
RT	12	seconion-...	3.772	2017-09-07 15:31:20	192.99.198.158	80	192.168.0.11
RT	1	seconion-...	3.784	2017-09-07 15:31:23	192.168.0.12	50474	208.113.1.1
RT	1	seconion-...	3.785	2017-09-07 15:31:23	192.168.0.12	50474	208.113.1.1

seconion-eth0-1_728

File

Sensor Name: seconion-eth0-1
 Timestamp: 2017-09-07 15:31:15
 Connection ID: seconion-eth0-1_728
 Src IP: 192.168.0.12 (Unknown)
 Dst IP: 192.99.198.158 (Unknown)
 Src Port: 50467
 Dst Port: 80
 OS Fingerprint: 192.168.0.12:50467 - Windows XP/2000 (RFC1323, w+, tstamp) [GENERIC]
 OS Fingerprint: Signature: [8192:128:1:52:M1460,N,W2,N,N,S,;:Windows:7]
 OS Fingerprint: -> 192.99.198.158:80 (distance 0, link: ethernet/modem)

SRC: GET /3xdz3bcx8 HTTP/1.1
 SRC: Accept: text/html,application/xhtml+xml,*/*
 SRC: Referer: http://lifeinsidedetroit.com/02024870e4644b68814aadfb58a75bc.php?e=8bd3799ee8799332593b0b9caa1f426
 SRC: Accept-Language: en-US
 SRC: User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
 SRC: Accept-Encoding: gzip, deflate
 SRC: Host: qwe.mvduanalterableairreport.net
 SRC: Connection: Keep-Alive
 SRC:
 DST: HTTP/1.1 200 OK
 DST: Server: nginx/1.2.1
 DST: Date: Thu, 04 Dec 2014 18:27:33 GMT
 DST: Content-Type: text/html
 DST: Transfer-Encoding: chunked
 DST: Connection: keep-alive
 DST: Cache-Control: no-cache, must-revalidate, max-age=1

```
msf > search 234
```

Name	Disclosure Date	Rank	Description
auxiliary/scanner/http/bavision_cam_login		normal	BAVision IP Camera Web Server Login
auxiliary/scanner/http/coldfusion_locale_traversal		normal	ColdFusion Server Check
auxiliary/server/pxeexploit		normal	PXE Boot Exploit Server
exploit/linux/misc/hp_vsa_login_bof	2013-06-28	normal	HP StorageWorks P4000 Virtual SAN Appliance Login
exploit/multi/browser/java_jre17_reflection_types	2013-01-10	excellent	Java Applet Reflection Type Confusion Remote Code Execution
exploit/multi/misc/java_jmx_server	2013-05-22	excellent	Java JMX Server Insecure Configuration Java Code Execution
exploit/unix/ftp/vsftpd_234_backdoor	2011-07-03	excellent	VSFTPD v2.3.4 Backdoor Command Execution
exploit/unix/webapp/basilic_diff_exec	2012-06-28	excellent	Basilic 1.5.14 diff.php Arbitrary Command Execution
exploit/unix/webapp/clipbucket_upload_exec	2013-10-04	excellent	ClipBucket Remote Code Execution
exploit/windows/brightstor/lgservers	2007-01-31	average	CA BrightStor ARCserve for Laptops and Desktops LGServers Remote Code Execution
exploit/windows/browser/mcafeevisualtrace_tracetarget	2007-07-07	normal	McAfee Visual Trace ActiveX Control Buffer Overflow
exploit/windows/browser/novelliprint_getdriversettings_2	2010-11-15	normal	Novell iPrint Client ActiveX Control Buffer Overflow

NIST
 National Institute of Standards and Technology
 U.S. Department of Commerce

Special Publication 800-61
 Revision 2

Computer Security Incident Handling Guide

Jobs for Security Specialists

CCNA Security

(“doing” things)

- Network Security Specialist
- Security Administrator
- Network Security Support Engineer



CCNA CyberOps

(“watching” things)

- Security SOC Analyst
- Incident Responder
- Cyber Security and Privacy Analyst





Erfahrungsaustausch

Erfahrungsaustausch und Ideen für den Einsatz im Unterricht im
Bereich Fachinformatiker und Wirtschaftsinformatik



Erfahrungsaustausch

Wahlpflichtkurse MMBbS 2.-3. AJ IT-Berufe

6 Blöcke a 4 Stunden

Es wird das CCNA Cybersecurity Operations online Curricula aus der Cisco Networking Academy zur Verfügung gestellt

Notwendige Vorkenntnisse

Das der Kurs als Blended Learning ausgeführt wird, ist ein hohes Maß an Eigenmotivation für die E-Learning Phasen notwendig.

In der Präsenzphase wird es größten Teils um die Umsetzung gehen, daher sind Kenntnisse in den Betriebssystemen Windows und Linux, sowie in der Netzwerkinfrastruktur notwendig.

Es werden englisch sprachigen Unterlagen genutzt

Aufgabe 9.3

 Verschlüsseln und Entschlüsseln von Daten mit einem Hacker-Tool

Ein großes Unternehmen setzt Unternehmensrichtlinie für Wechselmedienarbeiten um. Im konkreten Fall dürfen nur gezippte Dokumente verschlüsselt auf USB-Sticks kopiert.

- 9.1.1.7 Verschlüsseln und Entschlüsseln von Daten mit einem Hacker-Tool

Aufgabe 9.4

 Telnet und SSH in Wireshark untersuchen

Topology



Konfigurieren Sie im Labor einen Router, der SSH-Konnektivität akzeptiert, und verwenden Wireshark, um Telnet- und SSH-Sitzungen zu erfassen und anzuzeigen. Das Labor finden Sie hier: [Lab - Examining Telnet and SSH in Wireshark](#)

Aufgabe 9.5

 Zertifizierungsstelle

Mit der Entwicklung des Internets entwickelte sich auch das Bedürfnis nach Sicherheit. Heute werden immer noch das von Netscape bereits 1994 eingeführte HTTPS und das Konzept der Zertifizierungsstellen verwendet.

- Auflisten der Zertifikate auf Ihrem Laptop
- Man-in-Middle auf Ihrem Laptop prüfen

In Anlehnung an 9.2.2.7 Lab - Certificate Authority Store



Erfahrungsaustausch

Wahlpflichtfach

Studiengang
Wirtschaftsinformatik
CCNA Cyber Ops

CCNA <u>Cyber Ops</u>								
Kontaktstunden (KS):	80 Std.	Studienabschnitt:	5. und 6. Semester (Sem)		ECTS (CP):	8 CP		
Selbstlernzeit (SZ):	160 Std.	Lehrformen:	Ü/N/E-Learn		Gewichtung:	4%		
<u>Workload</u> (WL):	240 Std.	Voraussetzung:	Studiengang Wirtschaftsinformatik		<u>Modultyp</u> :	Wahlpflicht		
Modulverantwortung:	Prof. Dr. Norbert Gülke				Angebotsfrequenz:	>jährlich<		
Name der Veranstaltung	Sem	CP	KS	SZ	WL	Prüfung		Gewichtung für Modulnote
						Art	Sem	
A CCNA Cybersecurity Operations <u>Teil 1</u>	5	4	40	80	120	Online Exam Hands On Skill Exam	5	50 %
B CCNA Cybersecurity Operations <u>Teil 2</u>	6	4	40	80	120	Online Exam Hands On Skill Exam	6	50 %



Erfahrungsaustausch

Idee

CCNA CyberOps als Klammer über alle 3 AJ

für den Fachinformatiker Systemintegration ??



Erfahrungsaustausch

CCNA Cybersecurity Operations

The student has successfully achieved student level credential for completing CCNA Cybersecurity Operations course administered by the undersigned instructor. The student was able to proficiently:

- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the Windows Operating System and Linux Operating System features and characteristics needed to support cybersecurity analyses.
- Explain the operation of network infrastructures.
- Analyze the operation of network protocols and services.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Use various methods to prevent malicious access to computer networks, hosts, and data.
- Explain the impacts of cryptography on network security monitoring.
- Explain how to investigate endpoint vulnerabilities and attacks.
- Evaluate network security alerts.
- Analyze network intrusion data to identify vulnerabilities and compromised hosts.
- Explain how security incidents are handled by CSIRTs.



Erfahrungsaustausch

Zuordnung zu den Lernfeldern

LF4 - Einfache IT-Systeme

LF7 - Vernetzte IT-Systeme

LF10 - Betreuung IT-Systeme

aus dem Rahmenlehrplan für den Fachinformatiker Fachrichtung Systemintegration
Stand 25.April 1997

-> Idee: [CCNA CyberOps als Klammer über alle 3
Ausbildungsjahre](#)



Erfahrungsaustausch

ToDo ?





Cisco CyberOps Skills Challenge Game

Cyber Ops Skills Challenge Game

The Cyber Ops Skills Challenge game is an optional activity that allows students to use their skills and knowledge to compete with other students. It consists of two VMs. A classroom server VM and a client VM for game players and game administration. Instructions for installing and administering the game are provided in the Instructor Guide.

Instructions for playing the game are included in the Student Guide.

[Server VM](#)

[Client VM](#)

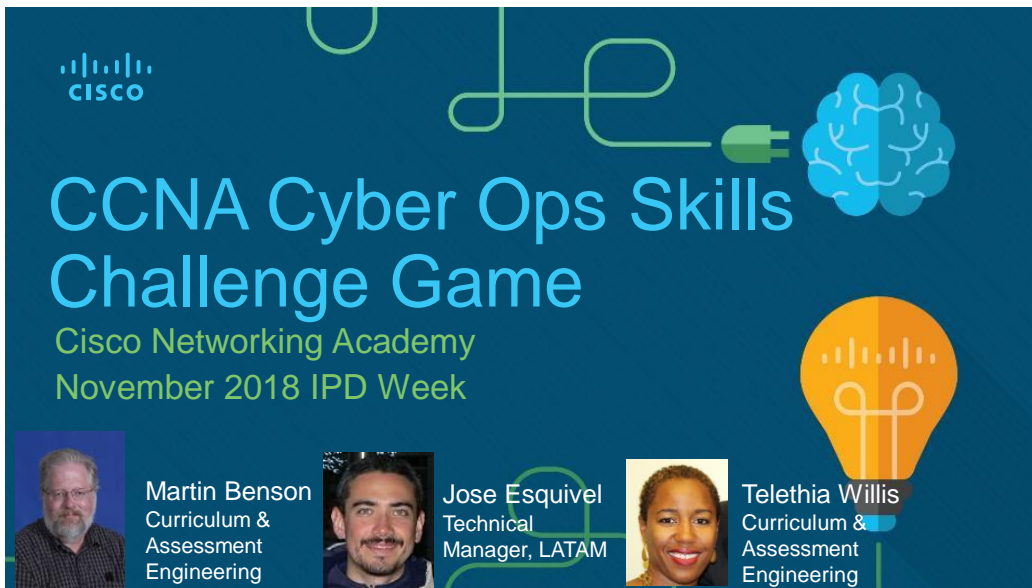
[Instructor Guide](#)

[Student Guide](#)


[Skills Challenge Game FAQ](#)



Cisco CyberOps Skills Challenge Game





The banner features a dark blue background with the Cisco logo in the top left. A green line graphic starts from the top center, loops around, and ends in a green plug icon connected to a blue brain icon. Below the brain is an orange lightbulb icon with a white filament and a Cisco logo inside. The main text is in light blue and green. At the bottom, there are three portrait photos of the organizing team members, each with their name and title.




CCNA Cyber Ops Skills Challenge Game

Cisco Networking Academy
November 2018 IPD Week

 **Martin Benson**
Curriculum & Assessment Engineering

 **Jose Esquivel**
Technical Manager, LATAM

 **Telethia Willis**
Curriculum & Assessment Engineering



Almut Leykauff-Bothe, MMBbS Hannover

Stefan Krieger BBS Rotenburg