Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik

INFORMATIONSBLATT ZUM

Cisco CCNA Cybersecurity Operations

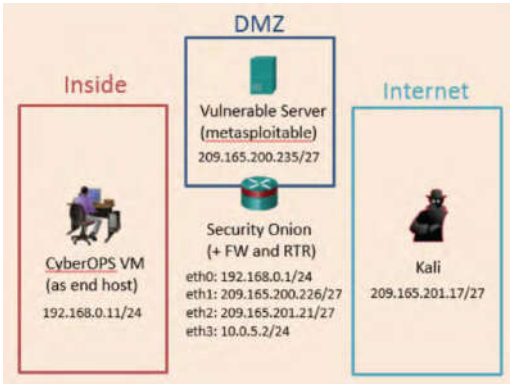
Der CCNA Cybersecurity Operations Fachkurs wird im Stil des "blended learning" abgehalten. Neben Präsentationen des Dozenten werden begleitete und selbstständige praktische Aufgaben innerhalb einer Simulationsumgebung (ggf. auch an realer HW im Labor) sowie Online-Selbststudium zur Vertiefung der Theorie mittels eines CBTs (Computer –based-trainings) mit ergänzenden kurzen Online-Tests zu den jeweiligen Themen durchgeführt.
Abgeschlossen wird der Kurs mit einem praktischen Test innerhalb der Academy Umgebung.

Das CBT ist über die Networking Academy Seite (https://www.netacad.com) erreichbar, Sie werden auf dieser Plattform erfasst (falls noch nicht) und erhalten ein persönliches Login.

Zudem kriegen Sei Zugriff auf eine virtuelle Simulationsumgebung (siehe Bild), welche aus bis zu 4 VMs besteht und welche Sie auf Ihrem persönlichen Laptop installieren können. Empfohlen wird dabei folgende Hardware/Software Mindestausstattung:

- OS: Windows 7, 8, or 10, MAC OSX
- Processor: 64-bit processor with Virtualization Support
- Memory: 8 Gigabyte RAM - mehr ist besser!!
- Disk: 45 GB hard drive.
- Network: 1 Ethernet Card or 1 Wireless Ethernet Card

Als Virtualisierungssoftware wird Oracle VirtualBox eingesetzt.



Behandelte Themen innerhalb des Kurses

Modul	Lerninhalte
Chapter 1. Cybersecurity and the Security Operations Center	• Explain the role of the Cybersecurity Operations Analyst in the enterprise. • Explain why networks and data are attacked. • Explain how to prepare for a career in Cybersecurity operations.
Chapter 2. Windows Operating System	• Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses. • Explain the operation of the Windows Operating System. • Explain how to secure Windows endpoints.
Chapter 3. Linux Operating System	• Explain the features and characteristics of the Linux Operating System. • Perform basic operations in the Linux shell. • Perform basic Linux administration tasks.
Chapter 4. Network Protocols and Services	• Analyze the operation of network protocols and services. • Explain how the Ethernet and IP protocols support network communications and operations • Explain how network services enable network functionality.
Chapter 5. Network Infrastructure	• Explain network topologies and the operation of the network infrastructure.

	• Explain how network devices enable wired and wireless network communication. • Explain how devices and services are used to enhance network security.
Chapter 6. Principles of Network Security	• Classify the various types of network attacks. • Explain how networks are attacked. • Explain the various types of threats and attacks.
Chapter 7. Network Attacks: A Deeper Look	• Use network monitoring tools to identify attacks against network protocols and services. • Explain network traffic monitoring. • Explain how TCP/IP vulnerabilities enable network attacks. • Explain how common network applications and services are vulnerable to attack.
Chapter 8. Protecting the Network	• Use various methods to prevent malicious access to computer networks, hosts, and data. • Explain approaches to network security defense. • Use various intelligence sources to locate current security threats.
Chapter 9. Cryptography and the Public Key Infrastructure	• Explain the impacts of cryptography on network security monitoring. • Use tools to encrypt and decrypt data. • Explain how the public key infrastructure (PKI) supports network security.
Chapter 10. Endpoint Security and Analysis	• Explain endpoint vulnerabilities and attacks investigation process. • Use tools to generate a malware analysis report. • Classify endpoint vulnerability assessment information.
Chapter 11. Security Monitoring	• Evaluate network security alerts. • Explain how security technologies affect security monitoring. • Explain the types of log files used in security monitoring.
Chapter 12. Intrusion Data Analysis	• Analyze network intrusion data to identify compromised hosts and vulnerabilities • Explain how security-related data is collected. • Analyze intrusion data to determine the source of an attack.
Chapter 13. Incident Response and Handling	• Explain how network security incidents are handled by CSIRTs. • Apply incident response models, such as NIST 800-61r2 to a security incident. • Use a set of logs to isolate threat actors and recommend an incident response plan.

Alle Unterlagen, Laboranleitungen sowie das Online-Training sind in englischer Sprache gehalten und werden als PDF auf dem ILIAS der Schule zur Verfügung gestellt.

Nach Abschluss des Kurses steht Ihnen die Option offen, in einem offiziellen Testcenter (zu finden unter https://home.pearsonvue.com/cisco.aspx): den Cisco Certifikatstest **SECOPS 210-255** zu absolvieren.

Literatur

Grundlagenbuch und Einstieg – empfehlenswert für „Neulinge“:
CCNA Cyber Ops SECFND 210-250 Cert Guide: ISBN-13: 978-1-58714-702-9
(Link wo man dieses Buch im PDF Format runterladen kann (inoffiziell):
http://dl.hellodigi.ir/dl.hellodigi.ir/dl/book/CCNA%20Cyber%20Ops%20SECFND%20%23210-250%20Official%20Cert%20Guide.pdf)

Buch welches Cyber Sec Ops Themen behandelt (“Kursbuch“):
CCNA Cyber Ops SECOPS 210-255 Cert Guide: ISBN-13: 978-1-58714-703-6

(Link wo man dieses Buch im PDF Format runterladen kann (inoffiziell): https://builder.pearsonitcertification.com/Content/Product/1C536901-82BD-4765-B8BC-6690ECE3A45C/9780134608921_LogIn.pdf)

Links

Weitere Informationen zum Kurs
https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna-cyber-ops.html

Fragen?

Falls Sie noch Fragen oder Unklarheiten zu diesem Fachkurs haben sollten bitte einfach bei mir nachfragen.

Dozent: Peter Infanger Email: peter.infanger@hslu.ch