ISACA Cybersecurity Fundamentals (ITCA)

This ITCA - Cybersecurity Fundamentals training covers how to perform the basic, professional tasks required of an entry-level IT professional in a cybersecurity capacity. Although earning the ITCA Cybersecurity Fundamentals certification is valuable for cybersecurity hopefuls, the training is also excellent for non-IT professionals and teams who need a well-rounded understanding of the threats that exist in the modern world, how best to avoid them, and what to do if there is a successful attack against your network.

CBT Nuggets course material →

STUDY PLAN

WEEK 1

Defining Security and its Roles — 157 min.

IT Security	11
Information and Communications Technology (ICT)	7
Network Security	6
Cybersecurity	7
Specialized Systems	7
Validation	4

Roles, Governance, Continuity, and Recovery

Cybersecurity Roles	9
Resilience	6
Continuity and Recovery	6
Recovery Time and Point Objectives	5
Backup Location	3
Backup Media	7
Backup Types	9
Validation	7

CIA, Least Privilege, and Privacy

CIA: Confidentiality	8
CIA: Integrity	8
CIA: Availability	8
Principle of Least Privilege	10
Personal and Private Info	12
Validation	6

Threat Landscape

Threat Risk, Sources, Categories	11

WEEK 2

152 min.

Internal Risk (Insider Risk)	7
Insider Risk: Shadow IT	9
Emerging Threats	6
Threat Modeling	5
Vulnerabilities and Exploits	4
Validation	5

Motivations, Agents, and the Attack Sequence

Motivations and Agents	8
Reconnaissance and Entry	19
Foothold, Escalation, and Discovery	11
Lateral Movement, C2, and Exfiltration	8
Validation	1

Malware and its Symptoms

Types of Malware	11
Even More Types of Malware!	14
Live Discovery of Drive-By Malware	4
Camera and Microphone Hijacking	8
Symptoms of Malware	14
More Symptoms of Malware	10
Demonstration of Unauthorized Installation	3
Validation	5

WEEK 3

Common Attack Methods Part 1

151 min.

Advanced Persistent Threat (APT)	8
Back Door	5
Brute Force	10
Rainbow Tables and Password Spraying	5
Buffer Overflow	3
Covert Channels	5
Steganography Demonstration	9

Common Attack Methods Part 2

Cross-Site Scripting (XSS)	7
Denial of Service and Man-in-the-Middle	11
Social Engineering	10
Additional Attacks	13
SQL Injection and Validation	9

Risk Management

Addressing Risk and Criteria	10
Third-Party Risk	16
SolarWinds Case Study: Introduction	5
SolarWinds Cast Study: Attack Details	17
Validation	4

Regulatory Requirements, The Modern Perimeter

Standards Organizations	4

WEEK 4

153 min.

General Data Protection Regulation	4
PCI DSS and PSD2	5
HIPPA	6

Zero Trust	4
The Internal and External Perimeters	3
The Internet Perimeter	10
Validation	7

Network Security Controls

The Demilitarized Zone (DMZ)	7
Virtual Local Area Network (VLAN)	8
Switch Communication	5
Router Communication	4
WiFi Security with Wired Equivalency Protocol (WEP)	4
WiFi Protected Access (WPA) WPA2, WPA3	7
Securing a WiFi Access Point	12
Validation	4

Understand Firewall Functions

Basic Firewall Functions	10
Types of Firewalls	9
Hardware Firewalls	8
Application Firewalls	4
Next Generation Firewalls (NGFW)	7
Validation	7

Endpoint Firewalls and Windows Firewall

Endpoint Protection	3
Windows Firewall Default Settings	8
Allow an Application Through Windows Firewall	7

WEEK 5

165 min.

Configure Specific Firewall Settings	12
Use GPO to Apply Firewall Rules	8
Validation	12

Mac/Linux Firewalls and IDS/IPS

Azure Firewall	1
Mac Firewall	1
Linux Firewall Configuration	1
Linux Firewall Automation	1
Understanding Intrusion Detection Systems	1
Understanding Intrusion Prevention Systems	1

AAA Controls

What Are Endpoint Devices?	4
Authentication Controls	18
Authorization Controls	24
Accounting Controls	13
Validation	1

Cloud Services

Understand Cloud Computing from a Local Perspective	9
CAPEX vs OPEX, and Defining the Cloud	5
NIST Cloud Characteristics	9
Microsoft Cloud Layout	4
Explore Cloud Datacenters	11
Validation	9

Cloud Security and Models

Cloud Security Benefits	4
Cloud Security Risks and Recommendations	16

WEEK 6

153 min.

IaaS PaaS and SaaS	11
Public, Private, Hybrid, Community Cloud	7
Create an Azure VM	14
Validation	3

Data Security

Database Security	20
Data Classification	14
Data at Rest, in Motion, and in Use	4
Protecting Data via Timely Updates	11
Validation	3

Symmetric Encryption

Encryption Introduction	7
Where is Your Data	6
Symmetric Encryption	4
The Case for Symmetric Encryption	10
Symmetric Algorithms	9
Validation	15

Asymmetric Encryption, Hashing, Digital Signatures

Understand Asymmetric Encryption	5
Asymmetric Encryption Flow	2
Asymmetric Encryption Algorithms	8

WEEK 7

153 min.

Hashing Data	16
Digital Signatures	3
Validation	4

PKI and Applying Cryptography

Public Key Infrastructure (PKI)	8
TLS Transaction Flow	10
Virtual Private Networks (VPN)	8
VPN Features and Disadvantages	10
Secure Shell (SSH)	4
Validation	9

Security Operations and Vulnerability Management

What is a Security Operations Center (SOC)?	4
SOC Models	7
SOC Staff	12
SOC Areas of Responsibility	15
Vulnerability Management	8
Validation	3

Penetration Testing and EDR

Penetration Testing Overview	3
Pen Test Phase: Plan and Discover	16
Pen Test Phase: Attack and Report	5
Dangers of Pen Testing	8

WEEK 8

155 min.

Endpoint Detection and Response	8
Validation	7

Incident Response and Digital Forensics

SIEM and SOAR	13
Incident Response, Handling, and Phases	6
Incident Response Plan	6
Digital Forensics Investigations	2
Where is the Evidence?	11
Preserving Evidence	12
Chain of Custody	4
Validation	1

Network Command-Line Tools

PING	9
Traceroute	6
ARP	8
IPCONFIG, ifconfig and ip addr	6
Route and iptables	10
Validation	4

Penetration Testing Tools

nmap	6
SSH	6
hashcat	8
Crack Windows Passwords	10
Generate Hashes	4
Capture Network Traffic with Wireshark	8

WEEK 9 **56 min.**

Validation	4

Concluding Tools and Techniques

Netstat and SS	8
Pathping and MTR	9
NSLOOKUP	4
Netcat	10
Sysinternals Suite	18
Windows "god mode"	2
Validation	1