SEC301 or SEC401

Comparing Two Cyber Security Starting Points

SEC301: Introduction to Cyber Security

AND/OR

SEC401: Security Essentials - Network, Endpoint, and Cloud

Cyber Security Expertise – Where Should You Begin?

Choosing the right starting point based on your Prior Knowledge.

SEC301 About the Authors SEC401

Keith Palmgren

- 37+ Years in Cyber Security
- Air Force, AT&T, Sprint, NetIP
- Senior SANS Instructor
- CISSP, GCIF, GSEC, GCED, GCIH, GSLC, CEH, Security+, Network+, A+, CTT+
- Author: 24 courses including SEC301, numerous articles, awareness training videos, etc.

Bryan Simon

- 31+ Years in IT/Cyber Security
- Education, Environmental, Financial, Government Sectors
- GIAC: GSEC, GCWN, GCIH, GCFA, GPEN, GWAPT, GAWN, GISP, GCIA, GCED, GCUX, GISF, GMON, CISSP
- Technical Editor / Author: numerous books and courses

Both Have Deep Cyber Security Prior Knowledge!

SEC301 & SEC401 – The Students

New To Security

The Manager

Law Enforcement

(Cyber focused or not)

The difference – What is their Prior Knowledge?

SEC301 Prior Knowledge (1) SEC401

If you have **basic computer skills**:

- No formal IT training beyond
  - Send / Receive email & attachments
  - Create and print documents
  - Internet searches – Google, etc.
  - Make purchases from an ecommerce site
- Know basic computer terminology

If you already have **basic IT skills:**

- Convert binary & hexadecimal
- Know basic networking
  - Default gateway
  - LAN, WLAN
  - WiFi and Bluetooth
- Basic virtualization skills
- Know basic cyber security terminology

SEC301 Prior Knowledge (2) SEC401

If you know none of these:

- ➢ SEC301 Defines & Explains all of them and more

If you know the basics of these:

- ➢ SEC401 Assumes they are Prior Knowledge

AV*EF=SLE*ARO=ALE

NAT/PAT

FTPS

VPN

DHCP

IPSec

SSH

HTML

DNS

LAN

HTTP&HTTPS

TCP & UDP & ICMP

Lecture Topics

SEC301	SEC401
Cyber Management – Core Principles, Risk, & Policy	Defensible Network Architecture & Packet Analysis
Authentication / Authorization / Accountability	Wireless & Wired Network Security Measures
Computer Function and Networking	Cloud Security (AWS & Azure)
Introduction to Cryptography	Applying Cryptography
Wireless / Mobile / IoT	Identity, Access, & Password Management
Common Attacks & Malware	Advanced Attacks and Malware
Cyber Security Technologies	Red, Purple, & Blue Team
Browser Security	Data Loss Prevention & Incident Response
System Security - Virtual/Cloud/Backup/Patching	Windows, Linux, Mac, Mobile, Virtual, Containers

SEC301 – 9 Labs Lab Topics SEC401 – 19 Labs

SEC301 – 9 Labs	SEC401 – 19 Labs
Lab and Resource Familiarity	Application Control via Allow-Listing
Real-World Passwords	Cracking Passwords (Windows & Linux)
Converting Number Systems	Network Scanning
Decoding Network Traffic - Wireshark Intro	Network Traffic Analysis – Wireshark & tcpdump
Performing Cryptography	Cryptography Tools
Visual Cryptography	Intrusion Detection
Configuring Wireless	Cracking Wireless
Anti-Malware Scanning	Malicious Software
Building Firewalls	Windows Security Tools & PowerShell

SEC301 & SEC401 – Where Will We Take You?

Five years from today, I want to do “X”.

Tell us what your “X” is!

We will help you choose YOUR best entry point on the path to that expertise.

SEC301 or SEC401

Comparing Two Cyber Security Starting Points

SANS

SEC301: Introduction to Cyber Security

AND/OR

SEC401: Security Essentials - Network, Endpoint, and Cloud

Cyber Security Expertise – Where Should You Begin?

Choosing the right starting point based on your Prior Knowledge.