Skills Exercise: Communication & Network Security

This material is prepared for use in *Communication & Network Security* and was prepared by Henrik Kramselund, `xhek@kea.dk`.

These course and exercises are expected to be performed in a training setting with network connected systems, but what are the pre-requisites?!

As we go through the exercises today, try to focus on pre-requisites and skills needed.

- ☐ What are some technical skills needed?
- ☐ Do you need knowledge of specific platforms? (operating systems, application platforms)
- ☐ Do you need knowledge and skills about specific work flows?
- ☐ Is programming a requirement? is scripting? – what is the difference?

Security wise we also have presented a lot of terms, concepts, systems, which ones help with security?

- ☐ Does basic skills in an area help you secure it? (loaded question I think)
- ☐ How do we ensure that we know enough within each area?
- ☐ Which are the most important areas within information security?
- ☐ Which areas require specialist skills?
- ☐ Do you need to know about cloud to work in information security?

Do NOT look at the next pages yet!

Skills Exercise: Communication & Network Security

Baseline Skills

- Threat-Centric Security, NSM, and the NSM Cycle
- TCP/IP Protocols
- Common Application Layer Protocols
- Packet Analysis
- Windows Architecture
- Linux Architecture
- Basic Data Parsing (BASH, Grep, SED, AWK, etc)
- IDS Usage (Snort, Suricata, etc.)
- Indicators of Compromise and IDS Signature Tuning
- Open Source Intelligence Gathering
- Basic Analytic Diagnostic Methods
- Basic Malware Analysis

Source: *Applied Network Security Monitoring Collection, Detection, and Analysis*, Chris Sanders and Jason Smith

Skills Exercise: Communication & Network Security

Security engineering a job role

On any given day, you may be challenged to:

- Create new ways to solve existing production security issues
- Configure and install firewalls and intrusion detection systems
- Perform vulnerability testing, risk analyses and security assessments
- Develop automation scripts to handle and track incidents
- Investigate intrusion incidents, conduct forensic investigations and incident responses
- Collaborate with colleagues on authentication, authorization and encryption solutions
- Evaluate new technologies and processes that enhance security capabilities
- Test security solutions using industry standard analysis criteria
- Deliver technical reports and formal papers on test findings
- Respond to information security issues during each stage of a projects lifecycle
- Supervise changes in software, hardware, facilities, telecommunications and user needs
- Define, implement and maintain corporate security policies
- Analyze and advise on new security technologies and program conformance
- Recommend modifications in legal, technical and regulatory areas that affect IT security

Source: `https://www.cyberdegrees.org/jobs/security-engineer/`
also `https://en.wikipedia.org/wiki/Security_engineering`