Introduction to IT & Cybersecurity
Module 1

System Administration

Part 1

System Administration is responsible for a system or specific components of a system

- Install, configure, and maintain hardware and software
- Perform regular backups and data recovery as needed
- Provide Technical support to users

KSAs

- Reporting & Communication
- Server and client OS
- Enterprise IT architecture
- Identifung server performents, configuration and availability issues
- Directory services (LDAP, Active Directory ...)
- Customer Service

Part 2

Tools it depends on where you work but these are the major ones

- Wireshark: it's very good to identify Network Activity and errors
- Powershell / Terminal
- Sysinternals
- RDP / SSH
- MMC
- etc

Typical Day:

- Ticket systems
- Communication with users
- Basic troubleshooting
- Maintenance & Recovery
- Direct Support
- Disaster Preparedness/Recovery

Job Prospects

- Median Pay : $81,100
- 6% year over year growth

Common Certifications :

- A+
- Network +
- Security +
- LPIC System Administrator
- Server +

Network Engineering

Part 1

Network Engineer is responsible for building, maintaining and protecting networks and it's the next step for SysAdmins

- Analyze design and requirement documents from different departments and then make appropriate changes to network topology.
- Operate network services and systems, to include hardware and virtual environments.

KSAs:

- Reporting & Communication
- Operating network equipment
- Networking concepts, protocols and network security methodologies (OSI, TCP/IP)
- Analyzing network traffic
- Protecting Networks
- Laws, Regulations, and standards to follow

Part 2

Tools:

- Wireshark : To analyze Network Traffic
- Commands : tracert, ping, nslookup, ipconfig, netsat
- Speedtest.net
- IP calculator
- puTTY
- Network performance / analyzer tools

Typical Day :

- Reviewing logs : it's the huge part
- Rebooting devices
- Fixing issues
- Backups : Very Important , Always Back it up
- ACLs, VPNs
- Documentation to always stay organize with the Network

Part 3

Job Prospects:

- $55,000- 200,000
- $70,000-85,000

Common Certifications:

- Network + : Entry Level
- MCSA : Entry Level
- MCSE
- CCNA : Entry Level
- CCNP
- PCNSE

Incident Responder & Forensics Investigator

Part 1

Incident Response & Forensics is responsible for identifying and responding incidents.

- Follow a standard process to analyze data to determine if an incident occurred, the severity of the incident occured, the severity of the incident, mitigation of the incident and assess the effectiveness , mitigation
- Use forensic tools to harvest data for civil, administrative, and criminal investigations.

KSAs:

- Reporting & Communication
- Networking concepts, protocols, and network security methodologies
- Cyber threat and vulnerabilities
- Incident response and handling methodologies
- Laws and Regulations
- Preserving evidence integrity

Part 2

Tools:

- OSSIM
- Snort
- OpenVAS
- OCS Inventory
- SIFT

Typical Day:

- Risk assessments
- Abnormal system behavior
- Suspicious activity
- SOC Analyst

Job Prospects:

- $99,000

Common Certifications:

- ECIH
- GCIH
- CEIH
- CHFI
- CDFE

Offensive Security and Penetration Testing

Part 1

Penetration Tester is Responsible for identifying security gaps an vulnerabilities by emulating threat actors

- Perform security analysis against the networks of anything from small non-profits to multinational corporations.
- Use a combination of technical and social approaches to find weaknesses in the target organization, then document and provide remediation options for those weakneses.

KSAs:

- Communication & Reporting
- Network Protocols and Engineering
- Common OS
- Vulnerabilities & Vulnerability Develelopment
- Social Engineering
- Security standards

Part 2

Tools:

- Kali
- Metasploit
- Wireshark
- Zed Attack Proxy
- Aircrack-ng
- Cain
- etc

Typical Day:

- Client meetings
  - Establish Rules of Engagement
  - Discuss goals
  - Sign a whole bunch of paperwork

- Initial assessment
  - Broad but shallow

- Targeted attacks
  - Based on assessments
  - Problem solving & Critical Thinking

Job Prospects :

- Median Salary : $78,000
- 18-28% year over job growth
- Private and Public sector availabilities

Common Certification :

- SEC +
- CEH
- CPT
- LPT
- Pentest +
- GPEN
- CISSP
- OSCP

Module 2: System Administration

Lesson 1

Different Names:

- Tech Support
- Database Admin
- Network Admin
- Security Admin

What does a SysAdmin do ?

- Determines technical needs
- Install, maintain, upgrade and repair hardware and software
- Evaluate and optimize performance, security, and survivability
- Create, manage, and train users
- Follow and enforce policies and regulations
- Solve problems related to the items above

Determine Technical Needs ?

- Most people don't understand technology
- Most organizations aren't aware of potential technical solutions
- Your job is to understand the needs and be able to provide options

Install. Maintain. Upgrade. Repair.

- After you identify solutions, you have to implement them
- Track devices and products in your enterprise, keep them in working order
- Triage issues and determine solution paths, then implement

Performance. Security. Survivability

- Backups, backups, and more backups
  - Daily differential
  - Weekly Full-system
  - Monthly tape
- CIANA
  - Confidentiality
  - Integrity
  - Authentication

    - Non-Repudiation
    - Availability

Lesson 2

Create, manage, and train users

- IT is often one of the first, and one of the last, groups to interact with employees
- User roles are essential to security and performance
- People really don't understand technology

Policies and Regulations

- Organizational Policies
    - Password requirements
    - Data retention/destruction
    - Acceptable use
- Regulations
    - Consumer Protection
    - Encryption
    - Data retention /destruction

Problem Solving!

- Your Primary Job.
- Think on your feet
- Be prepared
- Stay Calm

Lesson 3

Where will you work ?

- Everywhere
    - Tech companies
    - Finance
    - Hospitals
- Usually office conditions but there are exceptions

How do you become a SysAdmin ?

Traditionally, you'll want a Bachelor's degree in something compsci-related
However, you can supplement or even avoid certs and experience !

- A+
- Network+
- Sec+
- CCNA

How much will you make ?

- Salaries can vary widely between $70k and $90k is the average

Lesson 4

Tools :
If you ask 10 sysadmins what tools you need, you'll get 10 different answers.

- Sysinternals- it is a suite of tools,
- Powershell
- Wireshark
- Microsoft Management Console (MMC)

Lesson 5

Wireshark

- The gold standard in packet-capture tools. -
- It has been around for many years and has become the standard

Really practice and learn this tool. It will be one of the most valuable assets
Microsoft Management Console (MMC)

- The one-stop-shop for all Microsoft built-ins

This is another tool that will be a valuable asset for Windows. Learn well.

Module 3: Network Engineering

Lesson 1

Differents Names:

- Network & Computer Systems Admin
- Network Architect
- Wireless Network Engineer

What does a Network Engineer do ?

- Determine network topology
- Configure, operate and maintain network equipment
- Evaluate network traffic and performance
- Backups
- Regulation and Policies
- Security
- Troubleshooting

Determine Network topology

- Manually
- Nmap
- SolarWinds Network Topology Mapper
- Lansweeper

Configure, operate and maintain network equipment

- Router - Switch - Modems - Cables - Bridges
- WAP - Firewalls - Proxy servers

Lesson 2

Evaluate network traffic and performance
- SolarWinds
- Wireshark
- Capsa

Backups
- Incremental
- Differential
- Full

Policies & Regulations
- Network Security Policy
  - Data encryption
  - Data retention/destruction
  - Acceptable use and access
- Regulation
  - GDPR (General Data Protection Regulation)
  - HB-1128 (Colorado)

Security
- C.I.A
- DLP
- Firewall
- Antivirus/Antimalware
- IDP/IPS
- Honeypots
- Segmentation
- Separation of duties

Lesson 3

Troubleshooting
- ping
- tracert/traceroute
- ipconfig/ifconfig
- nslookup
- netstat

Where can you work ?
- FInancial
- Healthcare
- Manufacturing
- Technology
- Government

How do you Become A Network Engineer ?
Traditionally, you'll want a Bachelor's degree in Computer Networking or CS. However, you can supplement or even avoid that with certs and experience!
- Network+
- CCNA
- MTA Networking Fundamentals
- AWS
- Azure
- Google Cloud

Many people start working Help Desk then gradually works towards network engineering.

How much will you make ?
- Salaries can vary widely, but between $70k and $85k is the average

Module 4: Incident Response and Forensics

Lesson 1

SOC Analyst - Job responsibilities :

- Monitor critical systems for security threats
- Analyze logs and reports to provide threat intelligence
- Perform Incident Response and triage
- Investigate security threats and breaches

Lesson 2

The process to Incident Response

- Preparation
- Detection and Analysis
- Containment
- Eradication and Recovery
- Post-Incident Activity

SOC Analyst- Work Environment

Security watchfloor

- Any hours are possible , 24/7
- often work rotating shifts
- Emergency response

On-site IR/Forensics

- Corporate clients
- Criminal cases

SOC Analyst is a 24/7 is more the discovery of intrusion. A Forensic investigator is about details after the intrusion. The who, what, when. where, why and how. Both use the same tools with different goals to an intrusion.

Lesson 3

Becoming a SOC Analyst

- Often a Bachelor's Degree
- CHFI, CEH, CySA+
- Public sector / law enforcement

SOC Analyst salary

- $45k-$99k
  Some Federal Contractors can make over $120K with a security clearance.

Analyst tools

- HEX editors
- Forensic Toolkits
- SIEMS
- Threat Intelligence Tools
- Reporting Mechanisms

Module 5: Offensive Security & Penetration Testing

Lesson 1

What does a Pentester do ?

Emulate threat actors in order to identify and remediate security gaps

- Perform security analysis against organizations
- Establish physical, social, and technological approaches to defeating security, then design solutions to those attacks
- Maintain awareness of new vulnerabilities and mitigations
- Way more paperwork than you think

Lesson 2

What is Threat Emulation ?

When providing analysis for an organization, you have to take a similar approach to the hacker. Study the weaknesses.

- Organizational weaknesses
  - Bad/no policies
  - Untrained employees
- Physical weaknesses
  - No entry controls
  - Unlocked/unmonitored doors
- Technological weaknesses

CYA: Cover Your Assets

- Your day job is violating half dozen federal and internal laws.
  - That sounds very cool, but practically it means that any lapse in authorization or documentation could lead to serious consequences.
- Before operations, you'll establish a scope of work, sign NDA's and more.
- During operations, you meticulously document every action you take and ensure it can be undone. Do Not Take Down A Production Environment.
- After operations, you'll provide a thorough report and No Trophy Taking.

Job Prospects

- Median Salary: $79,888
- 18-28% year-over-year job growth (Bureau of Labor Statistics)
- Work can be:
  - On-site
  - Remote
  - In offices
  - Stores
  - Anywhere a vulnerability might exist.

Lesson 3

How to become a Pentester ?

There aren't many official programs.

Cets go a long way

- CEH
- Pentest +
- LPT
- OSCP

Practice, Practice, Practice

The Pentesting Process :

- Reconnaissance
  - Google-hacking-database
- Scanning
  - Nmap
- Gaining Access
  - Creating a reverse Shell
- Maintaining Access
  - Schedule jobs
- Covering Tracks
  - Clearing event logs, clearing bash history

You will document, document and document. You really need to write well. Many of your reports are reviewed by levels of management.