Security+ Network Crash Course - Detailed Instructor Notes

Pre-Session Setup (5 min before student arrives)

- Have whiteboard/screen ready for drawing
- Prepare to show: OSI model diagram, basic network topology
- Have port number handout ready to give at end

Opening (2 minutes)

Say to student:
"Alright, so here's the deal - normally Network+ gives you weeks to learn this stuff, but we need to compress it into what you absolutely need for Security+. The good news? Sec+ doesn't require you to configure networks, just understand how they work and where security fits in. So we're going to focus on recognition and concepts, not deep technical implementation. Sound good?"

Set expectations:
"I'm going to throw a lot of terms at you today. Don't worry about mastering everything - just get familiar. The Sec+ exam will test whether you can identify what something is and where it belongs, not configure it from scratch."

PART 1: OSI MODEL & TCP/IP (15 minutes)

Introduction to the OSI Model (8 min)

[DRAW on whiteboard as you talk - 7 layers stacked]

Say:
"The OSI model is like the 'theory' of how networks communicate. It's a 7-layer framework that breaks down network communication into chunks. Security+ will reference this constantly when talking about where attacks happen or where security controls sit."

Draw and label all 7 layers:

```
7 - Application
6 - Presentation
5 - Session
4 - Transport
3 - Network
2 - Data Link
1 - Physical
```

Teaching tip: Use mnemonic: "**P**lease **D**o **N**ot **T**hrow **S**ausage **P**izza **A**way"

Now explain layer by layer - focus on 2, 3, 4, 7:

Layer 1 - Physical:
"This is the actual wire, fiber optic cable, radio waves. The physical stuff. Bits traveling as electrical signals."

Security callout: "Wiretapping happens here."

Layer 2 - Data Link: ⭐ IMPORTANT FOR SEC+

"This is where **MAC addresses** live. Every network card has a unique MAC address - think of it like a serial number burned into the hardware."

Key concept: "Switches operate at Layer 2. They use MAC addresses to figure out which port to send data to."

Security callout: "MAC filtering, ARP spoofing, and CAM table attacks happen here. You'll see these in Sec+."

Example: "When your laptop connects to a switch, the switch learns 'Oh, MAC address AA:BB:CC:DD:EE:FF is on port 3' and remembers that."

Layer 3 - Network: ⭐ CRITICAL FOR SEC+

"This is the **IP address** layer. Layer 3 is about routing - getting data from one network to another network."

Key concept: "**Routers** operate at Layer 3. They look at IP addresses to decide where to send packets."

Draw quick diagram:

```
[Network A: 192.168.1.0] <--Router--> [Network B: 192.168.2.0]
```

Say: "The router looks at the destination IP address and says 'This packet needs to go to Network B' and forwards it."

Security callout: "Firewalls often operate at Layer 3, filtering based on IP addresses. Ping sweeps, IP spoofing - all Layer 3 attacks."

Layer 4 - Transport: ⭐ CRITICAL FOR SEC+

"This is where **TCP and UDP** live. This layer handles how data gets transported - reliably or unreliably."

TCP (Transmission Control Protocol):

- Connection-oriented (handshake first)
- Reliable (guarantees delivery, retransmits if packets lost)
- Slower but accurate
- **Example:** Web browsing, email, file transfers

Use this analogy: "TCP is like certified mail - you get a receipt confirming it arrived."

UDP (User Datagram Protocol):

- Connectionless (just sends, no handshake)
- Unreliable (fire and forget, no guarantee)
- Faster but might lose packets
- **Example:** Streaming video, VoIP, DNS queries, gaming

Use this analogy: "UDP is like throwing a paper airplane across the room - fast, but might not make it."

Security callout: "Firewalls filter at Layer 4 based on **port numbers**. You'll need to memorize tons of port numbers for Sec+. SYN floods are a Layer 4 attack."

Layer 5 - Session:

"Manages sessions between applications - establishing, maintaining, terminating connections. Honestly, you won't see this tested much in Sec+."

Layer 6 - Presentation:

"Data formatting, encryption/decryption, compression. Converts data into a format the application can use."

Security callout: "SSL/TLS encryption happens here, so it's relevant to Sec+, but they won't ask you detailed Layer 6 questions."

Layer 7 - Application: ⭐ IMPORTANT FOR SEC+

"This is where users interact. Web browsers, email clients, FTP programs."

Say: "All those protocols you need to memorize - HTTP, HTTPS, FTP, SSH, DNS - they're all Layer 7."

Security callout: "Most attacks target Layer 7: SQL injection, XSS, DDoS attacks. Web Application Firewalls (WAFs) protect Layer 7."

TCP/IP Model (4 min)

Say: "The OSI model is theoretical. In the real world, we use the **TCP/IP model** - it's simpler, just 4 layers."

[DRAW next to OSI model]

```
TCP/IP Model          OSI Equivalent
--------------        --------------
Application    <-->   Application, Presentation, Session (7,6,5)
Transport      <-->   Transport (4)
Internet       <-->   Network (3)
Network Access <-->   Data Link, Physical (2,1)
```

Say: "See how it maps? TCP/IP just combines some layers. When you hear 'Layer 3' or 'Layer 4,' people are using OSI terminology even though we're really using TCP/IP in practice."

Key takeaway: "For Sec+, know both models exist, but focus on understanding what happens at each layer security-wise."

Quick Check-In Question (3 min)

Ask: "If I said 'firewall filtering by IP address,' what layer is that?"

- **Answer:** Layer 3 / Network layer

Ask: "If I said 'firewall filtering by port number,' what layer?"

- **Answer:** Layer 4 / Transport layer

Ask: "MAC address filtering?"

- **Answer:** Layer 2 / Data Link

PART 2: IP ADDRESSING (15 minutes)

IPv4 Basics (7 min)

Say: "IP addresses are like mailing addresses for computers. IPv4 uses 4 numbers separated by dots."

Write on board: `192.168.1.100`

Explain:
"Each number is called an **octet** (8 bits), ranges from 0-255. So an IP address is 32 bits total."

Private vs Public IP Addresses: ⭐ CRITICAL

Say: "There are two types of IP addresses you need to know:"

Private IP ranges (memorize these!):

- `10.0.0.0` to `10.255.255.255` (10.0.0.0/8)
- `172.16.0.0` to `172.31.255.255` (172.16.0.0/12)
- `192.168.0.0` to `192.168.255.255` (192.168.0.0/16)

Say: "Private IPs are used inside your home or business network. They're NOT routable on the internet - meaning if you try to send a packet to 192.168.1.1 from across the internet, routers will drop it."

Public IP addresses:
"Everything else. These ARE routable on the internet. Your router at home has a public IP that your ISP gave you."

Security callout: "Private IPs are more secure because they're not directly accessible from the internet. This is why we use **NAT**..."

NAT (Network Address Translation): ⭐ IMPORTANT

Draw diagram:

```
[Private Network]                [Internet]
Device 1: 192.168.1.10 ----\
Device 2: 192.168.1.11 -----[Router/NAT]---- Public IP: 24.5.67.89
Device 3: 192.168.1.12 ----/
```

Explain:
"NAT translates private IPs to public IPs. All your home devices use private IPs, but when they talk to the internet, the router translates them to its single public IP."

Say: "From the internet's perspective, all requests look like they're coming from one address. NAT provides security through obscurity - attackers can't directly see or target your internal devices."

Security callout: "NAT is NOT a firewall, but it provides a security benefit. For Sec+, know what NAT does and that it hides internal network structure."

Subnet Masks & CIDR Notation (5 min)

Say: "Subnet masks tell you which part of an IP address is the 'network' and which part is the 'host.' You'll see these in Sec+ but won't have to do complex subnetting math."

Write on board:

```
IP Address:     192.168.1.100
Subnet Mask:    255.255.255.0
```

Explain:
"The 255s say 'this part is the network.' So `192.168.1` is the network, and `.100` is the specific host on that network."

CIDR Notation:
"Shorthand for subnet masks. You'll see `/24`, `/16`, `/8`."

Write equivalents:

- `/8` = `255.0.0.0` (Class A - huge networks)
- `/16` = `255.255.0.0` (Class B - medium networks)
- `/24` = `255.255.255.0` (Class C - small networks, most common)

Say: "When you see `192.168.1.0/24`, that means all addresses from `192.168.1.0` to `192.168.1.255` are on the same network. That's 254 usable addresses."

Security callout: "Subnetting is used for **network segmentation** - splitting networks into smaller pieces for security. More on that later."

IPv6 Quick Overview (3 min)

Say: "IPv4 is running out of addresses - only 4 billion possible. IPv6 solves this."

Write on board: `2001:0db8:85a3:0000:0000:8a2e:0370:7334`

Say: "IPv6 addresses are 128 bits (vs IPv4's 32 bits). They're written in hexadecimal with colons. You don't need to memorize this format deeply for Sec+, just recognize it."

Key differences:

- Vastly more addresses (340 undecillion)
- No more NAT needed (every device can have a public IP)
- Built-in IPSec support

Security callout: "IPv6 is more secure by design, but many networks still run IPv4 or dual-stack. Attackers can exploit IPv6 if it's enabled but not monitored. For Sec+, just know IPv6 exists and offers more security features."

PART 3: PROTOCOLS & PORTS (20 minutes)

[This is the MOST IMPORTANT section for Sec+]

Introduction (2 min)

Say: "Alright, this next section is critical. Sec+ will absolutely hammer you with questions like 'What port does HTTPS use?' or 'Which protocol is unencrypted?' You need to memorize these cold."

Explain what a port is:
"Think of an IP address as a building address, and ports as apartment numbers. Port numbers tell the computer which application should handle the incoming data."

Write on board:

- Ports 0-1023: **Well-known ports** (standard services)
- Ports 1024-49151: **Registered ports** (vendor-specific)
- Ports 49152-65535: **Dynamic/ephemeral ports** (temporary)

Say: "You need to know the well-known ports. Let's go through them by category."

Web Protocols (3 min)

HTTP - Port 80 ⭐⭐⭐

- Hypertext Transfer Protocol
- Unencrypted web traffic
- **Security issue:** Everything sent in plaintext - passwords, data, cookies

HTTPS - Port 443 ⭐⭐⭐

- HTTP over SSL/TLS
- Encrypted web traffic
- **Security:** This is what you want. Look for the padlock in browsers.

Say: "Memorize these two ports. 80 is the old insecure web, 443 is secure web. Sec+ will test this constantly."

Remote Access Protocols (4 min)

Telnet - Port 23 ⭐⭐

- Remote terminal access
- **UNENCRYPTED** - sends passwords in cleartext
- **Security:** Never use Telnet. It's outdated and dangerous.

SSH - Port 22 ⭐⭐⭐

- Secure Shell
- **ENCRYPTED** remote access
- Also used for SFTP (secure file transfer)
- **Security:** This is what replaced Telnet. Always use SSH.

Say: "Telnet is 23, SSH is 22. Remember: SSH is one less than Telnet, and infinitely more secure. You'll see questions contrasting these."

RDP - Port 3389 ⭐⭐

- Remote Desktop Protocol (Microsoft)
- Graphical remote access (vs SSH's command line)
- Encrypted by default, but often misconfigured
- **Security:** RDP is a common attack target. Sec+ will ask about hardening RDP.

File Transfer Protocols (5 min)

FTP - Ports 20/21 ⭐⭐

- File Transfer Protocol
- Port 21 for commands, port 20 for data
- **UNENCRYPTED**
- **Security:** Credentials and files sent in cleartext. Don't use.

SFTP - Port 22 ⭐⭐⭐

- SSH File Transfer Protocol (uses SSH)
- **ENCRYPTED** file transfer
- **Security:** This is the secure way to transfer files. Same port as SSH.

FTPS - Ports 989/990 ⭐

- FTP over SSL/TLS
- Port 989 for data, 990 for control

- **ENCRYPTED**
- Less common than SFTP
- **Security:** Secure, but SFTP is more widely used.

Say: "Remember the pattern: protocols ending in 'S' are usually secure. HTTPS, SFTP, FTPS, LDAPS, etc. If there's no S, assume it's unencrypted and insecure."

Draw a comparison table:

```
Protocol   | Port       | Encrypted? | Status
-------------------------------------------
FTP        | 20/21      | NO         | ❌ Don't use
SFTP       | 22         | YES        | ✅ Use this
FTPS       | 989/990    | YES        | ✅ OK but less common
```

Email Protocols (3 min)

SMTP - Port 25 ⭐⭐

- Simple Mail Transfer Protocol
- For **sending** email (outgoing)
- Unencrypted by default
- Secure version: SMTPS (Port 587 or 465)

POP3 - Port 110 ⭐⭐

- Post Office Protocol v3
- For **receiving** email
- Downloads email to device and deletes from server
- **UNENCRYPTED**
- Secure version: POP3S (Port 995)

IMAP - Port 143 ⭐⭐

- Internet Message Access Protocol
- For **receiving** email
- Keeps email on server, syncs across devices
- **UNENCRYPTED**
- Secure version: IMAPS (Port 993)

Say: "For Sec+, know that SMTP sends, POP3 and IMAP receive. POP3 downloads and deletes, IMAP keeps on server. All three are unencrypted by default - their secure versions use different ports."

Network Services (3 min)

DNS - Port 53 ⭐⭐⭐

- Domain Name System
- Translates domain names (google.com) to IP addresses
- Uses UDP for queries (fast), TCP for zone transfers
- **Security:** DNS poisoning, DNS amplification attacks, DNS tunneling for data exfiltration

Say: "DNS is like the phone book of the internet. You type 'google.com,' DNS tells your computer it's actually 142.250.80.46."

DHCP - Ports 67/68 ⭐⭐

- Dynamic Host Configuration Protocol
- Automatically assigns IP addresses to devices
- Port 67 for server, 68 for client
- **Security:** DHCP spoofing attacks, rogue DHCP servers

Say: "When you connect to Wi-Fi and automatically get an IP address, that's DHCP working. Sec+ will test you on DHCP attacks where attackers run fake DHCP servers."

Directory Services (2 min)

LDAP - Port 389 ⭐⭐

- Lightweight Directory Access Protocol
- Queries directory services (like Active Directory)
- **UNENCRYPTED**

LDAPS - Port 636 ⭐⭐

- LDAP over SSL
- **ENCRYPTED** directory queries
- **Security:** Used for secure authentication lookups

Say: "LDAP is how computers talk to Active Directory to check 'Is this user allowed to log in?' LDAPS is the secure version."

Other Important Ports (1 min)

SMB - Port 445 ⭐⭐

- Server Message Block
- Windows file sharing
- **Security:** Common target for ransomware (WannaCry, NotPetya)

Say: "Port 445 should be blocked at your firewall. It's how ransomware spreads on networks."

Quick mention others:

- **SNMP - Port 161** (network device management)
- **RDP - Port 3389** (already covered)
- **SQL - Port 1433 (MS SQL)** or **3306 (MySQL)**

Memorization Strategy (1 min)

Hand out port number flashcard list

Say: "You MUST memorize these. I'm giving you a list. Make flashcards. For the next two weeks before Sec+ prep starts, drill yourself daily. The exam will give you scenarios like 'An attacker is scanning port 3389 - what are they targeting?' Answer: RDP."

Emphasize: "Focus on: 22, 23, 25, 53, 80, 110, 143, 443, 3389, 445. Those are the most tested."

PART 4: NETWORK DEVICES & SECURITY (10 minutes)

Core Network Devices (5 min)

Switch - Layer 2 Device ⭐⭐⭐

Say: "Switches connect devices within a network. They operate at Layer 2, using MAC addresses."

How it works:
"When Device A sends data to Device B on the same network, the switch looks at the MAC address and forwards it only to Device B's port. It doesn't broadcast to everyone."

Security features:

- **Port security:** Limit which MAC addresses can connect to a port
- **VLANs:** Virtually segment the network (more in a moment)

Security risks:

- MAC flooding attacks
- ARP spoofing

- CAM table overflow

Router - Layer 3 Device ⭐⭐⭐

Say: "Routers connect different networks together. They operate at Layer 3, using IP addresses."

How it works:
"Your home router connects your private network (192.168.1.x) to the internet. It looks at destination IP addresses and forwards packets between networks."

Security features:

- Basic packet filtering (ACLs)
- NAT (already covered)

Firewall - Layer 3/4 Device ⭐⭐⭐

Say: "Firewalls are security devices that control traffic. They're like bouncers - they decide what gets in and what gets out."

Types:

1. **Packet-filtering firewall:** Looks at IP addresses and ports (Layers 3-4)
2. **Stateful firewall:** Tracks connections, understands if traffic is part of an established session
3. **Next-gen firewall (NGFW):** Deep packet inspection, application awareness, IPS integration

Draw diagram:

```
[Internal Network] <--Firewall--> [Internet]
      ALLOW                       BLOCK
```

Say: "Firewalls use rules. Example: 'Allow HTTPS (443) from internal to external, but block Telnet (23) in both directions.'"

Security Devices (5 min)

IDS vs IPS ⭐⭐⭐ CRITICAL FOR SEC+

Say: "This is a huge Sec+ topic. They'll definitely test you on the difference."

IDS - Intrusion Detection System:

- **Passive monitoring** - watches traffic, alerts if suspicious
- Does NOT block anything
- **Analogy:** A security camera - sees the crime, raises alarm, but doesn't stop it

IPS - Intrusion Prevention System:

- **Active blocking** - watches traffic, blocks suspicious activity automatically
- In-line with traffic (traffic flows through it)
- **Analogy:** A security guard - sees the crime and stops it

Draw diagram:

```
IDS (passive):
Traffic -----> [Network] -----> [IDS monitors/alerts]

IPS (active):
Traffic -----> [IPS blocks threats] -----> [Network]
```

Key differences table:

```
Feature      | IDS                | IPS
-------------------------------------------------
Position     | Out-of-band        | In-line
Action       | Alert only         | Block + Alert
Risk         | False neg allowed  | False pos breaks traffic
```

Say: "IDS is safer (can't break your network with false positives) but less effective. IPS is more effective but riskier if misconfigured."

Security callout: "Sec+ loves questions like 'You need to detect but not block attacks' - that's IDS. 'You need to automatically stop attacks' - that's IPS."

Other Security Devices:

WAF - Web Application Firewall ⭐⭐

- Specifically protects web applications (Layer 7)
- Filters HTTP/HTTPS traffic
- Stops: SQL injection, XSS, CSRF
- **Say:** "Regular firewall protects the network, WAF protects the website/web app."

Proxy Server ⭐

- Intermediary between users and internet
- Can filter content, cache data, hide internal IPs
- **Forward proxy:** Internal users -> Proxy -> Internet (content filtering)
- **Reverse proxy:** Internet -> Proxy -> Internal servers (protects servers)

Load Balancer ⭐

- Distributes traffic across multiple servers
- Security benefit: Provides redundancy, helps mitigate DDoS
- **Say:** "Not primarily a security device, but Sec+ might mention it in high-availability contexts."

VLANs - Network Segmentation (2 min) ⭐⭐⭐

Say: "VLANs are Virtual LANs. They let you logically separate networks on the same physical switch."

Draw diagram:

```
        [Single Physical Switch]
             /           \
           /               \
    VLAN 10                VLAN 20
(Sales Dept)           (Finance Dept)
```

Explain:
"Sales and Finance are on different VLANs. Even though they're plugged into the same switch, they can't talk to each other without going through a router or firewall. It's like building walls inside a room."

Security benefit:
"Network segmentation. If Sales gets malware, it can't spread to Finance. Sec+ loves segmentation - it's a core security principle."

Say: "VLANs separate broadcast domains too, improving performance and security. You'll see this on the exam."

WRAP-UP & NEXT STEPS (5 minutes)

Review Key Concepts (3 min)

Say: "Let's rapid-fire review the absolute must-knows:"

Ask these questions:

1. "What layer are IP addresses?" (Layer 3)
2. "TCP or UDP for reliability?" (TCP)
3. "What port is HTTPS?" (443)
4. "SSH or Telnet - which is secure?" (SSH, port 22)
5. "IDS or IPS - which one blocks?" (IPS)
6. "What does NAT do?" (Translates private IPs to public)
7. "Name a private IP range" (10.x, 172.16-31.x, 192.168.x)

If she struggles with any, briefly re-explain.

Study Plan for Her (2 min)

Give her:

1. **Port number flashcard list** - "Drill these daily"
2. **OSI model diagram** - "Keep this handy during Sec+ class"
3. **Protocol comparison chart** (encrypted vs unencrypted)

Say: "Here's your homework before Sec+ starts:"

- Memorize the port numbers (at least the big ones)
- Review OSI model - know what happens at each layer
- Understand IDS vs IPS, TCP vs UDP, private vs public IPs

Reassure her:
"You don't need to be a network engineer. You need to recognize terms and understand where security fits in. As we go through Sec+, these concepts will come up again and you'll reinforce them. This crash course just gives you the foundation so you're not lost on day one."

Optional Session 2 Preview

If scheduling second session, say:
"Next time we'll cover wireless networking - WPA2, WPA3, security protocols - and more advanced security concepts like DMZs, VPNs, and ACLs. But honestly, if you nail what we covered today, you'll be in good shape to start Sec+."

POST-SESSION MATERIALS TO PROVIDE

Port Number Quick Reference Card

```
=== MEMORIZE THESE ===
SSH - 22 (encrypted remote access)
Telnet - 23 (unencrypted - don't use)
SMTP - 25 (send email)
DNS - 53 (name resolution)
DHCP - 67/68 (auto IP assignment)
HTTP - 80 (unencrypted web)
POP3 - 110 (receive email - downloads)
```

```
IMAP - 143 (receive email - syncs)
HTTPS - 443 (encrypted web)
SMB - 445 (file sharing - block at firewall!)
LDAP - 389 (directory queries)
LDAPS - 636 (encrypted directory)
FTP - 20/21 (unencrypted file transfer)
SFTP - 22 (encrypted file transfer - uses SSH)
FTPS - 989/990 (FTP over TLS)
RDP - 3389 (remote desktop)
```

OSI Model Reference

```
Layer 7 - Application  (Protocols: HTTP, FTP, DNS)
Layer 6 - Presentation (Encryption, formatting)
Layer 5 - Session      (Connection management)
Layer 4 - Transport    (TCP/UDP, port numbers)
Layer 3 - Network      (IP addresses, routing)
Layer 2 - Data Link    (MAC addresses, switches)
Layer 1 - Physical     (Cables, signals)
```

Encrypted vs Unencrypted Quick Reference

```
❌ UNENCRYPTED (Don't use):
- Telnet (23)
- FTP (20/21)
- HTTP (80)
- SMTP (25)
- POP3 (110)
- IMAP (143)
- LDAP (389)

✅ ENCRYPTED (Use these):
- SSH (22)
- SFTP (22)
- HTTPS (443)
- SMTPS (587/465)
- POP3S (995)
- IMAPS (993)
- LDAPS (636)
- FTPS (989/990)
```

TEACHING TIPS

1. **Use the whiteboard extensively** - Visual learners need diagrams
2. **Repeat port numbers** - Say them multiple times throughout
3. **Use real-world examples** - "When you visit amazon.com, you're using HTTPS on port 443"
4. **Check for understanding** - Pause and ask "Does that make sense?" frequently
5. **Don't get too deep** - If she asks complex questions, say "Great question, but for Sec+ you just need to know [basic concept]"
6. **Emphasize exam relevance** - Keep saying "Sec+ will test this"
7. **Be encouraging** - This is a lot in one hour. Remind her it's normal to feel overwhelmed

---

Good luck with the session! This should give her the foundation she needs to succeed in Security+.