Network Services Review

Chapter 3

SSAS F2016
Søren Debois

Meta

Office hours

- Mon **16-18** @4A14 (2 TAs)
- ~~Tue 9-10 @2A12~~
- Wed 16-17 @3A12
- Thu 16-17 @2A12
- ~~Fri 9-10 @2A12~~

Evaluation, Phase 1.

- Write something positive.
  Short. Only one thing on each line.

- Write something negative.
  Short. Only one thing on each line.

- Pass the paper along your row.

Evaluation, Phase 2.

- Read the paper.
- Put a + on each statement you agree with.
- Put a % on each statement you disagree with.
- Pass the paper along your row.

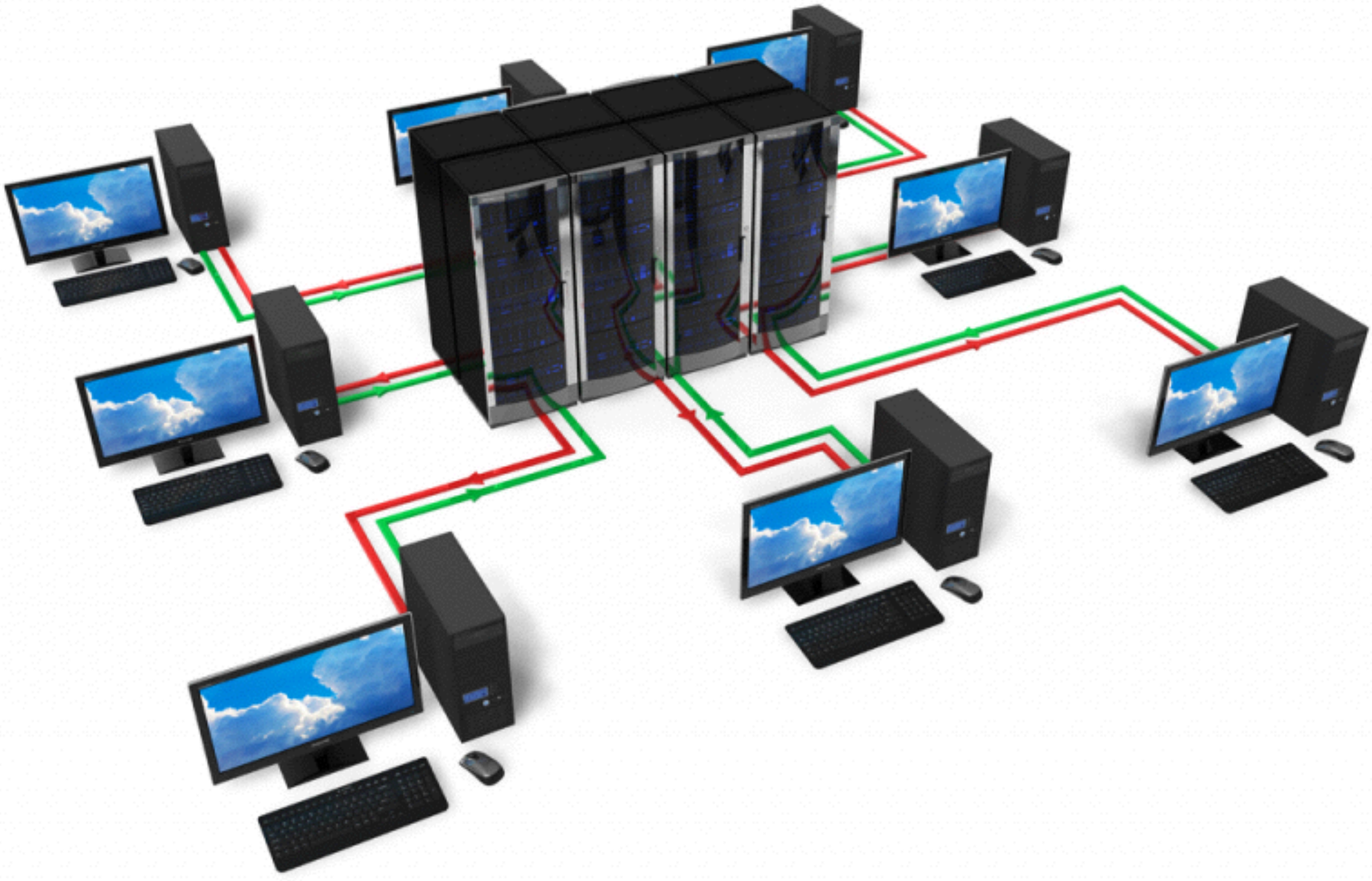
Chapter 3 Review: Network Services

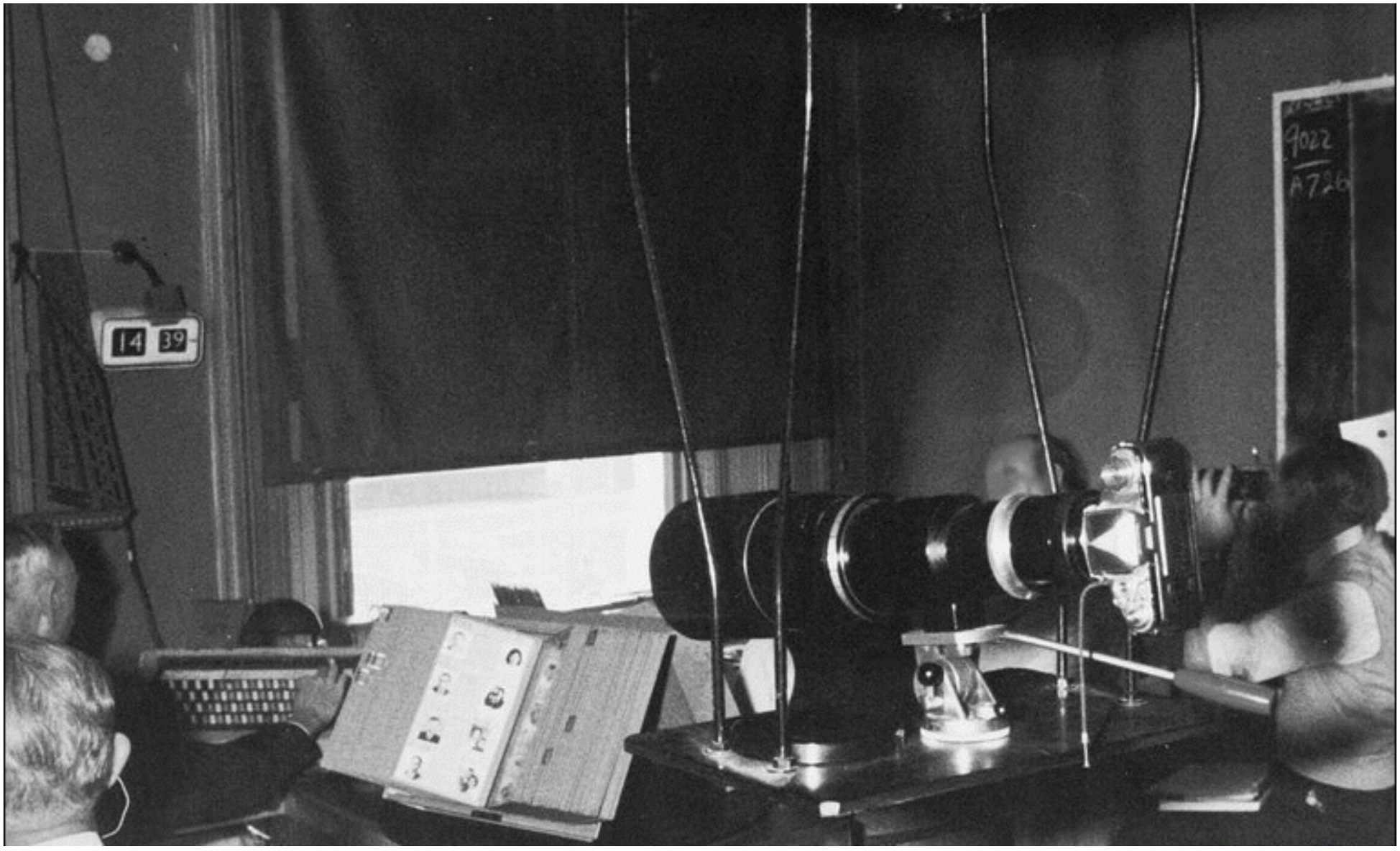
Network Services

- My host is providing services to users. (Web, file, media streaming, …)
- Users access these services over the network.
- So network service must be exposed to the network (duh).
- That means its exposed to both users and adversaries.

Network Services (ii)

- My service is a *process* running on a *host*.
- My process listens for connections on a *TCP port.*
- A host usually contain processes that are not network services.
- A host may run many network service processes.





Adversary's point of view

Adversary's motivation

- To violate either of confidentiality, integrity, availability or accountability.

- In practice dependent on the role and context of your system.

- The book focuses on achieving root privileges.

Information Gathering (i)

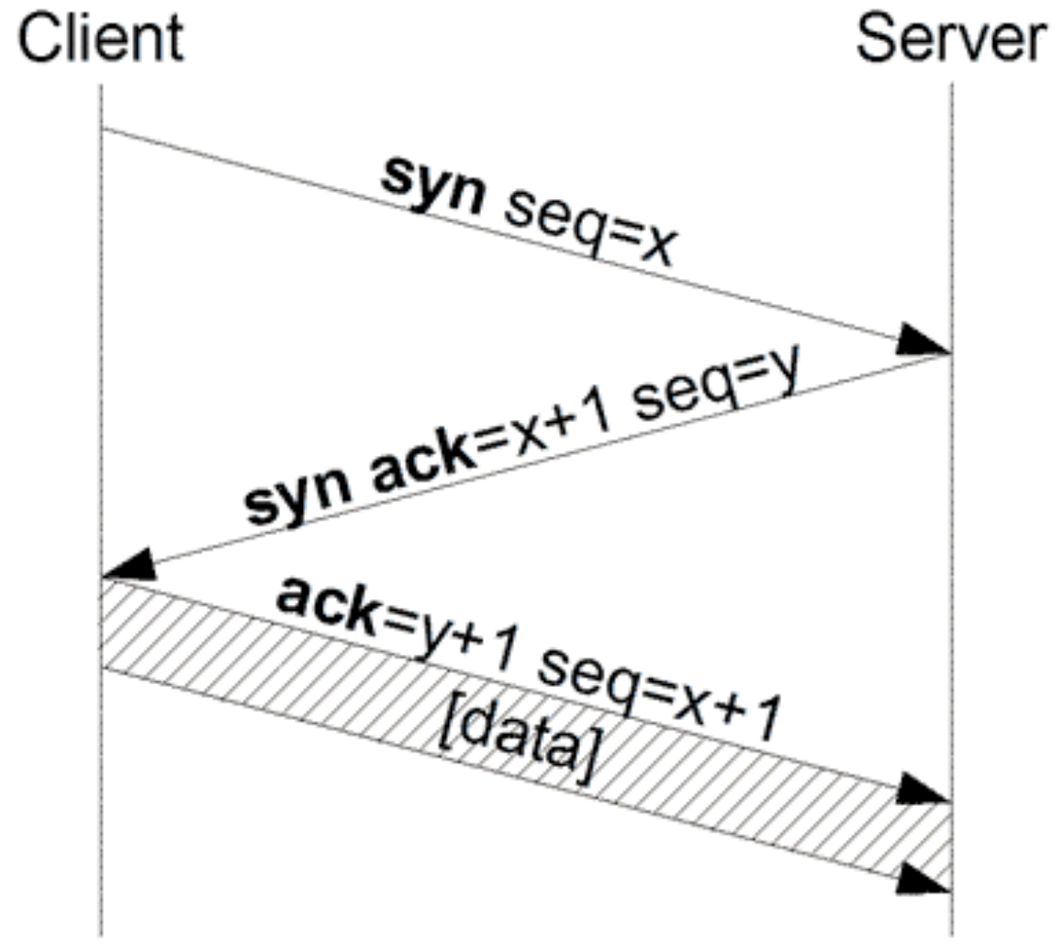
- I need to understand your system in order to attack it.
- IP, network structure, operating system, network services,…
- I am free to operate at any level abstraction

TCP Port scanning

- On what ports does my target accept connections?
- What services are running at those ports?
- What versions are those services?
- What OS is beneath the services?
- In practice:
  How does my target respond to various malformed TCP packets?

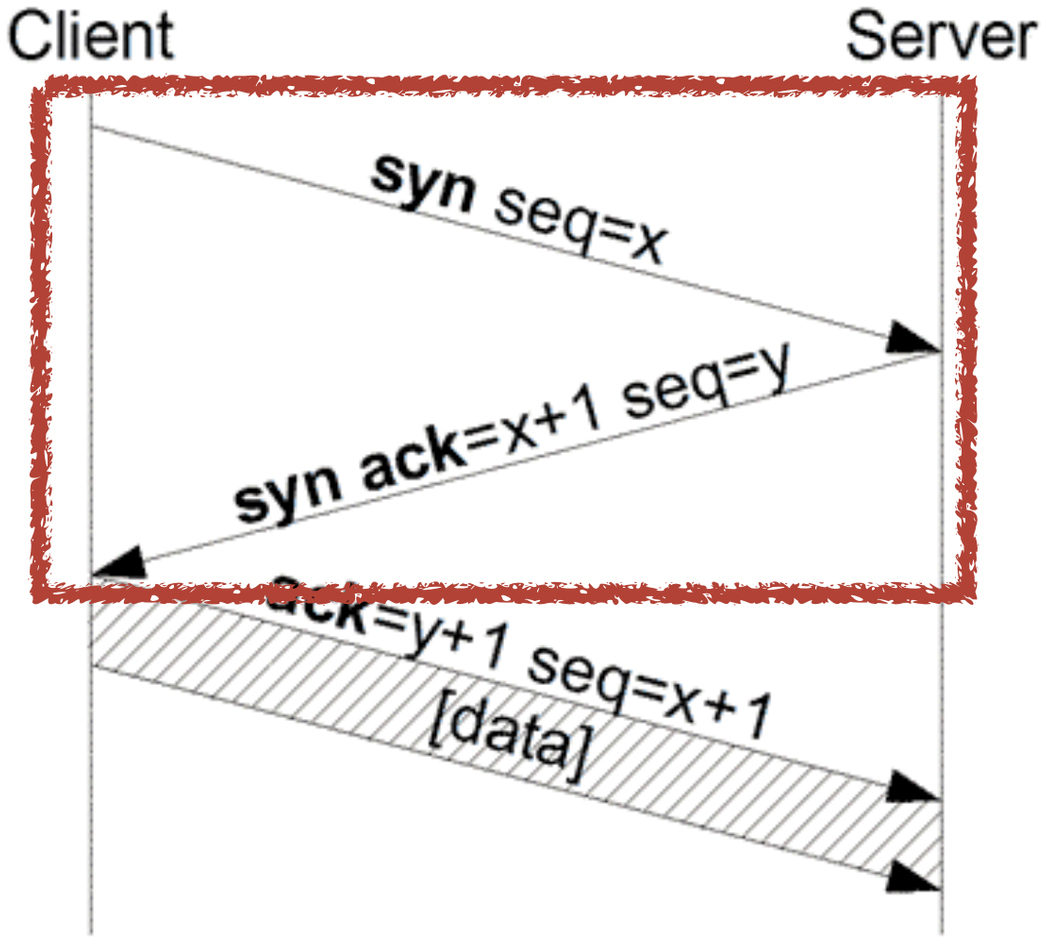
Connect scan

- Do the entire 3-way handshake.
- Reveals open TCP ports.
- Used if I don't have root on the scanning machine.



SYN scan

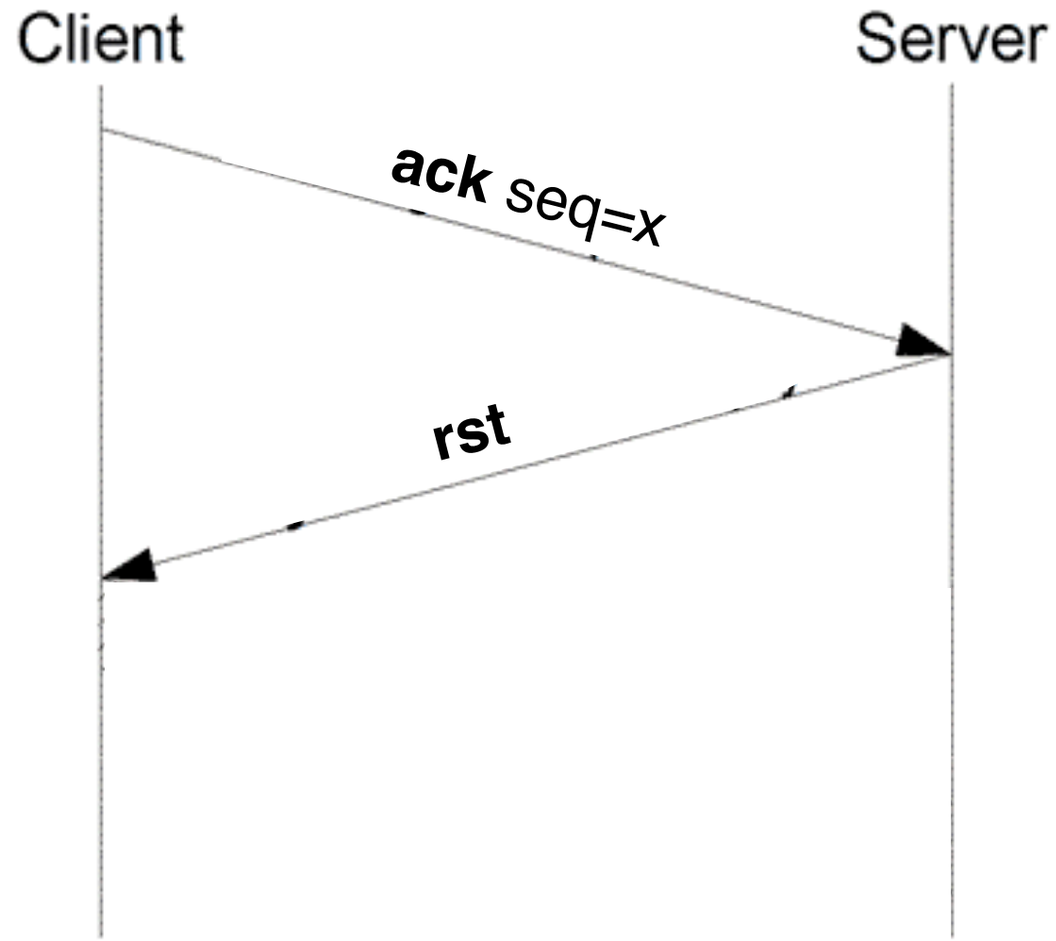
- SYN scan: first leg of 3-way handshake.
- Aka “half-open scanning”
- Reveals open TCP ports.
- Efficient.
- Only slightly suspicious.



ACK scan

- Send unsolicited ACK package. Server must respond RST.

- Reveals firewalled TCP ports.



Stealth scan

- A stealth scan never actually establishes a connection.
- This means the application will never see our scan.
  I.e., the web-server logs will contain no record of my scan.
- The OS does see my scan, though.
  It might log it. It might consider my malformed packets suspicious.
- SYN & ACK scans are stealth scans.

Using information

- From portscanning, I've learned that my target host is running Tomcat 1.1.29 using OpenSSL 1.0.1f.

- I go look for known vulnerabilities in that software.

- OpenSSL 1.0.1f suffers from the Heartbleed vulnerability. I'll exploit that, waiting to see someone's login credentials.

Using information (ii)

- In practice I'll use a tool such OpenVAS to exploitable services.

- I might use a tool like metasploit to actually exploit the vulnerability I've found.

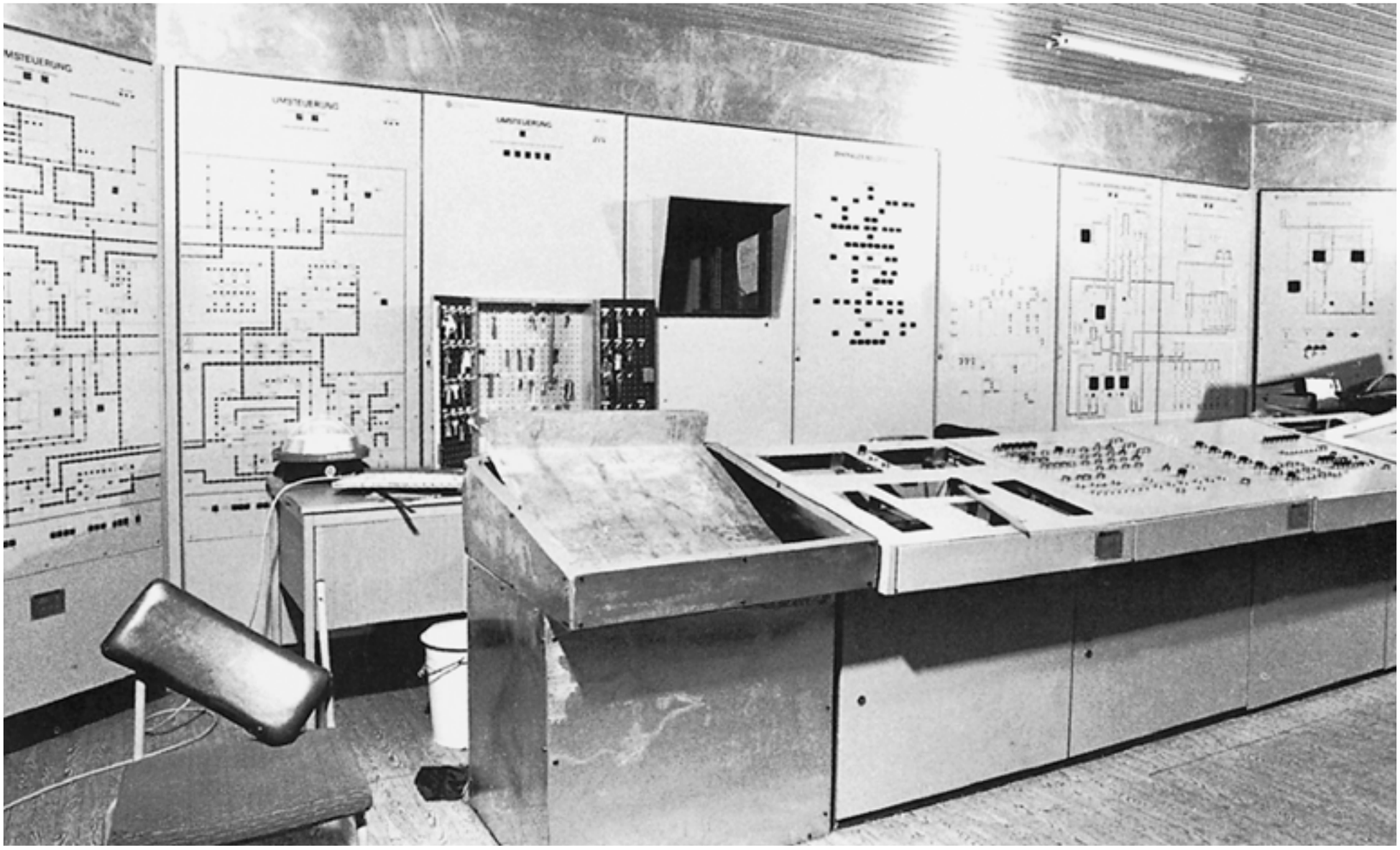
Vulnerabilities

- Make it crash. (Availability)
  WhatsApp crash

- Weak crypto. (Confidentiality)
  DVD CSS

- Information leaks (Confidentiality)
  Heartbleed.

- Privilege elevation (Integrity/Confidentiality)
  Buffer overflows, Shellshock.



Administrator’s point of view

Administrator's motivation

- To preserve all of confidentiality, integrity, availability or accountability.

- In practice dependent on the role and context of your system.

- The book focuses on preventing the adversary obtaining root privileges.

Hardening

- The process of reducing the surface of vulnerability of a system.
- viz. Minimum Exposure.
- Prerequisite: You must understand, exactly, the purpose of the system.

Hardening (ii)

- Disable unnecessary network services.
- Upgrade to patch known vulnerabilities of OS and network services.
- Compartmentalise services using local access control (users, file permission).
- Minimise exposure by protecting necessary local network-only services using firewalls.

Summary

Summary

- Network Services, adversary’s perspective.

- Network Services, administrators perspective.

Network services (Adversary)

- Actual goal dependent on context. (Confidentiality, Integrity, Availability, Accountability)

- Want to subvert running services.

- Need information to find exploits.

- Port-scanning, automated vulnerability detection tools.

- Automated vulnerability exploitation tools.

Network services (Administrator)

- Actual goal dependent on context.
  (Confidentiality, Integrity, Availability, Accountability)

- Hardening:
  - Reduce surface of vulnerability.
  - Disable unnecessary services.
  - Keep the system upgraded.
  - Keep the system compartmentalised.

Thank you!

- See learn-it for exercises etc.

- Questions?