

# **Network Security, Part I**

**Jeff King**

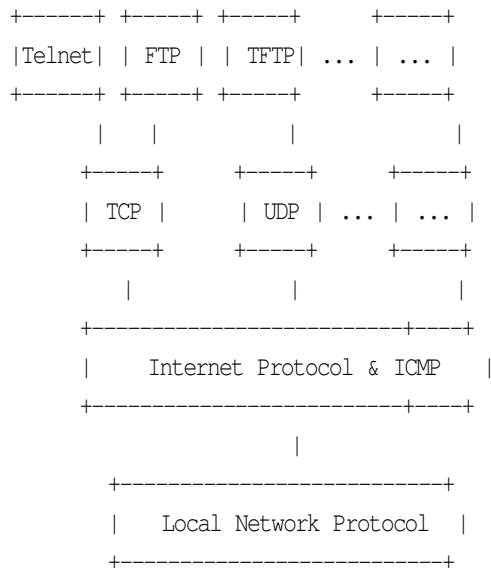
**June 28, 2007**

## Why are networks interesting attack targets?

- anonymity – who is on the other end?
- automation – attackers can manipulate systems
- distance – opportunity for attackers
- opaqueness – minimal details about remote end

# How do networks work?

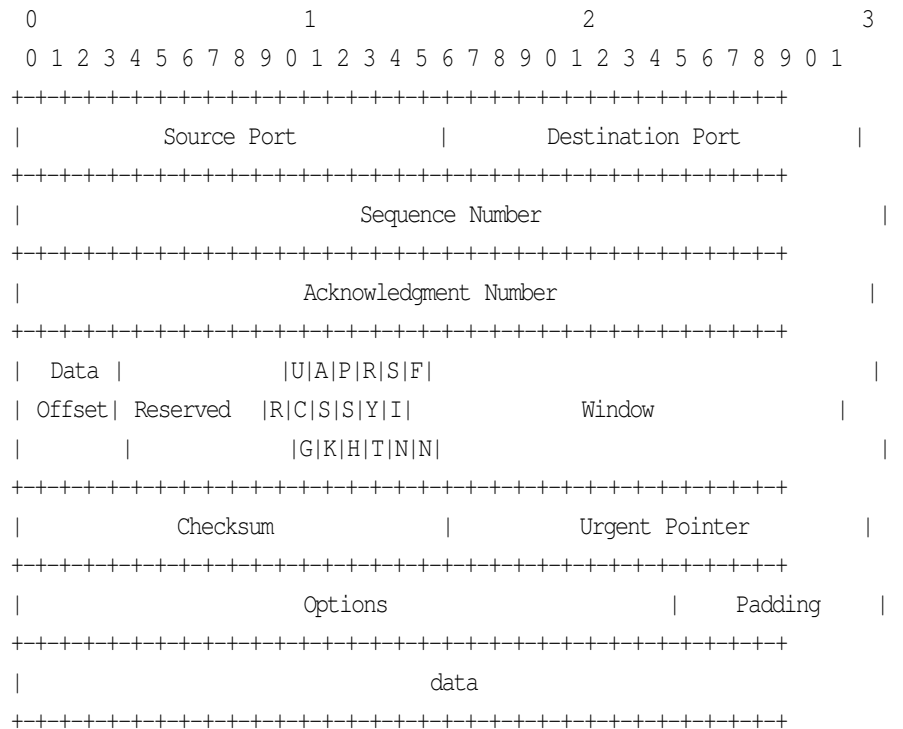
- OSI 7-layer model
- Each layer requests services from ones below
- From RFC 791 (Internet Protocol):



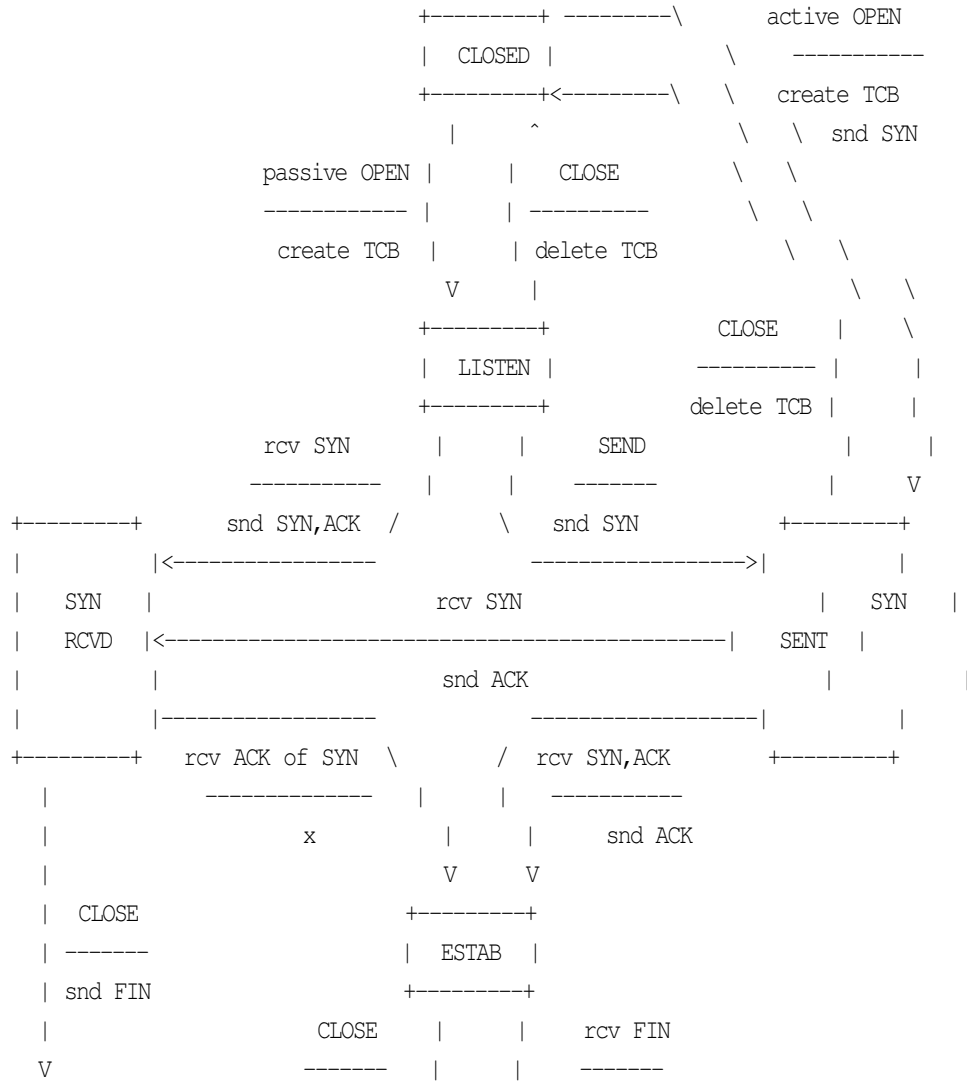
- Compromising one layer may compromise upper layers

# How do networks work?

- Protocols specify data formats (RFC 793, TCP):



# ...and behavior.



# Information gathering

- eavesdropping
- social engineering / phishing
- port scanning

```
$ nmap 10.0.0.1
Starting Nmap 4.20 ( http://insecure.org ) at 2007-06-26 13:05 EDT
Interesting ports on segfault.intra.peff.net (10.0.0.1):
Not shown: 1690 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
6667/tcp  open  irc
MAC Address: 00:60:67:33:AE:D8 (Acer Netxus)

Nmap finished: 1 IP address (1 host up) scanned in 0.453 seconds
```

# Information gathering

- OS / application fingerprinting
  - easy: version banners
  - hard: particulars of protocol implementation

```
$ nmap -A 10.0.0.1
Starting Nmap 4.20 ( http://insecure.org ) at 2007-06-26 13:06 EDT
Interesting ports on segfault.intra.peff.net (10.0.0.1):
Not shown: 1690 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         OpenSSH 4.3p2 Debian 9 (protocol 2.0)
25/tcp    open  smtp        netqmail smtpd 1.04
53/tcp    open  domain?
80/tcp    open  http        lighttpd 1.4.13
139/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.18
Uptime: 22.469 days (since Mon Jun  4 01:54:23 2007)
```

# Threats

- confidentiality / integrity / authenticity of communications
- information disclosure from host
- information integrity on host
- arbitrary code execution on host
- denial of service (against host or network)
- confidentiality of traffic flow

## Words You Should Know

- sniffing - eavesdropping on network communications
  - can be totally passive, difficult to detect
  - gather confidential information
  - gather authentication information for later use
- spoofing - impersonating one end of a network session
- session hijacking - impersonating one or both sides of an existing session

# Vulnerabilities

- lack of security precautions
- poor use of security precautions
- protocol flaws
- implementation flaws

## Lack of security precautions

- cleartext transmission of sensitive messages
- non-existent authentication
- lack of policies / trust in human behavior
- dubious trust assumptions
  - rhost relies on IP

## Poor use of security precautions

- failure to turn on / use tools (such as encryption)
- accounts with easily guessable (or no!) password
- failure to use access control mechanisms
- users ignoring policy / warnings

## Protocol flaws

- lack of authentication / secrecy of authentication tokens (SNMP)
- lack of cryptography
- authentication, but no integrity (telnet)
- easily spoofable sessions (TCP sequence numbers)
- inappropriate resource allocation (TCP SYN attack)
- amplification behavior (smurf attack)

## Implementation flaws

- buffer overflows
- failure to restrict input
  - changing immutable values
  - example: .. in web paths
- injection attacks
  - sql
  - shell

# Client Attacks

- traditionally, attacks have been initiated by malicious users
- servers are well protected
- users are not running services
- increasingly, attackers wait for clients to pull attacks from them
  - phishing / domain-typo sites
  - overflows in IE JPG parsing code
  - cross-site scripting / cookie theft

# Controls

- segmentation
- redundancy
- encryption / strong authentication
- firewalls
- intrusion detection

# Segmentation

- split logical functions with security barriers
- may be split inside host
  - leverage multi-user OS protections
  - different users for different services
  - example: www user, mail user
- may be split across hosts
  - hosts must authenticate to each other
  - actions are limited across host boundaries
- may split network traffic across physical or virtual segments