Lecture 08: Networking services: there's no place like 127.0.0.1

Hands-on Unix system administration DeCal

2012-10-15

DNS

About DNS

- **Domain Name Service**
- Internet's `/etc/hosts` file
- client software (e.g., web browser) automatically asks DNS server for records
  - ✦ requests passed between servers
- see also `host`, `dig`

Common DNS records

- **A**: IPv4 address
- **AAAA**: IPv6 address
- **CNAME** an alias for another record (Canonical Name)
- **MX**: mail server(s) for a domain (Mail Exchanger)
- **PTR**: reverse A record (Pointer)

Other DNS records

- **SRV**: service
- **TXT**: text

Networking

Too many TLAs

- OSI reference model, we focus on application layer
- transport protocols: TCP, UDP
- ports numbered between 1 and 65535 (unsigned 16 bit integer)
- ports below 1024 (e.g., 22/tcp – SSH, 80/tcp – HTTP), require root access on Unix

TCP

- **Transmission Control Protocol**
- reliable, more overhead, stateful
- most network services use TCP (HTTP, SMTP, SSH, etc.)
  - ✦ some may use both TCP and UDP

UDP

- **User Datagram Protocol**
- unreliable, simple (“fast”), stateless
- often used by DNS, DHCP, TFTP, VoIP, streaming media, etc.
  - ✦ DNS uses TCP, however, for larger responses

NATs

- **Network Area Translation**
- accomplished by home/office router
  - rewrite packets for many computers to use one public IP address (Source NAT, IP Masquerading)
  - private IP addresses: 192.168.0.0–192.168.255.255, 10.0.0.0–10.255.255.255, 172.16.0.0–172.31.255.255

Port forwarding

- also called Destination NAT (DNAT)
- forward a public IP addressed port to an internal IP addressed port
- required to access services behind a Source NAT

HTTP

- **Hyper-Text Transfer Protocol**
- simple, text-based protocol
  - ✦ basic web server can be implemented in a 25-line `bash` script with `netcat`
- popular servers: Apache, IIS, lighttpd, nginx

NFS

- **Network File System**
- mounts can be defined in `/etc/fstab`
- usually need to be root to mount

SSH

About SSH

- **Secure SHell**
- different authentication mechanisms: PAM, public key, GSSAPI (Kerberos)
- remote encrypted terminal/console on remote machine
- other features: port forwarding, X forwarding, file transfer, can be combined with other protocols

SSH public-private keys

- alternative to password-based authentication
  - ✦ uses public/private key cryptography
- SSH agent caches key in memory
- SSH forwarding forwards key challenges

Public-private keys

- public key: everyone can see lock
- private key: one person has key
- encrypt with public key, decrypt with private key
- sign with private key, verify with public key
- ciphers: RSA, DSA

Symmetric keys

- one shared key
- advantage: speed, security
- disadvantage: often impractical to verify, especially against man-in-the-middle attacks
- ciphers: AES, 3DES, blowfish, arcfour

PAM

- **Pluggable Authentication Modules**
- API for authentication commonly used on Unix
- pam_unix: `/etc/shadow` password hashes

Network users

LDAP

- **Lightweight Directory Access Protocol**
- distributed directory information service, like phone book
- arranged as records with attributes
- often used to populate user accounts across a network
- CalNet is an *LDAP directory*

Kerberos

- trusted third party provides mutual authentication between machines and users
- arranged as principals which can be fetched as tickets to authenticate
- CalNet is also a *Kerberos realm*