Lecture 08: Server services

Hands-on Unix system administration DeCal

2012-03-12

Final project

- sign up online if you haven't already
- proposals due next week

DNS

About DNS

- Domain Name Service
- Internet's phonebook
- client software automatically asks DNS server for records
  - requests passed between servers

Common DNS records

- **A**: IPv4 address
- **AAAA**: IPv6 address
- **CNAME** (Canonical Name): an alias for another domain (think "symlink")
- **MX**: mail server
- **PTR**: "reverse A record"

Other DNS records

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

Networking

Too many TLAs

- OSI reference model, we focus on application layer
- TCP, UDP
- ports numbered between 1 and 65536
- ports below 1024 are well-known, e.g. 22 – SSH 80 – HTTP 443 – HTTPS, require root access on Unix

TCP

- **Transmission Control Protocol**
- provides reliable transmission of data over inherently unreliable media
- most network services use TCP (HTTP, SMTP, SSH, etc.)

UDP

- **User Datagram Protocol**
- reliability is less important than speed, can and may drop packets at any time
- used by DNS, TFTP, VoIP, streaming media, etc.

NATs

- **Network Area Translation**
- accomplished by home/office router
- rewrite packets for many computers to use one public IP address
- 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

- forward a public IP addressed port to an internal IP addressed port
- required to access services behind a NAT

HTTP

- **Hyper-Text Transfer Protocol**
- simple, text-based protocol (see lab), basic web server can be implemented in a 25-line bash script
- popular servers: Apache, IIS, lighttpd, nginx

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

- **Plugable Authentication Module**
- API for authentication commonly used on Unix
- often password-based, but also used with Kerberos

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 LDAP

Kerberos

- trusted third party provides mutual authentication between machines and users
- arranged as principals which can be fetched as tickets to authenticate