Network and Server Security Essentials

Presented by Hansen Wu

Overview

1. Basic Networking and Terminology
2. The Simple Server
3. SSH and Bash Commands
4. Proxies
5. Securing a Server

Basic Networking and Terminology

This will be a bit dry…

IP Address

Internet Protocol Address

- IPv4
  - 4 blocks of 8 bits, 32 bit total
  - 2^32 = 4,294,967,296 total addresses
- IPv6
  - Be future ready and prepare for IPv6
  - 8 groups of 4 hexes, 2^128 total addresses
- Subnetting
  - I.e. 192.168.1.0/24 is all possible IPs with last block as wildcard
  - Calculating bits
  - Google is your friend

Port

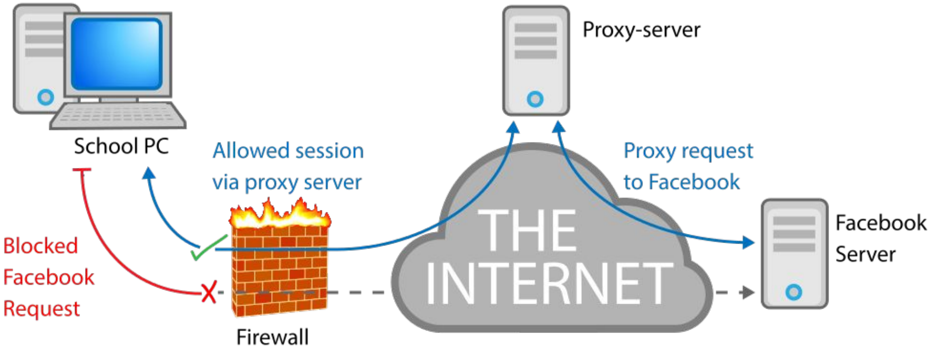
Port

- Logical construct
- Assigned to inbound/outbound packets
- Ranges up to 65535
- 1024 reserved well known ports
- Non enforced conventions
  - 21: FTP
  - 22: SSH
  - 80: HTTP
  - 443: HTTPS
  - 990: FTPS

Proxies

Proxies

- Think back to history class: proxy wars
- “intermediary for requests from clients seeking resources from other servers”
- Hides yo ass
- Reverse proxy: important for orgs for load balancing, caching, privacy, and more

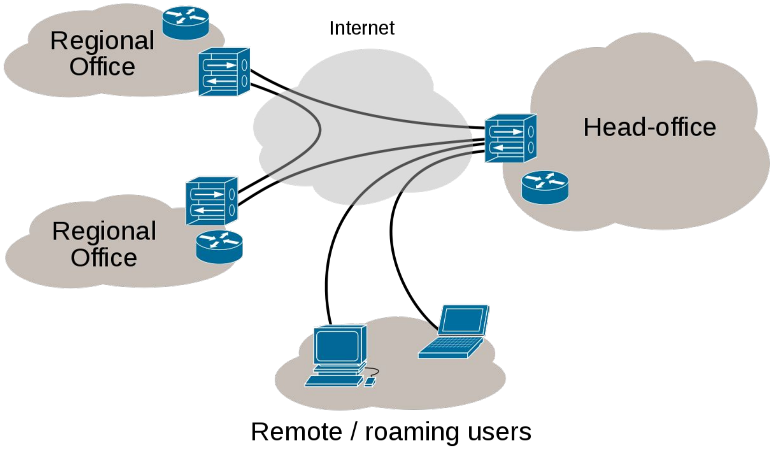


VPN

Virtual Private Network

- Virtualized network extending beyond physical limitations network
- “extends a private network across a public network”
- Can connect to a network and access intranet resources remotely and securely
- All traffic sent through vpn
  - DNS leaks

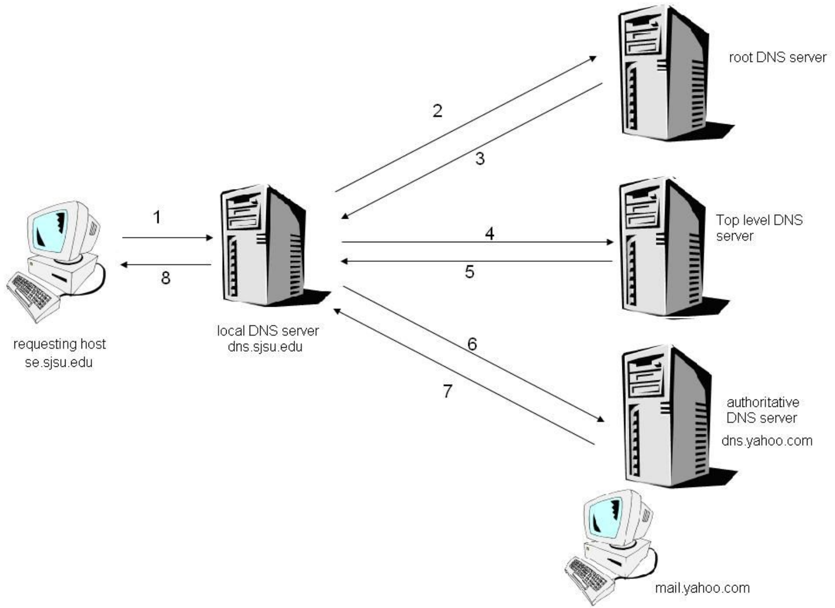
Internet VPN



DNS

Domain Name System

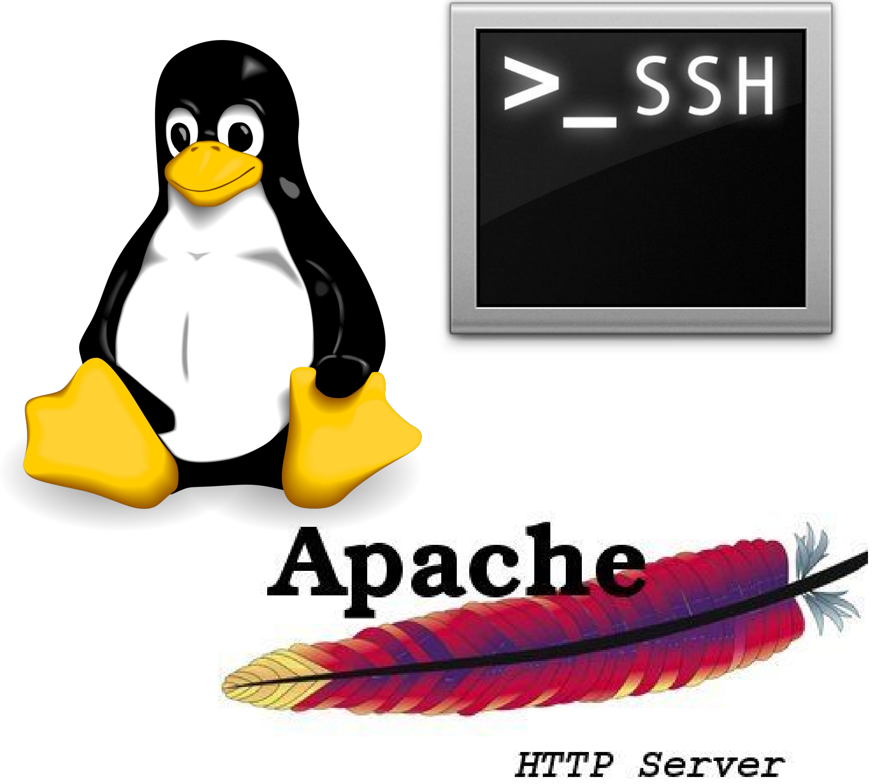
- Provides directions for network requests
- Database associating domain names and other information with IP addresses
- Useful for servers on dynamic IPs



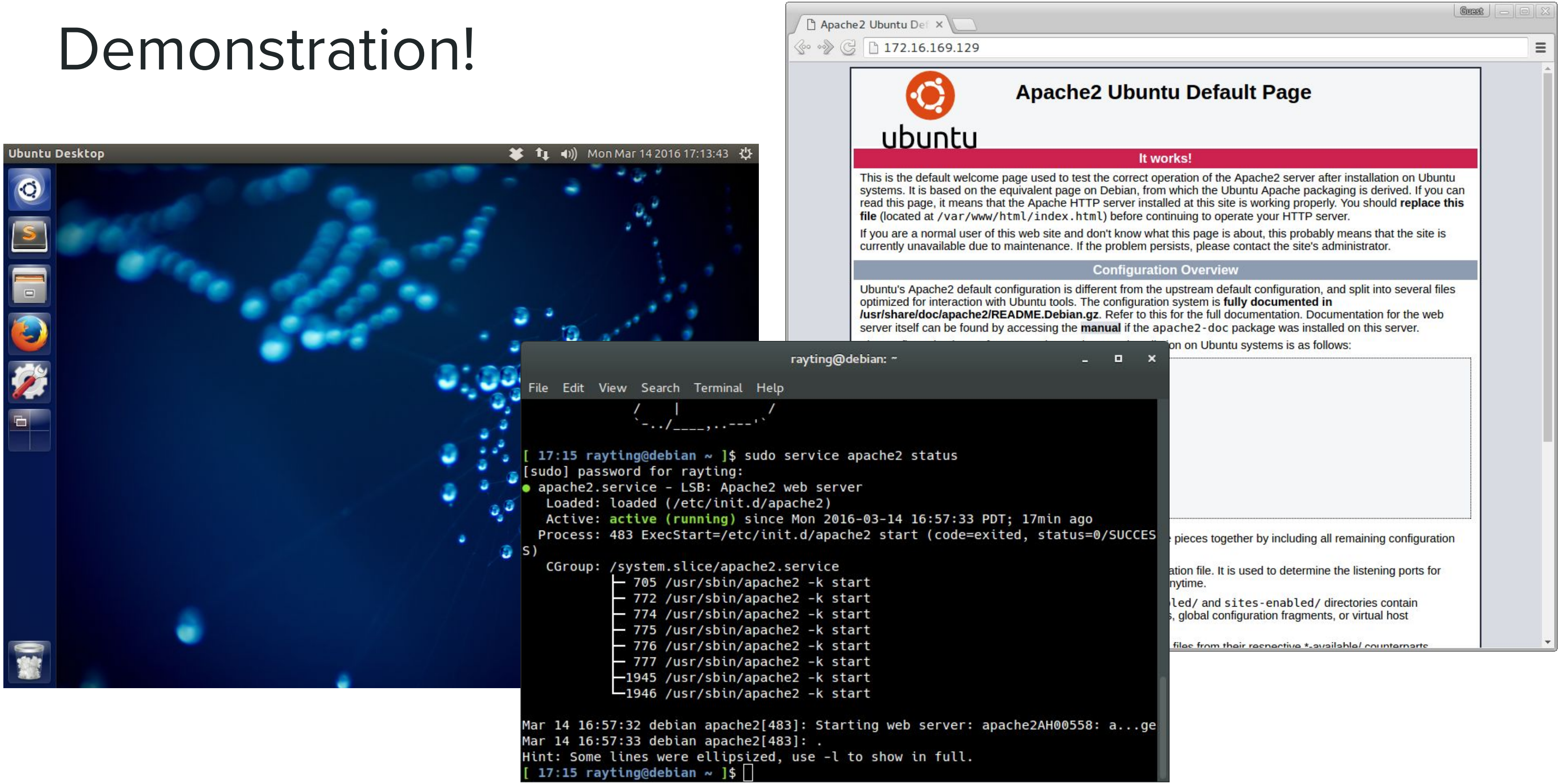
The Simple Server

Build your own server

- Web and SSH Linux stack
- Host a website
- Remote access
- Limitless expansion options



Demonstration!



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

on on Ubuntu systems is as follows:

pieces together by including all remaining configuration

ation file. It is used to determine the listening ports for nytime.

`led/` and `sites-enabled/` directories contain s, global configuration fragments, or virtual host

files from their respective *-available/ counterparts

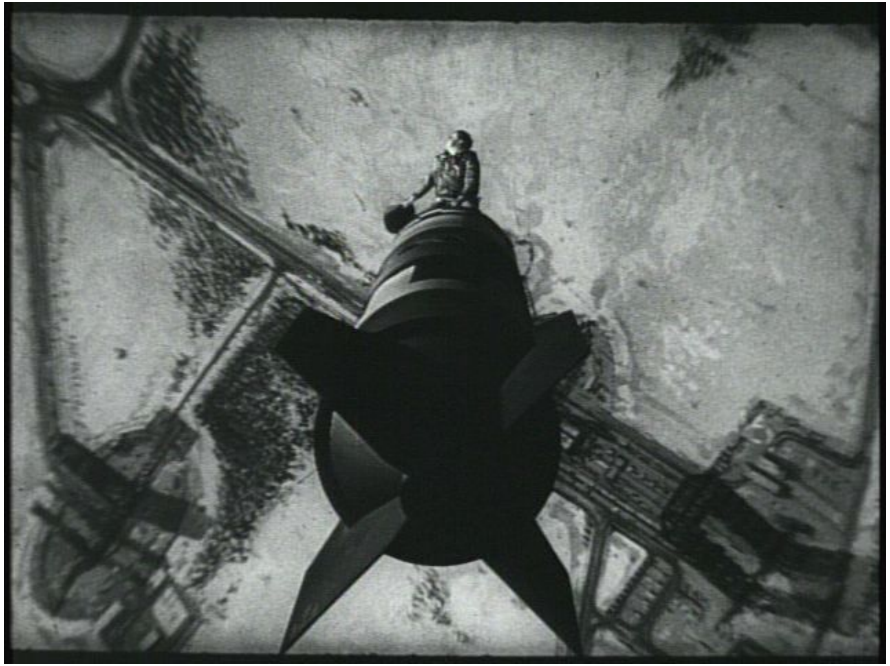
```
          /    |          /
          `-../____,..---'`

[ 17:15 rayting@debian ~ ]$ sudo service apache2 status
[sudo] password for rayting:
● apache2.service - LSB: Apache2 web server
   Loaded: loaded (/etc/init.d/apache2)
   Active: active (running) since Mon 2016-03-14 16:57:33 PDT; 17min ago
  Process: 483 ExecStart=/etc/init.d/apache2 start (code=exited, status=0/SUCCES
S)
   CGroup: /system.slice/apache2.service
           ├─ 705 /usr/sbin/apache2 -k start
           ├─ 772 /usr/sbin/apache2 -k start
           ├─ 774 /usr/sbin/apache2 -k start
           ├─ 775 /usr/sbin/apache2 -k start
           ├─ 776 /usr/sbin/apache2 -k start
           ├─ 777 /usr/sbin/apache2 -k start
           ├─1945 /usr/sbin/apache2 -k start
           └─1946 /usr/sbin/apache2 -k start

Mar 14 16:57:32 debian apache2[483]: Starting web server: apache2AH00558: a...ge
Mar 14 16:57:33 debian apache2[483]: .
Hint: Some lines were ellipsized, use -l to show in full.
[ 17:15 rayting@debian ~ ]$ 
```

SSH and Bash Commands

Linux or: How I Learned To Stop Worrying and Love the Command line

- Try out some Bash commands!
- Powerful network tools and capabilities
  - telnet
  - nc
  - curl
  - wget
  - ssh

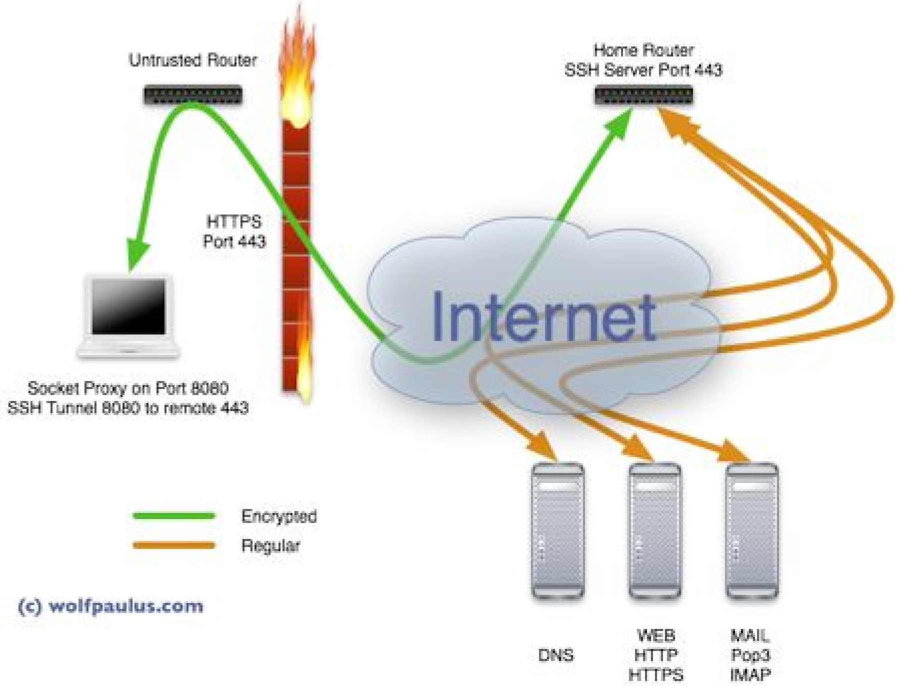
Demo!



Proxies

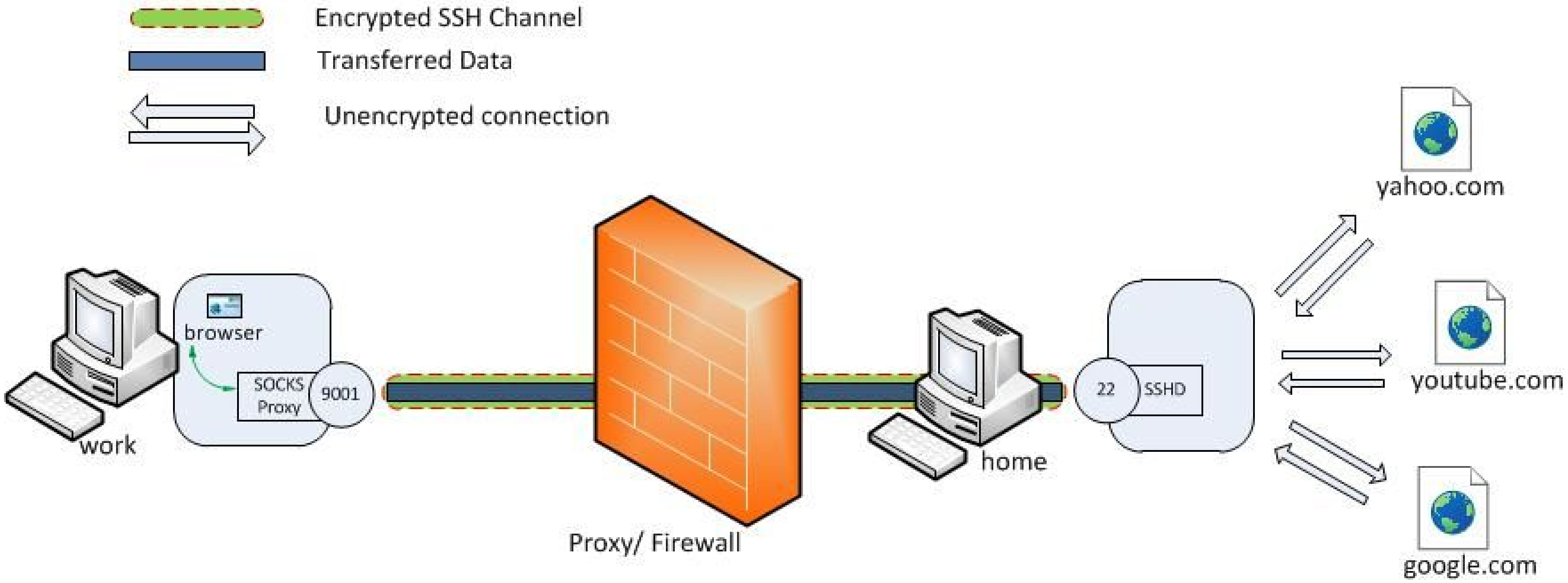
Proxies

- Recap: accessing network through another machine
- Wide range of uses
  - Bypass region limitations
  - Defeat censorship and firewalls
  - Security in an unsecure environment



(c) wolfpaulus.com

Demo!


Encrypted SSH Channel
Transferred Data
Unencrypted connection
yahoo.com
browser
SOCKS Proxy
9001
work
Proxy/ Firewall
home
22
SSHD
youtube.com
google.com

Server Security

Opening the Floodgates

- Sheltered and protected environment behind the router
- Router blocks most malicious traffic
- Enabling external access and port forwarding
- Attacks start the second you “open the door”
- Very well known and documented botnets bruteforcing SSH
  - https://blog.sucuri.net/2013/07/ssh-brute-force-the-10-year-old-attack-that-still-persists.html
  - root login, dictionary attack

Protective Measures

- SSH
  - Root login
  - Certificate access
  - fail2ban
  - Visual fingerprint
- Fail2ban
  - Ban duration
  - Attempts
- Apache
  - Index only, 403 your resources