



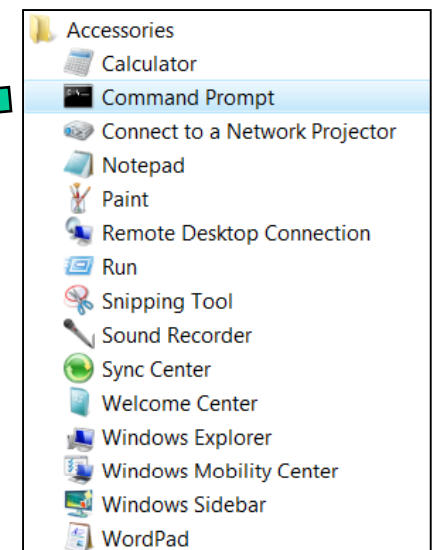
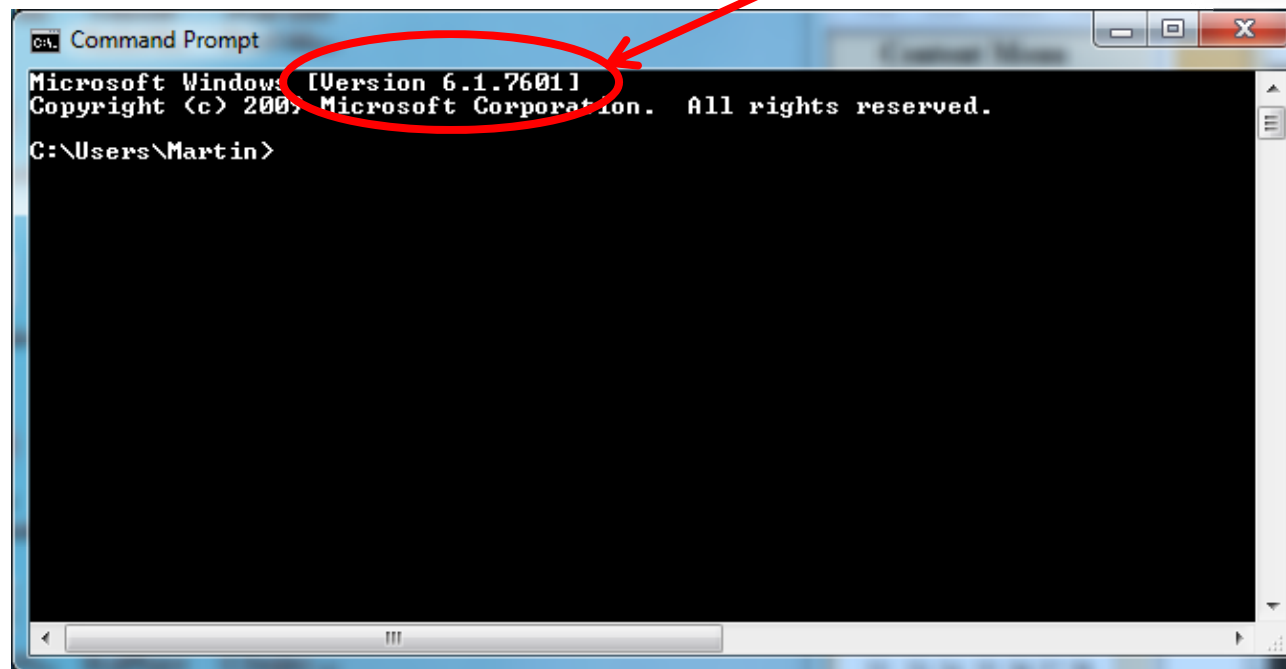
# DOS Review Lab



## Disk Operating System review

- Predates Windows – circa 1981
- (MS-DOS, PC-DOS, FreeDOS) for x86 systems
- Exploits, trojans often provide a DOS shell
- DOS Scripts are common in infections
- Many new DOS features – scriptable
- Useful, fast, small footprint

Win 7





# DOS Review Lab

- A Quick Review of DOS – Linux is similar
- Open a DOS window by clicking either:
  - ◆ Start|All Programs|Accessories|Command Prompt
  - ◆ It's the Black-window icon with "C:\"or
  - ◆ Start|Run and enter CMD
- Use up/down arrow to access previous commands
- Use TAB key to complete entering file names and directories
  - Makes Long File Names vastly easier
- DOS is a Command Line Interface – CLI
- Windows is a Graphical User Interface – GUI
- Tip: Right click Title Bar Select:Properties|Layout: adjust width
  - ◆ Make it wide enough to avoid wrap
  - ◆ Changes will persist



# DOS Review Lab

## DOS

- Microsoft's flagship product
- Single-user
- Single-tasking
- Has basic kernel functions
- Is non-reentrant
- Reads autoexec.bat at startup
- Still used for embedded systems

## Recent Addition

- Windows Power Shell
  - scripting language
  - .NET Framework
- 
- You should be familiar with the commands listed to the right.
  - If not – learn them now.

## DOS Commands

attrib  
cd, md, rd  
cls  
fc            file compare  
more  
rn  
sort  
tree           tree directory

## Network Related

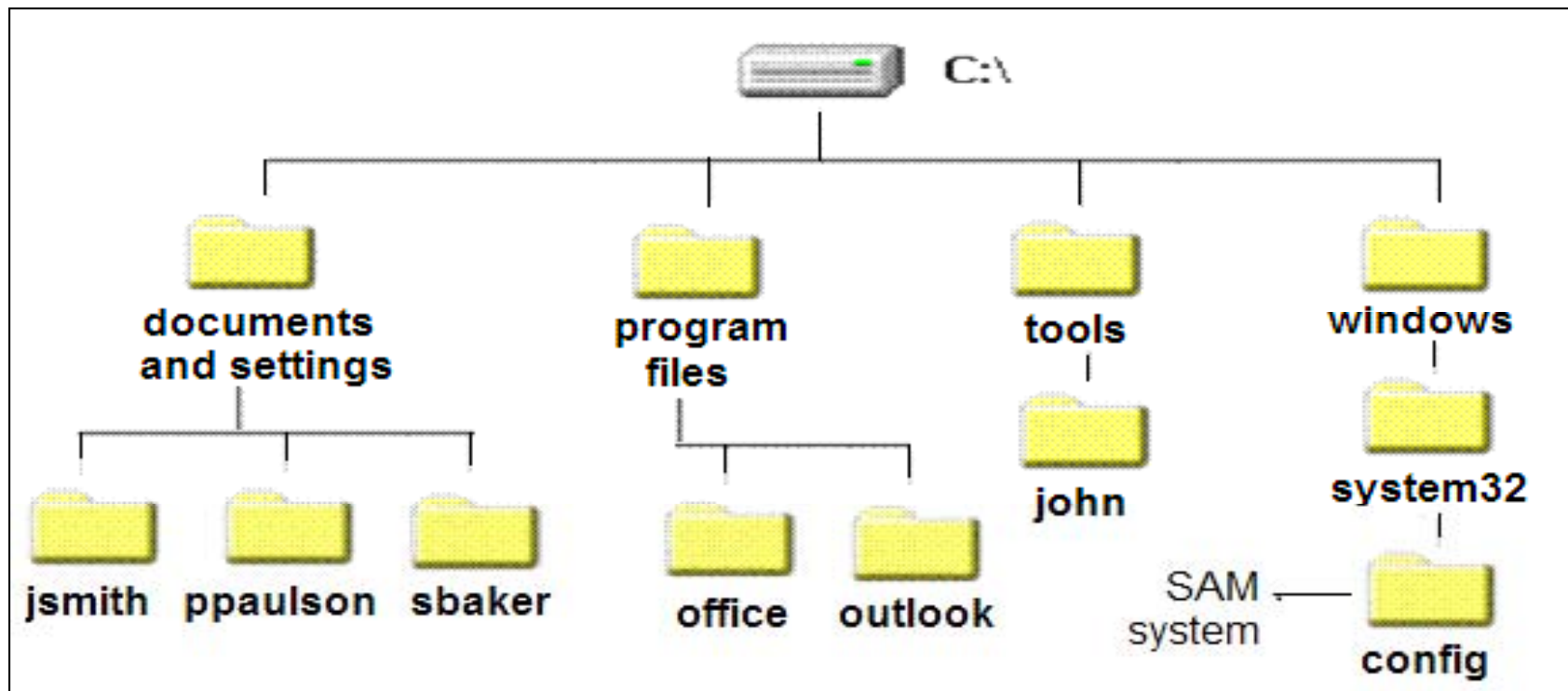
arp  
ftp  
ipconfig  
netstat  
nslookup  
ping  
telnet  
tracert



# DOS Review Lab

## Navigating the directory structure

- Can move down, up, across directory structure
- Starts with prompt in your subdirectory c:/Users/[account\_name]





# DOS Review Lab

## Change Directory – CD

Prompt shows **Drive**, **Location**, and **Prompt Character** e.g. `C:\>`

`C:\> cd \` Move to the top of the structure (`C:\`)

Note: it is a: back slash

`C:\> cd tools` Move down to tools (it's in `c:\`)

`C:\> cd \` or `cd ..` to move back up

The `\` is an *absolute* reference – a direct one

The `..` is a *relative* reference .. 'move up one'

`C:\> cd c:\windows\system32\config`      4b50lu73 Or r3l471v3 ?

`C:\> cp ..\..\filename .`      4b50lu73 Or r3l471v3 ?

What does the above do?



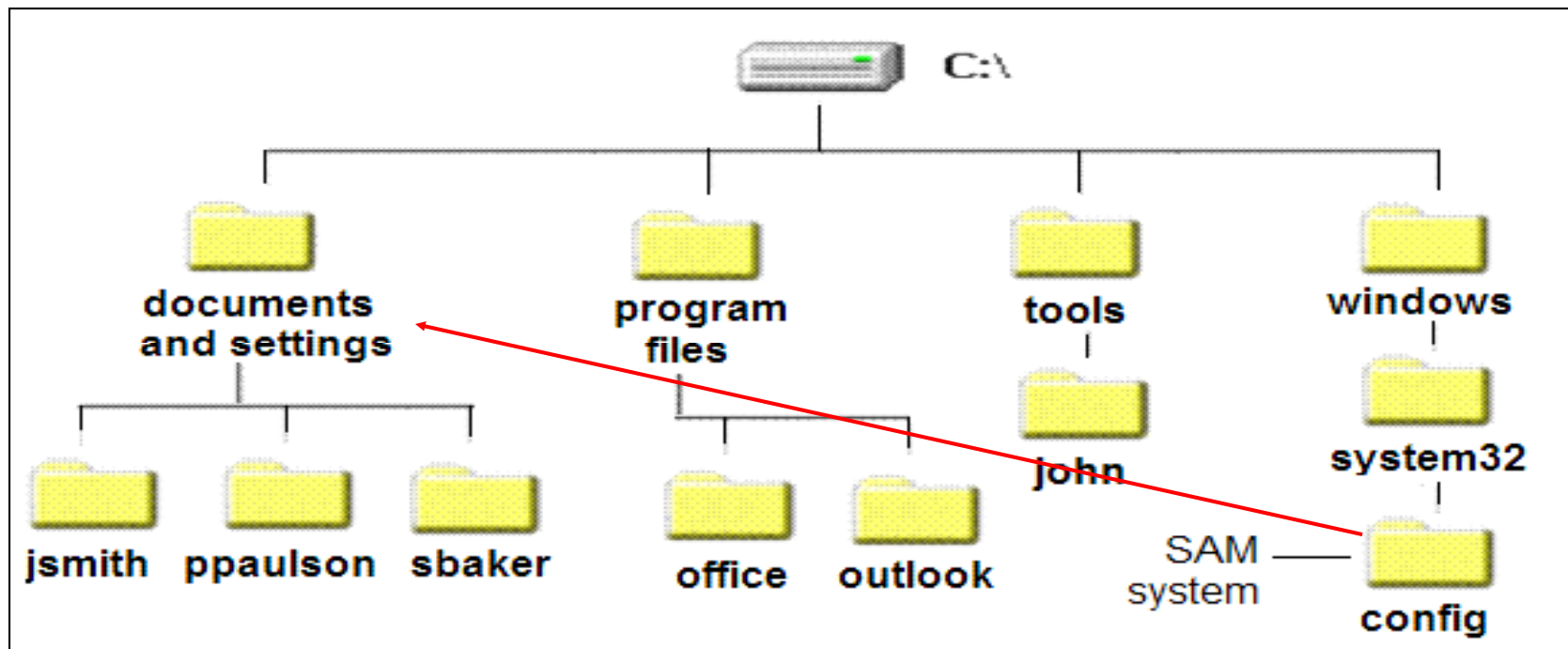
# DOS Review Lab

- C:\> cd c:\windows\system32\config)
- dir [Don't touch anything here]
- The (encrypted) SAM file contains the hashed users' passwords
- The system file "hides" the key used to encrypt the SAM file. It also contains most of the Registry
  - ◆ Note: Windows 7 keeps this folder more secure than XP.
  - ◆ Accessing the folder and seeing the file is easier in DOS
  - ◆ now enter: dir /ah
  - ◆ dir /? for help
- *You navigate directories via either relative or absolute paths*
- *You can execute commands, move files, etc. the same way*
- Relative vs Absolute will be used later in some web exploits



# DOS Review Lab

C:\>cd c:\documents and settings (XP) absolute  
C:\>cd c:\users (Win7) absolute  
C:\>dir [username] view the users' directories  
C:\>dir c:\tools\john view remote dir without going there





# DOS Review Lab

## Lesser Known DOS Commands

### File/directory

robocopy (Robust Copy) Look at the help - /? Very Fast!

type where whoami

### Network

pathping

### MS Networking

nbtstat net netsh

### System

systeminfo tasklist taskkill

### Configuration

msconfig

Robocopy is much faster than File Explorer when handling large numbers of files, such as backup up folders. You can specify the number of simultaneous threads to use (default is 8).

For a GUI version, see:

<http://technet.microsoft.com/en-us/magazine/2009.04.utilityspotlight.aspx>





# DOS Review Lab

- tasklist – list of active processes
- tasklist /? help
- tasklist /V /FO CSV
- tasklist /SVC
- Can connect to remote systems
- Can help detect malware
- net statistics workstation

```
Administrator: C:\Windows\System32\cmd.exe







C:\>tasklist

Image Name                      PID Session Name        Session#
=====
System Idle Process             0 Services             0
System                          4 Services             0
smss.exe                       340 Services            0
csrss.exe                      516 Services            0
wininit.exe                    576 Services            0
csrss.exe                      592 Console             1
services.exe                   624 Services            0
lsass.exe                      648 Services            0
lsm.exe                        656 Services            0
svchost.exe                    760 Services            0
svchost.exe                    856 Services            0
svchost.exe                    920 Services            0
svchost.exe                    952 Services            0
svchost.exe                    984 Services            0
winlogon.exe                   544 Console             1
svchost.exe                    720 Services            0
RtkAudioService64.exe         1036 Services            0
svchost.exe                   1096 Services            0
spoolsv.exe                   1276 Services            0
svchost.exe                   1304 Services            0
AppleMobileDeviceService.    1380 Services            0
```



# DOS Review Lab

- netsh is a command-line scripting utility that allows you to, either locally or remotely, display or modify the network configuration of a computer that is currently running.
- netsh also provides a scripting feature that allows you to run a group of commands in batch mode against a specified computer.
- netsh can also save a configuration script in a text file for archival purposes or to help you configure other servers.
- If you have a DOS shell on a remote computer you can reconfigure the system as needed.

- netsh 
- interface ipv4 
- show 
- show tcpconnections 
- show tcpstats 
- quit 

netsh is one of the reasons to make the command window larger.

Spend some time exploring netsh



# DOS Review Lab

You should develop working familiarity with:

- The DOS command line
- Windows system folders/file organization
- The Windows Registry

As well as

- Linux command line
- Linux system file organization

Exceed the scope  
and available time  
of this class

- Network security work easily crosses the boundaries of various technical specialties. Keeping current is an ongoing challenge.
- Quick tip - Drag to avoid typing: When your command acts on a file or folder, you must type the path to that folder after the command. You can save typing time by dragging the file or folder from Windows Explorer into the command window (which is just *wrong*). Why? It proves the Command Prompt display is a GUI, not a CLI.



# DOS Review Lab

- [Not DOS but worth knowing] The Windows Registry is a hierarchical database that stores configuration settings and options for low-level OS components and applications running on the platform.
- Edit with RegEdit (With caution)
- Contains two basic elements: keys and values.
- Root Keys (aka Hives) vary across Windows versions, some are:
  - ◆ HKEY\_CLASSES\_ROOT
  - ◆ HKEY\_CURRENT\_USER
  - ◆ HKEY\_LOCAL\_MACHINE aka HKLM (Tip: Start with this one)
  - ◆ HKEY\_USERS
  - ◆ HKEY\_CURRENT\_CONFIG
  - ◆ HKEY\_DYN\_DATA
- HKLM is a common target for malware.
- See: <http://msdn.microsoft.com/en-us/library/ms724871.aspx>



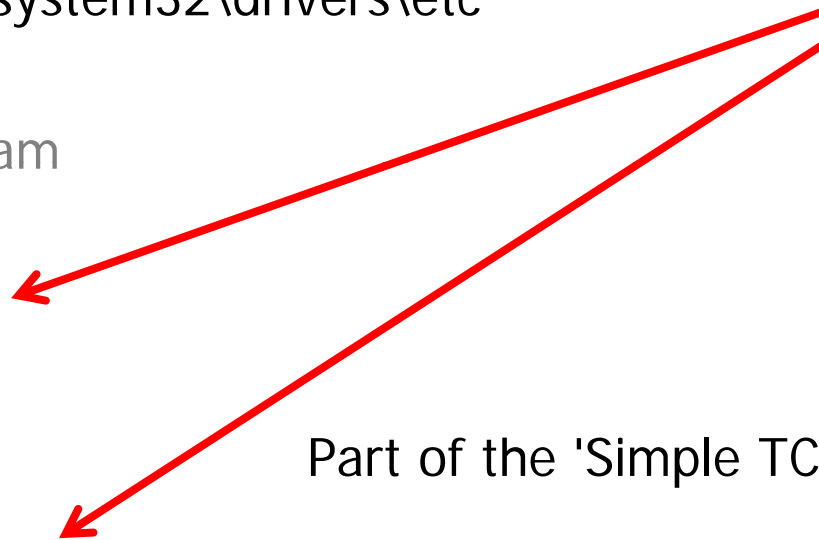
# DOS Review Lab

This folder contains files that are also present in Linux/Unix systems. Use the Type command to view the files. Most are the default file.

C:\windows\system32\drivers\etc

- hosts
- lmhosts.sam
- networks
- ntp.conf
- protocol
- quotes
- resolv.conf
- services

User added



Part of the 'Simple TCP/IP Services' (next slide)



# Simple TCP/IP Services

Simple TCP/IP Services are a collection of command line utilities, and includes the daytime protocol, character generator (chargen), echo protocol, and discard protocol. If installed: A telnet to localhost 13

```
CA: Command Prompt
1:46:27 PM 2/1/2010

Connection to host lost.
```

Echo - based on RFC 862 - uses port 7 - Echoes back data anything received. Echo can be useful as a network debugging monitoring tool. telnet localhost 7

```
CA: Telnet localhost

heel111loo
hheel111loo
tteesstt
tteesstt12123344
```

Chargen is on port 19, use CTRL ] to stop the manic scrolling.

Chargen and echo can be used to produce a DoS. Any ports not needed?

Disable!

```
CA: Telnet localhost

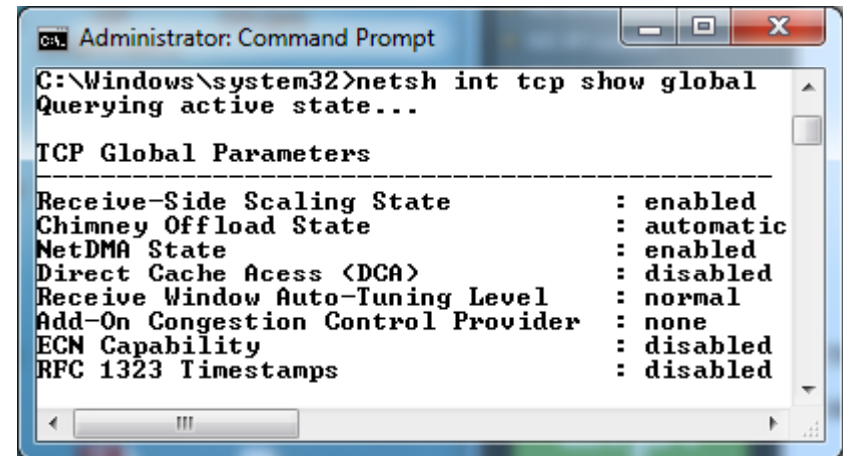
tuvwxyz<|> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`
uvwxyz<|> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`
uvwxyz<|> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`
xyz<|> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`a
yz<|> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`ab
z<|> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`abc
<|> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`abcd
!> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`abcde
!> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`abcdef
!> !"#%&'<>+,-./0123456789:;<=>?@ABCDEFGHIJKLMNopqrstuvwxyz[\]^_`abcdefg
```



# System Tuning via DOS

- Some system parameters can be tuned from the CLI. One example:

```
netsh int tcp show global
```



```
Administrator: Command Prompt
C:\Windows\system32>netsh int tcp show global
Querying active state...

TCP Global Parameters
-----
Receive-Side Scaling State      : enabled
Chimney Offload State          : automatic
NetDMA State                    : enabled
Direct Cache Access (DCA)     : disabled
Receive Window Auto-Tuning Level : normal
Add-On Congestion Control Provider : none
ECN Capability                  : disabled
RFC 1323 Timestamps           : disabled
```

- Add-On Congestion Control Provider

Traditional slow-start and congestion avoidance algorithms in TCP help avoid network congestion by gradually increasing the TCP window at the beginning of transfers until either the TCP Receive Window boundary is reached or packet loss occurs. For broadband internet connections that combine high TCP Window with higher latency (high Bandwidth Delay Product), these algorithms do not increase the TCP windows fast enough to fully utilize the bandwidth of the connection.

- Compound TCP (CTCP) available since Vista and Server 2008 increases the TCP send window more aggressively for broadband connections (with a large TCP Receive Window and BDP) attempting to maximize throughput by monitoring delay variations and packet loss. It also ensures that its behavior does not impact other TCP connections negatively.
- By default, CTCP is turned off except for Server 2008. Turning this option on can significantly increase throughput and packet loss recovery.
- To enable CTCP, in elevated command prompt type:

```
netsh int tcp set global congestionprovider=ctcp
```



# Security Tuning

Some settings appear to only available via Regedit, for example:

## SynAttackProtect

- An undocumented setting provides protection against SYN denial of service (DoS) attacks. When enabled, connections timeout sooner if SYN attack is detected. When set at 1, TCPMaxDataRetransmissions can be lowered further.

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

SynAttackProtect=1 (DWORD, recommended: 1)

Not present in registry by default

- Reference:  
<http://www.speedguide.net/articles>





# DOS Lab Assignment

From the files in the etc folder – *and some reflection...*

Turn in answers to the following to the lab assistant:

0. Name
1. What TCP/UDP uses port 666?
2. What is the assigned number for ICMP?
3. qotd stands for?
4. Effect of a hosts file entry like this:  
    127.0.0.1          pacific.edu
5. Effect of a hosts file entry like this:  
    18.9.22.169      pacific.edu

*A common malware trick is to modify the hosts file.*