The Keys to Using SSH

David Tomaschik
RHCE, LPIC-1
System Administrator, Kennesaw State University
MSCS Student, SPSU
david@systemoverlord.com
http://systemoverlord.com

Special ALE Central Edition!

What is SSH?

- SSH = Secure Shell
- Originally intended as “Encrypted Telnet”
- Allows remote shell (command-line) access
- Connection Encrypted Using Public Key Cryptography
- SSH Version 1: Developed 1995, Now Insecure
- SSH Version 2: Standardized 2006
- Only use SSH2!

Why use SSH?

- Useful for remote system administration
- Transfer files securely
- Run remote applications
- Secure OTHER communications
- Requires Little Bandwidth
- Industry Standard

SSH Clients

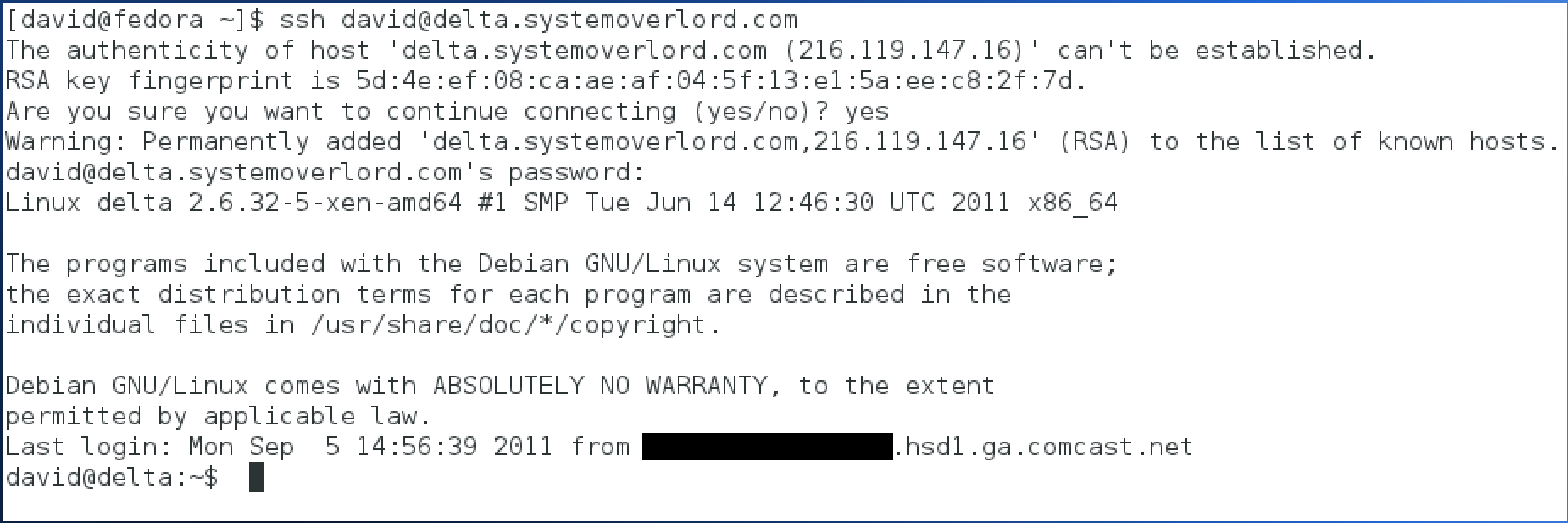
- Linux: OpenSSH; Usually Installed by Default
- OS X: OpenSSH; Installed by Default
- Windows: PuTTY, OpenSSH under Cygwin, Commercial SSH
- Android: ConnectBot + Others
- IOS: iSSH, Prompt, Others

About the Presentation

- Assumes OpenSSH on Linux for both Client and Server
- Some features may require relatively recent versions of OpenSSH

Basic Use

- `ssh user@host.name`



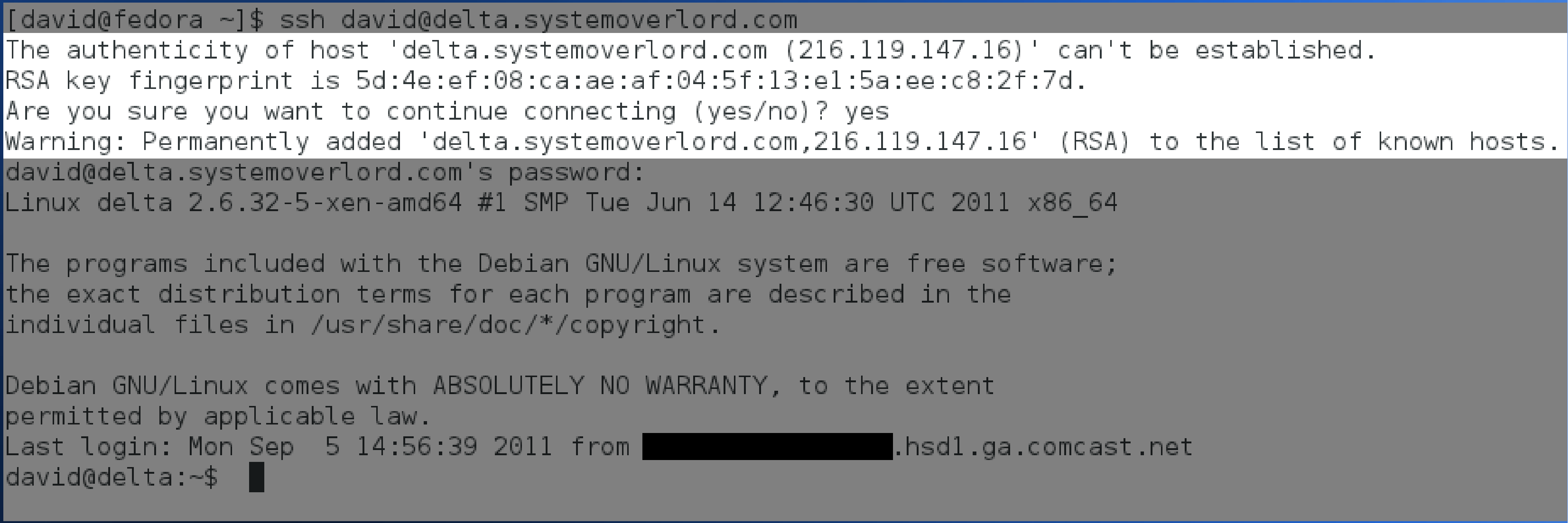
```
[david@fedora ~]$ ssh david@delta.systemoverlord.com
The authenticity of host 'delta.systemoverlord.com (216.119.147.16)' can't be established.
RSA key fingerprint is 5d:4e:ef:08:ca:ae:af:04:5f:13:e1:5a:ee:c8:2f:7d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'delta.systemoverlord.com,216.119.147.16' (RSA) to the list of known hosts.
david@delta.systemoverlord.com's password:
Linux delta 2.6.32-5-xen-amd64 #1 SMP Tue Jun 14 12:46:30 UTC 2011 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep  5 14:56:39 2011 from [redacted].hsd1.ga.comcast.net
david@delta:~$ █
```

Basic Use

- `ssh user@host.name`



```
[david@fedora ~]$ ssh david@delta.systemoverlord.com
The authenticity of host 'delta.systemoverlord.com (216.119.147.16)' can't be established.
RSA key fingerprint is 5d:4e:ef:08:ca:ae:af:04:5f:13:e1:5a:ee:c8:2f:7d.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'delta.systemoverlord.com,216.119.147.16' (RSA) to the list of known hosts.
david@delta.systemoverlord.com's password:
Linux delta 2.6.32-5-xen-amd64 #1 SMP Tue Jun 14 12:46:30 UTC 2011 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Sep  5 14:56:39 2011 from [redacted].hsd1.ga.comcast.net
david@delta:~$
```

Verifying Who You're Connecting To

- The highlighted lines show you which host you are connecting to along with the key fingerprint.
- The key fingerprint is cryptographic proof that your connection is not being tampered with.
- Depending on your level of paranoia:
  - Get the fingerprint from the system administrator
  - Make your first connection from a 'trusted' network
  - Just ignore it and hope its ok

What You Can Do Now

- Run Commands Remotely
  - Install packages/services
  - Configure applications
  - Start/stop services
- Edit Files Remotely
  - vi, nano, etc. (Masochists may even use emacs)
  - Command-line only
  - Plain Text Only

Login Environment

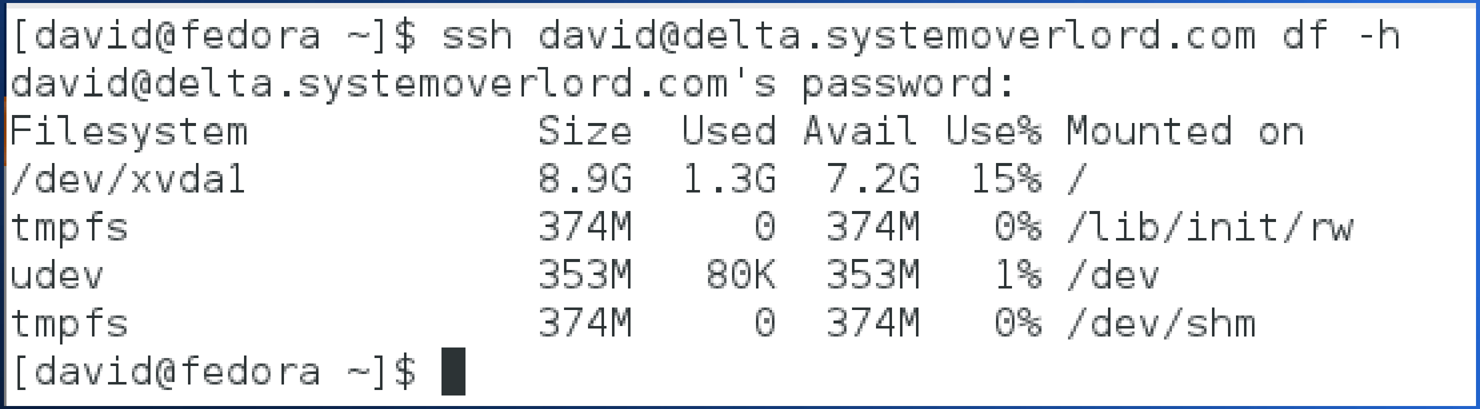
- After connecting
  - /etc/motd, unless ~/.hushlogin
  - Check /etc/nologin
  - Drop privileges (switch to user)
  - /etc/ssh/sshrc, ~/.ssh/rc
  - Run shell or command
- `SSH_CONNECTION`
  - <client ip> <client port> <server ip> <server port>

IPv6

- SSH works well over IPv6 (naturally)
- IPv6 Addresses should be specified in square brackets, e.g., [2600:3c03::f03c:91ff:fe93:f3fb]
    - Or use a hostname
- Can be forced
    - -6 to force IPv6
    - -4 to force IPv4

Run a Single Command

- ssh user@host.name COMMAND

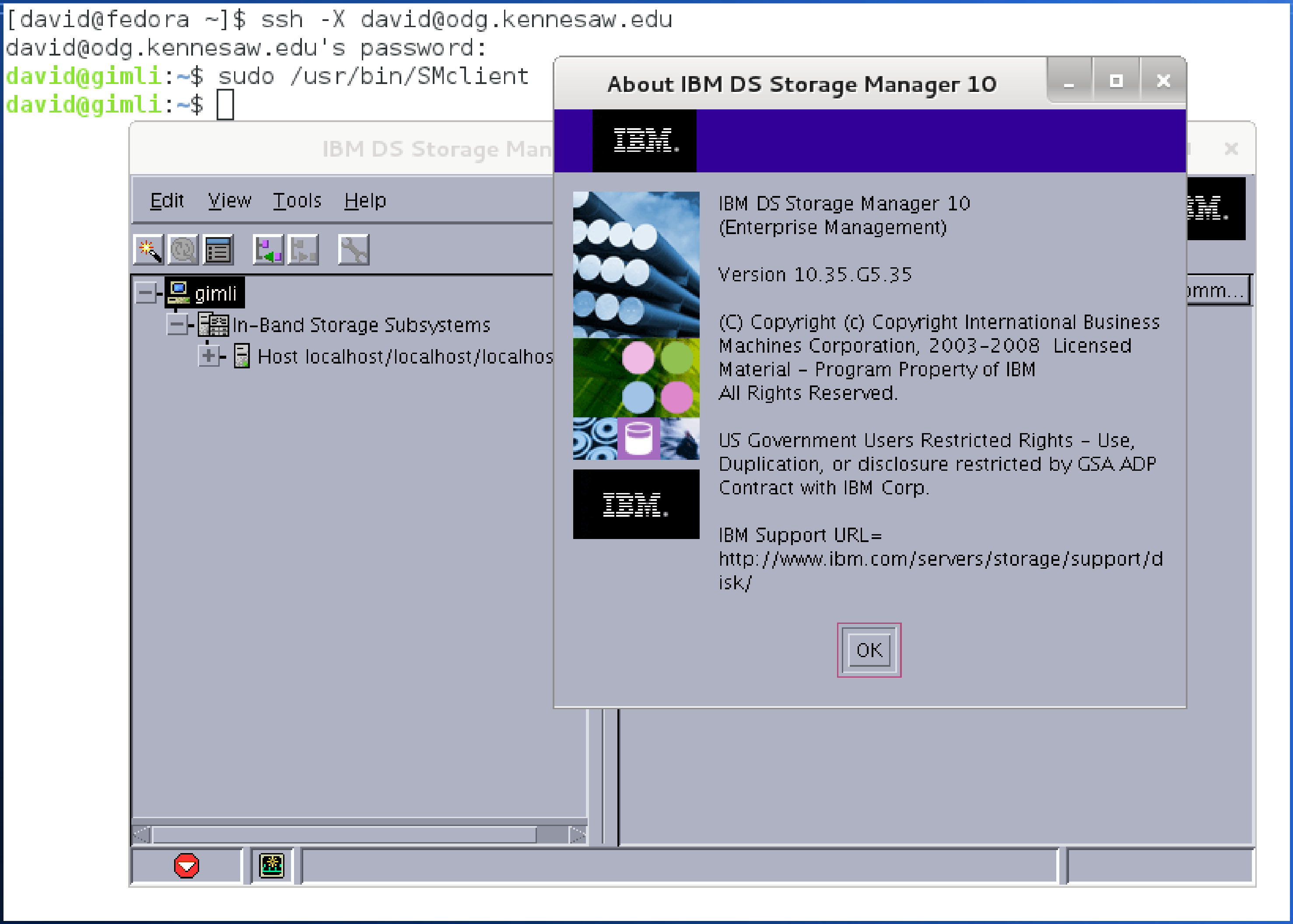


```
[david@fedora ~]$ ssh david@delta.systemoverlord.com df -h
david@delta.systemoverlord.com's password:
Filesystem            Size  Used Avail Use% Mounted on
/dev/xvda1            8.9G  1.3G  7.2G  15% /
tmpfs                 374M     0  374M   0% /lib/init/rw
udev                  353M   80K  353M   1% /dev
tmpfs                 374M     0  374M   0% /dev/shm
[david@fedora ~]$ 
```

Remote GUI (X Forwarding)

- Headless/Remote Server?
- Application that “must” be GUI?
- No Problem!
- `ssh -X user@host.name`
    - Then run command
- `ssh -X user@host.name command`

Remote GUI (X Forwarding)



```
[david@fedora ~]$ ssh -X david@odg.kennesaw.edu
david@odg.kennesaw.edu's password:
david@gimli:~$ sudo /usr/bin/SMclient
david@gimli:~$ 
```

About IBM DS Storage Manager 10

IBM DS Storage Manager 10
(Enterprise Management)

Version 10.35.G5.35

(C) Copyright (c) Copyright International Business Machines Corporation, 2003-2008 Licensed Material - Program Property of IBM
All Rights Reserved.

US Government Users Restricted Rights - Use, Duplication, or disclosure restricted by GSA ADP Contract with IBM Corp.

IBM Support URL=
http://www.ibm.com/servers/storage/support/disk/

Getting Files From Here to There (Or from There to Here)

- scp (Secure Copy)
- Basic form similar to cp
    - scp [path1] [path2]
- Path can be a local path or remote path:
    - user@host:/path/to/file
    - Relative paths from your home directory
- `scp Documents/Presentation.pdf david@work:Documents/`

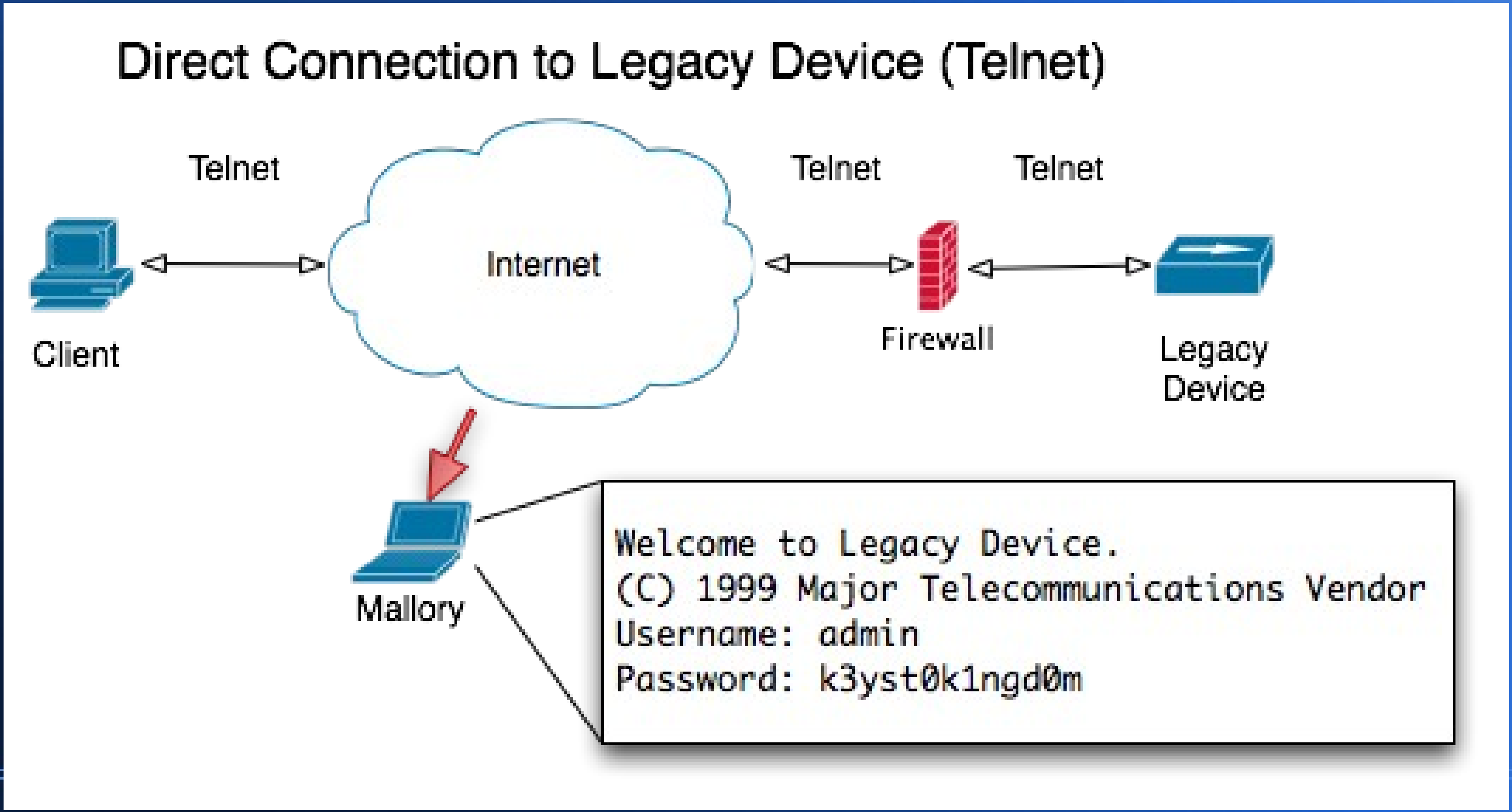
Another Way to Move Files

- SFTP
  - More like FTP, but encrypted via SSH
- GUIs Available
  - gftp on Linux
  - WinSCP on Windows
  - FireFTP (In Firefox)

SSH Tunneling (Port Forwarding)

- Tunnel Arbitrary TCP Connections Across SSH
  - Encrypted
  - Authenticated
  - Tunnel through Firewalls

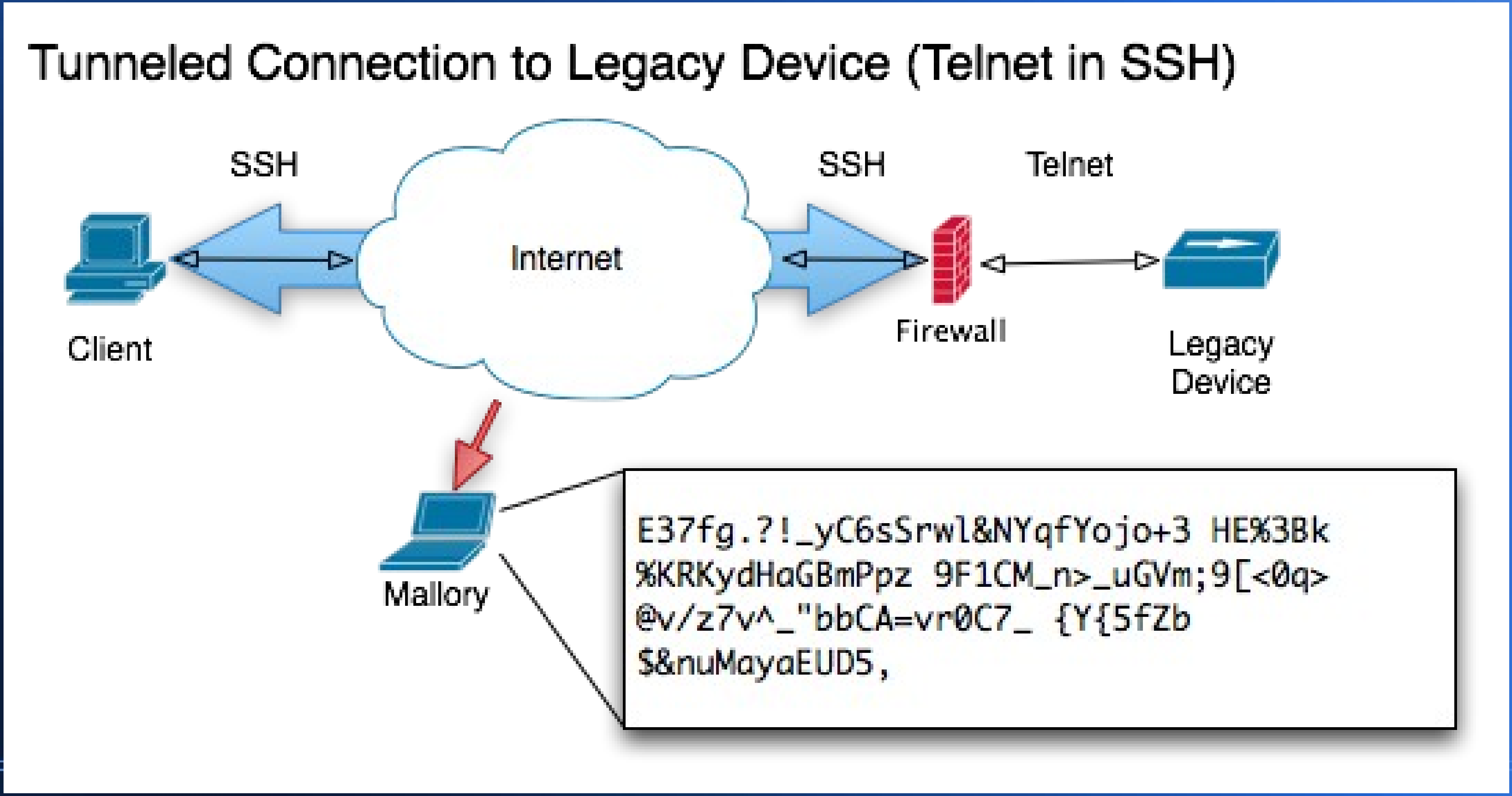
SSH Tunneling



Direct Connection to Legacy Device (Telnet)

```
Welcome to Legacy Device.
(C) 1999 Major Telecommunications Vendor
Username: admin
Password: k3yst0k1ngd0m
```

SSH Tunneling


Tunneled Connection to Legacy Device (Telnet in SSH)
SSH
Internet
SSH
Telnet
Client
Firewall
Legacy Device
Mallory
E37fg.?!_yC6sSrwl&NYqfYojo+3 HE%3Bk
%KRKydHaGBmPpz 9F1CM_n>_uGVm;9[<0q>
@v/z7v^_"bbCA=vr0C7_ {Y{5fZb
$&nuMayaEUD5,

SSH Tunneling (Syntax)

- Forward single point
  - Add -L <localport>:<remotehost>:<remoteport>
  - ssh -L8000:10.10.10.10:80 user@firewall
  - Open web browser to http://localhost:8000/
- Dynamic Proxy
  - Add -D <localport>
  - SOCKS 4/5 Protocol Support
  - Works with any SOCKS-aware application

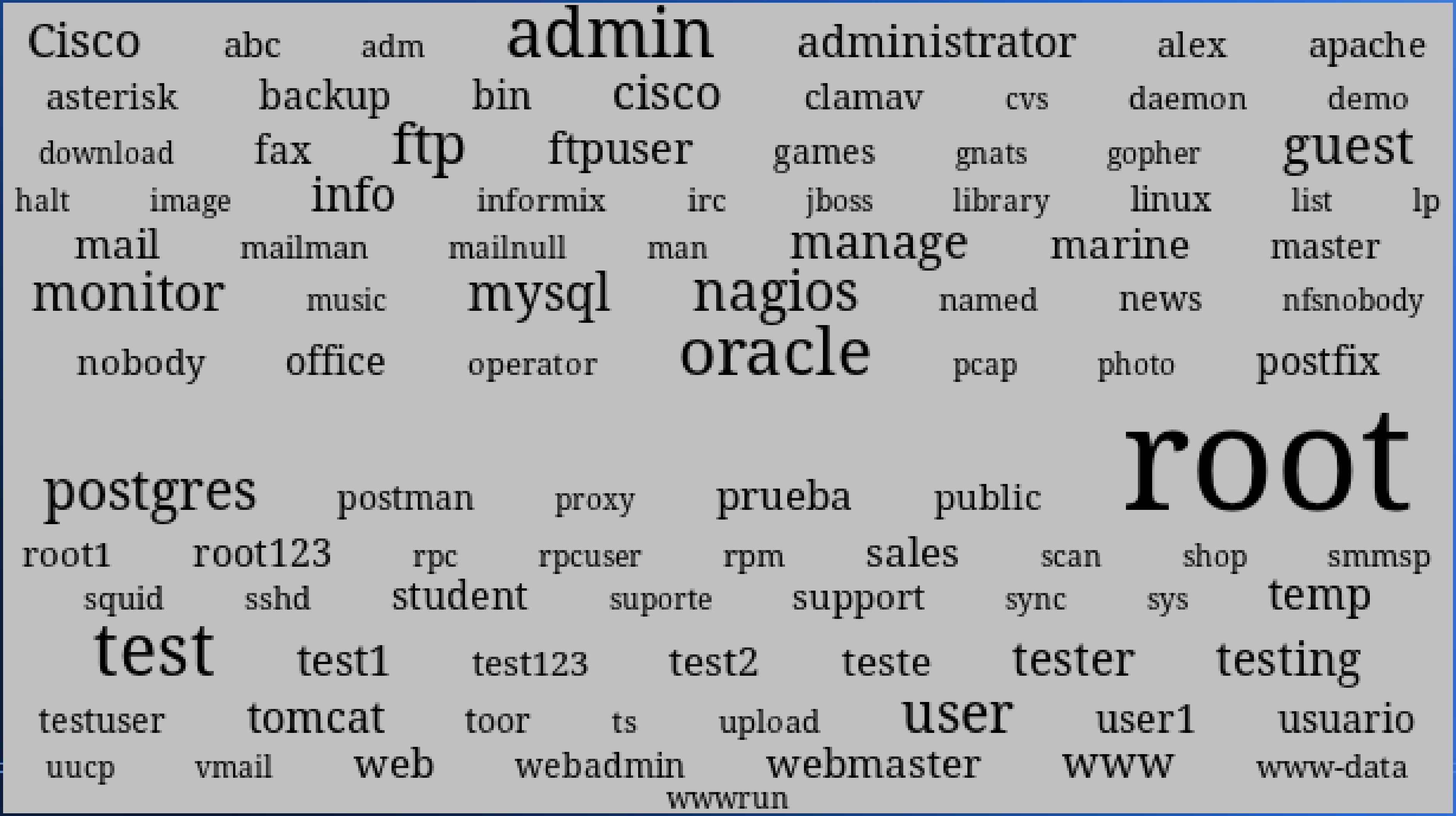
SSH Tunneling (Edge Cases)

- Reverse Tunnel
  - Tunnels connections from server to client
  - -R <remoteport>:<host>:<hostport>
- Allow others to use tunnels
  - -g option
  - Use with caution!
- Only do port forwarding
  - -N (No Command)

A Word About Security

- SSH gets brute forced. A lot.

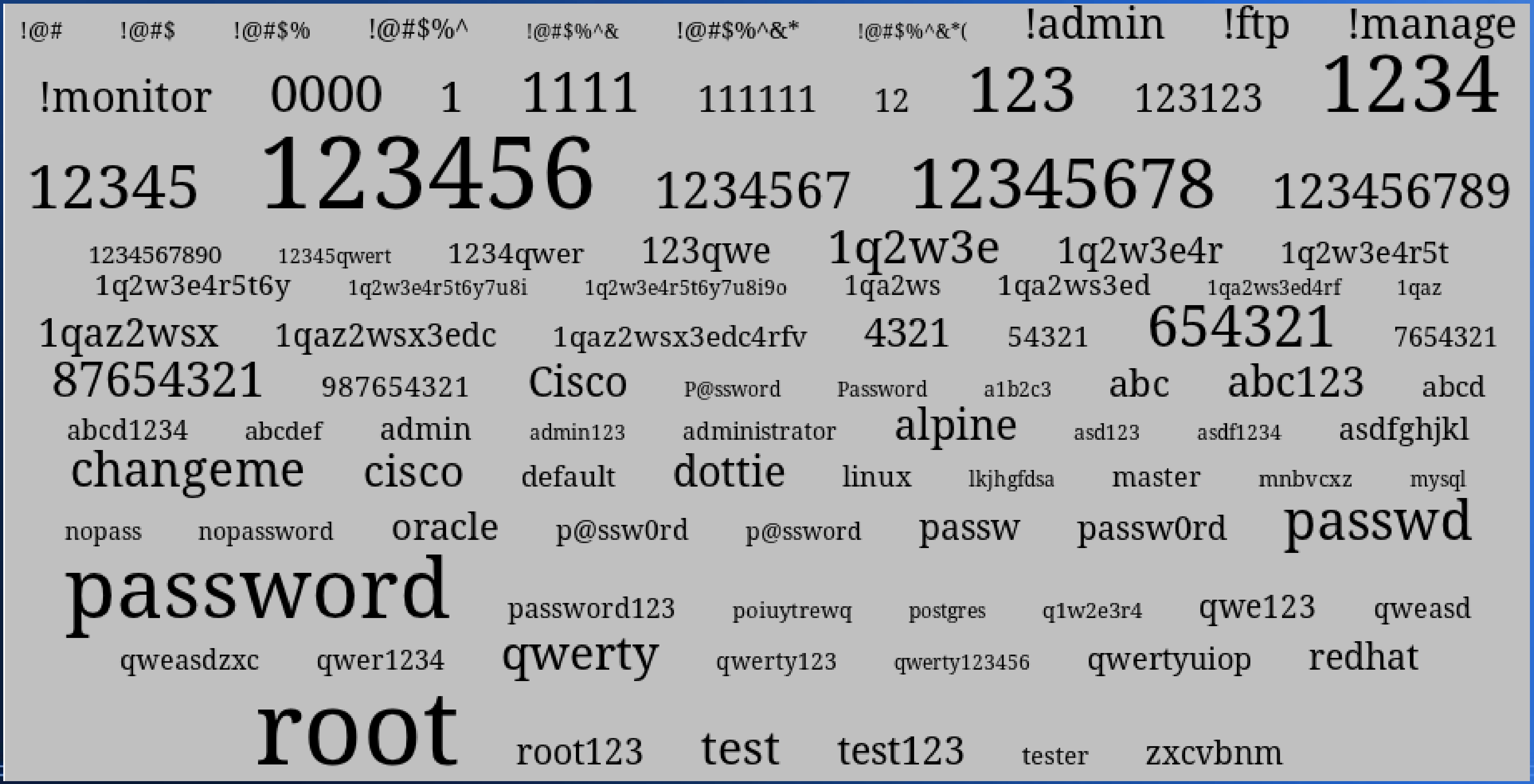
Popular Brute Force Usernames



Cisco abc adm admin administrator alex apache
asterisk backup bin cisco clamav cvs daemon demo
download fax ftp ftpuser games gnats gopher guest
halt image info informix irc jboss library linux list lp
mail mailman mailnull man manage marine master
monitor music mysql nagios named news nfsnobody
nobody office operator oracle pcap photo postfix
postgres postman proxy prueba public root
root1 root123 rpc rpcuser rpm sales scan shop smmsp
squid sshd student suporte support sync sys temp
test test1 test123 test2 teste tester testing
testuser tomcat toor ts upload user user1 usuario
uucp vmail web webadmin webmaster www www-data
wwwrun

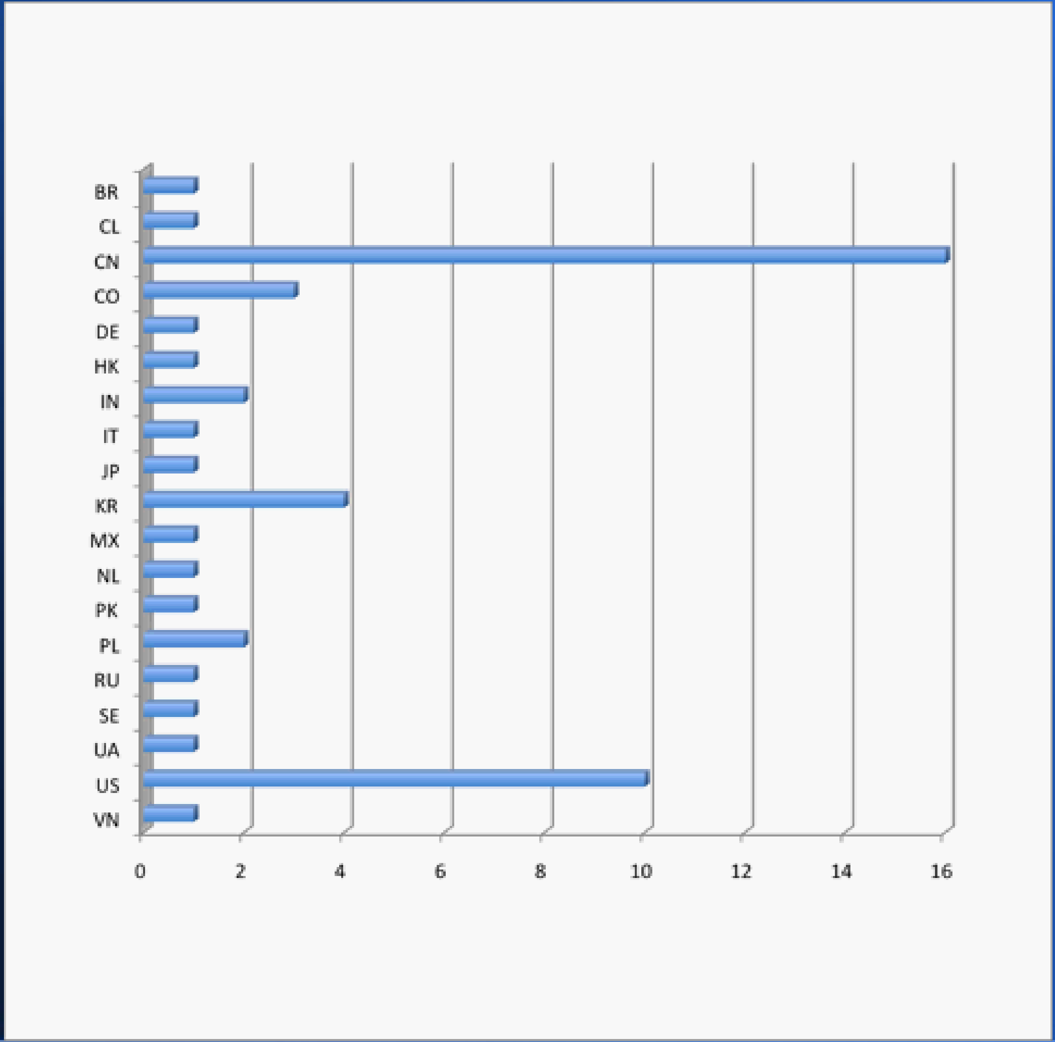
http://www.dragonresearchgroup.org/insight/sshpwauth-cloud.html

Popular Brute Force Passwords



http://www.dragonresearchgroup.org/insight/sshpwauth-cloud.html

Where are they coming from?



Source: Cisco Systems

Security Measures

- Use an alternate port (reduces noise, but is NOT security)
- Use a strong password (always a good idea)
- Use Fail2Ban (Firewall rules from too many bad logins)
- Use SSH Keys!

SSH Keys?

- An SSH Key 'replaces' your password
    - Private key: kept by user to authenticate
    - Public key: placed on servers to identify user
- ssh-keygen to create new key pair
    - Use a passphrase!
- ssh-copy-id will copy the public key over

SSH Key Strength

- Typically 2048 bit RSA
  - ~112 bits of entropy
- Not going to happen in an online attack
- Protect private key with passphrase
- Keep the private key private!
- On the other hand...
  - If your local system is compromised, you have all kinds of problems

Avoiding the Passphrase

- ssh-agent caches the key for you
- eval \`ssh-agent\` to load into current session
- Type passphrase once
- Many desktop environments start ssh-agent (or a clone) for you
- gpg-agent can also function as an agent for SSH keys
    - GPG Keys can also be used for authentication

SSH Access Control

- `/etc/ssh/sshd_config`
  - PasswordAuthentication
  - PubkeyAuthentication
  - HostBased, ChallengeResponse, KeyboardInteractive, etc.
  - AllowGroups, AllowUsers (intersection)
  - DenyGroups, DenyUsers (union)
  - UsePAM (default no, but most distros ship yes)
    - Only account and session for key-based auth

SSHD Permissions

- AllowTCPForwarding
  - PermitOpen
- AllowAgentForwarding
- X11Forwarding
- PermitTunnel (tun forwarding)
- PermitUserEnvironment

Shortcuts

- You could type something like this:

  -
    ```
    ssh -X -L 8000:10.10.10.10:80 -p 2200
      johndoe@devserver.somecompany.com
    ```
- Or you could set up to do:

  -
    ```
    ssh dev
    ```
- In a day, I make 20+ SSH connections
  - What would you do?

~/.ssh/config (Example)

```
Host dev
    User johndoe
    Hostname devserver.somecompany.com
    Port 2200
    ForwardX11 yes
    LocalForward 8000 10.10.10.10:80
```

Speeding Up SSH

- SSH2 Allows Multiple Channels Per Connection
- SSH Multiplexing

```
• ControlMaster    auto
• ControlPath      ~/.ssh/master/%r@%h:%p
• ControlPersist   yes
```

Stayin' Alive

- TCPKeepAlive [yes|no]
  - TCP-level Keep Alive packets
- ServerAliveInterval [sec.]
  - Encrypted packets requesting response from server.

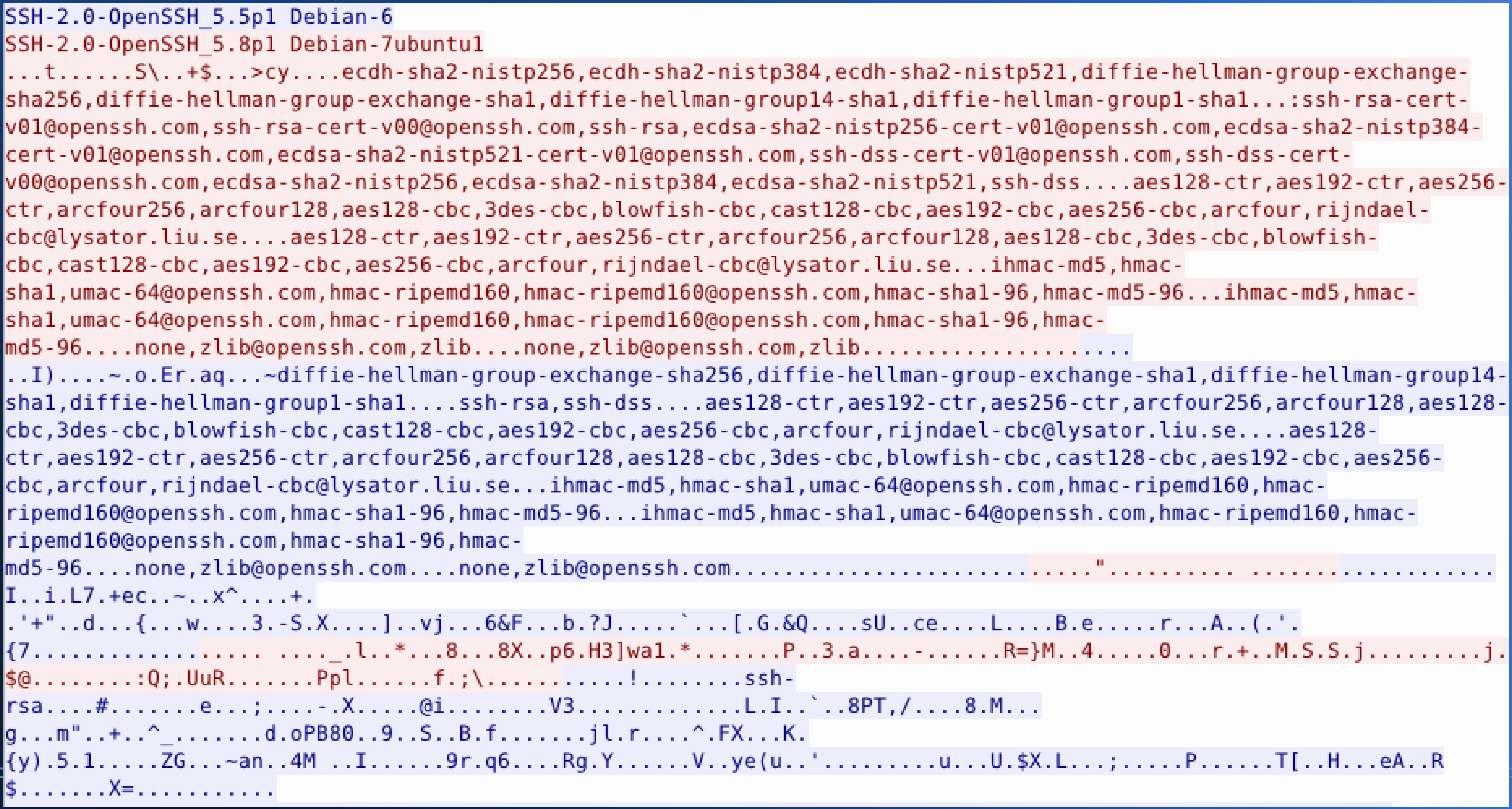
Let's Bust Out of Here!

- Some venues block port 22
    - More likely, allow limited ports
    - Like... this venue.
- Alternate Port
    - 443 if you're not running HTTPS on the server
    - Most places just let 443 out

Layer 7 Firewalls

- SSH is encrypted!
  - But the first step of the handshake is not
  - `SSH-2.0-OpenSSH_5.5p1 Debian-6`

Really!



```
SSH-2.0-OpenSSH_5.5p1 Debian-6
SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1
...t......S\..+$...>cy....ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-
sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1...:ssh-rsa-cert-
v01@openssh.com,ssh-rsa-cert-v00@openssh.com,ssh-rsa,ecdsa-sha2-nistp256-cert-v01@openssh.com,ecdsa-sha2-nistp384-
cert-v01@openssh.com,ecdsa-sha2-nistp521-cert-v01@openssh.com,ssh-dss-cert-v01@openssh.com,ssh-dss-cert-
v00@openssh.com,ecdsa-sha2-nistp256,ecdsa-sha2-nistp384,ecdsa-sha2-nistp521,ssh-dss....aes128-ctr,aes192-ctr,aes256-
ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-
cbc@lysator.liu.se....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-
cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se...ihmac-md5,hmac-
sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96...ihmac-md5,hmac-
sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-sha1-96,hmac-
md5-96....none,zlib@openssh.com,zlib....none,zlib@openssh.com,zlib......................
..I)....~.o.Er.aq...~diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1,diffie-hellman-group1-sha1....ssh-rsa,ssh-dss....aes128-ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-
cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-cbc,arcfour,rijndael-cbc@lysator.liu.se....aes128-
ctr,aes192-ctr,aes256-ctr,arcfour256,arcfour128,aes128-cbc,3des-cbc,blowfish-cbc,cast128-cbc,aes192-cbc,aes256-
cbc,arcfour,rijndael-cbc@lysator.liu.se...ihmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96...ihmac-md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-
md5-96....none,zlib@openssh.com....none,zlib@openssh.com...............................".......... ...................
I..i.L7.+ec..~..x^....+.
.'+"..d...{...w....3.-S.X....]..vj...6&F...b.?J.....`...[.G.&Q....sU..ce....L....B.e.....r...A..(.'.
{7................ ...._.l..*...8...8X..p6.H3]wa1.*.......P..3.a....-......R=}M..4.....0...r.+..M.S.S.j.........j.
$@........:Q;.UuR.......Ppl......f.;\...............!........ssh-
rsa....#.......e...;....-.X.....@i........V3.............L.I..`..8PT,/....8.M...
g...m"..+..^_.......d.oPB80..9..S..B.f.......jl.r....^.FX...K.
{y).5.1.....ZG...~an..4M ..I......9r.q6....Rg.Y......V..ye(u..'.........u...U.$X.L...;.....P......T[..H...eA..R
$.......X=...........
```

So what's left to do?

- Tunnel-in-tunnel
  - openssl s_client → stunnel
  - Bad for latency
  - Virtually indistinguishable from HTTPS or other SSL traffic (it **IS** SSL traffic)
- Obfuscated SSH
  - Requires patched client & server
  - https://github.com/inf0/obfuscated-openssh

Fun Things
(For Some Definition of “Fun”)

- Copy a file between two hosts that can't directly communicate
  - scp -3 host1:/file1 host2:/file2
- Force a user to run a certain command (sshd_config)
  - Match User <username>
  - ForceCommand <command>

Questions/Demos

- Questions?
- Comments?