

SSH

```
Terminal
RSA key fingerprint is e5:30:7a:d8:d8:57:ca:b9:a4:30:0d:0a:db:40:4c:d7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'saturn.cs.dixie.edu,144.38.192.86' (RSA) to the list
of known hosts.
Now try logging into the machine, with "ssh 'saturn.cs.dixie.edu'", and check in
:

~/.ssh/authorized_keys

to make sure we haven't added extra keys that you weren't expecting.

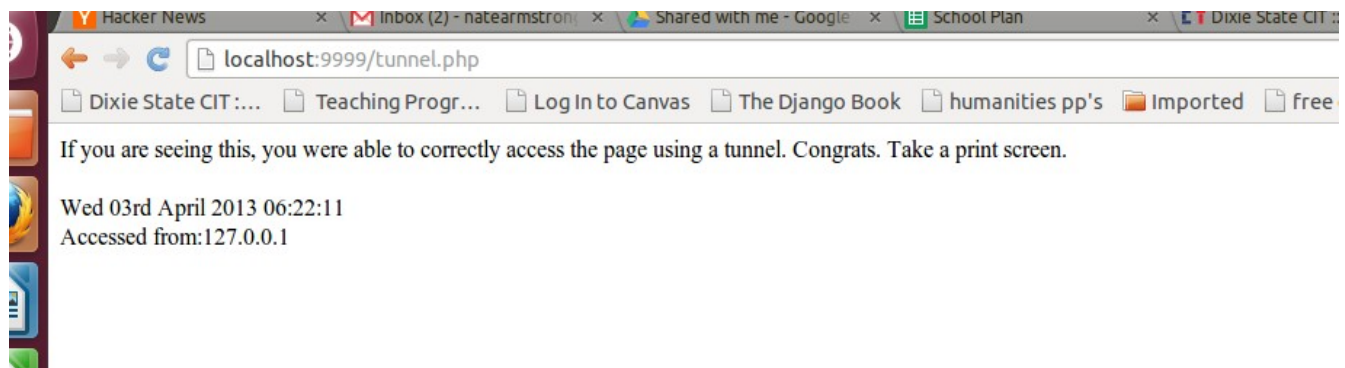
narmstrong@bismuth:~$ ssh saturn.cs.dixie.edu
Linux saturn 2.6.32-46-server #105-Ubuntu SMP Fri Mar 1 00:18:55 UTC 2013 x86_64
GNU/Linux
Ubuntu 10.04.4 LTS

Welcome to the Ubuntu Server!
* Documentation: http://www.ubuntu.com/server/doc

11 packages can be updated.
11 updates are security updates.

New release 'precise' available.
Run 'do-release-upgrade' to upgrade to it.
```

Tunnel



Look at the output for the netstat command on both machines (netstat -atu):

1:

```
tcp    0    0 it4500.cs.dixie.edu:ssh bismuth.cs.dixie.:33640 ESTABLISHED
tcp    0    0 bismuth.cs.dixie.:33640 it4500.cs.dixie.edu:ssh TIME_WAIT
```

```
tcp    0    0 it4500.cs.dixie.edu:ssh phony8-210.it2400:56893 ESTABLISHED
tcp    0    0 it4500.cs.dixie.edu:ssh bismuth.cs.dixie.:33640 ESTABLISHED
tcp    0    0 it4500.cs.dixie.edu:ssh polonium.cs.dixie:53356 ESTABLISHED
tcp    0    0 it4500.cs.dixie.edu:ssh astatine.cs.dixie:58491 ESTABLISHED
tcp    0    0 it4500.cs.dixie.edu:ssh saturn.cs.dixie.e:36468 ESTABLISHED
tcp    0    0 it4500.cs.dixie.edu:ssh saturn.cs.dixie.e:36470 ESTABLISHED
tcp    0    0 it4500.cs.dixie.edu:ssh saturn.cs.dixie.e:36462 ESTABLISHED
tcp6   0    0 [::]:ssh [::]:* LISTEN
udp    0    0 *:35745 *: *
udp    0    0 *:icpv2 *: *
it2400@it2400:~$ exit
logout
Connection to it2400.cs.dixie.edu closed.
narmstrong@bismuth:~$ netstat -atu
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address          State
tcp    0      0 *:sunrpc                 *: *                      LISTEN
tcp    0      0 *:35152                   *: *                      LISTEN
tcp    0      0 *:36950                   *: *                      LISTEN
tcp    0      0 *:49814                   *: *                      LISTEN
tcp    0      0 *:ssh                     *: *                      LISTEN
tcp    0      0 localhost:ipp             *: *                      LISTEN
tcp    0      0 *:54555                   *: *                      LISTEN
tcp    0      0 *:nfs                     *: *                      LISTEN
tcp    0      0 *:42371                   *: *                      LISTEN
tcp    0      0 bismuth.cs.dixie.:55555  uranus.cs.dixie.ed:ldap ESTABLISHED
tcp    0      0 bismuth.cs.dixie.:38254  saturn.cs.dixie.:sunrpc TIME_WAIT
tcp    0      0 bismuth.cs.d:supfilesrv  saturn.cs.dixie.e:45519 ESTABLISHED
tcp    0      0 bismuth.cs.dixie.:55844  uranus.cs.dixie.ed:ldap ESTABLISHED
tcp    0      0 bismuth.cs.dixie.ed:908  saturn.cs.dixie.edu:nfs ESTABLISHED
tcp    0      0 bismuth.cs.dixie.:55556  uranus.cs.dixie.ed:ldap ESTABLISHED
tcp    0      0 bismuth.cs.dixie.:51029  nuq04s08-in-f1.1e:https ESTABLISHED
tcp    0      0 bismuth.cs.dixie.:33640  it4500.cs.dixie.edu:ssh TIME_WAIT
tcp    0      0 bismuth.cs.dixie.:56893  phony8-210.it2400:56893 ESTABLISHED
```

Checksumming

md5sum -c alice.md5

```
it2400@it2400: ~
narmstrong@bismuth:~/school/it2400/labs/security$ md5sum -c alice.md5
alice.txt: OK
narmstrong@bismuth:~/school/it2400/labs/security$
```

md5 diff fails because it is Bllice and not Alice.

```
narmstrong@bismuth:~/school/it2400/labs/security$ diff alice.txt alice2.txtj
diff: alice2.txtj: No such file or directory
narmstrong@bismuth:~/school/it2400/labs/security$ diff alice.txt alice2.txt
1c1
<
    ALICE'S ADVENTURES IN WONDERLAND
---
>
    BLICE'S ADVENTURES IN WONDERLAND
narmstrong@bismuth:~/school/it2400/labs/security$ diff alice.md5 alice2.md5
1c1
< 94e10e8c6b62c921f30a5429afc2d817  alice.txt
---
> 94e10e8c6b62c921f30a5429afc2d817  alice2.txt
narmstrong@bismuth:~/school/it2400/labs/security$
```

Encryption part 1 was successful

```
out.txt ✖
IF you are reading this file, HOORAY! You have successfully decrypted it using
openssl. I know you are excited to do more with encryption, but this is as far as
we are going. By the way, we could have encrypted any type of file, this is just a
plain old text file!

~Cheers!|
```

More Encryption

```
2013-04-03 19:10:42 (89.4 MB/s) - 'image.txt' saved [669/669]

narmstrong@bismuth:~/school/it2400/labs/security$ base64 -d image.txt > image.gif
narmstrong@bismuth:~/school/it2400/labs/security$ ls
alice2.md5  alice2.txt  alice.md5  alice.txt  image.gif  image.txt  out.txt  secret.txt.enc
narmstrong@bismuth:~/school/it2400/labs/security$
```

