

How to SSH to Fermilab using Kerberos

BV

[2014-04-22 Tue 13:04]

It ain't easy.

1 Nominal procedure

If all is set up one does:

```
$ kinit principle@FNAL.GOV
$ ssh principle@somehost.fnal.gov
```

Of course, nothing is nominal.

2 Unknown realm

If kinit gives:

```
kinit: Cannot find KDC for requested realm while getting initial credentials
```

It means your system does not have the `FNAL.GOV` realm added to your `file:///etc/krb5.conf` file. It needs a `FNAL.GOV` stanza like shown in this example.

If you can not edit the system `krb5.conf` file you can make your own and call it out to Kerberos by setting:

```
$ wget http://security.fnal.gov/krb5.conf
$ export KRB5_CONFIG=$HOME/krb5.conf
```

If your local system uses Kerberos as well then you should merge its `krb5.conf` and the one from Fermilab.

3 Weak Authentication

Fermilab loves to call their use of Kerberos "strong authentication". Well, to use it the first thing you have to do is configure to connect with weak crypto. This boils down to adding the line:

```
allow_weak_crypto = true
```

To you `krb5.conf` file. See above for using a per-user version of this file.

4 Challenged for crypto card

When ssh'ing you might see:

```
$ ssh principle@somehost.fnal.gov
CryptoCard RB-1
Press ENTER and compare this challenge to the one on your display
Challenge is [34387079], Enter the displayed response:
```

What is this antiquated thing? Never mind, just try:

```
$ ssh -o "GSSAPIAuthentication yes" principle@somehost.fnal.gov
```

If that works, you can make it default by editing your file:///home/bv/.ssh/config file so it looks like:

```
host *.fnal.gov
    GSSAPIAuthentication yes
    # ... other options, "User" is a good one
```