**Error: Trying krb4 rlogin... krb\_sendauth failed: You have no tickets cached**

Resolution: You have no valid Kerberos tickets, which can be verified by running **klist** (the output will either be empty or show expired tickets). Obtain a new ticket using **kinit**:

### Error: Connection Refused

Let's take a look at this. First of all, you can see that **krb5-rsh** has some fallbacks built-in. It first tries to connect using the Kerberos 5 protocol, then Kerberos 4, and then using the normal, non-kerberized rsh. We are only interested in the krb5 result. If any of the other two methods succeed (the krb4 or plain rsh), it's still not what we want (and you will probably want to disable them somehow, because no one setting up a new Kerberos realm in the 21st century should be running either krb4 or unprotected rsh).

So where's the problem? Assuming that you did everything right (installed krb5-rsh-server and restarted inetd), the problem is very simple. Namely, by default, kerberized servers in Debian do not accept unencrypted connections! So, on next attempt, add -x on the command line.

### Error: Server not found in Kerberos database

As explained in the section called “The role of Kerberos within a network”, both the users and the services must have an appropriate principal entry in the Kerberos database. While users are in form of***NAME/ROLE***, services are in form ***SERVICE-NAME/HOSTNAME***. So we need to add a principal for service "host" (common name for all shell services), on host where the service is provided — ***abc.pqr.com***. (Strictly, the service is provided on the server, on krb1. ***pqr.com***, but in a single-machine setup, the hostname's FQDN returns ***abc.pqr.com*** so we must use that).

Within the same session, you will almost always want to export that principal's key to a keytab file. Exporting will not work as intended if the key was not created in a single **kadmin** session, so the below solution deletes the existing key (if any), creates it anew and exports it to a file. As to what you need to do with the keytab file after creation — you need to move it from the Kerberos server onto the machine providing the service. If that is the same machine, no moving is necessary.

As most of the errors really boil down to this step, we also take care of re-initializing the ticket properly, to minimize the chance of a mistake:

### Error: No such file or directory

The above error indicates that we should pay attention to the "e-text" (error text returned to the client). The error text tells us, in kind of a confusing way (since — you see — there is no filename reported), that the /etc/krb5.keytab file on the rsh server is missing altogether. This file needs to exist and contain the service key. The way to obtain the file and the key is to follow the recipe from the section called “Error: Server not found in Kerberos database”.

### Error: Key table entry not found

The server did accept the connection, but the e-text "Key table entry not found" indicates that the service principal (created earlier, host/***abc.pqr.com***) is not listed in the keytab file on rsh server. Follow the recipe in the section called “Error: Server not found in Kerberos database”.

### Error: Key version number for principal in key table is incorrect

The service key has changed on the Kerberos server, and the service did not succeed in proving its identity to the Kerberos server — the file /etc/krb5.keytab on the service did not contain the correct key. Have in mind that the key changes if you run ktadd from within the **kadmin** shell, and the only way to prevent that from happening is to use **kadmin.local** interface and use **ktadd -norandkey** in it. If curious, read up on ktadd behavior in kadmin(8). Follow the recipe in the section called “Error: Server not found in Kerberos database”.

### Error: Client not found in Kerberos database while getting initial credentials

This is Kerberos way of saying "User not found". You either misspelled the principal name ("root/admin" in this case), or you didn't add the principal to the kerberos database in the first place. Adding a principal is performed using the **addprinc** command as shown in the section called “Creating first privileged principal” or the section called “Creating first unprivileged principal”.

### Error: Client not found in Kerberos database while initializing kadmin interface

This is Kerberos way of saying "User not found". You either misspelled the principal name ("root/admin" in this case), or you didn't add the principal to the kerberos database in the first place. Adding a principal is performed using the **addprinc** command as shown in the section called “Creating first privileged principal” or the section called “Creating first unprivileged principal”.

### Error: Decrypt integrity check failed

This is Kerberos way of saying "Password incorrect". In this case, it means that the service key changed on the server, and your your ticket cache no longer contains the ticket with the correct key. Running**kdestroy; kinit** should obtain a new ticket and solve the problem.

### Error: Unsupported key table format version number while adding key to keytab

This usually happens when the local file to which you want to export the key (/etc/krb5.keytab) is in an incorrect format.

The most common reason why this would happen is if you have tried to create an empty file (using **touch** or similar commands) beforehand, and then export the key into it.

To verify that this is indeed the case, try running **klist** on the existing file to which you are attempting to export the key:

The solution is to delete the incorrectly created keytab file, or to choose a different keytab file to which the intended key should be exported.