Apache-Kerberos-AD Authentication

Sunday, May 17, 2015 4:34 PM

Test Kerberos:

- $ kinit username@WINDOWSDOMAIN
- Replace “username” and “WINDOWSDOMAIN” with your AD-credentials. Note that WINDOWSDOMAIN has to be written in CAPITALS for this to work.
- root@sso:~# **apt-get install libapache2-mod-auth-kerb krb5-user**
- root@sso:~# **kinit adminuser@GHFIP.LOCAL**
- root@sso:~# **klist**

Add Active Directory account:

- Created new user as kerberos@ghfip.local in Active Directory which will be used by Linux Host to get authenticated against AD.

Add DNS Record for Linux Host in AD DNS:

- Added DNS A Record as sso.ghfip.local in AD DNS and pointing it to Linux Apache machine 192.168.3.28

Create keytab-file on the AD and then Copy it to Web Server:

- We need to create keytab file on the On Domain Controller, issue the following from a command prompt:
- C:\>ktpass -princ HTTP/<fqdn-hostname-in-DNS>@WINDOWSDOMAIN -mapuser <kerberosuser-AD-username>@WINDOWSDOMAIN -pass <kerberosuser-AD-password> -crypto RC4-HMAC-NT -ptype KRB5_NT_PRINCIPAL -out C:\Temp \kerberos_hostname.keytab
-

```
C:\Users\AdminUser>ktpass -princ HTTP/sso.ghfip.local@GHFIP.LOCAL -mapuser kerberos@GHFIP.LOCAL -pass ghf2212S -crypto RC4-HMAC-NT -ptype KR
B5_NT_PRINCIPAL -out C:\Temp\kerberos_hostname.keytab
Targeting domain controller: GHFServer.GHFIP.local
Successfully mapped HTTP/sso.ghfip.local to kerberos.
Password succesfully set!
Key created.
Output keytab to C:\Temp\kerberos_hostname.keytab:
Keytab version: 0x502
keysize 67 HTTP/sso.ghfip.local@GHFIP.LOCAL ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength 16 (0x7bad4ad5ab30cc9f34b68a31
bcfbba13)
```

- Once keytab file is generated Copied it to Linux Web Server in /etc/apache2/kerberos_hostname.keytab

Configure apache:

```
<Location />
        # http://sso.ghfip.local/
        AuthType Kerberos
        AuthName "Some-Nifty-Name"
        KrbAuthRealms GHFIP.LOCAL
        KrbServiceName HTTP
        Krb5Keytab /etc/apache2/kerberos_hostname.keytab
        require valid-user

    </Location>
```

Testing:

- So now, If you open http://sso.ghfip.local or http://sso.ghfip.local/helloworld.html from the machine in which you are logged in with GHFIP domain user, it should open the Webpage without any credential prompt. (This is called "Integrated Windows Authentication")
- This works only if http://sso.ghfip.local is either automatically detected as "Local Intranet" site or manually added as "Local Intranet" Site in IE Settings in respective PC from which you are trying to open the http://sso.ghfip.local otherwise it will prompt for the credential and once you provide GHFIP domain user credentials you will be able to see the webpage or it will say "Unauthorized message"
- If you open http://sso.ghfip.local from any other PC which is not part of GHFIP AD domain, it will prompt for the credentials and after providing valid credentials, it will open the webpage otherwise it will display "Unauthorized Message" .