# Part 1: Startup Packet Traffic

In this section you will use Wireshark to examine startup traffic. This is partially review and partially new activities. Becoming comfortable with packet sniffing is very important in learning to trouble shoot problems with an Active Directory network. After examining traffic for services, you are familiar with in the next section you will examine Kerberos traffic.

Examine General Startup Traffic

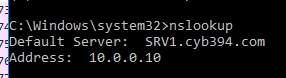
1. Start your SRV1 and SRV2 image and logon with your domain admin credentials.
2. Start Wireshark on both SRV1 and SRV2 and begin capturing packets on both.



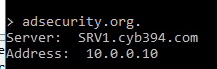
1. From your SRV1 computer, ping the IP address of your SRV2
2. From SRV2 in Apply a display filter.. type icmp



1. Stop and show your professor the number of packets displayed. (Why are there that many packets)
2. From SRV2 open an elevated command prompt and type **nslookup**
3. You should receive the following (IP address may differ). If you do not get this contact your professor or fix the problem on your own.



1. At the prompt type in adsecurity.org. (don’t forget the ending period)



1. On SRV1 in the Apply a display filter.. type dns



1. Locate the Standard query response A record for adsecurity.org. (Show the packet to your professor)
2. Stop the capture on SRV1

## Part 2: Kerberos Ticket Exchanges

In this section you will use Wireshark to examine Kerberos traffic.

1. Start a new Capture on SRV1
2. Start CLIENT1
3. Logon as your personal admin account and get the CLIENT1 ip address.

Continued next page……..

1. Back on SRV1 stop the capture and in the wireshark display filter type kerberos.msg\_type == 10 or kerberos.msg\_type == 11 or kerberos.msg\_type == 12 or kerberos.msg\_type == 13 and ip.addr == 10.0.0.11



\*You should see four **types** of KRB5 protocol ticket types. Look under the Protocol column for KRB5 and under the Info column for the ticket types. Locate the following

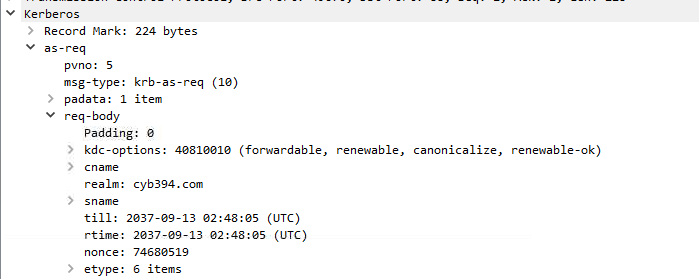
Which computer (SRV1 or CLIENT1) is the source of the AS-REQ packets?

Which computer (SRV1 or CLIENT1) is the source of the AS-REP packets?

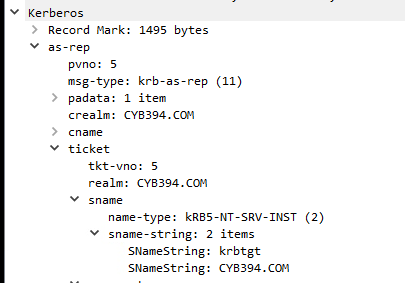
Which computer (SRV1 or CLINET1) is sending the TGS-REQ packets?

Which computer (SRV1 or CLIENT1) is sending the TGS-REP packets?

1. Highlight the **AS-REQ** packet and in the lower pane expand the Kerberos AS-REQ entry, then expand the KDC\_REQ\_BODY as shown below. (You may have different values.)



1. Note the realm name. The Kerberos realm should match your domain name.
2. Highlight the **AS-REP** packet.
3. Expand the content



Under “ticket” what are the KerberosString values?

Reference: “Ticket” is the Ticket Granting Ticket that your work station will need to get Service Tickets to access services on the domain controller.

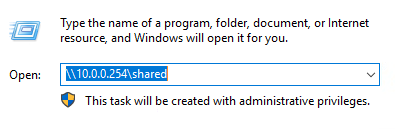
\*Also see if you can locate the port Kerberos operates on. You will notice it should be the Src Port from SRV1 REP packets.

Continued on Next page…….

# Part 3 SPNs

SPN Service Principal Names - is the name by which a Kerberos client uniquely identifies an instance of a service for a given Kerberos target computer. Many common applications will register an SPN. Some examples are SQL and EXCHANGE. These two applications usually have a service that is registered with domain admin credentials. Let’s take a look at some SPNS.

1. We are going to run some scripts as a standard user. But first we need to allow the scripts to run and disable windows defender.
2. Disable Windows Defender on Client1 using Group Policy (see the internet for help/you will need to do this as admin)
3. Log on to client1 as an administrator.
4. Launch powershell
5. Set-ExecutionPolicy Unrestricted
6. Log off
7. Log on to client1 as a standard user (finuser1)
8. Right click on the start menu and select run then type in



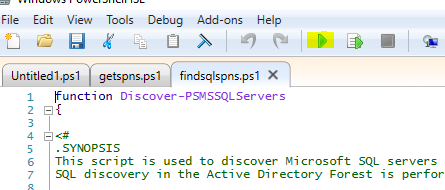
1. Locate the CYB394 folder and double click into it
2. Copy the following to scripts to the desktop



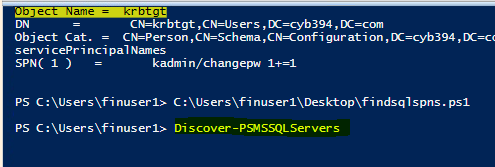
1. Launch Powershell ISE from the startmenu
2. Open the getspns script and run it by pressing the green play (arrow) button. If it fails to run just logout, then back on again
3. You should see a list of hosts and their registered SPNS.



1. All these SPNs are registered with a kerberos ticket.
2. From Powershell ISE open the second script called findsqlspns.ps1 Click the green arrow to run. (This script is making a function called Discover-PSMSSQLServers you will run the function in the next step.



1. Now in PowerShell ISE command window area type Discover-PSMSSQLServers

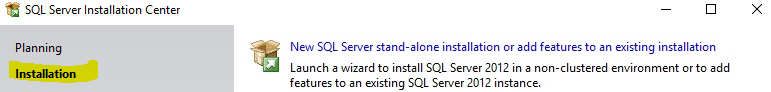


1. You should receive the following results. ) accounts were found because we don’t have SQL installed.

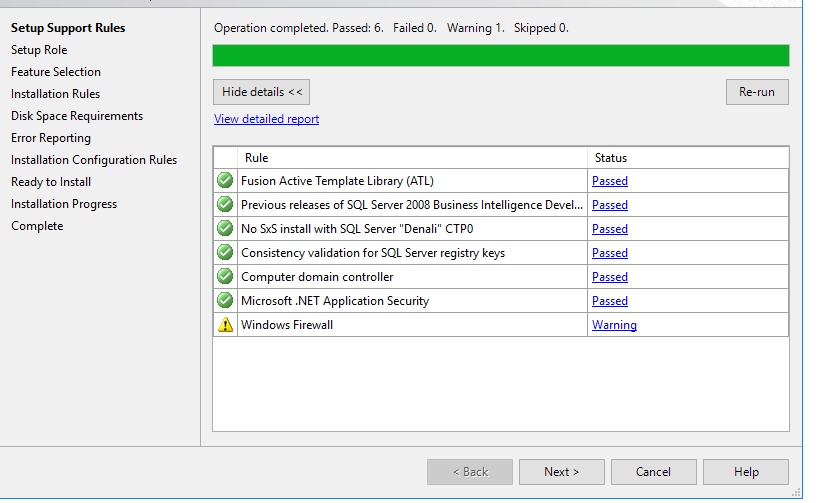


# Part 4 Creating a Bad SPN

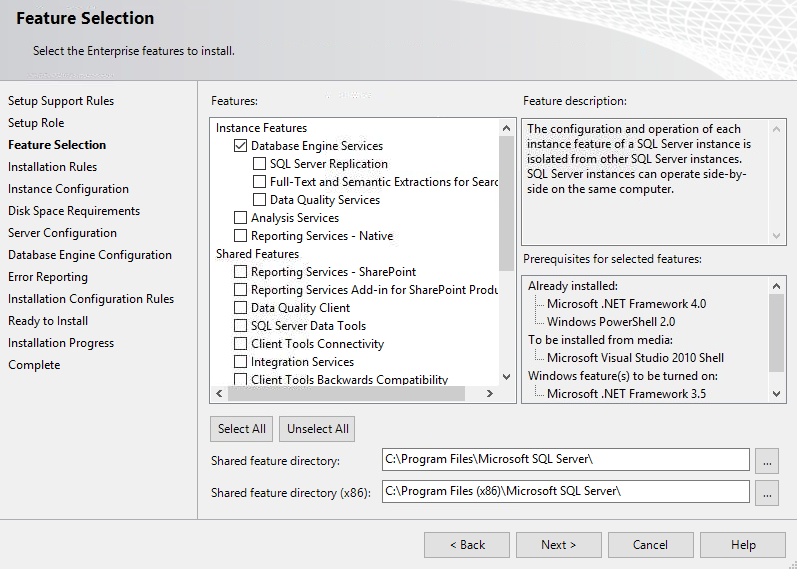
1. Logon to SRV4 using your Personal Domain Admin account
2. Right Click on the Start Menu and select Run
3. In the run box type [\\10.0.0.254\shared\](file:///\\10.0.0.254\shared\)
4. Locate the CYB394 folder and double click into it.
5. Copy the en\_sql\_server\_2017\_standard\_x64\_dvd\_11294407.iso folder to the E:\
6. On SRV1
7. Create a new user Called sqlserviceacct with a password of P@ssw0rd5 set it to never expire. MAKE SURE YOU USE THE PASSWORD I SET!!!! IT’S A ZERO NOT AN O
8. Put it in the domain administrators group.
9. Back on SRV4 mount the en\_sql\_server\_2017\_standard\_x64\_dvd\_11294407.iso SQL ISO by double clicking on it.
10. Locate the setup and double click it to install
11. Click on Installation then click New SQL Server stand-alone…



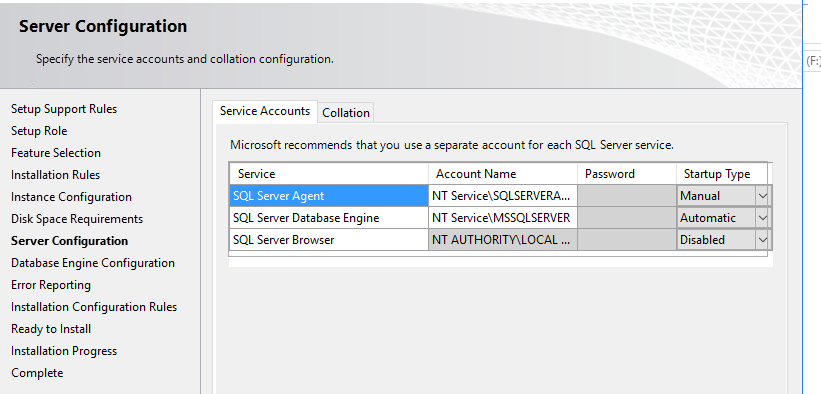
1. Click OK
2. Then Click next until you get to the feature selection



1. On the Feature Selection Page check mark Database Engine Services. Then Click Next

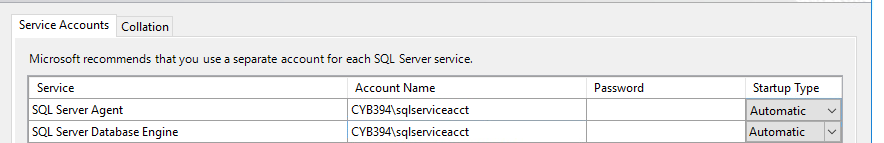


1. Click next until you get to the Server Configuration Page

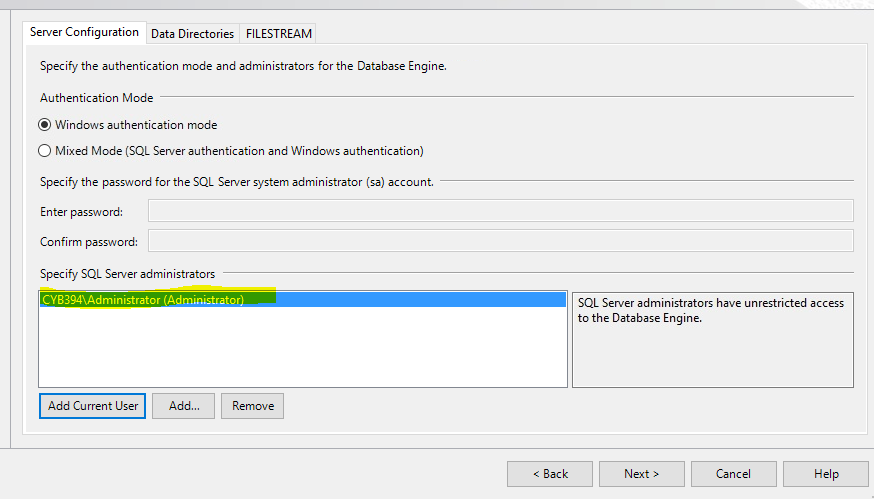


1. Where is says account name set the SQL Server Agent account and the SQl Server Database Engine Account to

CYB394\sqlserviceacct make sure to put in the password of P@ssw0rd5 and set Startup type to Automatic



1. Click Next and Make sure to Add Current User as a sql administrator

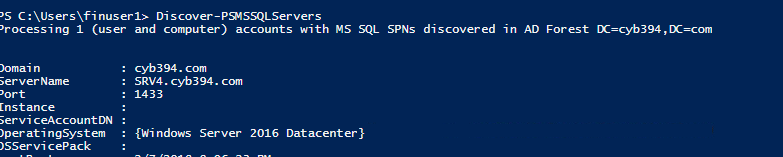


1. Click Next all the way through to complete the install.
2. Once install is complete reboot the server.

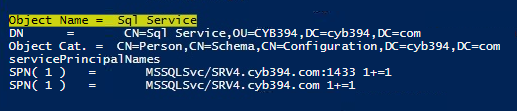
This process should have registered an SPN for SQL server.

# Part 5

1. On Client1 you will need to run the Discover-PSMSQLServers from Powershell ISE again.
2. This time you should get the following result.



1. Also for reference run the getspn script to see the following.



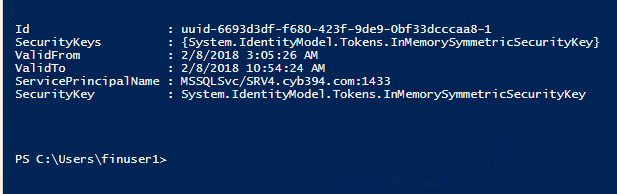
1. Now we will request a service ticket for the SQL service. In a new powershell ISE window. Type in the following



Add-Type –AssemblyName System.IdentityModel

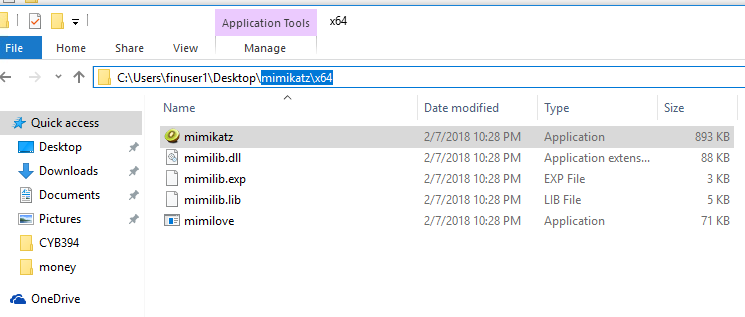
New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken –ArgumentList ‘MSSQLSvc/SRV4.cyb394.com:1433’

You should see the following output



We just stored ticket in memory.

1. Make sure windows defender is disabled. (This needs to be done via group policy) <https://social.technet.microsoft.com/wiki/contents/articles/52075.windows-10-how-to-permanently-disable-windows-defender.aspx>
2. From Client1 open the shared drive once more. Run à [\\10.0.0.254\shared\](file:///\\10.0.0.254\shared\)
3. Navigate to the CYB394 folder and locate the mimikatz folder. **Do not drill (open mimikatz) into the folder.**
4. Copy this folder to your Desktop
5. Double click on the folder and navigate to X64 then double click mimikatz.

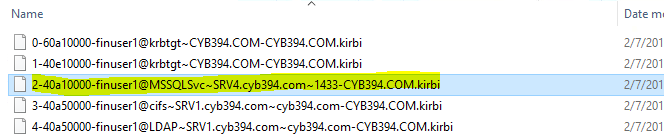


1. From the mimikatz console type

kerberos::list /export



1. This will dump all Kerberos tickets to your mimkatz x64 folder
2. You should see the file that contains the MSQL ticket we requested in memory.



1. Copy this ticket and paste it into a folder Called *Yourname* in the \\10.0.0.254\shared drive. (Hint you will have to make this folder.