This lecture is an overview of the 6 New DNS Features in Windows Server 2016

1. **DNS Policies.**

   You can now control how your DNS server handles queries, based upon DNS Policies that can be configured for different scenarios. For example, DNS responses can be based upon the clients IP address (location) The time of day, and several other parameters. DNS policies enable load balancing, split-brain DNS and other scenarios.

2. **IPv6 Root Hints.**

   You can use the native IPV6 root hints support to perform internet name resolution using IPV6 root servers. By default, the DNS Server service implements root hints using a file, named Cache.dns, stored in the C:\Windows\System32\DNS folder on the DNS server.

3. **Response Rate Limiting (or RRL).**

   RRL is used to prevent DNS amplification attacks or denial of service attacks. Where the DNS server is inundated with thousands of requests leaving DNS inoperable.

4. **(DANE) DNS Based Authentication of Named Entities**

   DANE prevents man-in-the-middle attacks on your DNS server by using TLSA or (Transport Layer Security Authentication) records to tell the DNS clients what Certificate Authority (CA) they should expect a certificate from. Thus eliminating the opportunity for a hacker to corrupt the DNS cache and injecting their own CA and pointing the client or server to their own website.

5. **Unknown Record Support.**

   Non-Microsoft DNS servers have records that are not directly supported by a Microsoft DNS server. You can now add records which are not explicitly supported.

6. **Extended Windows PowerShell Support.**

   There are 27 new PowerShell cmdlets introduced in Windows 2016 Server.