Active Directory: Supplement

Exercises

1. The domain controller diagnostics tool dcdiag can be used to test the health of a domain controller. Test DNS on a domain controller with the command dcdiag /test:DNS and test the services on the domain controller with dcdiag /test:Services How helpful are the results?
2. Windows checks the file C:\Windows\system32\drivers\etc\hosts before making a DNS query. Add an entry in that file and verify that the Windows uses it.
3. From the Windows command line, run ipconfig /displaydns. Try again with /flushdns.
4. A user with credentials can enumerate the structure of a domain, even from a system not connected to the domain. Download AdFind from <http://www.joeware.net/freetools/tools/adfind/index.htm>. AdFind uses an encoded form for passwords on the command line; to determine the encoded password to use, run

C:\Users\Hermann Weyl\Desktop\AdFind>AdFind.exe -encpwd password1!

AdFind V01.47.00cpp Joe Richards (joe@joeware.net) October 2012

Encoding password1! as ENCPWD:Z=Z=rQjIUxrQJm9cSvAdP39cWzgFhG9c

To query the domain corp.saturn.test at 10.0.6.120 as the domain user corp\ohahn with this password, run the command

C:\Users\Hermann Weyl\Desktop\AdFind>AdFind.exe -b "DC=corp,DC=saturn,DC=test" -dn -h 10.0.6.120 -u corp\ohahn -up ENCPWD:Z=Z=rQjIUxrQJm9cSvAdP39cWzgFhG9c

Using server: cassini.corp.saturn.test:389

Directory: Windows Server 2012

dn:DC=corp,DC=saturn,DC=test

dn:CN=Users,DC=corp,DC=saturn,DC=test

dn:CN=Computers,DC=corp,DC=saturn,DC=test

dn:OU=Domain Controllers,DC=corp,DC=saturn,DC=test

dn:CN=System,DC=corp,DC=saturn,DC=test

dn:CN=LostAndFound,DC=corp,DC=saturn,DC=test

dn:CN=Infrastructure,DC=corp,DC=saturn,DC=test

dn:CN=ForeignSecurityPrincipals,DC=corp,DC=saturn,DC=test

… Output Deleted …

311 Objects returned

Additional documentation for AdFind is available from Microsoft at <http://social.technet.microsoft.com/wiki/contents/articles/7535.adfind-command-examples.aspx>

1. Download and run Active Directory Explorer from Sysinternals. Use it to find the SID for the computers in the domain. Repeat for the users in the domain
2. Use Active Directory Explorer from Sysinternals to find the Active Directory entries for the Microsoft DNS services. Locate the entries for locally stored forward and reverse zones. Locate the entries for conditional forwarders. Are they stored in the same location?
3. Rename the domain administrator account.
4. Use the command net user to add an account to the domain from an administrator command prompt. Use the command net group to make this user a domain admin.
5. Run the Security Configuration Wizard on each Windows server. It is available from Server Manager.
6. The command c:\>bitsadmin /transfer n <http://site.example/document> "c:\Users\User Name\Desktop\results" is a command line technique to download the file <http://site.example/document> and save it locally in the file c:\Users\User Name\Desktop\results. Test it. See also <http://msdn.microsoft.com/en-us/library/aa362813.aspx>.
7. Run the command gpresult with the flag /z to see the result of the group policies applied to a system.
8. Edit an existing group policy or modify an existing group policy to lock out an account for five minutes if it receives ten failed login attempts within a single minute.
9. Use ssh to login to a Linux system as a Windows domain user; for example using ssh corp\\srobinson@rhea. Compare the user id numbers for the same user across different systems.