Active Directory Hacking Lab Build

* Active Directory is a directory service that was developed by Microsoft to manage window domain networks. This will setup a domain network and we will be storing information of objects on this network. Objects can be computers, users, printers, anything connected to the network. The DC or domain controller acts like a central hub for all this information (like a phone book).
* The clients we setup will connect to the domain controller and store the information of those objects.

1. Download Virtual Box Virtual Machine Environment
2. Download Windows Server 2019 ISO x64
3. Open Virtual Box.
4. Configure Domain Control Machine:
5. Select “New”
6. Enter in name of machine.
7. Select ISO image “Server Eval x64” where it located on your local drive.
8. Edition should automatically load. No need to change this here.
9. Check “Skip unattended installation” so this won’t automatically start.
10. Enter 2GB (2048MG) for RAM.
11. Depending on your system select the number of processors you’re comfortable with. I used 2.
12. Select “Create a virtual hard disk now” and allocate at least 20GB.
13. Select finish
14. Configure your Virtual Machine
15. In the General settings select the advanced tab.
16. In the Shared clipboard and Drag’n’Drop drop down menu select “Bidirectional”. This will you to drag and drop and share things from your local machine to your virtual machine.
17. Select Network.
18. Under the Adapter 1 tab make sure “enable network adapter” is checked.
19. In the attached to drop down select “NAT”
20. \*\*For Virtualbox Users follow steps F-H\*\* Create an internal NIC as well select “Adapter 2” tab and select “enable network adapter”
21. In the attached to drop down select “internal network” and name it.
22. Select okay at the bottom and run the machine.
23. At the windows server setup screen select your language, time and currency format and keyboard input. This should all default to English and USA. Select Next and install.
24. Select “Windows Server 2019 Standard Evaluation \*\*(DESKTOP EXPERIENCE)\*\*. Very important to select this or you will only have a command line.
25. Accept the license and select next.
26. Select “Custom Install”
27. Select your drive 0 unallocated and select “new” at the bottom. Hit next.
28. Your size should automatically populate from your pervious settings. Select “Apply”. Select okay. Hit next.
29. Create your password. I would make it something simple that you won’t forget. Remember this only for lab purposes. Select Finish.
30. Select input at the top of your screen, key board, ctrl+alt+del. Then enter the password you created.
31. Select devices at the top of your screen, select input guest additions cd image.
32. Select file explore at the bottom, select “this PC” then double click virtual box guest editions.
33. Next through all the screens and it will load. This will allow us to have a full screen. Don’t restart yet.
34. In the search bar at the bottom input “change pc name”
35. Enter in your computer name, hit next.
36. Restart computer
37. \*\*\*These steps are for virtualbox users to setup their internal network so the clients can connect to the server
38. Right click on your network icon in the bottom right of the screen and select open network settings.
39. Select change adapter options.
40. Figure out which ethernet is your internet connection by right clicking > status > details. Your IP address will show. Usually one starting with 10 is a home address and this will let you know this the “internet” connection. So rename this as such.
41. Rename the other as xINTERNALx
42. Right click xinternalx > properties > double-click ipv4 > select use the following IP address > enter 172.160.0.1 > enter subnet mask: 255.255.255.0 > in the DNS server use loop back address 127.0.0.1
43. Server manager > manage > add roles and features > Remote Access > Routing > install
44. Tools > routing and remote access > right click server > configure and enable > select NAT > choose your “Internet” (if you don’t see the options for both your networks then get out and reopen routing and remote access) > finish
45. Server manager > manage > add roles > DHCP > Install
46. Service manager > tools > DHCP > open domain > right click ipv4 > new scope > name: 172.16.0.100-200 > start address 172.16.0.100 > end address 172.16.0.200 > enter length as 24 > subnet mask should be 255.255.255.0 > keep 8 days as lease > Yes to configure > add DC IP address 172.16.0.1 > next through
47. \*\*If IPv4/6 is not green but red - Right click the DC in DHCP > all tasks > restart >
48. Select the Scope you just created > in the dropdown select Scope Options > you should see 003 for routing with 172.16.0.1, 006 DNS Servers 172.16.0.1, and 015 DNS Server Name with your domanname.local.
49. \*\*if you don’t see 003 Routing > right click in the middle box on “scope options” > configure options > select routing > input 172.16.0.1 > select add > apply. You should see it now in the list. Exit DHCP.
50. In the Server Manager Dashboard select “Manage”
51. Select “add roles and features” and select next until you get to the roles screen.
52. Select “Active Directory Domain Services”, select add features and next through all screens.
53. Select install.
54. Select flag next to manage and select “promote this server to a domain controller”.
55. Enter domain name” domainname.local
56. Select “new forest”, hit next.
57. Re-enter domain name in “root domain name” field.
58. Enter in a password. I made mine the same as the login for ease. Hit next.
59. The NetBIOS domain name should populate the name of your domain.
60. Hit next all the way through to the prerequisite check. Once finished, install, then reboot.
61. Install certificate for LDAP secure – Need this if we want to utilize attacks against LDAP s or something like an IPV6 takeover.
62. In server manager select manage
63. Select add roles and features
64. Next through the screens until you can select the roles.
65. Select Active Directory Certificate Services
66. Select add features and next until you get to the confirmation installation selections screen.
67. Check box for “restart automatically if required.”
68. Install.
69. Hit close and select the flag at the top next to manage and select “configure active directory certificate.”
70. Select next then check the box on the next screen for “certificate authority”.
71. Select next all the way to the private key and select new private key and next.
72. Next all the way to validity period and enter “99” for years.
73. Next, then select configure and close.
74. Restart the server.
75. In the server manager select tools – Active Directory Users and Computers
76. Right click Local domain and select new – organizational unit. Name it “Groups”.
77. Select the uses folder and move anything not administrator and move it to groups.
78. Add a new user by right clicking and selecting add new user. Enter in the full name and logon with first initial last name, hit next.
79. Enter password as the same password you’ve been using.
80. Uncheck “user must change password at next login” and check “password never expires”. Hit next and finish.
81. Copy this user and repeat with a different name.
82. \*To add 1000 users using powershell script\*\*
83. Server manager dashboard select 1 configure this local server > select blue link next to IE Enhanced Security config > select “off” for both > open internet browser > go to: <https://www.gitub.com/joshmadakor1/AD_PS> > download to the desktop > open Powershell ISE > open the AD\_PS folder you downloaded and open the names.txt > add your name to the top of the list and save the document > in powershell open the 1\_CREATE\_USERS script > enter the cmd: cd C:\users\administrator\desktop\AD\_PS-master > hit enter > enter cmd ls to view files > play the script by pressing the green play button at the top.
84. The script will run and add all those users to AD along with an OU (organizational unit) in the AD directory.
85. Copy admin account and add SQL for the first name and service for the last name to create a SQL Service account. (It is common to have service accounts in the network. It is common to see service accounts running as domain administrator which is a no no. This happens often and can allow a Kerberos attack which can be abused and a weak password can be attacked )
86. Create a weak password for the SQL Service account for a proof of concept.
87. Double click on the SQL user and in the description type: Password is MYpassword123# (a lot of domain admins put their passwords in this field. A hacker can obtain this information).
88. Setup a SPN or Service Principle name for the SQL Service user account which is needed for a service:
89. Run cmd as administrator.
90. Type the following command: setspn -a DOMAINNAME-DC/SQLService.DOMAINNAME.local: 60111 DOMAINNAME\SQLService
91. After the object has updated you can check it with this command: setspn -T DOMAINNAME.local -Q \*/\*
92. Note: This allows us to practice the Kerberos attack in our environment.
93. A lot of attacks in the environment are related to SMB (server message block). So we are going to open SMB ports 139 and 445.
94. Go to the C drive
95. Create a new folder and name it “hackme”.
96. Go to the server manager and select “File and Storage Services”.
97. Select shares on the menu on the left.
98. Select “Task” from the drop down at the top and select “new share”.
99. Select “SMB quick” and hit next.
100. Select custom path radial button, browse and select the “hackme” folder you just created, then hit next and the way through and select “create” on the final screen.
101. Hit close. Now SMB is open in the network so attacks can be performed against ports 139 and 445.
102. Open cmd and type “ipconfig”. Identify your IP address.
103. Create client 1 machine
104. Open Virtual Box and select New
105. Name the machine “Client 1”
106. Select Windows 10 iso (download this from here: <https://www.microsoft.com/en-us/software-download/windows10ISO>)
107. Give the RAM at least 2GB. Enter in how many processors you can allocate, if you can do at least 2.
108. Give the VM at least 20GB of storage.
109. Change Network settings to Internal. This will connect to the NIC on the DC and the DC will route to the internet.
110. Select Finish.
111. G. Repeat for Client 2.
112. Install windows 10 on each client per steps 7-19 except choose windows 10 Pro.
113. Go the command prompt and enter the command: ipconfig. Your IP and default gateway should match and be 172.16.0.1.
114. Enter the following command to verify your host can reach the internet: ping [www.google.com](http://www.google.com)
115. Now right click the start menu and select system > rename computer (advanced) > rename the computer > select domain at the bottom and enter your domain name > enter in your admin credentials > you will get a pop up that your connection was successful (the DC must be running too) > you will need to restart the computer.