2023 Midwest Collegiate Cyber Defense Competition

Windows Server 2012 R2 Guide by

Jacob Motley

Modified 2019 Guide by

Ethan Mitchell

Understanding the Walkthrough

General Information

This walkthrough is intended to provide new users with a basic understanding of the Windows Server 2019 machine, its services, and how to begin securing it for the CCDC competition. While this walkthrough could be used as a starting point for any new user, it should not, and is not intended to, be the only source of information used when securing this machine. Due to the ever-changing world of cyber-security, this walkthrough contains general and basic information regarding the server and its services. Use of external sources to learn more about the server and its services is highly recommended, and is encouraged, as it is the best way to get an advanced understanding of how the server and its services work, how they are scored, and, more importantly, how they can be secured. However, the best way to understand any machine or service is through practice, and the same is true for this machine.

Format & Text Styles

This walkthrough is formatted with the use of headers and sub headers to separate and organize information for easier navigation and access. Where images are used, a label and description are provided above each image for reference.

This walkthrough occasionally refers to code you should run. When referenced, the code will appear in the following format: `echo "Example"`

This walkthrough also refers to field types or entries within Windows Server 2012. These field types or entries will appear in this format: Field Type 1

What This Machine Does:

Windows Server 2019 AD/DNS is one of the two windows machines within the starting network. This Windows server serves 2 primary functions that are both scored…

(1) It confirms user lists through LDAP authentications with the Fedora Mail server. If the mail list is binding with Active Directory with no issues, then Active Directory is working, and you will receive points.

(2) It also serves as a Domain Name Server for clients outside of the main network. If the scoring server (outside of the network) is able to send a DNS request to Windows Server 2019, and receives the expected response, then you will receive points.

If either of these two functions are not working properly, you will not receive any points for Active Directory. Both functions must be working simultaneously.

About LDAP Authentication

LDAP Authentication follows a client/server model. Client(s) will send a bind request to the LDAP Server (Windows Server 2019) along with a user's information, such as their username and password. This information is cross-referenced with the information Windows Server 2019 stores in Active Directory (explained briefly below). If the credentials match, the user is authenticated, and granted access to information through the client (in the state competition, they are accessing their mail), thus it is scored positively. If the credentials do not match, then the user is not granted access to information, thus Windows Server 2019 will not receive a service score, until it is fixed.

About Active Directory (AD)

Active Directory is a database and set of services that contains user information. It allows users to access network resources through different forms of authentication. In this network environment, AD holds user information, and the information is cross-referenced with users in the Fedora (mail) server.

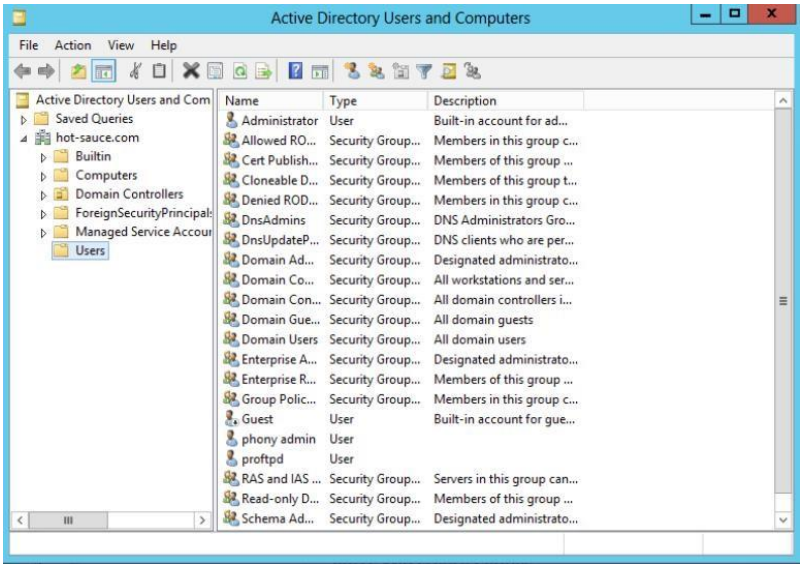
About Domain Name Server (DNS)

DNS stores domain names (i.e. google.com, hot-sauce.com, Allsafe.com, etc.) and distributes them to clients to use. This process is done through port 53. For the competition, Windows Server 2019 will receive DNS Queries from an IP Address(es), and if they receive the expected reply, DNS will be scored properly. If the client does not receive a response or receives information that does not match what is expected, then DNS will not be scored properly, and Windows Server 2019 will not receive a service score, until it is fixed.

Managing Scored Services:

Active Directory (LDAP)

Image 1: Example Active Directory Users and Computers screenshot



Active Directory is managed through “Active Directory Users and Computers” in Server Manager Tools. This is where you can add, delete, and edit users and groups. Ensuring the accuracy of these users and groups is essential to its proper functionality. The users and groups included in this list should match any authorized query a device in your network attempts to make.

Ensuring there are firewall rules in place to allow LDAP traffic to and from Windows Server 2019 is essential to the proper functionality of Windows Server 2019. The services associated (PowerShell: `services.msc`) with Active Directory and LDAP must also be running. It is a good idea to configure these rules and services to only accept traffic from the expected IP Addresses/hosts. In the State competition, this consists only of the Fedora Mail server.

Configuring these rules can be done in PowerShell, or the Graphic User Interface (GUI). Below is an example of what it looks like to configure the LDAP specific Firewall Rules through PowerShell*.

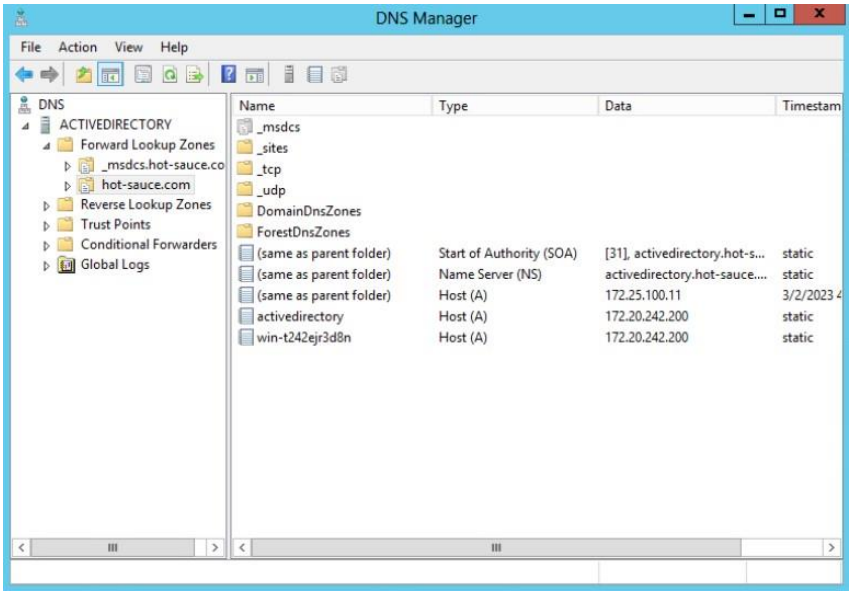
```
Set-NetFirewallRule -DisplayName "Active Directory Domain
Controller - LDAP (UDP-In)" -Enabled True -LocalAddress
$MailAddr
Set-NetFirewallRule -DisplayName "Active Directory Domain
Controller - LDAP (TCP-In)" -Enabled True -LocalAddress
$MailAddr
Set-NetFirewallRule -DisplayName "Active Directory Domain
Controller - LDAP for Global Catalog (TCP-In)" -Enabled True -
LocalAddress $MailAddr
Set-NetFirewallRule -DisplayName "Active Directory Domain
Controller - Secure LDAP (TCP-In)" -Enabled True -LocalAddress
```

```
$MailAddr
Set-NetFirewallRule -DisplayName "Active Directory Domain Controller - Secure LDAP for Global Catalog (TCP-In)" -Enabled True -LocalAddress $MailAddr
```

*`$MailAddr` is a placeholder for the domain IP address of the clients authenticating to AD through LDAP. On occasion, there may be users that are included in the Fedora Mail server list, that are not included in the Active Directory user list. This is fixed simply by adding the specified user to Active Directory through "Active Directory Users and Computers". Add the user with the username and password included in the Fedora Mail server list, and ensure they are in the "Domain Users" list. This should be done with any and all users that are included in the Fedora Mail server list, but not in Active Directory.

Domain Name Server (DNS)

Image 2: Example DNS Manager screenshot from Windows Server 2012



Active Directory DNS is managed through DNS Manager (display name "DNS"), located in the Server Manager Tools. Here is where you can view the DNS Servers and make changes to the response Active Directory will give, when it receives a DNS request.

Active Directory DNS will respond to a DNS request with the IP Address of the host it is asked for. Within DNS Manager, you can view what Active Directory will respond with here (Seen in Image 2):

DNS>YOUR_SERVER>your-domain.com

Column descriptions:

- Name: This is the identifier for each item.

    - The name (same as parent folder) refers to the folder you are currently viewing. For example, if you are in a folder named hot-sauce.com then the name for this item is also hot-sauce.com
- Type: This identifies what data type is associated with each name.
    - The most common Type is Host (A) and it is associated with an IPv4 Address in the Data column. If using IPv6, the Type will instead be Host (AAAA)
- Data: This is the information that is queried for. It can range from an IP Address to a Server Name.

A DNS request will ask for the Data associated with a given Name. Using the information in Image 2, if a DNS request asks for the Data associated with Name hot-sauce.com, DNS will respond with 172.25.100.11. If this matches the information expected by the scoring server, DNS will be scored properly.

The Firewall rules for DNS should also be configured in a similar fashion to Active Directory (LDAP). Below is an example of securing the DNS firewall rules through PowerShell.

```
Set-NetFirewallRule -DisplayName "DNS (TCP, Incoming)" -Enabled True -Profile Public,Private,Domain
Set-NetFirewallRule -DisplayName "DNS (UDP, Incoming)" -Enabled True -Profile Public,Private,Domain
```

In the event of complete DNS destruction, re-configuring DNS is a simple process. Adding a DNS server with the expected Name, Type, and Data can be done entirely within DNS Manager. If you need to configure DNS manager, and do not know what to input for each item, a WireShark packet capture search for a DNS query can show you what the scoring server is asking for. You can then create that item and give it the appropriate value.

Walkthroughs & Tips

The Elephant in the Room

Originally, with Windows Server 2019 R2 there was Windows Key on the taskbar. This is because this distribution of Windows Server 2012 R2 was rolled out with Windows 8, when Microsoft decided to incorporate their touch-screen interface with their computers. Do not make the mistake of wasting time trying to get it back, it is gone forever.

Fortunately, there are some quick workarounds:

1) You can open many applications simply with PowerShell.
    a. Example: Open Control Panel easily by typing ‘control’ or ‘control panel’ into PowerShell, and the Control Panel will open.
2) You may also open the home menu (windows-key equivalent), if you hover your mouse over the very top right corner of the screen. When you see a submenu with the windows key appear, carefully maneuver your mouse to the windows key and click it. You will be sent to the home screen, where you may freely search for applications as you would with a windows key.

    This section is kept within the guide in the chance that they do not stick with Windows Server 2019 for future competitions.

Installing Chrome

At the start, it is nearly impossible to download anything from the internet onto Windows Server 2019. Whether it’s your GitHub repo, a security tool, or a tool required for an inject, getting a different browser onto Windows Server 2019 should always be a top priority. Using Internet Explorer on Windows Server 2019 will likely prove to be a challenge, so below is one method of how to use Internet Explorer to quickly get Google Chrome installed. Open Internet Explorer

1. Right click the taskbar (bottom of screen)
    a. Toolbars > Address
2. Type in the new ‘Address’ box: google.com and hit ENTER.
3. If internet explorer asks you to add a ‘google.com’ website to your trusted sites, add it by following the on-screen instructions.
    a. (Yes, every single time. This is tedious but must be done.)
4. When you stop getting pop-ups and see the home google search screen, open your internet explorer settings.
    a. Click the settings cog at the top right (under the red “X”) > Internet Options
    b. Open the “Security” tab.
    c. Click the “Internet” logo, and select “Custom level…”

    d. Scroll until you see “Downloads > File download” and enable it. Click OK and save your settings.
    e. Apply and close the Internet Options window.
5. Use the google search box (not the top address bar) to download chrome, or if you see google recommending downloading chrome, you may use this link too. Remember to add every google.com address to your trusted sites UNTIL you get chrome to download.
    a. You will see a pop-up at the bottom of the screen asking what to do with “ChromeSetup.exe”. Click “Save” and then “Run”. This will install chrome.
6. Open your internet explorer “Internet Options” window again. Open the security tab and view the “Internet” zone as you did before.
    a. Near the bottom, click “Default level”. This will disable the “file download” feature you enabled earlier. This is done as a security measure, to ensure no unnecessary permissions are left on. You are putting Internet Explorer back the way you found it.
7. Close internet explorer and wait for google chrome to install, then open google chrome if it doesn’t do so automatically.

Allowing GitHub Access & Downloading it Quickly

At the start of the competition, you may find that when you try to access your GitHub repo that you are unable to view the page/download it. This may be a result of some wonky DNS settings. Here’s how to fix that.

1. Open the ‘Network and Sharing Center’
    a. Control Panel > Network and Internet > Network and Sharing Center
2. Click your ‘Ethernet’ connection.
3. Click ‘Properties’
4. Open IPv4 settings, then set the following:
    a. Preferred DNS: 8.8.8.8
    b. Alternate DNS: 1.1.1.1
5. Apply and close, then open your IPv6 settings.
    a. Select ‘Obtain DNS server address automatically’
    b. We have also found success disabling IPv6, this is an option as well.

6. Apply and close all networking windows.

Now that you've configured your DNS properly, you should be able to access your GitHub repo. There are many ways to do this, but a very quick way is to simply paste the 'Download Zip' URL into a browser (NOT Internet Explorer). Your URL should follow a format similar to the one below:

https://github.com/REPO-OWNER/REPO-NAME/archive/refs/heads/main.zip

You should note what your GitHub repo link is, so that on competition day you can quickly paste it into Chrome, and get it downloaded.

Firewall Tips

Alongside securing the firewall rules necessary to the scored services, it is also important to understand how the firewall works. For inbound rules, by default, the Windows Firewall settings are set to deny or block all inbound traffic, unless there is a rule that allows it. In contrast, the Windows Firewall by default allows all outbound traffic unless there is a rule that denies it.

It is important to understand which firewall rules are needed and which are not. Those that are not needed, particularly for the inbound connections, should be turned off, and those that are needed should be configured to be more specific as to the host/port that you specifically want traffic from.

Changing Passwords

Changing passwords should always be the first thing on your to-do list. However the potential existence of key-loggers and other malicious software on Windows Server 2012 at the start of the competition can make changing the password useless, unless done properly. The safest way would be to take the machine offline, ensure there is no malicious software, and then change the password. However, this process will likely result in a lot of lost service up-time points. The best way to do this initially is to follow these steps when the competition starts:

1) Turn off the Network Interface Card (NIC).
    a. In PowerShell/cmd, run: `ncpa.cpl`
    b. Right click the interface, click 'disable.'
2) Change the Administrator password.
    a. "Ctrl + Alt + Del" > Change password
3) Turn on the firewall (there are many ways to do this).

a. Open control panel (PowerShell: `control panel`)

b. Find the firewall under ‘System and Security’ > ‘Windows Firewall.’

c. Turn on the firewall.

4) Turn the NIC back on

a. PowerShell/cmd, run: `ncpa.cpl`

b. Right click the interface, click ‘enable.’

5) In the event that they disabled ncpa.cpl, as they have in the past, you still have many options.

a. Right click the internet logo in the bottom right

b. Open network & internet settings, change adapter settings

From here, you can maintain the steps above. In addition, it might be necessary to flush DNS after changing these settings, you can do so by typing: `ipconfig /flushdns`

While you changed the password without a key-logger actively transmitting what you were typing, it is always possible the key-logger cached what you typed and is sending it after you turn the firewall back on. Quickly securing the machine further and doing some threat-hunting (discussed below) should be done immediately after this, and then the password should be changed again.

Threat Hunting

Searching your machine for unauthorized software (malware, key-loggers, etc.), and properly removing them. In Windows systems, this process can be difficult, however with the number of tools at your disposal it’s immensely more straight forward than it is for Linux. There are helpful tools available for download online that will make you glad you chose a Windows operating system.

- Autoruns (by Microsoft) is a program that searches your system for files that are authorized, and those that are not, and displays them for analysis. You can also choose to delete the unauthorized files within autoruns, and it will safely remove them. You can download this quickly with Google Chrome, and it will work on any windows system.

- TCPView (by Microsoft) this program is essential for seeing the inbound and outbound connections made to your system. You can see process names, protocols, ports, IP addresses, time created, session status, among other things.
- Process Monitor (by Microsoft) Working with this, as well as Autorus, TCPview, task manager and scheduled tasks, should help you be able to identify and monitor any activity that isn't native to Windows.
- Another helpful tool is just looking at Task Manager. Simply viewing the running tasks can sometimes help you find unauthorized sessions that should not be running. Right clicking them and selecting "Open file location" will show you the file that is associated with the task, and you can remove the file to stop the task. However, this tool is only useful if you are certain what you are removing is not essential/important, so be careful.
- Wireshark: Learning how to separate the good network traffic from the bad is vital for not just learning the IP addresses of the scoring server, but in doing so you can help your team identify malicious red team activity, and properly handle it.

Threat Hunting is a process that should be done throughout the competition. It is always possible something unauthorized shows up later in the competition, and this is a good way to constantly monitor the security of your machine.

General CCDC Rules:

1. SERVICES: Your number 1 priority is making sure your light is green. This is easier said than done, I know. However, the points you get for keeping your services up is what separates the good teams from the bad.
2. INJECTS: If your next questions is what separates the good from the best, this would be incident response reports and injects. These don't have to be perfect, what's important is that they get done. Every inject should be submitted, and on time.
3. HAVE FUN: This is meant to be a learning experience. Nobody expects you to keep your service up for the entire competition, that's how stacked against you the deck is. We have had our firewall turn into a gif of a cat on multiple occasions, we've even had entire linux operating systems deleted. If you want to learn more about that, you can ask Dr. McMurtrey about the sudo rm -rf incident.