Access Control via Active Directory Lab

Ryan Coon

CYB-525

Dr. Emmett Ward

November 20, 2024

Part 1:

Screenshots:

A screenshot of a computer

Description automatically generated

Set Windows Server 2019 ip address to 192.168.1.10.

A screenshot of a computer

Description automatically generated

Network domain name WHATEVER as created through Active Directory.

A close-up of a white envelope

Description automatically generated

Again through the server manager under local servers, you can see the domain name WHATEVER.

A screenshot of a computer

Description automatically generated

This screenshot shows the ip range from start to end. We will start the DHCP ip addresses at 192.168.1.150 and end at 192.168.1.200.

A computer screen shot of a black screen

Description automatically generated

Checked the ip address on the windows 10 server to ensure that the DHCP ip address went through. As you can see the new ip address for the Windows 10 server is now 192.168.1.150, which is the start ip for the DHCP.

A screenshot of a computer screen

Description automatically generated

Error that I kept getting when trying to apply user DDuck onto STATION1.

A screenshot of a computer

Description automatically generated

Successful addition of user DDuck on Station 1 to sign in under the WHATEVER.COM domain.

A screenshot of a computer

Description automatically generated

Here is a screenshot of the event logs. You can see the successful logon and logoff. I was able to successfully apply user DDuck as a domain user and access it through the Windows 10 VM.

Part 2:

**Summarize the issues encountered, lessons learned, and successes in a bullet point format.**

There was only one issue that I encountered when getting the user from Active Directory linked on the Windows 10 VM. It turns out you need to update the Windows Server 2019 to start off. Then you will need to create a Group Policy allowing a group to rejoin. Then instead of adding users, you need to create a group to allow rejoin and add the users in there. Once I got that it worked flawlessly. Lesson learned was to anticipate road blocks. Be patient and work through them.

* Was able to add computers and users in Active Directory
* Was able to successfully get user in active directory linked on the Windows 10 VM
* Was able to successfully get user in active directory linked on the Ubuntu VM

**Describe the screenshots provided.**

Screenshots provided show the successful completion of the assignment. Each screenshot has the description under it. There is a screenshot of the only error I encountered, which turned out to be an update and group policy addition.

**Explain 2-3 benefits of having a hybrid network.**

A hybrid network offers several benefits, including enhanced security, improved performance, and increased flexibility. A hybrid network combines elements of both on-premises and cloud-based infrastructure, allowing organizations to leverage the strengths of each approach. This combination can lead to a more secure network, as sensitive data can be stored on-premises while cloud-based services can be used for less critical applications. Additionally, a hybrid network can improve performance by allowing organizations to distribute workloads across different locations, optimizing resource utilization(Kajeet, 2022). Finally, a hybrid network offers greater flexibility, allowing organizations to scale their infrastructure up or down as needed, adapting to changing business requirements.

**Describe the role of Active Directory in accessing information.**

Active Directory plays a crucial role in accessing information by acting as a central database that stores information about objects on the network, making it easy for administrators and users to find and use this information. It helps manage permissions and control access to network resources, ensuring that only authorized individuals can access specific files or applications(Microsoft, 2022). Active Directory checks user credentials for authentication and determines what resources they can access based on their role or assigned permissions.

**Explain how reviewing the security logs could be helpful in a security operations center (SOC).**

Reviewing security logs is crucial in a security operations center (SOC) because it provides valuable insights into system activities, user actions, and potential security threats(Cobb, 2021). By analyzing these logs, security analysts can identify suspicious patterns, detect potential breaches, and respond to incidents effectively. Security logs can help identify malicious activities, such as unauthorized access attempts, data exfiltration, or malware infections(Bunting, 2024). They can also help track user behavior, identify policy violations, and ensure compliance with security regulations.

References:

Bunting, D. (2024, July 18). *The Top 5 Security Logging Best Practices to Follow Now*. Chaossearch.io; CHAOSSEARCH. https://www.chaossearch.io/blog/cyber-security-logging

Cobb, M. (2021, December). *Security log management and logging best practices*. SearchSecurity. https://www.techtarget.com/searchsecurity/tip/Security-log-management-and-logging-best-practices

Coggins, J. (2020, October 22). *What Is Active Directory and How Does It Work?* Lepide Blog: A Guide to IT Security, Compliance and IT Operations. https://www.lepide.com/blog/what-is-active-directory-and-how-does-it-work/

Kajeet. (2022, January 4). *Hybrid Networks and PLTE: Why You Need Both and How to Manage*. Kajeet.com; Kajeet. https://www.kajeet.com/en/blog/hybrid-networks-and-plte-why-you-need-both-and-how-to-manage

Microsoft. (2022, August 16). *Active Directory Domain Services Overview*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview