**Active Directory Attack**

Network diagram

A diagram of a computer network

Description automatically generated

1. The project commences by bringing in the systems on a single **NAT network** to ensure seamless communication. **Windows Server** acts as the domain controller for Active Directory, while **Windows 10** (TARGET-PC) simulates a client environment. **Kali Linux** is used for security testing, and **Splunk** provides centralized log monitoring. This is the setup for AD configuration.  
  
Configuring the Splunk for the AD network was fun! Sharing the steps as follows:  
a) Download the Splunk Installer and mount it over to TARGET-PC through “share” folder

A screenshot of a computer

Description automatically generated

b) Install and configure the static IP address to 192.168.10.10, disabling DHCP.

c) At the end, we can access our Splunk server from any systems inside NAT configuration.

A screenshot of a computer screen

Description automatically generated

d) Login to Splunk to download the Splunk Forwarder to collect the system logs.

e) Customise “Inputs.conf” file, focusing only on those logs the Forwarder needs to send Splunk Server

A screenshot of a computer program

Description automatically generated

2. Create new “endpoint” in Splunk to log data mentioned in Inputs.conf from the Target-PC.

A screenshot of a computer

Description automatically generated

3. On the Windows Server, lets change the name for easier identification followed by installing Splunk and Sysmon the same way done above.  
If done right, we should be able to see both the hosts on the Splunk dashboard collecting logs.

A screenshot of a computer

Description automatically generated



4. Now, let’s host the AD in our Windows Server by configuring the local domain name to “ADDC.local” and checking in all the AD file boxes.

A screenshot of a computer

Description automatically generated



Some of the important files that we must observer are shown below.

A screenshot of a computer

Description automatically generated

5. The NTDS (NT Directory Services) files in a Windows Server include the ntds.dit database, which stores all Active Directory data such as user accounts, groups, and policies. Transaction log files, like edb.log, ensure data consistency by recording changes before they are committed to the database, allowing for recovery in case of failure.

6. Create user-groups in the AD based on the role access each user has with appropriate username and passwords.   
Note the username shall be affiliated with the domain name ADDC.local for each new user who is created as part of this directory.  
  
7. Back to TARGET-PC, it needs to be associated with the AD, i.e., TARGET-PC should become part of the ADDC.local domain. The network is slowly incorporating all the systems required for a seamless data movement as we see TAR-PC being displayed in the AD.

A screenshot of a computer program

Description automatically generated A screenshot of a computer

Description automatically generated



We may now login to TARGET-PC with any of the usernames configured in the AD!  
Note: Let us enable RDP for a good demonstration of this attack

Let’s Attack shall we?!  
  
8. Once the attacker can break into our subnet (NAT) threat to AD is on the way!

Crowbar is a password-cracking tool used on Kali Linux to perform brute-force attacks on various protocols, such as RDP, SSH, and HTTP. It works by systematically guessing usernames and passwords, leveraging a dictionary or custom wordlist to attempt authentication. Crowbar is often used in penetration testing to test the strength of login credentials and identify weak points in a system’s security.  
A screenshot of a computer program

Description automatically generated

9. We shall pass the following command and the description of each term is as follows:  


* -b rdp: Specifies the protocol to target, in this case, RDP (Remote Desktop Protocol).
* -u WSmith: Defines the username to attack, here, "WSmith".
* -C passwords.txt: Uses the "passwords.txt" file as the wordlist for password guesses.
* -s 192.168.10.100/32: Targets the IP address 192.168.10.100 with a subnet mask of /32, indicating a single host.

Were we successful in making the attack? Yes!

A computer screen with white text

Description automatically generated

The tool has cracked the credentials required for “WSmith”

10. Wait a minute, did we just record this on our Splunk logs?!! Let’s find out.

A screenshot of a computer

Description automatically generated

This depicts the brute force attack that is being tried on the user WSmith. Yes, all of this is recorded with other meta data for the attack as well.

11. Investigating further into the exact event log, we find the following information.

A screenshot of a computer

Description automatically generated  
The even code 4624 gives a hint that there was a login attempt. Further there’s also information on the number of failed login’s which will create room for suspicion.

This is by far a very interesting yet challenging project I took up and the conclusion and take away are as follws:  
Securing Active Directory requires a multi-layered approach, including strong password policies, multi-factor authentication (MFA), and regular monitoring for vulnerabilities.   
My future work is to focus on implementing advanced threat detection mechanisms, such as Security Information and Event Management (SIEM) systems, to identify and respond to suspicious activities in real-time. Additionally, exploring Privileged Access Management (PAM) solutions, enhancing group policy configurations, and conducting regular penetration tests will further strengthen AD security.