START COMPETITION:

Windows Server 2012 Windows Server 2012 R2, Windows Server 2016, Windows Server 2019: Server Manager method:

**After doing the top command on the screenshot, replace the 2 with 1 and replace true with false.**

A screenshot of a computer program

AI-generated content may be incorrect.

1. On the Server Manager Dashboard of the server where you want to remove SMBv1, under Configure this local server, select Add roles and features.
2. On the Before you begin page, select Start the Remove Roles and Features Wizard, and then on the following page, select Next.
3. On the Select destination server page under Server Pool, ensure that the server you want to remove the feature from is selected, and then select Next.
4. On the Remove server roles page, select Next.
5. On the Remove features page, clear the check box for SMB 1.0/CIFS File Sharing Support and select Next.
6. On the Confirm removal selections page, confirm that the feature is listed, and then select Remove.

The LM hash is relatively weaker than the NT and is prone to a fast brute-force attack. The best recommendation is to prevent Windows from storing the password's LM hash. You can access it through the following:

Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Network security - Do not store LM hash value on next password change policy > select "Define policy setting"

SMB stands for Server Message Block. Generally, Microsoft-based networks utilize this protocol for file and print communication. Moreover, it allows secure transmission over the network. Configuring SMB signing through group policy is crucial to detect Man in the Middle (MiTM) attacks that may result in modification of SMB traffic in transit.

Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > double click Microsoft network server: Digitally sign communication (always) > select Enable Digitally Sign Communications

Enable LDAP signing through the following:

Group Policy Management Editor > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options > Domain controller: LDAP server signing requirements > select Require signing from the dropdown

Microsoft Security Compliance Toolkit (MSCT) is an official toolkit provided by Microsoft to implement and manage local and domain-level policies. You don't have to worry about complex policy syntaxes and scripts, as Microsoft will provide pre-developed security baselines per the end user environment.

Open Microsoft Security Compliance Website > click Download > click Windows Servers Security Baseline.zip > Download (also download PolicyAnalyzer.zip)

Then open extracted folder > local\_script > right click, run with powershell the .ps1 file.

Then do the same with policyanalyzer > mergepolicyrules.ps1 > then open up policyanalyzer > add or manage local or domain policies.

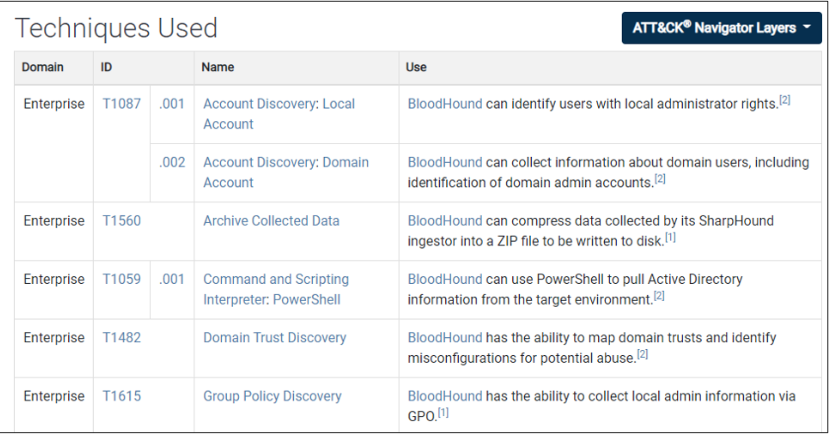
You can prevent the attack by ensuring an additional layer of authentication through MFA or by frequent and periodic Kerberos Key Distribution Centre (KDC) service account password reset

Active Directory Users and Computers. > Select View, and then select Advanced Features > double-click the domain container, and then select Users > right-click the krbtgt user account, and then select Reset Password. Reset password. The password that you specify isn't significant because the system will generate a strong password automatically independent of the password that you specify.

**If you are unsure a service is good or bad, do this.**

To understand Windows services further, let's dive deep into their structure. To start with, information on Windows services is stored in HKLM\SYSTEM\CurrentControlSet\Services

Right click the service and export > open the service in notepad and observe creation time.



Download GitHub to try out bloodhound.

Steps when you discover compromised AD, these are the order of operations: take backups of the domain, reset all the admin passwords, track GPO changes to ID the attacker, forward logs to SIEM, report.

The following script will get the AD users' created date, which will help identify any new user created after the hacking date.

Get-ADUser -Filter {((Enabled -eq $True) -and (Created -gt “\*Select day of week, month day, year time:time:time am/pm\*”))} -Property Created, LastLogonDate | select SamAccountName, Name, Created | Sort-Object Created

Example of \*\* “Monday, April 10, 2023 00:00:00 AM”))}

The following script lists all the computers that joined the Active Directory domain, along with the date and name of the person who joined it.

Get\_ADComputer -filter \* -properties whencreated | Select Name,@{n=”Owner”;e={(Get-acl ”ad:\$($\_.distinguishedname)”).owner}},whencreated

(alter the bits whencreated to LastLogonDate to find last logged)

Check event viewer for this PIDs

ID 4756: Member added to a universal security group.

ID 4757: Member removed from a universal security group.

ID 4728: Member added to a global security group.

ID 4729: Member removed from a global security group.

<https://www.pingcastle.com/> for auditing and identifying AD environment loopholes.

we must take preventive measures to limit users who can log in locally on computers with privileged access or domain controller. (Unless competition wise we have to RDP or SSH into the machine)

gpedit.msc > Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > User Rights Assignment, and double-click on Allow log on locally and then select the users and groups we want to be able to log in to the DC.

[UltimateAppLockerByPassList/AppLocker-BlockPolicies/README.md at master · api0cradle/UltimateAppLockerByPassList · GitHub](https://github.com/api0cradle/UltimateAppLockerByPassList/blob/master/AppLocker-BlockPolicies/README.md)

AppLocker hardening rules (could break stuff so dread lightly)

How to remove a domain controller that no longer exists?

Incomplete addition or removal of a domain controller can lead to inconsistency in data due to the presence of a domain controller that exists, but is not completely functional. This hinders other processes and complete cleanup is required. The following steps describe how to cleanup the metadata.

1. In the command line, type ntdsutil and press enter.  
   C:\WINDOWS→ntdsutil  
   You will see the following prompt displayed in the command prompt window:  
   ntdsutil:
2. At the Ntdsutil: prompt, type metadata cleanup  
   ntdsutil: metadata cleanup  
   Once you are done with that, the metadata cleanup prompt will appear like this:  
   metadata cleanup:
3. At the 'metadata cleanup:' prompt, type connections and press Enter.  
     
   metadata cleanup: connections  
   Now the server connections mode is on, as mentioned below:  
   server connections:
4. In 'server connections:', type :  
   connect to server < servername→

Here <servername→ is the domain controller (any functional domain controller in the same domain) from which you plan to clean up the metadata of the failed domain controller. Press Enter after entering your server name. In this case, consider the server name to be server100. You will see the following entry.  
server connections: connect to server server100  
Binding to server100 ...  
Connected to server100 using credentials of locally logged on user.

1. Type 'q' in server connections to quit and press Enter to return to the metadata cleanup prompt.  
   server connections: q  
   metadata cleanup:
2. In metadata cleanup, type select operation target and press Enter.  
   metadata cleanup: Select operation target  
   Now select operation target mode will come up.  
   select operation target:
3. Type list domains and press Enter.  
   select operation target: list domains  
   This lists all domains in the forest with a number associated with each.  
   Found 1 domain(s)  
   0 - DC=dorg,DC=net
4. Type select domain <number→, where <number→ corresponds to the domain in which the failed server was located. Press Enter.  
   select operation target: Select domain 0  
   We specify the number as 0 here, as the previous prompt let us know that 0 is the number assigned to the domain "dorg.net". Next you will see:  
   No current site  
   Domain - DC=dorg,DC=net  
   No current server  
   No current Naming Context
5. Type list sites and press Enter.  
   select operation target: List sites  
   The sites belonging to this domain are then listed as below:  
   Found 1 site(s)  
   0-CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=dorg,DC=net
6. Type select site <number→, where <number→ refers to the number of the site in which the domain controller was a member. Press Enter.  
   select operation target: Select site 0  
   We specify the number as 0 here, as the previous prompt let us know that 0 is the number assigned to the site available. Next you will see:  
   Site-CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=dorg,zC=net  
   Domain - DC=dorg,DC=net  
   No current server  
   No current Naming Context
7. Type list servers in site and press Enter.  
   select operation target: List servers in site  
   This will list all servers in that site with a corresponding number.  
   Found 2 server(s)  
   0-CN=SERVER200,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=dorg,DC=net  
   1-CN=SERVER100,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=dorg,DC=net
8. Type select server <number→ and press Enter, where <number→ refers to the domain controller to be removed.  
   select operation target: Select server 0  
   The number is 0 since we want to take out server200. You will be able to view:  
     
   Site-CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=dorg,DC=net Domain - DC=dorg,DC=net  
   Server-CN=SERVER200,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=dorg,DC=net  
   DSA-object-CN=NTDSSettings,CN=SERVER200,CN=Servers, CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=dorg, DC=net DNS host name - server200.dorg.net  
   Computer object-CN=SERVER200,OU= Domain Controllers,DC=dorg,DC=net
9. Type 'q' to quit and press Enter. The Metadata cleanup menu is displayed.  
   select operation target: q  
   metadata cleanup:
10. Type "remove selected server" and press Enter. You will receive a warning message. Read it, and if you agree, press Yes.

metadata cleanup: Remove selected server  
"CN=SERVER200,CN=Servers,CN=Default-First-Site-Name,  
CN=Sites,CN=Configuration,DC=dorg,DC=net" removed from server "server100"

1. Type quit, and press Enter until you return to the command prompt to remove the failed server object from the sites.
2. In Active Directory Users and Computers, expand the domain controllers container. Delete the computer object associated with the failed domain controller.
3. Windows Server 2003 AD might display a new type of question window, asking you if you want to delete the server object without performing a DCPROMO operation . Select “This DC is permanently offline…” and click on the Delete button.
4. AD will display another confirmation window. If you’re sure that you want to delete the failed object, click Yes to remove the failed server object from DNS.
5. In the DNS snap-in, expand the zone that is related to the domain from where the server has been removed. Remove the CNAME record in the \_msdcs.root domain of forest zone in DNS. You should also delete the HOSTNAME and other DNS records. If you have reverse lookup zones, also remove the server from these zones.