Disabling NTLM Authentication Guide – part 7 – Kerberos Logs

willssysadmintechblog.wordpress.com/2023/09/06/disabling-ntlm-authentication-guide-part-7-kerberos-logs

September 6, 2023

Part 6: Disabling NTLM Authentication Guide – part 6 – RDP

I forgot to include a post about Kerberos logs to watch, so I'll do that here. Seeing Kerberos authentication logs are useful to know for sure that a service is using Kerberos authentication. This can help you debug when testing with another admin. The logs you want to watch for are generated on domain controllers in the Security log.

Ticket-Granting Tickets – 4768

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4768

EventID 4768 records when a user account requests a ticket-granting ticket (TGT). TGTs are the first ticket granted when a user starts using Kerberos authentication. This ticket is later used to prove their identity to the KDC and get them service tickets (ST), which are used to authenticate to individual services.

Useful Fields to Watch

- TargetUserName: username that is being authenticated
- IpAddress: IP address the Kerberos auth is coming from, the clients IP
- EventType: Whether the auth succeeds or not

Kerberos Pre-Auth Failed – 4771

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4771

EventID 4771 tells if a user unsuccessfully requested a TGT (EventID 4768) and goes allong with EventID 4768s with EventType AUDIT_FAILURE. Something with the user's initial Kerberos authentication failed. You might want to check out the block post for Disabling NTLM Authentication Guide – part 3 – Migrating to Kerberos

Useful Fields to Watch

- TargetUserName: username that is being authenticated
- IpAddress: IP address the Kerberos auth is coming from, the clients IP

Service Ticket Was Requested – 4769

https://learn.microsoft.com/en-us/windows/security/threat-protection/auditing/event-4769

EventID 4769 tells when a user uses their already granted TGT to try to get a service ticket (ST). Once a user has a ST, they present their ST to a service. The ST's encryption is based off the service account's password, so only the service account can read the ticket's contents. The combination of the TGT and ST encryption ensures that the user and service both authenticate each other; they both know they are talking to the correct person and not an imposter.

These logs are very helpful to see if your authentication attempts are even requesting STs from the KDC, and if they're being granted properly. This can give a lot of clues as to where the errors are, and help identify if an application doesn't support Kerberos in its current configuration, even if you think everything is setup on the AD/KDC side.

Useful Fields to Watch

- ServiceName: The service account running the service you are authenticating to. This can be a normal user account, a computer account, or an AD group managed service account
- TargetUserName: username that is being authenticated
- IpAddress: IP address the Kerberos auth is coming from, the clients IP
- EventType: Whether the auth succeeds or not

Part 1: Disabling NTLM Authentication Guide – part 1 – Prerequisites

Part 2: Disabling NTLM Authentication Guide – part 2 – Logs

Part 3: Disabling NTLM Authentication Guide – part 3 – Migrating to Kerberos

Part 4: Disabling NTLM Authentication Guide – part 4 – NTLM Restrictions and Testing

Part 5: Disabling NTLM Authentication Guide – part 5 – Printers and Scanners

Part 6: Disabling NTLM Authentication Guide – part 6 – RDP

Part 7: Disabling NTLM Authentication Guide – part 7 – Kerberos Logs