SIGPwny

FA2024 Week 07 • 2024-10-17

System Administration
Active Directory

Michael Khalaf, Sagnik Chakraborty

Hardening Domain Controllers

Separation of Duties

- **Implementation**: Use different tiers (Tier 0 for Domain Controllers, Tier 1 for Servers, Tier 2 for Workstations). Only Tier 0 admins should have access to Domain Controllers.

- **Monitoring**: Regularly review admin group memberships (Enterprise Admins, Domain Admins) to ensure only those who need it have access. Set up alerts for any new additions to these groups.

Domain Controllers

Secure NTDS.dit:

- **Implementation**: Ensure that NTDS.dit (Active Directory’s database) is stored on encrypted volumes. Use BitLocker to protect disks on Domain Controllers.
- **Backups**: Use secure, off-site backups for NTDS.dit. Limit who can access these backups, and audit any access.
- **Monitoring**: Use Event ID 4662 (an object operation on NTDS.dit) to detect access attempts to sensitive AD objects.

Audit Log Settings:

- **Implementation**: Enable **"Audit Directory Service Access"** to track modifications to AD objects. Could use tools like Splunk or Microsoft Sentinel to aggregate logs.
- **Specific Events**: Monitor Event IDs:
  - **4624** (Successful Account Logon) for privileged account use.
  - **4662** for object access in AD.
  - **4742** for changes to user accounts.
  - **4771** (Kerberos pre-auth failure) and **4768** (Kerberos ticket requests) to detect Kerberos attacks.

Domain Controllers: CTF Defense

Restrict Admin Access:

- **Implement**: Limit Domain Admin access by immediately reviewing and restricting admin group membership using `net localgroup administrators` and `Get-ADGroupMember` PowerShell commands.
- **Triage**: Look for any unauthorized accounts or overly broad group memberships (service accounts in Domain Admins) and remove them.

Secure Backup of NTDS.dit:

- **Implement**: Ensure that no unauthorized users have access to the directory where NTDS.dit resides. This can be done by reviewing ACLs (`icacls C:\Windows\NTDS\NTDS.dit`) and adjusting permissions.
- **Triage**: Ensure only Domain Admins or higher-tier admins have access.

Mitigating Kerberos Abuse

SPN Management:

- **Implementation**: Periodically run scripts (using PowerShell or tools like BloodHound) to identify accounts with SPNs and ensure they’re necessary.
- **SPN Cleanup**: Remove unnecessary SPNs from accounts that don’t need them. This reduces the attack surface for Kerberoasting.
- **Monitoring**: Alert on excessive Service Ticket (TGS) requests (Event ID 4769), which could indicate Kerberoasting attempts.

AES Encryption Enforcement:

- **Implementation**: Set Kerberos encryption to use AES256 by default. Update Group Policy Objects (GPO) to disable RC4 encryption for Kerberos across the domain.
- **Monitoring**: Use Event ID 4769 to detect any instances of RC4 encryption still in use, and investigate those for potential weaknesses.

Mitigating Kerberos Abuse

Ticket Lifetime Policies:

- **Implementation**: Reduce the **Ticket Granting Ticket (TGT)** lifetime to something lower than the default (8 hours). Reduce this in CTF and rapid environments.

- **Monitoring**: Look for Event IDs like 4768 (Kerberos ticket-granting) and ensure the renew-lifetime settings are appropriate. Shorter ticket lifetimes reduce the risk of replay attacks with stolen tickets.

Mitigating Kerberos Abuse: CTF

SPN Cleanup:

- **Strategy**: Use PowerShell to identify accounts with Service Principal Names (SPNs) (`Get-ADUser -Filter {ServicePrincipalName -ne "$null"}`) and audit these quickly. If an account doesn’t need an SPN, remove it.
- **Triage**: Prioritize high-privilege accounts, ensuring none are exposed.

Ticket Lifetimes:

- **Strategy**: Immediately check and adjust Kerberos ticket policies (gpedit.msc -> Local Policies -> Security Options -> “Maximum lifetime for service ticket”). Set these to 4 hours or less to reduce the attack window.
- **Triage**: Focus on reducing TGT and service ticket lifetimes across the domain.

Defending Against Enumeration & BloodHound

Privileged Access Workstations (PAWs):

- **Implementation**: Create dedicated, isolated admin workstations (PAWs) that only allow high-privilege accounts (e.g., Domain Admins) to log in. These workstations should have strict access controls and be kept separate from the regular network.

- **Monitoring**: Set up alerts if privileged accounts attempt to log in from any workstation other than a PAW. This can be done by monitoring logon Event IDs (4624) and filtering by account and workstation.

Mitigating Kerberos Abuse

LDAP Query Throttling:

- **Implementation**: If possible, restrict large LDAP queries by setting limits through Group Policy (MaxQueryDuration or MaxPageSize) to slow down tools like BloodHound. This may not always be possible in CTFs, but it’s worth checking.
- **Triage**: Focus on monitoring LDAP traffic for large, suspicious queries and investigate.

Service Account Review:

- **Implementation**: Quickly list all service accounts and their privileges using `Get-ADUser -Filter {ServiceAccount -eq $true}`. Audit their group memberships and ensure they are not overly privileged.
- **Triage**: Remove unnecessary elevated permissions from any high-privileged service accounts.

Account Protection: MFA & More

Privileged Account Monitoring:

- **Implement**: Use Get-ADUser to quickly list privileged accounts and set up basic logging for these accounts. This can be done with PowerShell scripts that monitor logon events (4624) or any attempts to access sensitive data.
- **Triage**: Set up alerts for the most critical accounts (Domain Admins, KRBTGT) for any suspicious logon activity.

MFA for Admins:

- **Implement**: If the competition allows, set up MFA for at least the most privileged accounts (Domain Admins). Tools like Duo or Azure AD MFA can often be set up in under 30 minutes if allowed.
- **Triage**: Even if MFA for all accounts isn’t feasible, prioritize the highest-privilege users first.

Network Segmentation

Tiered Administration:

- **Implement**: Immediately review login rights and restrict admin accounts to specific machines (use Get-ADComputer to list machines). Ensure that Domain Admins can only log into Domain Controllers.
- **Triage**: Focus on reducing where admin accounts can log in. This can prevent red teamers from moving laterally across the network.

Block Unused Ports and Protocols:

- **Implement**: Disable SMB, RDP, and WinRM on systems that don’t need them. Use Set-Service in PowerShell to stop these services immediately.
- **Triage**: If lateral movement is happening, focus on killing these services on the systems red teamers are likely to target.

Block Lateral Movements

Disable WMI/WinRM:

- **Implement**: Immediately disable WMI and WinRM on as many systems as possible. This can be done quickly with:
  - `Stop-Service winrm`
  - `Stop-Service WMI`
- **Triage**: Prioritize disabling these services on high-value systems like Domain Controllers or critical servers.

Restrict Remote Access:

- **Implement**: Use Group Policy or psremoting to disable Remote PowerShell. Ensure RDP and other remote execution services are limited to essential systems only.
- **Triage**: Focus on closing these services on key targets (Domain Controllers, privileged accounts).

Threat Detection & Rapid Response

Event Log Monitoring:

Implementation: Set up basic monitoring for key Event IDs (e.g., 4624 for logon attempts, 4768 for Kerberos pre-auth, 4771 for NTLM failures) using native tools like Event Viewer or a SIEM if available.

Triage: Focus on logs from Domain Controllers and high-value targets, setting up alerts for any unusual or unauthorized activity.

Implement: Monitor for known lateral movement tools (PsExec, WMI, WinRM) using Event Logs. Set up quick alerts for process creations involving these tools (Event ID 4688).

Triage: Focus on monitoring these tools on sensitive systems like Domain Controllers and key servers.

Enumeration Rapid Response

BloodHound Defense:

- **Implement**: Detect BloodHound ingestors by monitoring LDAP queries. If possible, set up detection for unusual query volume using PowerShell or a SIEM tool.
- **Triage**: Prioritize tracking down unusual or excessive LDAP queries, which indicate enumeration attempts.

Kerberoasting Defense:

- **Implement**: Monitor Event ID 4769 for TGS requests, especially from accounts that aren’t typically used for service access. Set up real-time alerts if you suspect a Kerberoasting attack.
- **Triage**: Focus on TGS requests for high-privilege accounts, such as those with SPNs or service accounts.

Next Meetings

2024-10-22 • Next Tuesday

- Active Directory II with Ronan Boyarski

2024-10-24 • Next Thursday

- Running Secure DNS, E-Mail, FTP, SMB with Sagnik Chakraborty & Michael Khalaf