Purple Team Lifecycle

Overall Status: **Pending CM**

PB1110 - AD Best Practices – M1045 Password Policy

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2021
- Simulation Start: 2/3/2021
- Simulation End: 2/6/2021
- Configuration Identified: 11/29/2020
- Change Management Referred: 2/6/2021
- Configuration Deployed: TBD

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle Ingest and Research	• Lifecycle Type: **Best Practice** • Lifecycle Objective: **Deploy Best Practices**	• Ingest Source: **BHIS Webcast** https://www.blackhillsinfosec.com/webcast-group-policies-that-kill-kill-chains/ • Mitre Mitigation: M1027 https://attack.mitre.org/mitigations/M1027/
	• Strengthen credential storage by increasing password length requirements and reducing max password age.	
Attack methodology	• Review current GPO deployments. **8 minimum characters** **No complexity requirement** **180 days max age** **1-day minimum age**	
Defense methodology	• Update the existing Default Group Policy to update password policy.	
Lifecycle Adjustments	• Deploy Password Policy for best practices. **15 minimum characters** **Enable complexity requirements** **90 Day max password age** **1 Day min password age**	
Change Management	• Update password policy to Lifecycle Adjustment defined. • Affected Users: All Employees • Roll-back procedure: Revert password policy configuration.	
Lessons Learned	• Passwords less than 14 characters are considered weak and should be replaced with passwords over 14 characters in length.	

Purple Team Lifecycle

Overall Status: **Pending CM**

PB1112 - AD Best Practices – GPP T1552.006 Unsecured Credentials

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2021
- Simulation Start: 2/3/2021
- Simulation End: 2/6/2021
- Configuration Identified: 11/29/2020
- Change Management Referred: 2/6/2021
- Configuration Deployed: TBD

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle Ingest and Research	• Lifecycle Type: **Best Practice** • Lifecycle Objective: **Deploy Best Practices**	• Ingest Source: **BHIS Webcast** https://www.blackhillsinfosec.com/webcast-group-policies-that-kill-kill-chains/ • Mitre: T1552.006 https://attack.mitre.org/techniques/T1552/006/
	• Check for any Group Policy Preference Passwords. Update any group policies with alternative configuration	

Attack methodology	• Use Metasploit with a domain authenticated session.
	`msf > use post/windows/gather/credentials/gpp`
	`msf post(gpp) > sessions`
	`...sessions...`
	`msf post(gpp) > set SESSION <session-id>`
	`msf post(gpp) > show options`
	`...show and set options...`
	`msf post(gpp) > run`	

Defense methodology	• No GPP's were found in deployed Group Policies	
Lifecycle Adjustments	• No changes needed	
Change Management	• N/A	
Lessons Learned	• N/A	

Purple Team Lifecycle

Overall Status: **Pending CM**

PB1113 - AD Best Practices – M1036 Account Lockout Policies

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2021
- Simulation Start: 2/3/2021
- Simulation End: 2/6/2021
- Configuration Identified: 11/29/2020
- Change Management Referred: 2/6/2021
- Configuration Deployed: TBD

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle Ingest and Research	• Lifecycle Type: **Best Practice** • Lifecycle Objective: **Deploy Best Practices**	• Ingest Source: **BHIS Webcast** https://www.blackhillsinfosec.com/webcast-group-policies-that-kill-kill-chains/ • MITRE Mitigation: M1036 https://attack.mitre.org/mitigations/M1036/
	• Check for any Group Policy Preference Passwords. Update any group policies with alternative configuration	
Attack methodology	• Review current GPO deployments. **Account Lockout Duration: 10 minutes** **Account Lockout Threshold: 10 invalid logon attempts** **Reset account Lockout After: 5 minutes**	
Defense methodology	• Update the existing Default Group Policy to update password policy.	
Lifecycle Adjustments	• Deploy Password Policy for best practices. **Account Lockout Duration: 120 minutes** **Account Lockout Threshold: 5 invalid logon attempts** • **Reset account Lockout After: 15 minutes**	
Change Management	• Update account lockout policy to Lifecycle Adjustment defined. • Affected Users: All Employees • Roll-back procedure: Revert password policy configuration.	
Lessons Learned	• N/A	

Purple Team Lifecycle

Overall Status: **Pending CM**

PB1114 - AD Best Practices – LanMan Hashes

Lifecycle Project Manager
Kent Ickler
Office: 605-939-0331
Email: kent@defensiveorigins.com

- Lifecycle Kickoff: 2/1/2021
- Simulation Start: 2/3/2021
- Simulation End: 2/6/2021
- Configuration Identified: 11/29/2020
- Change Management Referred: 2/6/2021
- Configuration Deployed: TBD

Status Code Legend
- Attack Simulation
- Defense Simulation
- System Configuration Change
- Information

APT Lifecycle Ingest and Research	• Lifecycle Type: **Best Practice** • Lifecycle Objective: **Deploy Best Practices**	• Ingest Source: **BHIS Webcast** https://www.blackhillsinfosec.com/webcast-group-policies-that-kill-kill-chains/
	• Stop Active Directory from storing LanMan hashes	
Attack methodology	• Review current GPO deployments: LanMan hashes are currently utilized.	
Defense methodology	• Update the existing Default Group Policy to update password policy. GPO: Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network Security: Do not store LAN Manager hash value on the next password change: Enabled.	
Lifecycle Adjustments	• Deploy Lan Manager Hash Storage Prevention GPO to DC's	
Change Management	• Create a GPO that prevents LanManager hash storage. Apply GPO to domain controllers. • Affected Users: Domain Controllers • Roll-back procedure: Remove GPO	
Lessons Learned	• The existing LanManager Hash will not be removed from AD object attributes after setting the GPO.	