ATOMIC PURPLE TEAM

APPLIED PURPLE TEAMING

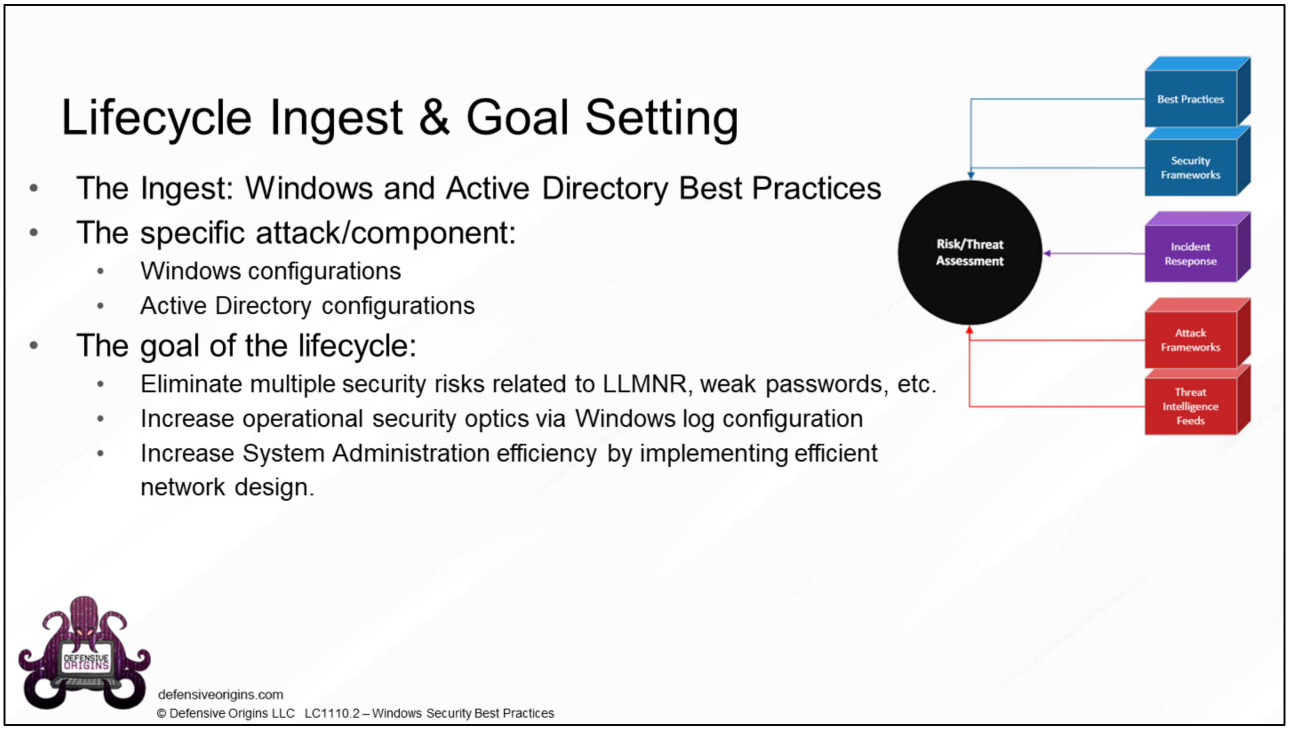
LC1110

APTLC: AD Best Practices

Microsoft Windows
Active Directory Best Practices

defensiveorigins.com

LC1110.1 – Windows Security Best Practices



Lifecycle Ingest & Goal Setting

- The Ingest: Windows and Active Directory Best Practices
- The specific attack/component:
  - Windows configurations
  - Active Directory configurations
- The goal of the lifecycle:
  - Eliminate multiple security risks related to LLMNR, weak passwords, etc.
  - Increase operational security optics via Windows log configuration
  - Increase System Administration efficiency by implementing efficient network design.

Best Practices

Security Frameworks

Risk/Threat Assessment

Incident Reseponse

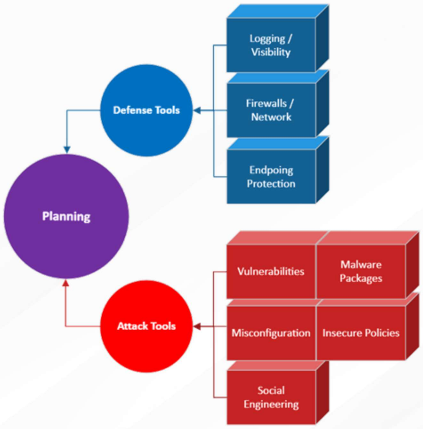
Attack Frameworks

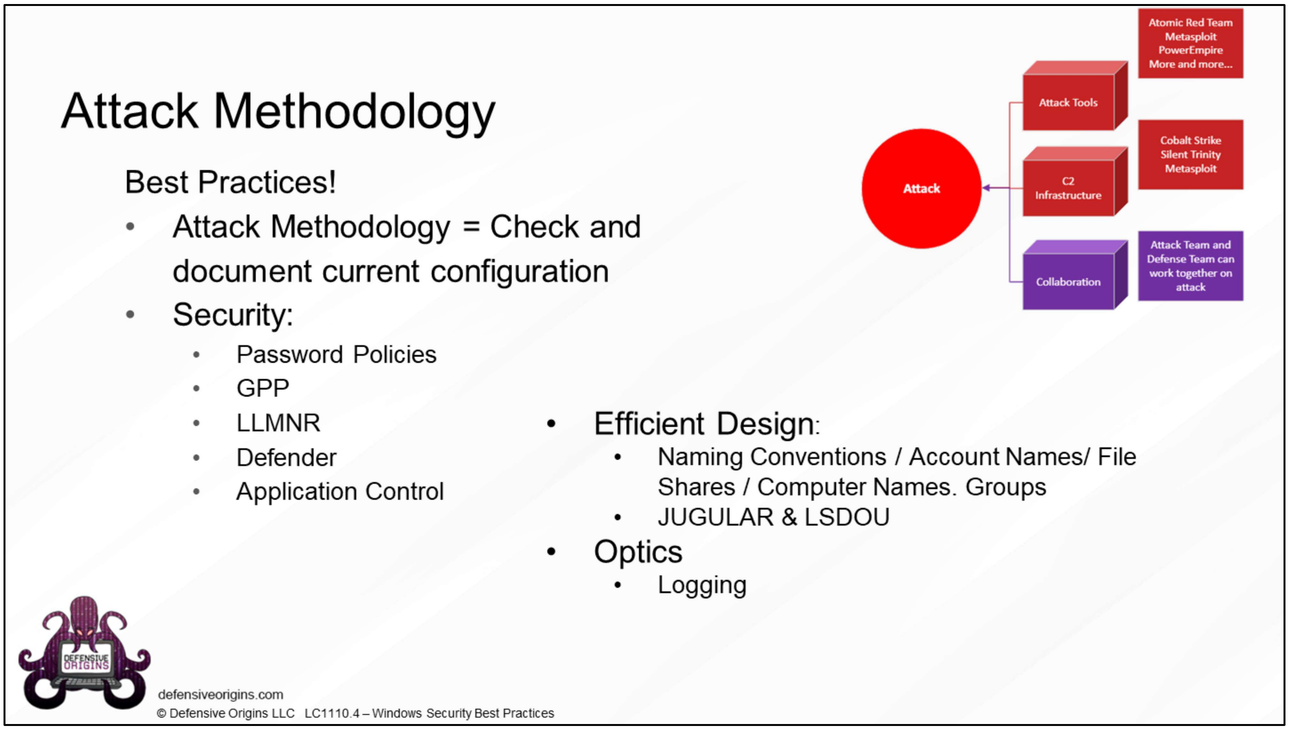
Threat Intelligence Feeds

- The Ingest: Windows and Active Directory Best Practices
- The specific attack/component:
  - Windows configurations
  - Active Directory configurations
- The goal of the lifecycle:
  - Eliminate multiple security risks related to LLMNR, weak passwords, etc.
  - Increase operational security optics via Windows log configuration
  - Increase System Administration efficiency by implementing efficient network design.

Planning – Methodology

- Review current system and Active Directory configurations - GPO, permissions, etc.
- Deploy best practices in controlled environment
- Ensure the deployment of configuration increased security posture and did not introduce new vulnerabilities or negatively impact business





Attack Methodology

Best Practices!

- Attack Methodology = Check and document current configuration
- Security:
  - Password Policies
  - GPP
  - LLMNR
  - Defender
  - Application Control

Attack

Attack Tools

Atomic Red Team
Metasploit
PowerEmpire
More and more…

C2
Infrastructure

Cobalt Strike
Silent Trinity
Metasploit

Collaboration

Attack Team and Defense Team can work together on attack

- Efficient Design:
  - Naming Conventions / Account Names/ File Shares / Computer Names. Groups
  - JUGULAR & LSDOU
- Optics
  - Logging

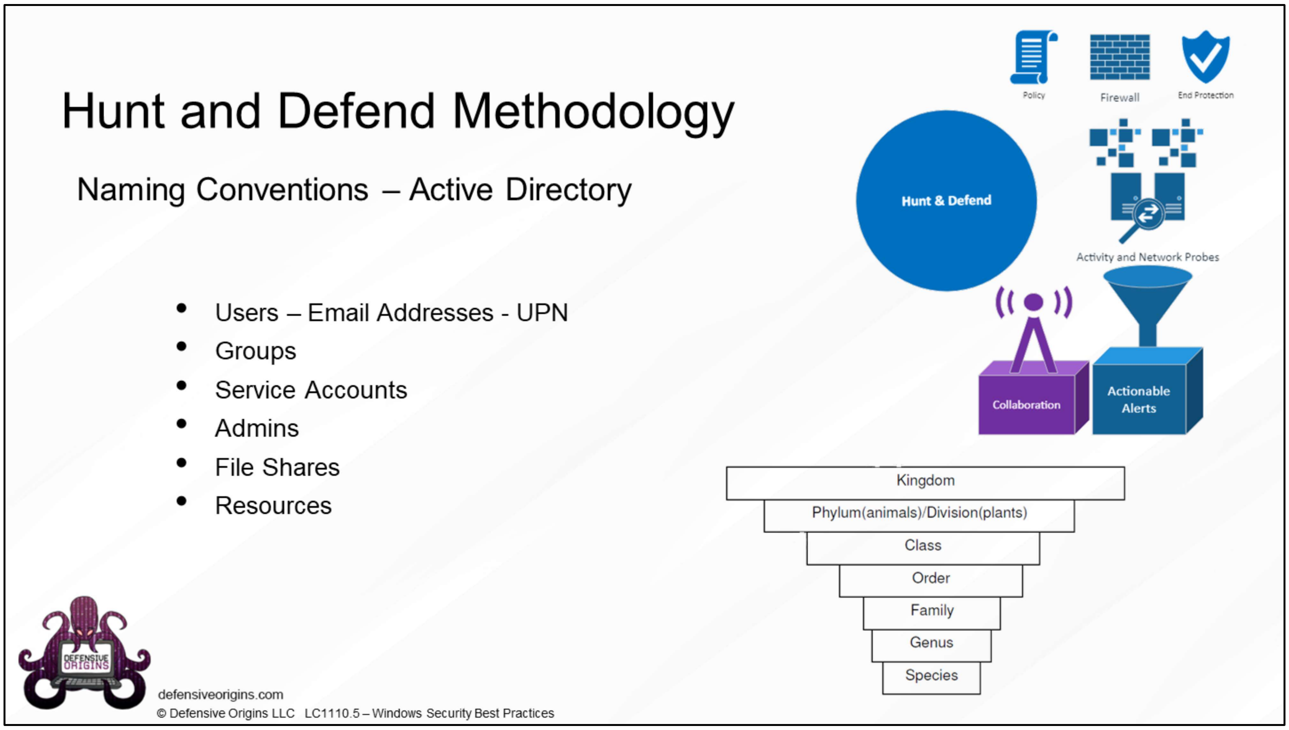
defensiveorigins.com

Best Practices!

- Attack Methodology = Check and document current configuration
- Security:
  - Password Policies
  - GPP
  - LLMNR
  - Defender
  - Application Control

- Efficient Design:
  - Naming Conventions / Account Names/ File Shares / Computer Names. Groups
  - JUGULAR & LSDOU
- Optics
  - Logging

Blog and Video: https://www.blackhillsinfosec.com/active-directory-best-practices-to-frustrate-attackers-webcast-write-up/



Hunt and Defend Methodology

Naming Conventions – Active Directory

- Users – Email Addresses - UPN
- Groups
- Service Accounts
- Admins
- File Shares
- Resources

Kingdom
Phylum(animals)/Division(plants)
Class
Order
Family
Genus
Species

defensiveorigins.com

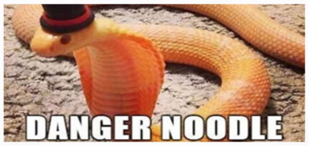
- Microsoft *KB number:* 909264: https://docs.microsoft.com/en-us/troubleshoot/windows-server/identity/naming-conventions-for-computer-domain-site-ou

Hunt and Defend Methodology

Naming Conventions – User Accounts

- Users
  - Login & UPN
  - Email Addresses (External)
- Administrators
- Service Accounts
- Contractors
- Vendors

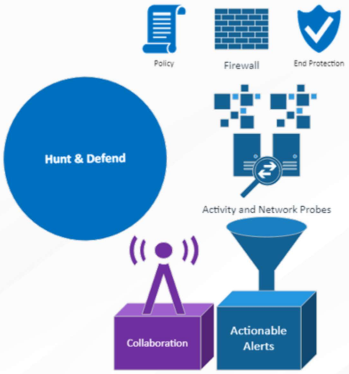
- Admin != Standard User



Hunt and Defend Methodology

Naming Conventions – File Shares

- Who "owns" the data?
- Share Data between Departments?
- Server Locations/Functions



PROTIP: NEVER LOOK IN SOMEONE ELSE'S DOCUMENTS FOLDER.

Hunt and Defend Methodology

AD Group Management

Policy
Firewall
End Protection
Hunt & Defend
Activity and Network Probes
Collaboration
Actionable Alerts

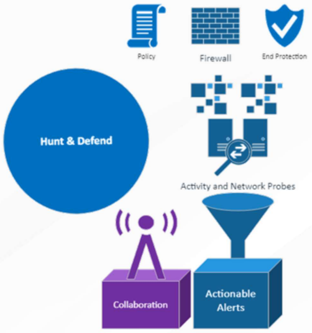
jUGULaR

- **J**ust because it needed to be clever
- **U**sers
- **G**lobal Groups
- **U**niversal Groups
- **L**ocal **A**ccess to **R**esources

Hunt and Defend Methodology

AD Group Management

- User Groups
- Security Groups
- Distribution Groups
- Mail Enabled Security Groups
- Domain Local
- Global
- Universal

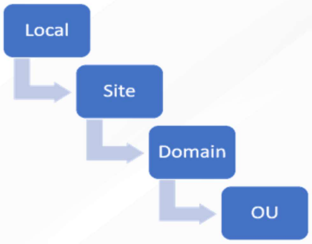


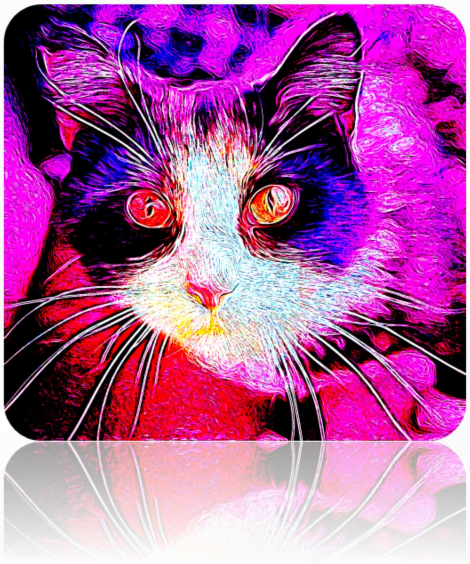
Hunt and Defend Methodology

Deploy Best Practice Configuration

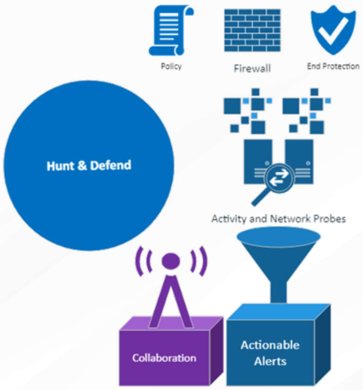
LSD-OU

- User or computer
- Templates or Policy Preferences
- Manage local administrators – workstation and server
- Password Policy
- Loopback Processing Mode?

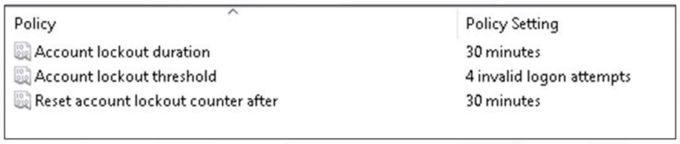




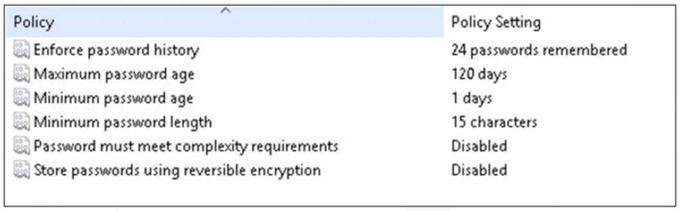
Hunt and Defend Methodology



- Deploy Best Practice Configuration
- Default Domain Policy

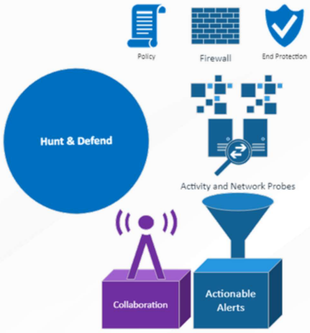


Policy	Policy Setting
Account lockout duration	30 minutes
Account lockout threshold	4 invalid logon attempts
Reset account lockout counter after	30 minutes

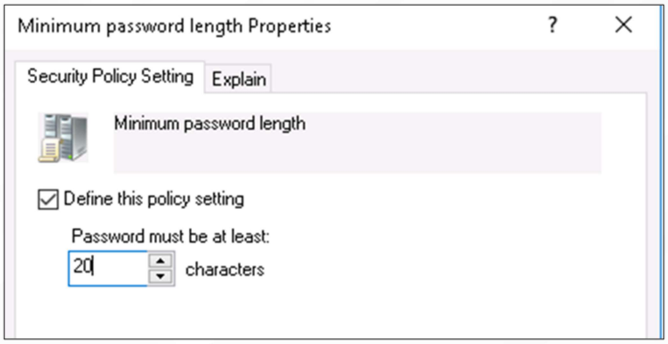


Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	120 days
Minimum password age	1 days
Minimum password length	15 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Hunt and Defend Methodology



- Deploy Best Practice Configuration – Password Policies
- #NotNIST
  - 2016 Active Directory = 20 Min Char ok!

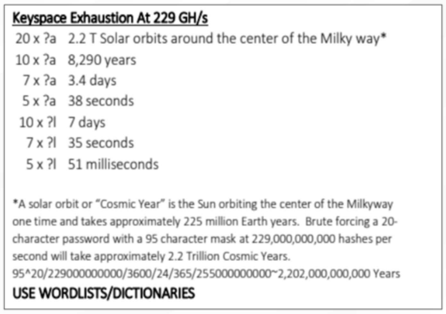


Minimum password length

☑ Define this policy setting

Password must be at least:

20 characters



Keyspace Exhaustion At 229 GH/s

20 x ?a	2.2 T Solar orbits around the center of the Milky way*
10 x ?a	8,290 years
7 x ?a	3.4 days
5 x ?a	38 seconds
10 x ?l	7 days
7 x ?l	35 seconds
5 x ?l	51 milliseconds

*A solar orbit or "Cosmic Year" is the Sun orbiting the center of the Milkyway one time and takes approximately 225 million Earth years. Brute forcing a 20-character password with a 95 character mask at 229,000,000,000 hashes per second will take approximately 2.2 Trillion Cosmic Years.
95^20/229000000000/3600/24/365/255000000000~2,202,000,000,000 Years

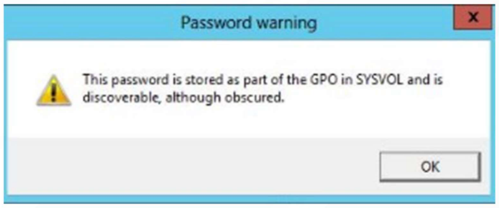
USE WORDLISTS/DICTIONARIES

Hunt and Defend Methodology

Policy
Firewall
End Protection
Hunt & Defend
Activity and Network Probes
Collaboration
Actionable Alerts

- Deploy Best Practice Configuration

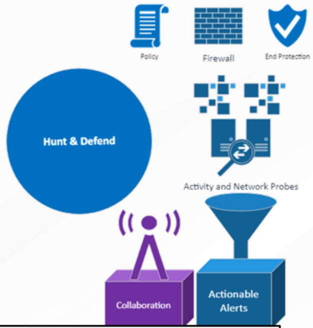
- Group Policy Preferences Password Storage
- Sysvol Scripts
- MS14-025


Password warning

This password is stored as part of the GPO in SYSVOL and is discoverable, although obscured.

```
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
```

Hunt and Defend Methodology



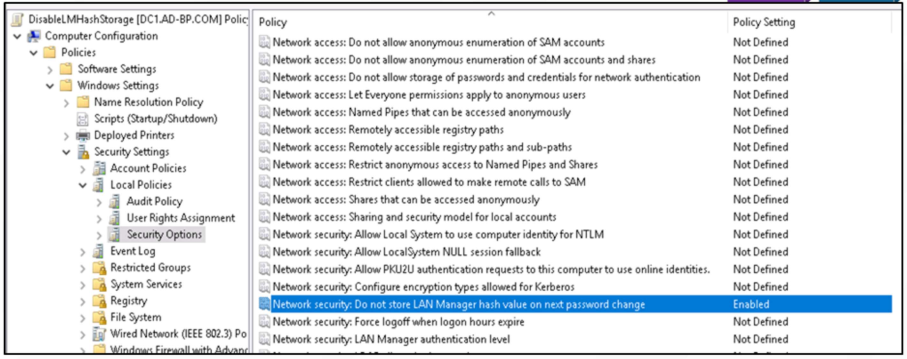
Deploy Best Practice Configuration

Destroying LANMAN

Do not store LANMAN hashes.

Powerful crackers shred these hashes – LM benchmark (Nvidia GTX 1080): **18382.7** MH/s

(that's 18B/sec)

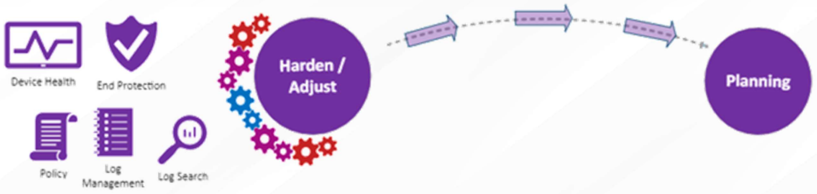


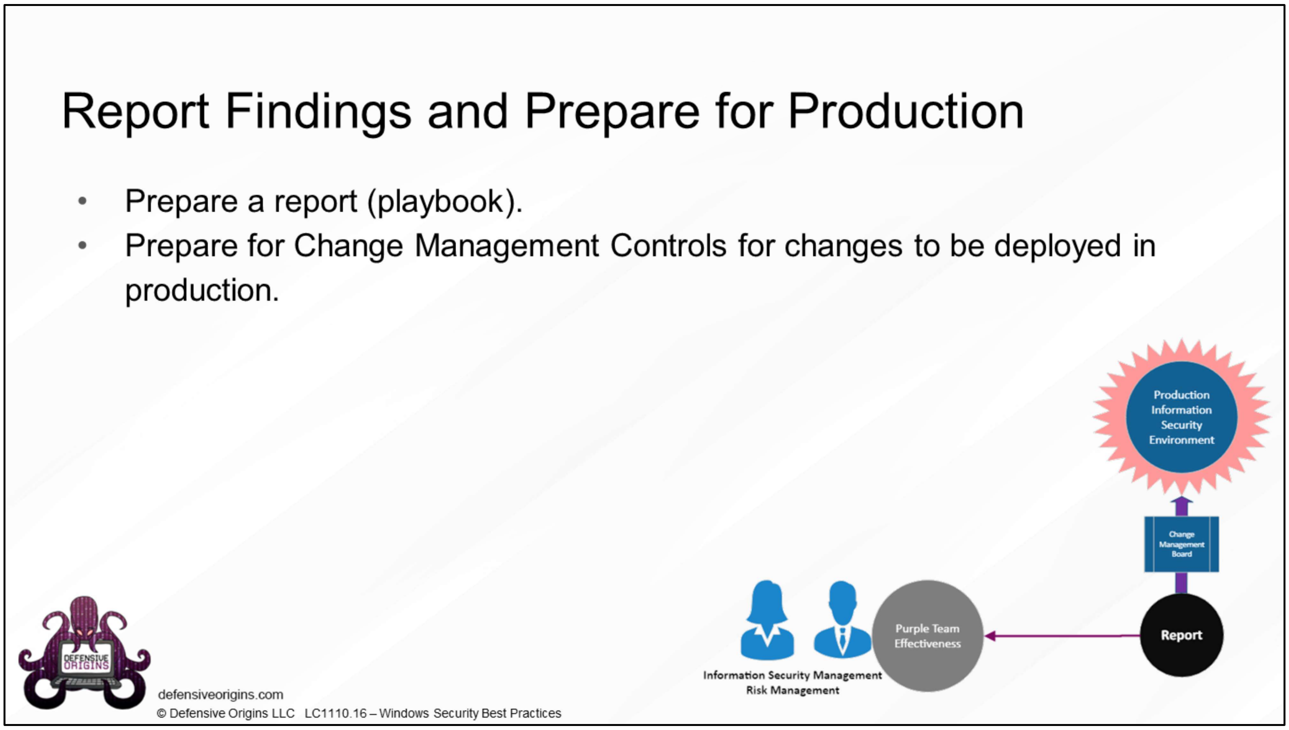
```
DisableLMHashStorage [DC1.AD-BP.COM] Polic
  Computer Configuration
    Policies
      Software Settings
      Windows Settings
        Name Resolution Policy
        Scripts (Startup/Shutdown)
        Deployed Printers
        Security Settings
          Account Policies
          Local Policies
            Audit Policy
            User Rights Assignment
            Security Options
          Event Log
          Restricted Groups
          System Services
          Registry
          File System
          Wired Network (IEEE 802.3) Po
          Windows Firewall with Advanc
```

Policy	Policy Setting
Network access: Do not allow anonymous enumeration of SAM accounts	Not Defined
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Not Defined
Network access: Do not allow storage of passwords and credentials for network authentication	Not Defined
Network access: Let Everyone permissions apply to anonymous users	Not Defined
Network access: Named Pipes that can be accessed anonymously	Not Defined
Network access: Remotely accessible registry paths	Not Defined
Network access: Remotely accessible registry paths and sub-paths	Not Defined
Network access: Restrict anonymous access to Named Pipes and Shares	Not Defined
Network access: Restrict clients allowed to make remote calls to SAM	Not Defined
Network access: Shares that can be accessed anonymously	Not Defined
Network access: Sharing and security model for local accounts	Not Defined
Network security: Allow Local System to use computer identity for NTLM	Not Defined
Network security: Allow LocalSystem NULL session fallback	Not Defined
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Not Defined
Network security: Configure encryption types allowed for Kerberos	Not Defined
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Not Defined
Network security: LAN Manager authentication level	Not Defined

Adjust / Harden

- Are adjustments needed to reach LC Goal?
- Document adjustments and attempt attack/defense again.





Report Findings and Prepare for Production

- Prepare a report (playbook).
- Prepare for Change Management Controls for changes to be deployed in production.

Production Information Security Environment
Change Management Board
Report
Purple Team Effectiveness
Information Security Management
Risk Management

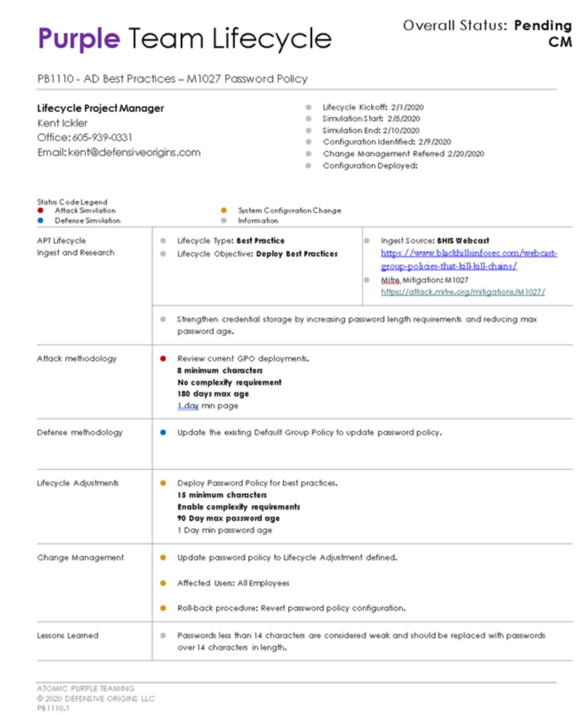
Lifecycle Reports?

Best Practice

Password Policy (way more than length)

- Storage
- Access
- Sharing
- Network Devices, Printers, et cetera

MITRE: M1027



Purple Team Lifecycle

Overall Status: **Pending CM**

PB1110 - AD Best Practices – M1027 Password Policy

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

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/5/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred 2/20/2020
- Configuration Deployed:

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 min page	
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.	

ATOMIC PURPLE TEAMING
© 2020 DEFENSIVE ORIGINS LLC
PB1110.1

Lifecycle Reports?

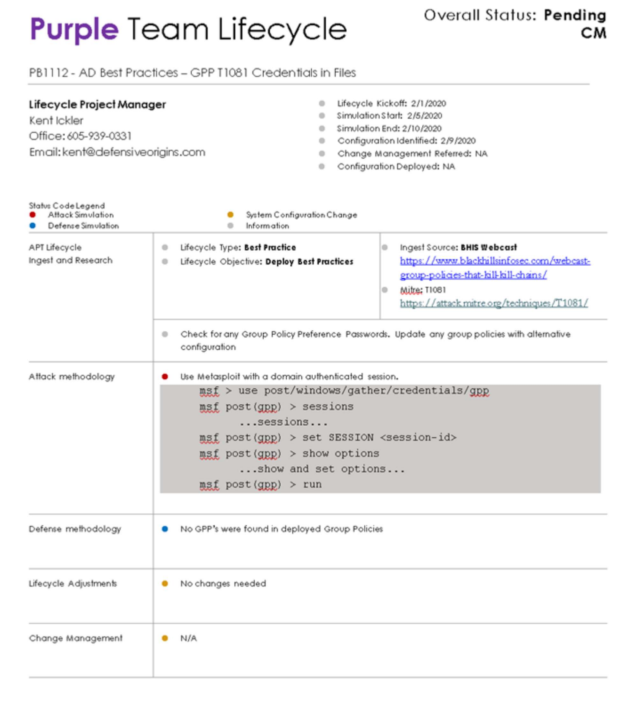
Best Practice

Group Policy Preferences (GPP) Check

- MS leaked the decrypt key while back
- Still find them on occasion

MITRE:

`https://attack.mitre.org/techniques/T1552/006/`



Purple Team Lifecycle

Overall Status: **Pending CM**

PB1112 - AD Best Practices – GPP T1081 Credentials in Files

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

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/5/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred: NA
- Configuration Deployed: NA

Status Code Legend

● Attack Simulation	● System Configuration Change
● Defense Simulation	● 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: T1081 https://attack.mitre.org/techniques/T1081/
	● Check for any Group Policy Preference Passwords. Update any group policies with alternative configuration	
Attack methodology	● Use Metasploit with a domain authenticated session.	
Defense methodology	● No GPP's were found in deployed Group Policies	
Lifecycle Adjustments	● No changes needed	
Change Management	● N/A	

```
    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
```

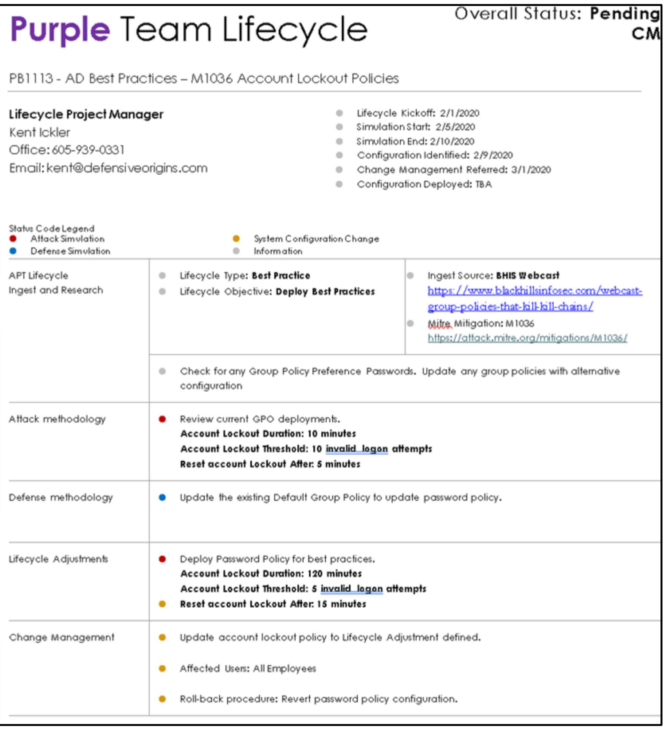
Lifecycle Reports?

Best Practice

Account Lockout Policies

- Widen the observation window
- Reduce the attempts
- Normalize the account unlock timer

MITRE: M1036



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: 2/1/2020
- Simulation Start: 2/5/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred: 3/1/2020
- Configuration Deployed: TBA

Status Code Legend

🔴 Attack Simulation	🟠 System Configuration Change
🔵 Defense Simulation	⚪ Information

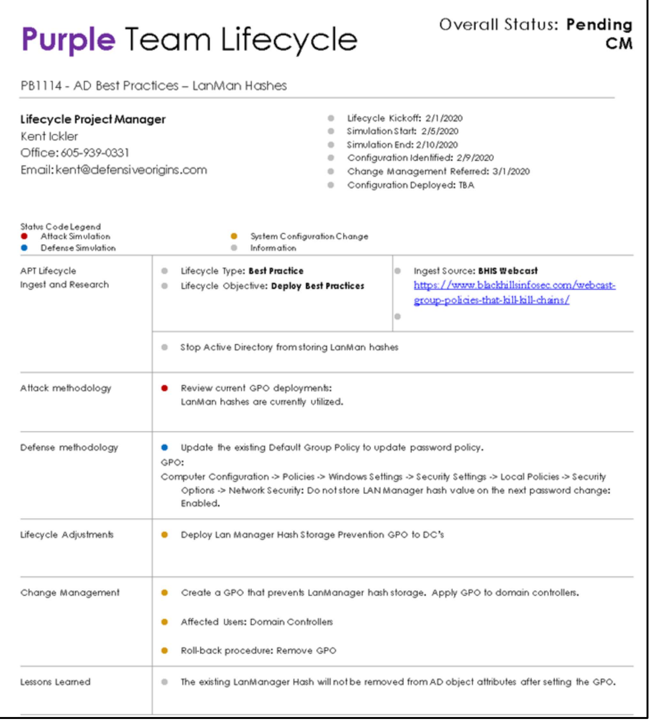
APT Lifecycle Ingest and Research	⚪ Lifecycle Type: **Best Practice** ⚪ Lifecycle Objective: **Deploy Best Practices**	⚪ Ingest Source: **BHIS Webcast** https://www.blackhillsinfosec.com/webcast-group-policies-that-kill-kill-chains/ ⚪ Mitre Mitigation: M1036 https://attack.mitre.org/mitigations/M1036/
	⚪ 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.	

Lifecycle Reports?

Best Practice

Eliminate LanManager Hash Storage

- Yeah, don't really need these much
- Trivial to crack
- Yes, they are still around (legacy)



Purple Team Lifecycle

Overall Status: **Pending CM**

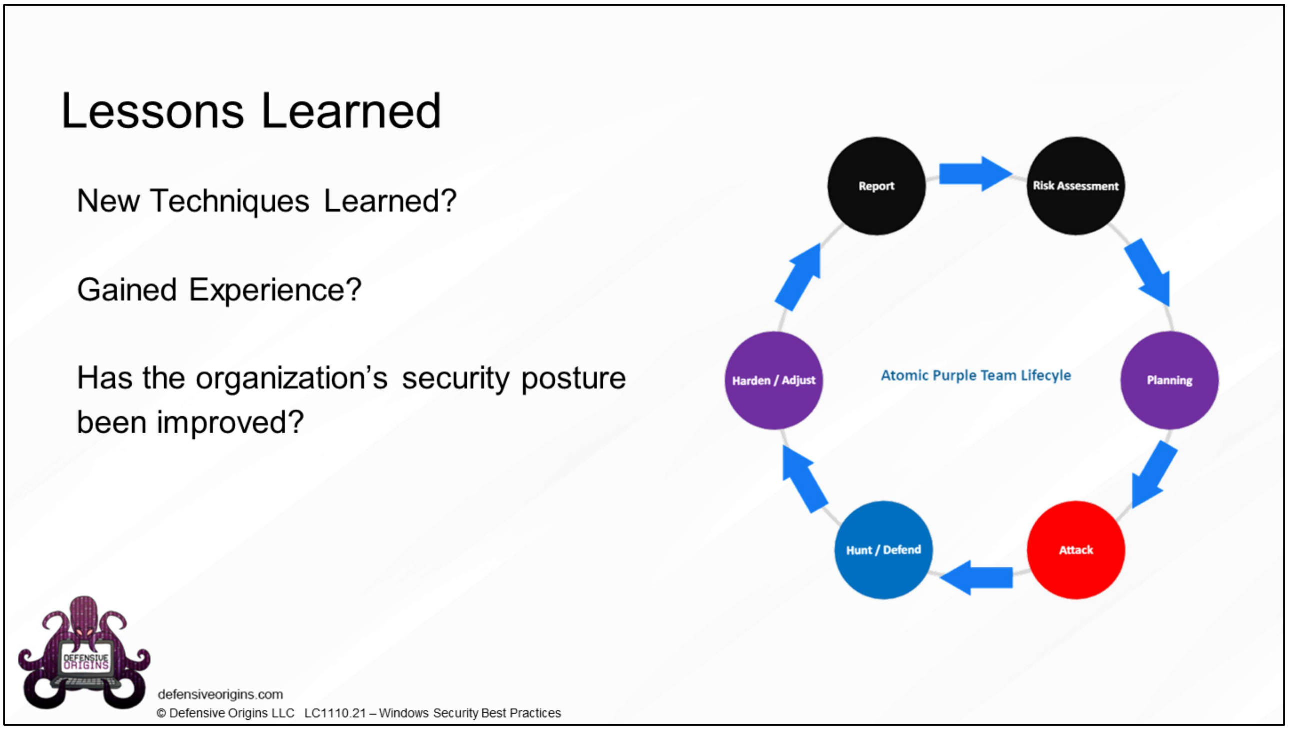
PB1114 - AD Best Practices – LanMan Hashes

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

- Lifecycle Kickoff: 2/1/2020
- Simulation Start: 2/5/2020
- Simulation End: 2/10/2020
- Configuration Identified: 2/9/2020
- Change Management Referred: 3/1/2020
- Configuration Deployed: TBA

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.	



Lessons Learned

New Techniques Learned?

Gained Experience?

Has the organization’s security posture been improved?

Atomic Purple Team Lifecyle

Report

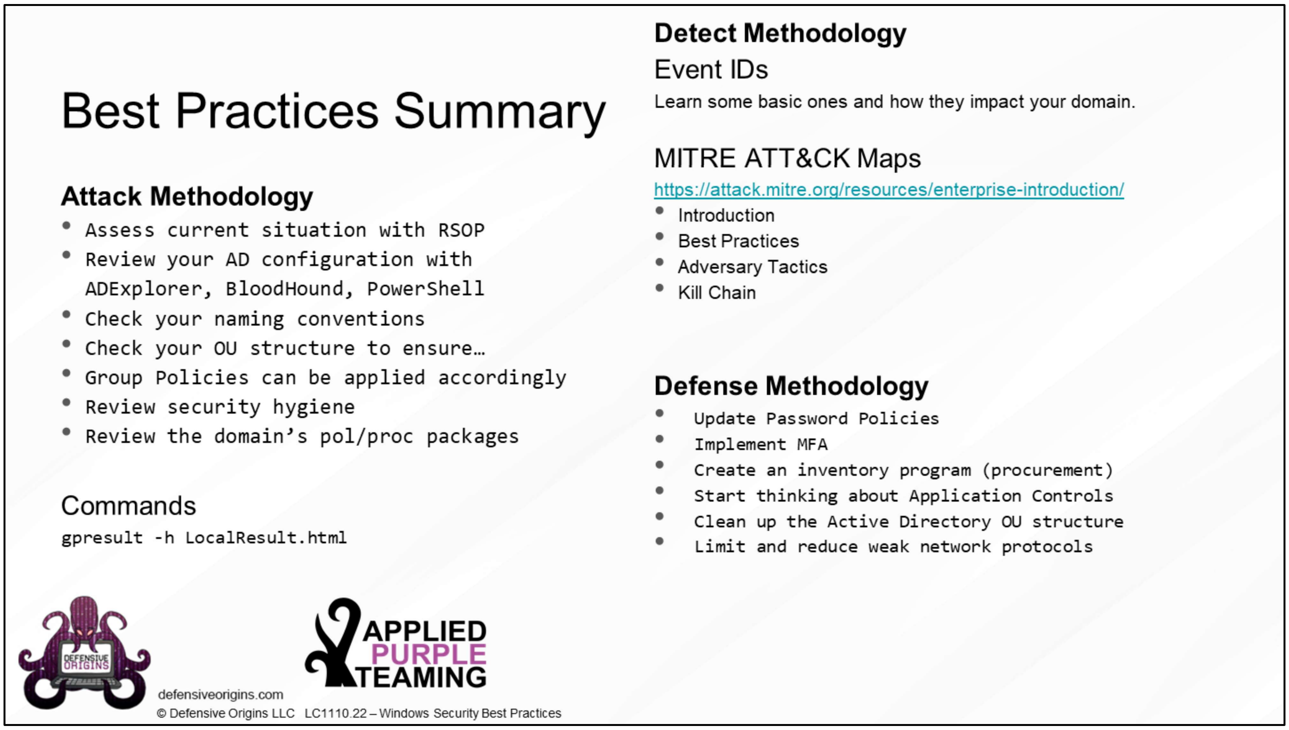
Risk Assessment

Planning

Attack

Hunt / Defend

Harden / Adjust



Best Practices Summary

Attack Methodology

- Assess current situation with RSOP
- Review your AD configuration with ADExplorer, BloodHound, PowerShell
- Check your naming conventions
- Check your OU structure to ensure…
- Group Policies can be applied accordingly
- Review security hygiene
- Review the domain’s pol/proc packages

Commands

```
gpresult -h LocalResult.html
```

Detect Methodology

Event IDs

Learn some basic ones and how they impact your domain.

MITRE ATT&CK Maps

https://attack.mitre.org/resources/enterprise-introduction/

- Introduction
- Best Practices
- Adversary Tactics
- Kill Chain

Defense Methodology

- Update Password Policies
- Implement MFA
- Create an inventory program (procurement)
- Start thinking about Application Controls
- Clean up the Active Directory OU structure
- Limit and reduce weak network protocols