MACS IN WINDOWS SERVER ENVIRONMENTS: *BINDING TO AD*

Luis Giraldo - Ook Enterprises Ltd.
luis@ook.co - @luisgiraldo

WHY?

WHY?

WHY?

WHY BIND TO AD?

- Password policy
- Single Sign-On (SSO)
- Managed access to resources
- User and Machine certificates can be requested
- Traversing DFS namespaces
- In some fixed-computer environments, still the least path of resistance

LET'S DISCUSS PASSWORD POLICY

- Queries AD for password policy at bind and periodically afterwards
- Policy enforced for all network/mobile accounts


The system was unable to unlock your login keychain.
If you remember your old password you can update the keychain password. If you do not remember your old password, you can create a new login keychain or choose to leave the login keychain using a different password.
Would you like to update the password, create a new keychain, or continue the login?
Continue Log In
Create New Keychain
Update Keychain Password

- Prompts for change once within 14 days of expiry
- If dismissed prompts every day until day before
- Within 24 hours, password change is required

HOW DO I FIX THIS?

USER TRAINING

OR DON’T BIND TO AD

LET'S DISCUSS SINGLE SIGN-ON

- Password only required once, get access to many services
- Token (TGT) expires, can't renew off network, Kerberos prioritized over other auth mechanisms
- Auth to screen saver attempts a TGT renewal
- Proper forward and reverse DNS is a must for kerberized servers
- Clock drift must be less than 5 minutes, use NTP!

KERBEROS COMMANDS

```
pipe:~ luis$ klist
klist: krb5_cc_get_principal: No credentials cache file found
pipe:~ luis$ kinit
luis@CORP.OOK.CO's password:
pipe:~ luis$ klist
Credentials cache: API:AD2D9709-1B41-437[redacted]
        Principal: luis@CORP.OOK.CO

  Issued                Expires               Principal
Jun 14 22:30:03 2016  Jun 15 08:29:59 2016  krbtgt/CORP.OOK.CO@CORP.OOK.CO
pipe:~ luis$ kdestroy
pipe:~ luis$ klist
klist: krb5_cc_get_principal: No credentials cache file found
```

LET'S DISCUSS
DFS NAMESPACE SUPPORT

- Can query WINS servers and use correct SMB server
- Use DFS namespace's FQDN in Finder
- Will use existing TGT

LET'S DISCUSS CERTIFICATES

Once bound, certificates easily requested with a config profile

AD Certificate

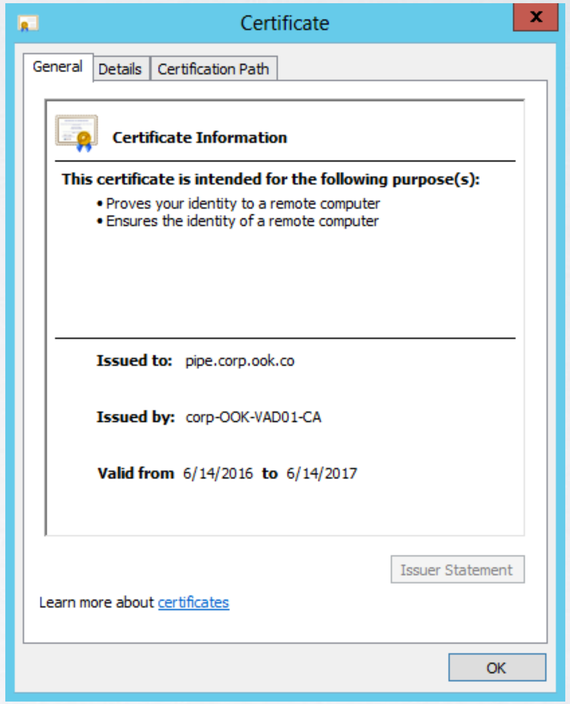
Description
The description of the certificate request as shown in the certificate selector of other payloads such as VPN and Network
Acquire certificate via DCE/RPC

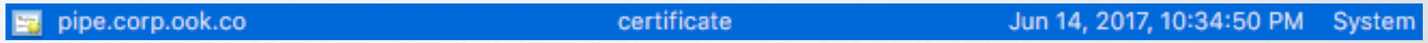
Certificate Server
The network address of the certificate server
ook-vad01.corp.ook.co

Certificate Authority
The name of the CA
corp-OOK-VAD01-CA

Certificate Template
The name of the certificate template, usually Machine or User
Machine

Certificate Expiration Notification Threshold
The number of days before the certificate expires at which to start showing the expiration notification
14





BUT...

DO WE REALLY NEED IT?

- Password policy - can be enforced with MDM
- Managed access to resources - Can still leverage binding
- Single Sign-On (SSO) - kinit + AppleScript
- User and Machine certificates - can be delivered via MDM
- And…can mostly be done OTA

NEW STRATEGIES NEEDED?

- Most of the original reasons for directory services are now available via MDM
- MDM can provide many of the same organizational security requirements, at scale and with remote capability for off-network mobile devices (iOS and macOS)
- Different strategy needed for portable computer users who transition frequently between networks

DEMO

DEMO ENVIRONMENT

ADDS, ADCS, DNS, FS

RESOURCES

Windows Server Trial

Troubleshooting and Debugging
List of available trusted root certs in OS X
Advanced AD options for profiles
Best Practices

Active Directory naming considerations when binding:
https://support.apple.com/en-us/HT203193
https://support.microsoft.com/en-ca/kb/909264

Requesting and renewing a certificate:
https://support.apple.com/en-ca/HT204602
https://support.apple.com/en-ca/HT204446

Export AD CS root cert

THANK YOU!

Luis Giraldo
luis@ook.co
@luisgiraldo