NTDS.DIT processing

The provided contest image “DEFCON.ova.xz.pgp” contained, besides the DEFCON.mf and DEFCON.ovf, one DEFCON-disk001.vmdk.
Such a “vmdk”-file can either be converted into a raw image or mounted directly. Later one was the first step chosen to access the stored data.

Under Linux, following commands were executed:

sudo modprobe nbd
sudo qemu-nbd -r -c /dev/nbd1 DEFCON-disk001.vmdk
sudo mount -o ro /dev/nbd1p1 <mount-point>

A quick search revealed 4 “ntds.dit”-files of which one was the target file to process:

Location: “\Windows\NTDS\ntds.dit”
Filesize: 1.9GB
SHA256: 93e3709f219295c8c5d464c43abc0713af0a6a63449cf1c1eaab86a121a51b03

There are several tools to parse “ntds.dit”-Files, of which the PowerShell-Tool “DSInternals” [https://www.dsinternals.com] proved to be the most reliable in this contest.

Following the Installation procedure from the Website (with PowerShell 5)

Install-Module -Name DSInternals -Force

Although the File was corrupted and needed repair first. (PowerShell)

esentutil /p .\ntds.dit [repair]
esentutil /d .\ntds.dit [defragmentation]
esentutil /g .\ntds.dit [integrity-check]

For processing the ntds.dit, the SYSTEM-Hive-File was required as well

Location: “\Windows\System32\config\SYSTEM”

Following the commands for processing

$key = Get-BootKey -SystemHivePath 'SYSTEM'
Get-ADDBAccount -All -DBPath 'ntds.dit' -BootKey $key

This output redirected into a file is a dump from the ntds.dit in “Little-endian UTF-16 Unicode text, with CRLF line terminators”. (an example object from this dump is presented below)

The dump contains:

- 8,999 User-Objects
- 670,181 Computer-Objects

After extraction of all user-accounts, each object-field was parsed and processed, which revealed 100 entries for “Training”-user and a filled “Description”-field containing “Description: Password_is_” and a 12 character plaintext password (digits, uppercase, lowercase)

Example User-Object from “ntds.dit”-dump:

DistinguishedName: CN=krbtgt,CN=Users,DC=crackmeifyoucan,DC=com
Sid: S-1-5-21-2081535704-4210724908-3814002959-502
Guid: ca988aff-d450-45fb-884a-9a98686a058e
SamAccountName: krbtgt
SamAccountType: User
UserPrincipalName:
PrimaryGroupId: 513
SidHistory:
Enabled: False
UserAccountControl: Disabled, NormalAccount
AdminCount: True
Deleted: False
LastLogonDate:
DisplayName:
GivenName:
Surname:
Description: Key Distribution Center Service Account
ServicePrincipalName: {kadmin/changepw}
SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent,
DiscretionaryAclAutoInherited, SystemAclAutoInherited,
DiscretionaryAclProtected, SelfRelative
Owner: S-1-5-21-2081535704-4210724908-3814002959-512
Secrets
  NTHash: 42a0648655a9037a87bc0562e96b958a
  LMHash:
  NTHashHistory:
        Hash 01: 42a0648655a9037a87bc0562e96b958a
  LMHashHistory:
        Hash 01: 6bc7d96f749793327ec16fc7cc5c3479
  SupplementalCredentials:
        ClearText:
        NTLMStrongHash: 2e21413116c097b2b214d6b91f8187e7
        Kerberos:
        Credentials:
        DES_CBC_MD5
        Key: c11c1cb0ce97ae52
        OldCredentials:
        Salt: CRACKMEIFYOUCAN.COMkrbtgt
        Flags: 0
        KerberosNew:

Credentials:
AES256_CTS_HMAC_SHA1_96
Key: 7bab1f9fe142bdd85e8170dddc1919e675f9120e021c1f5fb5fa2f53c25b5c75
Iterations: 4096
AES128_CTS_HMAC_SHA1_96
Key: 0e2a175d19c040da0813439b69a4446f
Iterations: 4096
DES_CBC_MD5
Key: c11c1cb0ce97ae52
Iterations: 4096
OldCredentials:
OlderCredentials:
ServiceCredentials:
Salt: CRACKMEIFYOUCAN.COMkrbtgt
DefaultIterationCount: 4096
Flags: 0
WDigest:
Hash 01: ae11e7d4368961f9fc2bb66fef654e2d
Hash 02: 978694c66095697ce240c15971fdb356
Hash 03: 5ee0e216063c9cc26ae0863e46e42451
Hash 04: ae11e7d4368961f9fc2bb66fef654e2d
Hash 05: 978694c66095697ce240c15971fdb356
Hash 06: 2a9749c68aaf27cfda6aa97484c4a79e
Hash 07: ae11e7d4368961f9fc2bb66fef654e2d
Hash 08: c464eb14eb60b4baaa5280687239321c
Hash 09: c464eb14eb60b4baaa5280687239321c
Hash 10: acc40afb4351d3135edf2a71b92351c7
Hash 11: efee4f60cdcb2a40566087f5e0fa8ee6
Hash 12: c464eb14eb60b4baaa5280687239321c
Hash 13: 4da2e66a296a8dc21d47edf3bad7abf9
Hash 14: efee4f60cdcb2a40566087f5e0fa8ee6
Hash 15: e3328603e58cf7961a53dd27efe1c20b
Hash 16: e3328603e58cf7961a53dd27efe1c20b
Hash 17: e06cb56b285eaadacc4b4ba2bc595df0
Hash 18: 8e7f6e22b5b66ff392e22f6241bb4ced
Hash 19: 9455da78d7269b2696a0e1603745e63d
Hash 20: 8a35d037b70e83ab54a06d7dcc005087
Hash 21: 847d95a8fb22a078ab0c57adf9008cd7
Hash 22: 847d95a8fb22a078ab0c57adf9008cd7
Hash 23: 5c5fcc294dde0724bb419185cab1abe2
Hash 24: ac74d2192821b285928c9299292e2206
Hash 25: ac74d2192821b285928c9299292e2206
Hash 26: 02930e172db9bb1801324ec0557c1c5b
Hash 27: ebf8f53349ad8f756ad81aa5b714cc6e
Hash 28: 4ba57f5456aaa6e9fe2528ed2509d1fe
Hash 29: 72ad827e33c280b7c78c0c75e4c2735a
Key Credentials:
Credential Roaming

Created:
Modified:
Credentials: