Defense Against the Dark Arts

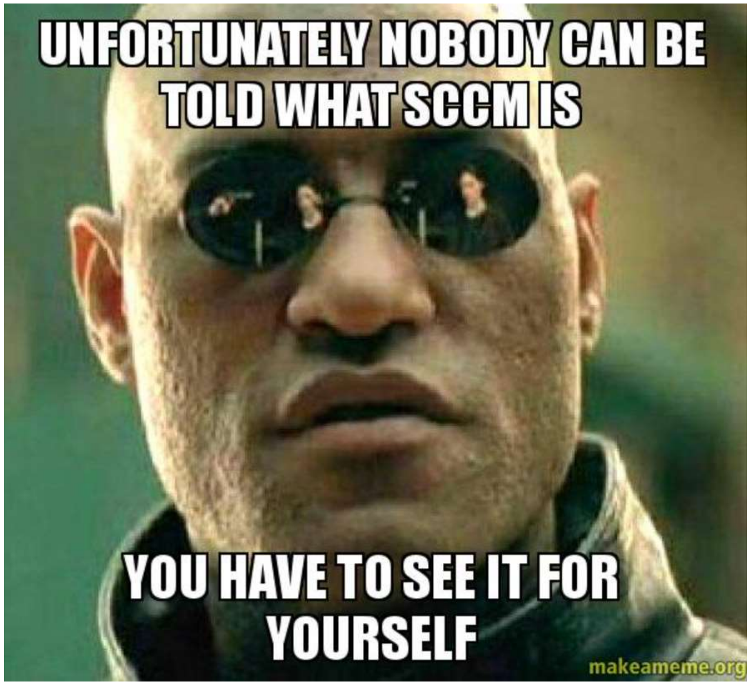
Stealing SCCM Credentials and Impersonating Servers

Chris Thompson (@_Mayyhem)

What is SCCM?

Command and Control for Administrators

- Microsoft Configuration Manager, formerly System Center Configuration Manager
- Enables wide-scale deployment of applications, software updates, operating systems, and compliance settings
- Allows real-time management of servers, desktops, and laptops
- Intended for **on-premises endpoint management**, whereas Intune is Microsoft's solution for cloud-based endpoint management


UNFORTUNATELY NOBODY CAN BE TOLD WHAT SCCM IS
YOU HAVE TO SEE IT FOR YOURSELF
makeameme.org

As an attacker/defender, why should I care?

Decades of Tech Debt

- SCCM is **used by the majority of organizations** that use Windows workstations, so you're very likely to encounter it
- The client software runs with SYSTEM privileges
- Often used to manage clients in separate Active Directory forests and segmented networks, **crossing security boundaries**
- It is **commonly misconfigured** due to some interesting default settings, community advice, and design issues that can allow an attacker to gain administrative control of SCCM and every client device
  - Allows domain dominance if DCs or admin workstations are clients

Terms and Definitions

SCCM Fundamentals

- **Hierarchy**
  - One instance of SCCM, consisting of one or more sites
  - This is the security boundary in ConfigMgr
- **Site**
  - An environment that provides services to a scope of client devices
  - Identified by a three-character site code (e.g., PS1)
- **Client/Device**
  - The systems that are joined to, managed by, and receive content from an SCCM primary site through installation of the SCCM client software (think C2 agent)

Terms and Definitions

SCCM Fundamentals

- **Primary Site**
  - A site that clients can be assigned to and that is administered using the Configuration Manager console software
- **Primary Site Server**
  - The system that handles processing of all client data in a primary site
  - Also referred to as just the “site server”
- **Site Database Server**
  - The server(s) that hosts the database where client and server data is stored for the primary site

Terms and Definitions

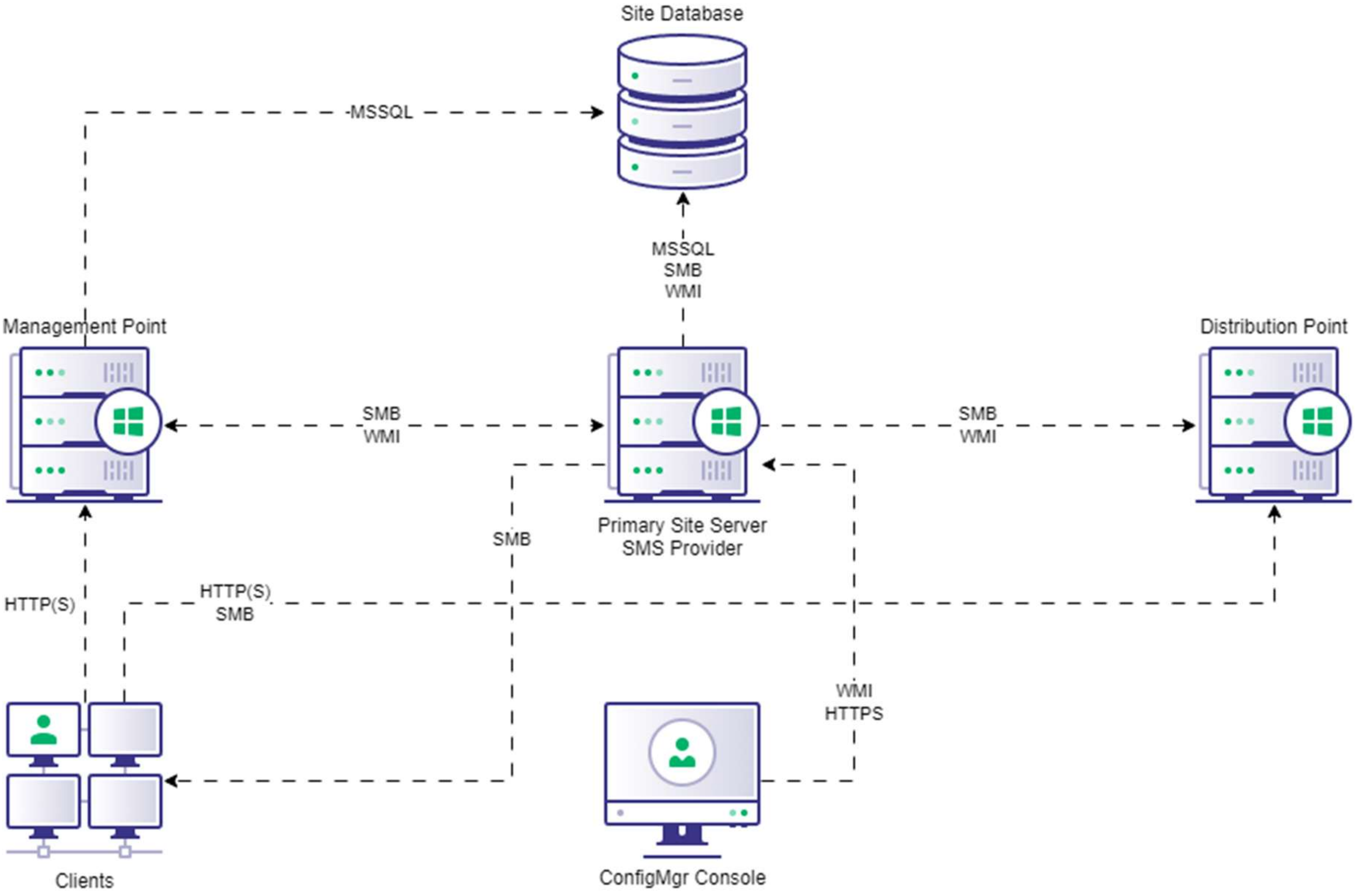
Site System Roles

- **Management Point**
    - Receives client HTTP(S) communications
        - Status and inventory messages
    - Relays client configuration data to the site server
    - Responds to client requests for policy and content locations
    - May be installed on the site server or on a separate Windows server

Terms and Definitions

Site System Roles

- **Distribution Point**
  - Receives and responds to client requests for content
    - Applications, software packages, scripts, etc.
  - Supports HTTP(S) and SMB
  - Clients download software from distribution points


Site Database
-MSSQL
MSSQL
SMB
WMI
Management Point
Distribution Point
SMB
WMI
SMB
WMI
Primary Site Server
SMS Provider
SMB
HTTP(S)
HTTP(S)
SMB
WMI
HTTPS
Clients
ConfigMgr Console

SCCM has *many* accounts…

Many accounts are used for many things, most are abusable…

Client Push Installation

- Used to install the client software on computers
- Must be admin on every target computer
- Results in many overprivileged scenarios

Network Access

- Used to retrieve software from DPs
- (Sometimes) optional but still wide-spread
- Stored on clients (DPAPI) and transmitted via computer policy (obfuscated, not encrypted)

Task Sequence

Various accounts:

- Domain join account
- RunAs account
- Network folder connection account
- Collection variables

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

Network Access Accounts

What are they and why do they exist?

- Domain account used to retrieve software from distribution points (DP)
- (Mostly) optional, required for specific actions / scenarios
- Requires minimal privileges: read the network share on the DP

The Worst (and Most Common) Misconfiguration

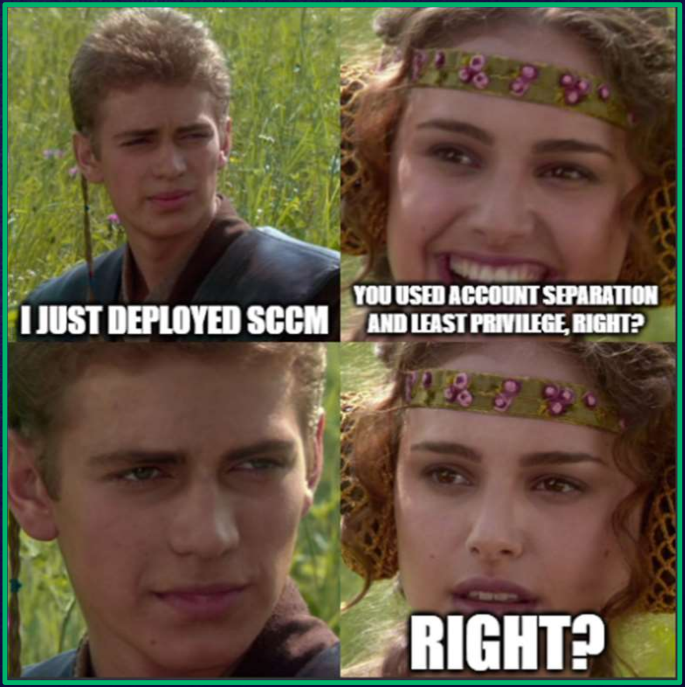
Overprivileged Network Access Accounts

- Included in computer policy sent to all clients
- Policy can be requested with control of a computer object
- Credentials are obfuscated on the wire (no encryption)
- Protected by DPAPI on the client, recoverable as admin

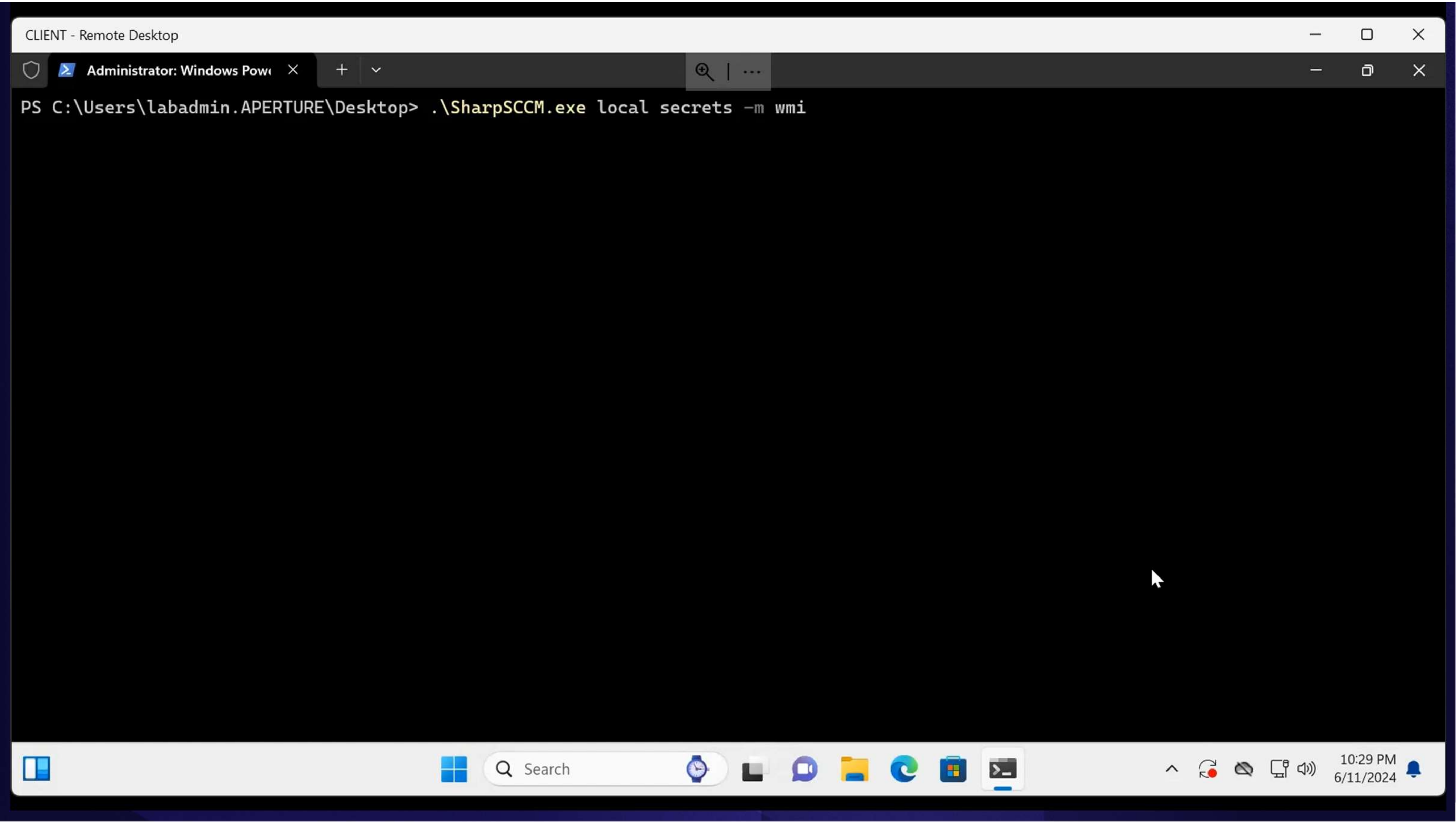
The Worst (and Most Common) Misconfiguration

Overprivileged Network Access Accounts

- Due to so many different accounts, the same god-mode account is often used
- E.g., Domain Admin, SCCM Admin, client push installation (local admin on all clients)
- **We find this *All. The. Time.***
- Creds may persist beyond account rotation



Demo: Dump Secrets



```
PS C:\Users\labadmin.APERTURE\Desktop> .\SharpSCCM.exe local secrets -m wmi
```

Hierarchy Takeover

Assuming full control of all systems in the SCCM hierarchy

How can attackers take over a hierarchy?

- Obtain the **Full Administrator** role in **ANY** site
- The site database is replicated to all sites
- Own one primary site, *own them all*

NTLM Relay Primer

Connecting the dots

If an account authenticates (NTLM) to an attacker-controlled machine, the attacker can forward the authentication to another system to access it using the relayed account's privileges

- E.g., to launch a C2 agent, add a user account, modify permissions/configurations, etc.

Several bugs that Microsoft won't fix can be abused to force a computer to authenticate to an arbitrary IP address using NTLM (a.k.a. coercion)

- Printerbug
- PetitPotam

Hierarchy Takeover

Key concepts

- The primary site server's domain computer account ***must*** be:
  - Local admin on the site database server
  - Sysadmin on the site database
  - Local admin on every other site system role

If we can ***coerce authentication from this account*** and relay the authentication to certain SCCM servers, we ***gain control of SCCM.***

SCCM Hierarchy Takeover Attack Paths

Because "Hierarchy takeover via NTLM coercion and relay to MSSQL on remote site database" does not roll off the tongue…

TAKEOVER-1

NTLM coercion and relay to MSSQL on remote site database

TAKEOVER-2

NTLM coercion and relay to SMB on remote site database

TAKEOVER-3

NTLM coercion and relay to HTTP on ADCS

TAKEOVER-4

NTLM coercion and relay from CAS to origin primary site server

TAKEOVER-5

NTLM coercion and relay to AdminService on remote SMS Provider

TAKEOVER-6

NTLM coercion and relay to SMB on remote SMS Provider

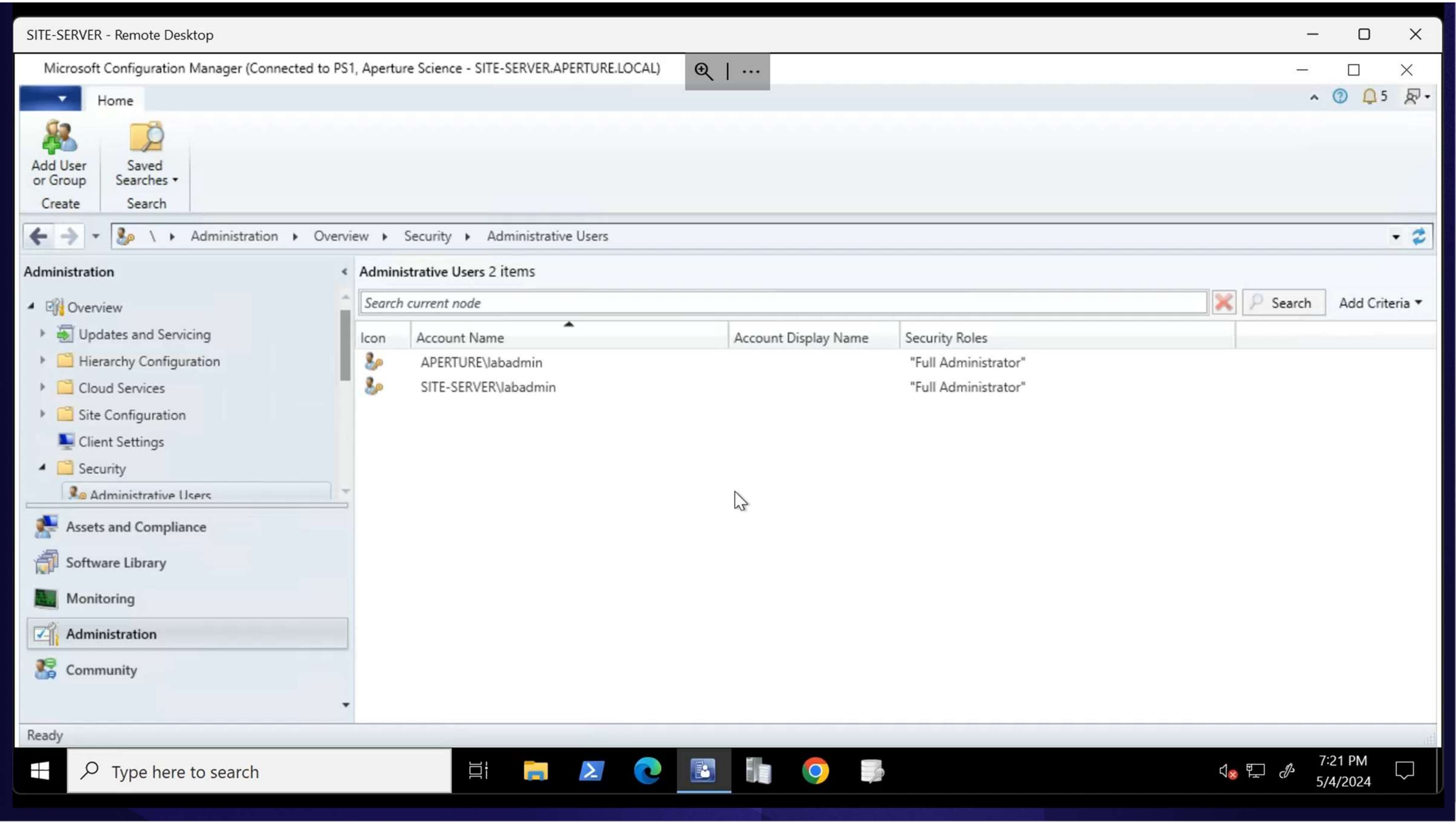
TAKEOVER-7

NTLM coercion and relay to SMB between primary and passive site servers

TAKEOVER-8

NTLM coercion and relay HTTP to LDAP on domain controller

Demo: TAKEOVER-1



Administrative Users 2 items

Icon	Account Name	Account Display Name	Security Roles
	APERTURE\labadmin		"Full Administrator"
	SITE-SERVER\labadmin		"Full Administrator"

Mitigation Guidance - Hierarchy Takeover

Prevent successful relay of coerced NTLM authentication:

- Require Extended Protection on the site database MSSQL service and on AD CS servers
- Require SMB signing on site servers, site database servers, and SMS Providers
- Require LDAP signing and channel binding on domain controllers
- Block MSSQL and SMB connections from unnecessary systems to site servers
- Do not enable WebClient on site servers

https://github.com/subat0mik/Misconfiguration-Manager/blob/main/defense-techniques/_defense-techniques-list.md

Detectable Events - Hierarchy Takeover

- Monitor for suspicious activity on site systems and using site accounts
  - Site server domain computer accounts or client push installation accounts authenticating from an IP address that isn't their static IP

https://github.com/Mayyhem/SharpSCCM/wiki#defensive-recommendations

Misconfiguration Manager

Helping you manage SCCM attack paths

- Living knowledge-base that aims to ease SCCM attack path management
- Contains foundational, offensive, and defensive write-ups for most known techniques
- Introduces a taxonomy to simplify and demystify concepts (à la Certified Pre-Owned)
- Based on MITRE ATT&CK and inspired by the SaaS Attacks Matrix

https://github.com/pushsecurity/saas-attacks
https://attack.mitre.org/

Misconfiguration Manager

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration
PXE Credentials	App Deployment	App Deployment	Relay to Site Server SMB	App Deployment	PXE Credentials	LDAP Enumeration	App Deployment	CMPivot		CMPivot
	Script Deployment	Script Deployment	Relay Client Push Installation	Script Deployment	Policy Request Credentials	SMB Enumeration	Script Deployment			
		ADCS Relay	Relay to DB MSSQL		DPAPI Credentials	HTTP Enumeration	Relay to Site Server SMB			
		LDAP Relay	Relay to DB SMB		Legacy Credentials	CMPivot	Relay Client Push Installation			
			Relay to ADCS				Relay to DB MSSQL			
			Relay to AdminService		Site Database Credentials		Relay to DB SMB			
			Relay CAS to Child				Relay CAS to Child			
			Relay to SMS Provider SMB				Relay to AdminService			
			Relay between HA				Relay to SMS Provider SMB			

https://misconfigurationmanager.com

Misconfiguration Manager Taxonomy

Because "Hierarchy takeover via NTLM coercion and relay to MSSQL on remote site database" does not roll off the tongue…

CRED

1. Retrieve credentials from PXE boot media
2. Deobfuscate computer policy
3. Decrypt via DPAPI
4. Legacy credentials (DPAPI)
5. SC_UserAccount on Site DB

ELEVATE

1. SMB relay on site server
2. Automatic client push NTLM relay

EXEC

1. Application deployment
2. Script deployment

RECON

1. LDAP Enumeration
2. SMB Enumeration
3. HTTP(S) Enumeration
4. CMPivot

SCCM Mitigation and Detection Guidance

You didn't think we'd leave you hanging, did you?

PREVENT

Currently 23 SCCM and AD configuration changes to mitigate the attack techniques covered

DETECT

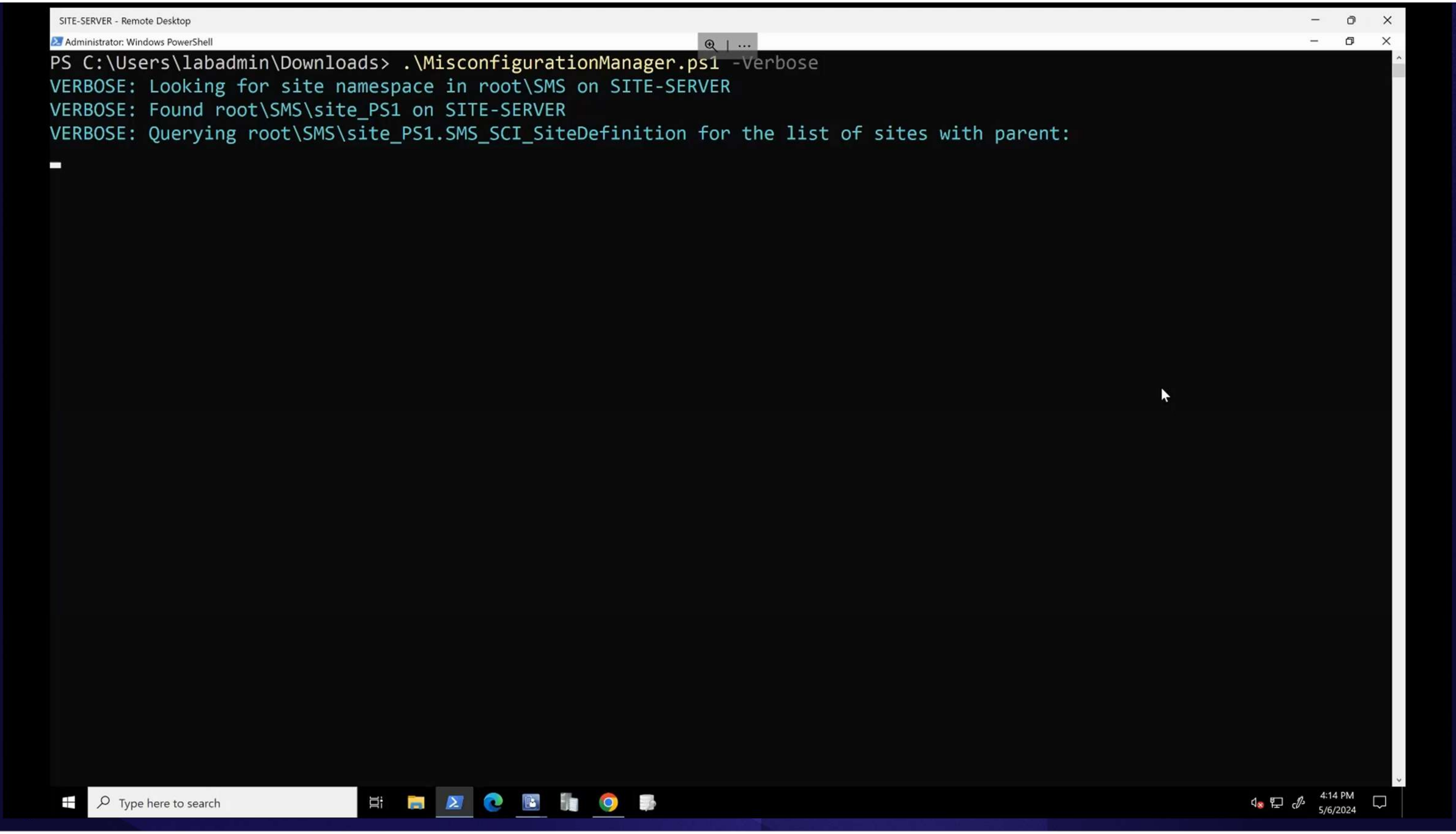
Strategies to detect SCCM attack techniques and attack paths

CANARY

Deception techniques that take advantage of SCCM misconfigurations

https://misconfigurationmanager.com

Demo: Misconfiguration Manager



SITE-SERVER - Remote Desktop
Administrator: Windows PowerShell
Type here to search
4:14 PM
5/6/2024

```
PS C:\Users\labadmin\Downloads> .\MisconfigurationManager.ps1 -Verbose
VERBOSE: Looking for site namespace in root\SMS on SITE-SERVER
VERBOSE: Found root\SMS\site_PS1 on SITE-SERVER
VERBOSE: Querying root\SMS\site_PS1.SMS_SCI_SiteDefinition for the list of sites with parent:
```

Questions?