SPECTEROPS | TROOPERS

Misconfiguration Manager

Still Overlooked, Still Overprivileged

Duane Michael & Garrett Foster
SpecterOps

Scan to download this slide deck

Duane Michael

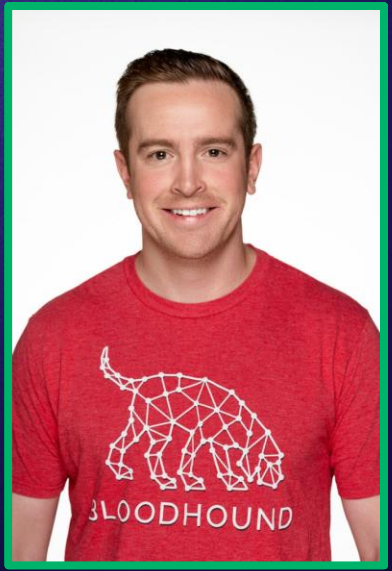
- Managing Consultant, Adversary Simulation at SpecterOps
- Contributor to SharpSCCM
- @subat0mik on all the things

Garrett Foster

- Senior Security Researcher at SpecterOps
- Primary author of SCCMHunter
- X: @unsigned_sh0rt

Chris Thompson

- Senior Security Researcher at SpecterOps
- Primary author of SharpSCCM and Maestro
- X: @_Mayyhem



Agenda

What this talk is (and is not) about

✓ **This presentation covers:**

- 2024 Summary
- 1 Year of MM
- New Technique Highlights
- Community Contributions
- Q&A

✗ **This presentation does NOT cover:**

- Walkthroughs of *all* offensive techniques
- Defensive and remediation walkthroughs
- Comprehensive treatment of topics discussed

Misconfiguration Manager

Where we started

- What is Misconfiguration Manager
  - Released at SO-CON & TROOPERS 24
  - Captures all known adversary tradecraft targeting SCCM
  - Provides detection and mitigation guidance
  - MisconfigurationManager.ps1

Misconfiguration Manager

Where we started…

- The initial release contained:
    - 9 TAKEOVERs
    - 5 RECONs
    - 5 CREDs
    - 3 ELEVATEs
    - 2 EXECs
    - 22 PREVENTs
    - 5 DETECTs
    - 1 CANARY

Misconfiguration Manager

Where we are now…

- Over the past year, with the help of the community, we've added:

  - 1 TAKEOVER
  - 2 RECONs
  - 3 CREDs
  - 2 ELEVATEs
  - 3 EXECs
  - New COERCE category
  - 3 COERCEs
  - 6 DETECTS

What we (and the community) have been up to…

TAKEOVER-1 Recap

Our favorite, and most common, TAKEOVER primitive

- Site database is not hosted on the coercion target
- Primary site servers and SMS Providers are "db_owner" on site DB
- Coerce a system with one of these roles
- Relay it to site DB
- Grant SCCM "Full Administrator" by modifying "RBAC_Admins" table

The Problem with TAKEOVER-1

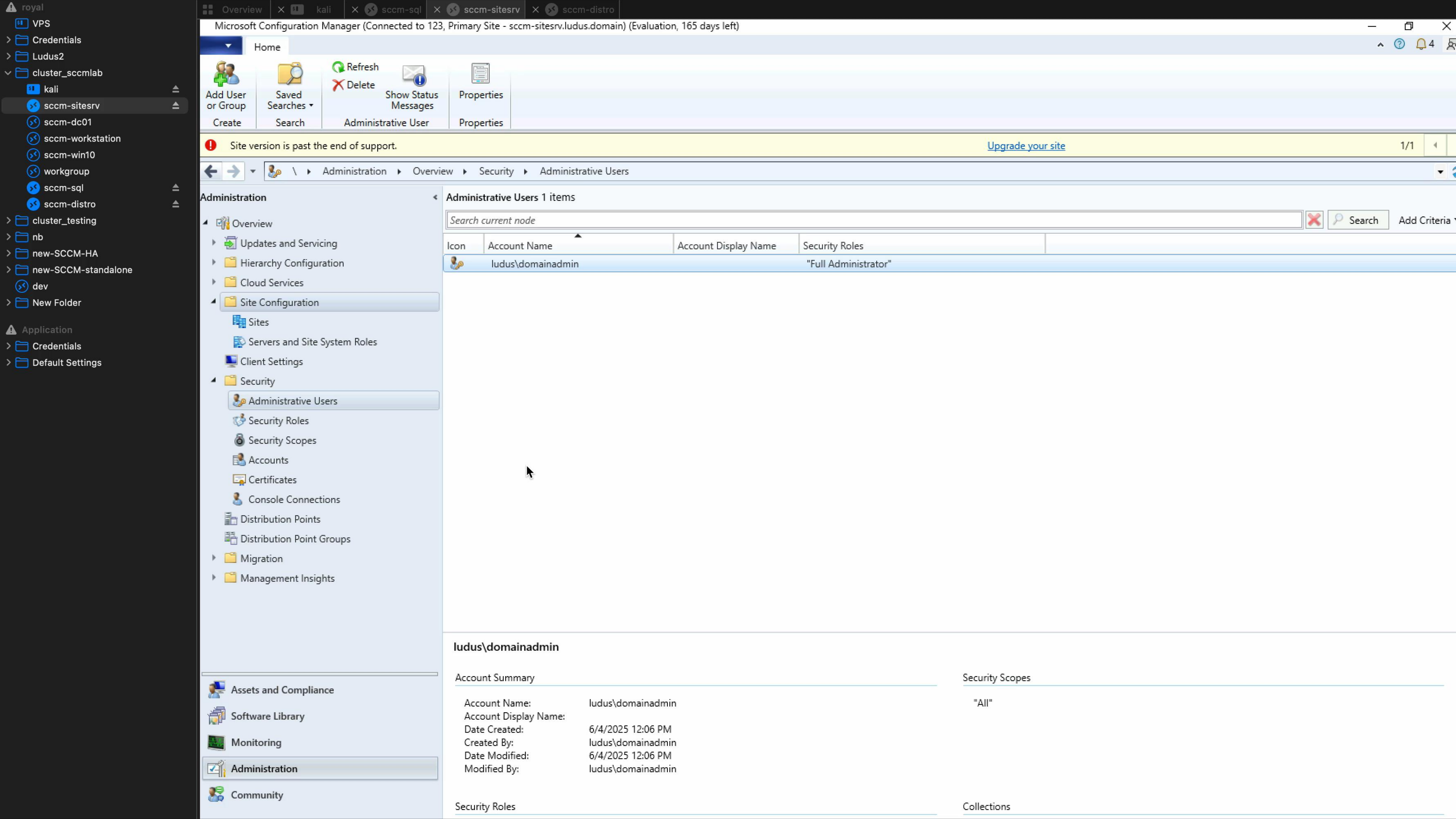
There was one glaring issue…

- When found, TAKEOVER-1 allows a privilege escalation from *Domain Users* to site/hierarchy compromise
- But… we couldn't reliably enumerate standalone site DBs
- We relied on SPNs and hostnames
    - *MSSQL/SQLSCCM01.CORP.LOCAL:1433*

RECON-6

The solution to our problem

- Primary site servers and distribution points create reg keys
  - *HKLM\SOFTWARE\MICROSOFT\SMS\**
- World-readable over WINREG, regardless of DACL
  - Key path set in local security policy on PSS and DP
- Keys contain site system information
- Weaponized in pssrecon
- *Discovered, weaponized, and contributed by Dylan Bradley (@slygoo)*



Microsoft Configuration Manager (Connected to 123, Primary Site - sccm-sitesrv.ludus.domain) (Evaluation, 165 days left)

Site version is past the end of support.

Administrative Users 1 items

Icon	Account Name	Account Display Name	Security Roles
	ludus\domainadmin		"Full Administrator"

ludus\domainadmin

Account Summary

Account Name:	ludus\domainadmin
Account Display Name:	
Date Created:	6/4/2025 12:06 PM
Created By:	ludus\domainadmin
Date Modified:	6/4/2025 12:06 PM
Modified By:	ludus\domainadmin

Security Scopes

"All"

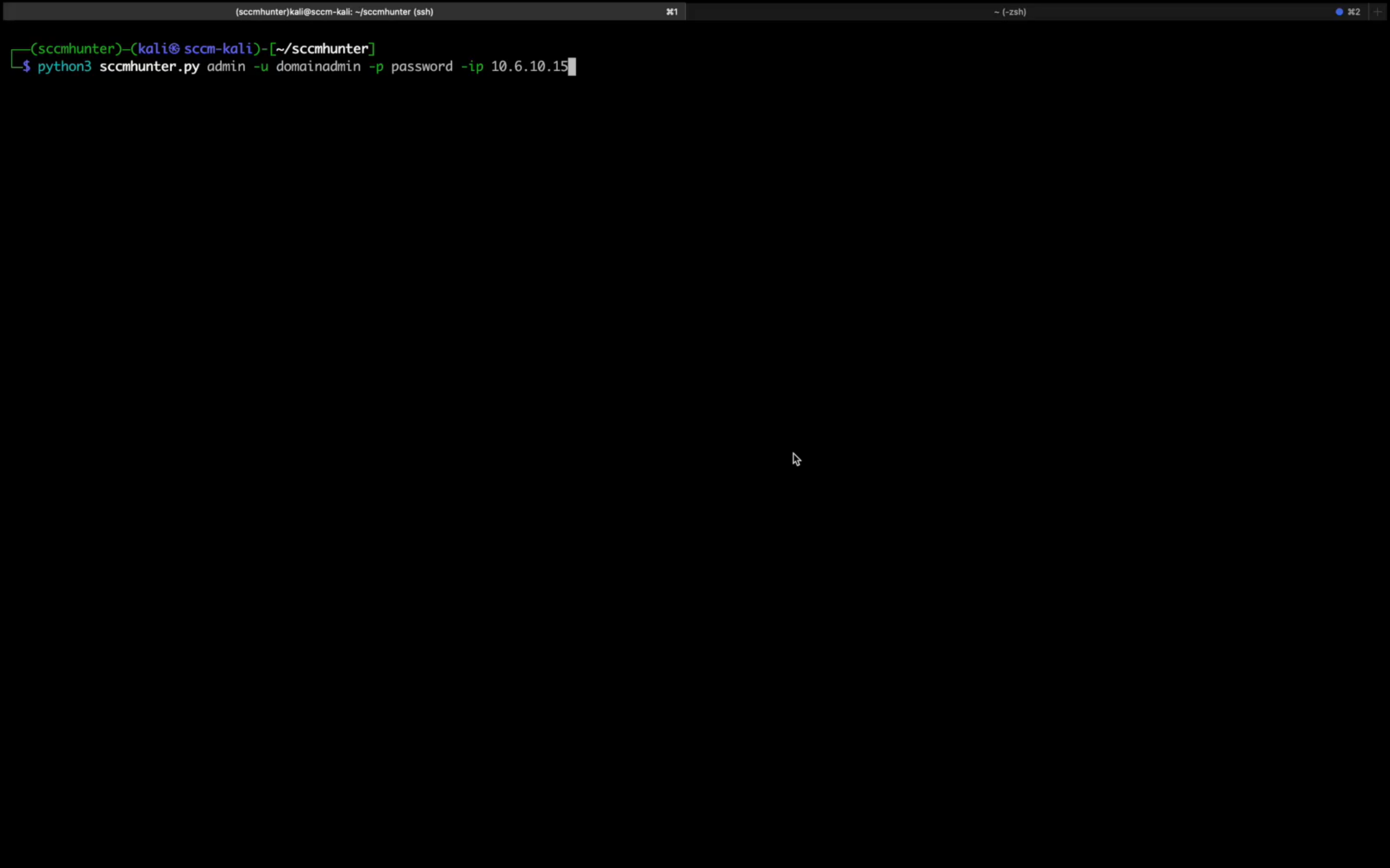
Security Roles

Collections

Time to Talk About Creds…

Again…

- There's more creds than we thought…
  - *Azure Application (Co-management), Discovery Accounts, Site-Installation Accounts, and more*
- All cred blobs retrievable via AdminService API and WMI (CRED-7 & 8)
  - CRED-7 weaponized by Garrett



```
┌──(sccmhunter)─(kali㉿ sccm-kali)-[~/sccmhunter]
└─$ python3 sccmhunter.py admin -u domainadmin -p password -ip 10.6.10.15
```

CRED-1 is More Practical

With the help of a little bit of PXE dust…

- CRED-1 can now be abused over SOCKS via C2
  - Previously required direct network access
  - Weaponized by Adam Chester in cred1py

Config Manager Remote Control

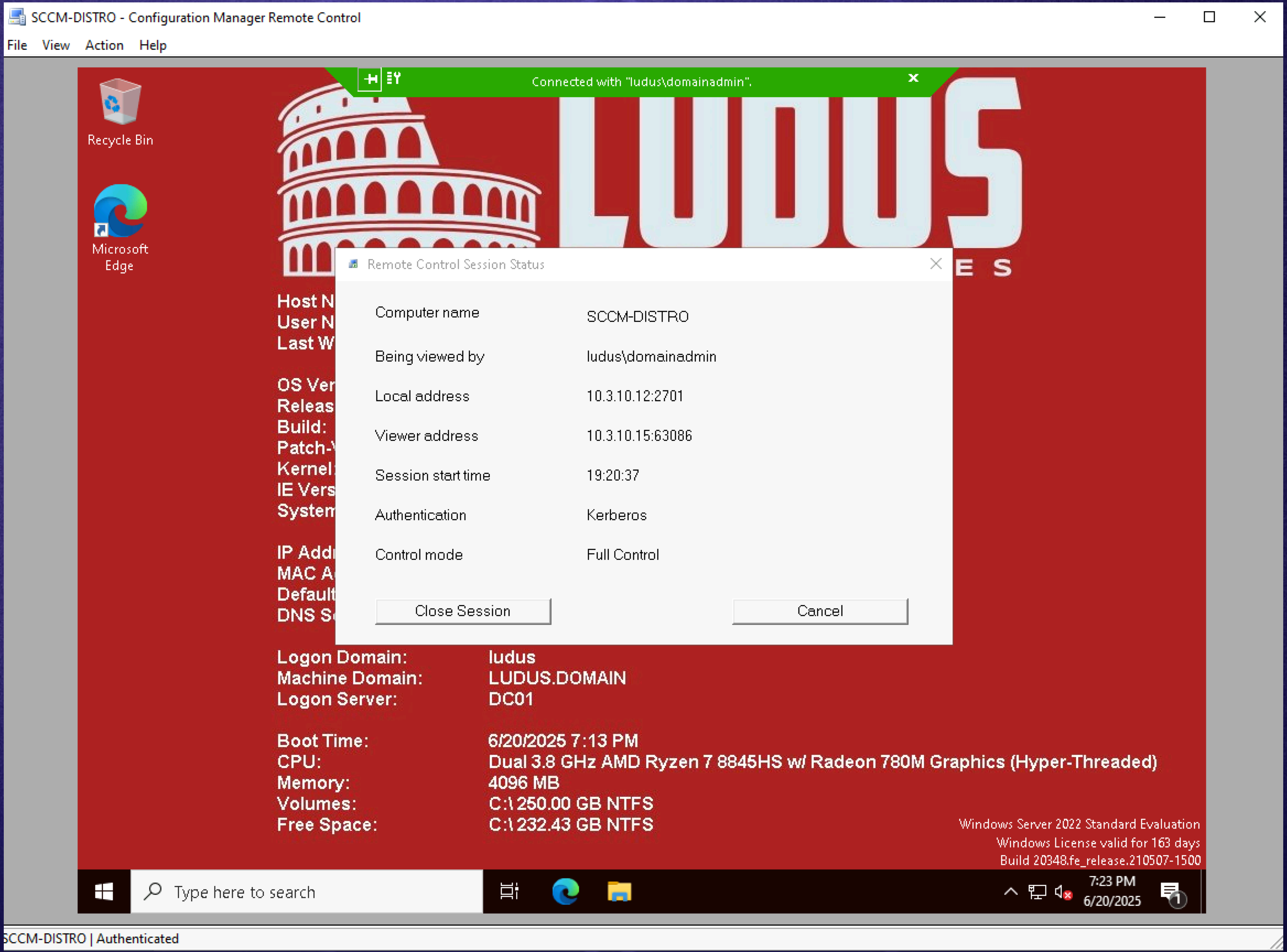
Overview

- ConfigMgr Remote Control
  - Allows admins to RDP to clients or shoulder surf users
  - Viable as a standalone tool, only requires admin on target
  - Settings controllable by local admin of target or SCCM Admin
  - Invisible to target users
  - Shared clipboard

Post-Exploitation with CmRc

Or, How to Give Someone a Heart Attack

- Viable as an execution technique a la VNC (EXEC-3)
- Requires local admin on target or SCCM admin
  - Blogged by Chris Au
- Also, a stealthy recon and credential access technique
  - Invisible to logged on users (shoulder surf)
  - Clipboard is shared
- *Allows taking over input and locking a user out while forcing them to watch you pillage!*



SCCM-DISTRO - Configuration Manager Remote Control

Connected with "ludus\domainadmin".

Remote Control Session Status

Computer name	SCCM-DISTRO
Being viewed by	ludus\domainadmin
Local address	10.3.10.12:2701
Viewer address	10.3.10.15:63086
Session start time	19:20:37
Authentication	Kerberos
Control mode	Full Control

Host N
User N
Last W

OS Ver
Releas
Build:
Patch-
Kernel
IE Vers
System

IP Addr
MAC A
Default
DNS S

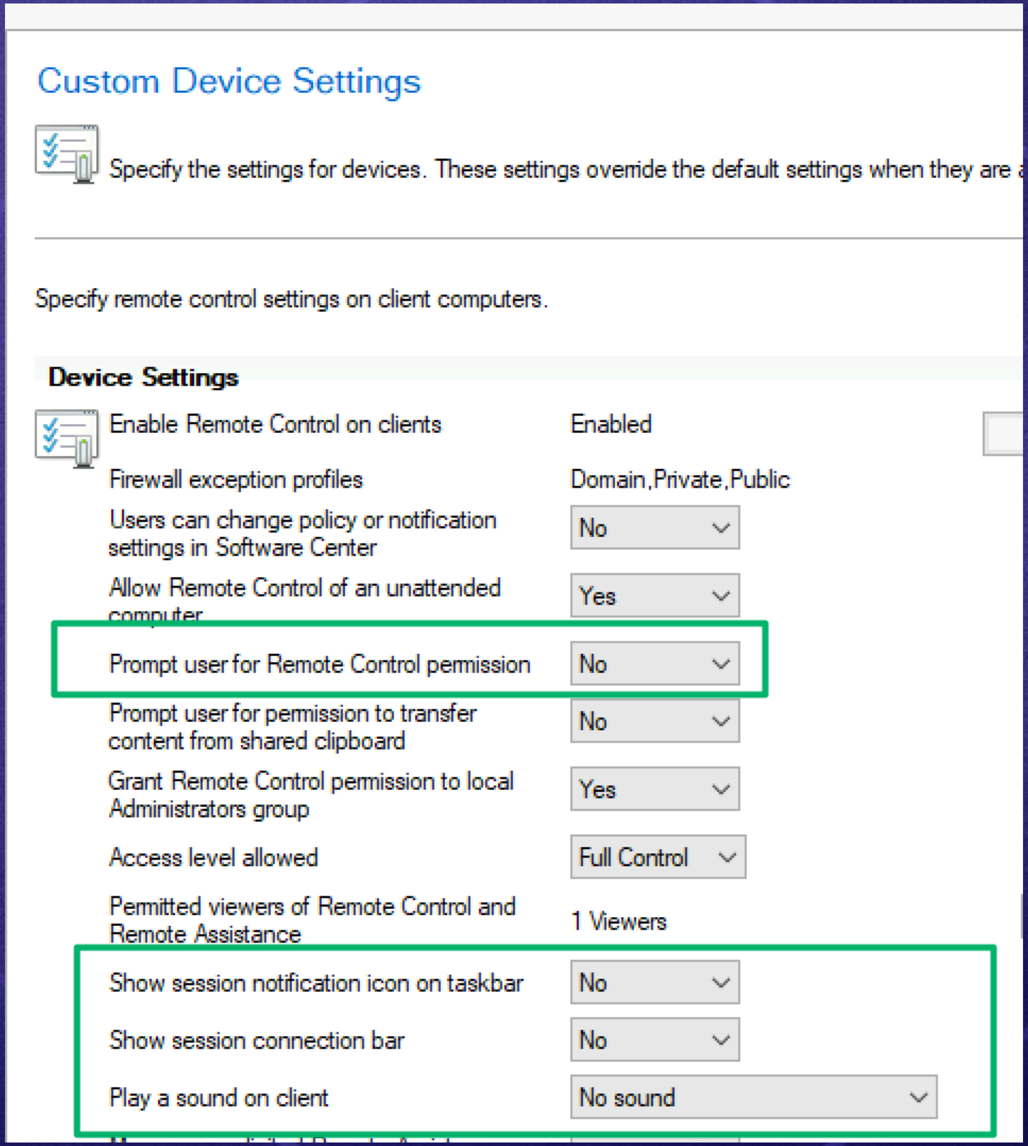
Logon Domain:	ludus
Machine Domain:	LUDUS.DOMAIN
Logon Server:	DC01
Boot Time:	6/20/2025 7:13 PM
CPU:	Dual 3.8 GHz AMD Ryzen 7 8845HS w/ Radeon 780M Graphics (Hyper-Threaded)
Memory:	4096 MB
Volumes:	C:\ 250.00 GB NTFS
Free Space:	C:\ 232.43 GB NTFS

Windows Server 2022 Standard Evaluation
Windows License valid for 163 days
Build 20348.fe_release.210507-1500

7:23 PM
6/20/2025

SCCM-DISTRO | Authenticated

TROOPERS



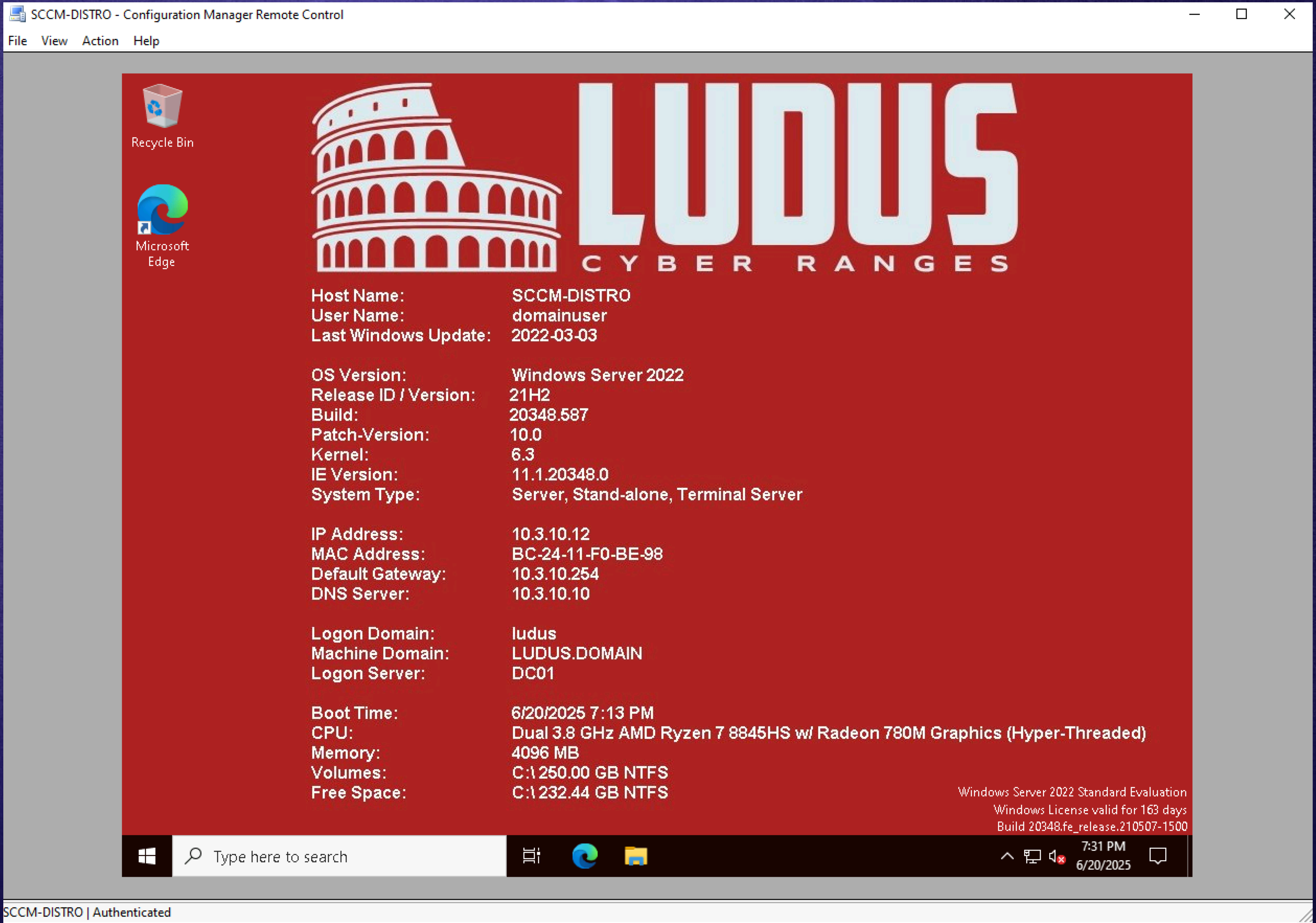
Custom Device Settings

Specify the settings for devices. These settings override the default settings when they are

Specify remote control settings on client computers.

Device Settings

Enable Remote Control on clients	Enabled
Firewall exception profiles	Domain,Private,Public
Users can change policy or notification settings in Software Center	No
Allow Remote Control of an unattended computer	Yes
Prompt user for Remote Control permission	No
Prompt user for permission to transfer content from shared clipboard	No
Grant Remote Control permission to local Administrators group	Yes
Access level allowed	Full Control
Permitted viewers of Remote Control and Remote Assistance	1 Viewers
Show session notification icon on taskbar	No
Show session connection bar	No
Play a sound on client	No sound



```
Host Name:              SCCM-DISTRO
User Name:              domainuser
Last Windows Update:    2022-03-03

OS Version:             Windows Server 2022
Release ID / Version:   21H2
Build:                  20348.587
Patch-Version:          10.0
Kernel:                 6.3
IE Version:             11.1.20348.0
System Type:            Server, Stand-alone, Terminal Server

IP Address:             10.3.10.12
MAC Address:            BC-24-11-F0-BE-98
Default Gateway:        10.3.10.254
DNS Server:             10.3.10.10

Logon Domain:           ludus
Machine Domain:         LUDUS.DOMAIN
Logon Server:           DC01

Boot Time:              6/20/2025 7:13 PM
CPU:                    Dual 3.8 GHz AMD Ryzen 7 8845HS w/ Radeon 780M Graphics (Hyper-Threaded)
Memory:                 4096 MB
Volumes:                C:\ 250.00 GB NTFS
Free Space:             C:\ 232.44 GB NTFS
```

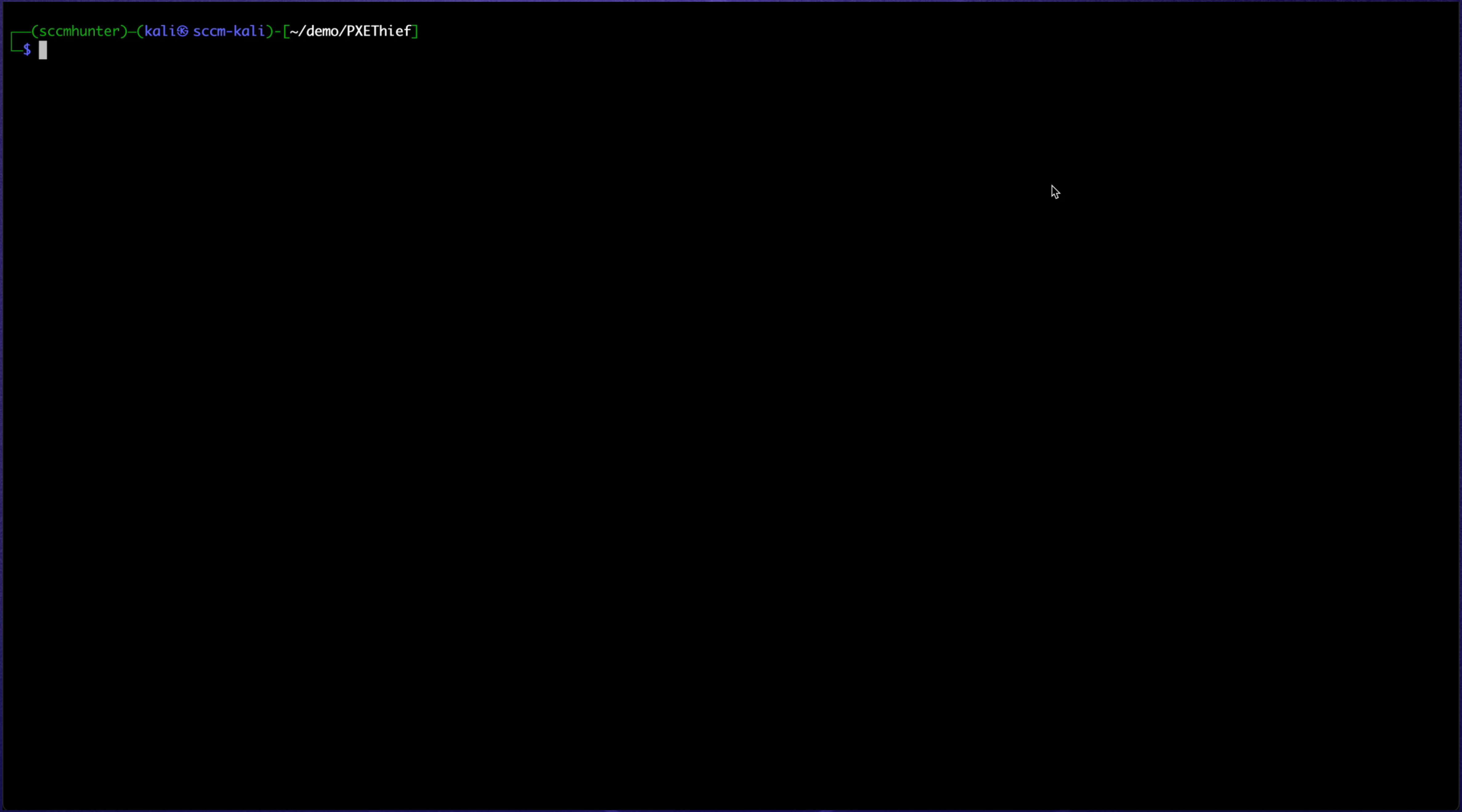
Windows Server 2022 Standard Evaluation
Windows License valid for 163 days
Build 20348.fe_release.210507-1500

ELEVATE-4

Pre-Owned PXE Boot

- SCCM PKI configurations require client authentication certs for OSD
  - Found by @onSec-fr
- The cert is distributed to every PXE client during deployment
- It’s a feature!*
  - "...only used during the OS deployment process."
  - "...use the same certificate for every OS deployment…"
- No PXE password = zero to hero
    - *Maybe even the site server…*

*https://learn.microsoft.com/en-us/intune/configmgr/core/plan-design/network/pki-certificate-requirements



```
┌──(sccmhunter)─(kali㉿sccm-kali)-[~/demo/PXEThief]
└─$ 
```

ELEVATE-5

Pre-Owned OSD Images

- Same PKI cert gets pushed into OSD images
- Images live on admin-selected distribution points as packages
  - Found with CRED-6
- Just need an authenticated user to retrieve images…
  - *But we've seen anonymous auth via HTTP…*

Community Contributions

Thank you to everyone who has contributed!

- Josh Prager – DETECT-5-8
- Diego Lomellini – RECON-4, COERCE-1
- Adam Chester – CRED-1 Update
- Alberto Rodriguez & Erik Hunstad – CRED-6
- Marshall Price – DETECT-4
- Dylan Bradley – RECON-6
- *And everyone that's furthering SCCM tradecraft research & discovery!*

Future Work

Where we're going…

- Microsoft is collaborating and taking this seriously!
- There is SO much more work to be done:
  - Offensive research
  - Detection strategies
  - Configuration guidance
- We want to hear your stories and ideas!
- Pull requests welcome and encouraged
- Collaborate with us in #sccm on BloodHound Slack
  - Invite link: https://ghst.ly/BHSlack

SPECTEROPS | TROOPERS

Thank you!

Chris Thompson | @_Mayyhem

Duane Michael | @subat0mik

Garrett Foster | @garrfoster

Scan to download this slide deck