Fooling The Hound

Deceiving Domain Admin Hunters

- Tom Sela -

> Whoami

TOM SELA

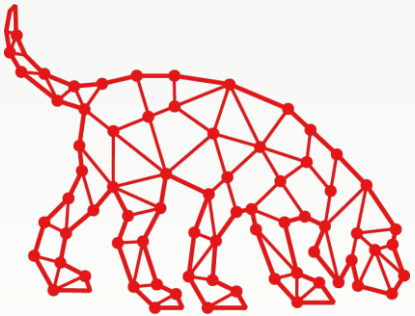
Security Researcher
tom@illusivenetworks.com
@4x6hw

> ls -l

Head Of Security Research at **“illusive networks”**

- Malware Research Team Leader in “Trusteer” (IBM Security)
- Telekom Innovation Labs - Ben-Gurion University

Acknowledge The Forefathers



@_wald0

@CptJesus

@harmj0y


Not
This
Hound

Agenda

1. Crash Course in Lateral Movement & Graphs

2. Deceptions

- Real world examples
- Deception techinques (x4) + Demos

3. Fooling the Hound

- Planting deceptions in the Lateral Movement Graph

4. Wrap Up \ Conclusions

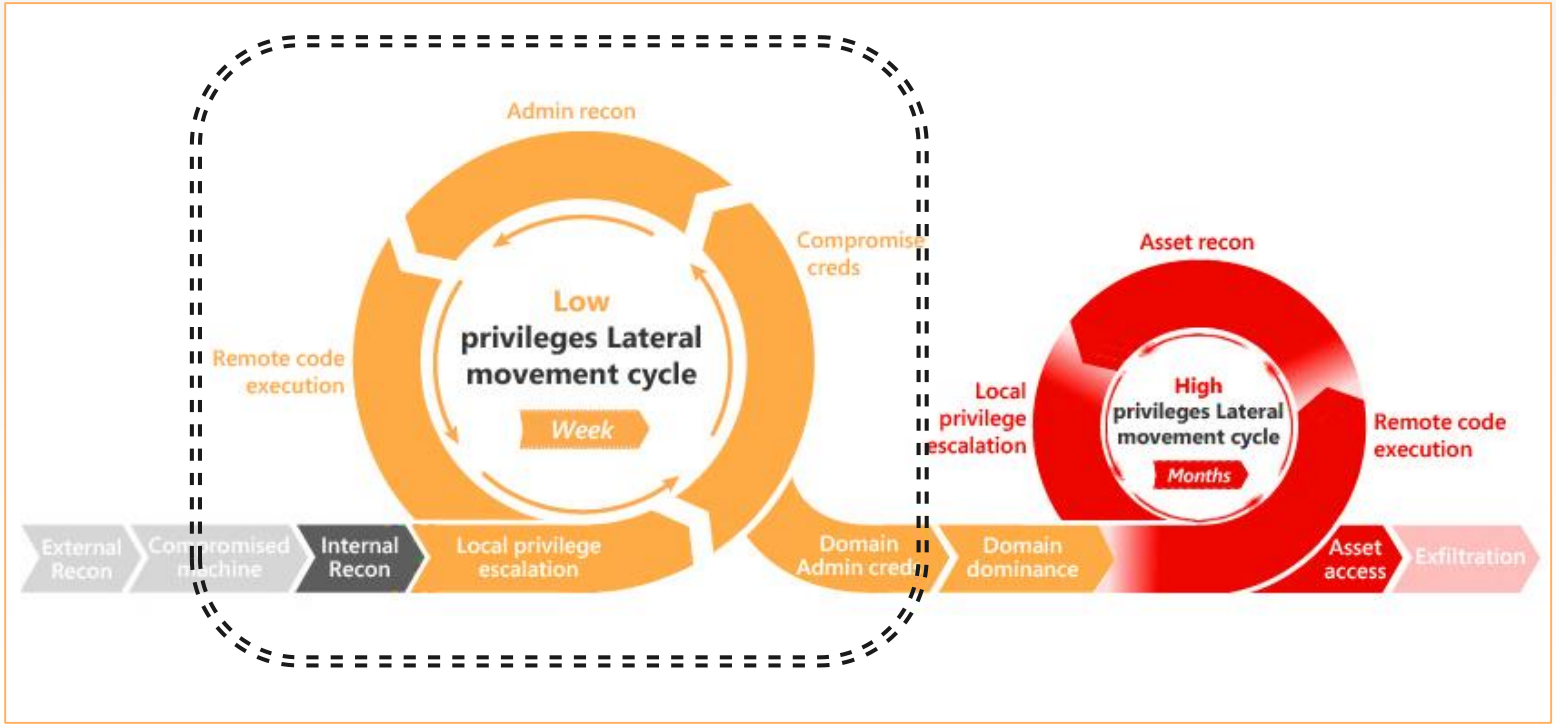
- Goal -

Detect Attackers Hunting Domain Admin Credentials

- Method -

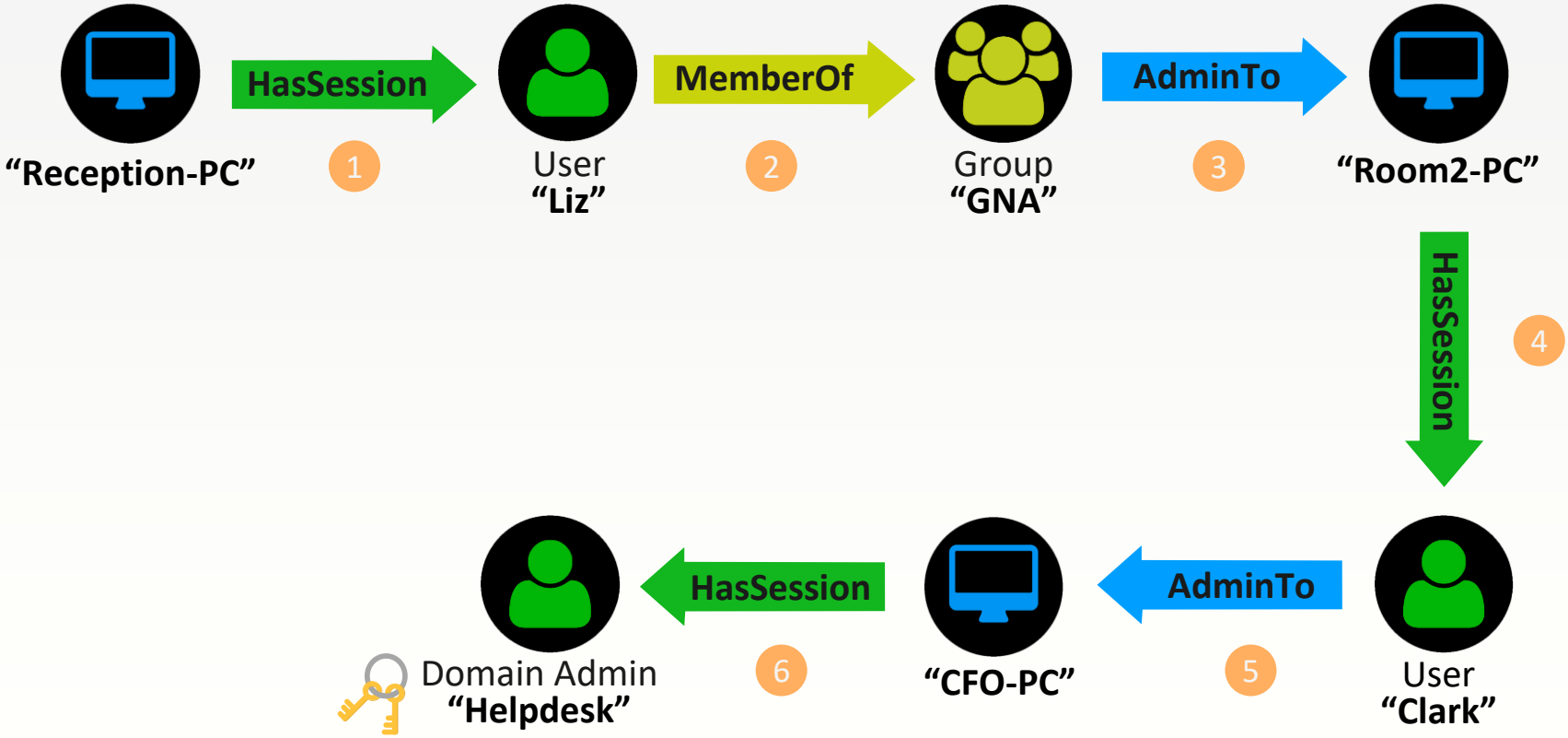
Plant and Monitor Deceptive Users and Computers

Attack Kill Chain



Credit: *Microsoft ATA*

From Breach to Complete Domain Control in 6 steps



Building a Lateral Movement Graph

Nodes

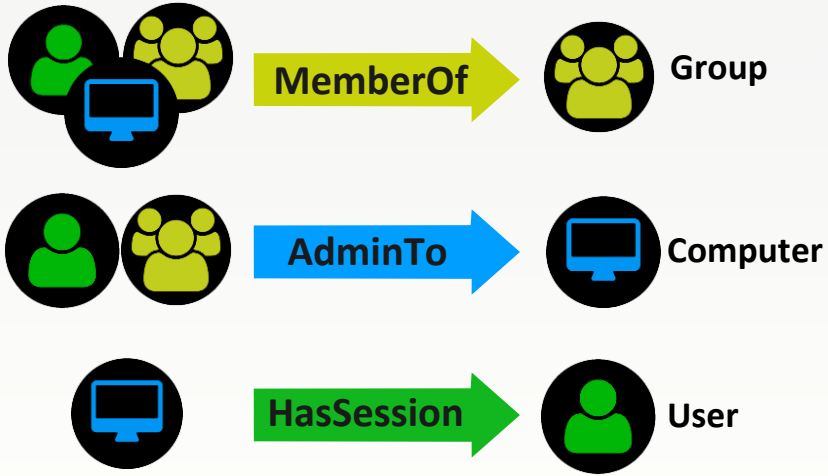
Edges

HasSession Who is logged in where?

AdminTo Who has admin rights where?

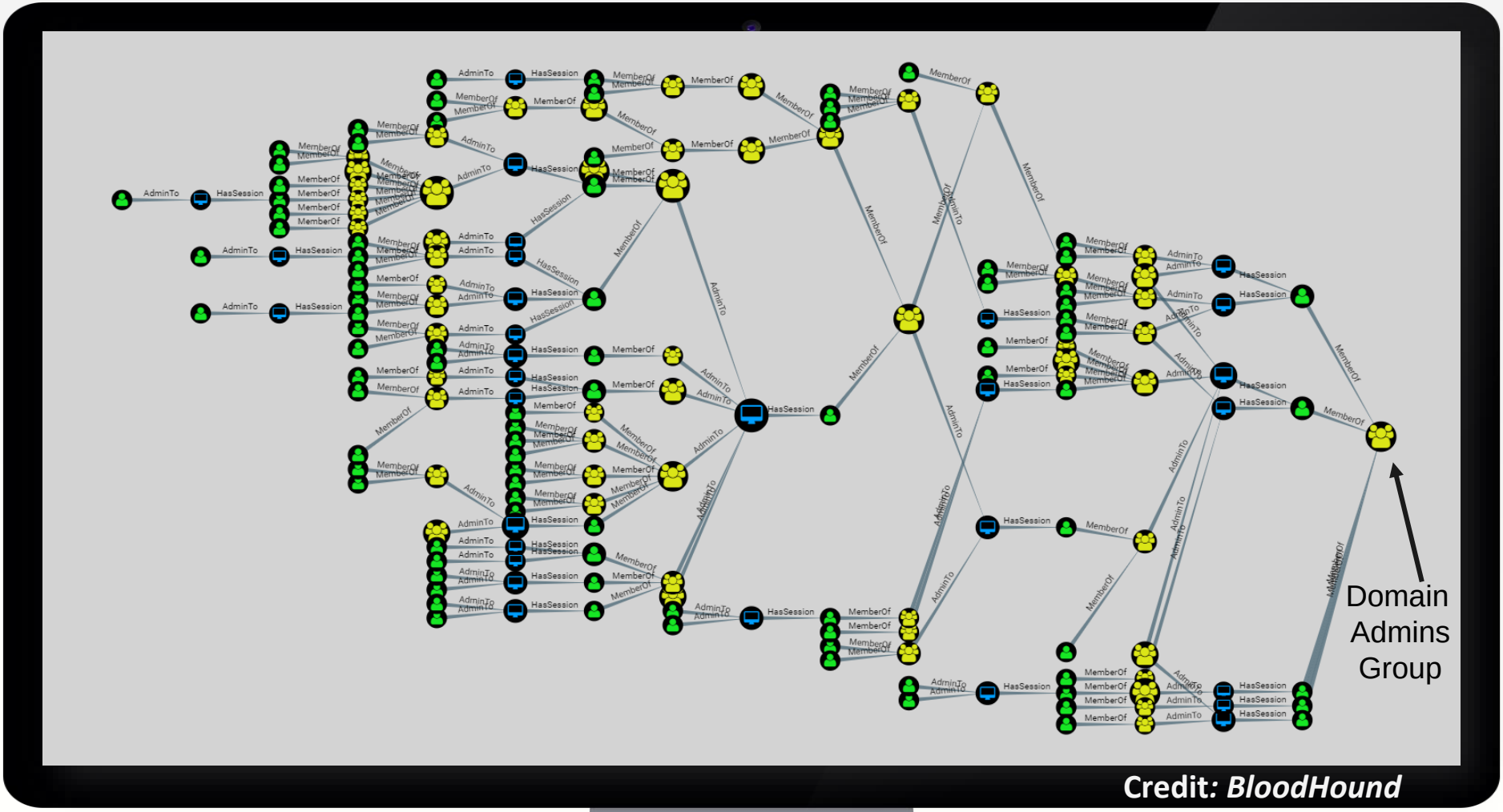
MemberOf Which users, groups and computers belong to which groups?

Connections



* No administrative privileges required

Credit: Six Degrees of Domain Admin - DEF CON 24


Domain Admins Group
Credit: BloodHound

Deception

“The act of causing someone to accept as true or valid what is false or invalid”

- Merriam-Webster’s Dictionary

Deceptions in Warfare

- Medieval Times-
Trip Stairs

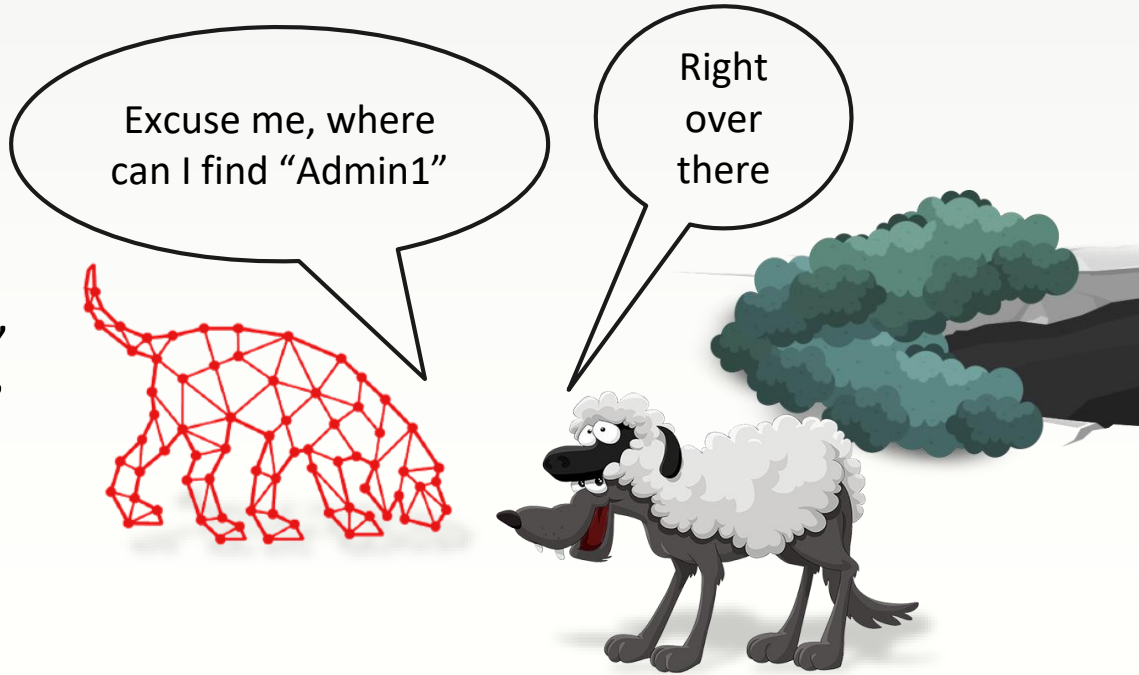
- WW2 -
Fake Tanks

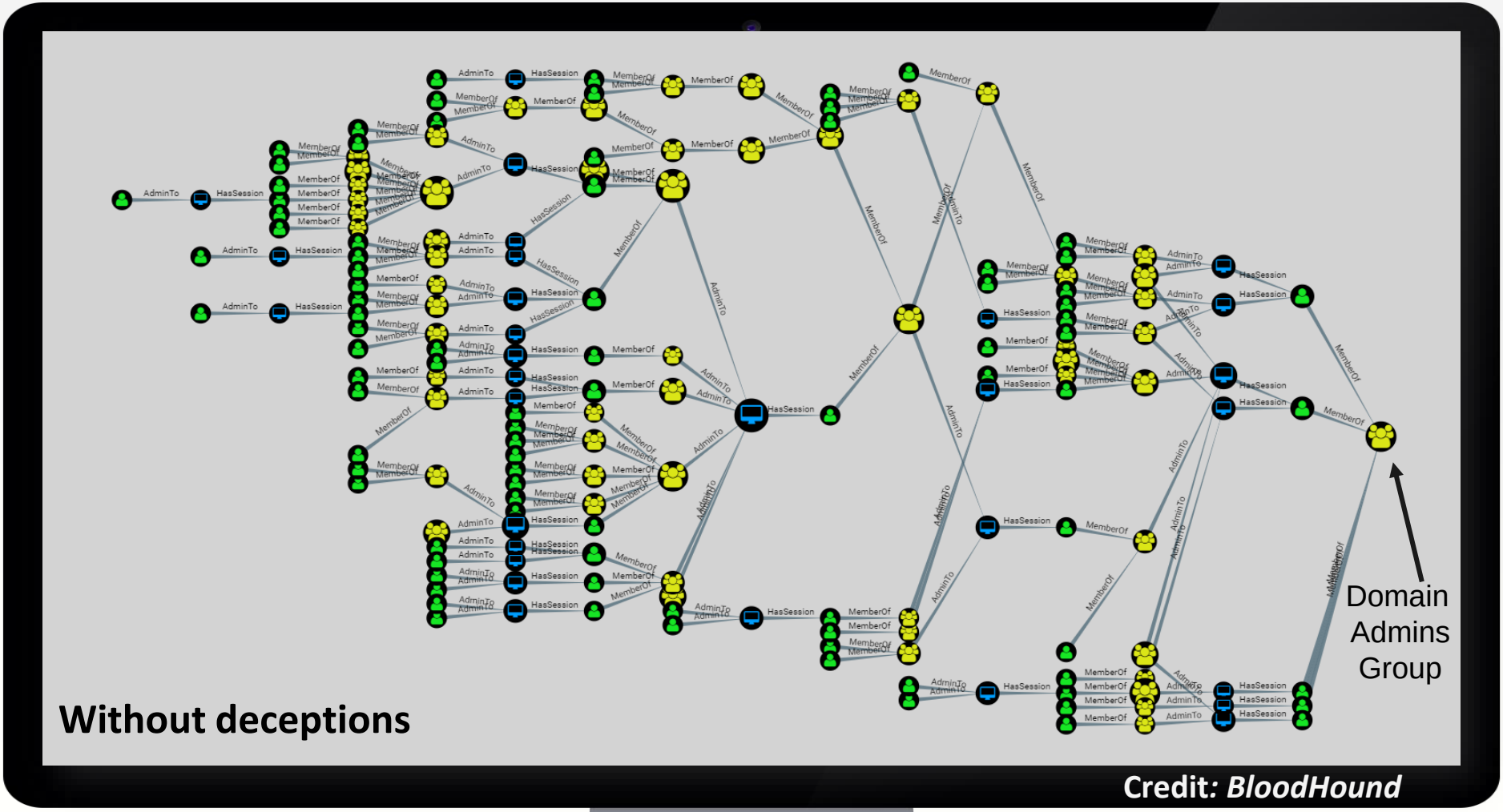
Take Control of the Attacker's Path With Deceptions

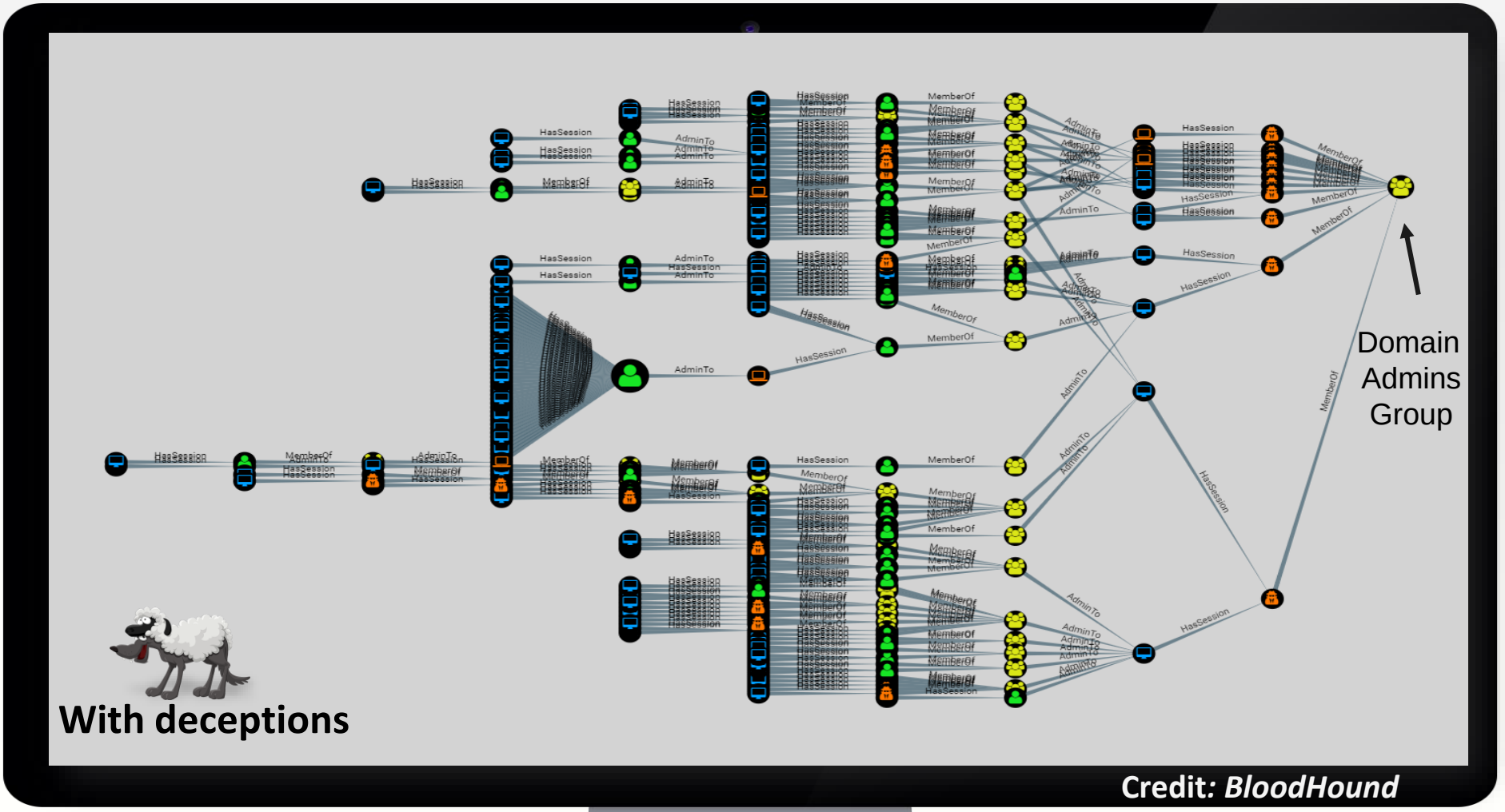
Bloodhound can produce a precise path to any target.

Using the same methods, defenders can predict where to look for attackers.

Even better, using deceptions, defenders can make attackers go where defenders want them to go.

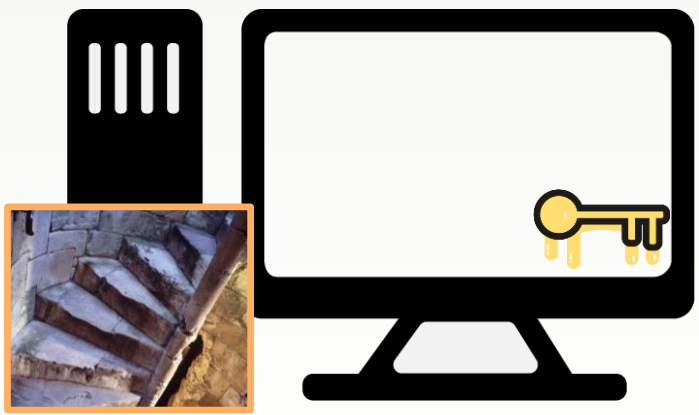



Domain Admins Group
Without deceptions
Credit: BloodHound


Domain Admins Group
With deceptions
Credit: BloodHound

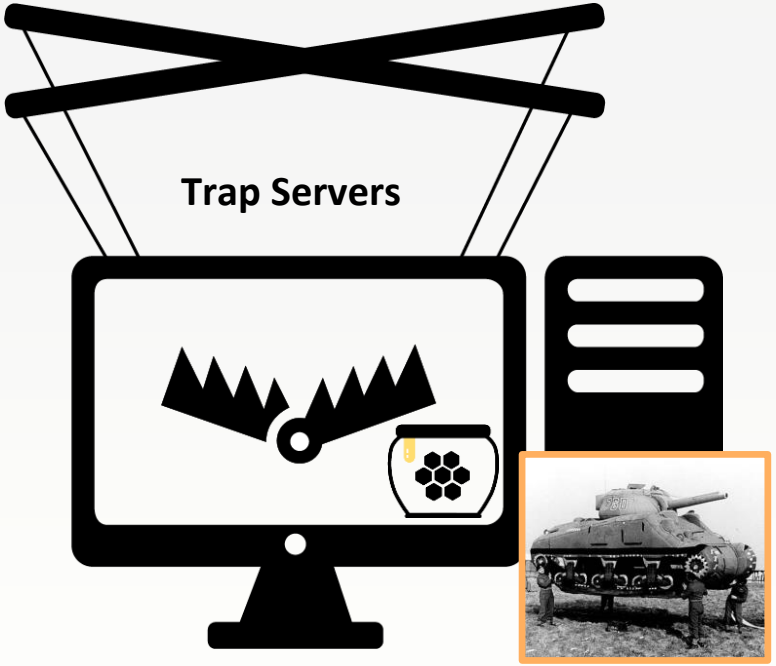
Where to Plant Deceptions?

Existing Machines



Detection: Monitor failed logins attempts

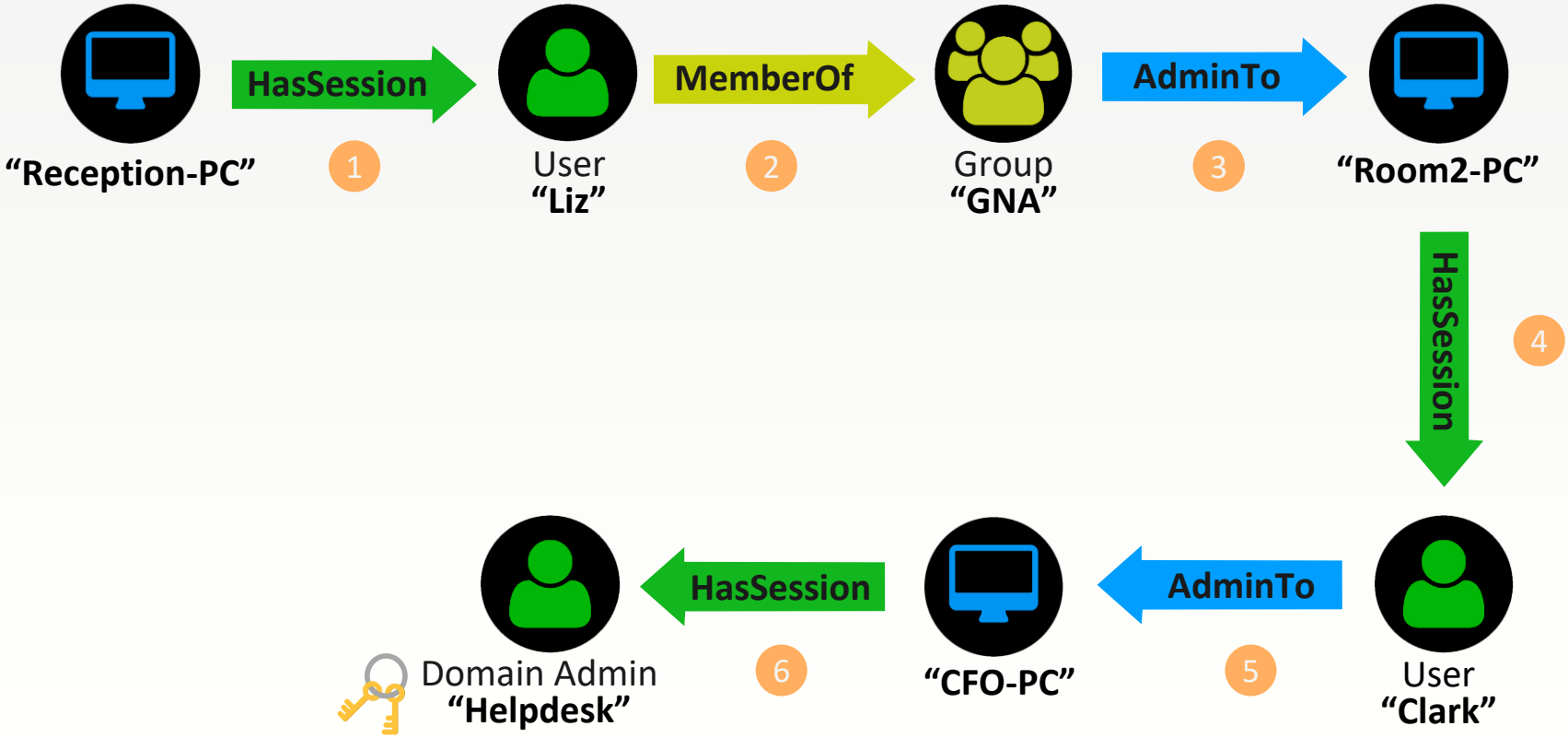
Trap Servers



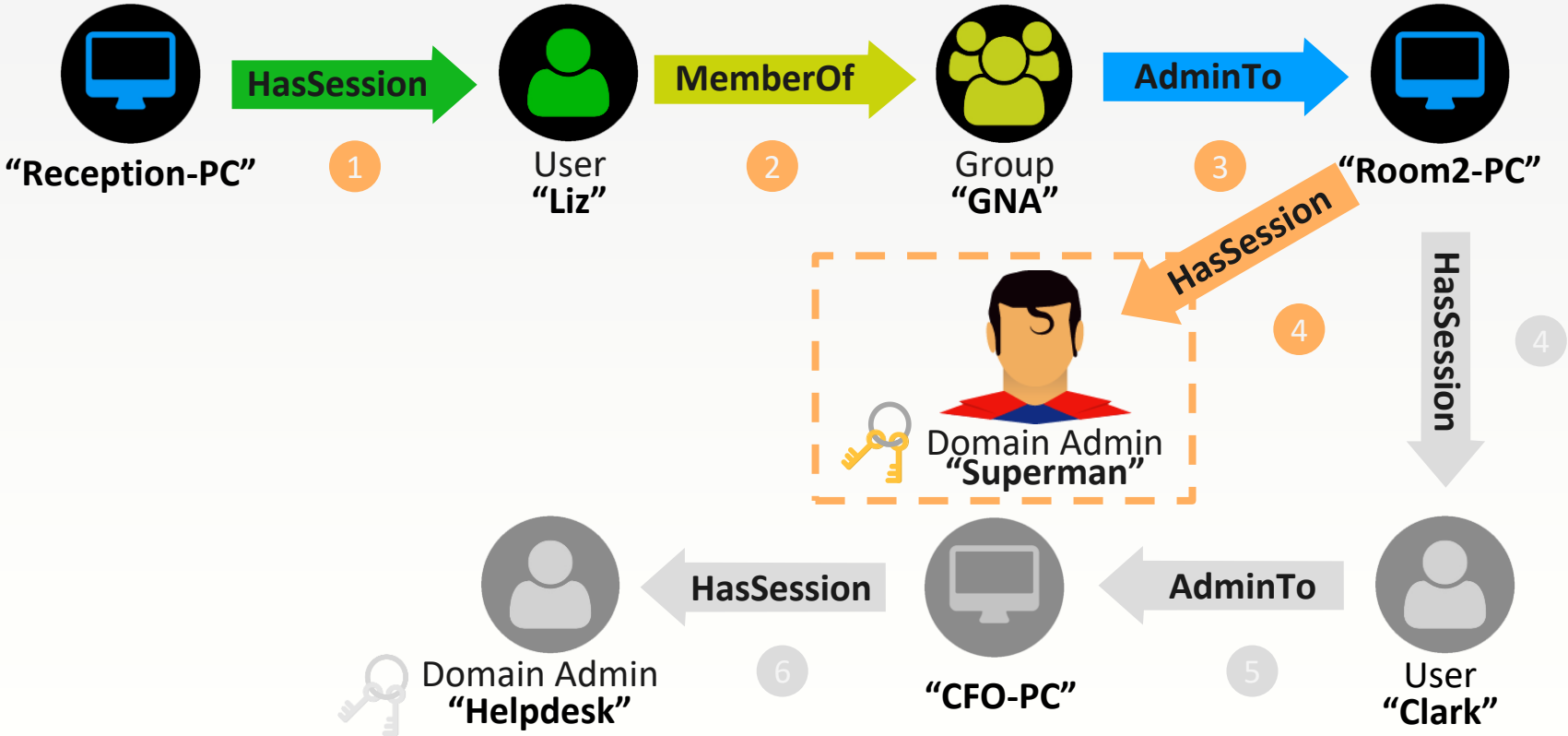
Detection: Monitor interaction with the server

How to Create Deceptive User Sessions?

From Breach to Complete Domain Control in 6 Steps

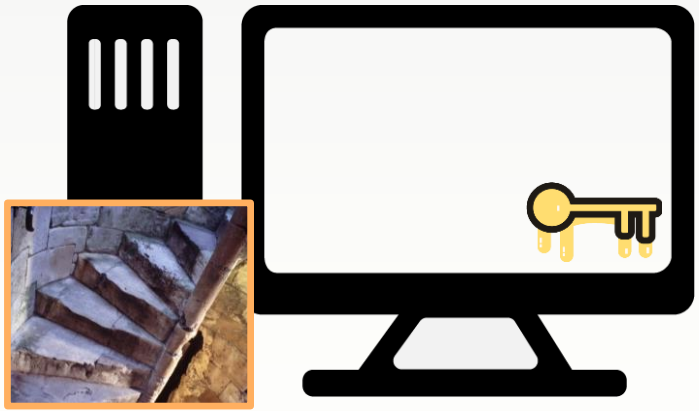


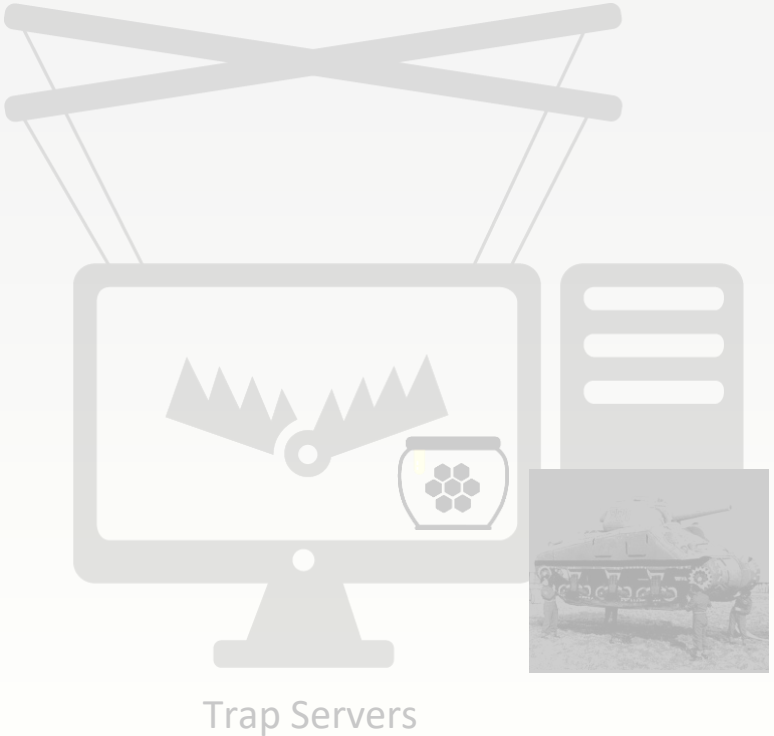
From Breach to Being Caught in 4 Steps



Where to Plant Deceptions?

Existing Machines





Trap Servers

Detection: Monitor failed logins attempts

How to Create Deceptive User Sessions?

Method 1: HKU Registry SIDs

Method 1: Extracting Registry SIDs

Win API: RegEnumKey

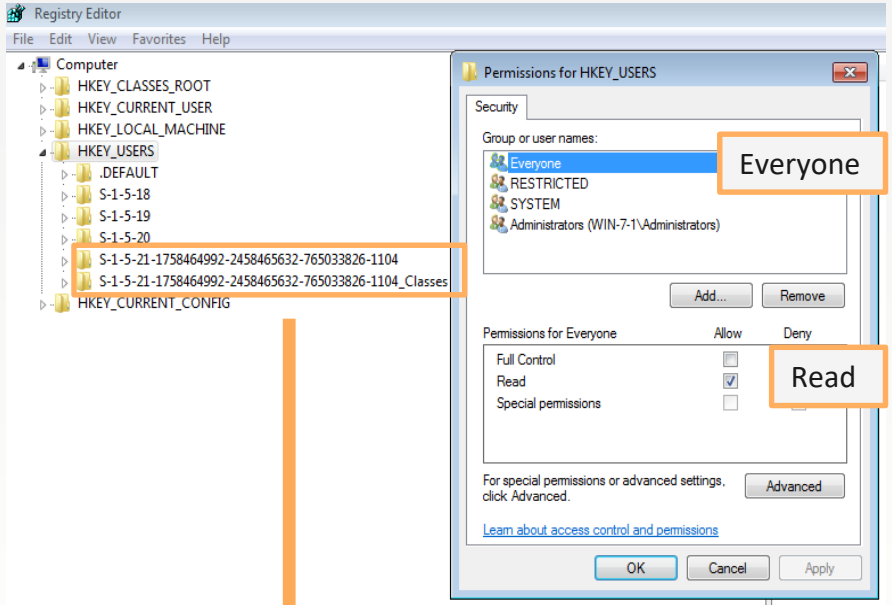
Tools: Get-LoggedOnLocal , PsLoggedon.exe, PVEFindADUser.exe

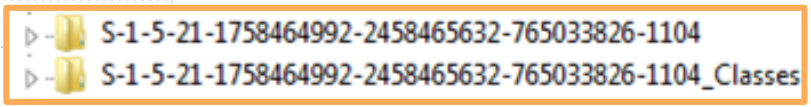
Location: Registry HKU

Deception Planting: “reg load HKU\<SID> dummy.dat”

Extracting Registry SIDs - cont.

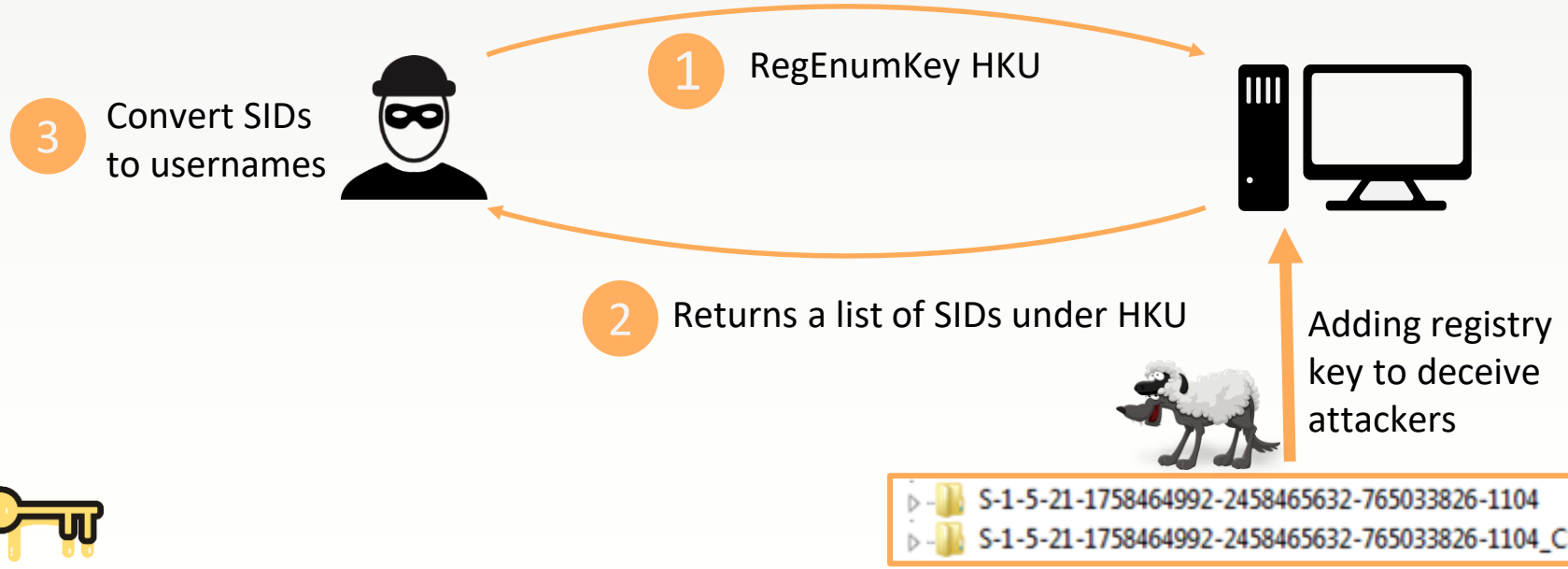
- HKU Registry Hive holds read permission to “Everyone” by default
- Any Domain User can query the SIDs under HKU of any domain machine
- Converting the SID to username, provides a list of logged-in users.

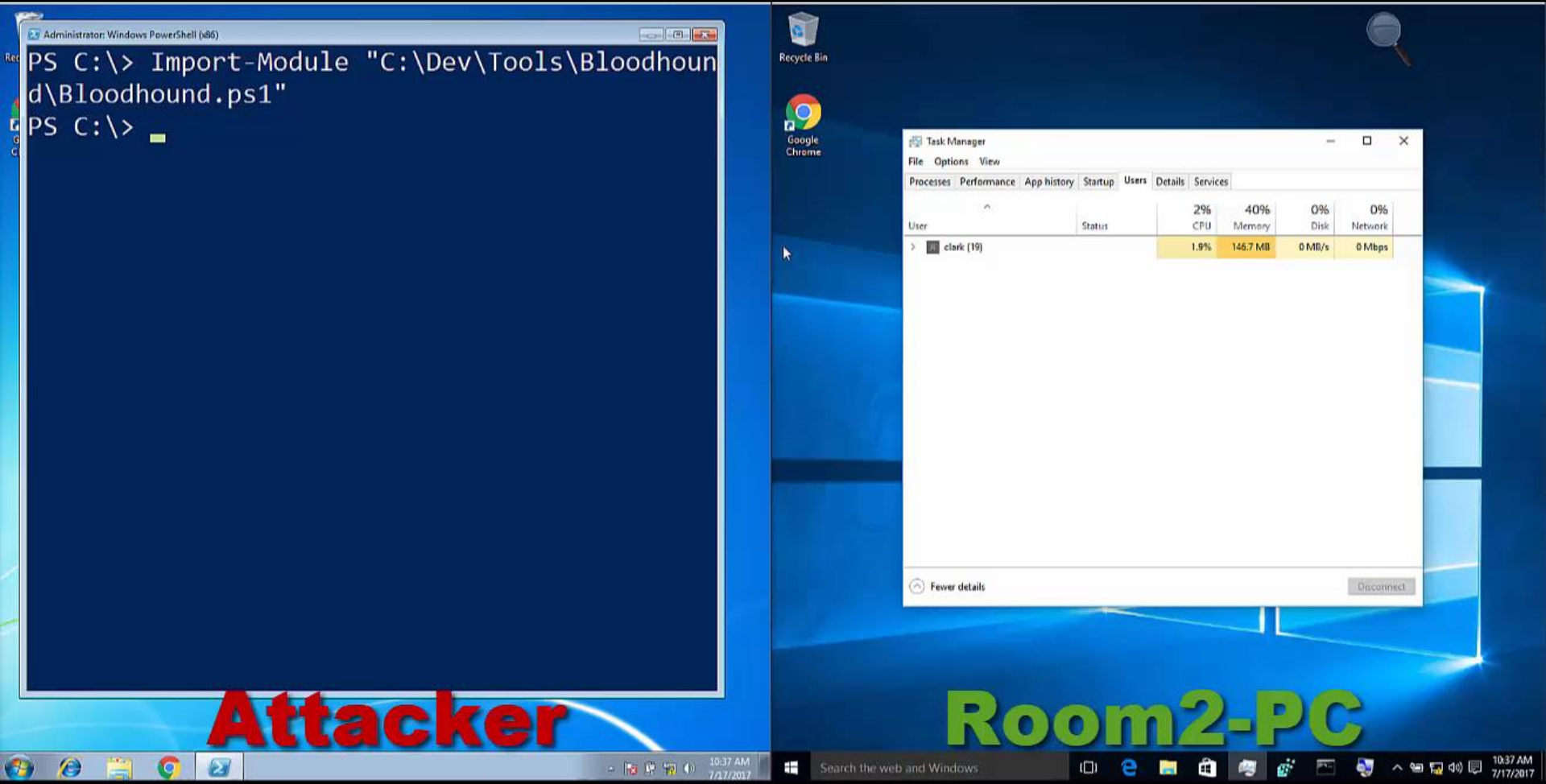




***Fun Fact**: Enumerating the HKU can give lots of additional information on the target machine: Wifi connections, Geolocation, installed programs etc...*

Extracting Registry SIDs - cont.

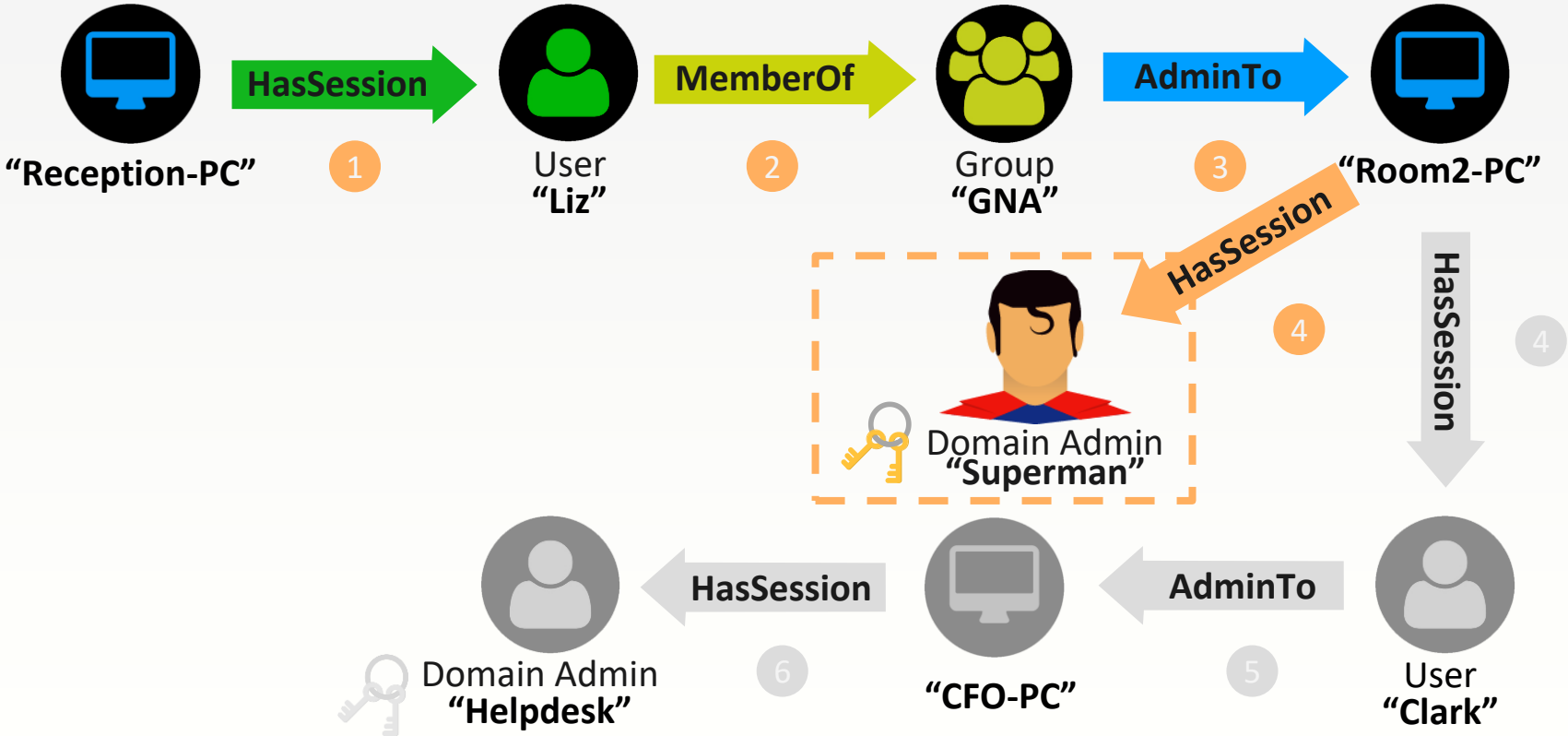



Administrator: Windows PowerShell (x86)
PS C:\> Import-Module "C:\Dev\Tools\Bloodhound\Bloodhound.ps1"
PS C:\>
Attacker
Recycle Bin
Google Chrome
Task Manager
File Options View
Processes Performance App history Startup Users Details Services
User Status 2% CPU 40% Memory 0% Disk 0% Network
clark (19) 1.9% 146.7 MB 0 MB/s 0 Mbps
Fewer details
Disconnect
Search the web and Windows
10:37 AM 7/17/2017
Room2-PC

How to Create Deceptive User Sessions?

Method 2: Logon-Sessions' Information

From Breach to Being Caught in 4 Steps



Method 2: Extracting Logon-Sessions' Information

Win API: NetWkstaUserEnum

Tools: Get-LoggedOn , PsLoggedon.exe, NetView.exe, Mimikatz, WCE

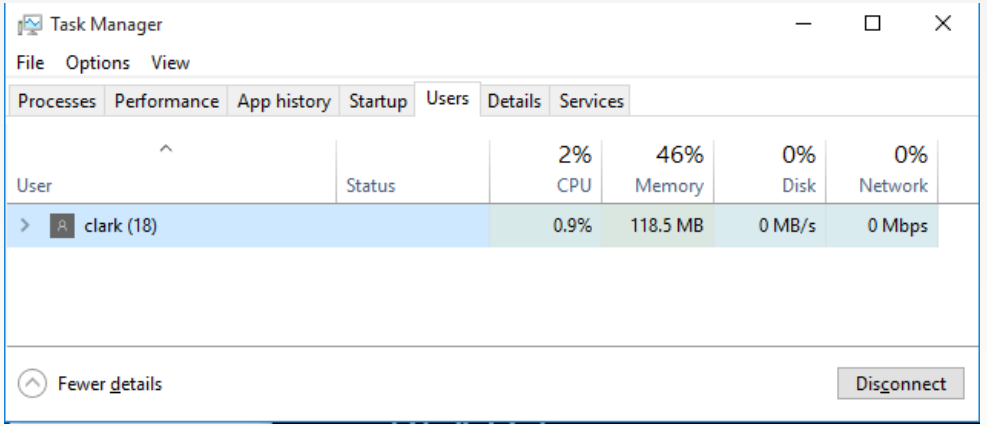
How To Access: Wkssvc named pipe

Deception Planting: "runas /netonly /noprofile /user:<Domain>\<User> <process>"

Open Source Tool: "Dcept" by secureworks https://github.com/secureworks/dcept

Extracting Logon-Sessions' Information - cont.

- For every successful login, Windows creates a logon session and returns a user token
- NetWkstaUserEnum returns the information of all existing tokens



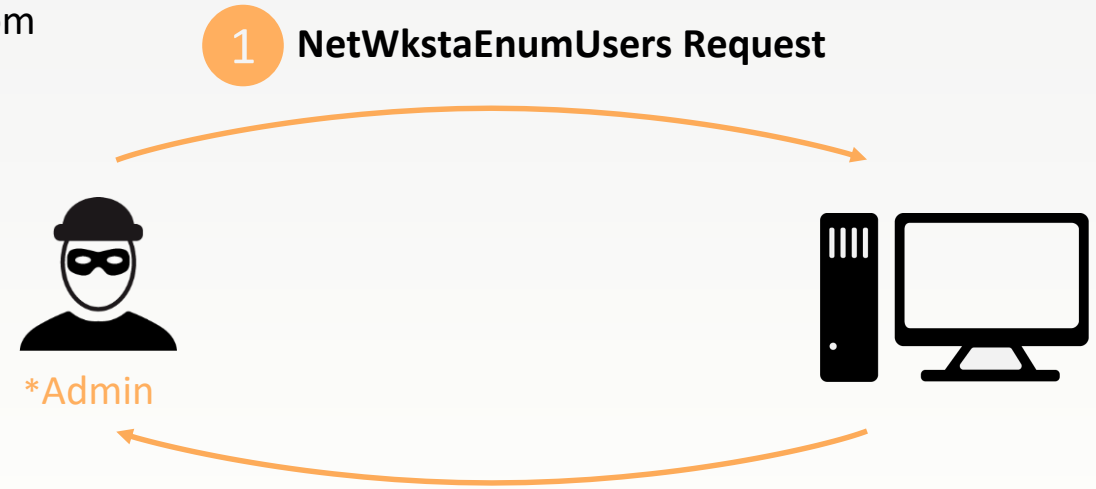
- No successful authentication -> no token
- Except for.... "RunAs /netonly"

Extracting Logon-Sessions' Information - cont.

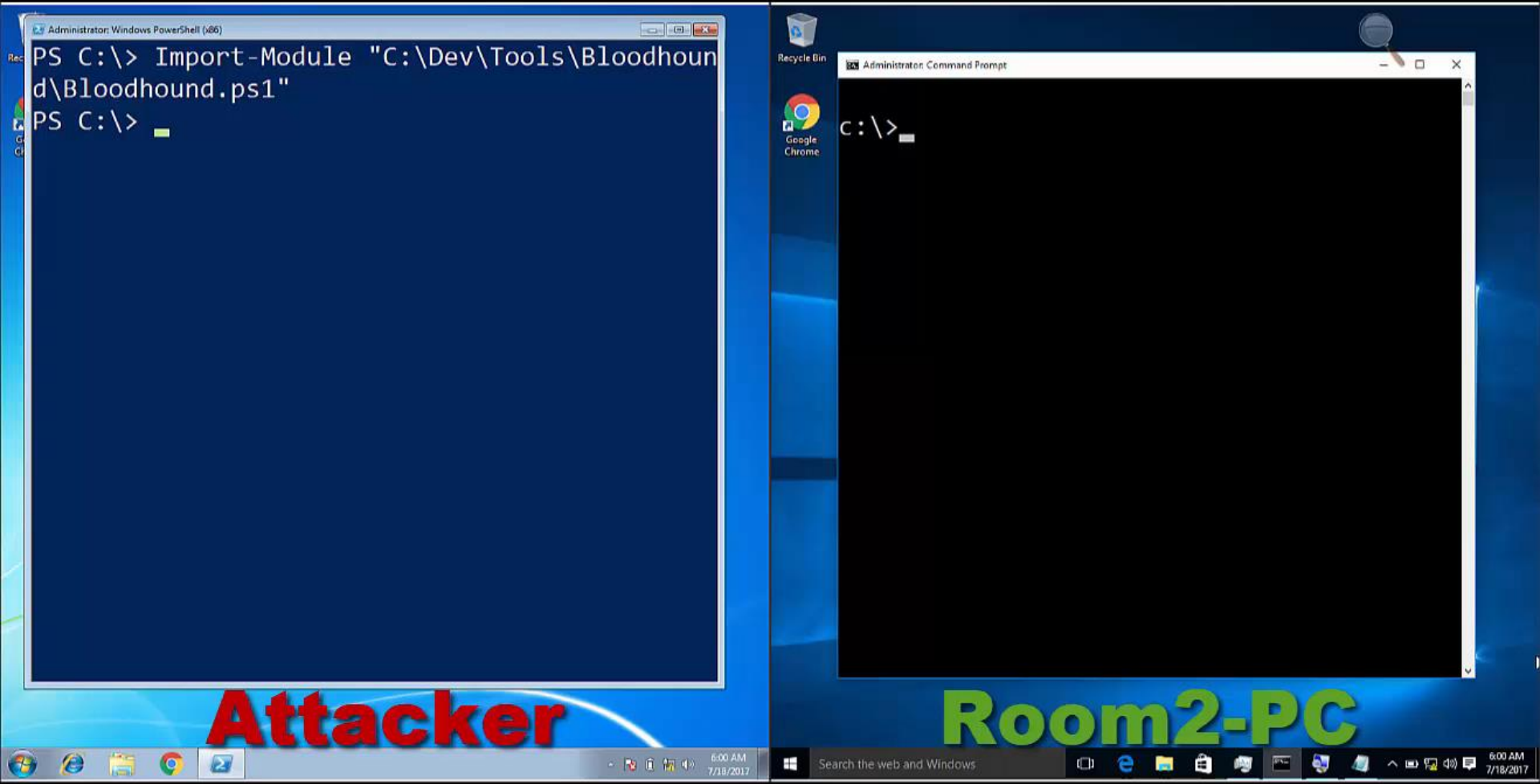
3 Extract the usernames from **WKSTA_USER_INFO_1**

Syntax

```C++
typedef struct _WKSTA_USER_INFO_1
{
  LMSTR wkui1_username;
  LMSTR wkui1_logon_domain;
  LMSTR wkui1_oth_domains;
  LMSTR wkui1_logon_server;
} WKSTA_USER_INFO_1,
*PWKSTA_USER_INFO_1,
*LPWKSTA_USER_INFO_1;
```



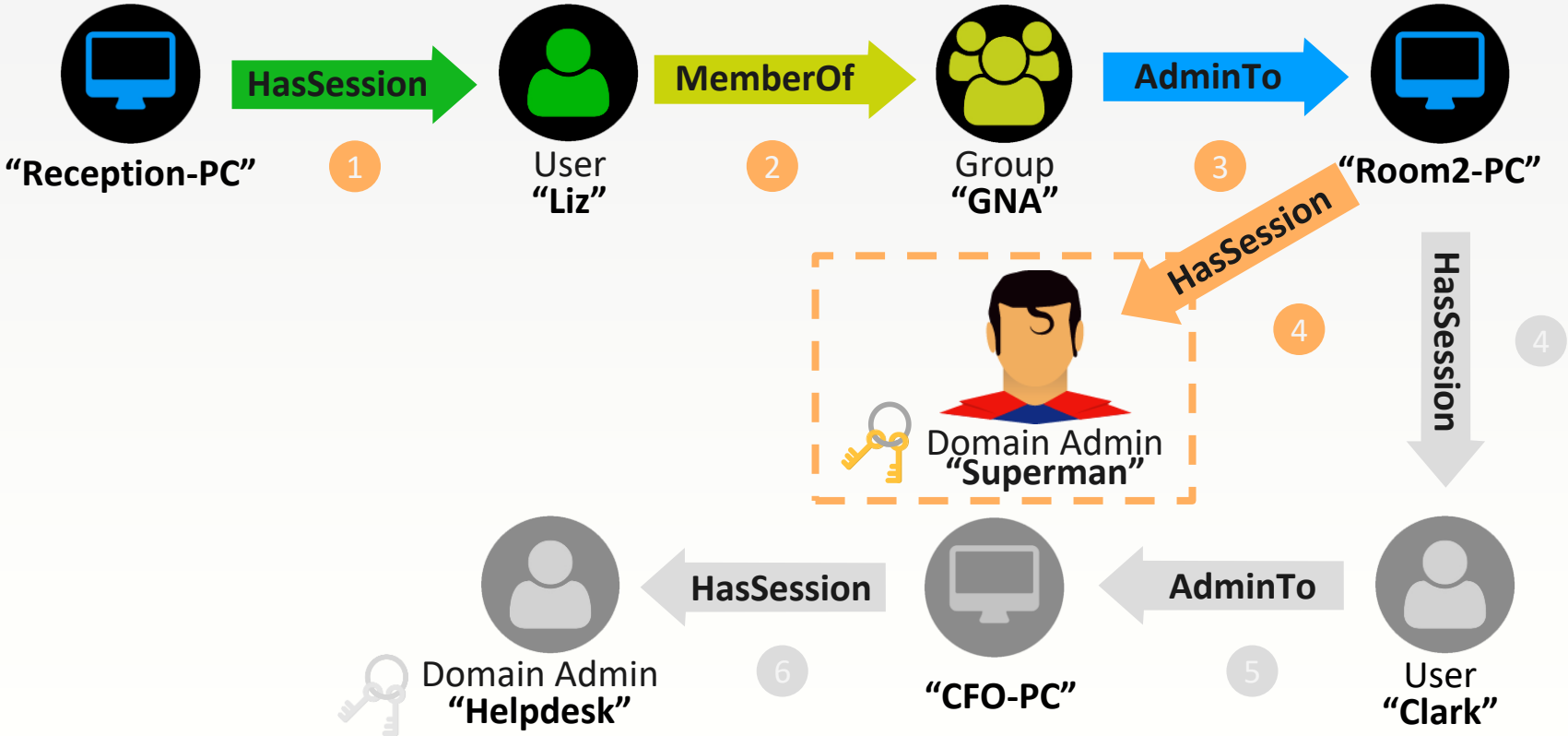
*The API requires administrative privileges on the target


Administrator: Windows PowerShell (x86)
PS C:\> Import-Module "C:\Dev\Tools\Bloodhound\Bloodhound.ps1"
PS C:\>
Attacker
Recycle Bin
Google Chrome
Administrator: Command Prompt
c:\>
Room2-PC
Search the web and Windows
6:00 AM
7/18/2017

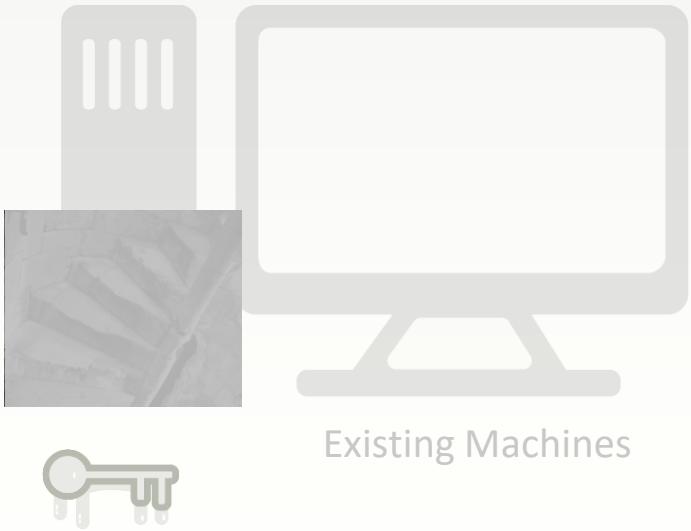
How to Create Deceptive User Sessions?

Method 3: SMB Sessions

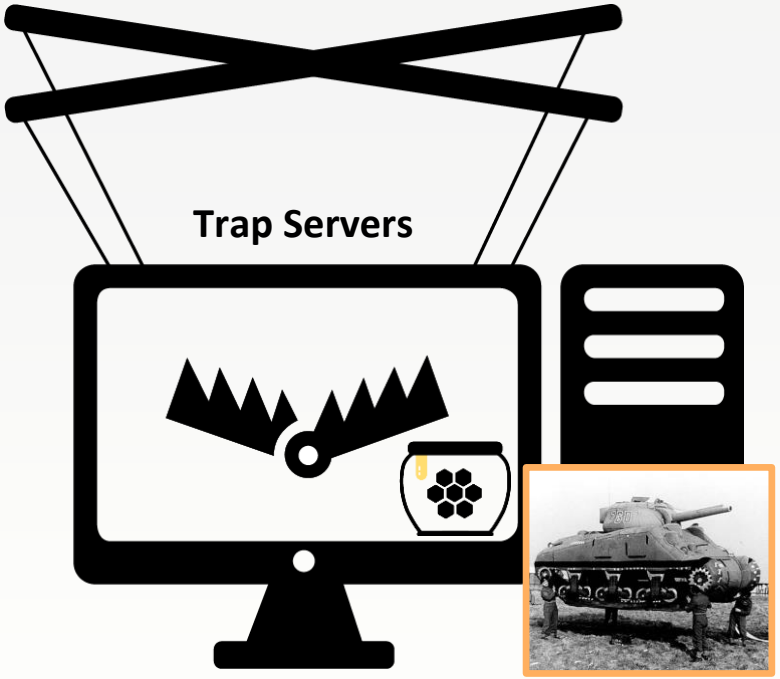
From Breach to Being Caught in 4 Steps



Where to Plant Deceptions?



Existing Machines



Detection: Monitor interaction with the server

Method 3: Extracting SMB Sessions

Win API: NetSessionEnum

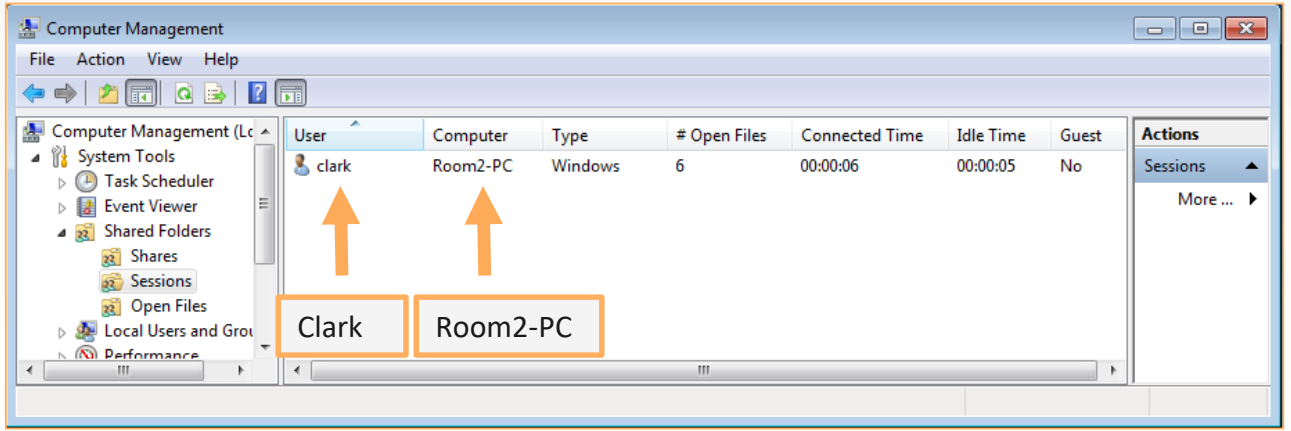
Tools: Get-NetSession, Netsess.exe, NetView.exe

How To Access: Srvsvc named pipe

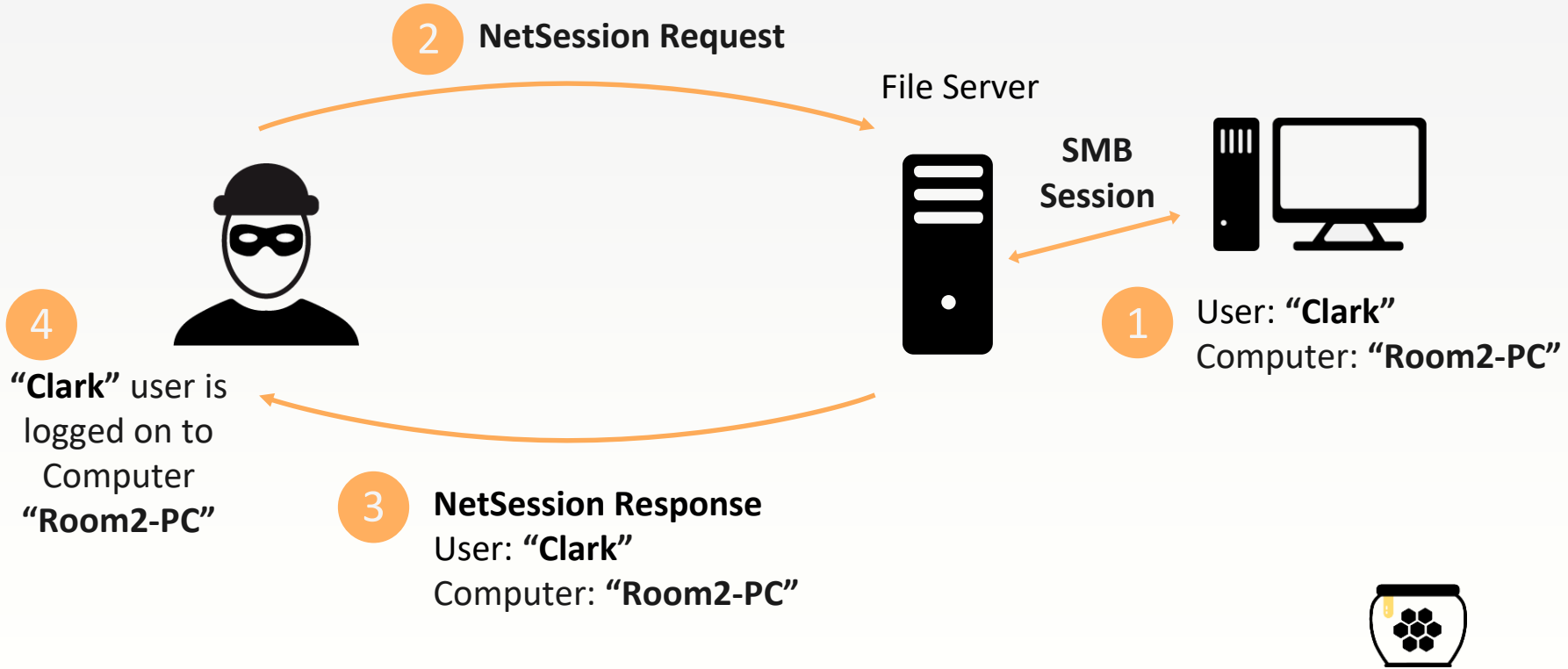
Deception Planting: Deceptive server response to NetsessionEnum

Extracting SMB Sessions - cont.

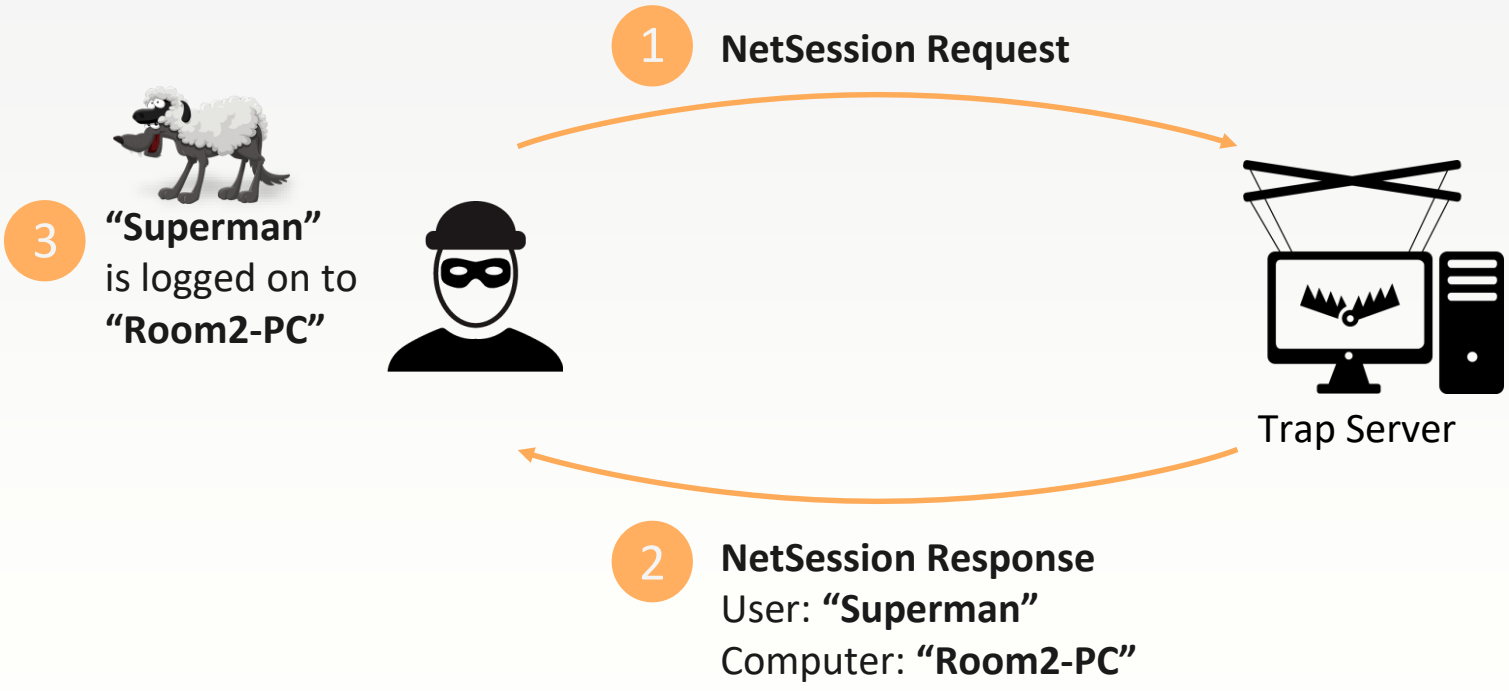
- The “Lanman SMB server” is installed by default on any windows machine
- SMB session information contains the source **host** and **username**
- Remote access of session information does **not require** admin privileges

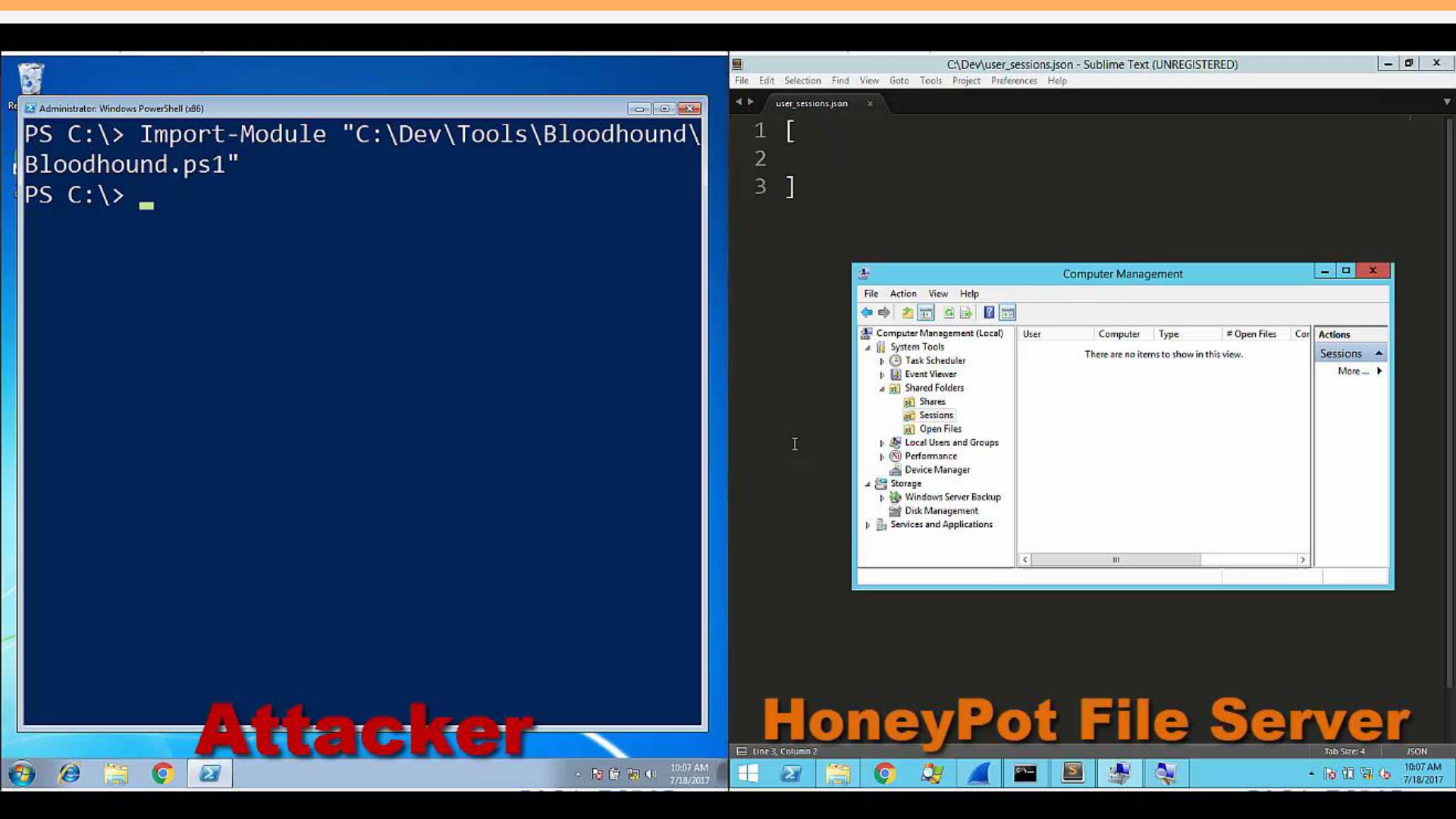


Extracting SMB Sessions - cont.



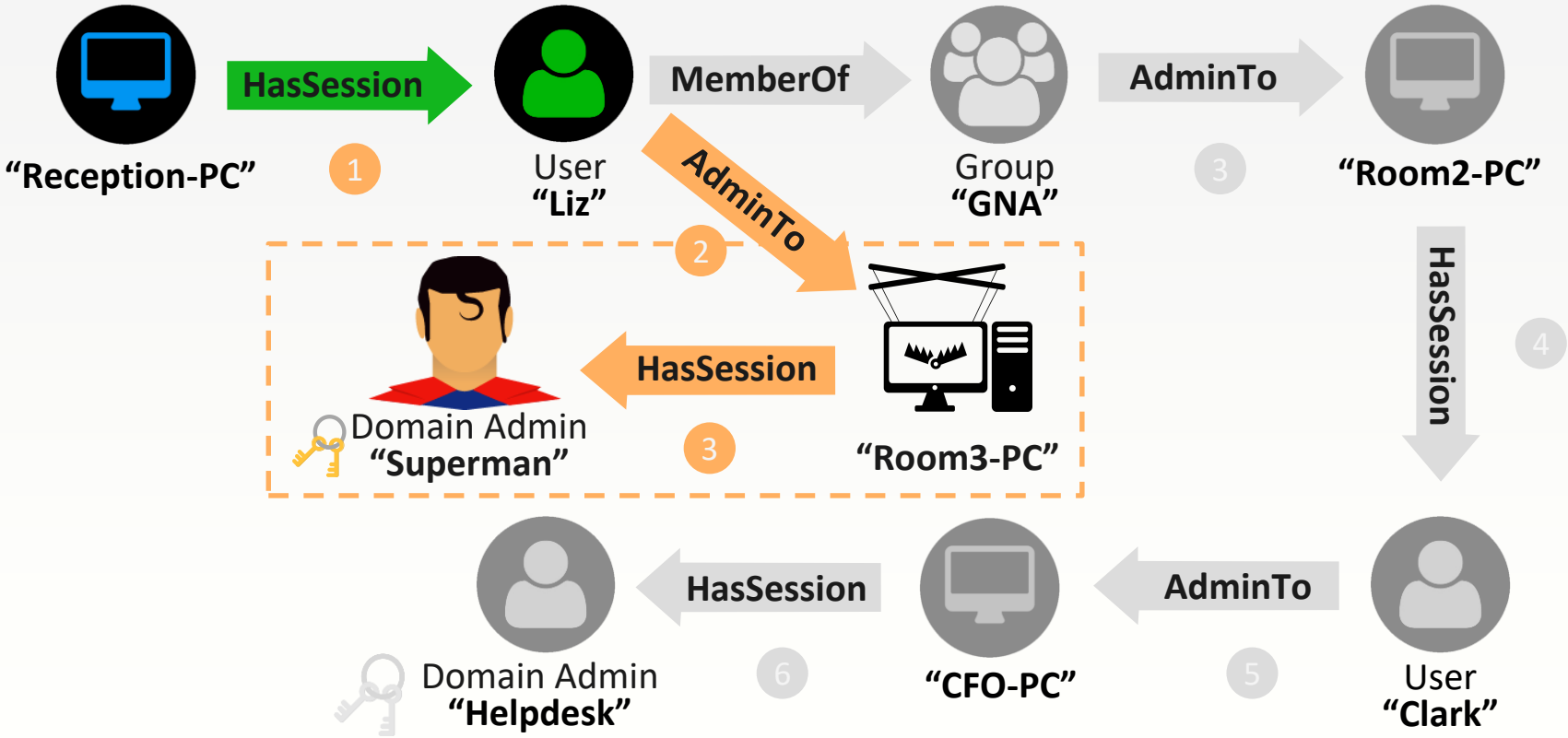
Extracting SMB Sessions - cont.




Administrator: Windows PowerShell (x86)
PS C:\> Import-Module "C:\Dev\Tools\Bloodhound\Bloodhound.ps1"
PS C:\>
Attacker
C:\Dev\user_sessions.json - Sublime Text (UNREGISTERED)
File Edit Selection Find View Goto Tools Project Preferences Help
user_sessions.json
1 [
2
3]
Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Shared Folders
Shares
Sessions
Open Files
Local Users and Groups
Performance
Device Manager
Storage
Windows Server Backup
Disk Management
Services and Applications
User
Computer
Type
Open Files
There are no items to show in this view.
Actions
Sessions
More ...
HoneyPot File Server
Line 3, Column 2
Tab Size: 4
JSON
10:07 AM
7/18/2017

How to Create Deceptive Local Admins?

From Breach to Being Caught in 3 Steps



How to Create Deceptive Local Admins?

Method 1: Administrator's Group Members

Method 1: Extracting Local Admins

Win API: NetLocalGroupGetMembers

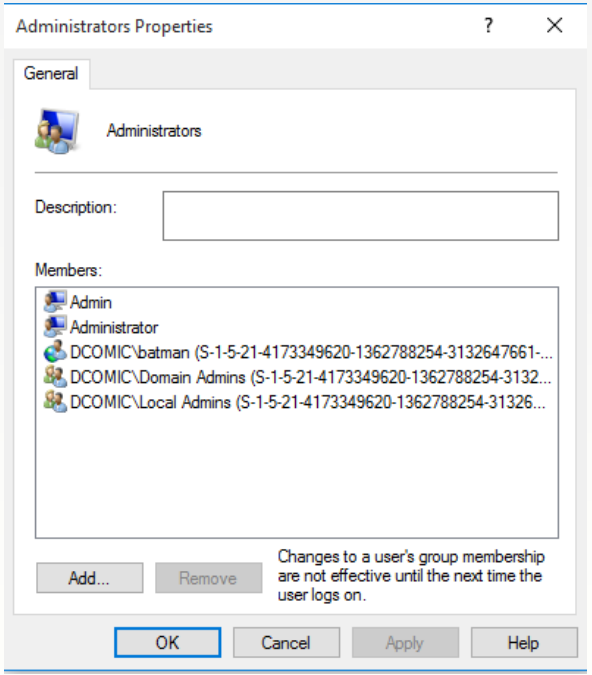
Tools: Get-NetLocalGroup

Location: SAM database

Deception Planting: Deceptive server response to NetLocalGroupGetMembers

Extracting Local Admins – cont.

- “NetLocalGroupGetMembers” API remotely retrieves members of a particular local group
- Remote access of group membership does **not require** admin privileges



Extracting Local Admins – cont.

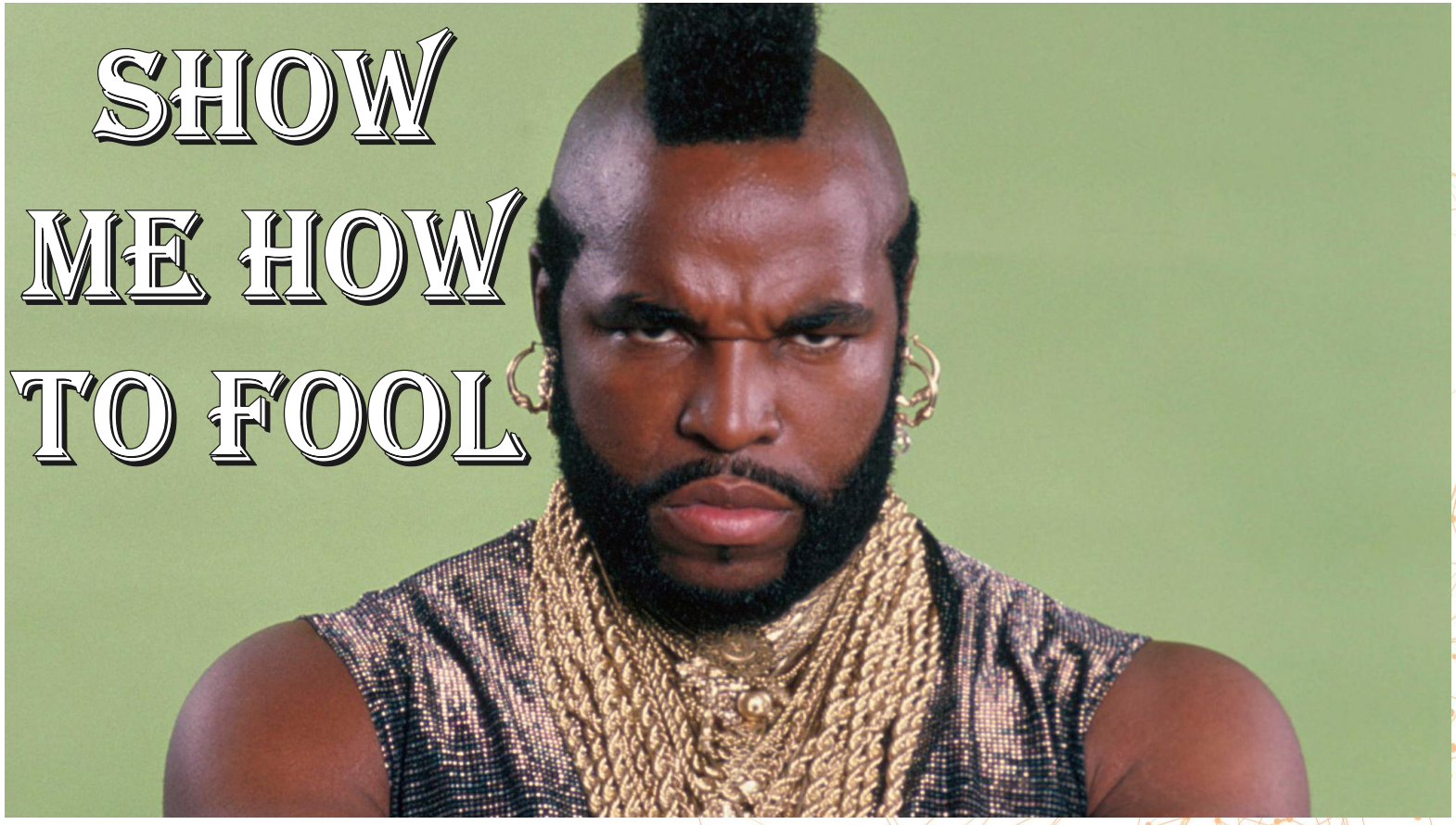
1 **NetLocalGroupGetMembers Request**

3

“Liz” is an administrator of **“Room3-PC”**

Trap Server **“Room3-PC”**

2 **NetLocalGroupGetMembers Response**
‘Administrators’ group member**: “Liz”**

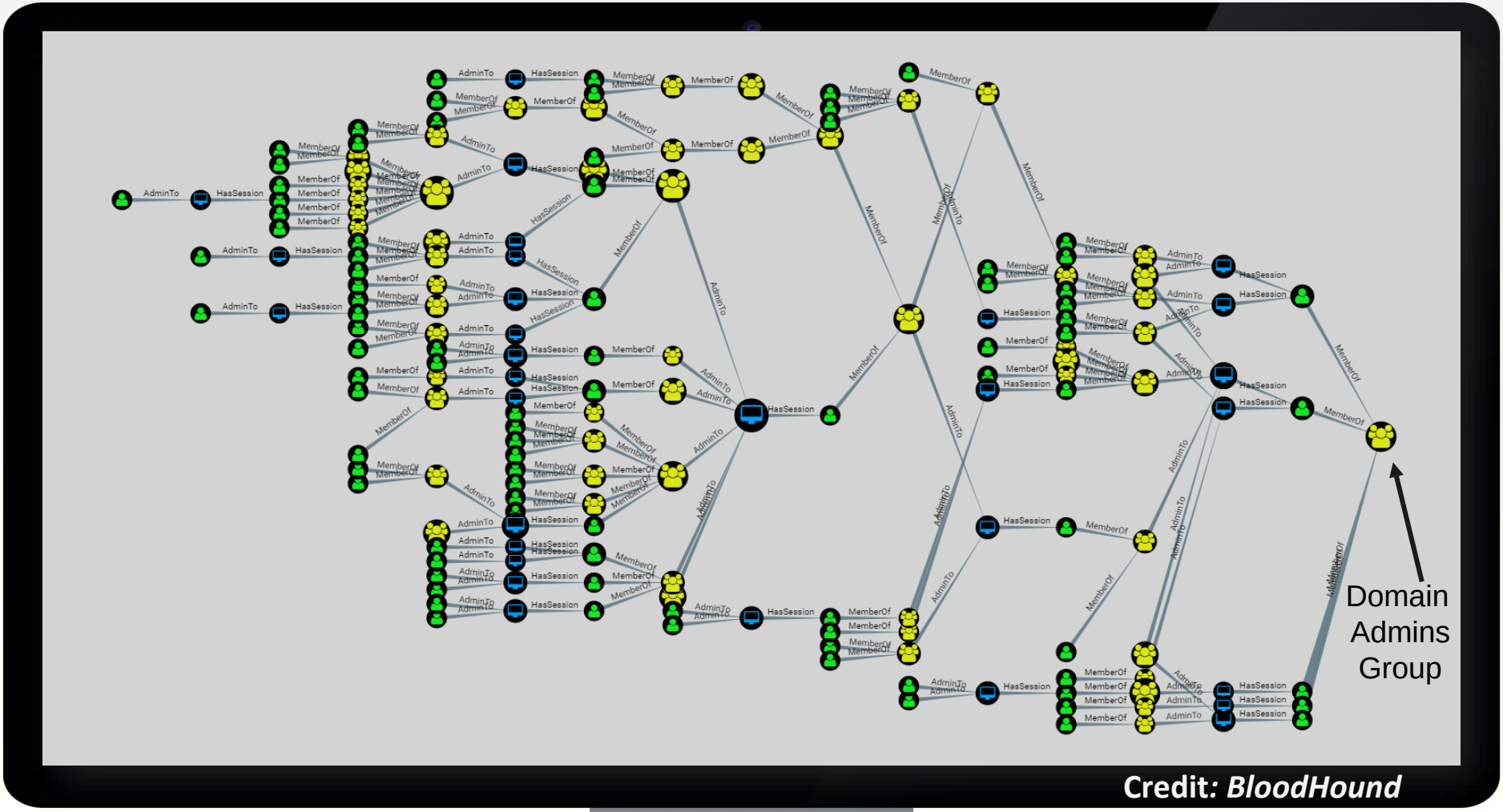

SHOW
ME HOW
TO FOOL

Planting Deceptions in The Lateral Movement Graph

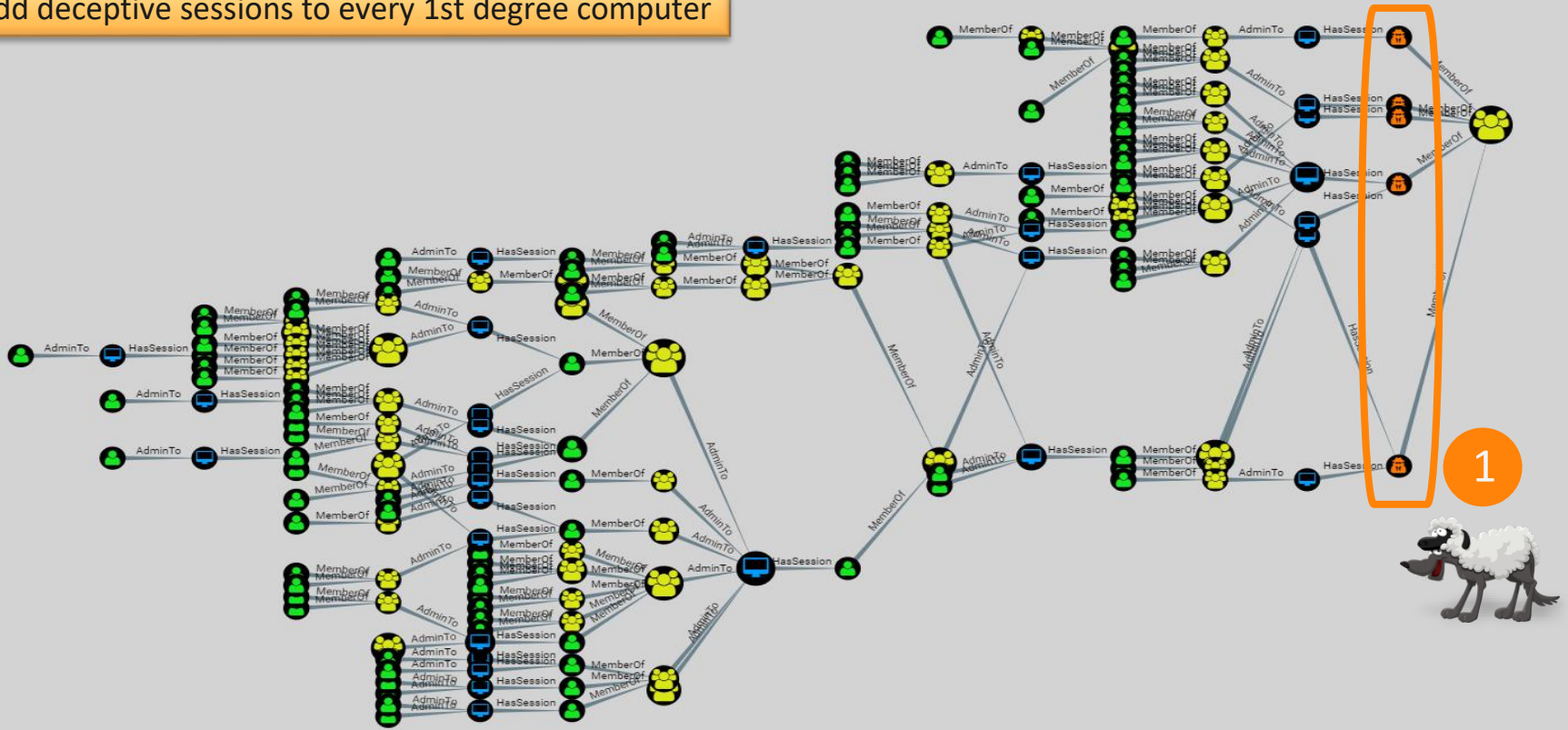
Goal: Make every ‘shortest path’ contain at least one deception

Method:

1. Add deceptive sessions to every 1st degree computer
2. Add deceptive computers to the top 1st degree groups
3. Add non-connected computers to the graph

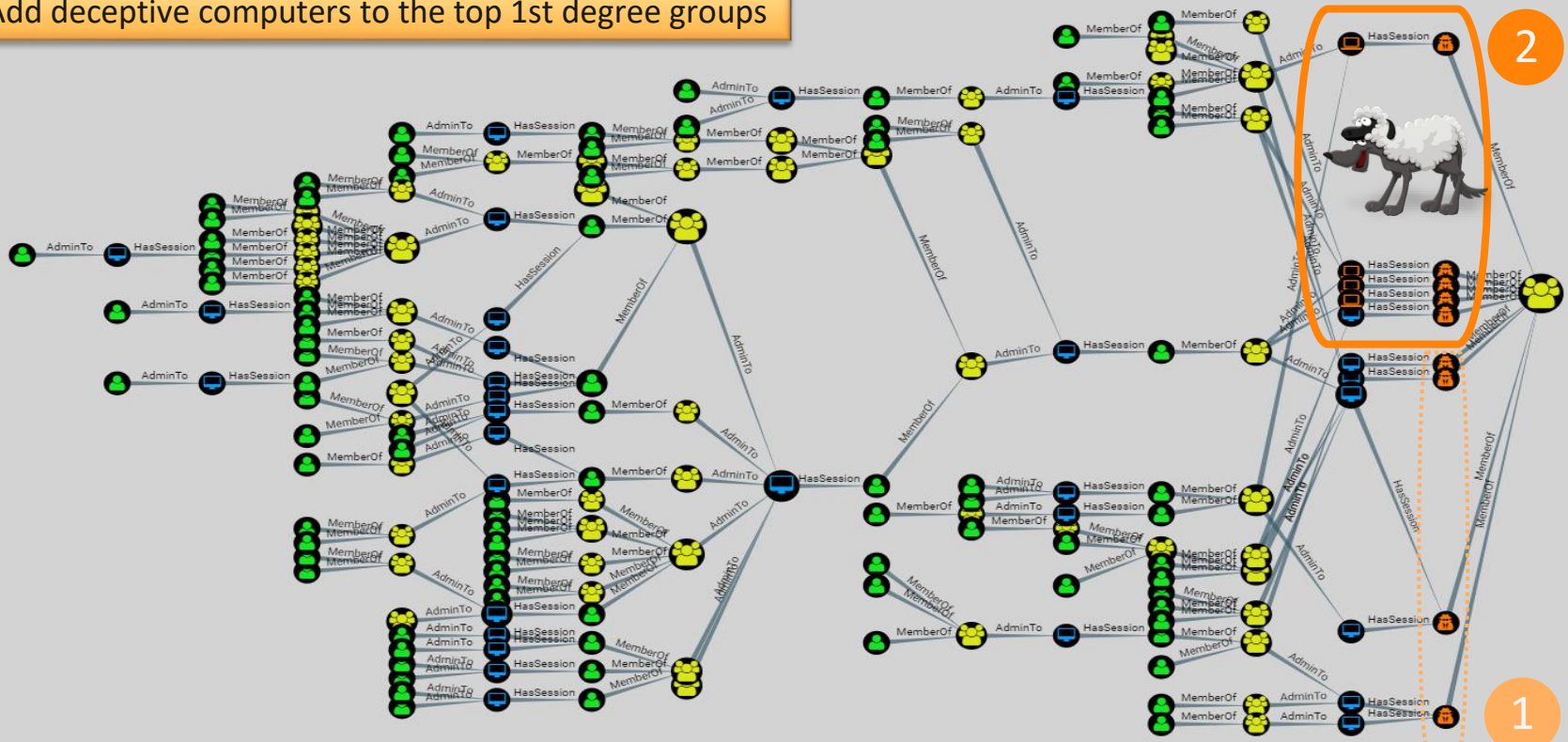

Domain Admins Group
Credit: BloodHound

Add deceptive sessions to every 1st degree computer



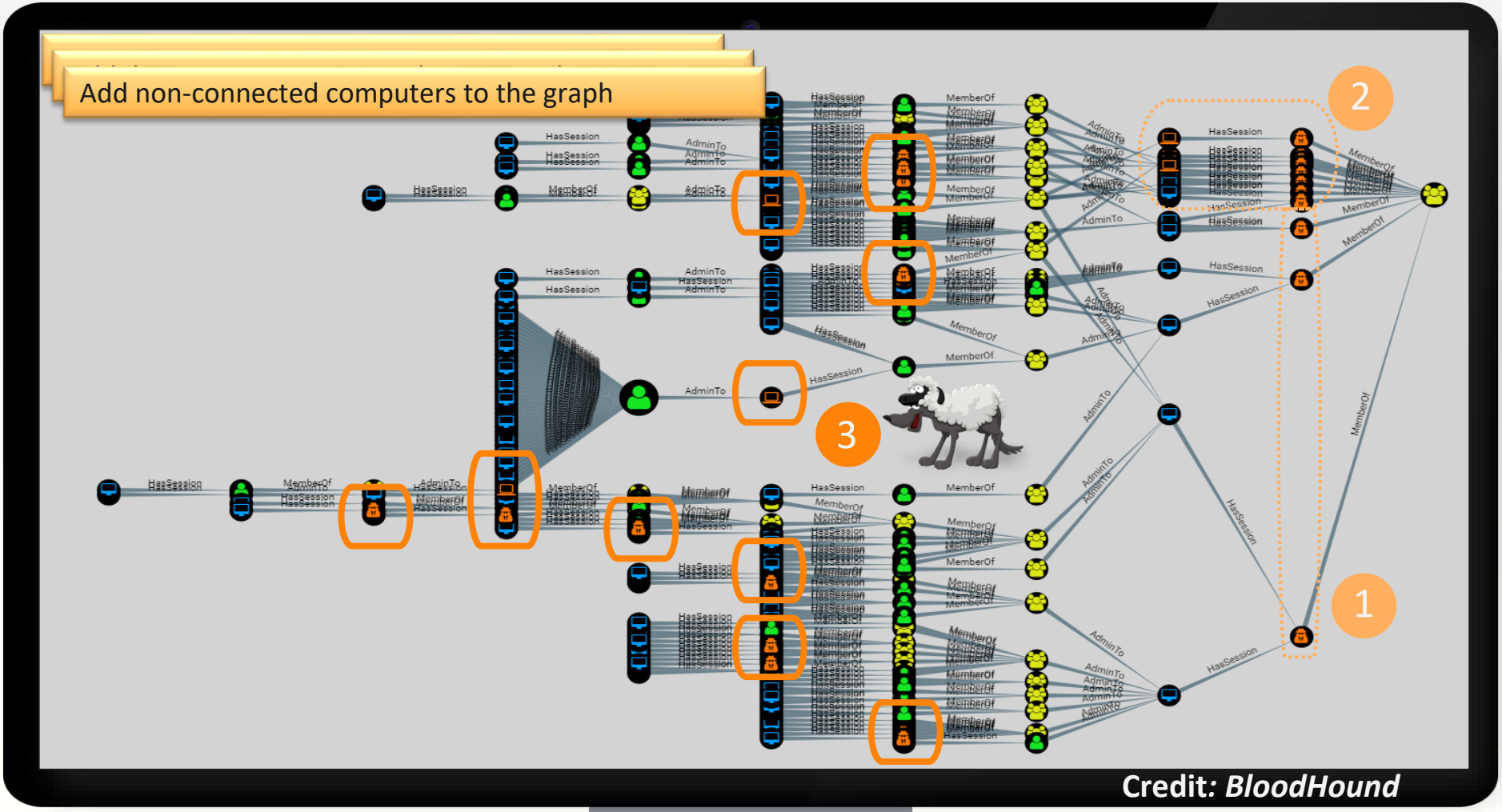
Credit: *BloodHound*

Add deceptive computers to the top 1st degree groups



Credit: *BloodHound*

Add non-connected computers to the graph



Credit: *BloodHound*

Wrap Up

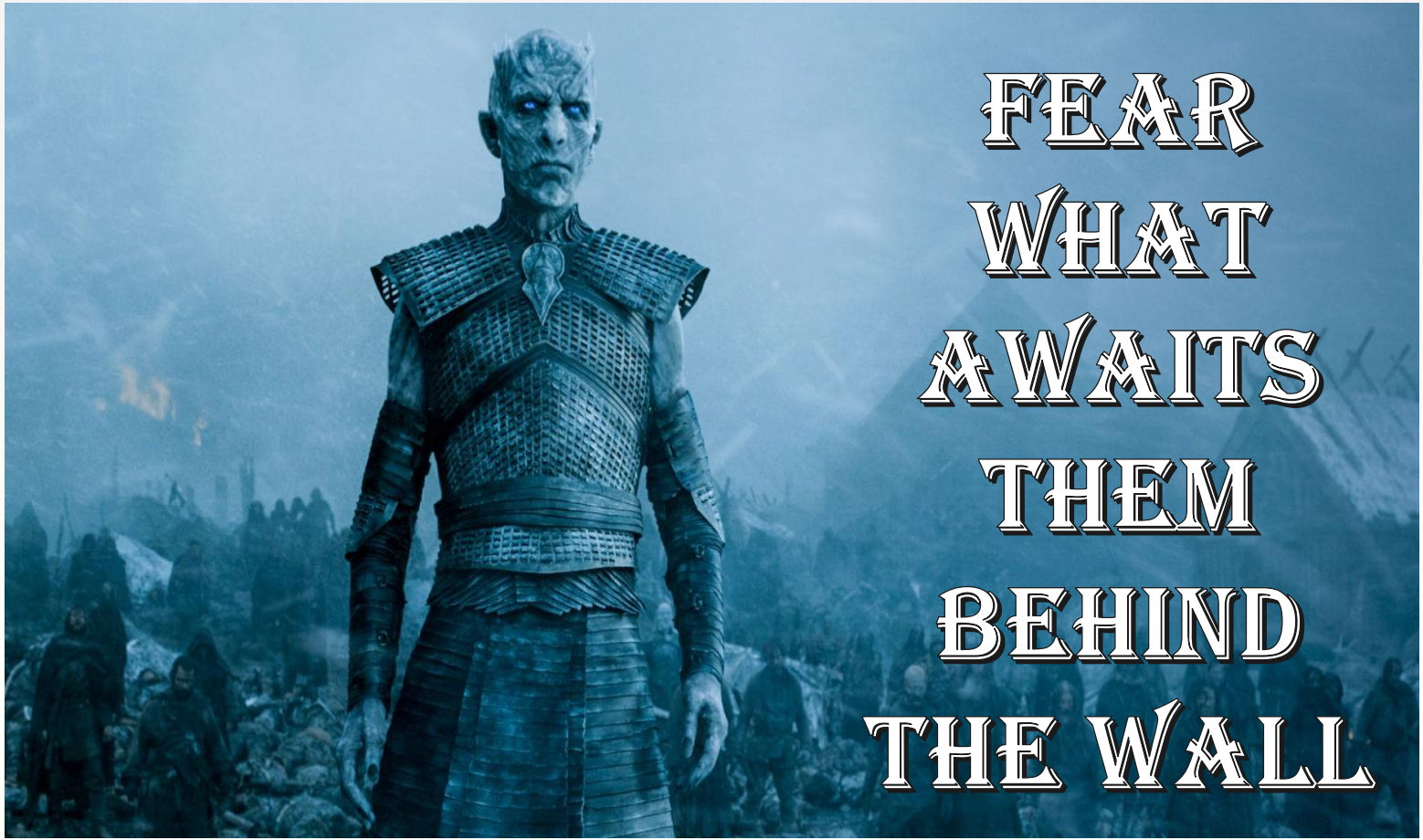
We Covered

1. Lateral movement and graphs
2. 4 methods to plant deceptions
3. How to control the path of an attacker
4. How to plant deceptions in every ‘shortest path’ to domain admin

Conclusions

1. Deceptions bring doubt and uncertainty to the operations of attackers
2. As a security strategy, walls are good, but we have to assume that walls will be breached
3. Using deceptions, we could make attackers fear what awaits them behind the walls

Using Deceptions, We Could Make Attackers...



illusive™

Questions?

tom@illusivenetworks.com
@4x6hw

illusive™

Thank You

tom@illusivenetworks.com

@4x6hw