



# CYBER JUDO: OFFENSIVE CYBER DEFENSE

Tal Be'ery, Sr. Security Research Manager, Microsoft ATA, @TalBeerySec  
Itai Grady, Security Researcher, Microsoft ATA, @ItaiGrady



# Speaker Info – Tal Be'ery

- Sr. Security Research Manager @Microsoft
- Developing MicrosoftATA (Advanced Threat Analytics)
- Former VP for Research @Aorato (Acquired by Microsoft)
- 15 years of security research experience
- Author of the TIME attack on SSL
- Regular speaker in top international security conferences
- Named a “Facebook Whitehat”
- Twitter: @TalBeerySec



# Speaker Info – Itai Grady

- Security Researcher @Microsoft
- Developing MicrosoftATA (Advanced Threat Analytics)
- Twitter : @ItaiGrady

# Agenda

- Intro
  - The Cyber Boxer vs. the Cyber Judoka
  - Targeted attacks: TTPs, Kill-chain, MicrosoftATA
- Lateral Movement Reconnaissance
  - Attacker's TTPs + BloodHound + Automated Lateral Movement 
  - Cyber Boxer Defense: Net Cease and Friends 
  - Cyber Judo Defense
    - NetSess to Detect PtH 
    - SAMR to Detect Local Users attacks 
- Kerberos Error Injection:
  - Attacks, Cyber Boxer Defense, Cyber Judo Defense 
- Outro

# Intro

# Level 0: The “Fighting in the Dark” Model

“If you know the enemy and know yourself,  
you need not fear the result of a hundred  
battles.

If you know yourself but not the enemy, for  
every victory gained you will also suffer a  
defeat.

If you know neither the enemy nor yourself,  
you will succumb in every battle.”



# Level 1 : The “Boxer” Model

- Defenders Learn attackers' TTPs:
  - Tactics
  - Techniques
  - Procedures
- Defenders build their own TTPs
- Defenders practice the attackers' TTPs
  - Red Team
- Defenders practice their TTPs
  - Blue Team
- Some time same team for both
  - Purple Team



# Level 2 : The Judoka Model

- Judoka, a Judo warrior, uses the opponent's strength and movement against him
- Defenders Learns attackers' TTPs:
- Defenders adopts some attackers' TTPs in order to defeat them!
- That's our topic for today's talk



# Defenders and Attackers: Not so Apart

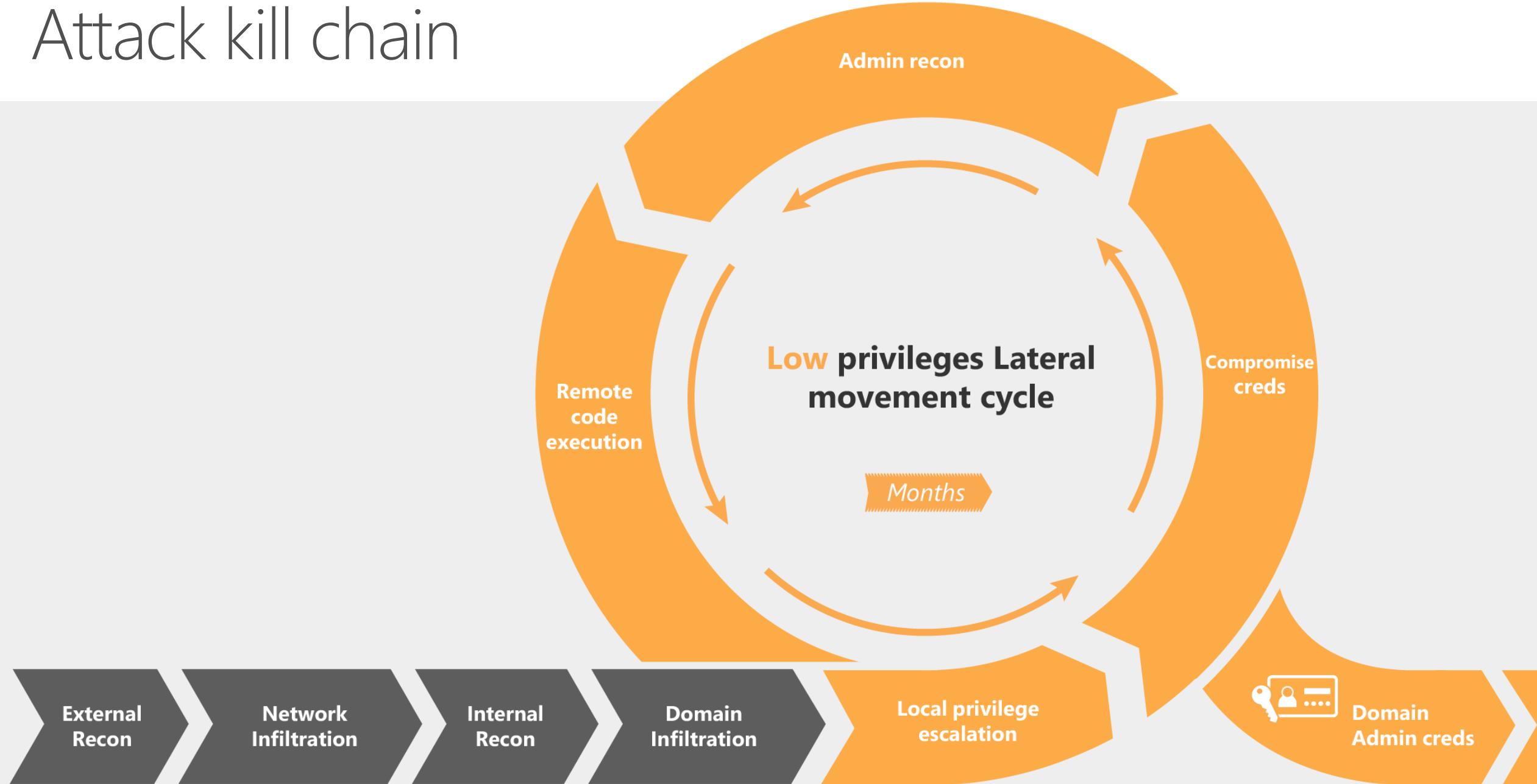
- Similar tools, challenges and scenarios

	<b>Defenders</b>	<b>Attackers</b>
<b>Network Deployment</b>	Proxy / Network Monitoring	MITM / Eavesdropper
<b>Host Deployment</b>	Agent (but they prefer to refrain: compatibility, performance)	Malware (but they prefer to refrain: compatibility, performance, detection)
<b>Privileges</b>	Least, otherwise part of the problem (see: @taviso)	Least, privileged users are more monitored
<b>Integrations</b>	“living off the land”. Core functionality must be delivered independently, opportunistic integrations	“living off the land”. Core functionality must be delivered independently, opportunistic existing non-default capabilities abuse
<b>Expertise</b>	OS internals, networking	OS internals, networking

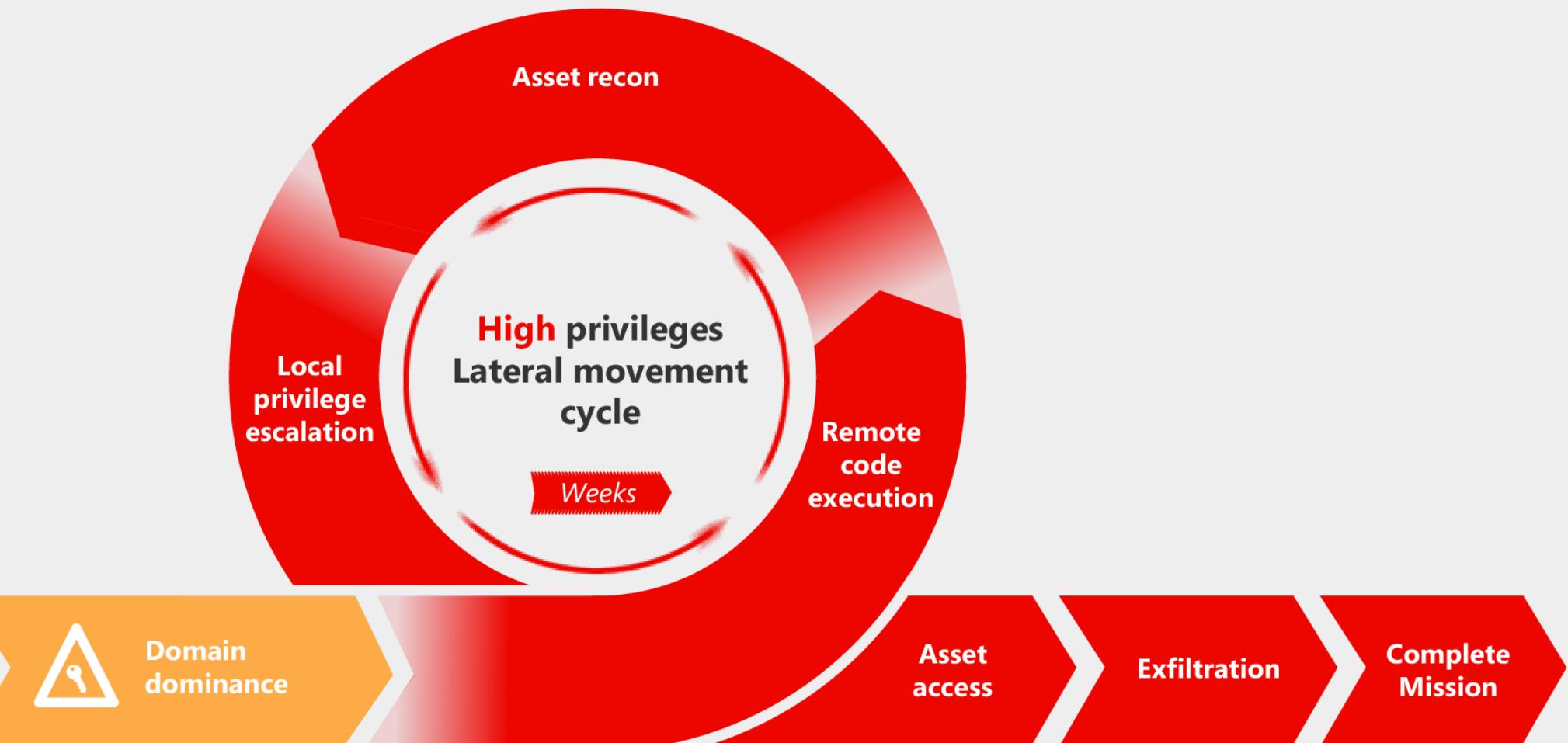
# Targeted Attacks



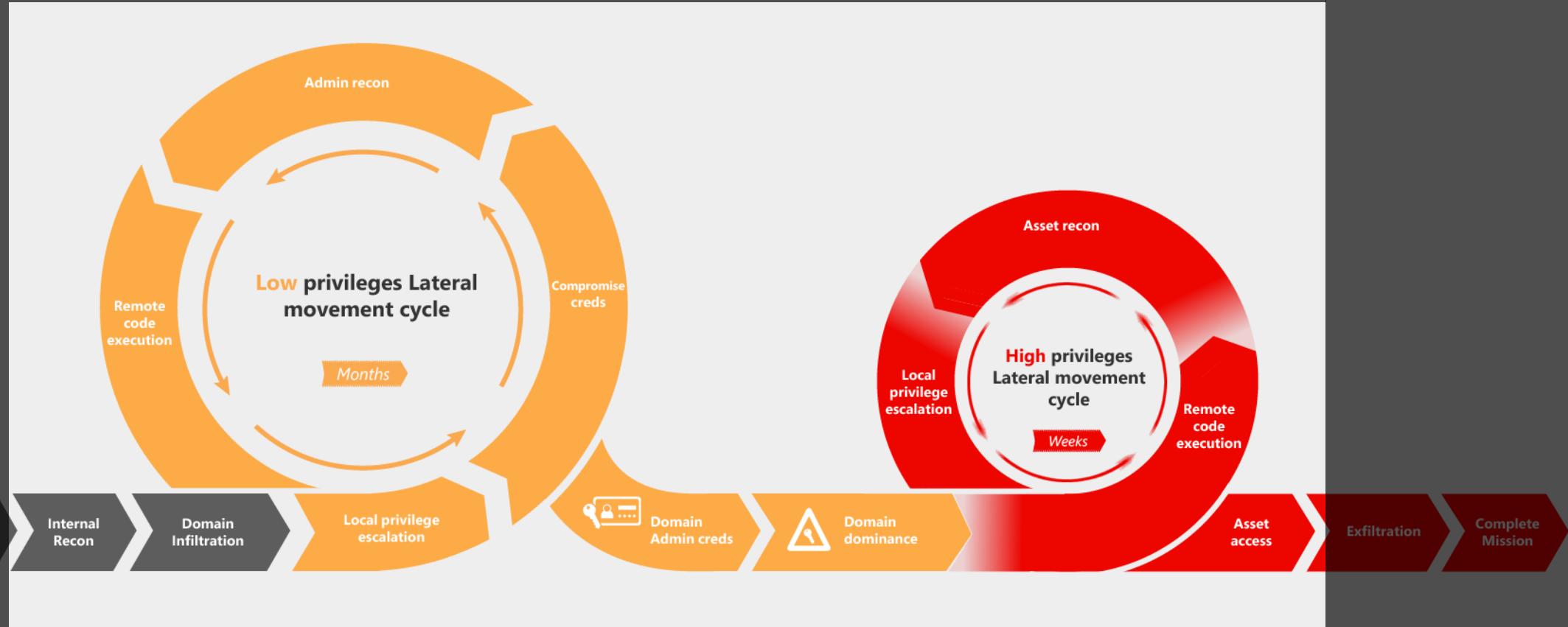
# Attack kill chain



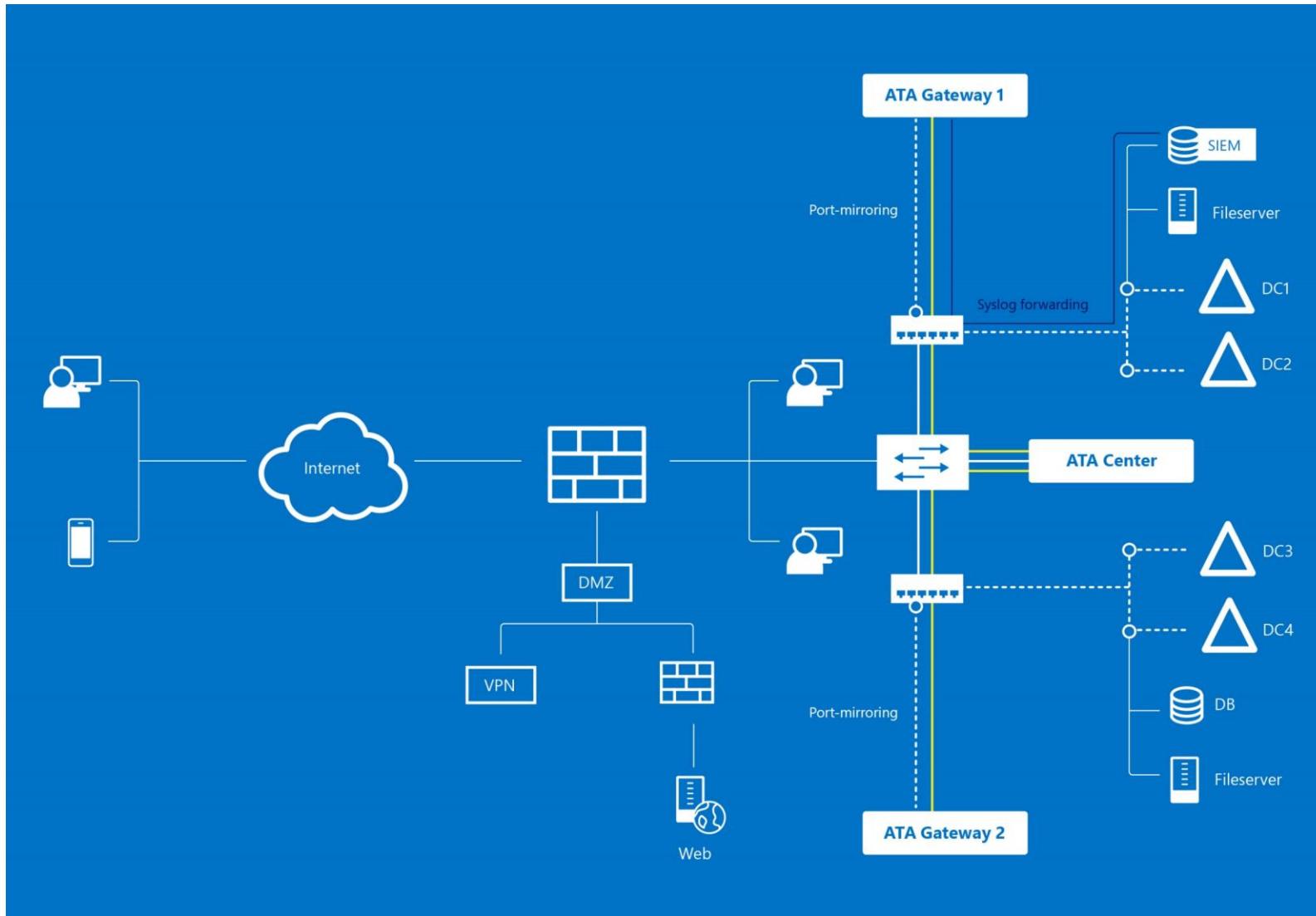
# Attack kill chain



# Attack kill chain and ATA

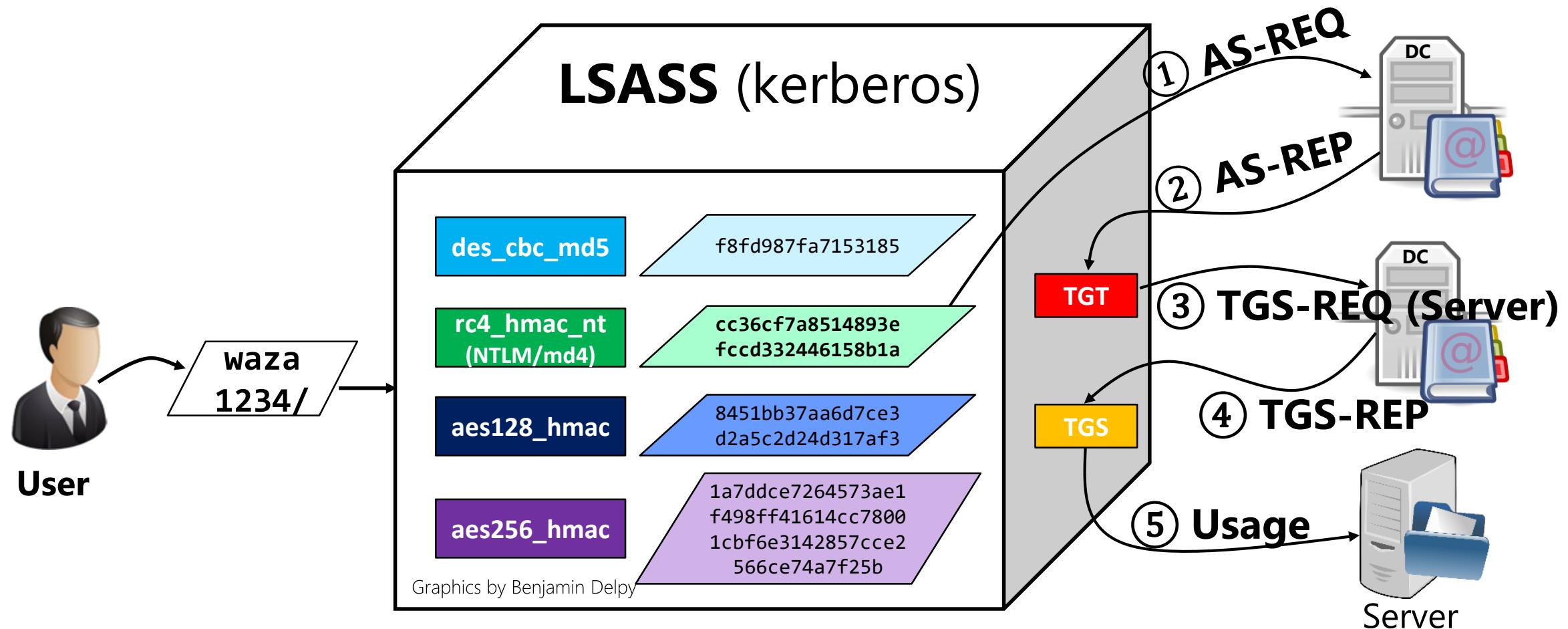


# Microsoft ATA topology



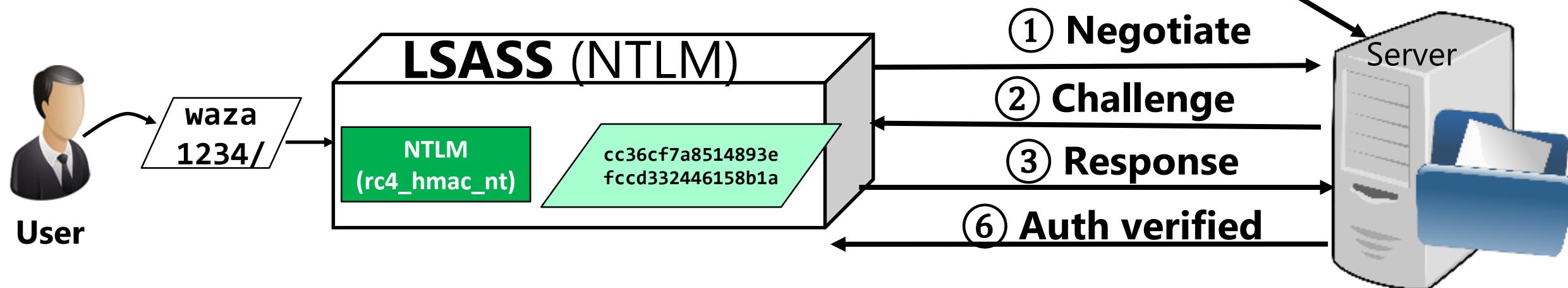
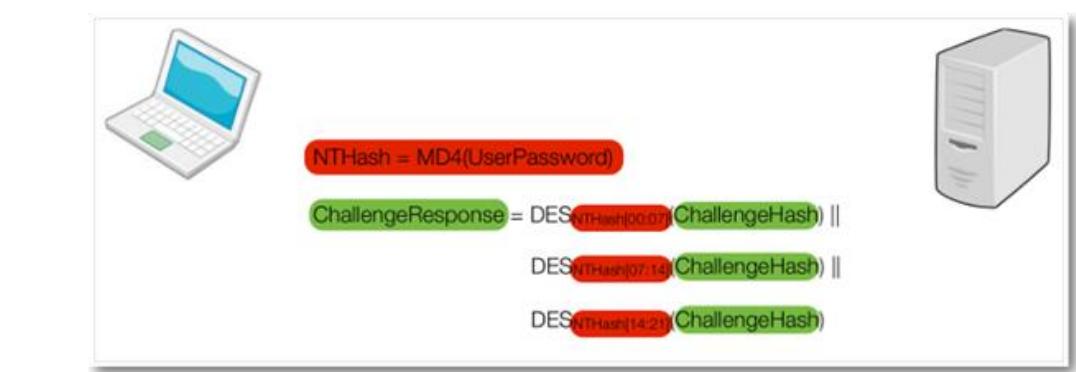
# Kerberos Authentication

- Windows default authentication (+ authorization) protocol



# NTLM Authentication

- Authentication
- Authorization



# Lateral Movement Reconnaissance

# Lateral Movement

- Attackers' mission
- Get from **HERE**:
  - The gullible user who clicked the phishing email
  - Not always the manager ☺
  - Probably low privileged
- To **THERE**:
  - Full domain dominance
  - Control the Domain Controller



# How to get from HERE to THERE?

- A map! (CS: Graph)
- Cities (CS: Nodes)
  - Computers and logon user
- Roads (CS: Edges)
  - Computer and users permissions
- Computer A → Computer B
  - Logged on users in computer A have code execution permissions on Computer B



# Building the map

- To build the map attackers need to know:
  - Cities: Where users are logged-on
  - Roads: User's permissions to computers
  - Destination: Who are the Domain Admins
- Knowledge must be gained with just a low privileged user account
- "Reconnaissance": Gaining knowledge on adversary in a hostile environment



# Logged-on User Recon

- SMB service can be remotely queried for active sessions
  - Returns: IP address, User
  - Implemented in NetSess tool (others)
  - On the wire SRVSVC protocol
  - Required Permissions: Any domain user
- Every logged-on user fetches Group Policy (GP) from DC
  - On logon and periodically (every ~1.5 hour)
  - GP is a bunch of files, sent over SMB
- 1.5 hour of periodic sampling of DC is enough to find all currently logged-on users' computers

SRVSVC 350 NetSessEnum request

```
C:\Research>NetSess.exe win-2008r2 /full
NetSess V02.00.00cpp Joe Richards <joe@joeware.net> January 2004
Enumerating Host: win-2008r2
Client          User Name      Client Type      Opens   Time
Idle Time Transport
-----
\\10.0.0.2        theadmin
0:00 000:00:00               1  000:0
Total of 1 entries enumerated
```

# Computer's Local Admin Recon

- PS cmdlet
  - 'Get-NetLocalGroup'
  - PowerSploit by @mattifestation
  - <https://github.com/PowerShellMafia/PowerSploit>
- Can list local groups & users
- Queries the Computer over SAMR protocol
- Required Permissions: Any domain user

SAMR	222	GetMembersInAlias request
SAMR	362	GetMembersInAlias response

PS C:\Users\DomainUser2> Get-NetLocalGroup -ComputerName Client1 -ListGroups			
Server	Group	SID	Description
Client1	Access Control Assistance ...	S-1-5-32-579	Members of this group can ...
Client1	Administrators	S-1-5-32-544	Administrators have comple...
Client1	Backup Operators	S-1-5-32-551	Backup Operators can over...
Client1	Cryptographic Operators	S-1-5-32-569	Members are authorized to ...
Client1	Distributed COM Users	S-1-5-32-562	Members are allowed to lau...
Client1	Event Log Readers	S-1-5-32-573	Members of this group can ...
Client1	Guests	S-1-5-32-546	Guests have the same acces...
Client1	Hyper-V Administrators	S-1-5-32-578	Members of this group have...
Client1	IIS_IUSRS	S-1-5-32-568	Built-in group used by Int...

# Users + Group Membership Recon

- Simple command line
- Full enumeration
  - Net User /domain
  - Net Group /domain
- Specific entity info
  - Net user /domain <user name>
  - Net group /domain <group name>
- Queries the DC over SAMR protocol
- Required Permissions: Any domain user

```
C:\>net user /domain
The request will be processed at a domain controller for domain redacted.corp.fernwick.com.

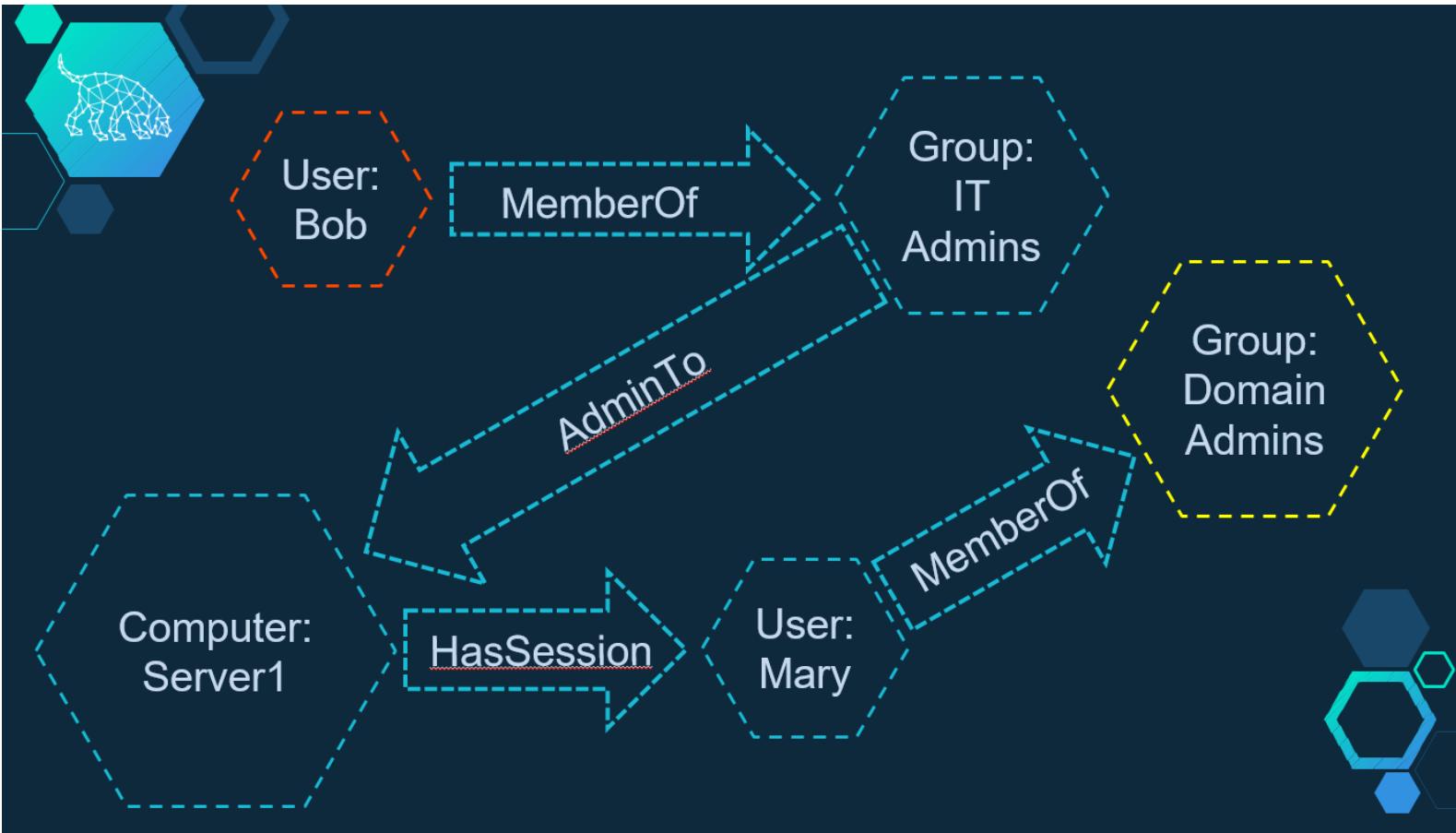
User accounts for \\192.168.1.16.redacted.corp.fernwick.com
-----
```

Account name	Type	Full name	Comment	Last logon
Administrator	User			2019-08-20 12:30:00
Guest	User			2019-08-20 12:30:00
PowerUser	User			2019-08-20 12:30:00
Domain Admins	Group			2019-08-20 12:30:00
Domain Users	Group			2019-08-20 12:30:00
Domain Guests	Group			2019-08-20 12:30:00
PowerUsers	Group			2019-08-20 12:30:00
Administrators	Group			2019-08-20 12:30:00
Administrators\$	Group			2019-08-20 12:30:00
PowerUsers\$	Group			2019-08-20 12:30:00
Administrators@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
PowerUsers@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Guests@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Domain Admins@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Domain Guests@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
PowerUsers@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Administrators@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Guests@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
PowerUsers\$@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Administrators\$@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Administrators@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
PowerUsers@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Guests@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
PowerUsers\$@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00
Administrators\$@redacted.corp.fernwick.com	Group			2019-08-20 12:30:00

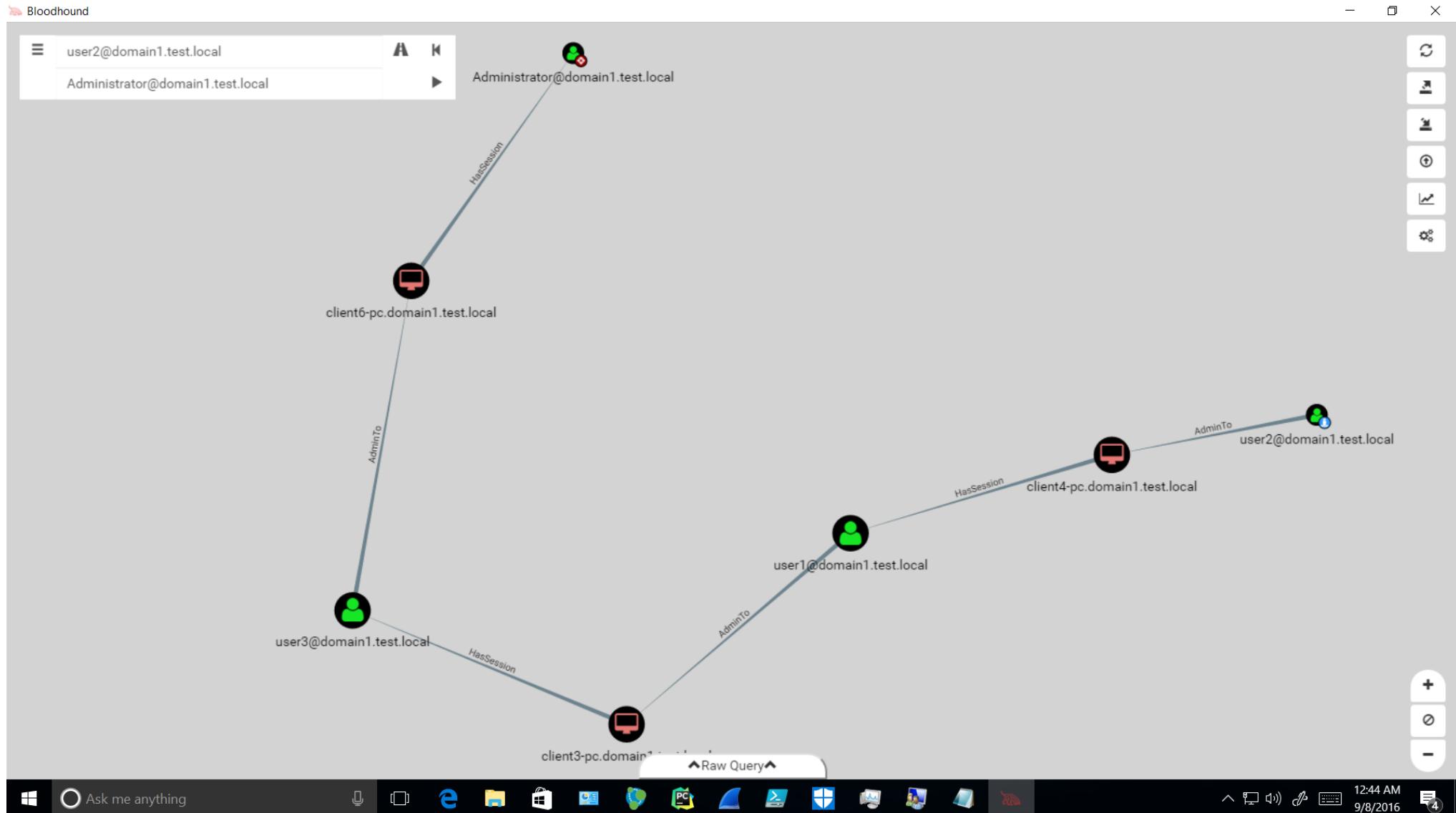
Info
Connect5 request
Connect5 response
EnumDomains request
EnumDomains response
LookupDomain request
LookupDomain response
OpenDomain request
OpenDomain response
EnumDomainUsers request
EnumDomainUsers response
Close request
Close response
Close request
close response

# Putting it All Together: BloodHound

- BloodHound: developed by @\_wald0, @CptJesus, and @harmj0y.
- <https://github.com/adaptivethreat/BloodHound>

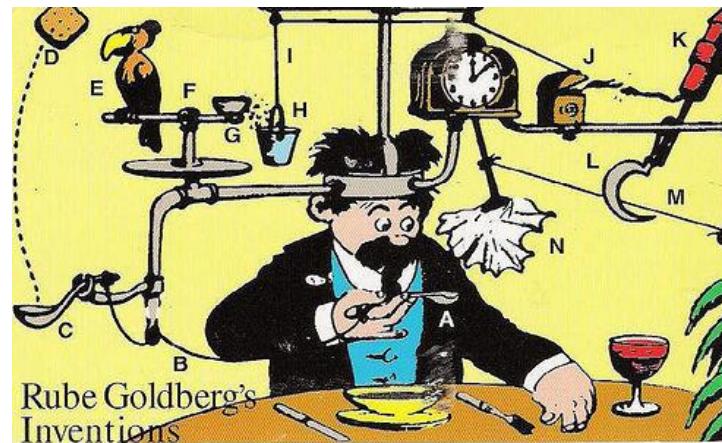


# BloodHound's Shortest Path Functionality



# Imagine: Automatic Internal Network Campaign

- Attackers launch a massive phishing email campaign
  - A single low privileged domain user Clicks phishing email
  - gets infected with a malware
- The malware *automatically* executes a “bloodhound” style recon
  - Computes shortest path to Domain Admin
- The malware *automatically* do Lateral Movement all the way to domain admin
- The malware *automatically* downloads all users’ domain keys using DC-SYNC
  - All domain keys are sent to attackers

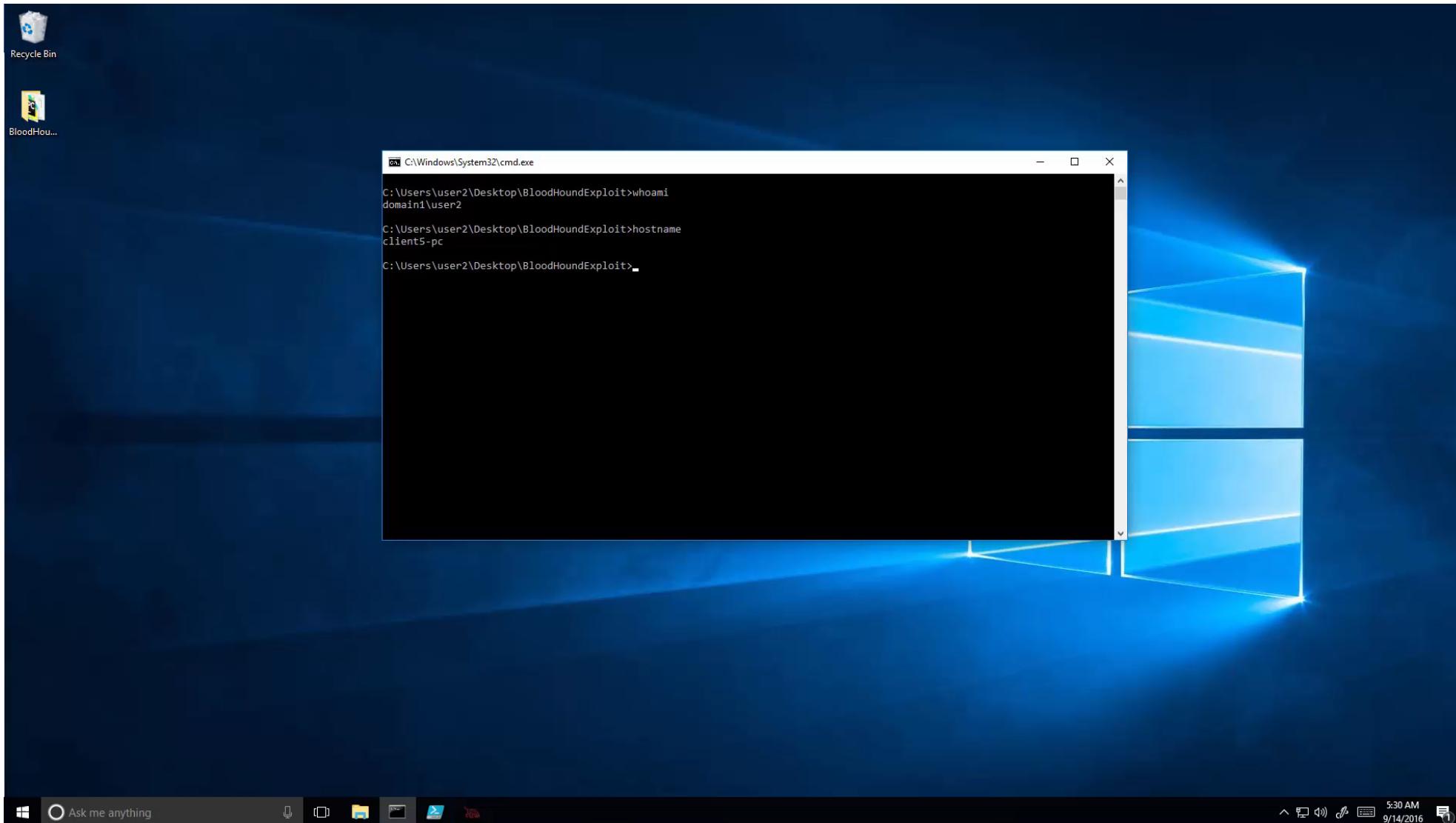


# Now Open Your Eyes.. 😊

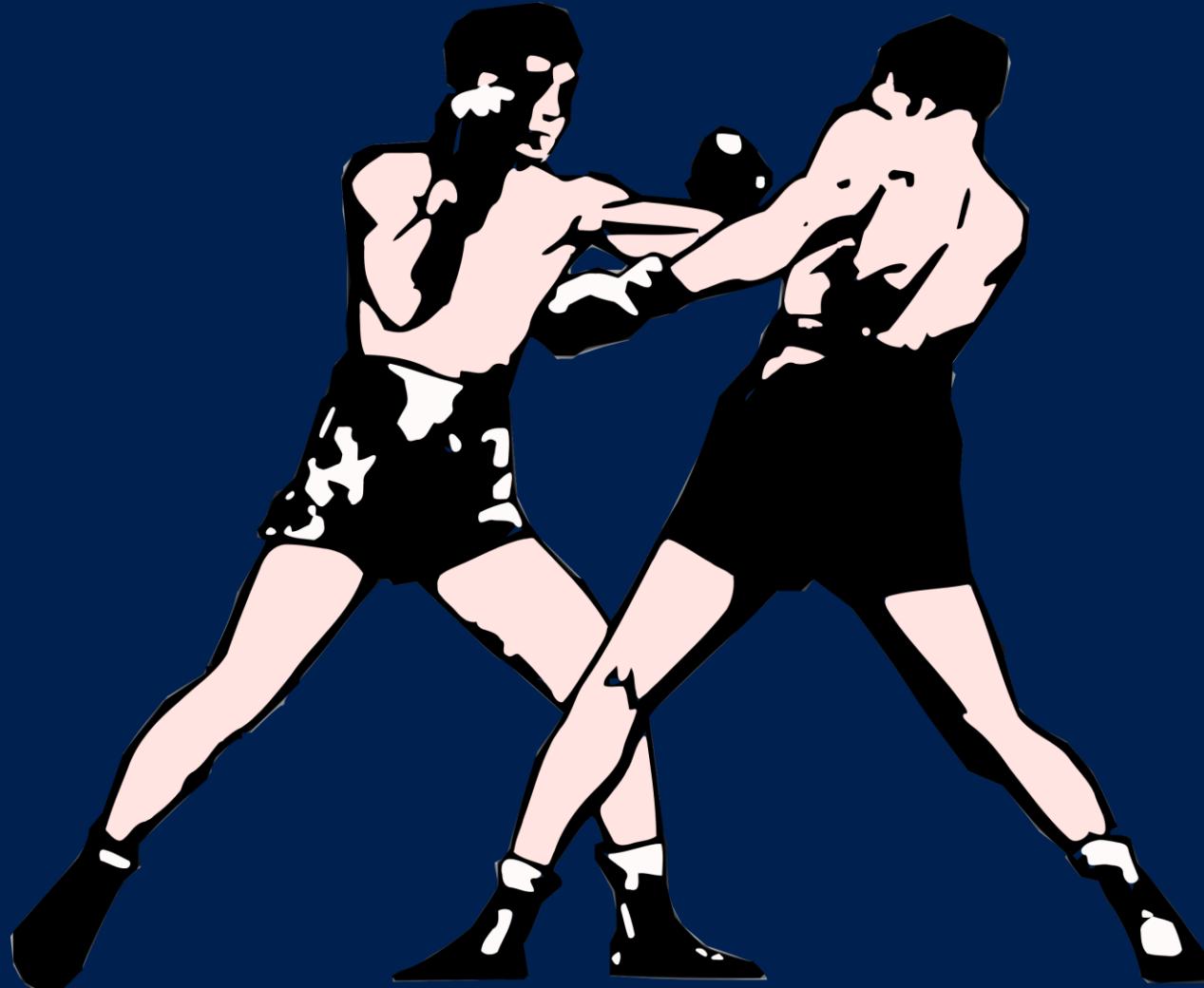
- Automatic Lateral Movement tool
- Developed by MicrosoftATA researcher @talthemaor
- Gets a bloodhound exported graph (JSON) as “attack plan” input
- Executes the attack plan
  - Remote Code Execution (RCE) via Remote PS
  - Credential harvesting via Mimikatz



# DEMO!



# Lateral Movement Reconnaissance: Defense



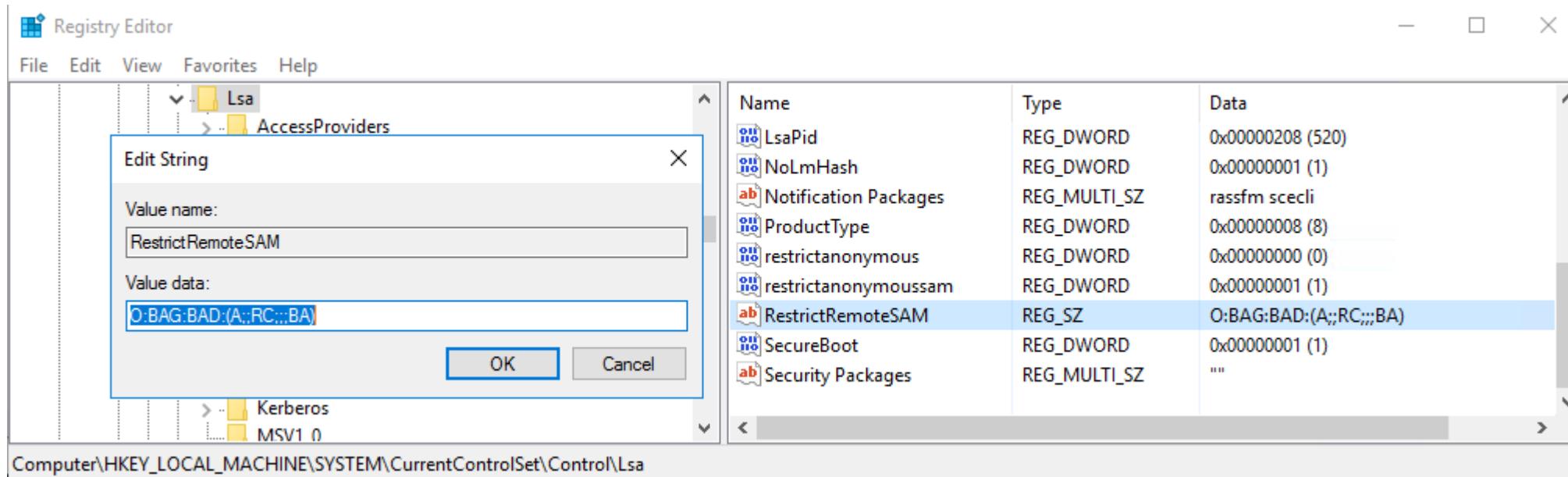
# “SAMR Moved On” Hardening #1

- Win10 allows admins to control SAMR Recon
  - Registry: HKLM\System\CurrentControlSet\Control\Lsa\RestrictRemoteSAM
  - GP: “Network Access: Restrict clients allowed to make remote calls to SAM”

Win version	Who can query SAMR by default	Can default be changed
< Win10	Any domain user	No
Win10	Any domain user	Yes (only via registry)
> Win10 (e.g. anniversary)	Only local administrators	Yes (registry or GPO)

# “SAMR Moved On” Hardening #2

- Windows Server 2016 allows admins to control SAMR Recon on DC
- Net User/Group queries on Domain can be limited!

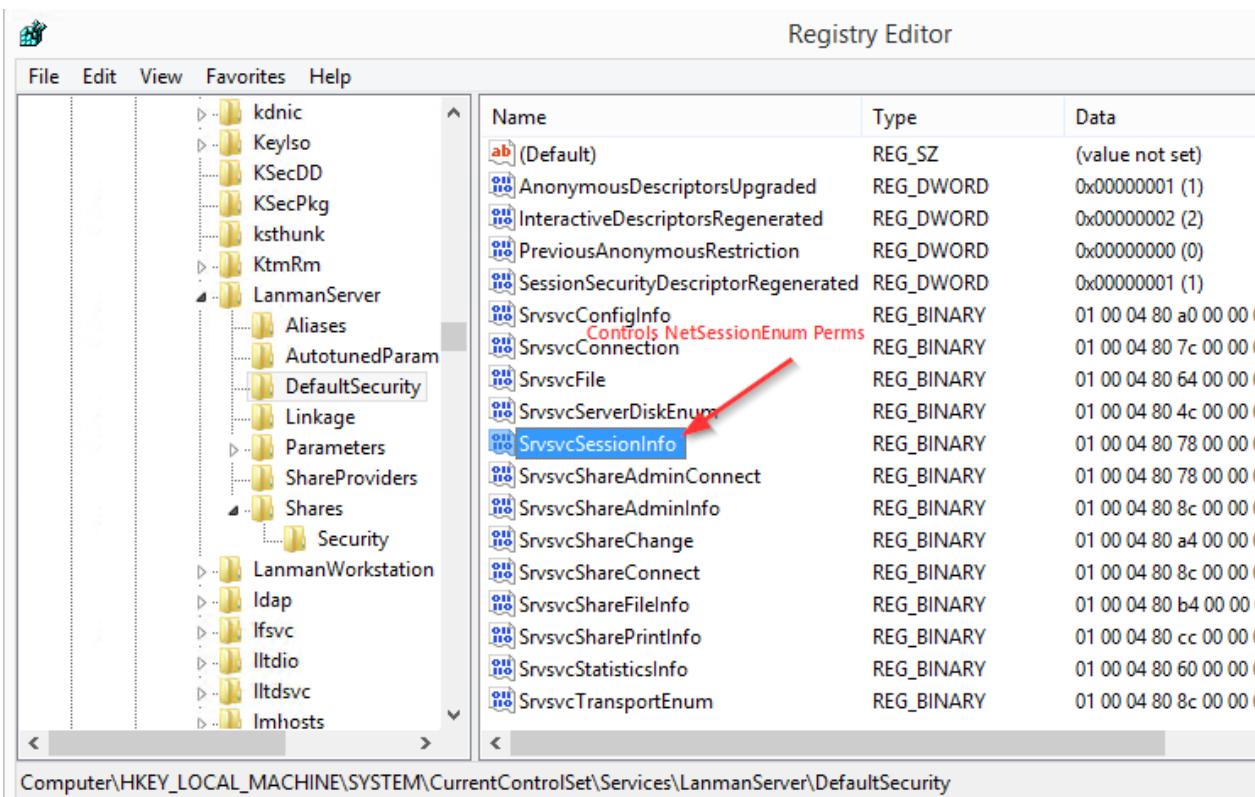


```
C:\Users\user1>net group "Domain Admins" /Domain
The request will be processed at a domain controller for domain domain2016.local
-
System error 5 has occurred.
Access is denied.

C:\Users\user1>
```

# “Net Cease” Hardening

- NetSess API access can be controlled by ACL in the Registry!
- Remove “Authenticated Users” group manually, or use our tool
  - <https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dc5b>



```
C:\Tools\NetSsess>NetSess.exe 192.168.0.3
NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004

Enumerating Host: 192.168.0.3
Client           User Name      Time     Idle Time
-----+-----+-----+-----+-----+
\\\\\\192.168.0.2   spAdmin    002:17:35  000:03:39
\\\\\\192.168.0.1   user3     000:00:03  000:00:02
\\\\\\192.168.0.1   user3     000:00:02  000:00:02
\\\\\\192.168.0.1   user3     000:00:02  000:00:02
\\\\\\192.168.0.1   user3     000:00:02  000:00:02
\\\\\\192.168.0.2   spAdmin    000:00:00  000:00:00

Total of 6 entries enumerated

C:\Tools\NetSsess>NetSess.exe 192.168.0.3
NetSess V02.00.00cpp Joe Richards (joe@joeware.net) January 2004

Enumerating Host: 192.168.0.3
Client           User Name      Time     Idle Time
-----+-----+-----+-----+
Error: NetSessionEnum (5) Access is denied.

Total of 0 entries enumerated
```

# Detection (Microsoft ATA): NetSess Recon

**Reconnaissance using SMB Session Enumeration**  
SMB session enumeration attempts were successfully performed from USER1-PC against DC1, exposing 4 accounts.

Note  Share  Export to Excel  Details  Input  Open

**Session Enumeration**

**Exposed Accounts (4)**

<input type="checkbox"/>	SECRETS-DB\$ on 192.168.0.210
<input type="checkbox"/>	user1 on 192.168.0.1
<input type="checkbox"/>	APP2\$ on 192.168.0.5
<input type="checkbox"/>	user2 on 192.168.0.5

**Recommendations**

- Disconnect USER1-PC from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Verify that all enumerated accounts use a strong password.

# Detection (MicrosoftATA): SAMR Recon

**Reconnaissance using directory services enumeration**

The following directory services enumerations using SAMR protocol were attempted against DC5 from CLIENT4:

- Successful enumeration of all users in domain2.test.local by user4

Note  Share  Export to Excel  Details  Input  Open

**Directory Services Enumeration**

Operations (1)

- Enumerate all users in domain2.test.local

**Recommendations**

- Disconnect CLIENT4 from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

# Detection (MicrosoftATA): Abnormal Access

5:24 AM > 4:24 PM

Monday, July 18, 2016

## Suspicion of identity theft based on abnormal behavior

user2 exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Requested access to 6 abnormal resources.

 Note  Share  Export to Excel  Details  Input

 Open

 user2  
Software Engine...



15 normal  
computers

Accessed



25 normal  
resources



6 abnormal  
resources

## Recommendations

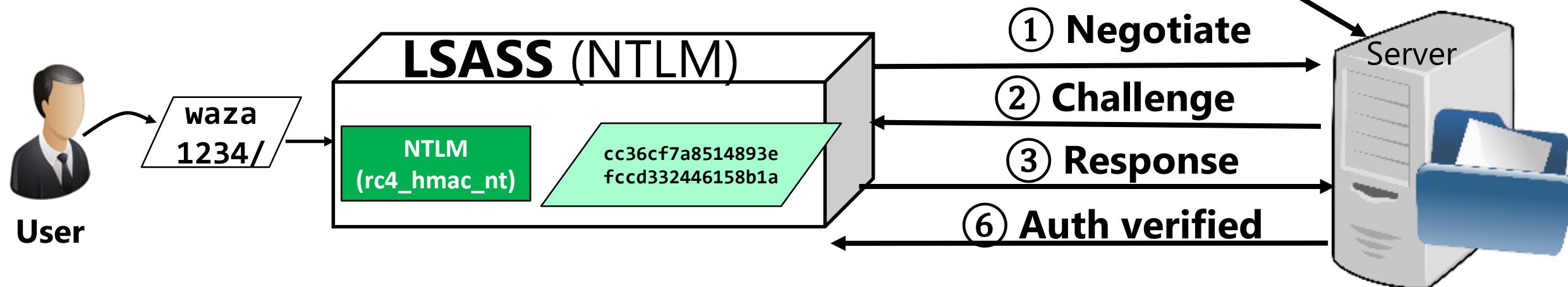
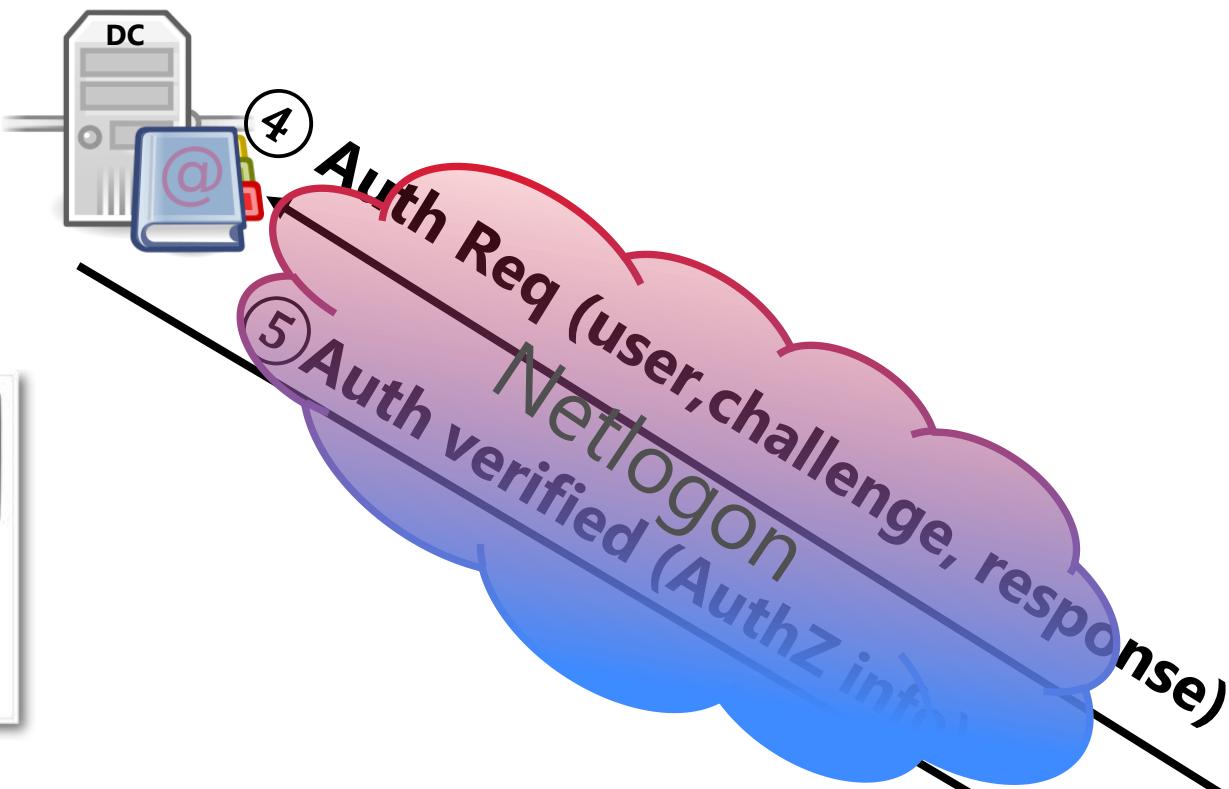
- Contact user2 and investigate if the user has logged in to abnormal computers and accessed abnormal resources.

# Cyber Judo with NetSess



# NTLM Authentication

- Authentication
- Authorization



# NTLM in attacks

- NTLM is the essence
  - NTLM authentication is very relevant to Pass-the-Hash attacks
  - NTLM relay attack
- NTLM by default:
  - Many attack tools did not “upgrade” to Kerberos
  - Access by IP (e.g. “\\10.0.0.1\C\$”) defaults to NTLM (no SPN for Kerberos)
  - Kerberos failures (e.g. port 88 is blocked in FireWall)

# NTLM Visibility Problem

- Netlogon messages are encrypted ☹
  - The opcode is visible, but parameters are encrypted
- A security device eavesdropping to DC traffic only learns
  - “Someone performed NTLM logon to a computer”
- Missing info
  - Which user?
  - From which computer?



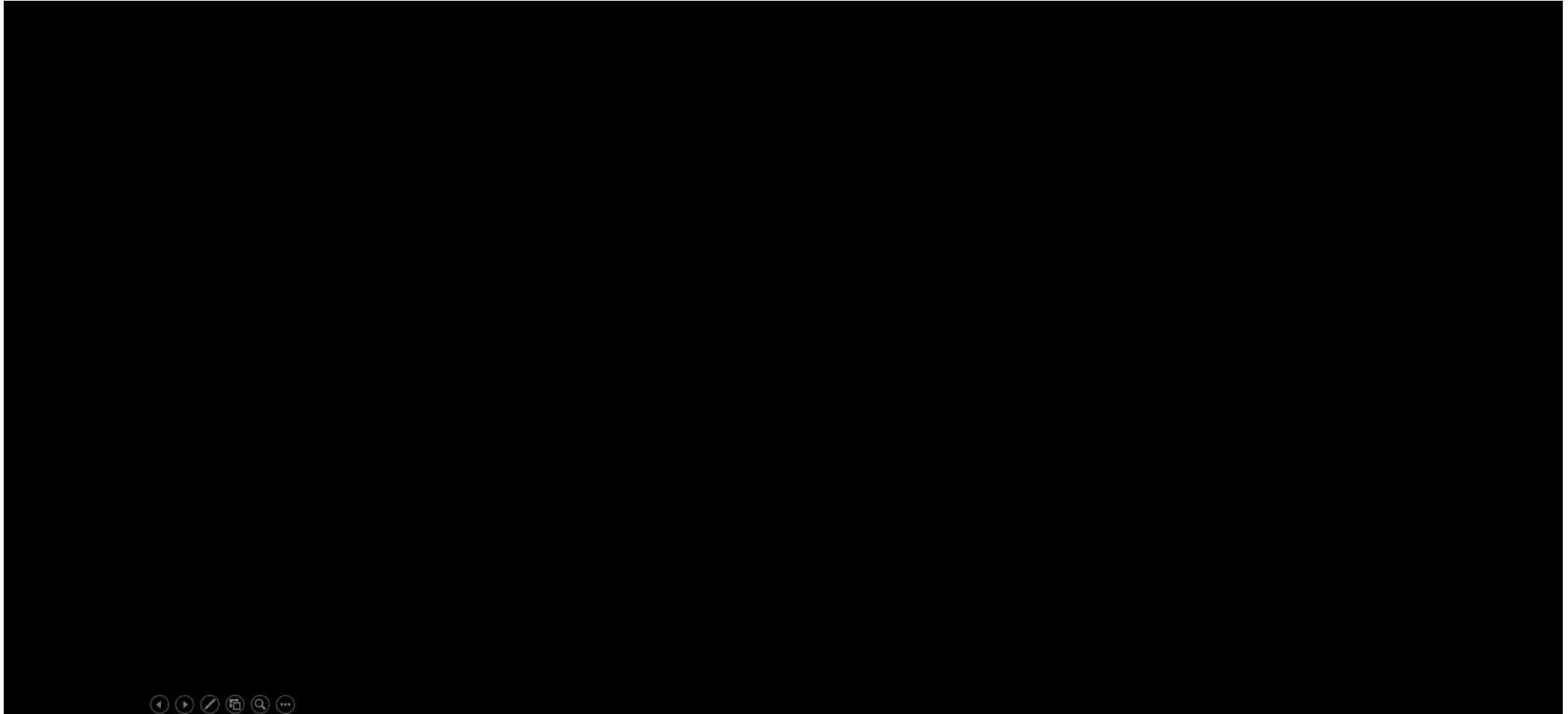
RPC NETLOGON	NetrLogonSamLogonWithFlags request
>	Frame 28: 1090 bytes on wire (8720 bits), 1090 bytes captured (8720 bits) on interface 0
>	Ethernet II, Src: Microsoft (00:15:5d:c5:46:b0), Dst: Microsoft (00:15:5d:c5:46:9e)
>	Internet Protocol Version 6, Src: daf::5, Dst: daf::200
>	Transmission Control Protocol, Src Port: 49754 (49754), Dst Port: 49158 (49158), Seq: 222, Ack: 223
>	Distributed Computing Environment / Remote Procedure Call (DCE/RPC) Request, Fragment: Segment 1 of 1
▼	Microsoft Network Logon, NetrLogonSamLogonWithFlags
	Operation: NetrLogonSamLogonWithFlags (45)
	<a href="#">[Response in frame: 29]</a>
	Encrypted stub data: 0cc2bb6864ebd473e2a7a883b73abe9964612ac424cf6f37...

# NTLM Visibility Solution

- When observing a relevant successful NETLOGON message
  - Extract source IP
- Perform NetSess Recon on that IP
- Extract original user information from NetSess results
- Win! (at least for SMB)



# Demo!



# Cyber Judo with SAMR



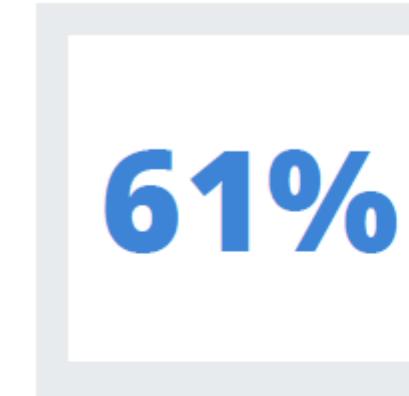
# Local User in Attacks

- Very relevant
  - Identical passwords problem
  - PtH against local admins is successfully Used in 60% of Praetorian's pen-tests

## Local Administrator Attacks (aka Pass the Hash)

### Summary of the Attack

Organizations often configure all systems with the same Local Admin password. If an attacker is able to compromise the LM/NT hash representation of the password, then the attacker can use the hash to authenticate and execute commands on other systems that have the same password. This is exacerbated by the fact that the attacker only needs the LM/NT hashes; the attacker doesn't need to crack the password at all. Having a very good understanding of this attack, how it works, and what it looks like from a defensive perspective is the best way to be able to properly mitigate it.



**Attack Vector #3:** Out of 100 internal pentests, Pass the Hash was used to compromise the environment 61% of the time.

Source: Praetorian

# Local Users Attacks in the Wild

<https://twitter.com/JohnLaTwC/status/777569424156921856>



John Lambert  
@JohnLaTwC



Following

Common post-compromise steps by RDP brute  
forcers on #Azure IaaS. Spot them w/ sysmon  
or #AzureSecurityCenter. #DFIR

```
//They don't like those pesky "unauthorized use is prohibited" dialogs during login
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticecaption /f
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v legalnoticetext /f

//They don't like IE and install Chrome & FF :/
"C:\Program Files (x86)\Google\Chrome\Application\52.0.2743.116\Installer\chromstp.exe" --configure-user-settings --verbose-logging --
system-level --multi-install --chrome
"C:\Users<user>\Downloads\Firefox Setup Stub 48.0.2.exe"

//They create backdoor admin accounts
net.exe user admin kast43 /ADD /ACTIVE:YES /EXPIRES:NEVER
/FULLNAME:admin
net.exe localgroup Administrators admin /ADD

net user ASPNET crystal123!@# /add
net localgroup Administrators ASPNET /add

net user __VMware_Conv_SA__ crystal123!@# /add
net localgroup Administrators __VMware_Conv_SA__ /add
```

# Local User Visibility Problem

- Local users authentication is... well... Local
- A network security device cannot see it ☹



# Local Users Visibility Solution

- Periodically query Local Users over SAMR
  - Users Info
  - Group membership
- To discover:
  - Abnormal login patterns
  - BruteForce attempts
  - Privileged group modifications
  - Password configuration issues
- And much more...

```
test <1004>/LastPassChange: 2016-07-05 11:13:38.657533
USER1 <1001>/FullName:
USER1 <1001>/UserComment:
USER1 <1001>/PrimaryGroupId: 513
USER1 <1001>/BadPasswordCount: 0
USER1 <1001>/LogonCount: 3
USER1 <1001>/LastLogon: 2016-08-29 09:54:53.853097
USER1 <1001>/LastPassChange: 2016-08-29 08:42:47.516191
Exl_Passwd_Cntr=1
```



# Local User Logon Anomalies Detection

- Dormant Local User Logon:
  - Compare current last logon time to previous last logon time
  - If user never logged-on, time is 0 ("1.1.1601 00:00:00")

```
newuser <1004>/FullName: New User  
newuser <1004>/UserComment:  
newuser <1004>/PrimaryGroupId: 513  
newuser <1004>/BadPasswordCount: 0  
newuser <1004>/LogonCount: 0  
newuser <1004>/LastLogon: 1601-01-01 00:00:00
```



```
last <1004>/LastLogonChange: 1601-01-01 00:00:00  
newuser <1004>/FullName: New User  
newuser <1004>/UserComment:  
newuser <1004>/PrimaryGroupId: 513  
newuser <1004>/BadPasswordCount: 0  
newuser <1004>/LogonCount: 1  
newuser <1004>/LastLogon: 2016-09-15 12:42:12.675018
```

- Local User Brute Force
  - Compare current BadPwdCount with previous

```
Administrator <500>/FullName:  
Administrator <500>/UserComment:  
Administrator <500>/PrimaryGroupId: 513  
Administrator <500>/BadPasswordCount: 0  
Administrator <500>/LogonCount: 7
```



```
last user: 00:00z, rid: 100z  
Administrator <500>/FullName:  
Administrator <500>/UserComment:  
Administrator <500>/PrimaryGroupId: 513  
Administrator <500>/BadPasswordCount: 12964  
Administrator <500>/LogonCount: ?
```

# User Added to Privileged Local Group Detection

```
PS C:\Windows\system32> Get-NetLocalGroup -ComputerName CLIENT2

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/Administrator
SID          : S-1-5-21-2855241813-3116034789-286929080-500
Disabled     : True
IsGroup      : False
IsDomain    : False
LastLogin   : 4/13/2014 5:37:53 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/testadmin
SID          : S-1-5-21-2855241813-3116034789-286929080-1001
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin   : 8/5/2015 2:51:48 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/USER2
SID          : S-1-5-21-2855241813-3116034789-286929080-1002
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin   : 8/31/2016 11:25:41 AM

Server      : CLIENT2
AccountName : VLAB1.com/Domain Admins
SID          : S-1-5-21-3383964581-1309953776-2693364552-512
Disabled     : False
IsGroup      : True
IsDomain    : True
LastLogin   :

Server      : CLIENT2
AccountName : VLAB1.com/USER2
SID          : S-1-5-21-3383964581-1309953776-2693364552-1106
Disabled     : False
IsGroup      : False
IsDomain    : True
LastLogin   : 9/15/2016 5:19:55 PM
```



```
Server      : CLIENT2
AccountName : VLAB1/CLIENT2/Administrator
SID          : S-1-5-21-2855241813-3116034789-286929080-500
Disabled     : True
IsGroup      : False
IsDomain    : False
LastLogin   : 4/13/2014 5:37:53 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/testadmin
SID          : S-1-5-21-2855241813-3116034789-286929080-1001
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin   : 8/5/2015 2:51:48 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/USER2
SID          : S-1-5-21-2855241813-3116034789-286929080-1002
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin   : 8/31/2016 11:25:41 AM

Server      : CLIENT2
AccountName : VLAB1.com/Domain Admins
SID          : S-1-5-21-3383964581-1309953776-2693364552-512
Disabled     : False
IsGroup      : True
IsDomain    : True
LastLogin   :

Server      : CLIENT2
AccountName : VLAB1.com/USER2
SID          : S-1-5-21-3383964581-1309953776-2693364552-1106
Disabled     : False
IsGroup      : False
IsDomain    : True
LastLogin   : 9/15/2016 5:19:55 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/MaliciousUser
SID          : S-1-5-21-2855241813-3116034789-286929080-1005
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin   :
```

# Users Removed from Privileged Group Detection

```
PS C:\Windows\system32> Get-NetLocalGroup -ComputerName CLIENT2

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/Administrator
SID         : S-1-5-21-2855241813-3116034789-286929080-500
Disabled    : True
IsGroup     : False
IsDomain   : False
LastLogin   : 4/13/2014 5:37:53 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/testadmin
SID         : S-1-5-21-2855241813-3116034789-286929080-1001
Disabled    : False
IsGroup     : False
IsDomain   : False
LastLogin   : 8/5/2015 2:51:48 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/USER2
SID         : S-1-5-21-2855241813-3116034789-286929080-1002
Disabled    : False
IsGroup     : False
IsDomain   : False
LastLogin   : 8/31/2016 11:25:41 AM

Server      : CLIENT2
AccountName : VLAB1.com/Domain Admins
SID         : S-1-5-21-3383964581-1309953776-2693364552-512
Disabled    : False
IsGroup     : True
IsDomain   : True
LastLogin   :

Server      : CLIENT2
AccountName : VLAB1.com/USER2
SID         : S-1-5-21-3383964581-1309953776-2693364552-1106
Disabled    : False
IsGroup     : False
IsDomain   : True
LastLogin   : 9/15/2016 5:19:55 PM
```



```
Server      : CLIENT2
AccountName : VLAB1/CLIENT2/Administrator
SID         : S-1-5-21-2855241813-3116034789-286929080-500
Disabled    : True
IsGroup     : False
IsDomain   : False
LastLogin   : 4/13/2014 5:37:53 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/testadmin
SID         : S-1-5-21-2855241813-3116034789-286929080-1001
Disabled    : False
IsGroup     : False
IsDomain   : False
LastLogin   : 8/5/2015 2:51:48 PM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/USER2
SID         : S-1-5-21-2855241813-3116034789-286929080-1002
Disabled    : False
IsGroup     : False
IsDomain   : False
LastLogin   : 8/31/2016 11:25:41 AM

Server      : CLIENT2
AccountName : VLAB1/CLIENT2/MaliciousUser
SID         : S-1-5-21-2855241813-3116034789-286929080-1005
Disabled    : False
IsGroup     : False
IsDomain   : False
LastLogin   :
```

# Local User Password Configuration Issues

- “Shallow copied” Local users:
  - E.g. Created via HD copy, VM export, etc.
  - Shares the same password
  - Can be identified via same username, password change time

```
PS C:\Users\user1.TESTDOMAIN.000> Get-NetLocalGroup -ComputerName "Client3Prep" -GroupName "Guests"

ComputerName : Client3Prep
AccountName : TESTDOMAIN\Client3Prep/Guest
SID          : S-1-5-21-2937651619-4167467795-303580696-501
Description   : Built-in account for guest access to the computer/domain
Disabled     : True
IsGroup      : False
IsDomain    : False
LastLogin    :
PwdLastSet  : 9/19/2016 11:24:21 AM
PwdExpired   : False
UserFlags    : 66147

ComputerName : Client3Prep
AccountName : TESTDOMAIN\Client3Prep/test_user
SID          : S-1-5-21-2937651619-4167467795-303580696-1006
Description   :
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin    :
PwdLastSet  : 9/13/2016 3:30:29 PM
PwdExpired   : False
UserFlags    : 66049

ComputerName : Client3Prep
AccountName : TESTDOMAIN\Client3Prep/new_user
SID          : S-1-5-21-2937651619-4167467795-303580696-1008
Description   :
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin    :
PwdLastSet  : 9/18/2016 11:46:17 AM
PwdExpired   : False
UserFlags    : 66049
```

```
PS C:\Users\user1.TESTDOMAIN.000> Get-NetLocalGroup -ComputerName "client3" -GroupName "Guests"

ComputerName : client3
AccountName : TESTDOMAIN/client3/Guest
SID          : S-1-5-21-473845342-2774817237-2297341088-501
Description   : Built-in account for guest access to the computer/domain
Disabled     : True
IsGroup      : False
IsDomain    : False
LastLogin    :
PwdLastSet  : 9/18/2016 11:46:47 AM
PwdExpired   : False
UserFlags    : 66147

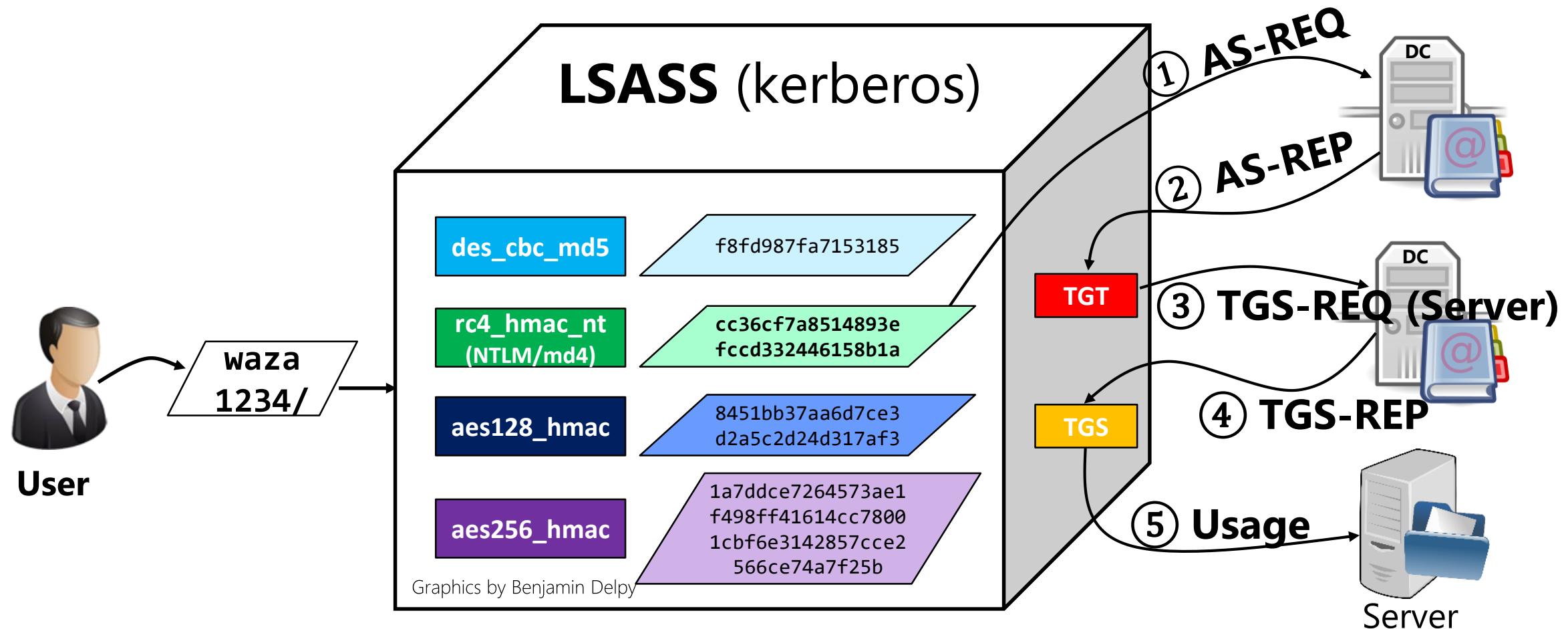
ComputerName : client3
AccountName : TESTDOMAIN/client3/test_user
SID          : S-1-5-21-473845342-2774817237-2297341088-1006
Description   :
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin    :
PwdLastSet  : 9/13/2016 3:30:29 PM
PwdExpired   : False
UserFlags    : 66049

ComputerName : client3
AccountName : TESTDOMAIN/client3/new_user
SID          : S-1-5-21-473845342-2774817237-2297341088-1008
Description   :
Disabled     : False
IsGroup      : False
IsDomain    : False
LastLogin    :
PwdLastSet  : 9/18/2016 11:46:17 AM
PwdExpired   : False
UserFlags    : 66049
```

# Kerberos Error Message Injection

# Kerberos Authentication

- Windows default authentication (+ authorization) protocol



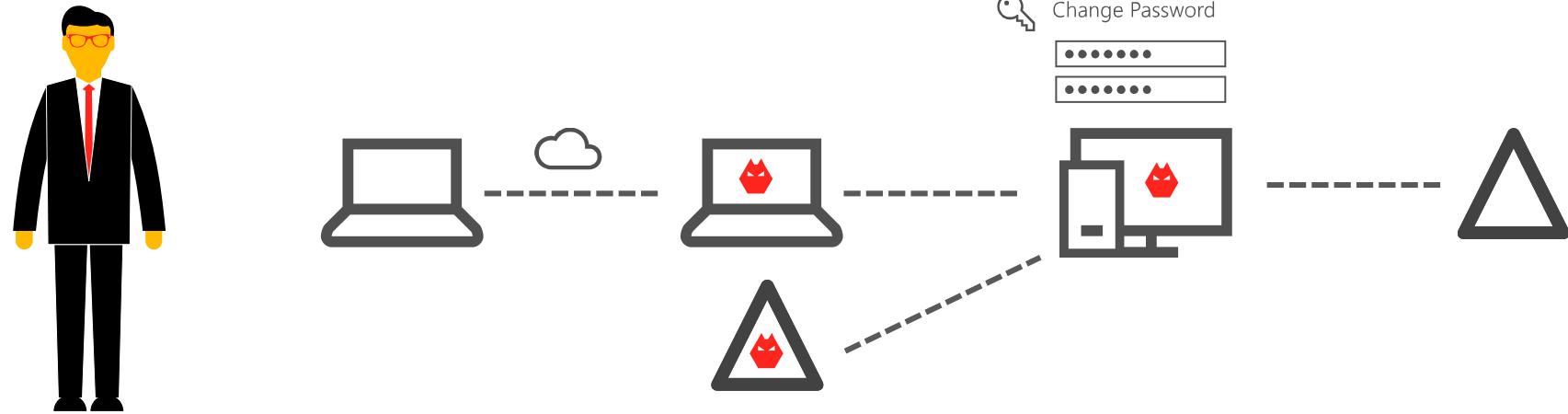
# Malicious Kerberos Error Injection

- A MITM Attacker can cause the following effects by sending the following error messages:
  - Downgrade encryption: KDC\_ERR\_PREAMPT\_REQUIRED
  - Change password: KDC\_ERR\_KEY\_EXPIRED
  - Re-enter password: KDC\_ERR\_TGT\_REVOKED
  - Block users: KDC\_ERR\_CLIENT\_REVOKED

# Password Expired Injection: Remote Butler

- Presented in BlackHat USA 2016 by Tal Be'ery & Chaim Hoch
- Demo: <https://www.youtube.com/watch?v=CSdJ -Phaul>

Evil  
Butler



# Kerberos Encryption Negotiation



User1

waza  
1234/

**LSASS (kerberos)**

des\_cbc\_md5

f8fd987fa7153185

rc4\_hmac\_nt  
(NTLM/md4)

cc36cf7a8514893e  
fccd332446158b1a

aes128\_hmac

8451bb37aa6d7ce3  
d2a5c2d24d317af3

aes256\_hmac

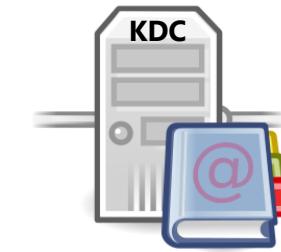
1a7ddce7264573ae1  
f498ff41614cc7800  
1cbf6e3142857cce2  
566ce74a7f25b

① AS-REQ  
Name: user1  
Etype: DES, RC4,  
AES128, AES256

② KERB-ERR  
Pre-auth-REQ  
Etype: RC4,AES  
Salt:user1

③ AS-REQ  
PA-ENC-TS  
Etype:AES

④ AS-REP  
TGT+Enc



user	rc4_hmac_nt	aes256_hmac
Joe	21321...	543..
user1	cc36cf7a	1a7ddc
	...	...
Doe		

# Kerberos Authentication: Over the Wire

```
as-req
pvno: 5
msg-type: krb-as-req (10)
padata: 1 item
PA-DATA PA-PAC-REQUEST
req-body
Padding: 0
kdc-options: 40810010 (forwardable, renewable, canonicalize, renewable-ok)
cname
realm: aorato.research
sname
till: 2037-09-13 02:48:05 (UTC)
rtime: 2037-09-13 02:48:05 (UTC)
nonce: 160211996
etype: 6 items
ENCTYPE: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
ENCTYPE: eTYPE-AES128-CTS-HMAC-SHA1-96 (17)
ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5 (23)
ENCTYPE: eTYPE-ARCFOUR-HMAC-MD5-56 (24)
ENCTYPE: eTYPE-ARCFOUR-HMAC-OLD-EXP (-135)
ENCTYPE: eTYPE-DES-CBC-MD5 (3)
```

```
krb-error
pvno: 5
msg-type: krb-error (30)
stime: 2014-03-10 20:05:07 (UTC)
susec: 165032
error-code: eRR-PREAUTH-REQUIRED (25)
realm: aorato.research
sname
e-data: 30543031a103020113a22a04283026301da003020112a116...
PA-DATA PA-ENCTYPE-INFO2
padata-type: KRB5-PADATA-ETYPE-INFO2 (19)
padata-value: 3026301da003020112a1161b14414f5241544f
ETYPE-INFO2-ENTRY
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
salt: AORATO.RESEARCHbugsb
ETYPE-INFO2-ENTRY
etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
```

```
as-req
pvno: 5
msg-type: krb-as-req (10)
padata: 2 items
PA-DATA PA-ENC-TIMESTAMP
padata-type: KRB5-PADATA-ENC-TIMESTAMP (2)
padata-value: 3041a003020112a23a0438c871bc029b90195c7d2981b0cd...
etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
cipher: c871bc029b90195c7d2981b0cd8e4c98fa5fa747689f86e1...
```

# AES vs. RC4: Key Derivation

- Salting
  - Goal: Same passwords, different users = different keys
  - Create-Key(password + salt)
  - AES uses the username for salt
  - **RC4-HMAC does not have any!**
- “Key Stretching”
  - Goal: increase CPU load per password
  - AES uses PBKDF2= Thousands of SHA rounds
  - **RC4-HMAC does not have any!**

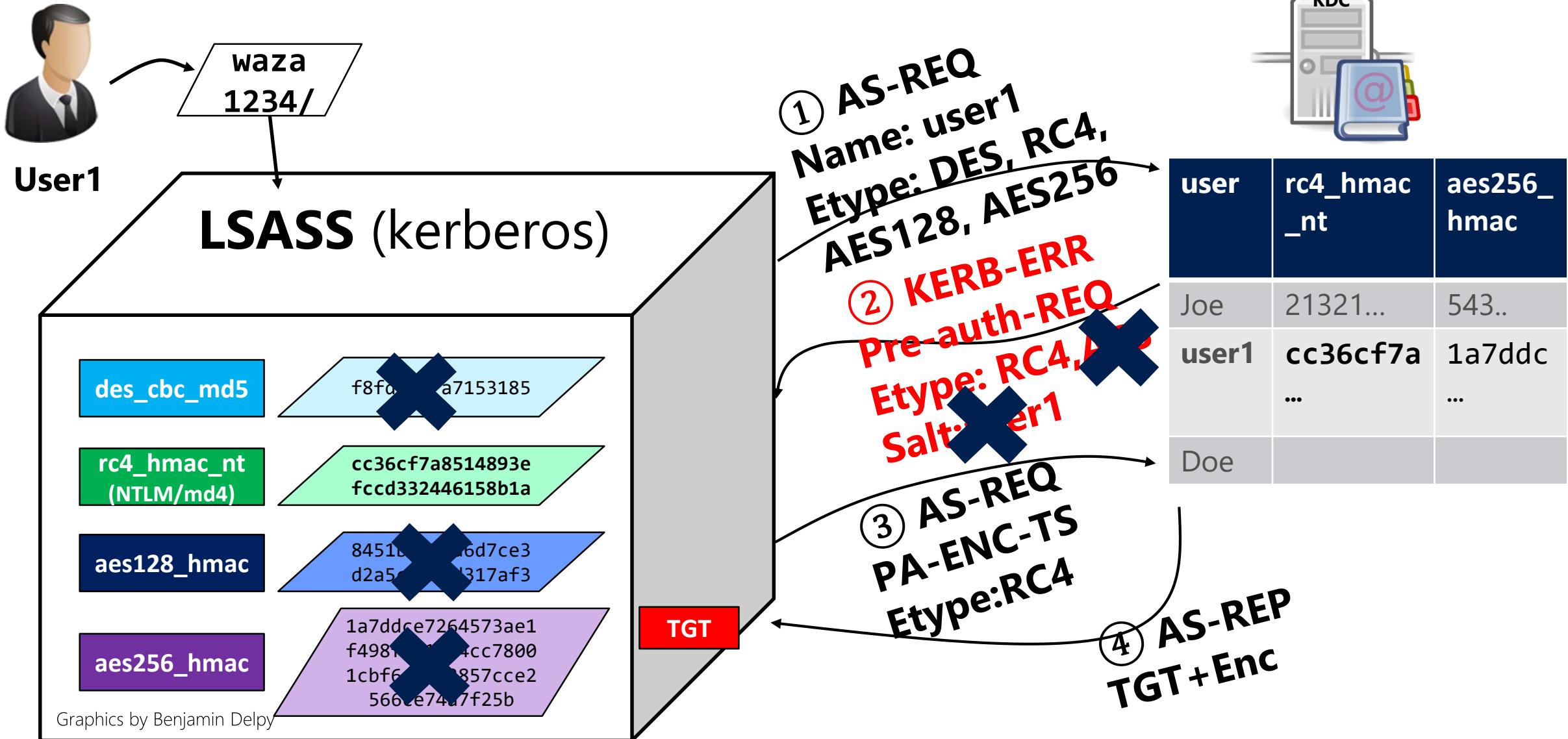


[https://commons.wikimedia.org/wiki/File:Jodsalz\\_mit\\_Fluor\\_und\\_Folsaeure.jpg](https://commons.wikimedia.org/wiki/File:Jodsalz_mit_Fluor_und_Folsaeure.jpg)

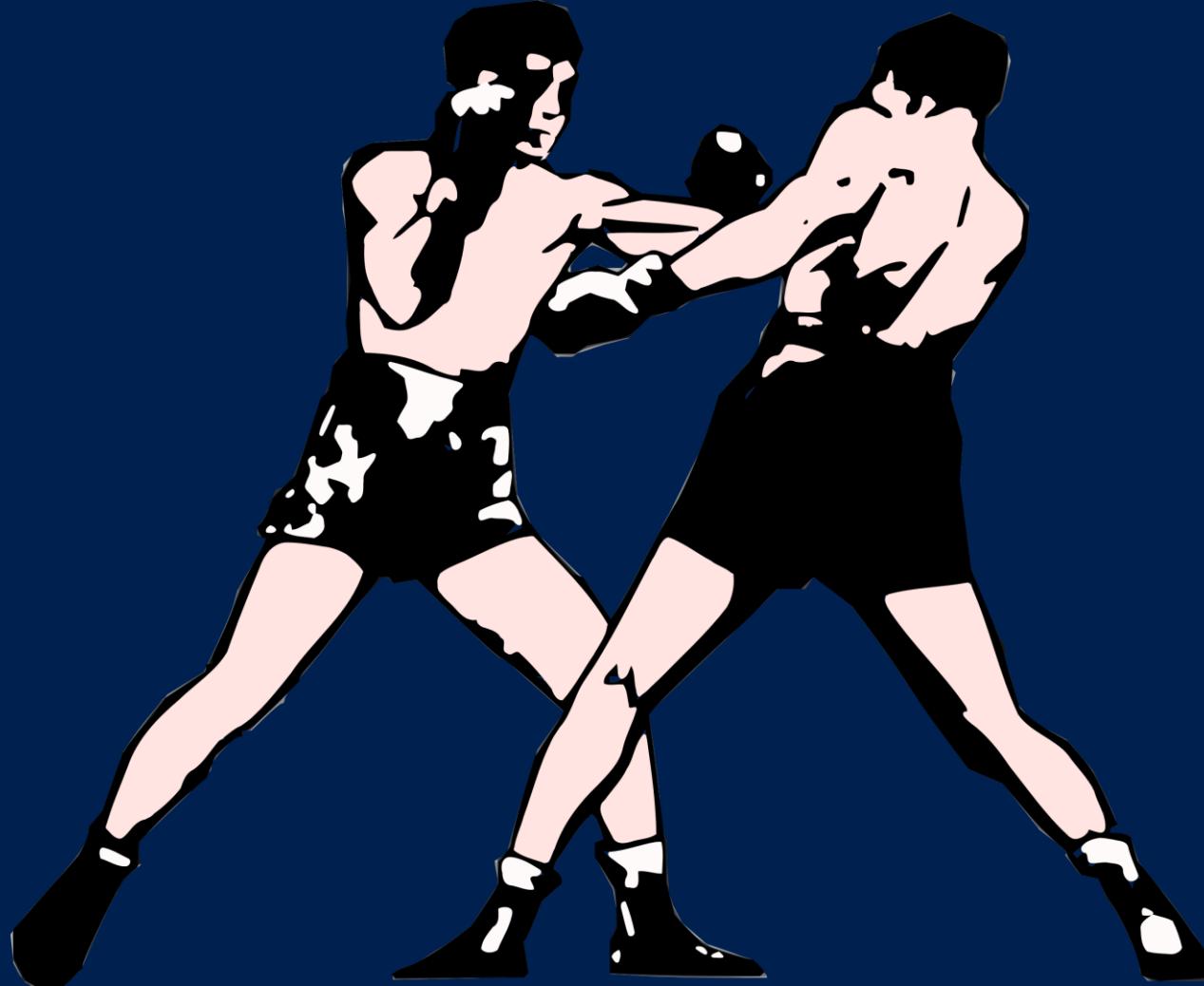
Attacker + RC4 = ❤

- Due to salting, identical passwords create different AES keys for different users
  - Attacker cannot prepare a rainbow table in advance
- Due to “Key Stretching” Brute Force is much more CPU intensive
- Attacker’s Solution: Downgrade to RC4

# Encryption Downgrade Injection Attack



# Kerberos Error Injection: Defense



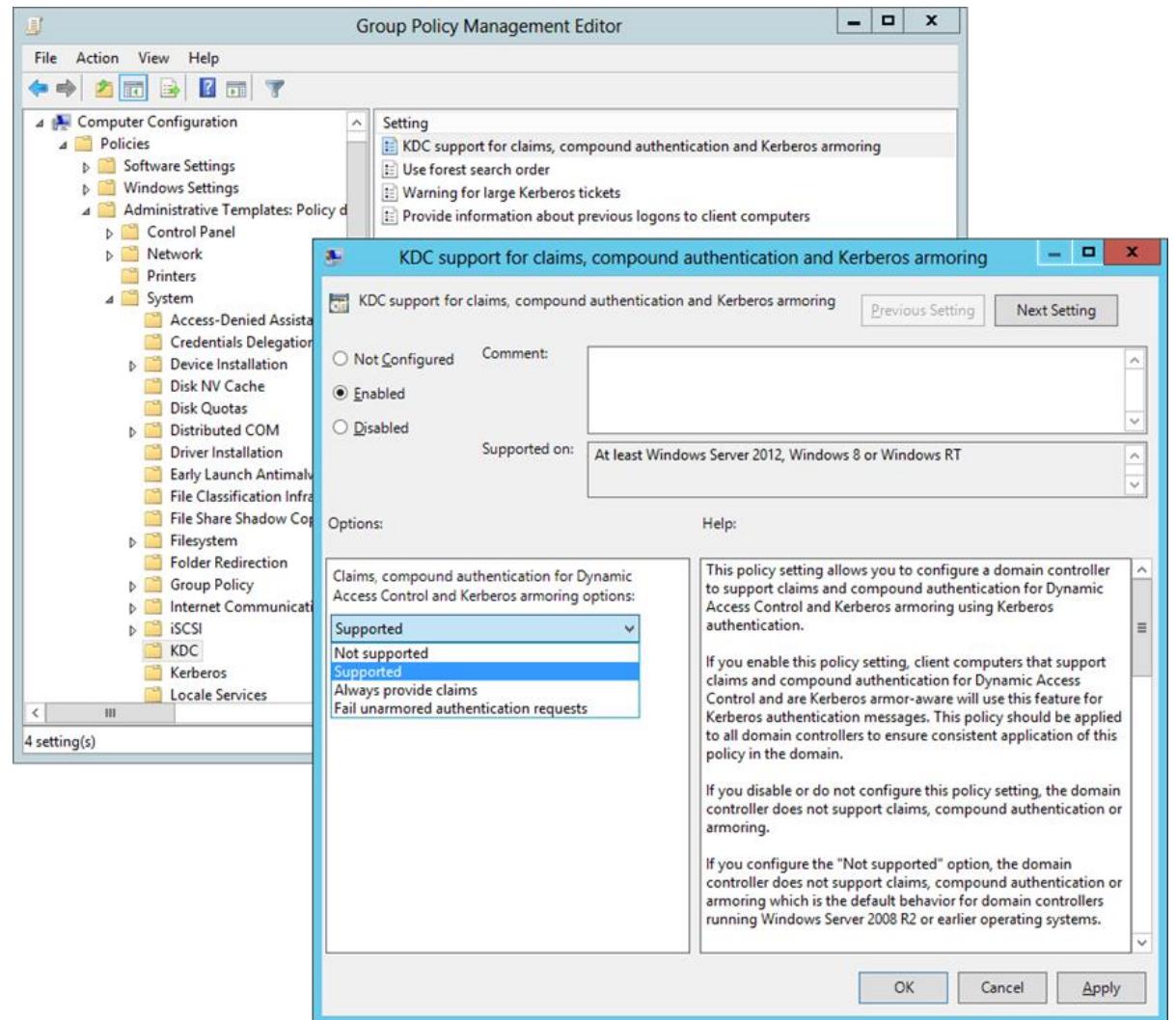
# Hardening: Kerberos Armoring

- The computer's Kerberos session key protects the user's Kerberos messages
  - Kerberos errors get signed with the computer's session key
- Prevents MITM Kerberos error injections as attackers don't have the computer's credentials / keys

Name	Value	Bit Offset	Bit Length	Type
Length	Length: 430	0	32	Kerbero...
Message	KRB_ERROR	32	3440	Kerbero...
Pvno	5 (0x0000000000000005)	96	40	Int64
MsgType	KRB_ERROR(30) (0x000000000000001E)	136	40	MsgType
Stime	2014-03-10T22:10:56.000000	176	152	DateTime
Susec	927784 (0x0000000000E2828)	328	56	Int64
ErrorCode	KDC_ERR_PRAUTH_REQUIRED(25) (0x0000000000000019)	384	40	ErrorCo...
Realm	aorato.research	424	152	String
Sname	krbtgt/aorato.research	576	304	Kerbero...
EData	MethodData{MethodData=[PA-FX-FAST (136)]}	880	2592	Kerbero...
MethodData	[PA-FX-FAST (136)]	0	2528	ArrayVa...
[0]	PA-FX-FAST (136)			Kerbero...
PAD.DataType	PA-FX-FAST (136) (0x000000000000088)	64	48	Int64
PAD.addValue	PA-FX-FAST-REPLY	112	2416	Kerbero...
PAD.addValue	KrbFastArmoredRep{EncFastRep=EncryptedData{Etype=18,Kvno=not...}	0	2352	Kerbero...

# Hardening: Kerberos Armoring (Cont.)

- Available since Windows 8, Server 2012

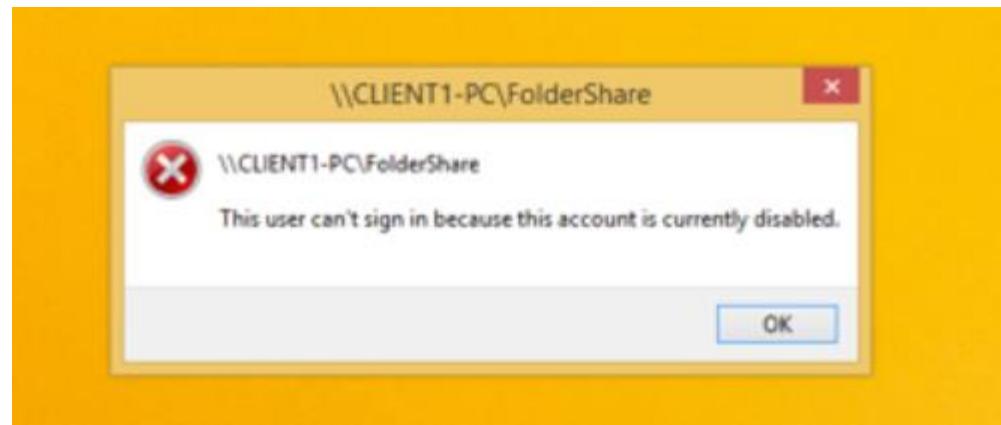
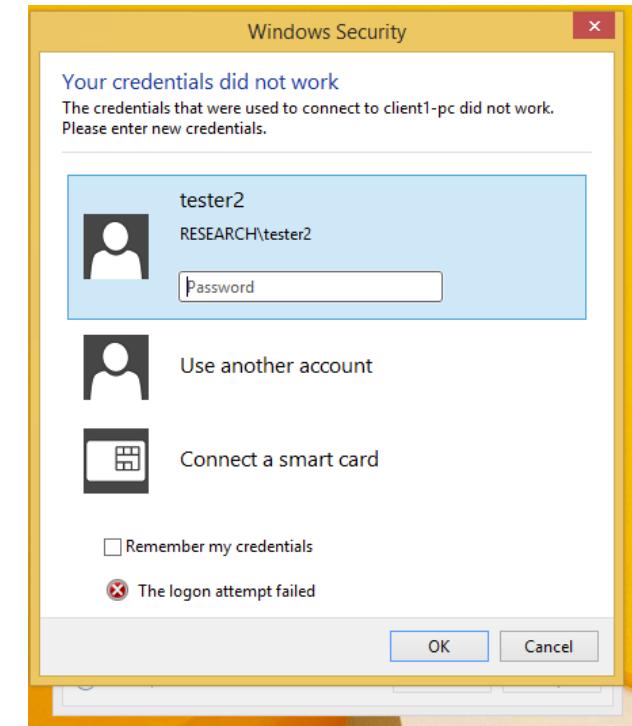


# Cyber Judo with Kerberos Error Injection



# Injecting to Client: Kerberos Error Injection

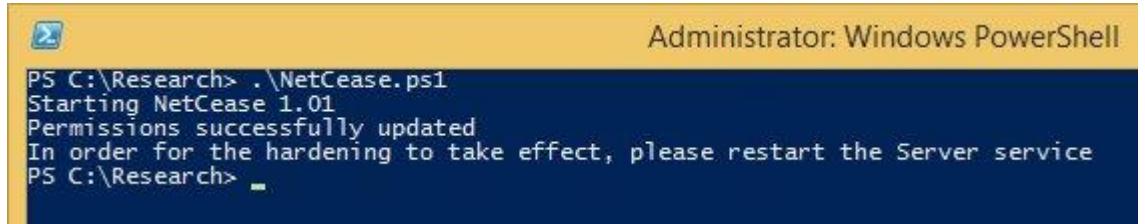
- Security Devices can use this method too!
  - Aorato (acquired by Microsoft) patent
  - "System, method and process for mitigating advanced and targeted attacks with authentication error injection"
- A "followed action" to detection
  - Force password change: KDC\_ERR\_KEY\_EXPIRED
  - Force re-enter password: KDC\_ERR\_TGT\_REVOKED
  - Elegantly block users: KDC\_ERR\_CLIENT\_REVOKED



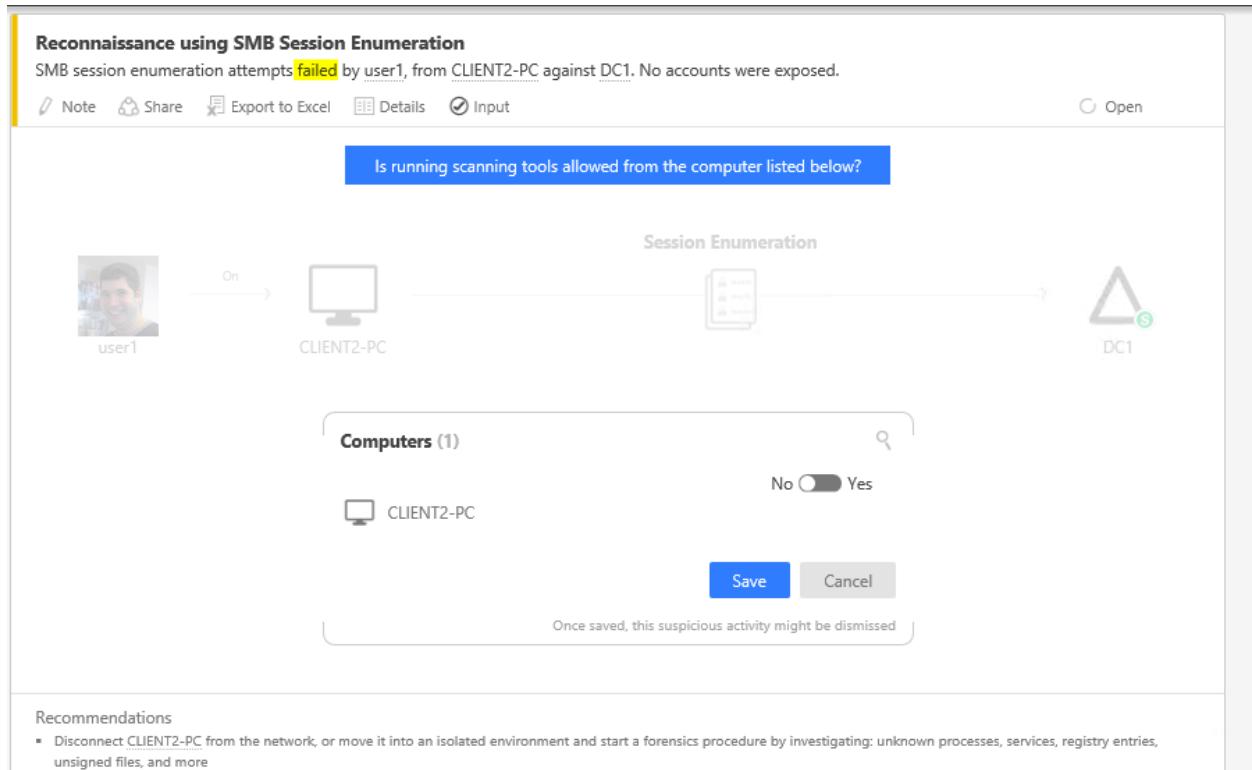
# Parting Thoughts

# Judo or Boxing?

- Should defenders
  - be boxers and block?
  - Be Judokas and use?
- Why not both?
- For reconnaissance APIs
  - Harden generic excessive access
    - But allow defenders' user
  - Detect failed attempts



```
Administrator: Windows PowerShell
PS C:\Research> .\NetCease.ps1
Starting NetCease 1.01
Permissions successfully updated
In order for the hardening to take effect, please restart the Server service
PS C:\Research>
```



Reconnaissance using SMB Session Enumeration  
SMB session enumeration attempts failed by user1, from CLIENT2-PC against DC1. No accounts were exposed.

Is running scanning tools allowed from the computer listed below?

Session Enumeration

user1 → CLIENT2-PC → DC1

Computers (1)
CLIENT2-PC

No  Yes

Save Cancel

Once saved, this suspicious activity might be dismissed

Recommendations

- Disconnect CLIENT2-PC from the network, or move it into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more

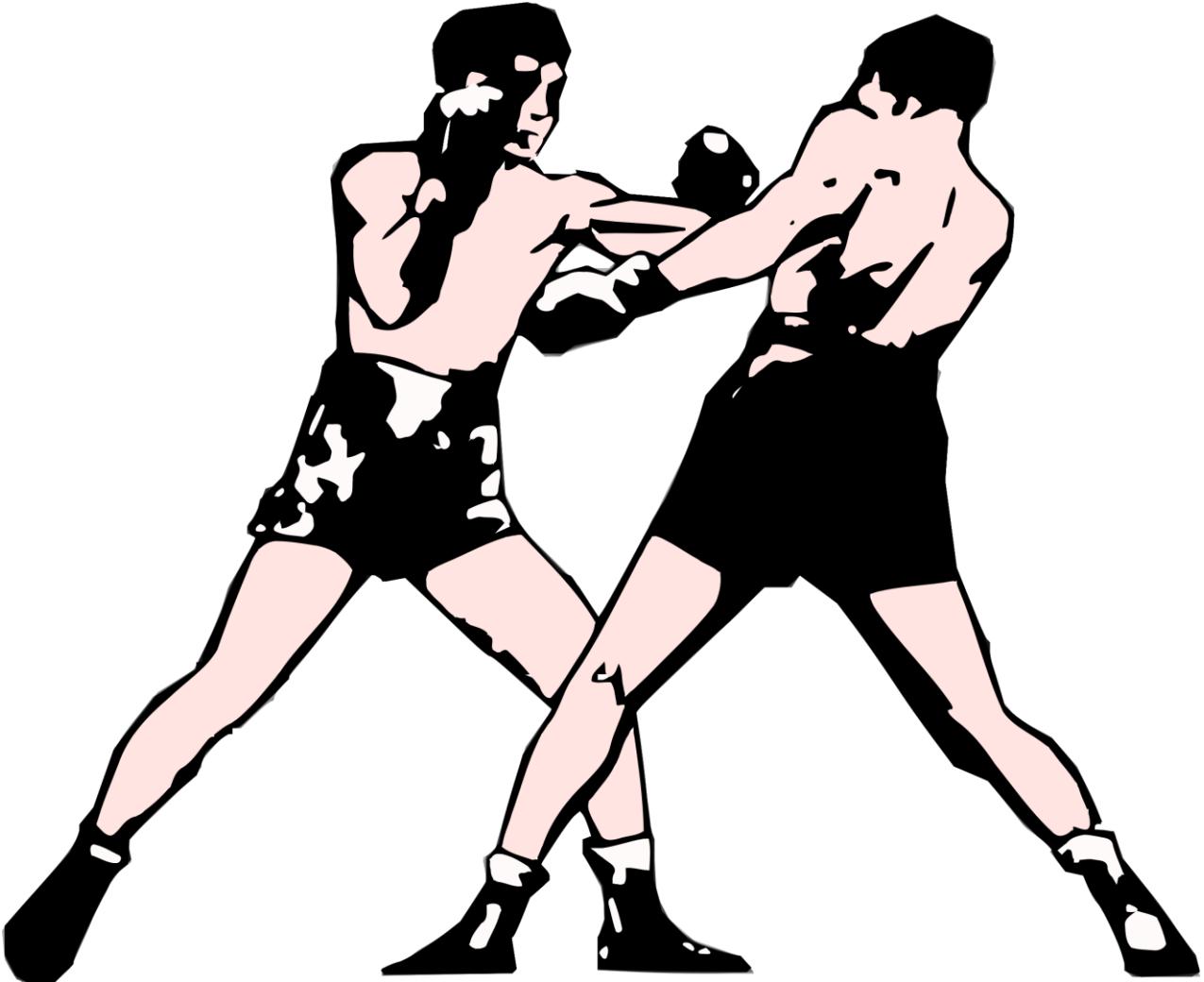
# New Contributions

- Lateral Movement automation Module
- “Boxer” Defenses:
  - Detections
    - NetSess recon
    - SAMR recon
  - Hardening
    - Kerberos Armoring
    - SAMR access
- Judo defenses
  - Kerberos defensive error injection
  - NTLM authentication visibility via NetSess Recon
  - Local Users visibility via SAMR Recon



# Conclusions

- To defeat the enemy
  - Learn the enemy
  - Know the enemy
  - Be the enemy



# Credits and Thanks

- Reviewers
  - BloodHound's Andrew Robbins @\_wald0
- Microsoft ATA Research team (other members)
  - Tal Maor @TaltheMaor
  - Marina Simakov
  - Chaim Hoch @chaimh90
- Microsoft ATA Designer
  - Dan Mor @danmor84

# Questions?

©2016 Microsoft Corporation. All rights reserved. This presentation is provided "as-is." Information and views expressed in this presentation, including URL and other Internet Web site references, may change without notice. You bear the risk of using it. Some examples are for illustration only and/or are fictitious. No real association is intended or inferred.

This presentation does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use the contents of this presentation for your internal, reference purposes.