Know your creds or Die Trying

Chad Tilbury
CrowdStrike
SANS Institute
ATTACK CYCLE

- Priority #1 post-exploitation
  - Domain admin is ultimate goal
- Nearly everything in Windows is tied to an account
  - Difficult to move without one
- Easy and relatively stealthy means to traverse the network
  - Account limitations are rare
- “Sleeper” credentials can provide access after remediation
"Text file w/ creds in share, found where creds are admin, dumped local admin, use to find DA, dumped DA, dumped Domain"

#PentestReportTweet
Do You Know Your Credentials?
HASHES
The password for each user account in Windows is stored in multiple formats: LM and NT hashes are most well known.

Common Attacks
- Dumping
- Cracking
- Pass the Hash

Common Tools
- Mimikatz
- Fgdump
- Gsecdump
- Metasploit
- SMBshell
- PWDumpX
- Creddump
- WCE
HASH DUMPING (Gsecdump)

```
Administrator(current): 500: aad3b435b51404 eeaad3b435b51404: ee7d58f0d8d560861d105513c74b
Guest(current-disabled): 501: aad3b435b51404 eeaad3b435b51404: 31d6cfe0d16ae931b73c59d7e
krbtg(current-disabled): 502: aad3b435b51404 eeaad3b435b51404: 70b2c6e6b837b3a18f8c9f9e
svc-printandscan(current): 1104: aad3b435b51404 eeaad3b435b51404: 8846f7eae8fb117ad06bdf
nbfury(current): 1105: aad3b435b51404 eeaad3b435b51404: 0fbd18b0b323b7d759b9ac32b3c44f6b
mhill(current): 1106: aad3b435b51404 eeaad3b435b51404: 8846f7ee8fb117ad06bdf830b7586c
tdungan(current): 1107: aad3b435b51404 eeaad3b435b51404: 5af5c9adddf45a352074bac862b2e0bac
pcoulson(current): 1108: aad3b435b51404 eeaad3b435b51404: 8846f7ee8fb117ad06bdf830b7586c
nromanoff(current): 1109: aad3b435b51404 eeaad3b435b51404: 5073beed7c83324ab7ddabed5360
svc-bitlocker(current): 1113: aad3b435b51404 eeaad3b435b51404: 8846f7ee8fb117ad06bdf830b7586c
rsydow(current): 1114: aad3b435b51404 eeaad3b435b51404: ea600320ec9e2f47fdd29cf37f5a98
sharepoint(current): 1503: aad3b435b51404 eeaad3b435b51404: 5bca1afe41eab3f827caeb93293
malsteele(current): 1508: aad3b435b51404 eeaad3b435b51404: 3d05f165da97e2d5632743a1b6438
nicsteele(current): 1509: aad3b435b51404 eeaad3b435b51404: ccece70d8e760e9a826bf97483a0f
theylons(current): 1510: aad3b435b51404 eeaad3b435b51404: 266e2bb22867a0a3a1834f327fe660
davdawson(current): 1511: aad3b435b51404 eeaad3b435b51404: 7264fa7996434c1003921a82730cb
dewturner(current): 1512: aad3b435b51404 eeaad3b435b51404: 93997c0c1d03e559ed982748ed5b2
gebennett(current): 1513: aad3b435b51404 eeaad3b435b51404: 29955116a5dd31a6db3efb5ff
```
PASS THE HASH

(Mimikatz)
TOKENS

Delegate tokens are powerful authentication resources used for SSO. They allow attackers to impersonate a user’s security context.

Common Attacks
- Token Stealing
- Privilege Escalation

Common Tools
- Mimikatz
- Incognito
- Metasploit
- PowerShell
TOKEN STEALING

(Mimikatz)
The Method of Privileged Account Usage Matters
<table>
<thead>
<tr>
<th>Admin Action</th>
<th>Logon Type</th>
<th>Credentials on Target?</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console logon</td>
<td>2</td>
<td>Yes*</td>
<td>*Except when Credential Guard is enabled</td>
</tr>
<tr>
<td>Runas</td>
<td>2</td>
<td>Yes*</td>
<td>*Except when Credential Guard is enabled</td>
</tr>
<tr>
<td>Remote Desktop</td>
<td>10</td>
<td>Yes*</td>
<td>*Except for enabled Remote Credential Guard</td>
</tr>
<tr>
<td>Net Use</td>
<td>3</td>
<td>No</td>
<td>Including /u: parameter</td>
</tr>
<tr>
<td>PowerShell Remoting</td>
<td>3</td>
<td>No</td>
<td>Invoke-Command; Enter-PSSession</td>
</tr>
<tr>
<td>PsExec alternate creds</td>
<td>3 + 2</td>
<td>Yes</td>
<td>-u &lt;username&gt; -p &lt;password)</td>
</tr>
<tr>
<td>PsExec w/o explicit creds</td>
<td>3</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>Remote Scheduled Task</td>
<td>4</td>
<td>Yes</td>
<td>Password saved as LSA Secret</td>
</tr>
<tr>
<td>Run as a Service</td>
<td>5</td>
<td>Yes</td>
<td>(w/ user account) – PW saved as LSA Secret</td>
</tr>
<tr>
<td>Remote Registry</td>
<td>3</td>
<td>No</td>
<td></td>
</tr>
</tbody>
</table>
**TICKETS**

Kerberos issues tickets to authenticated users that can be reused to access computers and services. Tickets are cached in memory.

<table>
<thead>
<tr>
<th>Common Attacks</th>
<th>Common Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass the Ticket</td>
<td>Mimikatz</td>
</tr>
<tr>
<td>Over Pass the Hash</td>
<td>WCE</td>
</tr>
<tr>
<td>Golden Ticket</td>
<td>Kerberoast</td>
</tr>
<tr>
<td></td>
<td>PowerShell</td>
</tr>
</tbody>
</table>
PASS THE TICKET

(Mimikatz)
<table>
<thead>
<tr>
<th><strong>KERBEROS ATTACKS</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pass the Ticket</strong></td>
</tr>
<tr>
<td>Steal ticket from memory and pass or import on other systems</td>
</tr>
<tr>
<td><strong>Kerberroasting</strong></td>
</tr>
<tr>
<td>Request service ticket for highly privileged service and crack hash</td>
</tr>
<tr>
<td><strong>Silver Ticket</strong></td>
</tr>
<tr>
<td>All-access pass for a single service or computer</td>
</tr>
<tr>
<td><strong>Overpass the Hash</strong></td>
</tr>
<tr>
<td>Use NT hash to request a service ticket for the same account</td>
</tr>
<tr>
<td><strong>Golden Ticket</strong></td>
</tr>
<tr>
<td>Kerberos TGT for any account with no expiration. Survives full password reset</td>
</tr>
<tr>
<td><strong>Skeleton Key</strong></td>
</tr>
<tr>
<td>Patch LSASS on domain controller to add backdoor password that works for any domain account</td>
</tr>
</tbody>
</table>
Detection
As any pass-the-ticket attack, the attacker replays the golden ticket in a standard Kerberos protocol. Therefore, there is no clear indication of such attack in Windows logs.
Kerberoasting uses RC4 encryption downgrade.
Golden Ticket events may have one of these issues:

• The Account Domain field is *blank* when it should be **DOMAIN**

• The Account Domain field is **DOMAIN FQDN** when it should be **DOMAIN**.

"Sean Metcalf, adsecurity.org"
**SIMPLE DETECTS**

**Authentication Auditing**
- Mapping Admin$ Shares
- PsExec
- Scheduled Tasks
- VSSAdmin
- RDP/VPN Activity

**Tool Artifacts**
- New Services
- Random File / Host names
- Code Injection
- Crashes and Security Alerts

**Behavioral Analysis**
- Local Admin Account Use
- Domain Admin Anomalies
- Service Account Anomalies
- Workstation-to-Workstation Connections
Mitigation
Privilege Escalation
- User Access Control (UAC)*
- Pass the Hash
  - User Access Control (UAC)*

Kerberos Attacks
- Managed Service Accounts
- Backporting Win8.1 Mitigations
  - KB2871997
Credential Dumping
✓ SSP password mitigations
✓ Protected processes*

Remote Creds & Tickets
✓ Domain Protected Users
✓ Restricted Admin*
✓ LSA Cache Cleanup

Pass the Hash
✓ Local Account Remote Logon Restrictions

Token Theft
✓ Restricted Admin*
✓ Protected Users

Kerberos Attacks
✓ Group Managed Service Accounts
Credential Dumping

✓ Credential Guard
✓ Device Guard

Remote Creds & Tickets

✓ Remote Credential Guard
## KERBEROS ATTACKS

<table>
<thead>
<tr>
<th>Attack</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass the Ticket</td>
<td>Steal ticket from memory and pass or import on other systems</td>
<td>Credential Guard, Remote Credential Guard</td>
</tr>
<tr>
<td>Overpass the Hash</td>
<td>Use NT hash to request a service ticket for the same account</td>
<td>Credential Guard; Protected Users Group; Disable RC4 authentication</td>
</tr>
<tr>
<td>Kerberoasting</td>
<td>Request service ticket for highly privileged service &amp; crack NT hash</td>
<td>Long and complex service account passwords; Managed Service Accounts</td>
</tr>
<tr>
<td>Golden Ticket</td>
<td>Kerberos TGT for any account with no expiration. Survives full password reset</td>
<td>Protect domain admin accounts; Change KRBTGT password regularly</td>
</tr>
<tr>
<td>Silver Ticket</td>
<td>All-access pass for a single service or computer</td>
<td>Regular computer and service account password updates</td>
</tr>
<tr>
<td>Skeleton Key</td>
<td>Patch LSASS on domain controller to add backdoor password to any account</td>
<td>Protect domain admin accounts; Smart card usage for privileged accounts</td>
</tr>
</tbody>
</table>
## KERBEROS ATTACKS (Simplified)

<table>
<thead>
<tr>
<th>Attack</th>
<th>Description</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass the Ticket</td>
<td>Steal ticket from memory and pass or import on other systems</td>
<td>Protect Tickets</td>
</tr>
<tr>
<td>Overpass the Hash</td>
<td>Use NT hash to request a service ticket for the same account</td>
<td>Protect Hashes</td>
</tr>
<tr>
<td>Kerberoasting</td>
<td>Request service ticket for highly privileged service &amp; crack NT hash</td>
<td>Protect Service Accts</td>
</tr>
<tr>
<td>Golden Ticket</td>
<td>Kerberos TGT for any account with no expiration. Survives full password reset</td>
<td>Protect Domain Admin</td>
</tr>
<tr>
<td>Silver Ticket</td>
<td>All-access pass for a single service or computer</td>
<td>Protect Hashes</td>
</tr>
<tr>
<td>Skeleton Key</td>
<td>Patch LSASS on domain controller to add backdoor password to any account</td>
<td>Protect Domain Admin</td>
</tr>
</tbody>
</table>
Top Credential Mitigations
Domain Protected
Users Group
Plan for Credential Guard (Upgrade!)
Group Managed Service Accounts
Empty Domain Admins Group (Tiered Admin)
BUT WAIT, THERE’S MORE!

- LSA Secrets
- NTDS.DIT
- Smart Card Pins
- Windows Hello
- Certificates
- Cached Credentials
- Microsoft Cloud Accounts
- DPAPI
- DC Sync

93° Sunny Austin

Sunny Austin
Make Windows Great Again!

Chad Tilbury

chad.tilbury@crowdstrike.com
http://ForensicMethods.com
@chadtilbury