THE SECRET LIFE OF
KRBTGT
Bio

- Security Researcher/Tester (Harris Corp)
- Former Army Red Team Operator
- One of the developers of PowerSploit
- Twitter: @obscuresec
- Blog: www.obscuresec.com
There will be FUD. Convince your boss to go to another talk.
Say hello to krbtgt
He’s been here since the beginning
The Early Years: 2001-2004
Growing Pains: 2005-2008
Maturity Realized: 2009-2012

Windows Server 2008

Group Policy Preferences
WE PREVENT ADMIN ACCOUNT ABUSE
WITH GROUP POLICY PREFERENCES
Skeletons in the Closet: 2013-2014
Meme Count: 2

So you implemented a full Kerberos domain?

You must feel secure now.

http://blog.gentilkiwi.com/securite/mimikatz/golden-ticket-kerberos
How old is your krbtgt hash?

```cmd
C:\Users\Admin>net user krbtgt /domain
User name    krbtgt
Full Name    Key Distribution Center Service Account
Comment      
User's comment         
Country code         
Account active       No
Account expires      Never
Password last set   3/23/2014 11:12:59 AM
Password expires    5/4/2014 11:12:59 AM
Password changeable 3/24/2014 11:12:59 AM
Password required   Yes
User may change password Yes
Workstations allowed All
Logon script       
User profile       
Home directory     
Last logon         Never
Logon hours allowed All
Local Group Memberships *Denied RODC Password
Global Group memberships *Domain Users
The command completed successfully.
```
Know where your krbtgt hash is?

<table>
<thead>
<tr>
<th>User</th>
<th>krbtgt_hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>Guest</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>krbtgt</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>carrie</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>brett</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>niki</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>kevin</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>sean</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>nina</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>cory</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>jeff</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
<tr>
<td>joe</td>
<td>e1e0d341a7f2fddd8be5e5fa66a6e3b9</td>
</tr>
</tbody>
</table>
The point is...

If your enterprise has ever been compromised, it may still be compromised – even if you changed every password.
We scan so we are secure
Good luck with that
Meme Count: 3

Kerberos Authentication

How does it work?

XXX

Defcon
Kerberos Authentication

1. TGT requested by client
2. AS sends TGT and session key
3. Client requests access from TGS
4. TGS sends encrypted session key & ticket
5. Client sends service ticket to server
6. Server sends time stamp for client to verify
“Spoofed PAC” Attack
“Golden Ticket” Attack

https://twitter.com/gentilkiwi/status/415147415474167808
Mitigation

- Don’t get owned again
- Use RODC where appropriate
- Upgrade functional level
- Reset the krbtgt account password on the PDC-emulator **TWICE**
Detection

• Needle in a hay stack
• Harder to detect than PtH
• Look for strange account activity
  – Low privileged account performing privileged actions
Thanks

• Skip Duckwall
• Benjamin Delpy
• Joe Bialek
• Will Peteroy
• Carlos Spicyweiner
• Matt Graeber
• Many others...
Questions?