
Hacker Halted USA 2014
EC-Council
TECHNOLOGY &
THE ZOMBIE APOCALYPSE
How to create permanent Domain Administrator privilege
Balazs Bucsay
ATLANTA, GEORGIA
www.hackerhalted.com

Bio / Balazs Bucsay

- Hungarian Hacker
- 14 years of experience in IT-Security
- Strictly technical certificates: OSCE, OSCP, GIAC GPEN
- Currently working for world's second largest mobile company (Vodafone)

Bio / Balazs Bucsay

- Started with ring0 debuggers and disassemblers in 2000 (13 years old)
- Major project in 2009: GI John a distributed password cracker (22 years old)
- 27 years old right now
- Webpage: http://rycon.hu
- Twitter: **@xoreipeip**
- Linkedin: http://hu.linkedin.com/pub/balazs-bucsay/30/911/379

mimikatz

- Made by Benjamin Delpy (gentilkiwi) - Big up!
- First version was introduced in 2007 (v0.1)
- Right now it is at **2.0 alpha** (Windows only)
- http://blog.gentilkiwi.com/mimikatz
- Exploiting conceptional bugs/features, not vulnerabilities
- Lots of features (not a full list):
  - Pass the hash
  - Exporting protected unexportable private keys
  - Credential dumps (even cleartext)
  - and of course Golden Ticket

Me and mimikatz

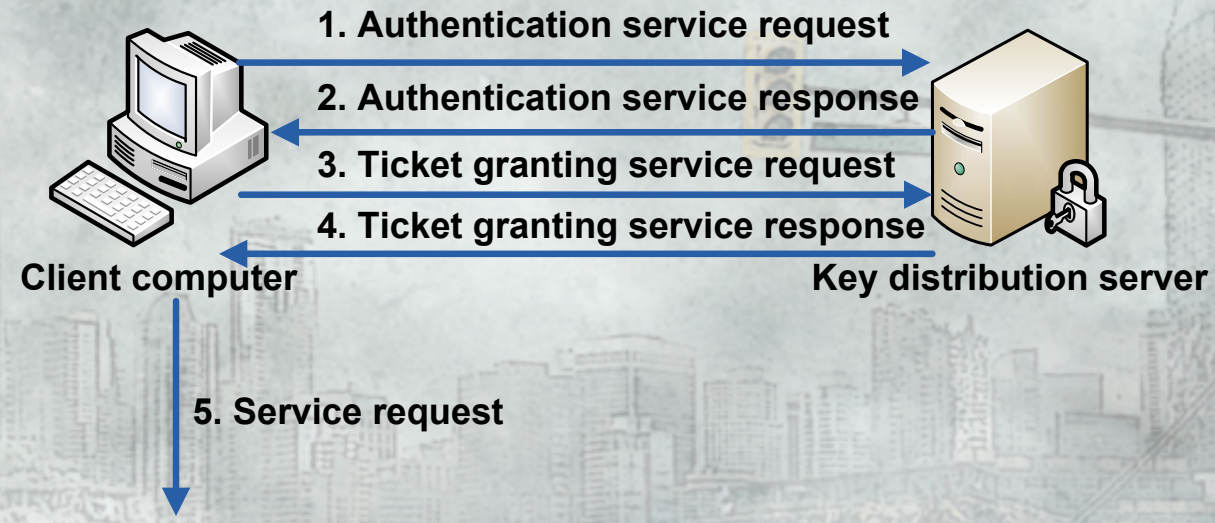
- Love at first sight
- Daily usage in penetration testing
- Hacker's best friend!
- First English documentation about the Golden Ticket
- First presentation in Hungarian

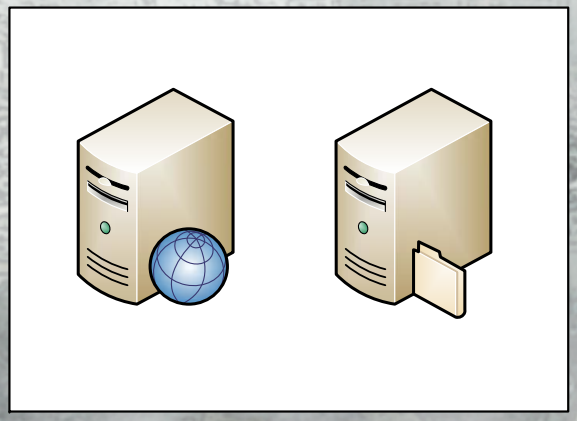
Golden Ticket

- Post Exploitation Technique
- Backdoor for **unlimited** time (20 years default)
- Offensive side: good fun, easy to use backdoor
- Defensive side: hard problem to solve
- Well known **feature** of Kerberos, not a bug
- Cannot be fixed

Cerberus

Kerberos





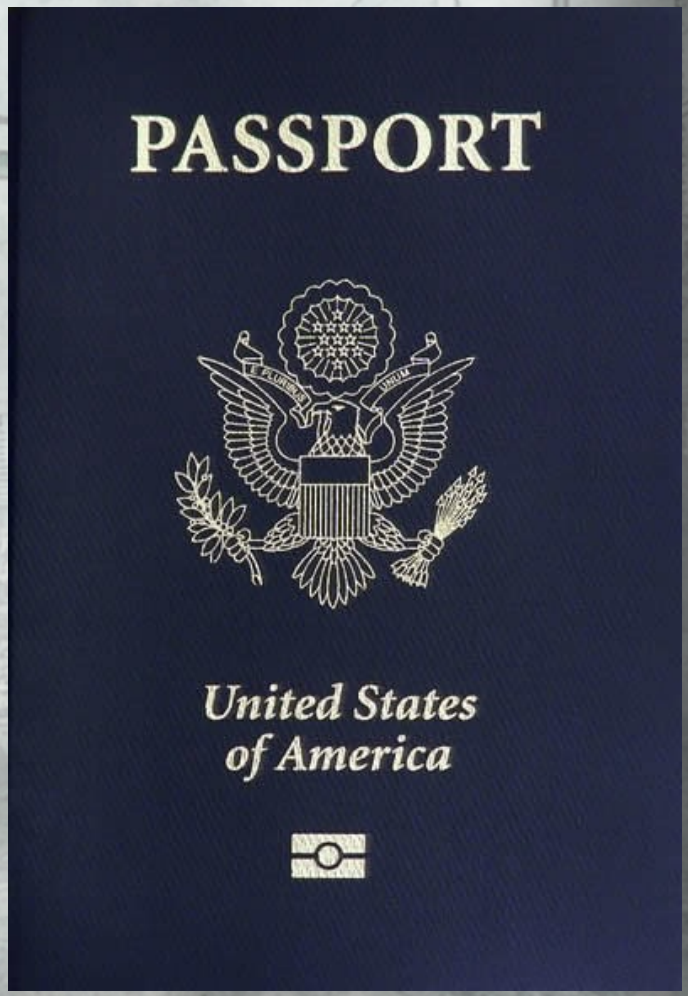
Application server (e.g. Fileserver)

Kerberos

- Developed by MIT (v5 - 1993)
- Main goal to ensure secure communication and authentication over an insecure channel
- Single Sign On
- Mutual authentication with tickets
- Tickets are encrypted
- Encryption keys are stored in the AD
- Supported authentication protocol since Windows 2000

Ticket Granting Ticket

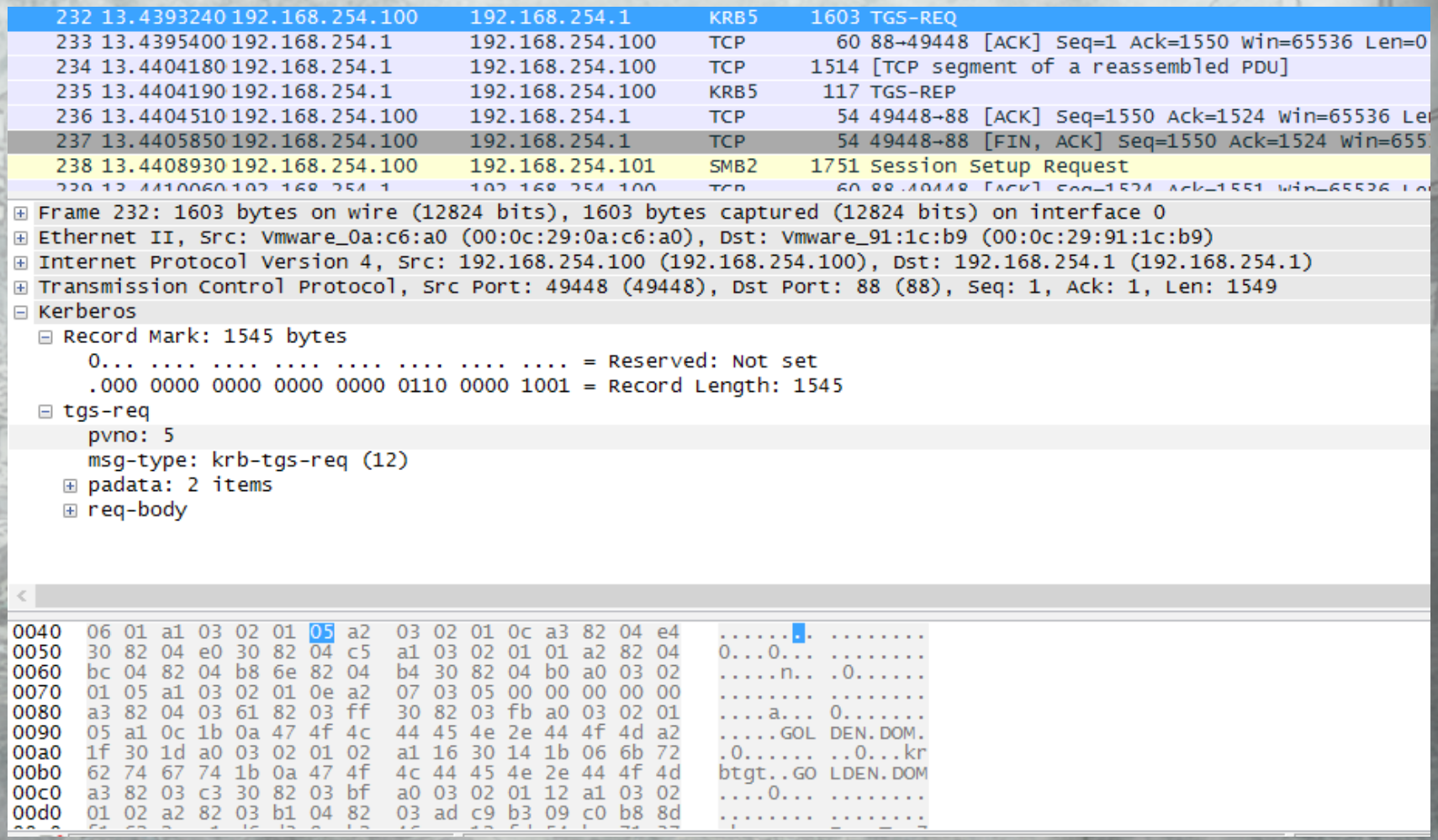
- Similar to a **passport**
- Issued by the Authentication Service (**Government**)
- User's password is needed to create the ticket
- Default session is valid for 10 hours
- Circumvents the need for password

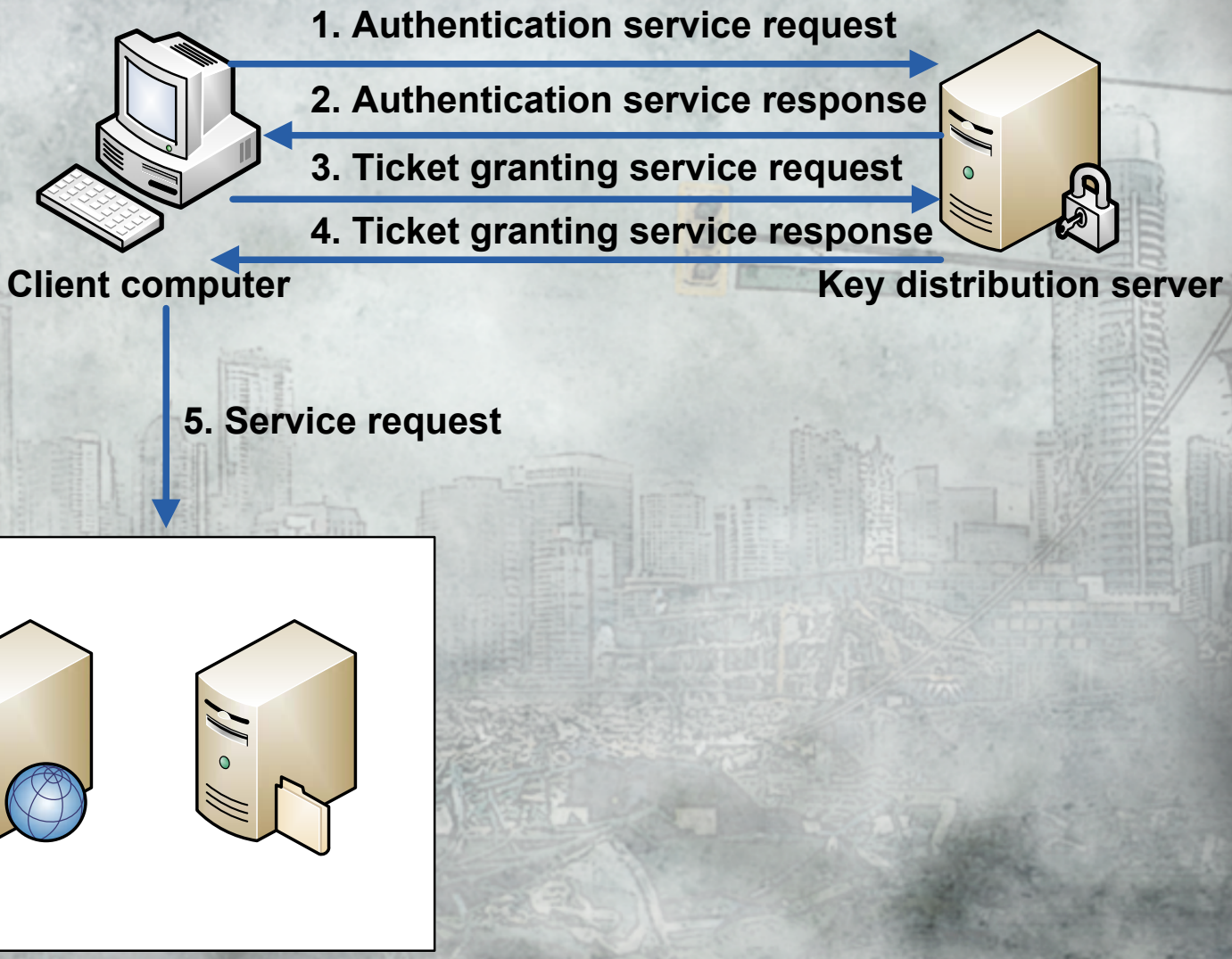


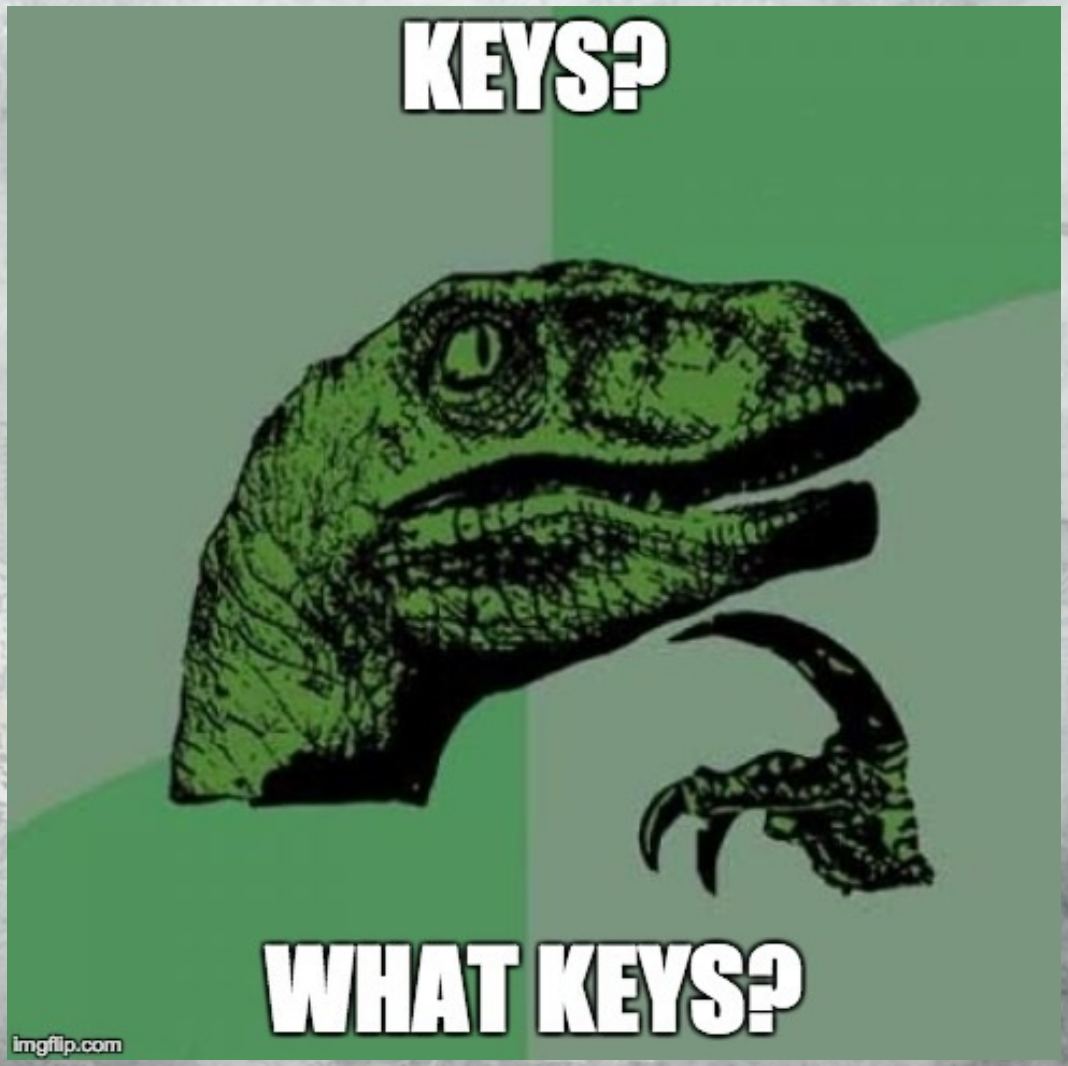
Service Ticket

- Similar to a **visa** (issued by the **Embassy**)
- Ticket Granting Service issues the Service Ticket
- Service Ticket contains the information for authentication
- Sending Service Ticket to the Service results in session

Ticket Granting Service Request




1. Authentication service request
2. Authentication service response
3. Ticket granting service request
4. Ticket granting service response
Client computer
Key distribution server
5. Service request
Application server (e.g. Fileserver)


KEYS?
WHAT KEYS?
imgflip.com

Keys

- NTLM/AES hashes of the entities from Active Directory
- Ticket Granting Ticket is encrypted with the ***krbtgt*** user's hash
- Service Tickets are encrypted with the server's and the session key

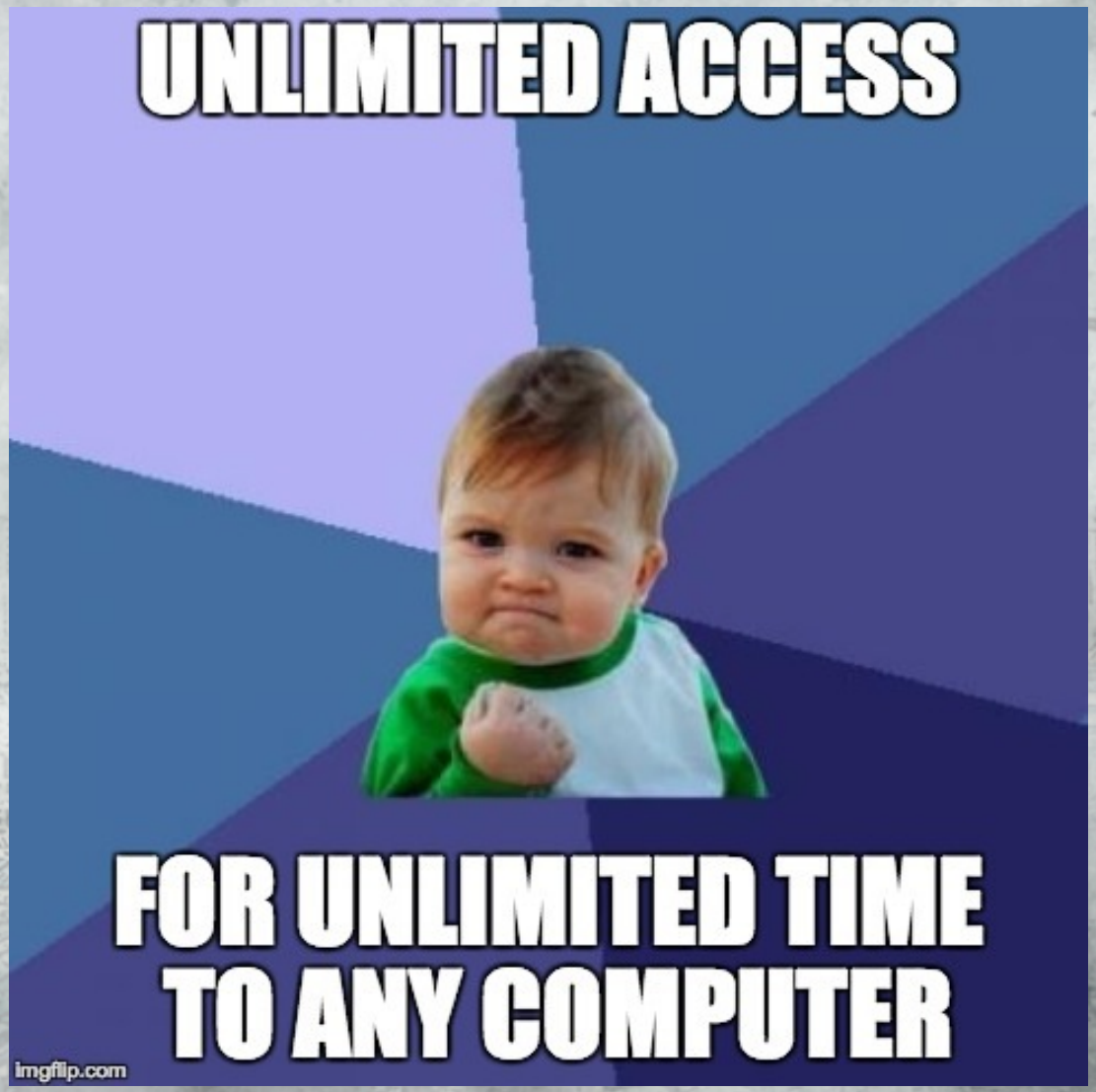
krbtgt user

```
User name                    krbtgt
Full Name
Comment                      Key Distribution Center Service Account
User's comment
Country/region code          000 (System Default)
Account active               No
Account expires              Never

Password last set            9/1/2014 10:08:25 PM
Password expires             10/13/2014 10:08:25 PM
Password changeable          9/2/2014 10:08:25 PM
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.
```

krbtgt user

- Default, must have Active Directory account
- Previous Domain Controller compromise
- ***krbtgt*** user NTLM/AES hash dump
- Arbitrary Ticket Granting Ticket can be created with the ***krbtgt*** user's hash

What does it mean for us?


UNLIMITED ACCESS
FOR UNLIMITED TIME
TO ANY COMPUTER
imgflip.com


DEMO

Mitigation

- No real way to do this
- It is a feature and not a bug
- Change password of ***krbtgt*** (twice)
- Long-time tickets could be a problem
- There can be outage in some services (Lync, Sharepoint)


Thank you
Q&A