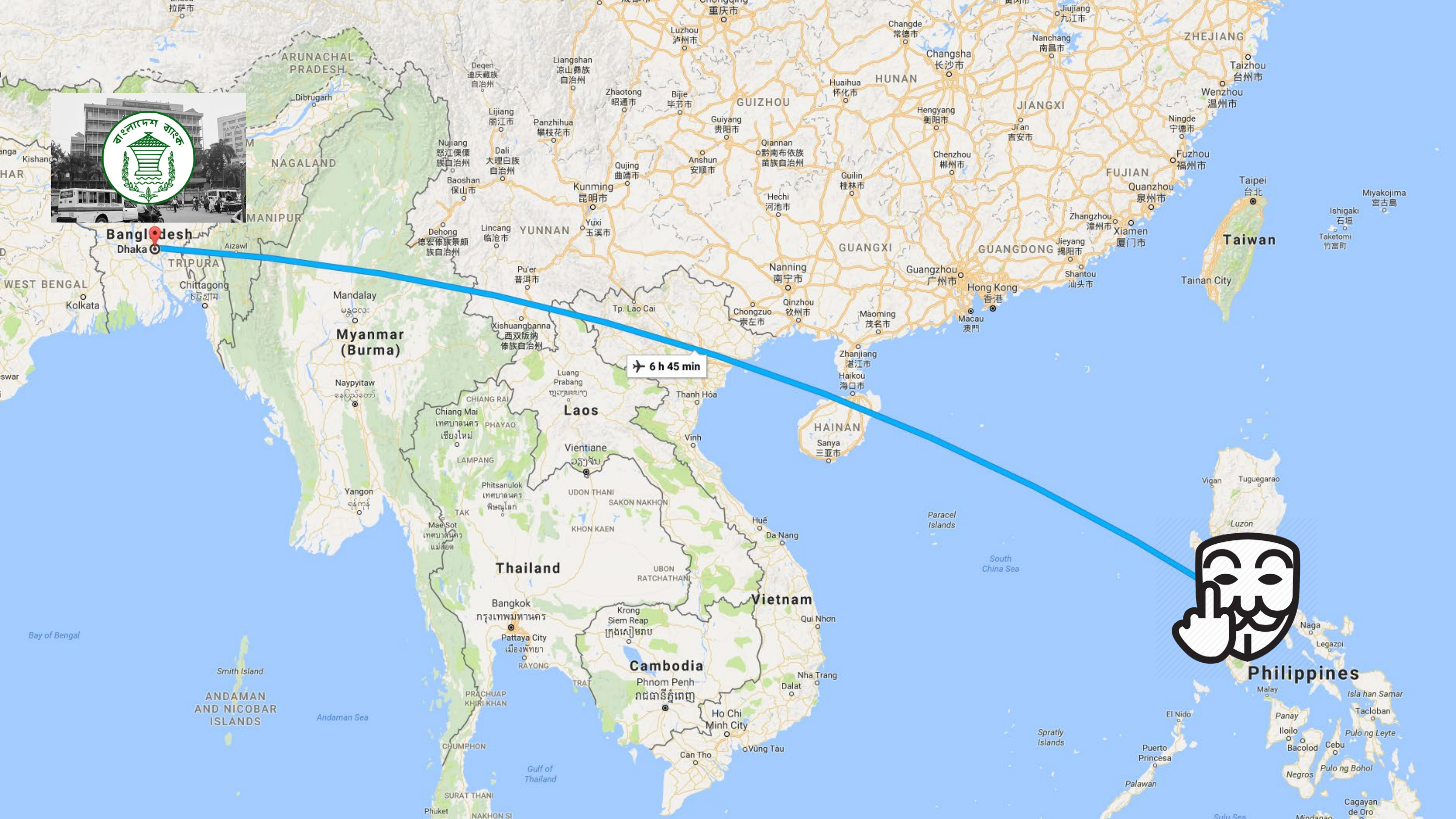
Advanced targeted attack

Golden Ticket PoC



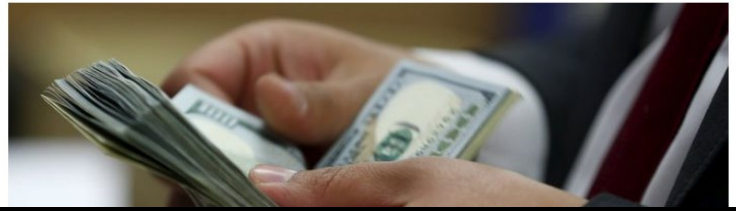
Bangladesh
Dhaka
6 h 45 min
Myanmar (Burma)
Laos
Thailand
Cambodia
Vietnam
Philippines
Taiwan
Bay of Bengal
South China Sea
Andaman Sea
Gulf of Thailand
Paracel Islands
Spratly Islands
HAINAN
YUNNAN
GUANGXI
GUANGDONG
GUIZHOU
HUNAN
JIANGXI
FUJIAN
ZHEJIANG
NAGALAND
MANIPUR
TRIPURA
ARUNACHAL PRADESH
WEST BENGAL
ANDAMAN AND NICOBAR ISLANDS
Kolkata
Chittagong
Mandalay
Naypyitaw
Yangon
Bangkok
Vientiane
Hanoi
Phnom Penh
Ho Chi Minh City
Hong Kong
Guangzhou
Taipei
Luzon

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


FOUNDATION

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

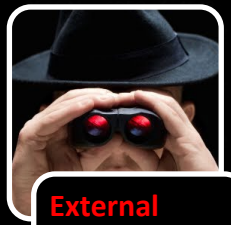
Contrary to:

Distributed Denial of Service (DDoS)

Opportunistic endpoint attacks (ex. Ransomware)

Quick, targeted attacks (ex: Support Call Scams)

Phases of an Advanced Attack



External Recon

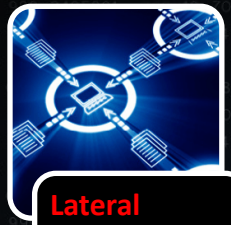
- OSINT
- Passive Scanning

Breach

- Phishing
- USB Drops
- Exploits

Internal Recon

- Network Queries
- Passive Listening
- Probing



Lateral Movement

- Seek Creds
- See Access

Domain Compromise

- Golden Ticket
- Persistence

Endgame

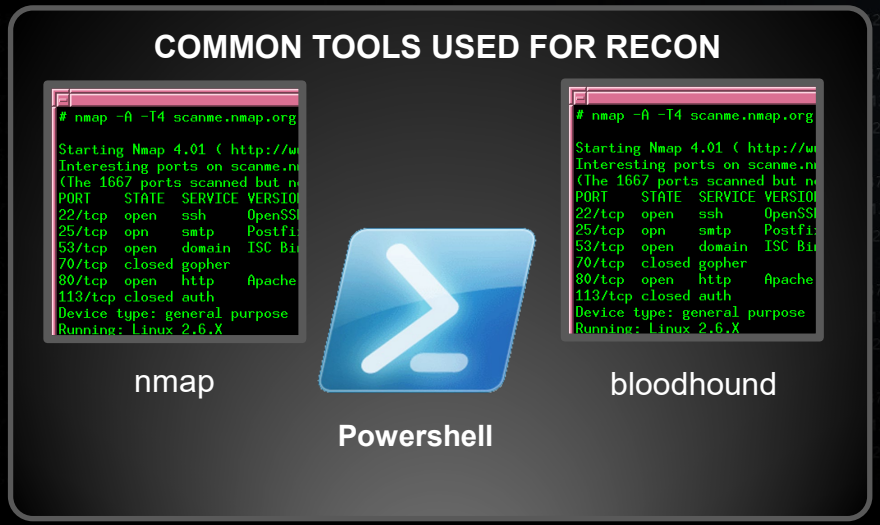
- Exfiltration
- DoS
- Corrupt

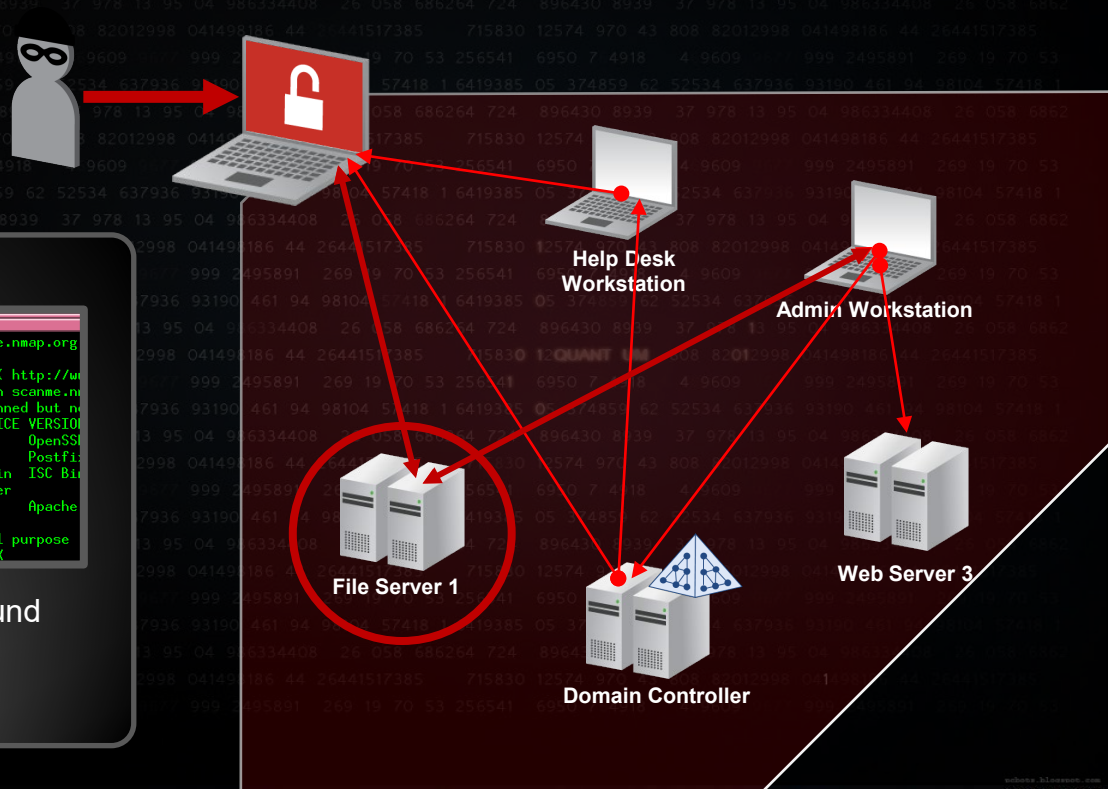
Breach

- File with malicious attachment

Internal Recon

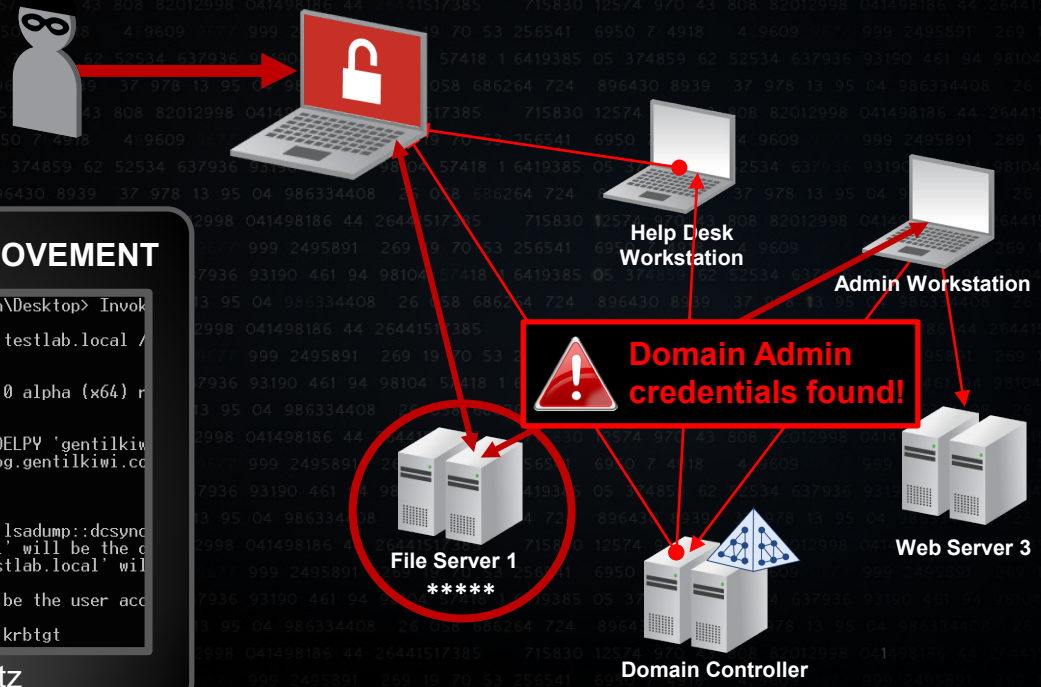
- WHAT computers are there in the network?
- WHO are the privileged users?
- WHERE are they connected?
- What privileges can I GET?





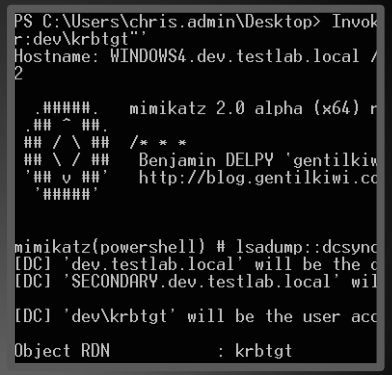
Lateral Movement

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



COMMON TOOLS USED FOR LATERAL MOVEMENT

PsExec

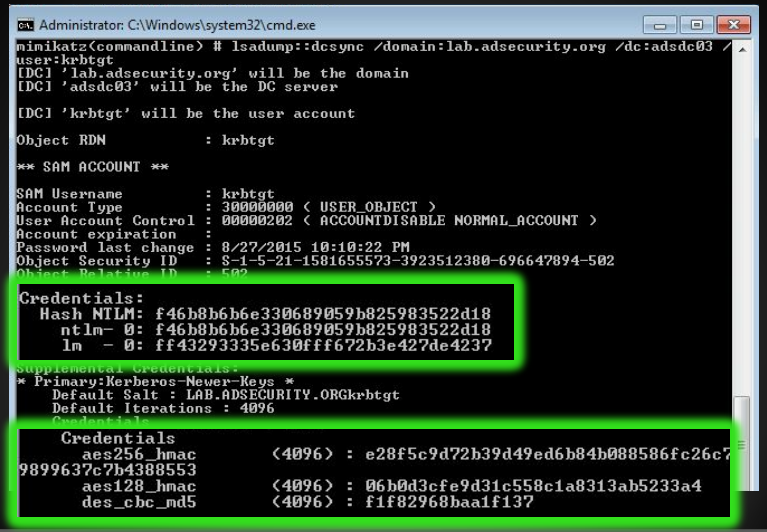


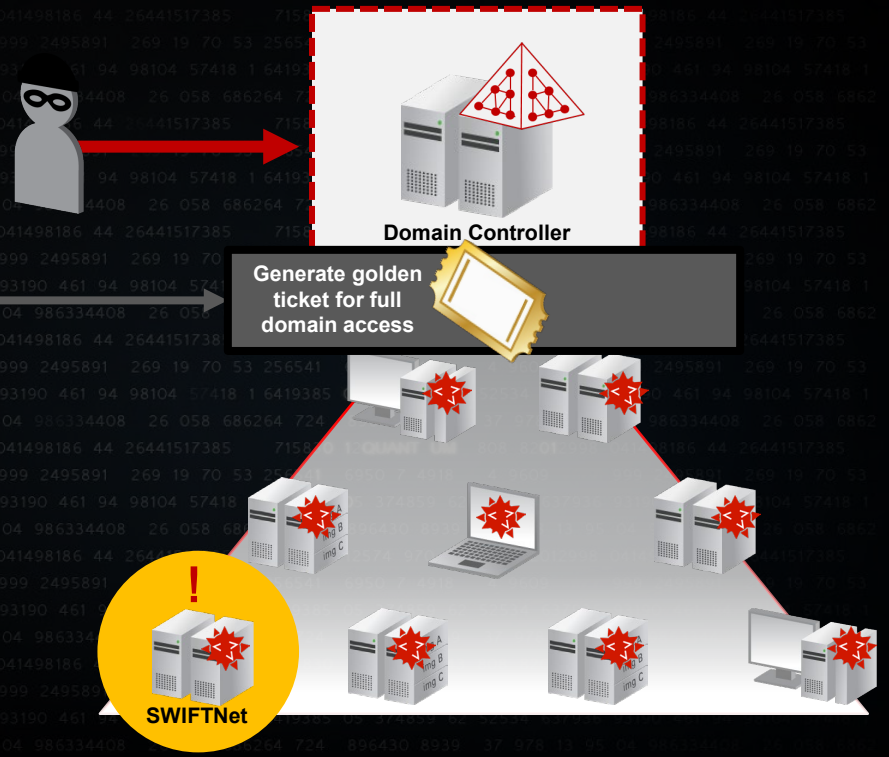
mimikatz

Domain Compromise

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

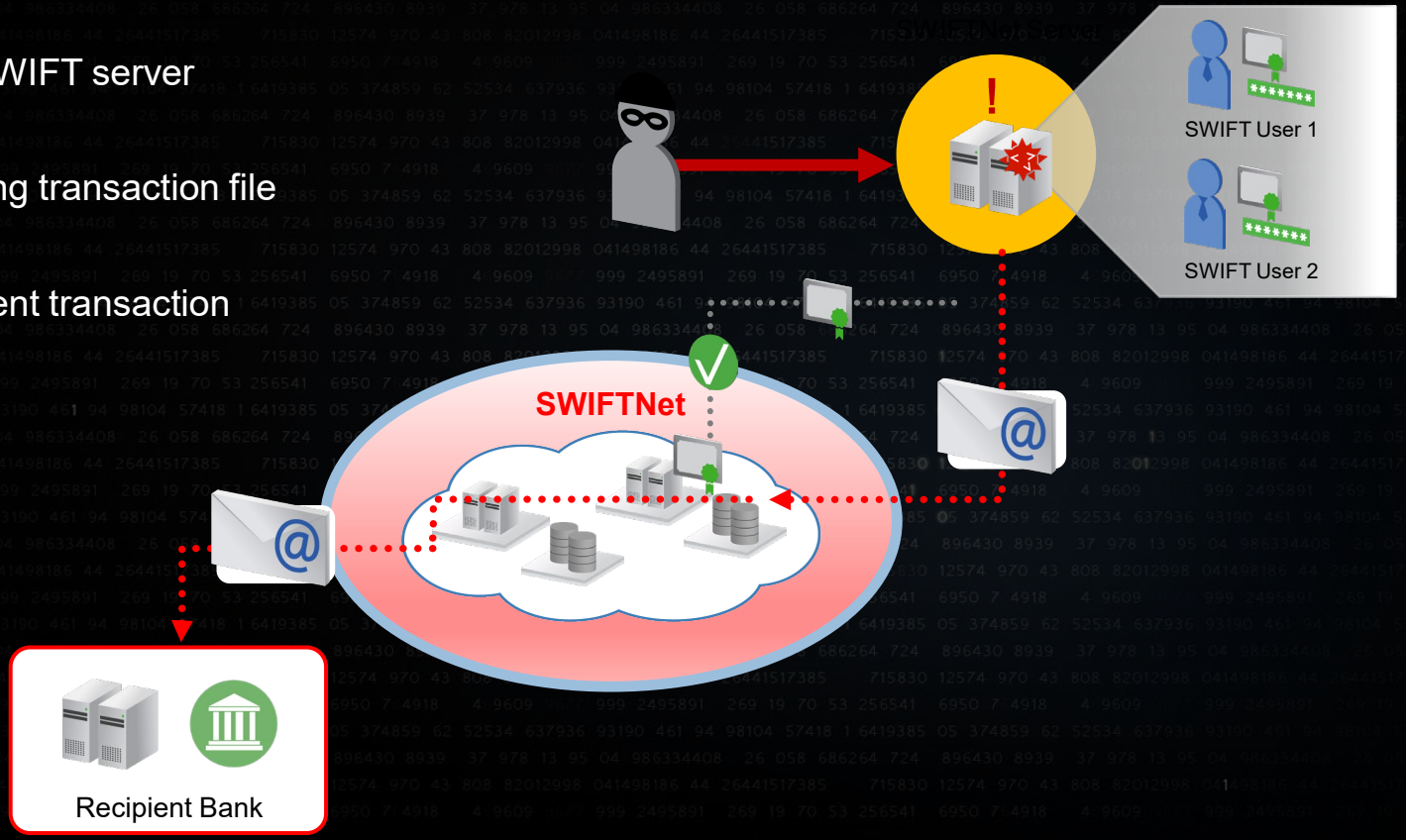
NEXT: Steal the krbtgt hash





Actions on target

- Access the SWIFT server
- Locate pending transaction file
- Inject fraudulent transaction



Profit!

IAM Best Practices

Endpoint Least Privilege

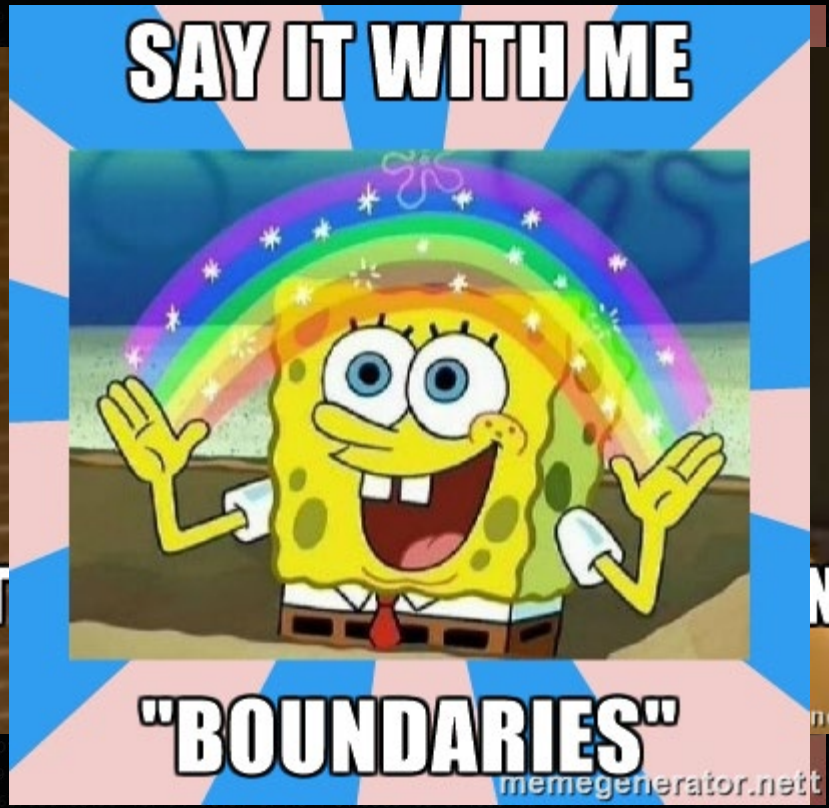
- Remove Unnecessary Privileges
  - Revoke Local Admin from regular users.
  - Allow programs that need admin rights the ability to run w/o granting access to the end user.
- Manage Application Access
  - Block unauthorized applications
  - Allow others through.

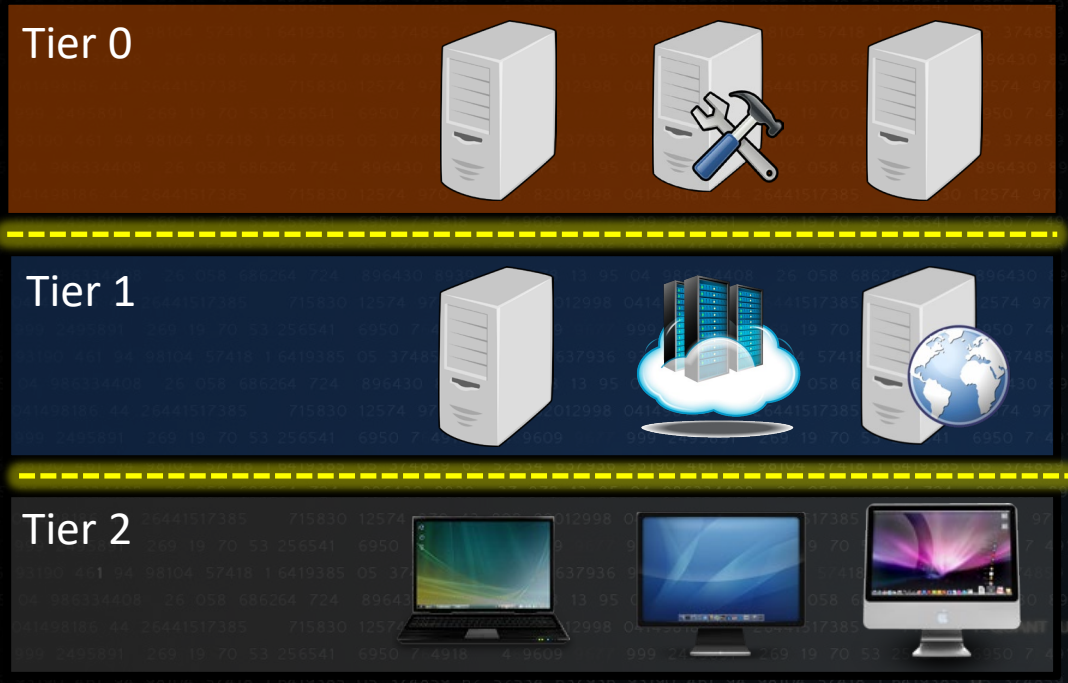
Network Segmentation

- 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





Tier 0 – Forest Admins: Direct of 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

Exchange

Active Directory

amazon web services

docker

Microsoft SQL Server

AThompson

JVealey

NLiran

KJermyn

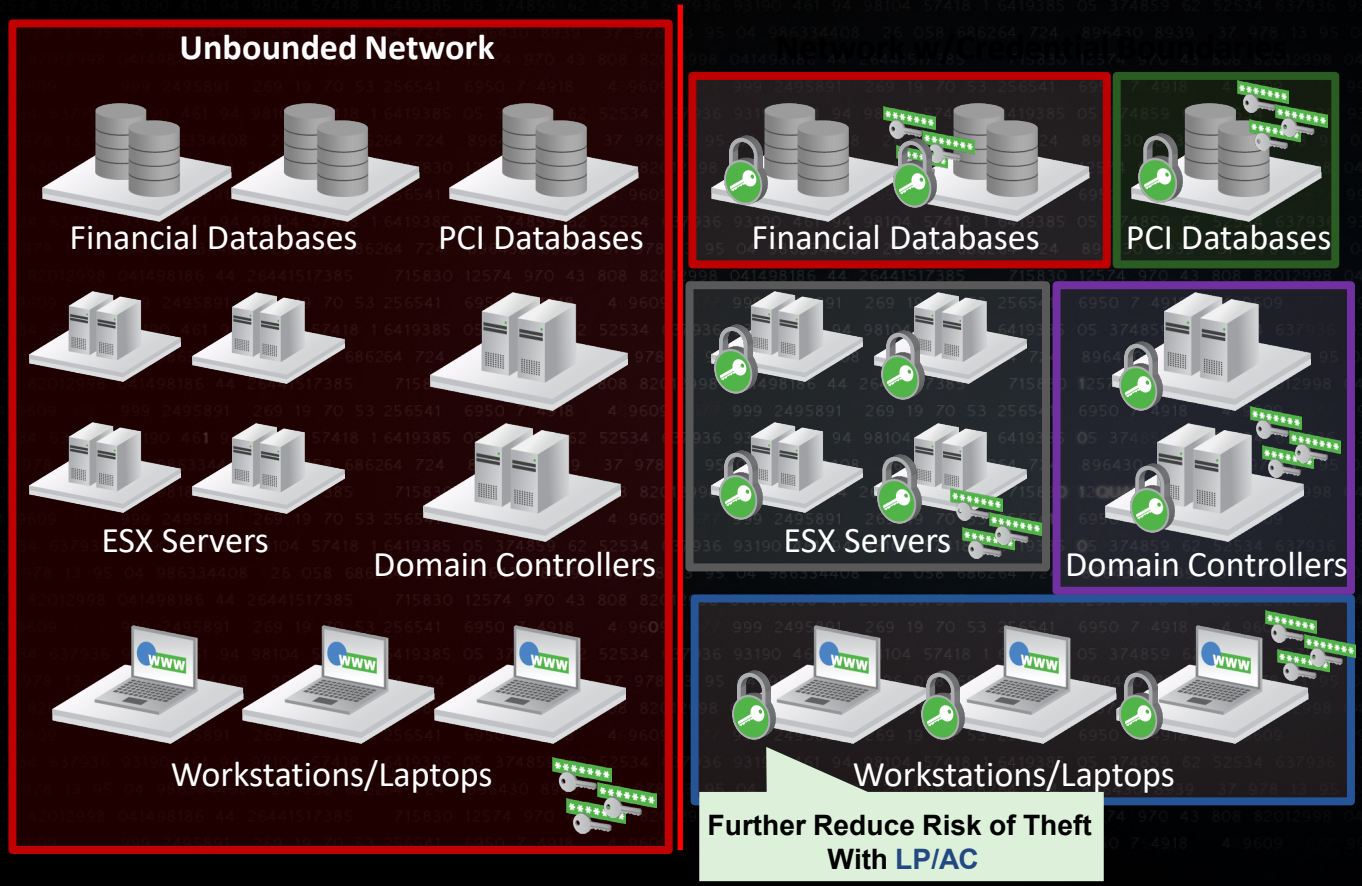
PLi

ADM-Functional-Account

5 Privileged Accounts

1 Privileged Account

The whole - shabang !



Monitoring

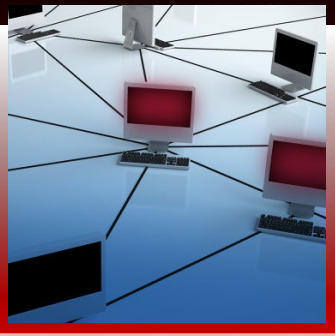
- Monitor privileged users
  - Internal employees & 3rd Party Access
- Alerting on high risk or malicious events
  - DCSync
  - IOC behavior.
- Alert on behavior anomalies
- Logons outside your IAM controls.

Iam Best Practices . . . In review.

Endpoint

- Remove local privileges
- Control applications

Network

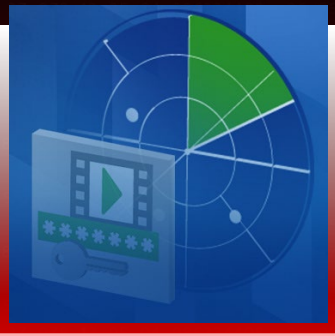


- Segment off sensitive assets
- Route access through jump servers

Credentials

- Enforce credential tiers
- Require multi-factor authentication
- Secure and manage privileged credentials

Monitoring



- Set alerts on malicious events
- Monitor behavior to detect anomalies
- Monitor privileged users

Thank You!

Andy Thompson

- Email: Andy@MeteorMusic.com
- Website: MeteorMusic.com
- Twitter: R41nM4kr
- LinkedIn: AndyThompsonInfoSec