




Unternehmensweite Echtzeit Risikobewertung

Tanium - Stefan Molls – Technical Account Manager





Wie priorisieren Sie sicherheitsrelevante
Vorfälle aktuell?

Problemstellung



- Das Passwort eines Benutzers taucht im Internet auf
- Ein Antivirenprogramm findet Spuren von einem „Credential Dumper“ auf einem System



- Wissen Sie wie „mächtig“ Ihre Active Directory Gruppen sind?
- Wie viele Domänenadministratoren haben Sie?
- Und wo sind die überall angemeldet?



- Antivirenalarme auf einem Serversystem
- Endlos lange Listen mit Schwachstellen. Wo fängt man an?
- Ein Server zeigt auffälliges Verhalten

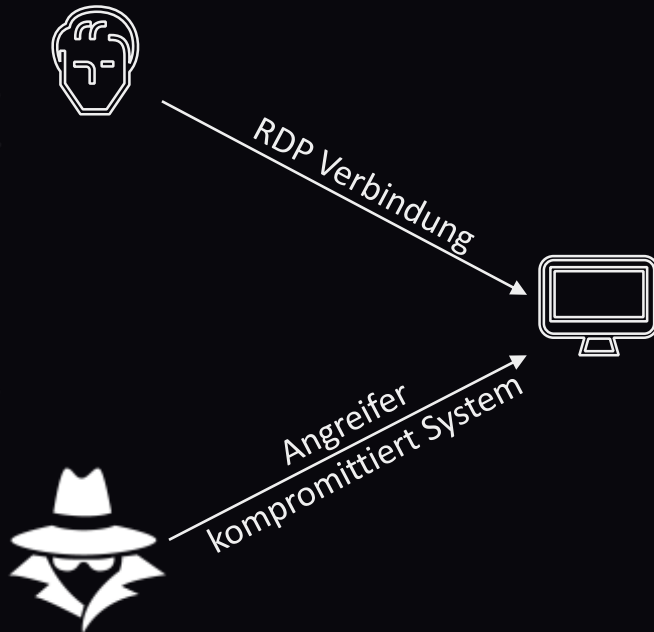
Herausforderungen

- Komplexe & nicht transparente Berechtigungen von Benutzern und Gruppen
- „Bauchgefühl“ bzw. rein funktionale Sicht bei der Bewertung des Impacts
- Betrachtung meist erst „Nach“ einem Vorfall. Keine pro-aktiven Analysen



Bevor wir in die Details gehen ...

Vorwissen: Was ist "Lateral Movement"



```
mimikatz 2.1 x64 (oe.eo)

#####   mimikatz 2.1 (x64) built on Jan 21 2017 01:22:06
.## ^ ##.   "A La Vie, A L'Amour"
## < > ##   /* * *
## \ / ##   Benjamin DELPY 'gentilkiwi' < benjamin@gentilkiwi.com >
'## v ##'   http://blog.gentilkiwi.com/mimikatz           (oe.eo)
#####           with 20 modules * * */

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # log sekurlsa.log
Using 'sekurlsa.log' for logfile : OK

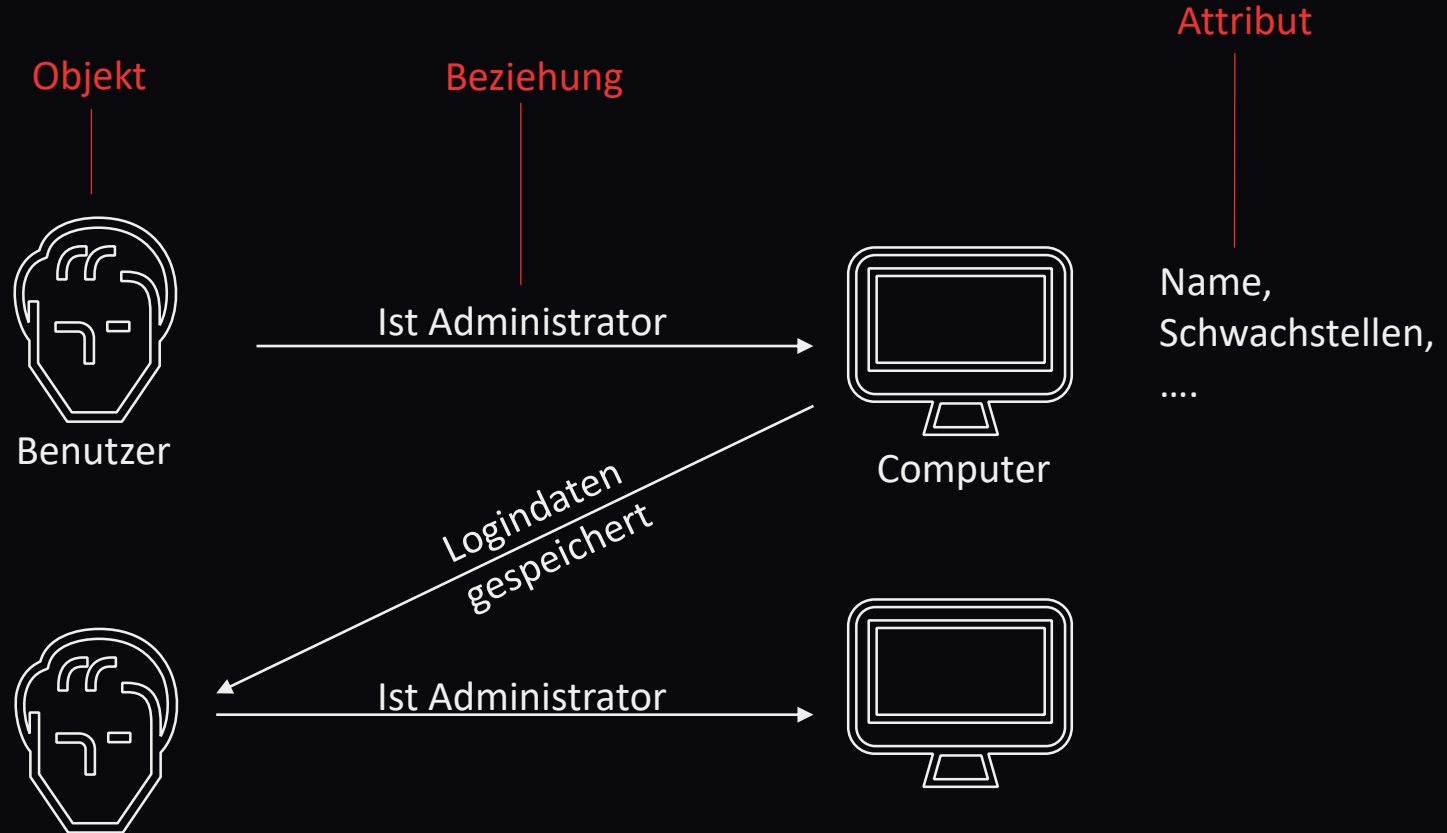
mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 110295 (00000000:0001aed7)
Session           : Interactive from 1
User Name         : Adam
Domain            : PC1
Logon Server      : PC1
Logon Time        : 29/01/2017 13:04:50
SID               : S-1-5-21-3717405039-3355736400-127772160-1001

msv :
[00000003] Primary
* Username : Adam
* Domain   : PC1
* LM       : e52cac67419a9a22664345140a852f61
* NTLM     : 58a478135a93ac3bf058a5ea0e8fdb71
* SHA1     : 0d7d930ac3b1322c8a1142f9b22169d4eef9e855
tspkg :
* Username : Adam
* Domain   : PC1
* Password : Password123
wdigest :
* Username : Adam
* Domain   : PC1
* Password : Password123
kerberos :
* Username : Adam
* Domain   : PC1
* Password : Password123
ssp :
credman :
```

Angreifer hat Zugriff auf Logindaten

Vorwissen: Was ist ein Graph?



Credits: Initiale Idee der Darstellung als Graph



Andrew Robbins
@_wald0

Pentester and Red Team Lead at [@SpecterOps](#). Co-creator of [#BloodHound](#) with [@CptJesus](#) and [@harmj0y](#). Please consider donating to MDA: bit.ly/2pz7plo

📍 Seattle, WA
wald0.com



Will
@harmj0y

Offensive Engineer [@SpecterOps](#) | co-founder Empire, BloodHound, GhostPack, Veil-Framework | Microsoft MVP | security at the misfortune of others

📍 Seattle, WA
blog.harmj0y.net



Rohan Vazarkar
@CptJesus

Penetration Tester and BloodHound Developer [@specterops](#)


blog.cptjesus.com

<https://bloodhoundgang.herokuapp.com/>
<https://github.com/BloodHoundAD/>

Was hat Tanium damit zu tun?



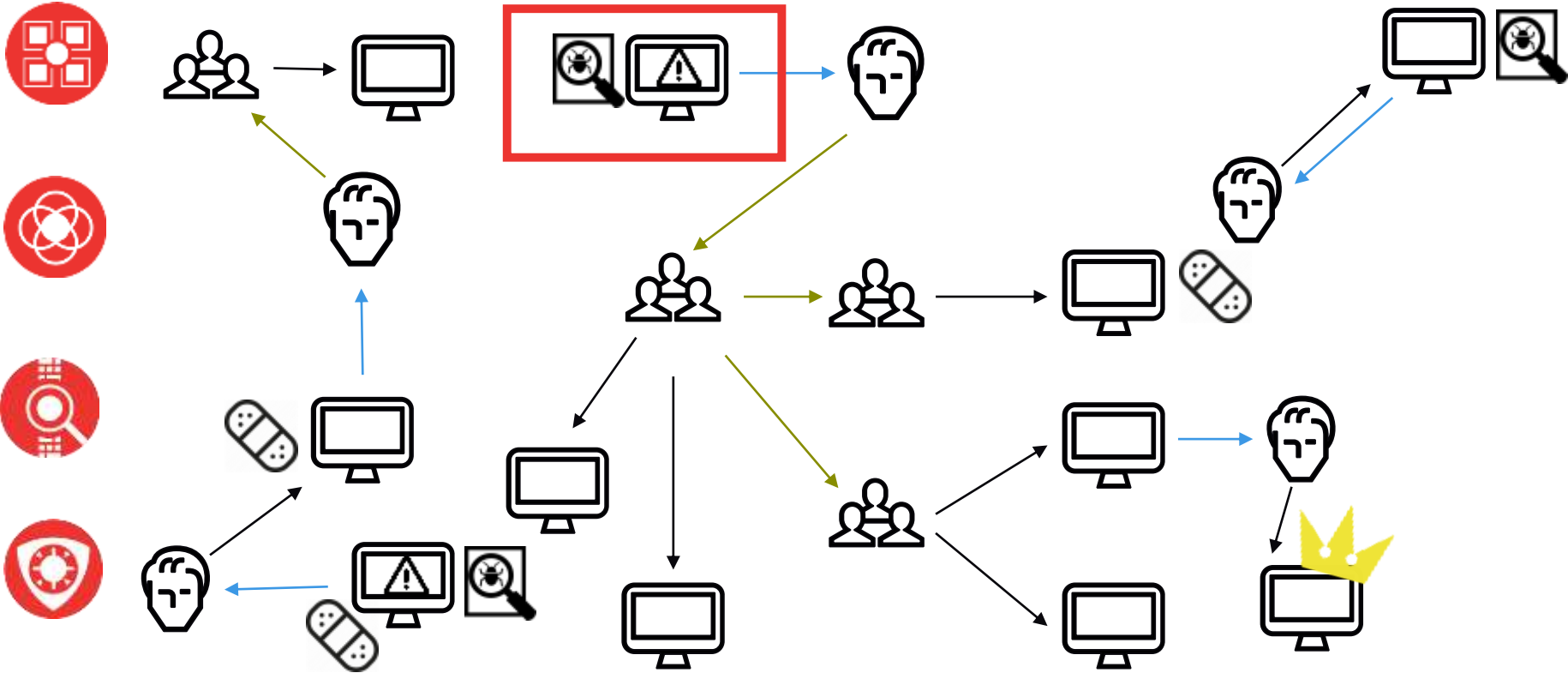
- Voller Überblick über alle Endpunkte in Sekunden
- Schwachstellenscans, Fehlende Patches, Berechtigungen, Identifikation von auffälligem Verhalten ...
- Möglichkeit Fehler direkt zu beheben



Wie können uns Graphen helfen Risiken
besser einzuschätzen?

Visualize, Contextualize, Prioritize

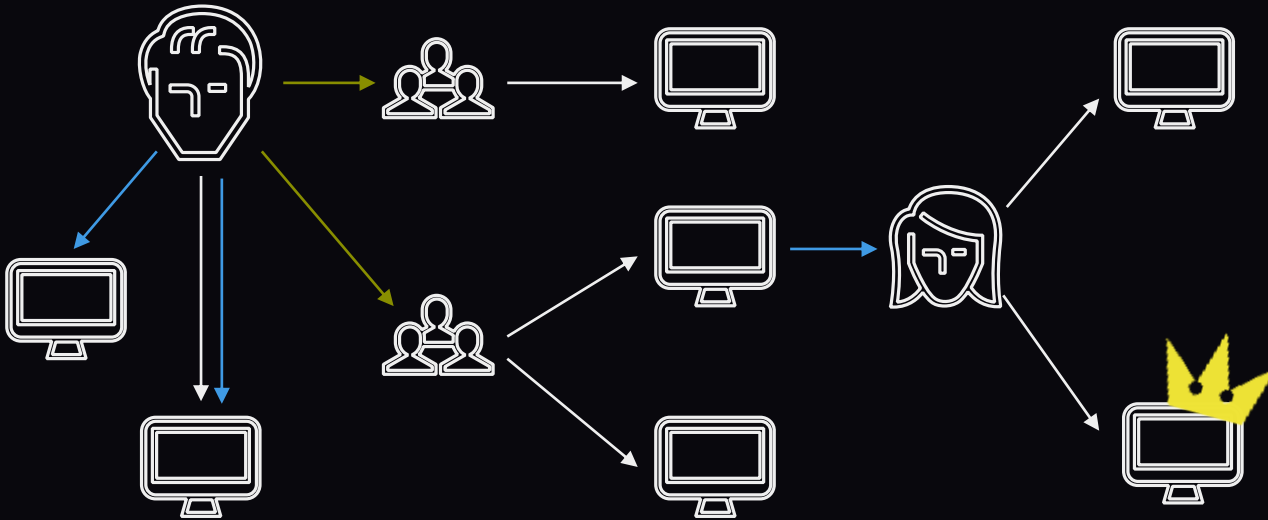
- AdminTo
- MemberOf
- HasSession





Welche Werte können helfen?

Details: Benutzer



- Name: Bob
- Direkter Admin zu: 1
- Sessions: 2
- Indirekter Admin zu: 3
- Breach Zugriff auf: 2
- Zugriff auf kritische Assets: 1

Example risk formula:

$((\text{Direct Admin Rights} + \text{Group Administrators Rights} + \text{Total Admin Rights}) * (\text{Sessions} + 1)) * (\text{No of critical assets access} + 1)$

Details: Active Directory Gruppen

- Groupname: service_desk@awesome.local
- Direct Members: 10
- Indirect Members: 5
- Direct Admin to: 25
- Indirect Admin to: 3
- Lateral Movement access to: 50
- Access to critical assets: 2

Example risk formula AD groups:

$((\text{Direct Members} + \text{Indirect Members}) * (\text{Admin to} + \text{Indirect Admin To}) + \text{Lateral Movement access}) * (\text{Critical Assets} + 1)$

Umsetzung in der Praxis (Benutzerdaten)

User Data

Show entries Search:

Name	Direct Admin to	Indirect Admin to (Group Membership)	Derivative Admin rights (Lateral Movement)	Sessions	No of direct group memberships	Direct Risk Rate	Derivative Risk Rate
AWESOME\SVC_TANIUM	3	7	7	2	2	60	81
AWESOME\BARBER	3	7	7	1	2	40	54
AWESOME\ADMIN	2	7	7	1	3	36	50
AWESOME\ADMINISTRATOR	1	7	7	1	3	32	46
AWESOME\MMOSS	1	2	7	2	2	18	39
AWESOME\SMOLLS	2	7	7	0	2	18	25
AWESOME\DREYNHOLM	1	1	1	1	1	8	10
AWESOME\RTRENNEMAN	1	1	7	1	1	8	22
AWESOME\ABBOTASH	0	1	1	0	1	2	3
AWESOME\ABBOTDON	0	1	1	0	1	2	3

Umsetzung in der Praxis (Computerdaten)

Computer Data

Show 10 entries

Search:

Name	Direct Administrators	Indirect Administrators (Due to Group memberships)	Derivative Access (Lateral Movement)	Sessions	Missing Critical Patches	Vulnerabilities	Direct Risk Rate	Derivative Risk Rate
TESTRAILTS1.AWESOME.LOCAL	1	5	6	1	7	588	599	605
SPLUNK.AWESOME.LOCAL	2	551	0	1	31	No recorded vulns	585	585
CLIENT2.AWESOME.LOCAL	8	5	8	2	52	No recorded vulns	65	71
JENKINS1.AWESOME.LOCAL	3	6	8	2	29	No recorded vulns	40	46
DC1.AWESOME.LOCAL	1	5	6	2	20	No recorded vulns	28	34
TESTRAILTMS1.AWESOME.LOCAL	1	5	6	1	7	588	14	20
TESTRAILSQL.AWESOME.LOCAL	0	0	0	0	7	585	7	7

Umsetzung in der Praxis

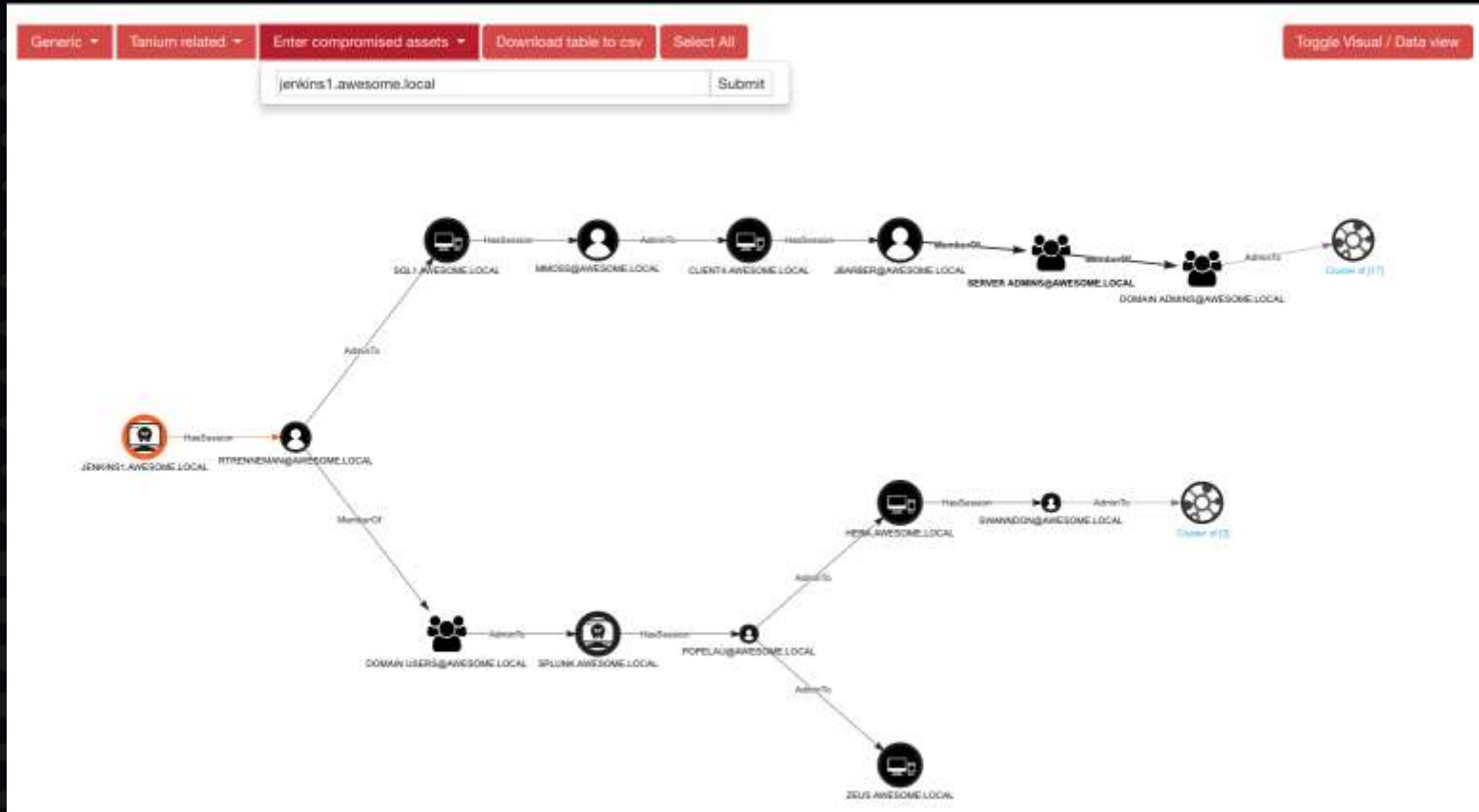
Vulnerability Data

Show 10 entries

Search:

Name	CVSS	Severity	Direct Affected	Derivative Impact
.NET and .NET Core Denial of Service Vulnerability - CVE-2018-0755	5	Medium	3	7
.NET Core Denial Of Service Vulnerability - CVE-2018-0764	5	Medium	2	7
.NET Core Information Disclosure Vulnerability - CVE-2018-8282	5	Medium	0	0
.NET Framework and .NET Core Denial of Service Vulnerability - CVE-2019-0820	5	Medium	5	7
.NET Framework and .NET Core Denial of Service Vulnerability - CVE-2019-0980	5	Medium	3	7
.NET Framework and .NET Core Denial of Service Vulnerability - CVE-2019-0981	5	Medium	5	7
.NET Framework and Visual Studio Remote Code Execution Vulnerability - CVE-2019-0613	9.3	High	3	7
.NET Framework and Visual Studio Spoofing Vulnerability - CVE-2019-0657	4.3	Medium	3	7
.NET Framework Denial Of Service Vulnerability - CVE-2018-8517	5	Medium	3	7
.NET Framework Device Guard Security Feature Bypass Vulnerability - CVE-2018-1039	4.6	Medium	3	7

Umsetzung in der Praxis (Visualisierung)



Besuchen Sie unseren Stand:
Hall 10.1, Stand 420

Stefan Molls | Technical Account Manager – EMEA, Tanium