Adrian Vollmer

THE PENTEST EXPERTS.

Better Passwords Project

The State of Active Directory Passwords

Who am I?

```
C:\> whoami /all
USER INFORMATION
----------------

Full Name:         Adrian Vollmer
Organisation:      SySS GmbH
Occupation:        Penetration Tester
Focus:             Active Directory
Account created:   Jan 2015
Social:            github.com/AdrianVollmer; @mr_mitm
```

Why this talk?

- ➔ Web services have different threat models than Active Directory
- ➔ Clear up misinformation about passwords
- ➔ Tool release
- ➔ Finding weak points in AD networks
- ➔ New insight on security-related topics in an AD network

When are password guessing attacks relevant? (in Active Directory)

- ➔ Online Password Guessing
- ➔ Kerberoast
- ➔ NTLM-Authentication
- ➔ Domain Cached Credentials (DCC)
- ➔ NT-Hashes?

Online Password Guessing

- Tools:
  - Metasploit's `smb_login`
  - `kerbrute`
  - ...
- Typical frequency:
  - $10/\mathrm{s}$ (without lockout threshold)
  - $5/\mathrm{h}$ (with lockout threshold)
- Unauthenticated $\longrightarrow$ Domain User

Kerberoast

- Crack Kerberos tickets
- Potential “quick win”
- Tools:
  - Impacket’s `GetUserSPNs.py`
  - PowerSploit’s `Invoke-Kerberoast`
  - ...
- Typical frequency: $10^9/\text{s}$ (etype23)
- Domain User $\rightarrow$ Domain User

```
$krb5tgs$23$*SVC_SAP2014$ACME.CORP$acme.copr/SVC_SAP2014*$f6df40df22cf4fc
ba657d88271cb6588ea4185126ab66cdd893947702d2b9b40afc1cb1915f84d7d9e9fa23c
e478a2a0278c3e9fc14b97338852bac5eb812b829e79e5cdf97e66bcf8f3ac754a7b866e4
ef3cbe42b5006ec9b2925b4a52fc1f5f20665cfcb9525ce06fe471ca1abcb8c43b3ef3492
7fc6342a2fe8ef64aee52abda141d89e4592d7e0971f86618d193d9cc3dfbf39a3642e511
b49a2a90aade825413b28043ec6323857143621fad0be904e65c8810e80658e9e89e280dd
18f7f95526da0966d64caf04ac835913224cab7856600422831f6349e104ab601936665d4
a09c1d4d999b2f30f1e8fea9a8b18bdf52cfe37137a1d2a8374e603281540cffeb21be3b3
666b02bd1eaa787136ef639e9d5a17d04465f932c5252fca912c1885d600c83356afd9a63
7eed1f5647b7733b118599cb03a95031ad840ce9bc2297d07bc5c06e7cd60f661143535781
d7dfa83a9df385e41bc6000453526d938a07ed4e199c0a22d86f5b0c62d3444834749f726
ca
```

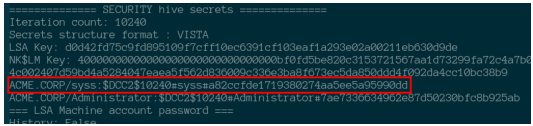
NTLM-Authentication

- Widespread in Windows networks: used in SMB, LDAP, RDP, HTTP, ...
- Tools:
  - `responder`
  - `wireshark`
  - `seth`
  - ...
- Typical frequency: $10^8/\mathrm{s}$
- Unauth. $\rightarrow$ Local User/Domain User

```
DomAdmin1::RD14:0e5b912786ee3f95:dd23d1aa5622408398bb4
0101000000000000047e99827a098d201862b2213032bac62000000
0044003100340001000800440043003000310004001400720064006
6c006f00630061006c0003001e00640063003000310002e00720064
006c006f00630061006c0005001400720064003100340002e006c00
6c000700080047e99827a098d2010600040002000000080030003000
0000000000002000004cfa6e96109bd90f6a4080daaa8e264e4ebf
787f53e389d96b180a0010000000000000000000000000000000000000
00450052004d00530052005600 2f00640063003000310002e007200
2e006c006f00630061006c000000000000000000000000000000
```

Domain Cached Credentials

- Provide Offline Logon Functionality
- Stored in `HKLM:/SECURITY`
- Tools:
  - Impacket's `secretsdump`
  - `pypykatz`
  - Metasploit's `post/windows/gather/cachedump`
- Typical frequency: $10^6/\mathrm{s}$ (DCC2)
- Local Admin $\rightarrow$ Domain User



NT-Hash

- How Windows and AD store passwords
- Stored in `HKLM:/SAM` or `ntds.dit`
- Cracking usually not necessary! Simply pass the hash.
- Tools:
  - Impacket's `secretsdump`
  - `pypykatz`
  - ...
- Typical frequency: $10^{11}/\mathrm{s}$
- Domain Admin $\xrightarrow{?}$ Domain User; Local Admin $\xrightarrow{?}$ Local User

Overview

Scenario	Freq [1/s]*	Escalation
Online	10	Unauthenticated $\longrightarrow$ Domain User
DCC	10^6	Local Admin $\longrightarrow$ Domain User
NTLM	10^8	Unauthenticated $\longrightarrow$ Domain User
Kerberoast	10^9	Domain User $\longrightarrow$ Domain User
NT	10^{11}	(Domain/Local) Admin $\xrightarrow{?}$ (Domain/Local) User
LM	10^{11}	(Domain/Local) Admin $\xrightarrow{?}$ (Domain/Local) User

* on an i7-6800K@3.40GHz, 64GB RAM, twelve cores, four GeForce RTX 2080

Idea: Benchmark

- ➔ Customers love being rated
- ➔ Can it be done objectively?
- ➔ Choose a fixed wordlist
- ➔ Choose a fixed ruleset
- ➔ Build a corpus of non-identifying results

Hashcathelper Workflow

1. Become Domain Admin
2. Retrieve hashes (e.g. with `secretsdump`)
3. `hashcathelper ntlm dc01.ntds`
4. `hashcathelper analytics -H dc01.ntds -A dc01.ntds.out -f json -o report.json`
5. `hashcathelper db submit report.json`
6. `hashcathelper db stats`

Hint: Use `secretsdump` with `-user-status`

Hashcathelper Analytics

Remove deactivated accounts and computer accounts and determine:

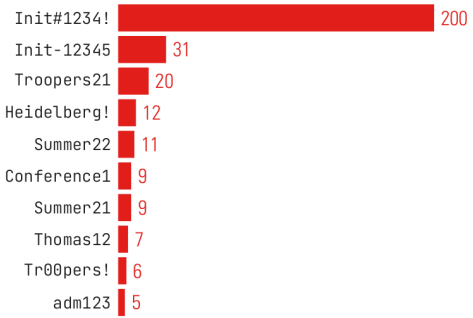
1. Cracked passwords
2. User equals password
3. Non-empty LM hashes
4. Accounts with non-unique passwords
5. Accounts with blank passwords
6. Password clusters
7. Top 10 passwords, Top 10 basewords

Store statistical information in database

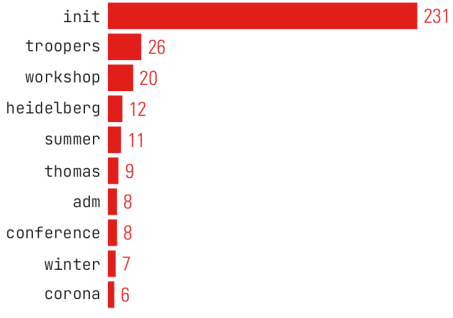
Hashcathelper: Key Results

Total accounts	4360
Removed	1861
Accounts considered	2499
Passwords cracked	892 (35.69%)
User name = password	0 (0.0%)
Non-empty LM hashes	0 (0.0%)
Accounts with nonunique passwords	912 (36.49%)
Accounts with blank password	0 (0.0%)
Average password length	9.84
Median password length	10.0
Average number of character classes	3.37

Hashcathelper: Top 10



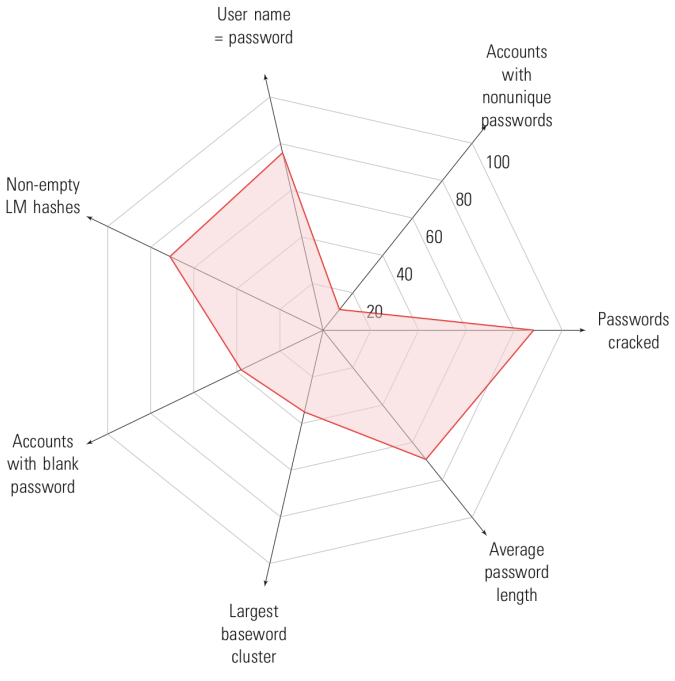
Top 10 of cracked passwords



Top 10 Bases of cracked passwords

Hashcathelper: Statistics

	Value	Mean	Std. Dev.	Percentile
Passwords cracked (%)	35.69	54.92	16.59	88
Accounts with nonunique passwords (%)	36.49	23.8	12.85	11
User name = password (%)	0.0	2.16	7.07	76
Non-empty LM hashes (%)	0.0	7.69	13.82	71
Accounts with blank password (%)	0.0	2.53	9.14	38
Largest baseword cluster (%)	10.24	9.81	8.91	35
Average password length	9.84	9.42	1.11	69


User name
= password
Accounts
with
nonunique
passwords
100
80
60
40
20
Passwords
cracked
Average
password
length
Largest
baseword
cluster
Accounts
with blank
password
Non-empty
LM hashes

Our Dictionary Attack

- Wordlist: Crackstation[1] + Hashes.org (2 316 703 347 unique entries; 26GB)
  - Contains Wikipedia (all languages), Project Gutenberg, password breaches, other wordlists, dictionaries, ...
- Rule set: OneRule[2]
- 120 460 563 559 138 candidates
- Takes around seven hours on our rig
- $\mathcal{O}(1)$, not $\mathcal{O}(n)$

[1] `https://crackstation.net/crackstation-wordlist-password-cracking-dictionary.htm`

[2] `https://notsosecure.com/one-rule-to-rule-them-all`

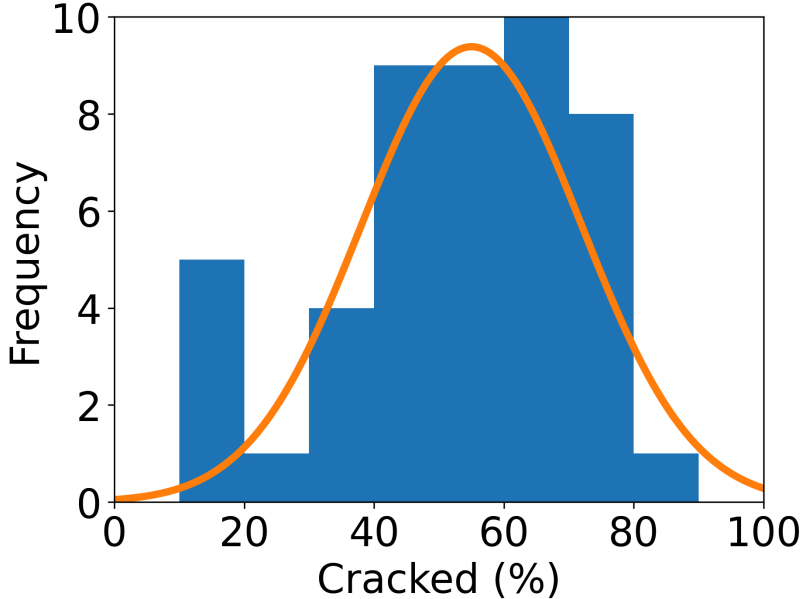
Result

Average percentage of cracked accounts

$$55 \pm 17\%$$

based on 167 135 accounts from 44 organizations

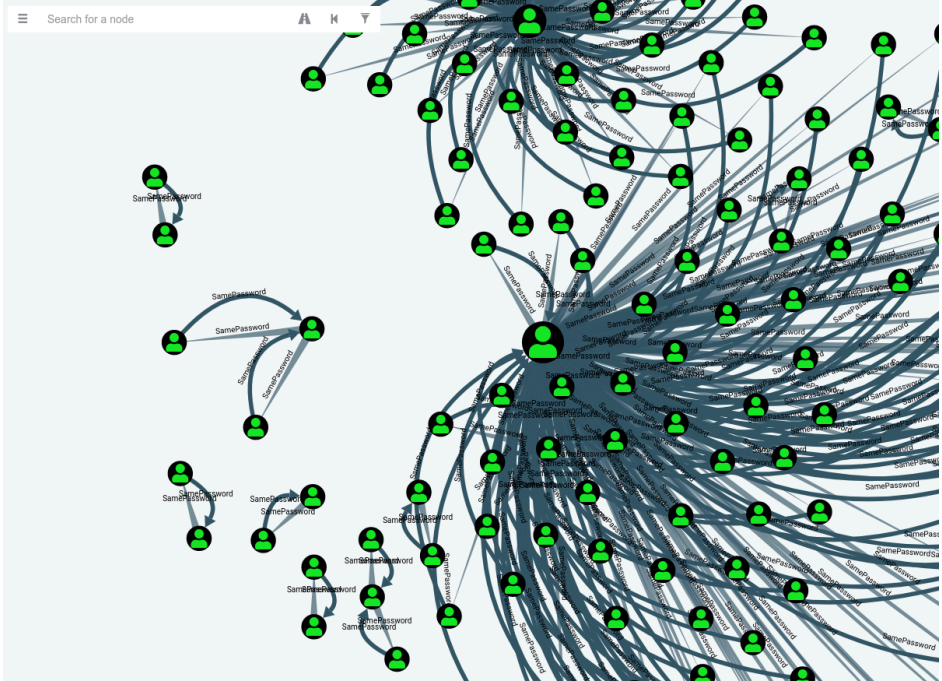
Actual distribution vs. normal distribution



More features

THE PENTEST EXPERTS.

- ➔ Find passwords in “Have I Been Pwnd?” database
- ➔ Use Cypher queries as filters
- ➔ Add Bloodhound edges of type `SamePassword`


Search for a node
SamePassword


Shortest Paths from Kerberoastable Users
Shortest Paths to Domain Admins from Kerberoastable Users
Shortest Path from Owned Principals
Shortest Paths to Domain Admins from Owned Principals
Shortest Paths to High Value Targets
Shortest Paths from Domain Users to High Value Targets
Find Shortest Paths to Domain Admins
Custom Queries
Hashcathelper
Show SamePassword clusters
Show SamePassword cluster for specific user
Show SamePassword clusters of admins (adjust the regex in the Raw Query - needs Query Debug Mode)
Uncategorized Query
SamePassword
Raw Query
MATCH p=((a:User)-[:SamePassword*1..2]-(b:User)) WHERE a.name =~ '(?i)adm_.*' return p


GenericAll
SamePassword
SamePassword
AdminTo
HasSession
SamePassword
MemberOf

Common counter measures

- Minimum length and complexity
  - `Passw0rd123!` is long, complex and weak
- Password filters
  - Banned words
  - Check with HIBP
  - Only proactive
  - May disallow perfectly fine passwords
  - Does not find password reuse
  - Doesn't even have 120 trillion entries

Lessons for admins

THE PENTEST EXPERTS.

- ➔ Forget about Greg and Janet in accounting; just use a blocklist, MFA and lockout thresholds for low priv accounts
- ➔ Focus on administrative accounts and service accounts. Generated passwords. No excuses!
- ➔ Don't forget about password reuse between tiered accounts
- ➔ If you can, run secretsdump+hashcathelper yourself

Lessons for admins

- Forget about Greg and Janet in accounting; just use a blocklist, MFA and lockout thresholds for low priv accounts
- Focus on administrative accounts and service accounts. Generated passwords. No excuses!
- Don't forget about password reuse between tiered accounts
- If you can, run secretsdump+hashcathelper yourself
- Don't use Windows and Active Directory, I guess?

Download Hashcathelper

THE PENTEST EXPERTS.

https://github.com/SySS-Research/hashcathelper

THE PENTEST EXPERTS

WWW.SYSS.DE