I Know Your Password

Patrick Laverty
whoami

Patrick Laverty
Penetration Tester for Rapid7
Work in Rhode Island
Run Defcon 401, OWASP RI, Layer 8 Conference
@plaverty9 (Twitter & LinkedIn)
I crack passwords for fun!
*Guidelines*

All cracked passwords were type NTLM
All were taken from real, production Active Directory instances
Cracking used the 95 available characters on a typical US keyboard
YMMV with other types of password hashes
What Are You Talking About?

Cracking real, active password hashes
How strong are the passwords?
Password policy effectiveness
Commonly seen passwords
Password patterns
Password cracking basics
You can try it too!
Wait, these are real?!?

Not just my pentests, other testers
Achieve Domain Administrator access
Extract hashes from NTDS.dit
Extract password policy
What does it look like?
[*] Windows Server (R) 2008 Enterprise 6001 Service Pack 1 x64 [name:DC1] (domain:EMPIRE) (signing:True) (SMBv1:True)

[*] EMPIRE:Vader|LördVader! (Pun3d!)

[+] Dumping the NTDS, this could take a while so go grab a redbull...

Administrator:500:aadd3b4555104aeaaa3b4555104ae:aee4f12ccdaa0b0857e0ababa0b34e773b499b:
Guest:501:aadd3b4555104aeaaa3b4555104ae:a316e90916e5931c595d70089c0:
Krbtgt:502:aadd3b4555104aeaaa3b4555104ae:a224a85d12477a4ab1e:
Vader:1000:aadd3b4555104aeaaa3b4555104ae:73ae3dcb25ef88b5006e6f4d3c7550:

eempire\.local\jarjar:1105:aadd3b4555104aeaaa3b4555104ae:60952501d6fd51a0105d4a43b3b23:

eempire\.local\luke:1107:aadd3b4555104aeaaa3b4555104ae:385455bbd6d87c929b2ff52058a:

eempire\.local\luke:1109:aadd3b4555104aeaaa3b4555104ae:58c7dbaf8a1875b8d7422c84e1650b09:

[+] Dumped 43 NTDS hashes to /root/.cme/Logs/DC1 192.168.253.53 2018-08-01 123053.ntds of which 7 were added to the database.
I’m ready for my close-up
What is all that?

Administrator – Username
What is all that?

Administrator – Username
500 – Windows Relative Identifier (RID)
What is all that?

Administrator – Username
500 – Windows Relative Identifier (RID)
aad3b4... - LanManager (LM) Hash
What is all that?

Administrator – Username
500 – Windows Relative Identifier (RID)
aad3b4… - LanManager (LM) Hash
64f12cdd – NTLM Hash
About LM Hashes

Pre-Windows NT password hashes
Still exist for backwards compatibility
(should be) Disabled when replaced

“aad3b435b51404eeaad3b435b51404ee”
About LM Hashes – Why Do We Care?
About LM Hashes – Why Do We Care?

Max password length is 14 chars
Letters stored in uppercase
Broken in half, each half hashed
Two 7 char passwords, no lowercase
Easy to bruteforce
Existence means NTLM matches
Start cracking here
Example?
Moving on...NTLM

Most cracking is on the second part
Using Hashcat

https://hashcat.net

Works better with GPU

Manual: https://hashcat.net/wiki/

How does it work?
Using Hashcat

hashcat hashes.txt –m1000 –a0 –w4 –O –r rules.txt words.txt

m – hashtype (1000 = NTLM)
a – attack type ( 0 = “straight”, rules/wordlist)
w – workload profile (4 = “nightmare”, “insane” power consumption)
O – enable optimized kernel
r – file containing cracking rules
Check the Potfile

Efficiency/speed
File containing known hash/password
Updates when new combination found
Can be manually updated
Plain text

7F4F718D5029000926A9278C5CFD0872:Summer2018
Using Hashcat

Session.........: hashcat
Status...........: Exhausted
Hash.Type........: NTLM
Hash.Target......: hashes.txt
Time.Estimated...: Mon Aug 6 11:41:50 2018 (0 secs)
Guess.Base.......: File (wordlists/rockyou.txt)
Guess.Mod.........: Rules (rules/InsidePro-PasswordsPro.rule)
Guess.Queue......: 1/1 (100.00%)
Speed.Dev.#1.....: 5976.2 MH/s (38.13ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#2.....: 5755.9 MH/s (37.93ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#3.....: 5754.0 MH/s (38.40ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#4.....: 6085.4 MH/s (38.78ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#*......: 23571.6 MH/s
Recovered........: 3234/12523 (25.82%) Digests, 0/1 (0.00%) Salts
Recovered/Time...: CUR:N/A,N/A,N/A AVG:80071,4804289,115302907 (Min,Hour,Day)
Progress.........: 44755903920/44755903920 (100.00%)
Rejected..........: 20398560/44755903920 (0.05%)
Restore.Point.....: 10469932/14344841 (72.99%)
Candidates.#1.....: chasiangcarr --> Zalix
Candidates.#2.....: 1994_arabbit --> Zurich710$
Candidates.#3.....: 8475/a8475 --> 1994_ralou
Candidates.#4.....: ZALISaSA3207 --> 8475

HwMon.Dev.#1.....: Temp: 38c Fan: 27% Util: 0% Core:1860MHz Mem:4513MHz Bus:16
HwMon.Dev.#2.....: Temp: 46c Fan: 27% Util: 99% Core:1873MHz Mem:4513MHz Bus:16
HwMon.Dev.#3.....: Temp: 46c Fan: 28% Util: 97% Core:1860MHz Mem:4513MHz Bus:16
HwMon.Dev.#4.....: Temp: 47c Fan: 30% Util: 58% Core:1847MHz Mem:4513MHz Bus:16
Using Hashcat

Session.........: hashcat
Status.........: Exhausted
Hash.Type......: NTLM
Hash.Target....: hashes.txt
Time.Estimated.: Mon Aug  6 11:41:50 2018 (0 secs)
Guess.Base.....: File (wordlists/rockyou.txt)
Guess.Mod......: Rules (rules/InsidePro-PasswordsPro.rule)
Guess.Queue....: 1/1 (100.00%)
Speed.Dev.#1....: 5976.2 MH/s (38.13ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#2....: 5754.0 MH/s (38.40ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#4....: 6085.4 MH/s (38.78ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#4*...: 23571.6 MH/s
Recovered......: 3234/12523 (25.82%) Digests, 0/1 (0.00%) Salts
Recovered/Time.: CUR:N/A,N/A,N/A AVG:80071,4804289,115302907 (Min,Hour,Day)
Progress........: 44755903920/44755903920 (100.00%)
Rejected........: 20399560/44755903920 (0.05%)
Restore.Point...: 14469932/14344841 (72.99%)
Candidates.#1...: chasiangcarr -> Zalix
Candidates.#2...: 994_arabbit -> Zurich710$
Candidates.#3...: 84755/84750 -> 7994_ralou
Candidates.#4...: ZALISaSA3207 -> 84750
HwMon.Dev.#1....: Temp: 38c Fan: 27% Util: 0% Core:1860MHz Mem:4513MHz Bus:16
HwMon.Dev.#2....: Temp: 46c Fan: 27% Util: 99% Core:1873MHz Mem:4513MHz Bus:16
HwMon.Dev.#3....: Temp: 46c Fan: 28% Util: 97% Core:1860MHz Mem:4513MHz Bus:16
HwMon.Dev.#4....: Temp: 47c Fan: 30% Util: 58% Core:1847MHz Mem:4513MHz Bus:16
Using Hashcat

<table>
<thead>
<tr>
<th>Session............</th>
<th>hashcat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status...............</td>
<td>Exhausted</td>
</tr>
<tr>
<td>Hash.Type............</td>
<td>NTLM</td>
</tr>
<tr>
<td>Hash.Target.. ........</td>
<td>hashes.txt</td>
</tr>
<tr>
<td>Time.Estimated.......</td>
<td>Mon Aug 6 11:41:50 2018 (0 secs)</td>
</tr>
<tr>
<td>Guess.Base...........</td>
<td>Fite (wordlists/rockyou.txt)</td>
</tr>
<tr>
<td>Guess.Mod............</td>
<td>Rules (rules/InsidePro-PasswordsPro.rule)</td>
</tr>
<tr>
<td>Guess.Queue..........</td>
<td>1/1 (100.00%)</td>
</tr>
<tr>
<td>Speed.Dev.#1.........</td>
<td>5976.2 MH/s (38.13ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev.#2.........</td>
<td>5755.9 MH/s (37.93ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev.#3.........</td>
<td>5754.0 MH/s (38.40ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev.#4.........</td>
<td>6085.4 MH/s (38.78ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev.#*.........</td>
<td>23571.6 MH/s</td>
</tr>
<tr>
<td>Recovered............</td>
<td>3234/12523 (25.82%) Digests, 0/1 (0.00%) Salts</td>
</tr>
<tr>
<td>Recovered/Time.......</td>
<td>CUR:N/A,N/A,N/A AVG:80071,4804289,115302907 (Min,Hour,Day)</td>
</tr>
<tr>
<td>Progress.............</td>
<td>44755903920/44755903920 (100.00%)</td>
</tr>
<tr>
<td>Rejected.............</td>
<td>20398560/44755903920 (0.05%)</td>
</tr>
<tr>
<td>Restore.Point.........</td>
<td>10469932/14344841 (72.99%)</td>
</tr>
<tr>
<td>Candidates.#1........</td>
<td>chasiangcarr --&gt; Zalix</td>
</tr>
<tr>
<td>Candidates.#2........</td>
<td>1994_arabibit --&gt; Zurich710$</td>
</tr>
<tr>
<td>Candidates.#3........</td>
<td>8475/a8475 --&gt; 1994_ralou</td>
</tr>
<tr>
<td>Candidates.#4........</td>
<td>ZALIsaSA3207 --&gt; 84750</td>
</tr>
<tr>
<td>HwMon.Dev.#1.........</td>
<td>Temp: 38c Fan: 27% Util: 0% Core:1860MHz Mem:4513MHz Bus:16</td>
</tr>
<tr>
<td>HwMon.Dev.#2.........</td>
<td>Temp: 46c Fan: 27% Util: 99% Core:1873MHz Mem:4513MHz Bus:16</td>
</tr>
<tr>
<td>HwMon.Dev.#3.........</td>
<td>Temp: 46c Fan: 28% Util: 97% Core:1860MHz Mem:4513MHz Bus:16</td>
</tr>
<tr>
<td>HwMon.Dev.#4.........</td>
<td>Temp: 47c Fan: 30% Util: 58% Core:1847MHz Mem:4513MHz Bus:16</td>
</tr>
</tbody>
</table>
Using Hashcat

<table>
<thead>
<tr>
<th>Session</th>
<th>hashcat</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Exhausted</td>
</tr>
<tr>
<td>Hash.Type</td>
<td>NTLM</td>
</tr>
<tr>
<td>Hash.Target</td>
<td>hashes.txt</td>
</tr>
<tr>
<td>Time.Estimated</td>
<td>Mon Aug 6 11:41:50 2018 (0 secs)</td>
</tr>
<tr>
<td>Guess.Base</td>
<td>File (wordlists/rockyou.txt)</td>
</tr>
<tr>
<td>Guess.Mod</td>
<td>Rules (rules/InsidePro-PasswordsPro.rule)</td>
</tr>
<tr>
<td>Guess.Queue</td>
<td>1/1 (100.00%)</td>
</tr>
<tr>
<td>Speed.Dev. #1</td>
<td>5976.2 MH/s (38.13ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev. #2</td>
<td>5755.9 MH/s (37.93ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev. #3</td>
<td>5754.0 MH/s (38.40ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev. #4</td>
<td>6005.4 MH/s (38.78ms) @ Accel:64 Loops:256 Thr:1024 Vec:1</td>
</tr>
<tr>
<td>Speed.Dev. #**</td>
<td>23571.6 MH/s</td>
</tr>
<tr>
<td>Recovered</td>
<td>323471293 (25.82%) Digests, 0/1 (0.00%) Salts</td>
</tr>
<tr>
<td>Recovered/Time</td>
<td>CUR:N/A,N/A,N/A AVG:80071,4804289,115302907 (Min,Hour,Day)</td>
</tr>
<tr>
<td>Progress</td>
<td>44755903920/44755903920 (100.00%)</td>
</tr>
<tr>
<td>Rejected</td>
<td>20398560/44755903920 (0.05%)</td>
</tr>
<tr>
<td>Restore.Point</td>
<td>10469932/14344841 (72.99%)</td>
</tr>
<tr>
<td>Candidates #1</td>
<td>chasiangarcia -&gt; Zalix</td>
</tr>
<tr>
<td>Candidates #2</td>
<td>1994_arabbit -&gt; Zurich710$</td>
</tr>
<tr>
<td>Candidates #3</td>
<td>8475/a8475 -&gt; 1994_ralou</td>
</tr>
<tr>
<td>Candidates #4</td>
<td>ZALIsaSA3207 -&gt; 84750</td>
</tr>
<tr>
<td>HWMon.Dev. #1</td>
<td>Temp: 38c Fan: 27% Util: 0% Core:1860MHz Mem:4513MHz Bus:16</td>
</tr>
<tr>
<td>HWMon.Dev. #2</td>
<td>Temp: 46c Fan: 27% Util: 99% Core:1873MHz Mem:4513MHz Bus:16</td>
</tr>
<tr>
<td>HWMon.Dev. #3</td>
<td>Temp: 46c Fan: 28% Util: 97% Core:1860MHz Mem:4513MHz Bus:16</td>
</tr>
<tr>
<td>HWMon.Dev. #4</td>
<td>Temp: 47c Fan: 30% Util: 58% Core:1847MHz Mem:4513MHz Bus:16</td>
</tr>
</tbody>
</table>
Using Hashcat

| Session.........: hashcat |
| Status..........: Exhausted |
| Hash.Type.......: NTLM |
| Hash.Target.....: hashes.txt |
| Time.Estimated.: Mon Aug  6 11:41:50 2018 (0 secs) |
| Guess.Base.....: File (wordlists/rockyou.txt) |
| Guess.Mod.......: Rules (rules/InsidePro-PasswordsPro.rule) |
| Guess.Queue.....: 1/1 (100.00%) |
| Speed.Dev.#1....: 5976.2 MH/s (38.13ms) @ Accel:64 Loops:256 Thr:1024 Vec:1 |
| Speed.Dev.#2....: 5755.9 MH/s (37.93ms) @ Accel:64 Loops:256 Thr:1024 Vec:1 |
| Speed.Dev.#3....: 5754.0 MH/s (38.04ms) @ Accel:64 Loops:256 Thr:1024 Vec:1 |
| Speed.Dev.#4....: 6085.4 MH/s (38.78ms) @ Accel:64 Loops:256 Thr:1024 Vec:1 |
| Speed.Dev.#5....: 33571.6 MH/s |

**Recovered:** 3234/12523 (25.82%) Digests, 0/1 (0.00%) Salts

**Recovered/Time:** Cor:80071,4804289,115302907 (Min,Hour,Day)

**Progress:** 34755903920/44755903920 (100.00%)

**Rejected:** 20398560/44755903920 (0.05%)

**Restore.Point:** 10469932/14344841 (72.99%)

**Candidates.**
- #1: chasiangcarr -> Zalix
- #2: 1994_arabbit -> Zurich710$
- #3: 8475/a8475 -> 1994_ralou
- #4: ZALIaSA3207 -> 84750

**HwMon.Dev.#1:** Temp: 38c Fan: 27% Util: 0% Core:1860MHz Mem:4513MHz Bus:16

**HwMon.Dev.#2:** Temp: 46c Fan: 27% Util: 99% Core:1873MHz Mem:4513MHz Bus:16

**HwMon.Dev.#3:** Temp: 46c Fan: 28% Util: 97% Core:1860MHz Mem:4513MHz Bus:16

**HwMon.Dev.#4:** Temp: 47c Fan: 30% Util: 58% Core:1847MHz Mem:4513MHz Bus:16
Using Hashcat

Session.........: hashcat
Status.........: Exhausted
Hash.Type.......: NTLM
Hash.Target.....: hashes.txt
Time.Estimated.: Mon Aug 6 11:41:50 2018 (0 secs)
Guess.Base......: File (wordlists/rockyou.txt)
Guess.Mod.......: Rules (rules/InsidePro-PasswordsPro.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.Dev.#1....: 5976.2 MH/s (38.13ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#2....: 5755.9 MH/s (37.93ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#3....: 5754.0 MH/s (38.40ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#4....: 6085.4 MH/s (38.78ms) @ Accel:64 Loops:256 Thr:1024 Vec:1
Speed.Dev.#5....: 23571.6 MH/s
Recovered.......: 3234/12523 (25.82%) Digests, 0/1 (0.00%) Salts
Recovered/Time.: CUR:N/A,N/A,N/A AVG:80071,4804289,115302907 (Min,Hour,Day)
Progress........: 44755903920/44755903920 (100.00%)
Rejected........: 203985607/44755903920 (0.05%)
Restore.Point...: 10469932/14344841 (72.99%)
Candidates.#1...: chasiangcarr --> Zalix
Candidates.#2...: 1994_arabbit --> Zurich710$
Candidates.#3...: 8475/a8475 --> 1994_ralou
Candidates.#4...: ZALISaSA3207 --> 84750
HWMon.Dev.#1....: Temp: 38c Fan: 27% Util: 0% Core:1860MHz Mem:4513MHz Bus:16
HWMon.Dev.#2....: Temp: 46c Fan: 27% Util: 99% Core:1873MHz Mem:4513MHz Bus:16
HWMon.Dev.#3....: Temp: 46c Fan: 28% Util: 97% Core:1860MHz Mem:4513MHz Bus:16
HWMon.Dev.#4....: Temp: 47c Fan: 30% Util: 58% Core:1847MHz Mem:4513MHz Bus:16
Using Hashcat

hashcat -m1000 hashes.txt --show --username

Guest:31d6cfe0d16ae931b73c59d7e0c089c0:
empire.local\jarjar:60952501d6fd316015da46c4e33b8b23:I'mStupid
Administrator:64f12cddaa88057e06a81b54e73b949b:Password1
empire.local\ben:58c7d08fa1875b8d7422c84be165b0b9:MasterYoda!
Vader:73ad6cb025fe88b0500ee6f4cd37650e:L0rdV@der!
empire.local\luke:385455b8b6b04db792c9bbff2508aae:TheForce!
Using Hashcat – What’s Next?

Try different wordlists (ie. rockyou, linkedin, crackstation, potfile)
Try different rule files
Try patterns
Analysis
Wordlists Password Lists!

Find leaked lists
  • Skull Security
  • Daniel Miessler Seclists
  • Hashes.org
  • Crackstation
  • The Hacker Playbook
  • RockYou
  • LinkedIn
  • Paste sites
  • HaveIBeenPwned
Follow the Rules

Need rules with password lists

Examples:

- Password -> Password1
- Password -> Password01 to Password9999
- Password -> P@$w0rd
- Password -> Drowssap
- Password -> PasswordPassword
Password Policy

Typical:
• Minimum 8 characters
• Change every 90 days
• At least 3 of:
  • Uppercase character
  • Lowercase character
  • Digit
  • Special character (ie. !@#$)

• Doesn’t match NIST though…
Patterns

u-l-l-l-l-d-d-s
u-l-l-l-l-l-l-d-d-d-d
u-l-l-l-l-l-l-d-l
u-l-l-l-l-l-l-d-d-d
u-l-l-l-l-l-l-d-d-d-d
l-l-l-l-l-l-d-d-d
u-l-l-l-l-l-l-d-d
u-l-l-l-l-d-l-l
u-l-l-l-l-l-l-d-d-s
l-l-l-l-l-l-l-l
l-l-l-d-d-d-d-d
Pipal


Shows Top 10:
• Passwords
• Base words
• Patterns
• Password length
• Common character positions
Pipal – HaveIBeenPwned – Top 1M

**Top 10 base words**

- love = 1360 (0.14%)
- alex = 679 (0.07%)
- angel = 619 (0.06%)
- qwerty = 611 (0.06%)
- password = 527 (0.05%)
- june = 509 (0.05%)
- baby = 490 (0.05%)
- chris = 410 (0.04%)
- blue = 402 (0.04%)
- sexy = 399 (0.04%)
Password length (count ordered)
8 = 266482 (26.74%)
6 = 243843 (24.47%)
7 = 178067 (17.87%)
9 = 130190 (13.06%)
10 = 95066 (9.54%)
5 = 27385 (2.75%)
4 = 18004 (1.81%)
11 = 15341 (1.54%)
12 = 8583 (0.86%)
3 = 5794 (0.58%)
Last digit
1 = 145828 (14.63%)
3 = 83747 (8.4%)
2 = 70064 (7.03%)
0 = 55798 (5.6%)
7 = 51424 (5.16%)
9 = 50660 (5.08%)
5 = 50329 (5.05%)
4 = 49956 (5.01%)
6 = 47488 (4.76%)
8 = 44594 (4.47%)
Pipal – HavelBeenPwned – Top 1M

Last 4 digits (Top 10)
1234 = 6213 (0.62%)
2345 = 3007 (0.3%)
2010 = 2962 (0.3%)
2008 = 2483 (0.25%)
2009 = 2402 (0.24%)
3456 = 2278 (0.23%)
2000 = 2262 (0.23%)
2007 = 2088 (0.21%)
2006 = 1835 (0.18%)
1990 = 1779 (0.18%)
# Pipal – HaveIBeenPwned – Top 1M

## Hashcat masks (Top 10)

<table>
<thead>
<tr>
<th>Mask</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
</table>
Bonus Material!

What are the 3 most common passwords?
Password Policy

Typical:
• Minimum 8 characters
• Change every 90 days
• At least 3 of:
  • Uppercase character
  • Lowercase character
  • Digit
  • Special character (ie. !@#$)
Bonus Material!

Variants of “Password”
Variants of Company Name
Variants of SeasonYear

Easy to audit...pick a password, hash it, search for it:

ie. 7F4F718D5029000926A9278C5CFD0872 is Summer2018
But wait...there’s more!


• https://blog.rapid7.com/2018/07/19/password-tips-from-a-pen-tester-what-is-your-companys-default-password/

• https://blog.rapid7.com/2018/06/12/password-tips-from-a-pen-tester-common-patterns-exposed/

• https://blog.rapid7.com/2018/05/10/password-tips-from-a-pen-tester-3-passwords-to-eliminate/

• https://www.rapid7.com/info/under-the-hoodie/
Thank you!

Patrick_Laverty@rapid7.com
@plaverty9
https://www.linkedin.com/in/plaverty9/