Modern Password Cracking as a Methodology

HELLO!

Joshua Platz – OSCP, OSWP, CEH – Not here :(

- Principal Security Consultant @ Optiv
- Breaks Stuff, Contalker, Tool Developer, CTF Champion
- 12 Years Security Experience, 18 Years in Technology
- Started GPU Cracking with LinkedIn Breach
- Unhealthy Obsession with Cats (I have a cat nicknamed hashcat)

HELLO!

Lee Wangenhiem

- Security Consultant @ Optiv
- Hacks things for fun as well as for a job
- 5 years Infosec Experience
- Helps Joshua run the crackers at Optiv

HELLO!

Optiv – http://optiv.com/careers

Optiv Security is the world's leading security solutions integrator (SSI).

Cyber Digital Transformation

Identity and Access Management

Risk Management

Cyber Operations

Threat Management

HELLO!

We’re looking to hire a Senior Security Consultant on the Attack & Penetration team at Optiv.
This hire will perform nation-state and cybercrime syndicate simulations which includes advanced logical, physical, and social engineering attack vectors.

https://www.optiv.com/join-optiv-team

```
Session..........: jplatz
Status...........: Cracked
Hash.Type........: NetNTLMv1 / NetNTLMv1+ESS
Hash.Target......: [redacted]
Time.Started.....: Mon Oct 14 13:17:46 2019 (1 sec)
Time.Estimated...: Mon Oct 14 13:17:47 2019 (0 secs)
Guess.Base.......: File (/usr/local/bin/wordlists/rockyou.txt)
```

aspserver

Why does it matter?

Fall2019

Because it only takes one...

paste.png

Microsoft SQL Server sa Account Default Blank Password

paste.png

Cisco Device Default Password

Default Password (db2admin) for 'db2admin' Account on Windows

paste.png

VNC Server 'password' Password

paste.png

Web Common Credentials

1.
Hardware

Set Up For Success

Super Computing?

320 GPU's, 2,560 CPU's, 8TB Ram, and 1TB VRAM Give You?

So you want to do some cracking?

The Old:

CPU – Not really worth it at all

Rainbow Tables – Mostly irrelevant

The New:

GPU – Any Desktop gaming setup will do

Cloud – Scalable but spendy

Laptops – Good for when hashes cannot leave client site

Mining Rigs – Great source of used video cards, with an income stream

CLOUD

AI and Machine Learning Opening New Doors

So cracking in the CLOUD?

Summer 2017:

AWS's best GPU enabled system is the G2.8XLarge powered by 4 Nvidia GRID 520's **($2.28)**

Hashes at 16 GH's Per Second

14 Cents per GH Hour

Fall 2017:

AWS releases their new P3.16XLarge instances powered by 8 Nvidia Tesla V100's **($24.48)**

Hashes at 633 GH's Per Second

3 Cents per GH Hour

Optiv Built Cracker 2017:

6x1080 GPU's in fully redundant server configuration **(~$25,000)**

Hashes at 250 GH's Per Second

If used 80% of the time for 2 years

.7 Cents per GH Hour

AWS News – Sept 20, 2019

Summer 2019:

AWS's releases a new GPU system is the G4DN.16XLarge powered by 4 Nvidia T4 GPUS **($3.91)**

Hashes at 143 GH's Per Second

2.7 Cents per GH Hour

Not much better than the P3s (3 cents)
Still 385% more expensive then the BYO system (.7 cents)

I was not happy!

```
OpenCL Platform #1: NVIDIA Corporation
======================================
* Device #1: Tesla T4, 3769/15079 MB allocatable, 40MCU
* Device #2: Tesla T4, 3769/15079 MB allocatable, 40MCU
* Device #3: Tesla T4, 3769/15079 MB allocatable, 40MCU
* Device #4: Tesla T4, 3769/15079 MB allocatable, 40MCU

Benchmark relevant options:
===========================
* --optimized-kernel-enable

Hashmode: 1000 - NTLM

Speed.#1.........: 35792.8 MH/s (35.93ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
Speed.#2.........: 36230.0 MH/s (35.50ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
Speed.#3.........: 35598.3 MH/s (36.12ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
Speed.#4.........: 36138.1 MH/s (35.60ms) @ Accel:32 Loops:1024 Thr:1024 Vec:1
Speed.#*.........:   143.8 GH/s
```

2.
Glossary

So We Can Speak The Same Language

A Couple Terms

Masks – The makeup of a word, broken into it's character set

Hybrid Attack – An attack where a Brute-Force or mask is either appended or prepended to a wordlist

Wordlist – A file which contains a list of candidate words to either run by themselves or be modified with rules, typically dictionary words

Password Dump – A file which contains passwords obtained from previous cracking attempts, will contain more complex words than a wordlist

3.
Tools

Creating Your Environment

Building an arsenal

"If Your Only Tool Is a Hammer Then Every Problem Looks Like a Nail"

Mark Twain

The Kit

Hashcat – The Hammer

Hashtopolis – The Toolbelt

Cewl – Nails

PW Tools – Wrenches

HashID – Magnifying Glass

PW_Spy – Measuring Tape

Hashcat

Defacto standard. Supports almost every hash imaginable. Fast. Constant updates/improvements.

Replaced JohnTheRipper

Easy to setup and integrate with other tools

Hashtopolis

Hashtoplis

Wrapper for Hashcat

Manage agents, jobs, wordlists, and hashcat binaries from a central location

Distributed cracking made easy!!!

CeWL

Crawls Website for Words

Set word length and spider depth

Great for WPA cracking for industry specific terms

PW Tools

Collection of likely shoddly coded python tools

- Combination-Builder – Merge Wordlists – Create Sentences
- DictPhase-Builder – Ham a single Wordlist
- Phrase-Builder – Convert Song/Script to Passphrases
- Mask-Builder – Identify most common masks
- Language-Xmute – Transform wordlists
- find-non-complex.py

https://github.com/binary1985/PWTools

HashID

```
sh-3.2$ md5 -s "Password123"
MD5 ("Password123") = 42f749ade7f9e195bf475f37a44cafcb
sh-3.2$ hashid -m -j 42f749ade7f9e195bf475f37a44cafcb
Analyzing '42f749ade7f9e195bf475f37a44cafcb'
[+] MD2 [JtR Format: md2]
[+] MD5 [Hashcat Mode: 0][JtR Format: raw-md5]
[+] MD4 [Hashcat Mode: 900][JtR Format: raw-md4]
[+] Double MD5 [Hashcat Mode: 2600]
[+] LM [Hashcat Mode: 3000][JtR Format: lm]
[+] RIPEMD-128 [JtR Format: ripemd-128]
[+] Haval-128 [JtR Format: haval-128-4]
[+] Tiger-128
[+] Skein-256(128)
[+] Skein-512(128)
[+] Lotus Notes/Domino 5 [Hashcat Mode: 8600][JtR Format
```

Find likely hashing algorithms

If its not helpful

- Research Application – Source code?
- Try a commonly used password first
- Self register known password

PW_spy

Tool built out of our Enterprise Password Audits

Pipal was found not always being reliable

Finds:

- Most common masks
- Weak Passwords
- Password Lengths
- Base words

https://github.com/lwangenheim/pw_spy

4.
Techniques

Honing Your Skills

How do I begin?

What's the best way to crack a hash?

This is a loaded question, what's the best way to use Nmap?

Think about the engagement, are you going after one hash? Multiple hashes?

What algorithm are you trying to crack?

NTLM is MUCH faster than WPA2

How do I look?

Where do we get hashes?

- Hashdump – local accounts
- /etc/shadow or .conf files
- Mimikatz
- WebApps
- Responder
- DCSync/NTDS

Developing a Methodology

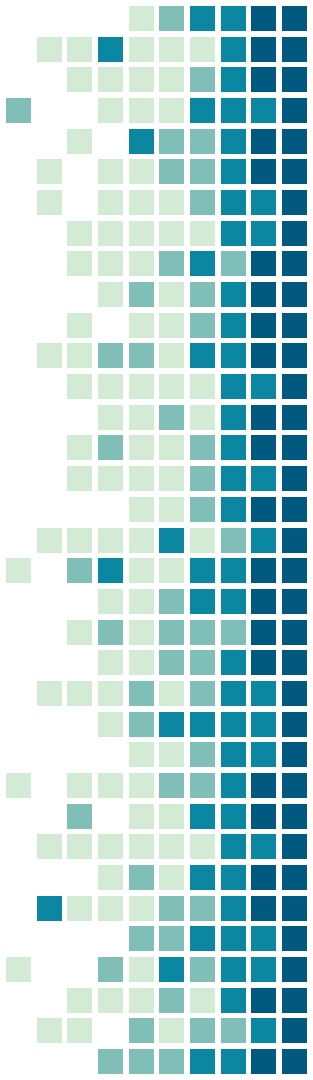
Methodology – Password Audit

- Creating a repeatable process for others to follow
- Looks at the entire enterprise
- Very analysis based
- Looking for patterns, common words, easy wins, etc.
- Some claim they do pw audits but they don't do it effectively
- Need heavy hitting cracking rigs / cloud setup

What do I do?

How did we get there? (quick wins)

- Proprietary wordlists without rules
- Adding rules to those same lists
- Loopback attacks
- 1-8 char brute force
- Masks (start with uppercase, end with digits/special chars)



Executing the Methodology

Help Your Future Self

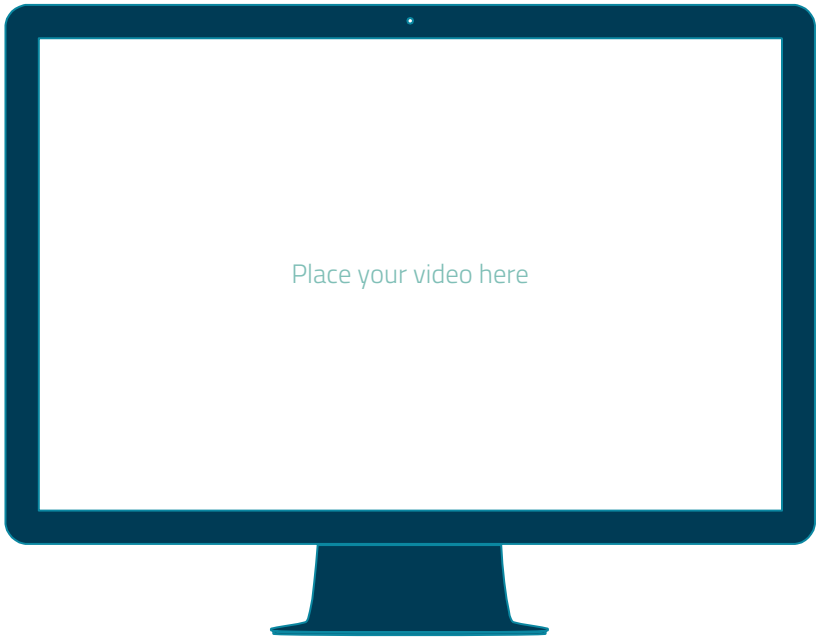
- Pot Files
  - Historical record of your cracked hashes
  - Useful to see if you've already cracked a hash on another engagement
  - Be wary of bloat, it can slow down the process as each hash is run through the existing potfile
- Common Masks
  - Build a list of masks > 8 characters to run through

5.
Demo

Multi TeraHash Cloud Supercomputer

Demo Gods Hate Me

Watch ~~1~~ ~~2~~ 22 Trillion Guesses Per Second.



Estimated Password Recovery Times — 1x Terahash Brutalis, 44x Terahash Inmanis (448x Nvidia RTX 2080)

Full US keyboard mask attack with Terahash Hashstack

	Speed	Length 4	Length 5	Length 6	Length 7	Length 8	Length 9	Length 10	Length 11	Length 12	Length 13
NTLM	31.82 TH/s	Instant	Instant	Instant	Instant	3 mins 29 secs	5 hrs 30 mins	3 wks 0 day	5 yrs 7 mos	538 yrs 1 mo	51.2 mil
MD5	17.77 TH/s	Instant	Instant	Instant	Instant	6 mins 14 secs	9 hrs 50 mins	1 mo 1 wk	10 yrs 1 mo	963 yrs 4 mos	91.6 mil
NetNTLMv1 / NetNTLMv1+ESS	16.82 TH/s	Instant	Instant	Instant	Instant	6 mins 35 secs	10 hrs 24 mins	1 mo 1 wk	10 yrs 8 mos	1 mil	96.8 mil
LM	15.81 TH/s	Instant	Instant	Instant	Instant						
SHA1	5.89 TH/s	Instant	Instant	Instant	Instant	18 mins 47 secs	1 day 5 hrs	3 mos 3 wks	30 yrs 7 mos	2.9 mil	276.3 mil
SHA2-256	2.42 TH/s	Instant	Instant	Instant	Instant	45 mins 39 secs	3 days 0 hr	9 mos 1 wk	74 yrs 4 mos	7.1 mil	671.9 mil
NetNTLMv2	1.22 TH/s	Instant	Instant	Instant	Instant	1 hr 30 mins	5 days 23 hrs	1 yr 6 mos	147 yrs 10 mos	14.1 mil	1335.5 mil
SHA2-512	801.9 GH/s	Instant	Instant	Instant	1 min 28 secs	2 hrs 17 mins	1 wk 2 days	2 yrs 4 mos	224 yrs 9 mos	21.4 mil	2029.7 mil
descrypt, DES (Unix), Traditional DES	647.59 GH/s	Instant	Instant	Instant	1 min 48 secs	2 hrs 50 mins	1 wk 4 days	2 yrs 11 mos	278 yrs 3 mos	26.5 mil	2513.3 mil
Kerberos 5, etype 23, TGS-REP	206.97 GH/s	Instant	Instant	Instant	5 mins 38 secs	8 hrs 54 mins	1 mo 0 wk	9 yrs 2 mos	870 yrs 10 mos	82.8 mil	7864 mil
Kerberos 5, etype 23, AS-REQ Pre-Auth	206.78 GH/s	Instant	Instant	Instant	5 mins 38 secs	8 hrs 54 mins	1 mo 0 wk	9 yrs 2 mos	871 yrs 8 mos	82.9 mil	7871.2 mil
md5crypt, MD5 (Unix), Cisco-IOS 1 (MD5)	7.61 GH/s	Instant	Instant	1 min 37 secs	2 hrs 33 mins	1 wk 3 days	2 yrs 7 mos	249 yrs 5 mos	23.7 mil	2252.6 mil	213995.1 mil
LastPass + LastPass sniffed	1.78 GH/s	Instant	Instant	6 mins 52 secs	10 hrs 52 mins	1 mo 1 wk	11 yrs 2 mos	1.1 mil	101.1 mil	9600.8 mil	912079.6 mil
macOS v10.8+ (PBKDF2-SHA512)	335.09 MH/s	Instant	Instant	36 mins 34 secs	2 days 9 hrs	7 mos 2 wks	59 yrs 7 mos	5.7 mil	538.2 mil	51127.7 mil	4857134 mil
WPA-EAPOL-PBKDF2	277.23 MH/s					9 mos 0 wk	72 yrs 0 mo	6.8 mil	650.5 mil	61799.3 mil	5870931.8 mil
TrueCrypt RIPEMD160 + XTS 512 bit	211.78 MH/s	Instant	Instant	57 mins 52 secs	3 days 19 hrs	11 mos 3 wks	94 yrs 3 mos	9 mil	851.6 mil	80899.5 mil	7685455.6 mil
7-Zip	181.51 MH/s	Instant	Instant	1 hr 7 mins	4 days 10 hrs	1 yr 1 mo	110 yrs 0 mo	10.5 mil	993.6 mil	94389.2 mil	8966975.1 mil
sha512crypt 6, SHA512 (Unix)	119.46 MH/s	Instant	1 min 5 secs	1 hr 42 mins	6 days 18 hrs	1 yr 9 mos	167 yrs 2 mos	15.9 mil	1509.7 mil	143419.6 mil	13624861.4 mil
DPAPI masterkey file v1	47.23 MH/s	Instant	2 mins 44 secs	4 hrs 19 mins	2 wks 3 days	4 yrs 5 mos	422 yrs 10 mos	40.2 mil	3818.1 mil	362723.1 mil	34458696.1 mil
RAR5	28.15 MH/s	Instant	4 mins 35 secs	7 hrs 15 mins	4 wks 0 day	7 yrs 5 mos	709 yrs 7 mos	67.4 mil	6407.6 mil	608720.6 mil	57828453.9 mil
DPAPI masterkey file v2	27.82 MH/s	Instant	4 mins 39 secs	7 hrs 20 mins	4 wks 1 day	7 yrs 6 mos	717 yrs 10 mos	68.2 mil	6482.1 mil	615797.6 mil	58500769.5 mil
RAR3-hp	20.84 MH/s	Instant	6 mins 12 secs	9 hrs 47 mins	1 mo 1 wk	10 yrs 1 mo	958 yrs 2 mos	91.1 mil	8652.3 mil	821972.3 mil	78087367.8 mil
KeePass 1 (AES/Twofish) and KeePass 2 (AES)	17.8 MH/s	Instant	7 mins 15 secs	11 hrs 28 mins	1 mo 2 wks	11 yrs 9 mos	1.1 mil	106.7 mil	10131.9 mil	962529.5 mil	91440305.8 mil
bcrypt $2*$, Blowfish (Unix)	11.37 MH/s	Instant	11 mins 21 secs	17 hrs 57 mins	2 mos 1 wk	18 yrs 5 mos	1.8 mil	167 mil	15860.3 mil	1506727.9 mil	143139150.9 mil
Bitcoin/Litecoin wallet.dat	3.55 MH/s	Instant	36 mins 18 secs	2 days 9 hrs	7 mos 2 wks	59 yrs 1 mo	5.6 mil	534.1 mil	50743.7 mil	4820655.6 mil	457962282.7 mil

Prof B Buchanan OBE @billatnapier · 9h

Be worried about the power of the Cloud to crack hashed passwords ... the threat is not rainbow tables anymore, but Hashcat rules. You say that you "salt" you are passwords, but the salt is their with the hashed password.

11 173 266

THANKS!

Any questions?

You can find us at:

@joshuaplatz

@Hx_fifty

CREDITS

Special thanks to all the people who dedicate time to content in this presentation:

- Hashcat
- Hashtopolis
- Optiv
- Presentation template by SlidesCarnival
- Photographs by Unsplash