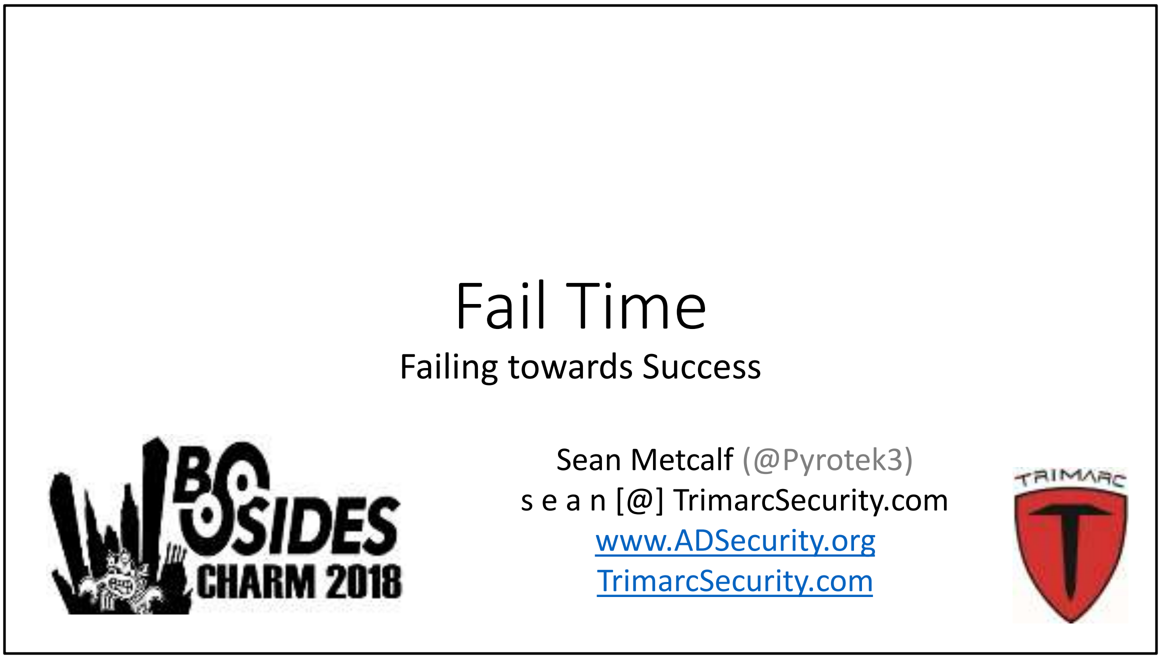


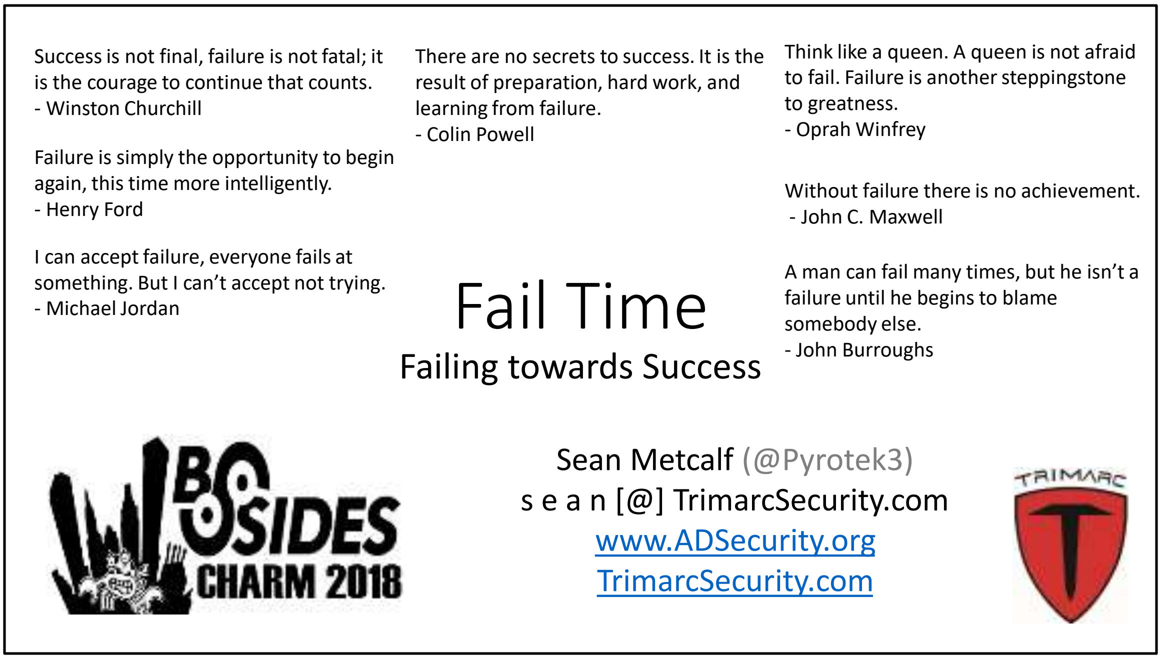
Fail Time

Failing towards Success

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

BSIDES CHARM 2018
TRIMARC

I will not be using motivational quotes in this talk…



Fail Time

Failing towards Success

Success is not final, failure is not fatal; it is the courage to continue that counts.
- Winston Churchill

Failure is simply the opportunity to begin again, this time more intelligently.
- Henry Ford

I can accept failure, everyone fails at something. But I can't accept not trying.
- Michael Jordan

There are no secrets to success. It is the result of preparation, hard work, and learning from failure.
- Colin Powell

Think like a queen. A queen is not afraid to fail. Failure is another steppingstone to greatness.
- Oprah Winfrey

Without failure there is no achievement.
- John C. Maxwell

A man can fail many times, but he isn't a failure until he begins to blame somebody else.
- John Burroughs

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

GAVE THE BAKERY A PHOTO ON THE USB DRIVE
TO PUT ON THE CAKE. THIS IS THE CAKE THEY MADE.

Why this talk?

Why not?
Most con talks cover the successes and highlights of what worked.
This is not that talk.
Failures happen all the time. Mistakes are made.
Sometimes we go ahead and do something that doesn’t make sense because we were told to

Sp4rkCon
Save Data. Hack Better.

DERBYCON
VII
LEGACY
LOUISVILLE 2017 KENTUCKY

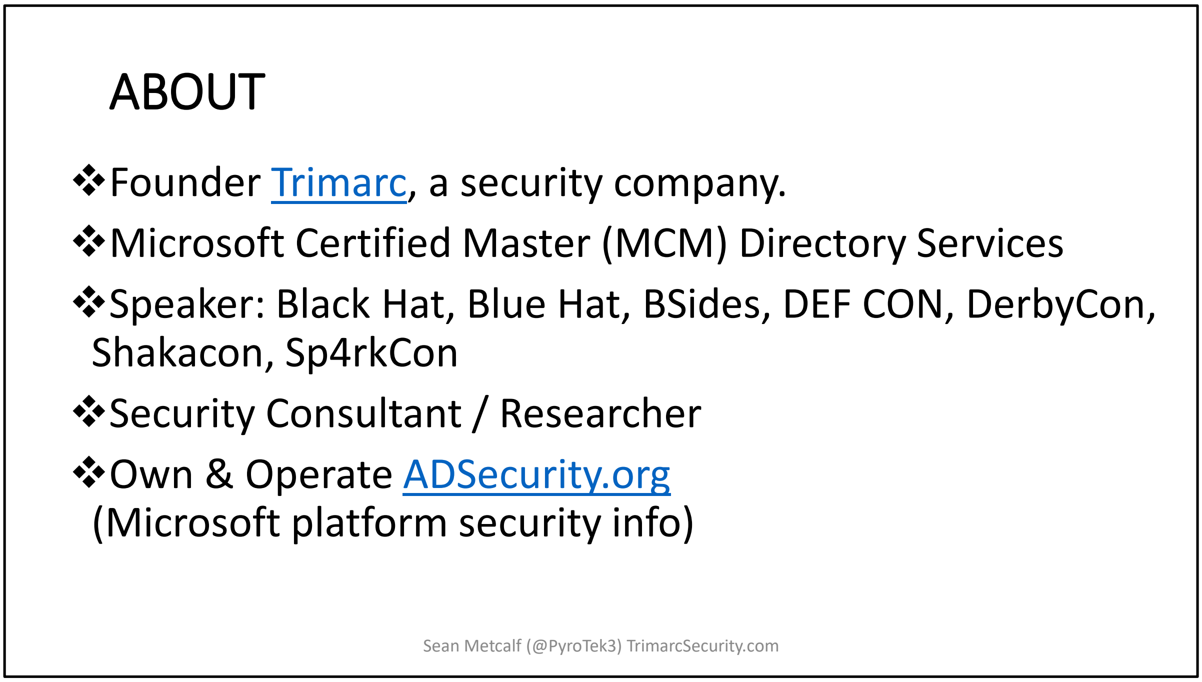
The idea of a talk on failure started with my talk at Walmart's SparkCon conference about a year ago.
During the usual post-talk Q&A someone asked me: have you failed at any of this?
My immediate answer was that I fail all the time.
The idea was re-sparked when talking about the concept of failure at DerbyCon with WaxWing while I was manning the Trimarc booth.

AGENDA

- Joke
- Personal Anecdote
- Technical Fails
- Being Better
- Failure as part of Success
- Motivational Quotes
- Alphabetize Agenda

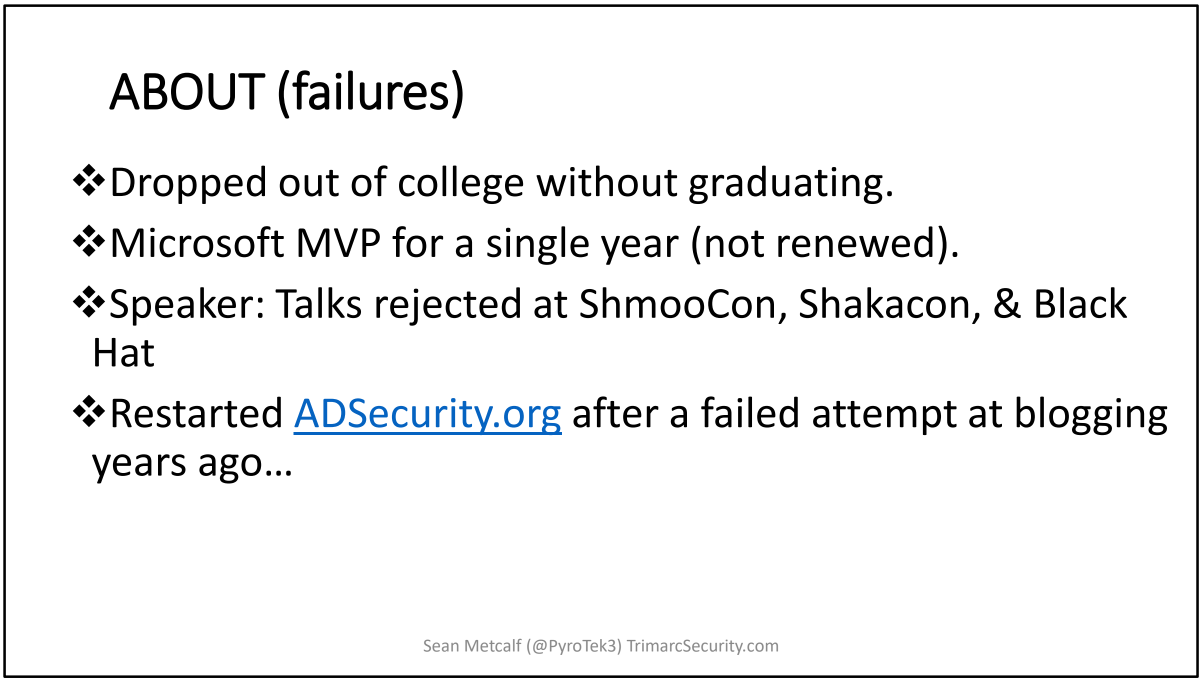
Slides: Presentations.ADSecurity.org

So here we are.
This… is not a real agenda. So chalk this up as a failure of expectation.
You expected something that outlines this journey.
LOTS to cover, so let’s get started!



ABOUT

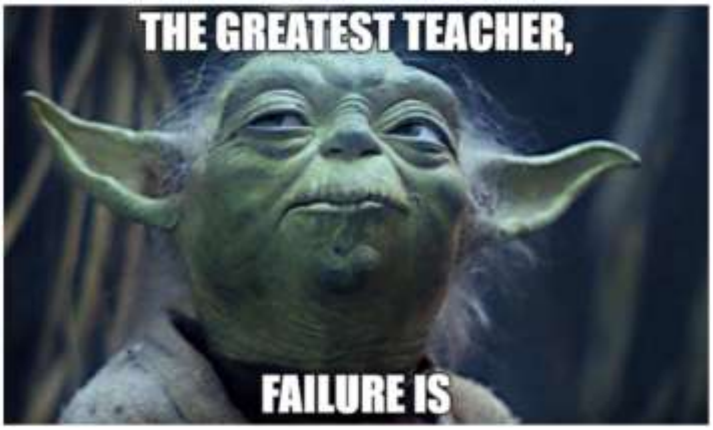
- ❖Founder Trimarc, a security company.
- ❖Microsoft Certified Master (MCM) Directory Services
- ❖Speaker: Black Hat, Blue Hat, BSides, DEF CON, DerbyCon, Shakacon, Sp4rkCon
- ❖Security Consultant / Researcher
- ❖Own & Operate ADSecurity.org (Microsoft platform security info)



ABOUT (failures)

- ❖Dropped out of college without graduating.
- ❖Microsoft MVP for a single year (not renewed).
- ❖Speaker: Talks rejected at ShmooCon, Shakacon, & Black Hat
- ❖Restarted ADSecurity.org after a failed attempt at blogging years ago…

Again, this is a different type of talk, so let's highlight some corresponding failures.

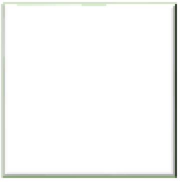
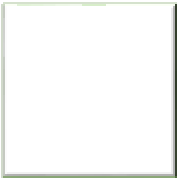
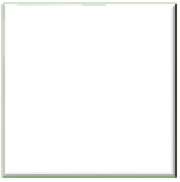
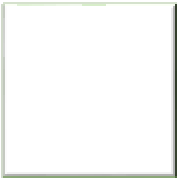
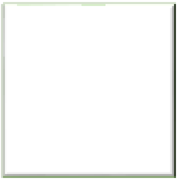


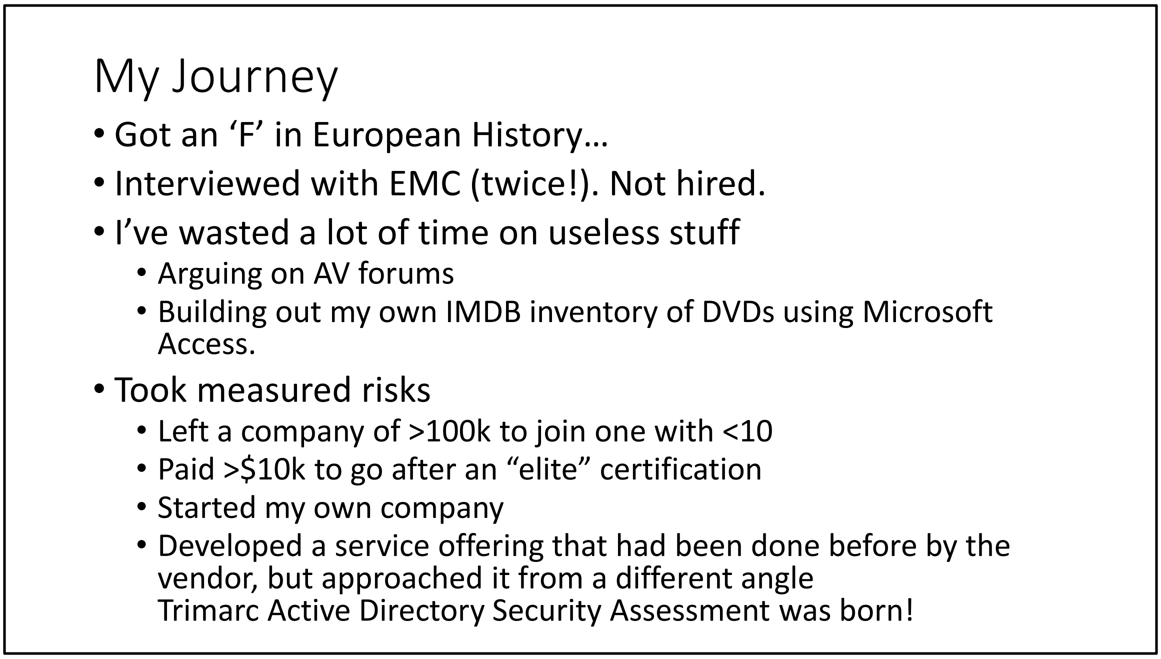
Why are you here?

You saw the talk was about failing…
Why are you here?
What compelled you to show up?
Maybe to see what could happen?
That works…

Photography anecdote
I am into photography.

Baby Photos

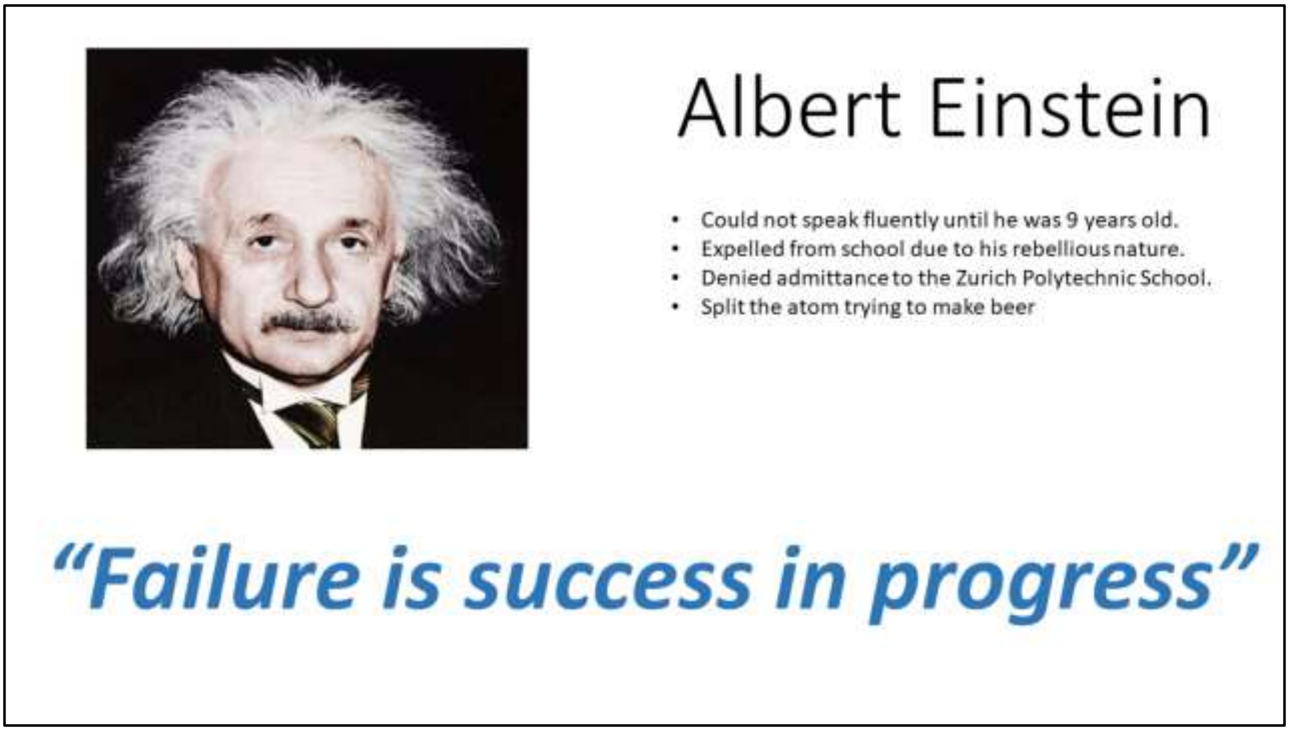








My Journey

- Got an ‘F’ in European History…
- Interviewed with EMC (twice!). Not hired.
- I’ve wasted a lot of time on useless stuff
  - Arguing on AV forums
  - Building out my own IMDB inventory of DVDs using Microsoft Access.
- Took measured risks
  - Left a company of >100k to join one with <10
  - Paid >$10k to go after an “elite” certification
  - Started my own company
  - Developed a service offering that had been done before by the vendor, but approached it from a different angle
    Trimarc Active Directory Security Assessment was born!

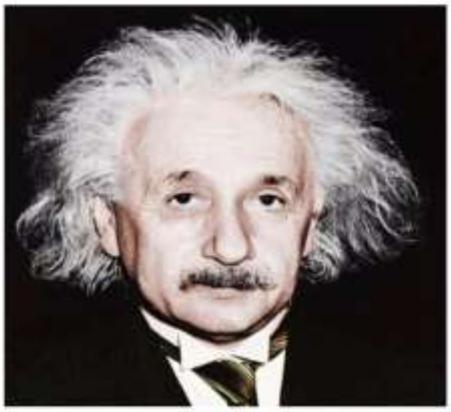
Here are some other failures and major risks I tool
I got an F in European History because I didn’t understand that the tests were entirely based on what the instructor wrote on the white board and was not directly related to the information in the book. I was lazy and didn’t want to take a bunch of notes. First test failed. I started taking notes after that but I still didn’t take seriously studying from these notes.
I had an interview with EMC many years ago and honestly, I wasn’t good enough to get the job. I insisted on another interview, which they granted me. I failed that interview as well. My technical ability wasn’t where it needed to be and it wasn’t a good fit. I wouldn’t have hired me either back then.



Albert Einstein

- Could not speak fluently until he was 9 years old.
- Expelled from school due to his rebellious nature.
- Denied admittance to the Zurich Polytechnic School.
- Split the atom trying to make beer

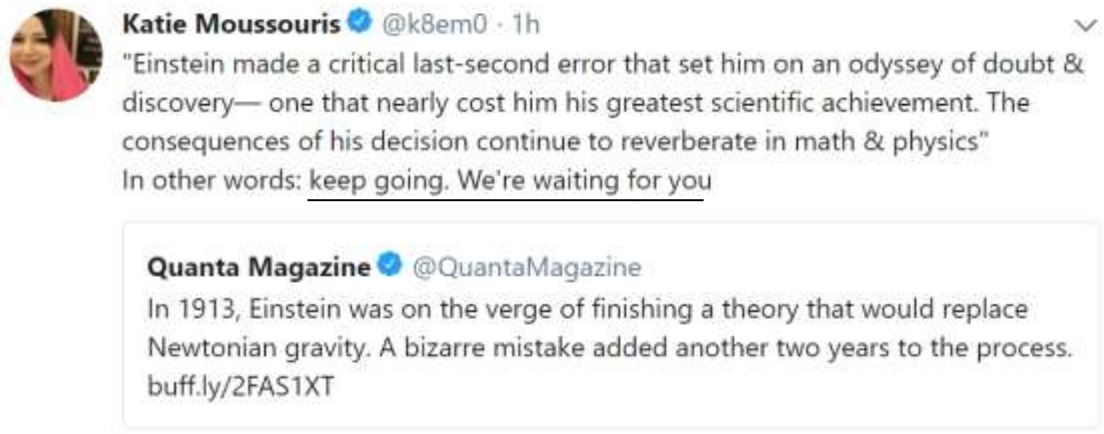
"Failure is success in progress"



Albert Einstein

- Could not speak fluently until he was 9 years old.
- Expelled from school due to his rebellious nature.
- Denied admittance to the Zurich Polytechnic School.
- ~~Split the atom trying to make beer~~

"Failure is success in progress"

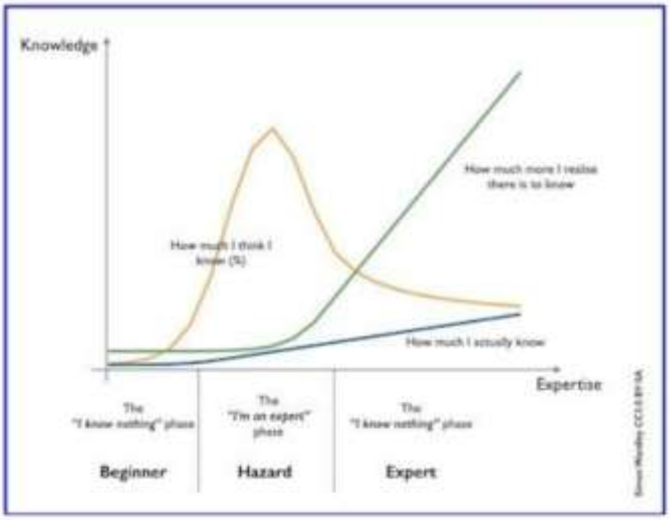


Katie Moussouris @k8em0 · 1h

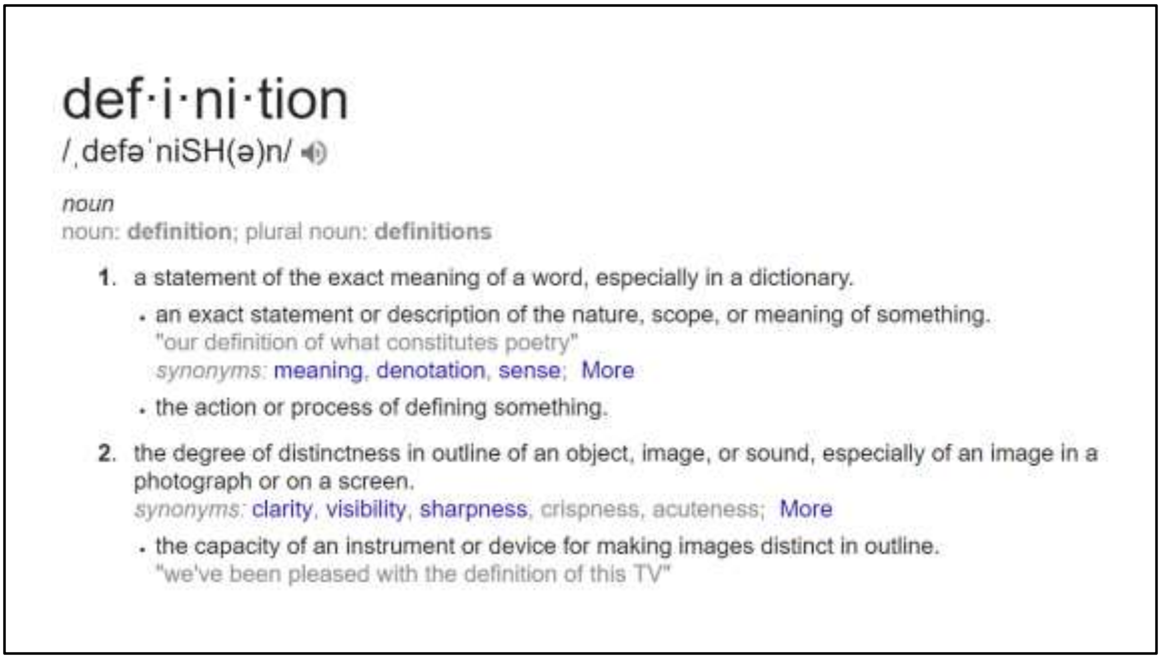
"Einstein made a critical last-second error that set him on an odyssey of doubt & discovery— one that nearly cost him his greatest scientific achievement. The consequences of his decision continue to reverberate in math & physics"
In other words: keep going. We're waiting for you

> **Quanta Magazine** @QuantaMagazine
> In 1913, Einstein was on the verge of finishing a theory that would replace Newtonian gravity. A bizarre mistake added another two years to the process.
> buff.ly/2FAS1XT

This is not a typical con talk



Simon Wardley CC3.0 BY-SA



def·i·ni·tion

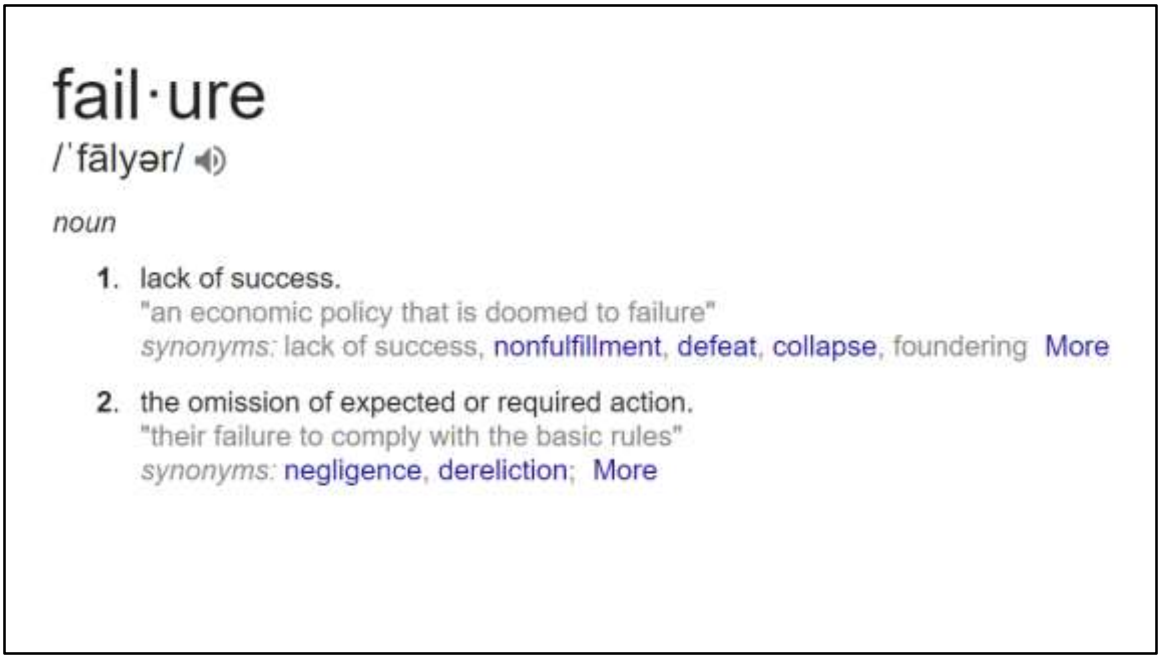
/ˌdefəˈniSH(ə)n/

noun

noun: **definition**; plural noun: **definitions**

1. a statement of the exact meaning of a word, especially in a dictionary.
   - an exact statement or description of the nature, scope, or meaning of something.
     "our definition of what constitutes poetry"
     synonyms: meaning, denotation, sense; More
   - the action or process of defining something.
2. the degree of distinctness in outline of an object, image, or sound, especially of an image in a photograph or on a screen.
   synonyms: clarity, visibility, sharpness, crispness, acuteness; More
   - the capacity of an instrument or device for making images distinct in outline.
     "we've been pleased with the definition of this TV"

These types of talks usually include definitions, so let’s be meta and define “definition”



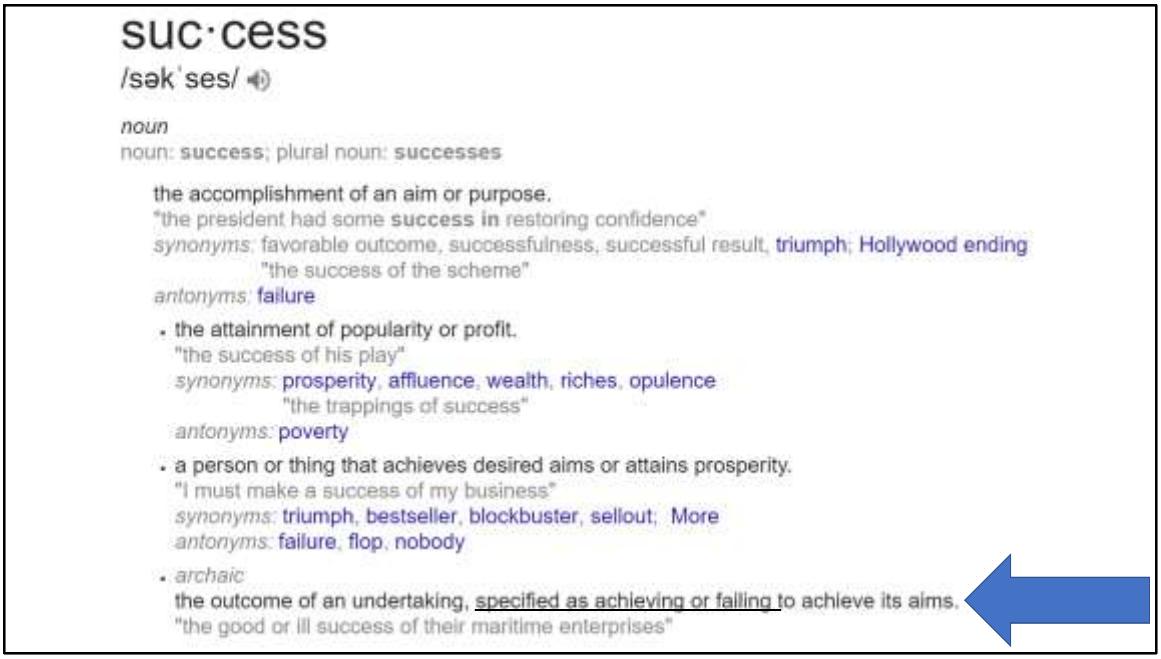
fail·ure

/ˈfālyər/ 🔊

noun

1. lack of success.
   "an economic policy that is doomed to failure"
   synonyms: lack of success, nonfulfillment, defeat, collapse, foundering More
2. the omission of expected or required action.
   "their failure to comply with the basic rules"
   synonyms: negligence, dereliction; More

Failure, what is it?



suc·cess

/səkˈses/

noun

noun: **success**; plural noun: **successes**

the accomplishment of an aim or purpose.

"the president had some **success in** restoring confidence"

synonyms: favorable outcome, successfulness, successful result, triumph; Hollywood ending

"the success of the scheme"

antonyms: failure

- the attainment of popularity or profit.

  "the success of his play"

  synonyms: prosperity, affluence, wealth, riches, opulence

  "the trappings of success"

  antonyms: poverty

- a person or thing that achieves desired aims or attains prosperity.

  "I must make a success of my business"

  synonyms: triumph, bestseller, blockbuster, sellout; More

  antonyms: failure, flop, nobody

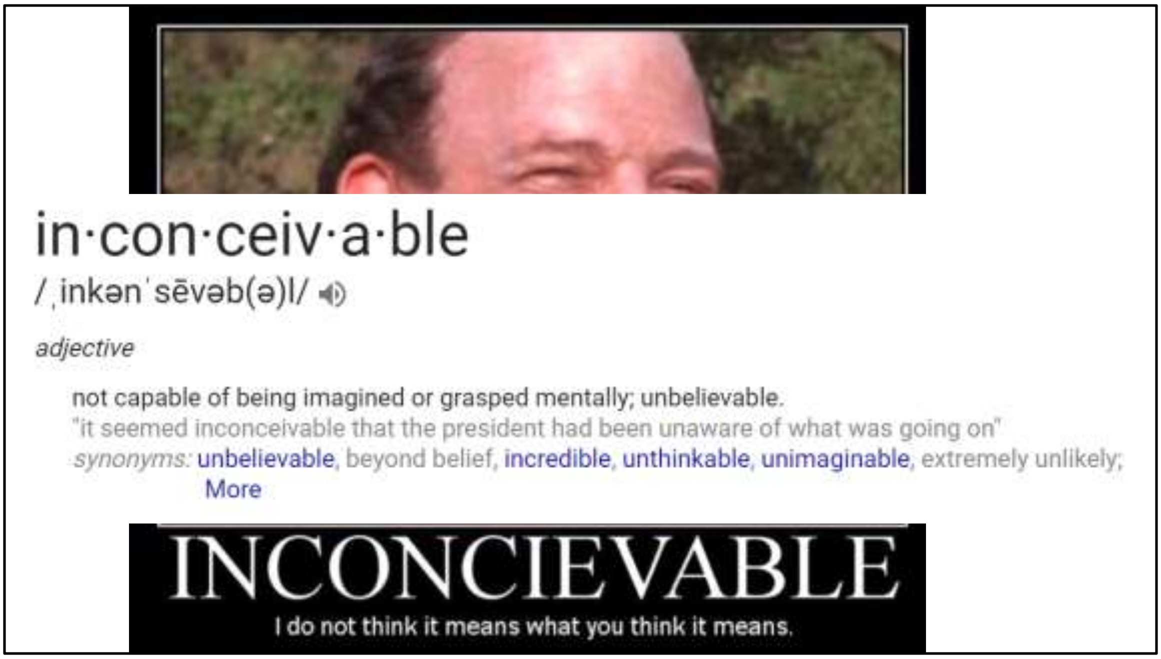
- *archaic*

  the outcome of an undertaking, specified as achieving or failing to achieve its aims.

  "the good or ill success of their maritime enterprises"

…and what is "success"

Note that the definition of success used to be failing at something



in·con·ceiv·a·ble

/ˌinkənˈsēvəb(ə)l/

adjective

not capable of being imagined or grasped mentally; unbelievable.

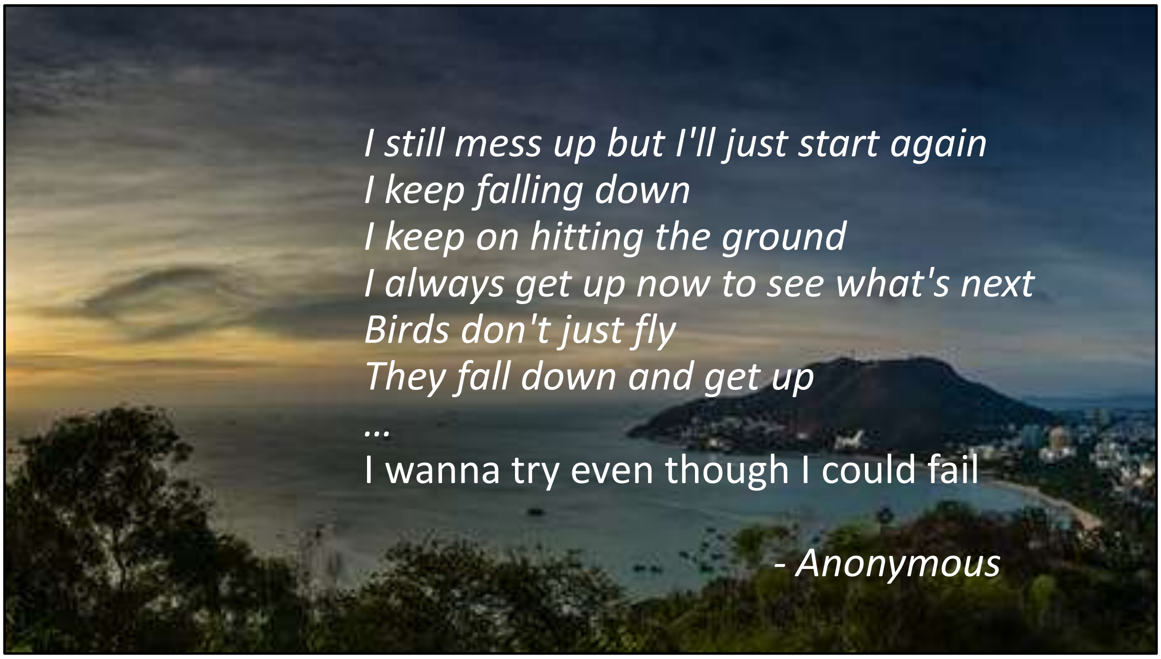
"it seemed inconceivable that the president had been unaware of what was going on"

synonyms: unbelievable, beyond belief, incredible, unthinkable, unimaginable, extremely unlikely;

More

Inconceivable!

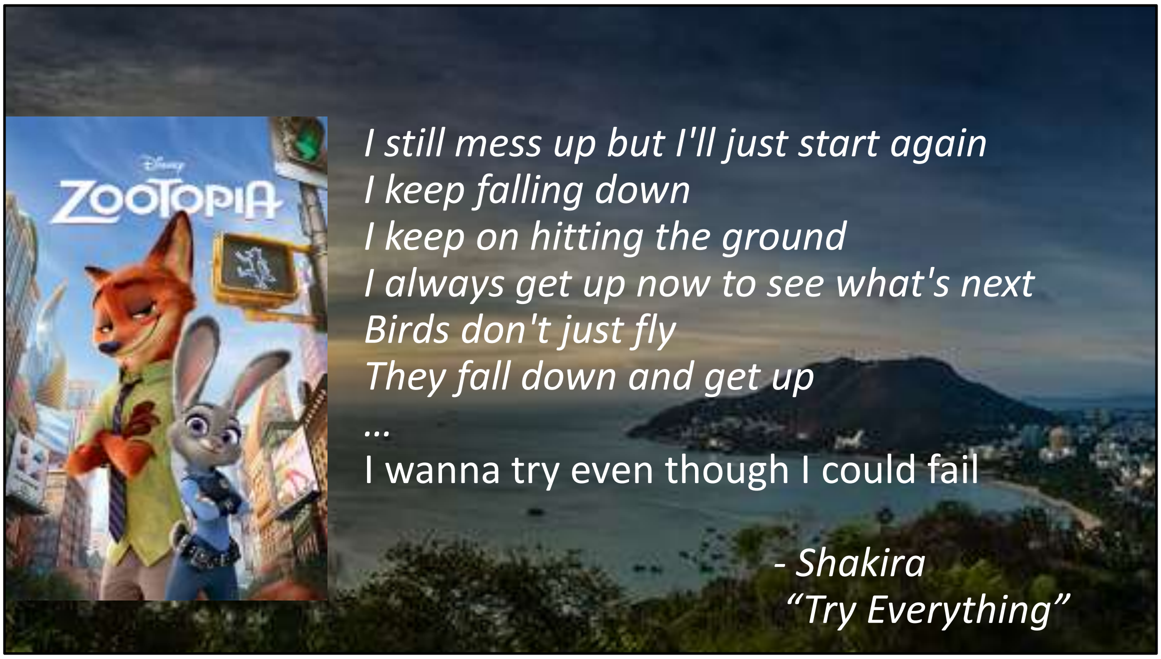
Is it used correctly in the context of the movie “The Princess Bride”?



I still mess up but I'll just start again
I keep falling down
I keep on hitting the ground
I always get up now to see what's next
Birds don't just fly
They fall down and get up
…
I wanna try even though I could fail

- Anonymous

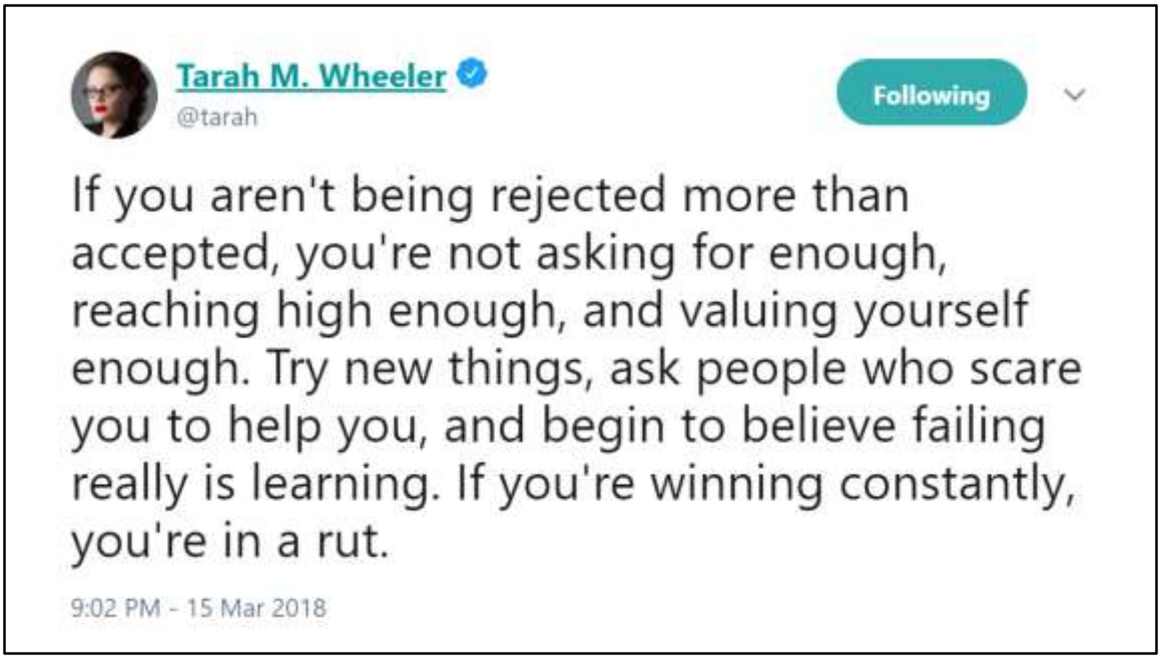
Such a great poem by a poet we may never know…


Disney
ZOOTOPIA

I still mess up but I'll just start again
I keep falling down
I keep on hitting the ground
I always get up now to see what's next
Birds don't just fly
They fall down and get up
…
I wanna try even though I could fail

- Shakira
"Try Everything"

Actually this is from the song "Try Everything" by Shakira

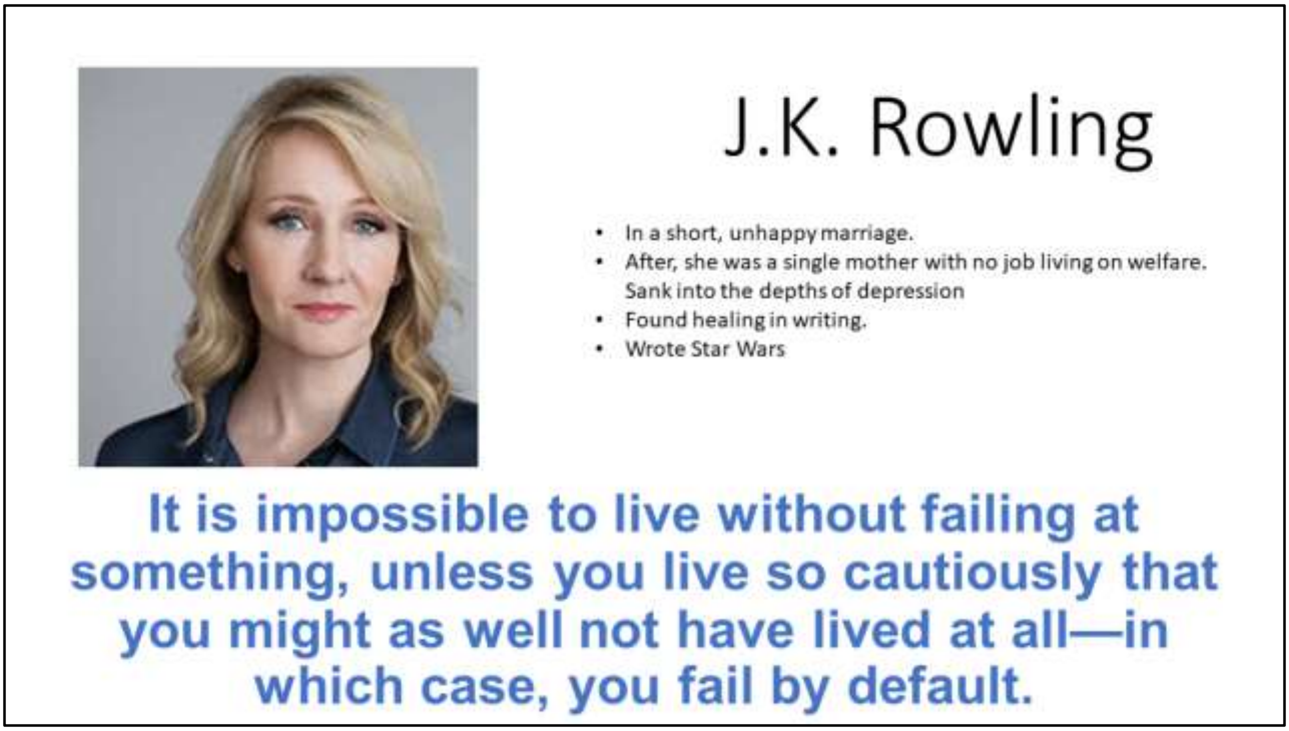


Tarah M. Wheeler
@tarah

If you aren't being rejected more than accepted, you're not asking for enough, reaching high enough, and valuing yourself enough. Try new things, ask people who scare you to help you, and begin to believe failing really is learning. If you're winning constantly, you're in a rut.

9:02 PM - 15 Mar 2018

Tarah makes an excellent point. No Failure = not reaching for the next level in many things.

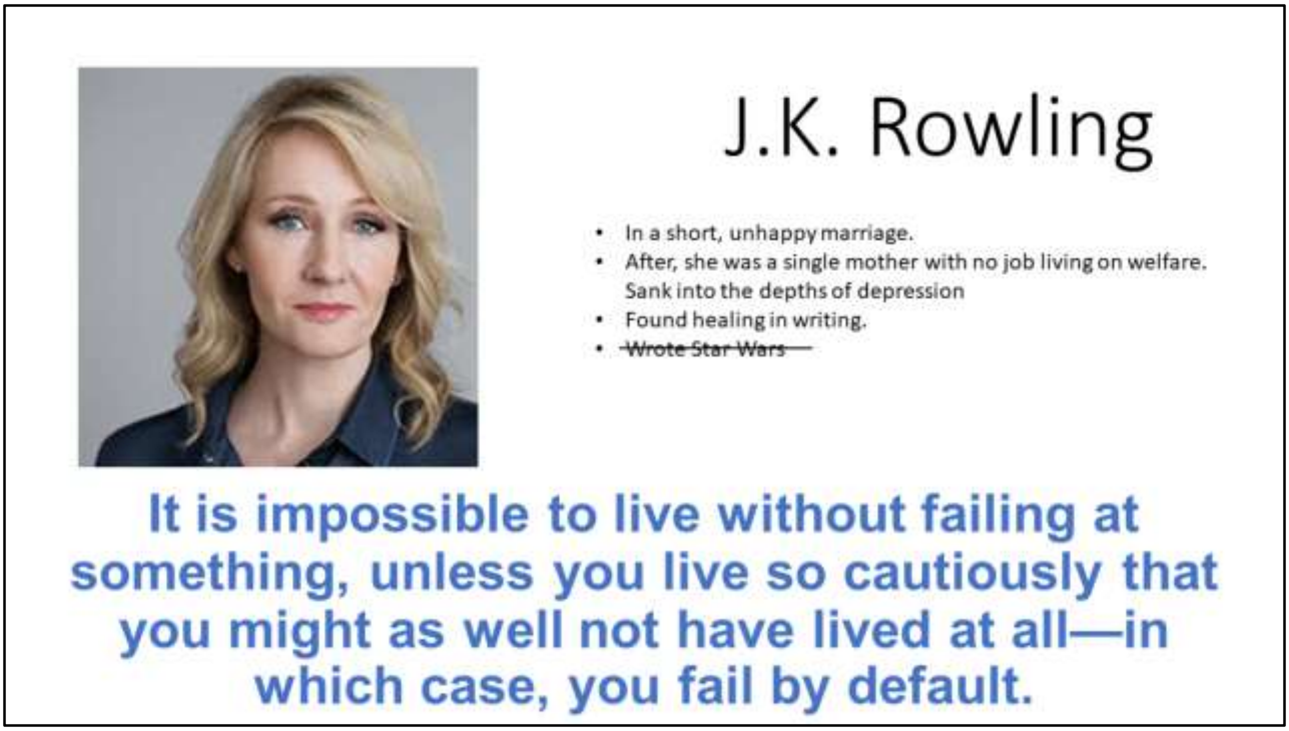


J.K. Rowling

- In a short, unhappy marriage.
- After, she was a single mother with no job living on welfare. Sank into the depths of depression
- Found healing in writing.
- Wrote Star Wars

It is impossible to live without failing at something, unless you live so cautiously that you might as well not have lived at all—in which case, you fail by default.

J.K. Rowling endured a short, unhappy marriage. Once it ended, she was a single mother with no job living on welfare. She then sank into the depths of depression and even contemplated suicide. She found healing in writing.



J.K. Rowling

- In a short, unhappy marriage.
- After, she was a single mother with no job living on welfare. Sank into the depths of depression
- Found healing in writing.
- ~~Wrote Star Wars~~

It is impossible to live without failing at something, unless you live so cautiously that you might as well not have lived at all—in which case, you fail by default.

J.K. Rowling endured a short, unhappy marriage. Once it ended, she was a single mother with no job living on welfare. She then sank into the depths of depression and even contemplated suicide. She found healing in writing.

Mental Barriers

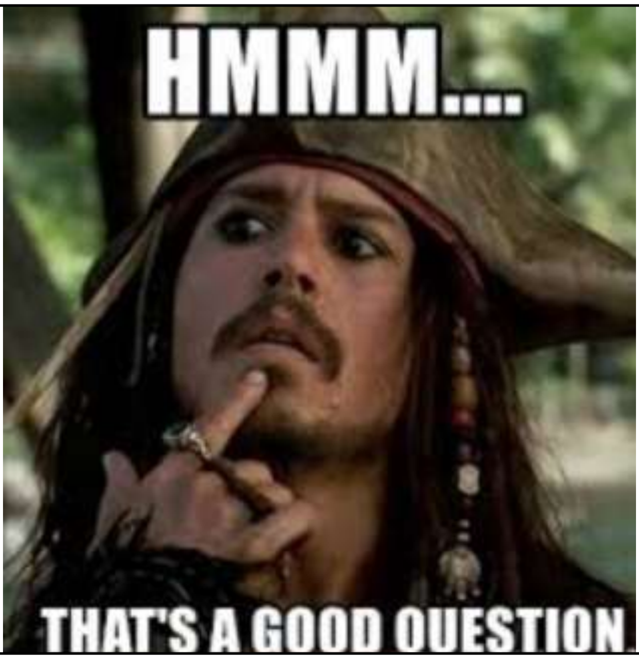
Mental barriers are the things that prevent us from trying something (new or again) and keep us from succeeding in those areas.

Most see a wall and look for a way around or give up
Others look for hand and footholds to climb over

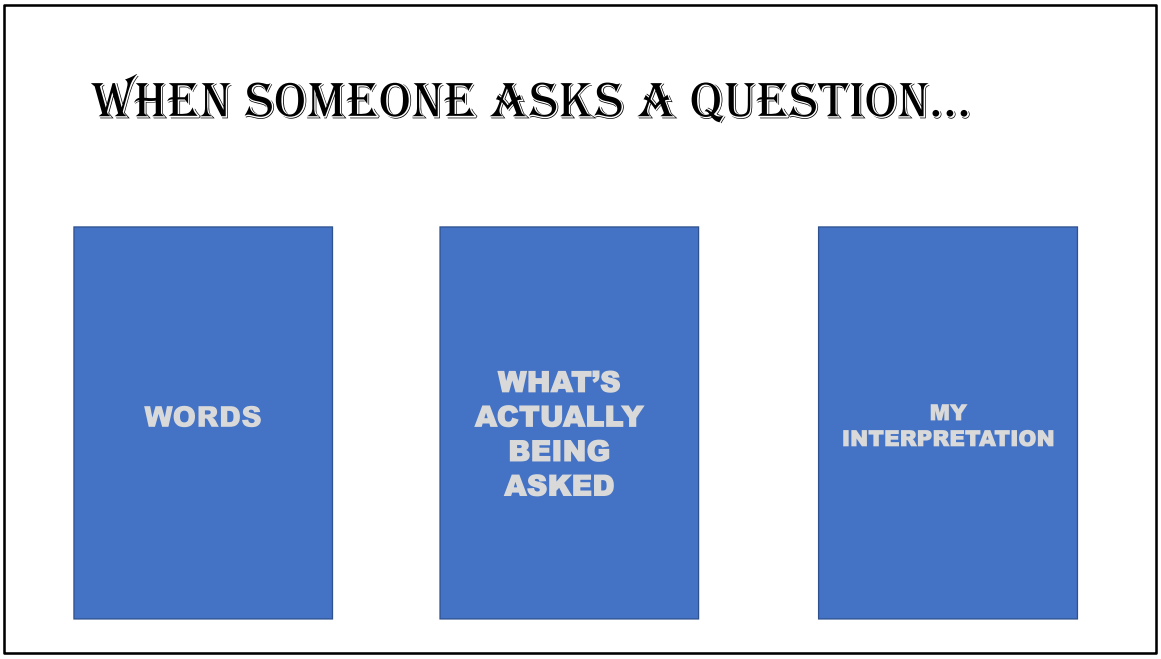
When someone is talking, we may miss what they are saying…

Darmok and Jalad... at Tanagra.
Temba, his arms wide.
Shaka, when the walls fell.
Know what I mean...
geek e cards
Night of the Living Trekkies

Everyone communicates things a bit differently, try to determine what they are actually saying. Ask if uncertain.



When a question is asked, try to determine what is actually being asked.



When someone asks a question…

WORDS

WHAT'S ACTUALLY BEING ASKED

MY INTERPRETATION

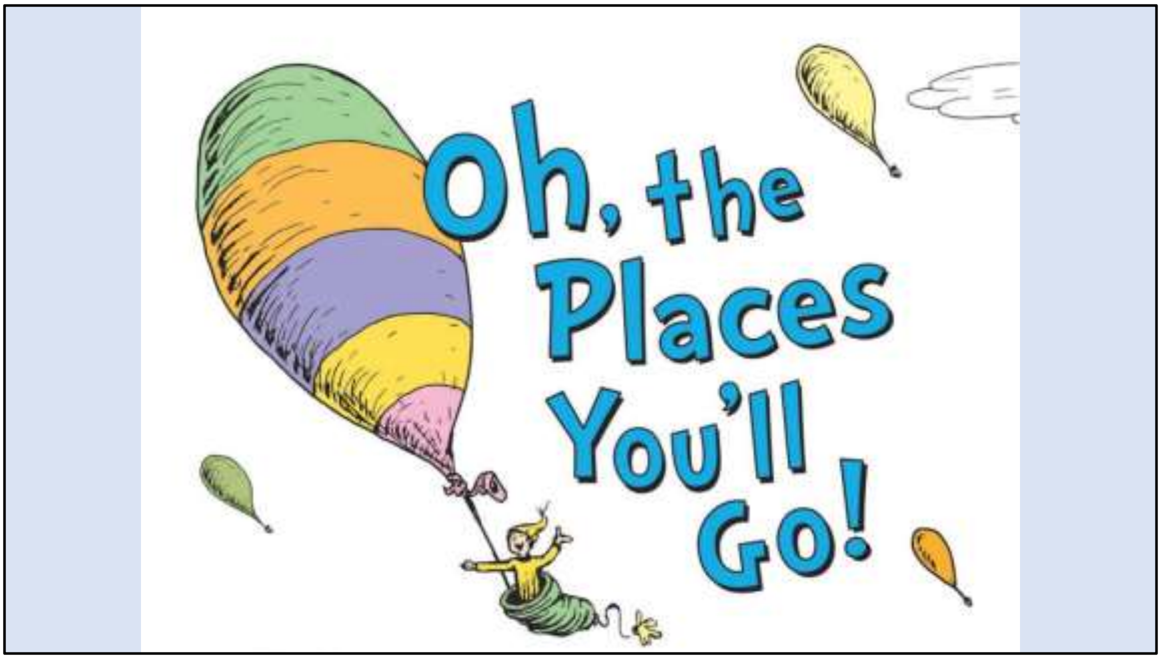
When someone asks a question,

1. There are the words they say
2. My interpretation of what's being asked
3. And the actual question the person is attempting to get an answer on

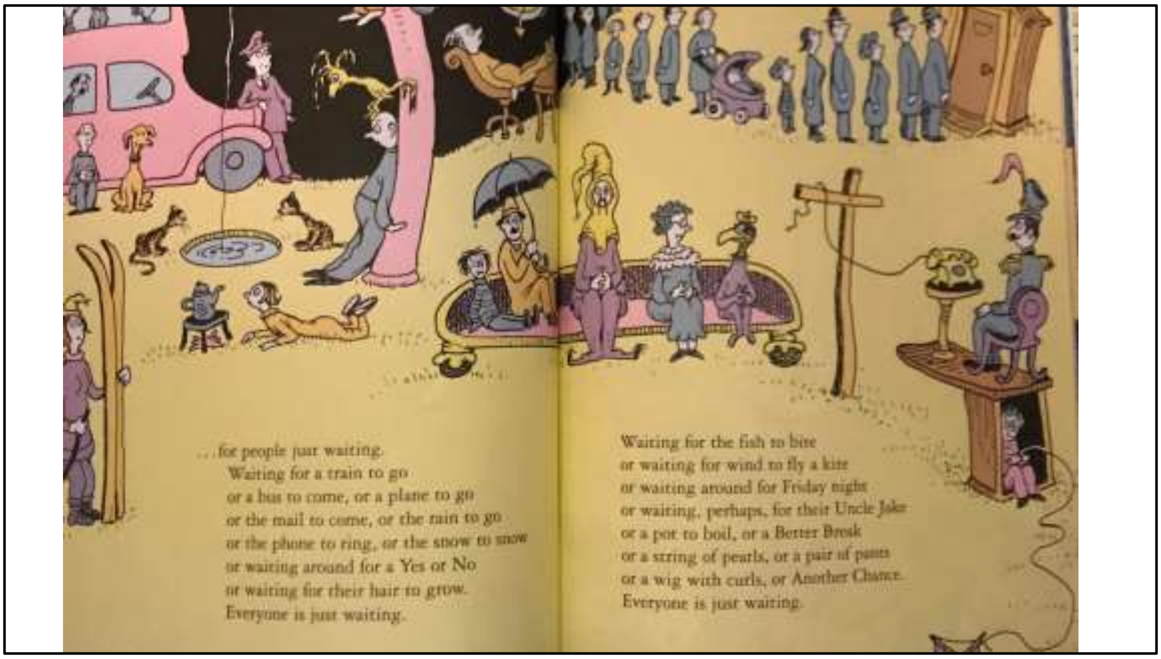
Walt Disney

- Dropped out of school to join the army -the army refused to accept him.
- Before starting Disney, he founded Laugh-o-Gram Studios which went bankrupt due to his inability run a successful business.
- Fired from a Missouri newspaper for not being creative enough.

“The difference in winning and losing is most often…not quitting”



The book “Oh the places you’ll go” by Dr Seuss covers a lot of the ups and downs in life

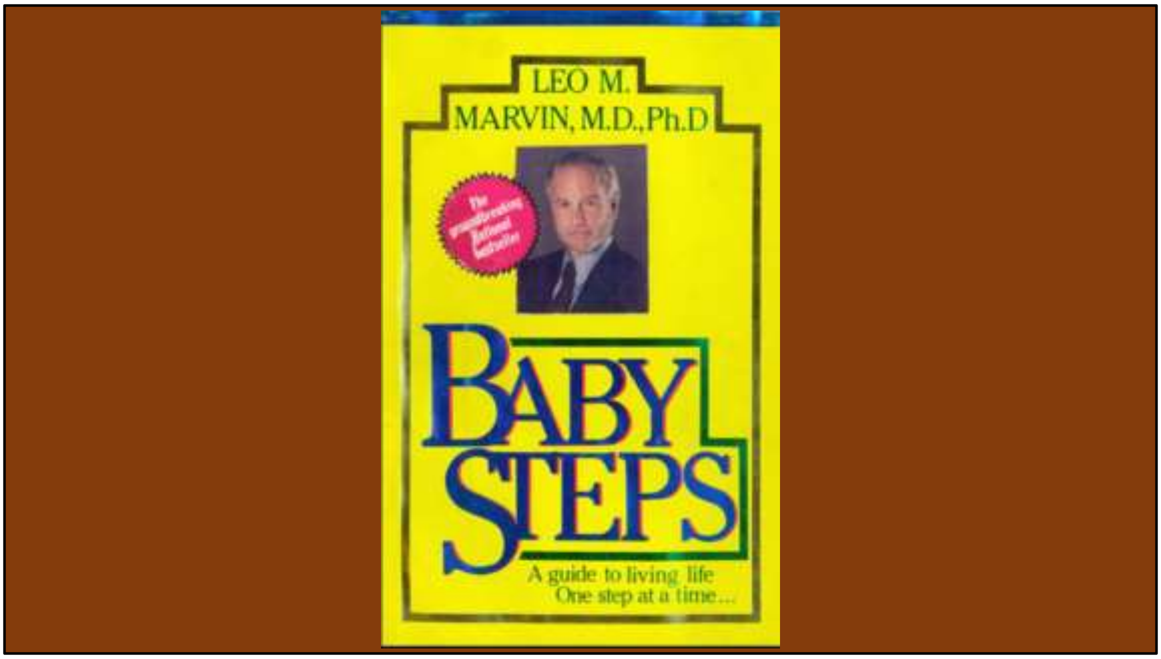


...for people just waiting.
Waiting for a train to go
or a bus to come, or a plane to go
or the mail to come, or the rain to go
or the phone to ring, or the snow to snow
or waiting around for a Yes or No
or waiting for their hair to grow.
Everyone is just waiting.

Waiting for the fish to bite
or waiting for wind to fly a kite
or waiting around for Friday night
or waiting, perhaps, for their Uncle Jake
or a pot to boil, or a Better Break
or a string of pearls, or a pair of pants
or a wig with curls, or Another Chance.
Everyone is just waiting.

Stop Waiting

The toughest problems start with that first bite… first step…..
Just starting can be the toughest part



Baby steps
Start small

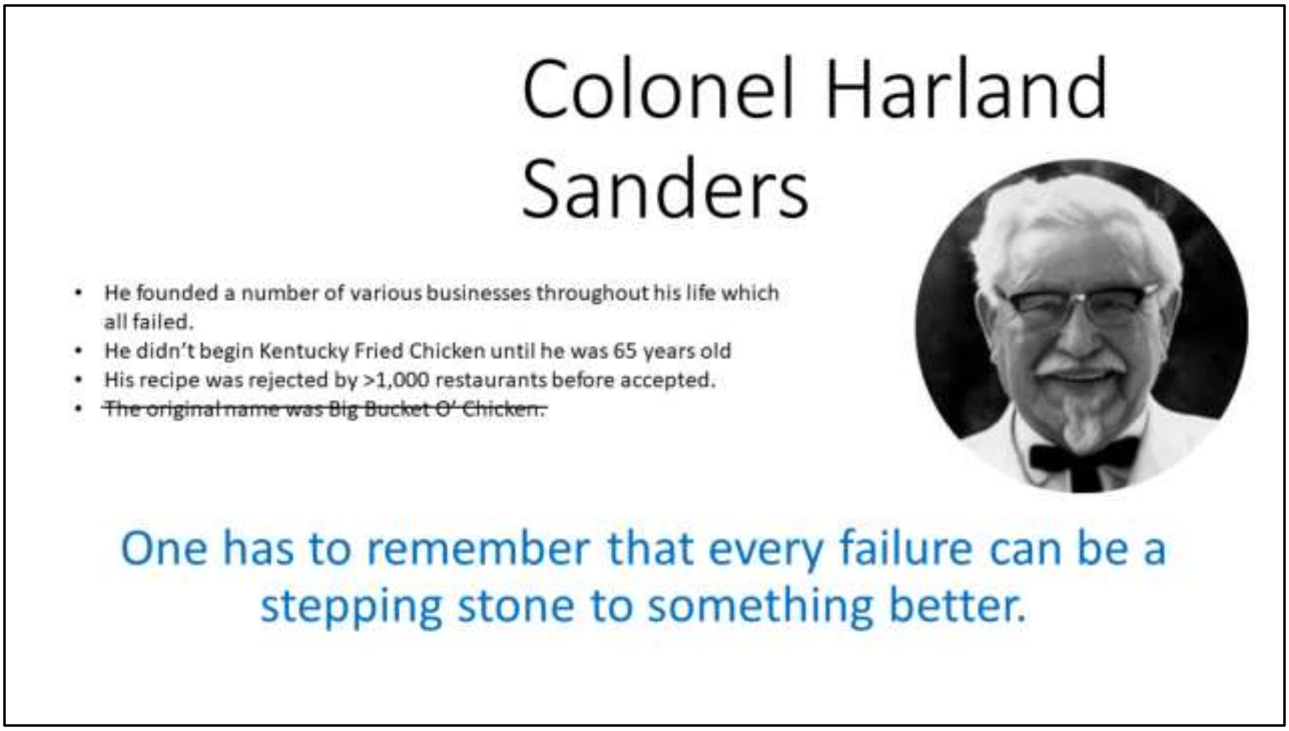
To many starting something or working on a difficult problem, it looks in front of them like an expansive desert.

To others, they see the beach on the other side. They build in reward and things to look forward to.
Milestones to track progress and to learn from mistakes

Colonel Harland Sanders

- He founded a number of various businesses throughout his life which all failed.
- He didn't begin Kentucky Fried Chicken until he was 65 years old
- His recipe was rejected by >1,000 restaurants before accepted.
- The original name was Big Bucket O' Chicken.

One has to remember that every failure can be a stepping stone to something better.

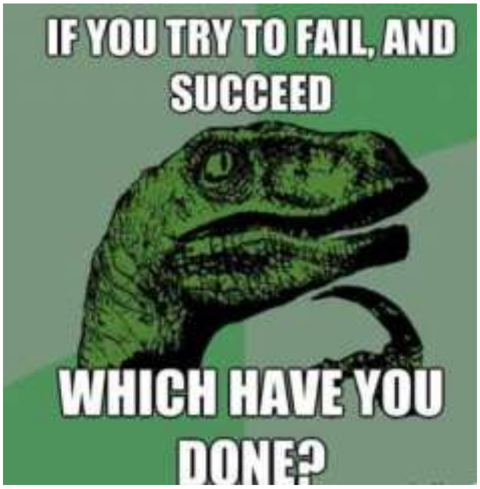


Colonel Harland Sanders

- He founded a number of various businesses throughout his life which all failed.
- He didn't begin Kentucky Fried Chicken until he was 65 years old
- His recipe was rejected by >1,000 restaurants before accepted.
- ~~The original name was Big Bucket O' Chicken.~~

One has to remember that every failure can be a stepping stone to something better.

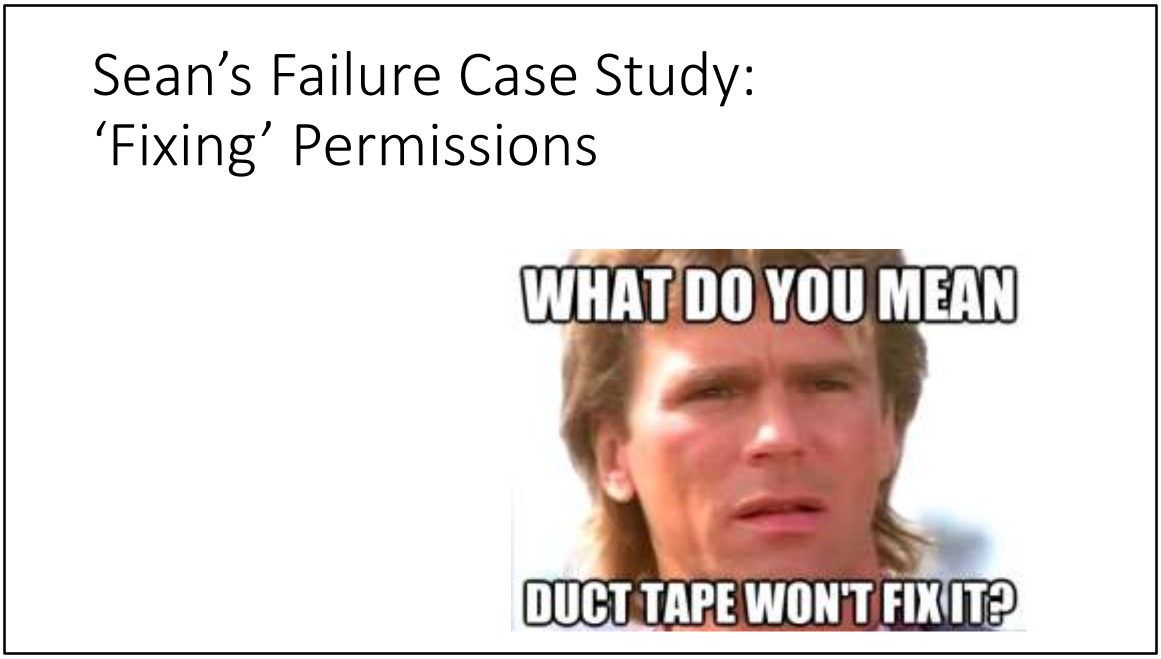
Colonel Sanders founded a number of various businesses throughout his life which all failed.
He didn't begin Kentucky Fried Chicken until he was 65 years old, and his recipe was rejected by 1,009 restaurants before he found one that would use it.



Technically Accurate

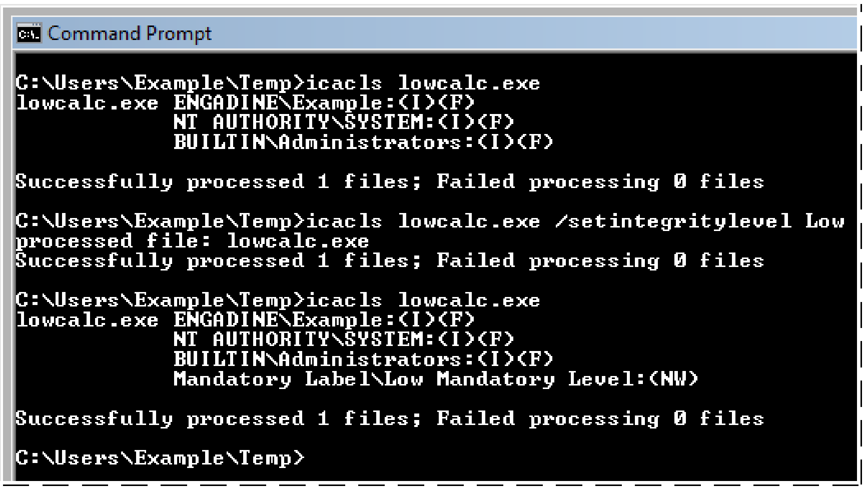
Case Studies in Failing forward…

In this section, I will cover some of my failures and how I handled them

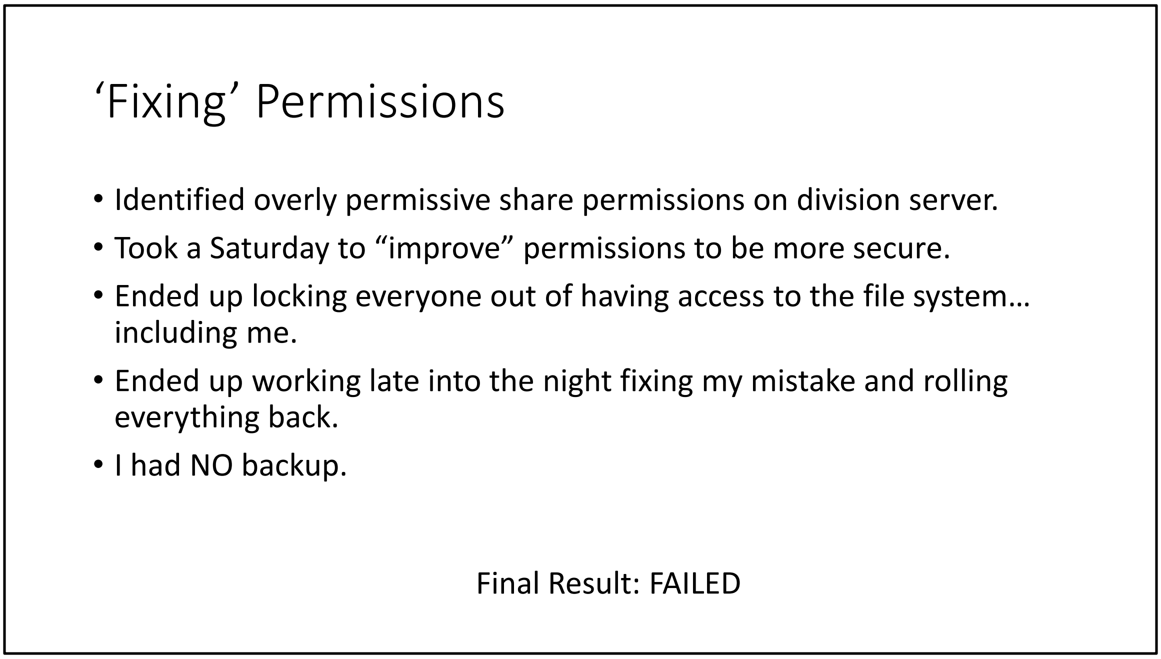


Sean’s Failure Case Study: ‘Fixing’ Permissions

icacls



```
C:\Users\Example\Temp>icacls lowcalc.exe
lowcalc.exe ENGADINE\Example:(I)(F)
            NT AUTHORITY\SYSTEM:(I)(F)
            BUILTIN\Administrators:(I)(F)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Example\Temp>icacls lowcalc.exe /setintegritylevel Low
processed file: lowcalc.exe
Successfully processed 1 files; Failed processing 0 files

C:\Users\Example\Temp>icacls lowcalc.exe
lowcalc.exe ENGADINE\Example:(I)(F)
            NT AUTHORITY\SYSTEM:(I)(F)
            BUILTIN\Administrators:(I)(F)
            Mandatory Label\Low Mandatory Level:(NW)

Successfully processed 1 files; Failed processing 0 files

C:\Users\Example\Temp>
```

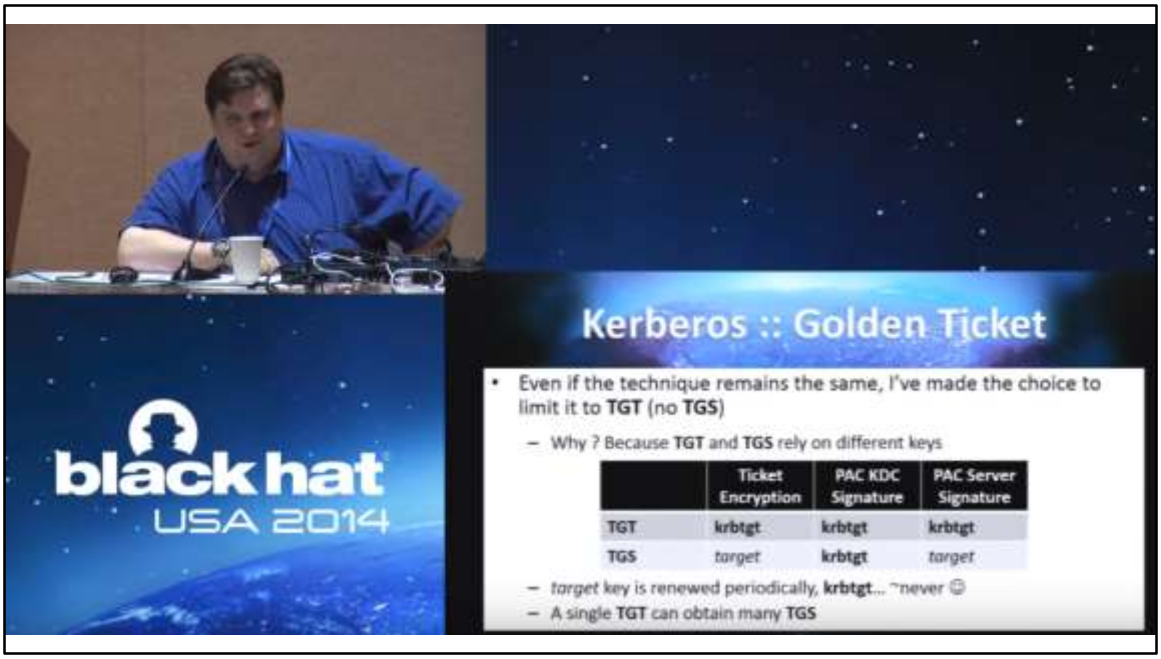


‘Fixing’ Permissions

- Identified overly permissive share permissions on division server.
- Took a Saturday to “improve” permissions to be more secure.
- Ended up locking everyone out of having access to the file system… including me.
- Ended up working late into the night fixing my mistake and rolling everything back.
- I had NO backup.

Final Result: FAILED

Sean's Failure Case Study: Detecting Golden Tickets



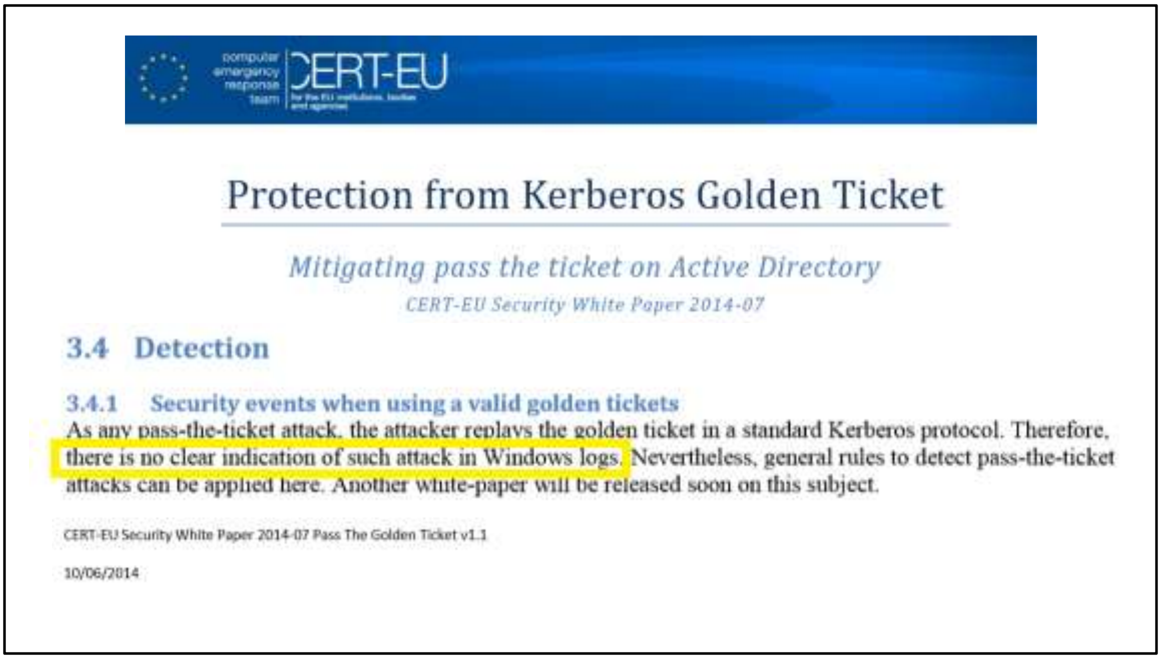
Kerberos :: Golden Ticket

- Even if the technique remains the same, I've made the choice to limit it to **TGT** (no **TGS**)
  - Why ? Because **TGT** and **TGS** rely on different keys

	Ticket Encryption	PAC KDC Signature	PAC Server Signature
TGT	**krbtgt**	**krbtgt**	**krbtgt**
TGS	*target*	**krbtgt**	*target*

  - *target* key is renewed periodically, **krbtgt**... ~never ☺
  - A single **TGT** can obtain many **TGS**

Skip & Ben: Black Hat 2014



Protection from Kerberos Golden Ticket

Mitigating pass the ticket on Active Directory

CERT-EU Security White Paper 2014-07

3.4 Detection

3.4.1 Security events when using a valid golden tickets

As any pass-the-ticket attack, the attacker replays the golden ticket in a standard Kerberos protocol. Therefore, there is no clear indication of such attack in Windows logs. Nevertheless, general rules to detect pass-the-ticket attacks can be applied here. Another white-paper will be released soon on this subject.

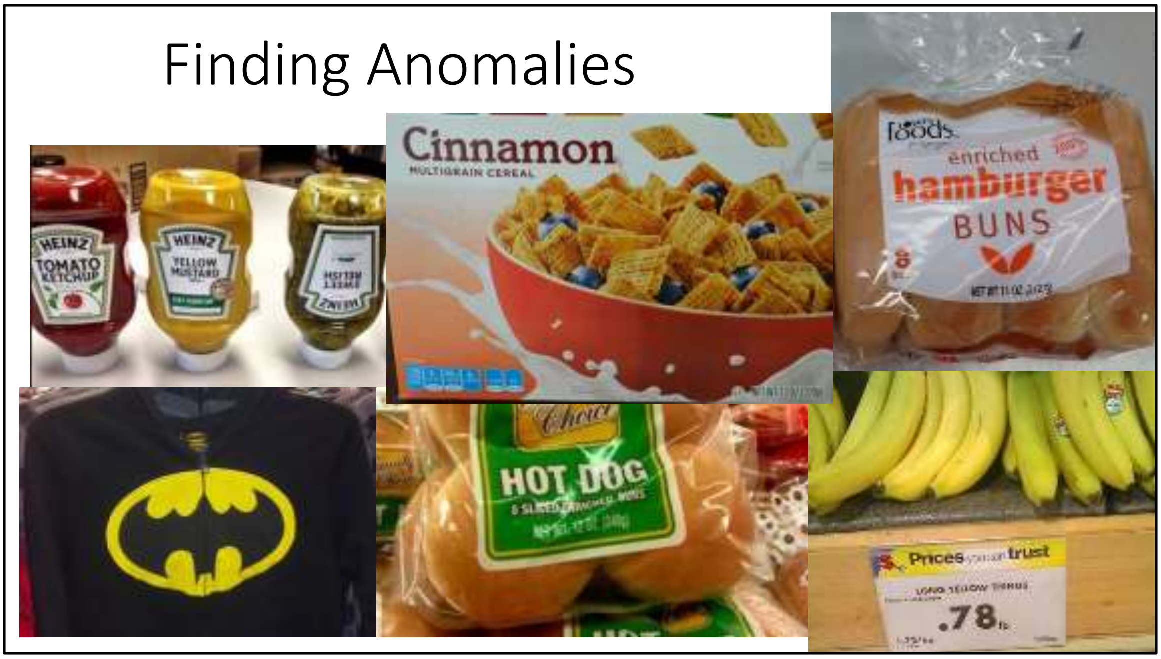
CERT-EU Security White Paper 2014-07 Pass The Golden Ticket v1.1

10/06/2014

According to CERT-EU's Golden Ticket whitepaper released last summer and last updated in October 2014, Golden Ticket attacks do not have clear indication in Windows logs.

======

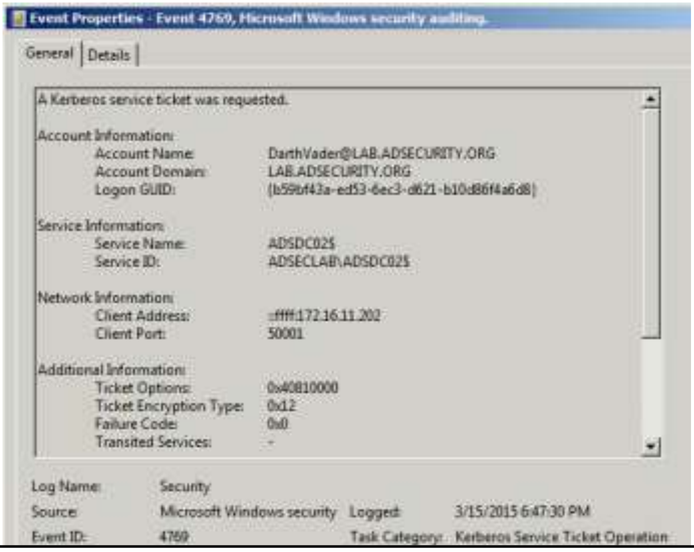
Protection from Kerberos Golden Ticket
Mitigating pass the ticket on Active Directory
CERT-EU Security White Paper 2014-07
http://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf



Finding Anomalies

In order to find something that shouldn't be, look for anomalies (things that don't fit)

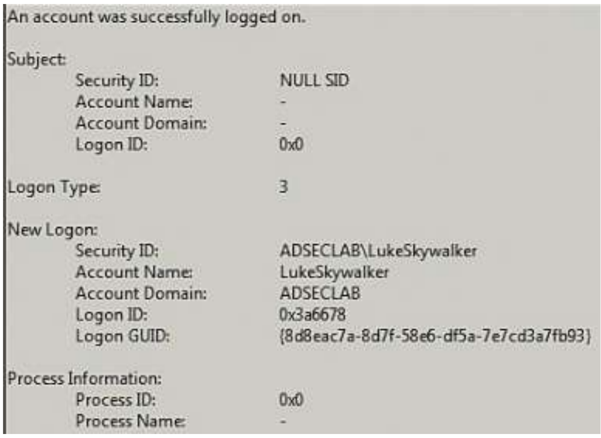
Nope, Nothing Unusual Here


Event Properties - Event 4769, Microsoft Windows security auditing.
General
Details

```
A Kerberos service ticket was requested.

Account Information:
        Account Name:           DarthVader@LAB.ADSECURITY.ORG
        Account Domain:         LAB.ADSECURITY.ORG
        Logon GUID:             {b59bf43a-ed53-6ec3-d621-b10d86f4a6d8}

Service Information:
        Service Name:           ADSDC02$
        Service ID:             ADSECLAB\ADSDC02$

Network Information:
        Client Address:         ::ffff:172.16.11.202
        Client Port:            50001

Additional Information:
        Ticket Options:         0x40810000
        Ticket Encryption Type: 0x12
        Failure Code:           0x0
        Transited Services:     -
```

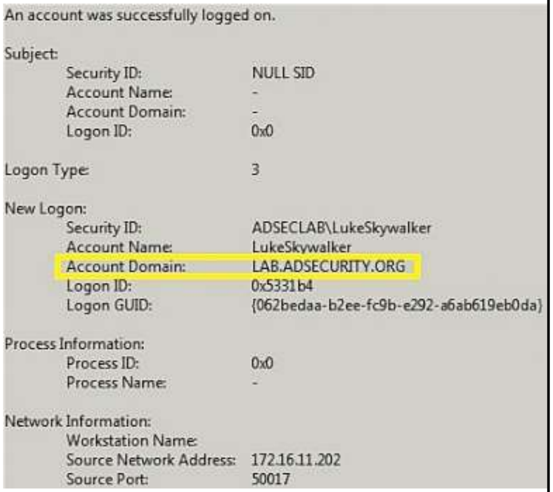
```
Log Name:     Security
Source:       Microsoft Windows security   Logged:         3/15/2015 6:47:30 PM
Event ID:     4769                         Task Category:  Kerberos Service Ticket Operation
```

Silver Ticket Event 4624: Account Logon



```
An account was successfully logged on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

New Logon:
        Security ID:            ADSECLAB\LukeSkywalker
        Account Name:           LukeSkywalker
        Account Domain:         ADSECLAB
        Logon ID:               0x3a6678
        Logon GUID:             {8d8eac7a-8d7f-58e6-df5a-7e7cd3a7fb93}

Process Information:
        Process ID:             0x0
        Process Name:           -
```

Valid

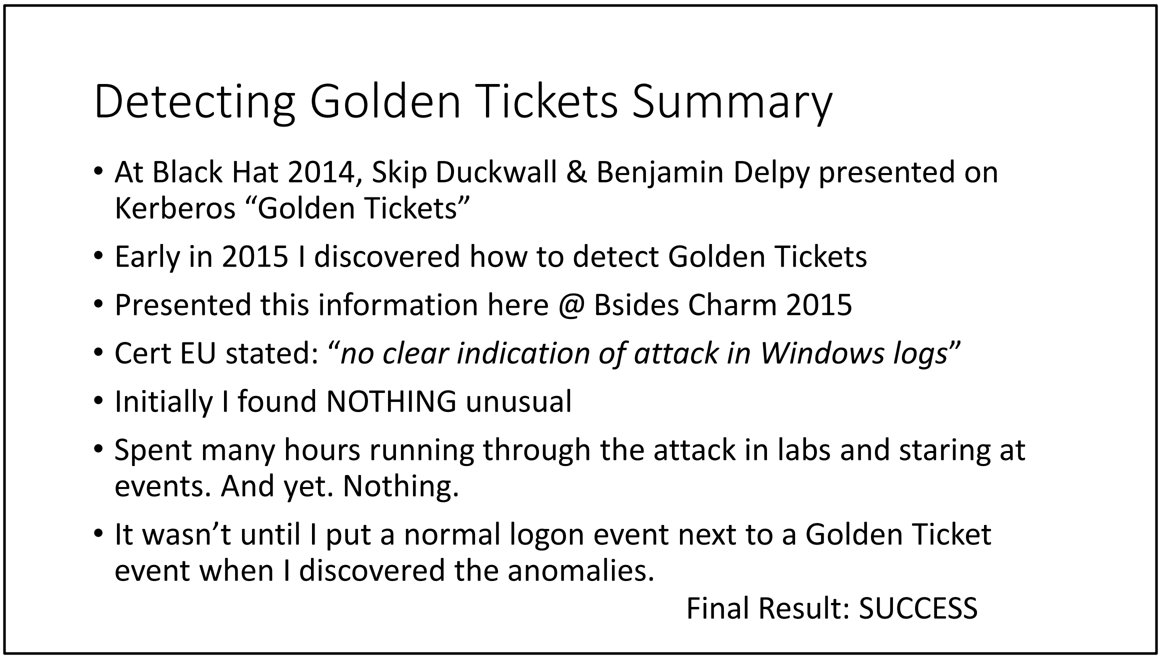


```
An account was successfully logged on.

Subject:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
        Logon ID:               0x0

Logon Type:                     3

New Logon:
        Security ID:            ADSECLAB\LukeSkywalker
        Account Name:           LukeSkywalker
        Account Domain:         LAB.ADSECURITY.ORG
        Logon ID:               0x5331b4
        Logon GUID:             {062bedaa-b2ee-fc9b-e292-a6ab619eb0da}

Process Information:
        Process ID:             0x0
        Process Name:           -

Network Information:
        Workstation Name:
        Source Network Address: 172.16.11.202
        Source Port:            50017
```

Forged Ticket

Let’s look at some events - Note: These are just some of the events I discovered while researching forged ticket detection.

In this Silver Ticket event on a member server, the domain field is the domain FQDN when compared with a valid event which has the short Domain Name.

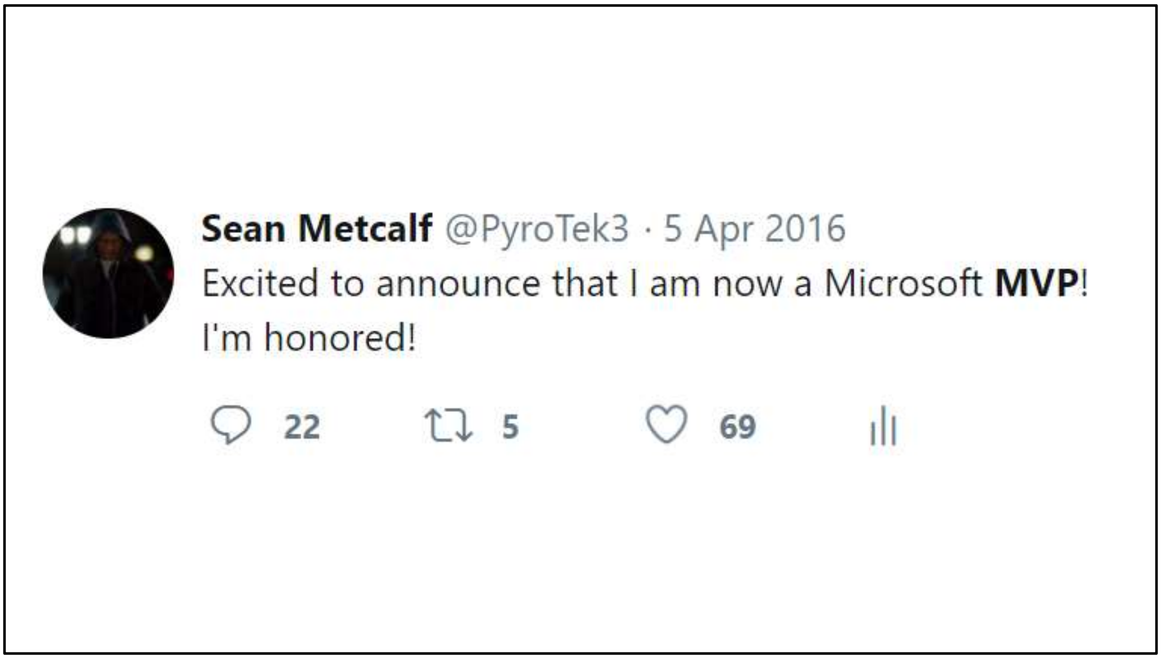


Detecting Golden Tickets Summary

- At Black Hat 2014, Skip Duckwall & Benjamin Delpy presented on Kerberos “Golden Tickets”
- Early in 2015 I discovered how to detect Golden Tickets
- Presented this information here @ Bsides Charm 2015
- Cert EU stated: *“no clear indication of attack in Windows logs*”
- Initially I found NOTHING unusual
- Spent many hours running through the attack in labs and staring at events. And yet. Nothing.
- It wasn’t until I put a normal logon event next to a Golden Ticket event when I discovered the anomalies.

Final Result: SUCCESS

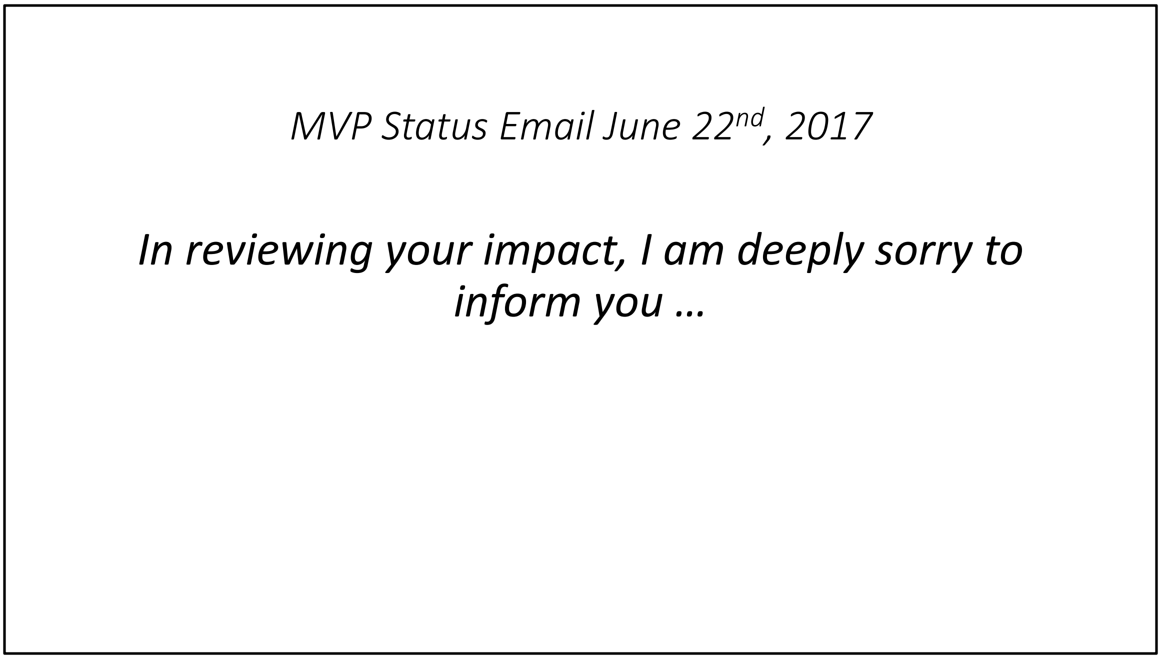
Sean’s Failure Case Study: Microsoft MVP Status



Sean Metcalf @PyroTek3 · 5 Apr 2016

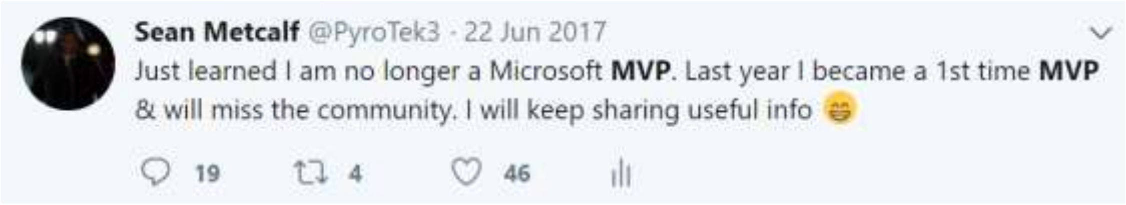
Excited to announce that I am now a Microsoft **MVP**! I'm honored!

22 5 69



MVP Status Email June 22nd, 2017

In reviewing your impact, I am deeply sorry to inform you …



Sean Metcalf @PyroTek3 · 22 Jun 2017

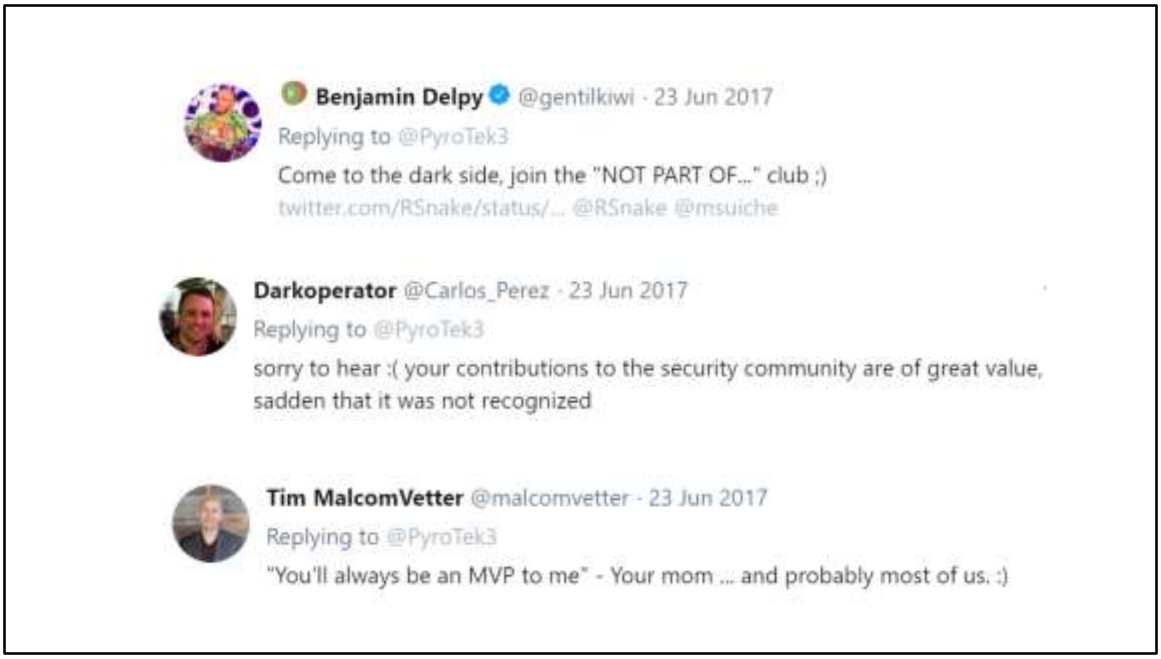
Just learned I am no longer a Microsoft **MVP**. Last year I became a 1st time **MVP** & will miss the community. I will keep sharing useful info 😁

Chris Thompson @retBandit · 27 Jun 2017

eponymous unum @_devonkerr_ · 22 Jun 2017

Replying to @PyroTek3

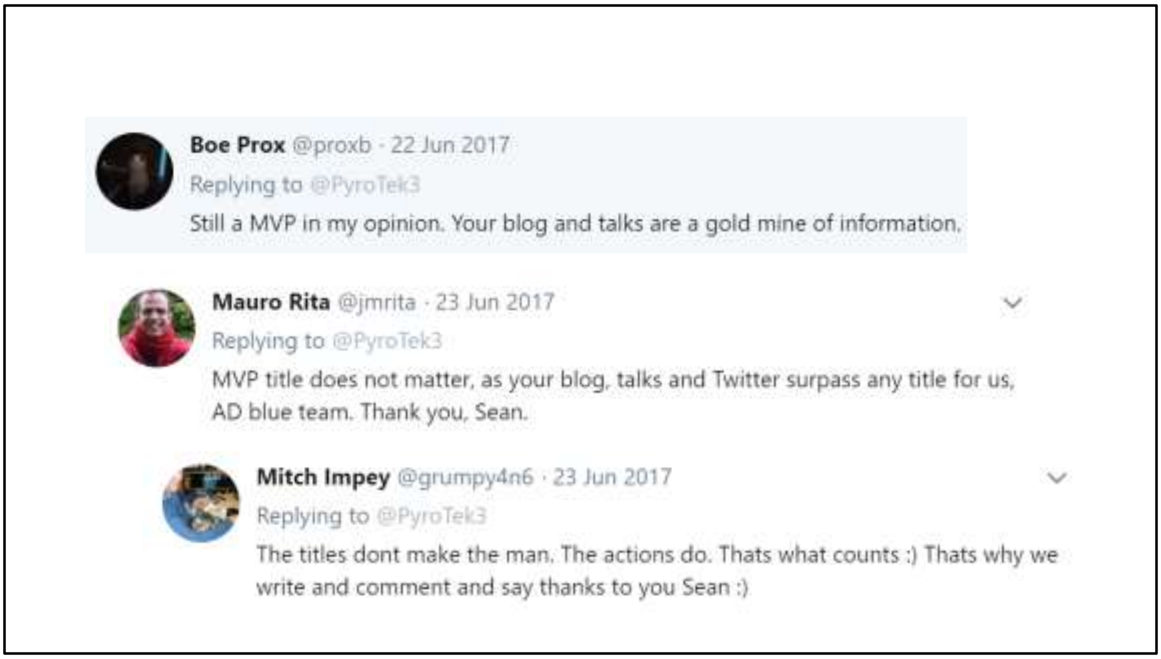
Sean, in my heart of hearts you are the top MS MVP



Benjamin Delpy @gentilkiwi · 23 Jun 2017
Replying to @PyroTek3
Come to the dark side, join the "NOT PART OF..." club ;)
twitter.com/RSnake/status/... @RSnake @msuiche

Darkoperator @Carlos_Perez · 23 Jun 2017
Replying to @PyroTek3
sorry to hear :(your contributions to the security community are of great value, sadden that it was not recognized

Tim MalcomVetter @malcomvetter · 23 Jun 2017
Replying to @PyroTek3
"You'll always be an MVP to me" - Your mom ... and probably most of us. :)



Boe Prox @proxb · 22 Jun 2017

Replying to @PyroTek3

Still a MVP in my opinion. Your blog and talks are a gold mine of information.

Mauro Rita @jmrita · 23 Jun 2017

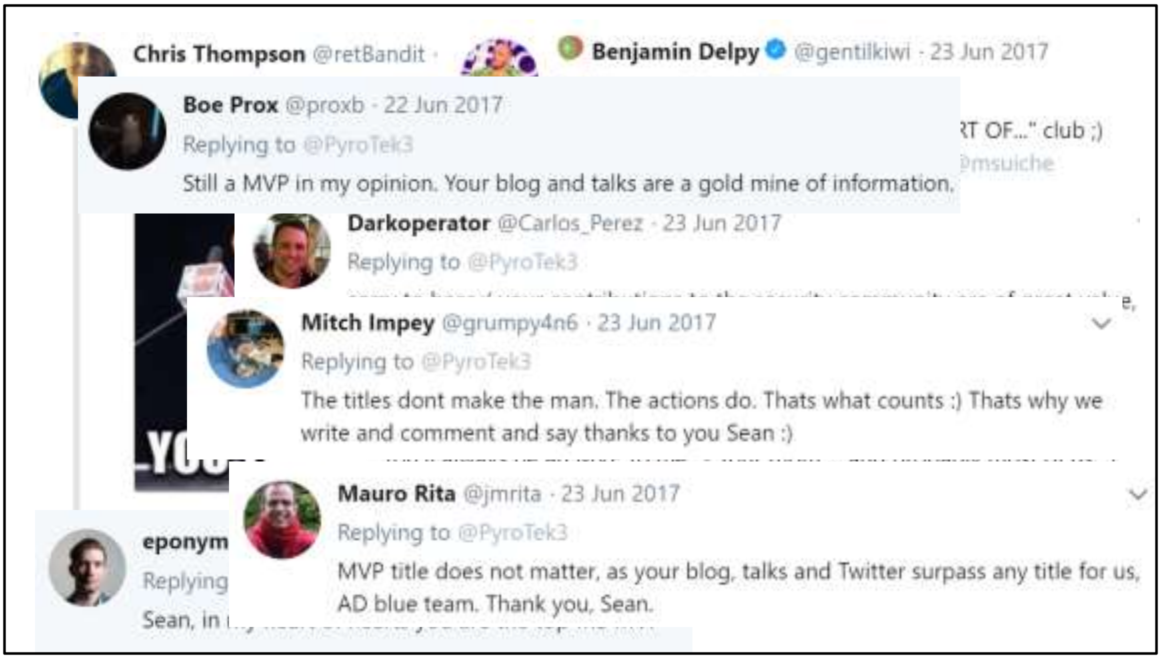
Replying to @PyroTek3

MVP title does not matter, as your blog, talks and Twitter surpass any title for us, AD blue team. Thank you, Sean.

Mitch Impey @grumpy4n6 · 23 Jun 2017

Replying to @PyroTek3

The titles dont make the man. The actions do. Thats what counts :) Thats why we write and comment and say thanks to you Sean :)



Chris Thompson @retBandit ·

Benjamin Delpy @gentilkiwi · 23 Jun 2017

RT OF..." club ;)

@msuiche

Boe Prox @proxb · 22 Jun 2017

Replying to @PyroTek3

Still a MVP in my opinion. Your blog and talks are a gold mine of information.

Darkoperator @Carlos_Perez · 23 Jun 2017

Replying to @PyroTek3

Mitch Impey @grumpy4n6 · 23 Jun 2017

Replying to @PyroTek3

The titles dont make the man. The actions do. Thats what counts :) Thats why we write and comment and say thanks to you Sean :)

Mauro Rita @jmrita · 23 Jun 2017

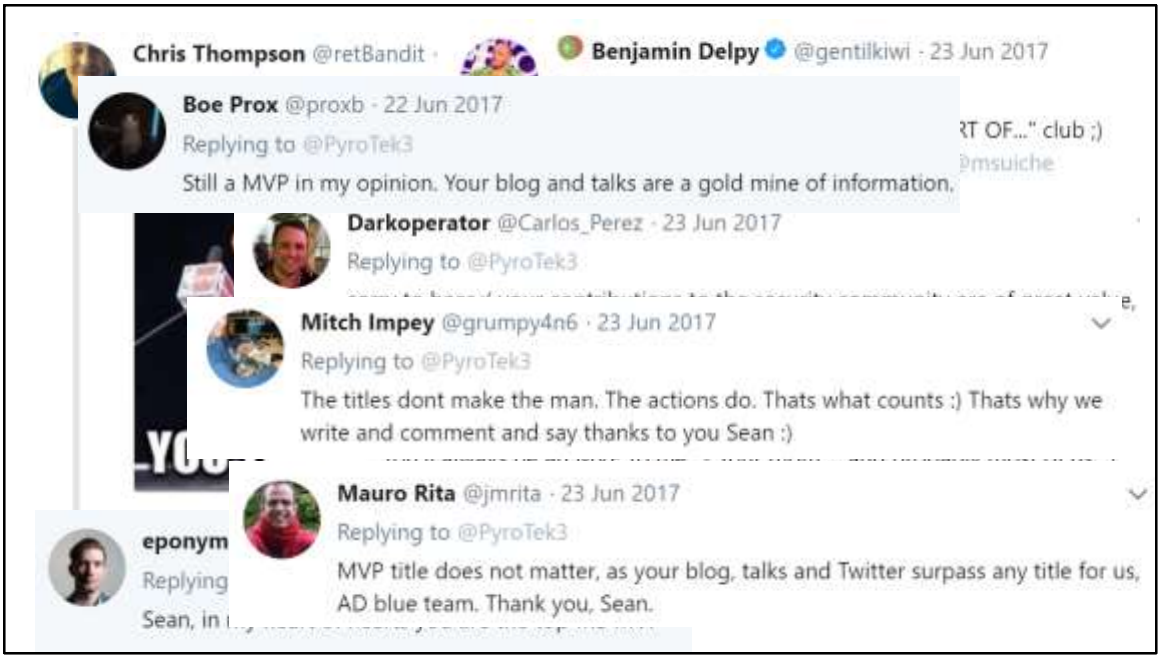
Replying to @PyroTek3

MVP title does not matter, as your blog, talks and Twitter surpass any title for us, AD blue team. Thank you, Sean.

eponym

Replying

Sean, in



Chris Thompson @retBandit ·

Benjamin Delpy @gentilkiwi · 23 Jun 2017

RT OF..." club ;)

@msuiche

Boe Prox @proxb · 22 Jun 2017

Replying to @PyroTek3

Still a MVP in my opinion. Your blog and talks are a gold mine of information.

Darkoperator @Carlos_Perez · 23 Jun 2017

Replying to @PyroTek3

Mitch Impey @grumpy4n6 · 23 Jun 2017

Replying to @PyroTek3

The titles dont make the man. The actions do. Thats what counts :) Thats why we write and comment and say thanks to you Sean :)

Mauro Rita @jmrita · 23 Jun 2017

Replying to @PyroTek3

MVP title does not matter, as your blog, talks and Twitter surpass any title for us, AD blue team. Thank you, Sean.

eponym

Replying

Sean, in

Active Directory Security:
The Journey

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

Despite not being renewed as an MVP, my talk submission was selected for Microsoft’s mostly internal conference, BlueHat, in Redmond, WA.

ABOUT

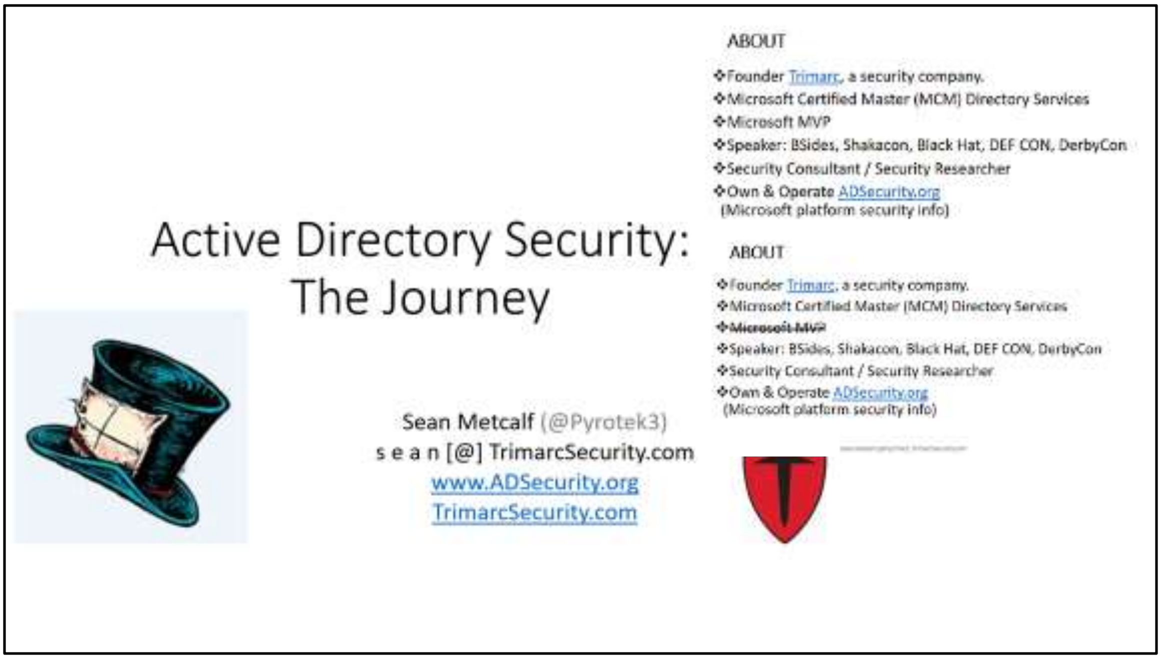
- ❖Founder Trimarc, a security company.
- ❖Microsoft Certified Master (MCM) Directory Services
- ❖Microsoft MVP
- ❖Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- ❖Security Consultant / Security Researcher
- ❖Own & Operate ADSecurity.org (Microsoft platform security info)

[illegible]

Active Directory Security: The Journey

Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

I live edited my “About” slide in front of the Microsoft audience.



Active Directory Security: The Journey

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

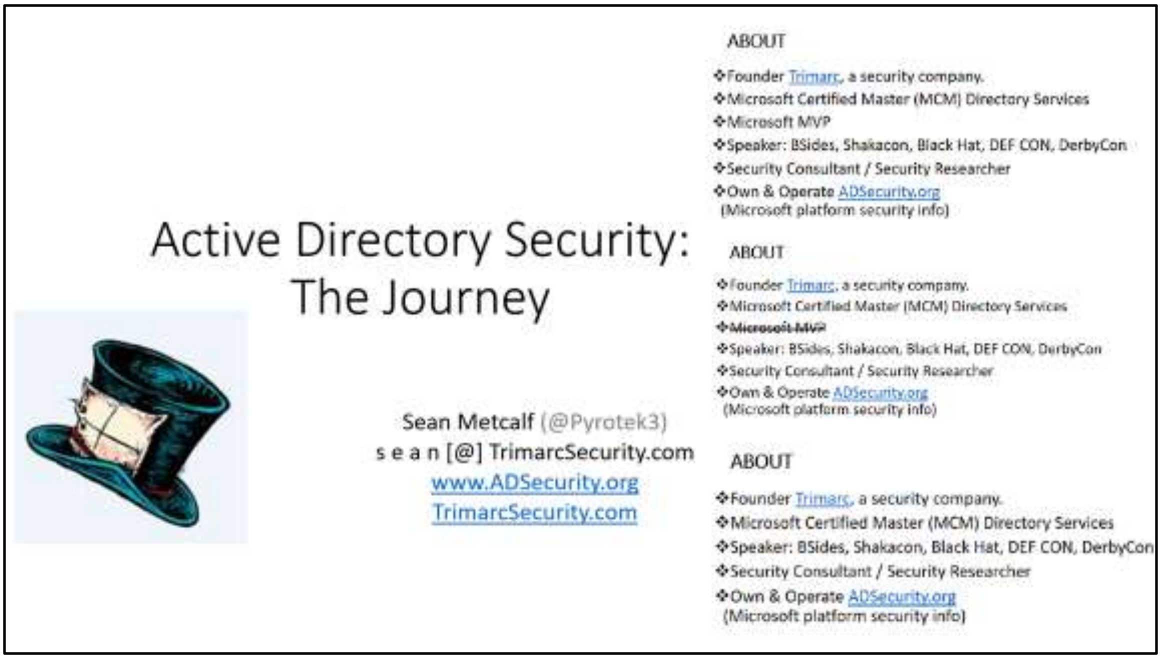
ABOUT

- ❖Founder Trimarc, a security company.
- ❖Microsoft Certified Master (MCM) Directory Services
- ❖Microsoft MVP
- ❖Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- ❖Security Consultant / Security Researcher
- ❖Own & Operate ADSecurity.org (Microsoft platform security info)

ABOUT

- ❖Founder Trimarc, a security company.
- ❖Microsoft Certified Master (MCM) Directory Services
- ❖~~Microsoft MVP~~
- ❖Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- ❖Security Consultant / Security Researcher
- ❖Own & Operate ADSecurity.org (Microsoft platform security info)

I live edited my “About” slide in front of the Microsoft audience.



Active Directory Security: The Journey

Sean Metcalf (@Pyrotek3)
s e a n [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com

ABOUT

- ❖Founder Trimarc, a security company.
- ❖Microsoft Certified Master (MCM) Directory Services
- ❖Microsoft MVP
- ❖Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- ❖Security Consultant / Security Researcher
- ❖Own & Operate ADSecurity.org
(Microsoft platform security info)

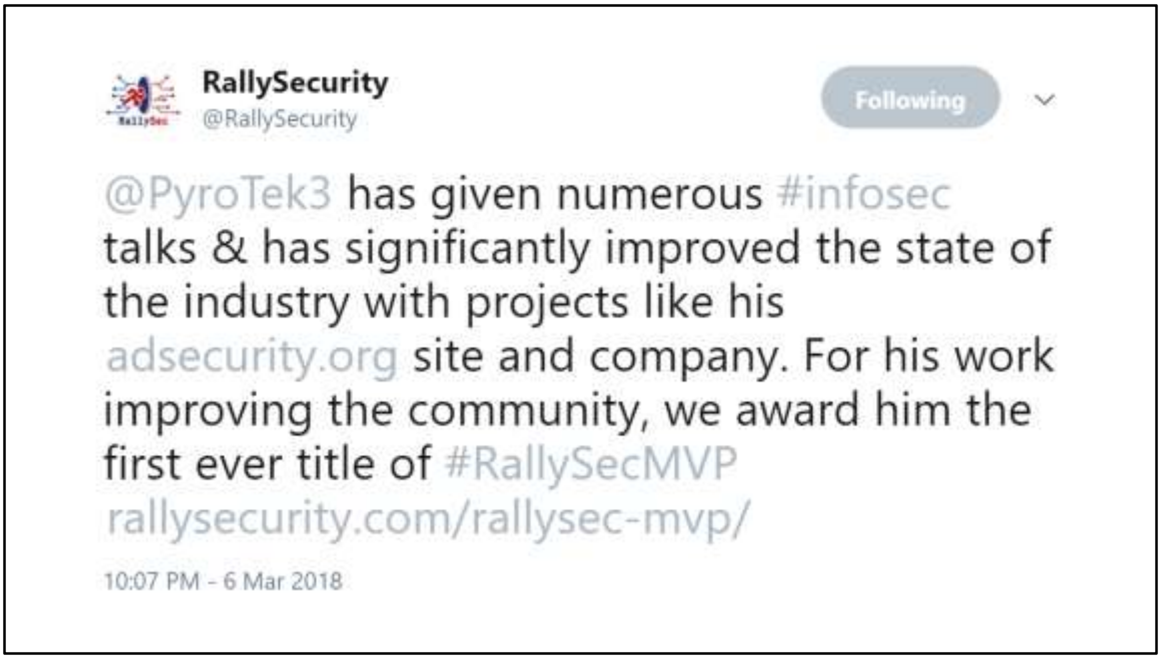
ABOUT

- ❖Founder Trimarc, a security company.
- ❖Microsoft Certified Master (MCM) Directory Services
- ❖~~Microsoft MVP~~
- ❖Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- ❖Security Consultant / Security Researcher
- ❖Own & Operate ADSecurity.org
(Microsoft platform security info)

ABOUT

- ❖Founder Trimarc, a security company.
- ❖Microsoft Certified Master (MCM) Directory Services
- ❖Speaker: BSides, Shakacon, Black Hat, DEF CON, DerbyCon
- ❖Security Consultant / Security Researcher
- ❖Own & Operate ADSecurity.org
(Microsoft platform security info)

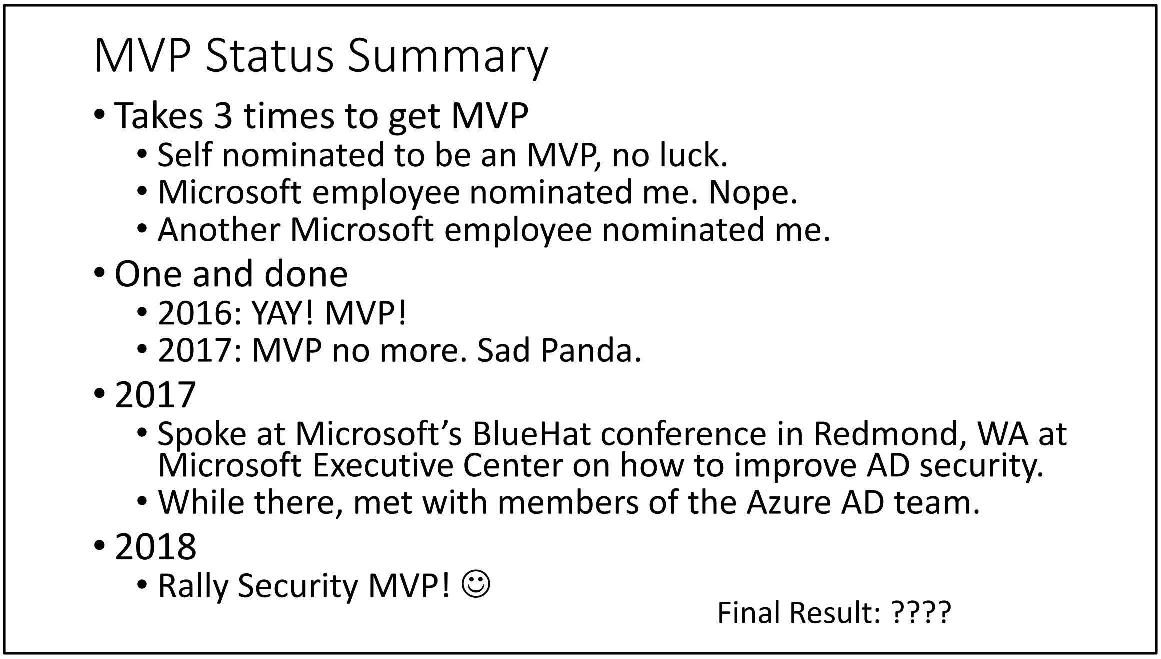
I live edited my "About" slide in front of the Microsoft audience.



RallySecurity
@RallySecurity

@PyroTek3 has given numerous #infosec talks & has significantly improved the state of the industry with projects like his adsecurity.org site and company. For his work improving the community, we award him the first ever title of #RallySecMVP rallysecurity.com/rallysec-mvp/

10:07 PM - 6 Mar 2018

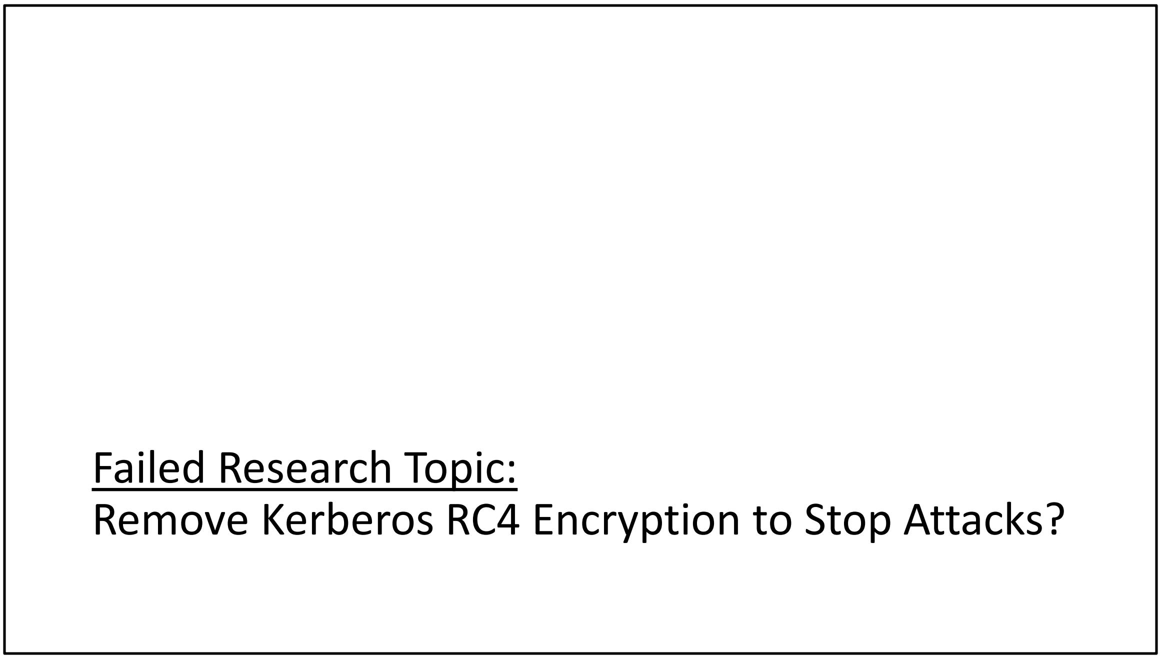


MVP Status Summary

- Takes 3 times to get MVP
  - Self nominated to be an MVP, no luck.
  - Microsoft employee nominated me. Nope.
  - Another Microsoft employee nominated me.
- One and done
  - 2016: YAY! MVP!
  - 2017: MVP no more. Sad Panda.
- 2017
  - Spoke at Microsoft’s BlueHat conference in Redmond, WA at Microsoft Executive Center on how to improve AD security.
  - While there, met with members of the Azure AD team.
- 2018
  - Rally Security MVP! ☺

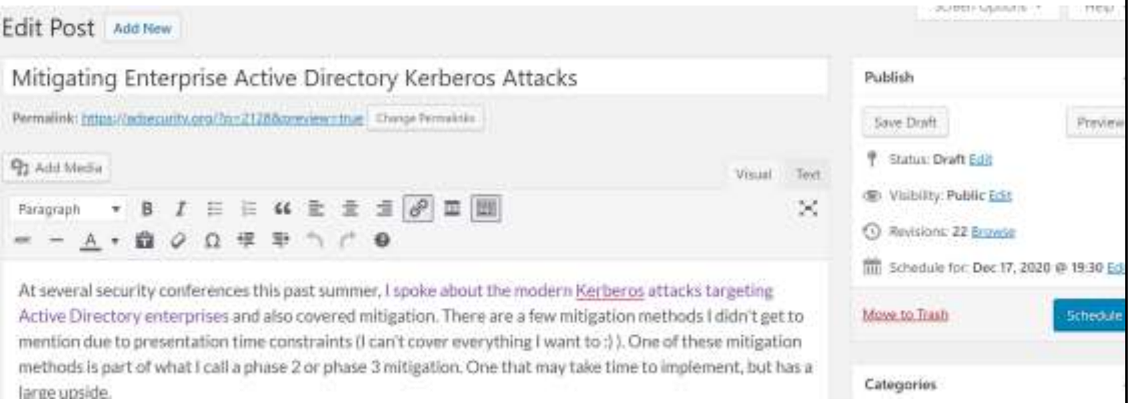
Final Result: ????

Sean’s Failure Case Study: Failed Research Topics



Failed Research Topic:
Remove Kerberos RC4 Encryption to Stop Attacks?

I hypothesized this might work



Edit Post

Mitigating Enterprise Active Directory Kerberos Attacks

Permalink: https://adsecurity.org/?p=2128&preview=true

At several security conferences this past summer, I spoke about the modern Kerberos attacks targeting Active Directory enterprises and also covered mitigation. There are a few mitigation methods I didn't get to mention due to presentation time constraints (I can't cover everything I want to :)). One of these mitigation methods is part of what I call a phase 2 or phase 3 mitigation. One that may take time to implement, but has a large upside.

Publish

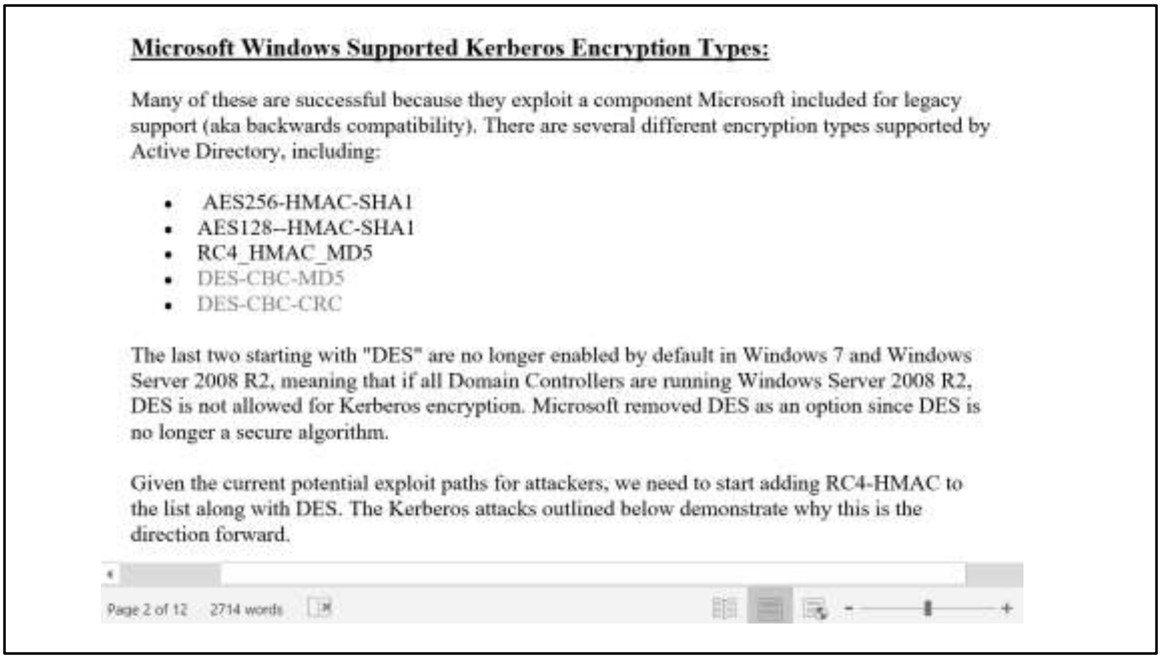
Status: Draft Edit

Visibility: Public Edit

Revisions: 22 Browse

Schedule for: Dec 17, 2020 @ 19:30 Edi

I even started writing the background information in an ADSecurity.org blog post that I was unable to publish since I was wrong.



Microsoft Windows Supported Kerberos Encryption Types:

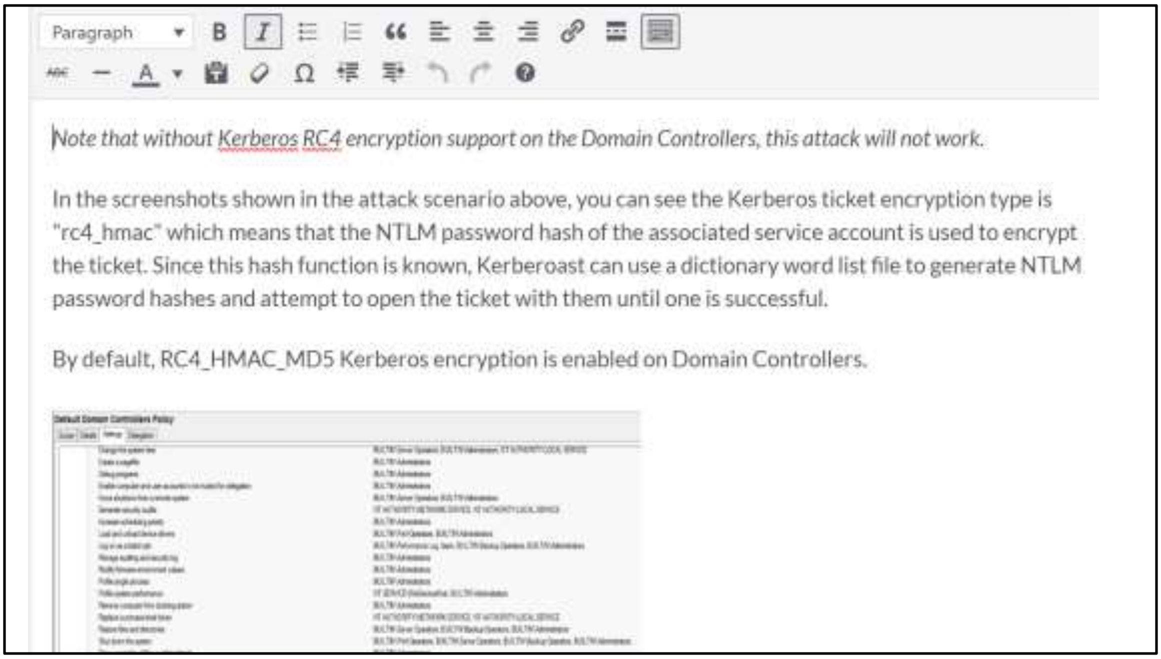
Many of these are successful because they exploit a component Microsoft included for legacy support (aka backwards compatibility). There are several different encryption types supported by Active Directory, including:

- AES256-HMAC-SHA1
- AES128--HMAC-SHA1
- RC4_HMAC_MD5
- DES-CBC-MD5
- DES-CBC-CRC

The last two starting with "DES" are no longer enabled by default in Windows 7 and Windows Server 2008 R2, meaning that if all Domain Controllers are running Windows Server 2008 R2, DES is not allowed for Kerberos encryption. Microsoft removed DES as an option since DES is no longer a secure algorithm.

Given the current potential exploit paths for attackers, we need to start adding RC4-HMAC to the list along with DES. The Kerberos attacks outlined below demonstrate why this is the direction forward.

I even started writing the background information in an ADSecurity.org blog post that I was unable to publish since I was wrong.

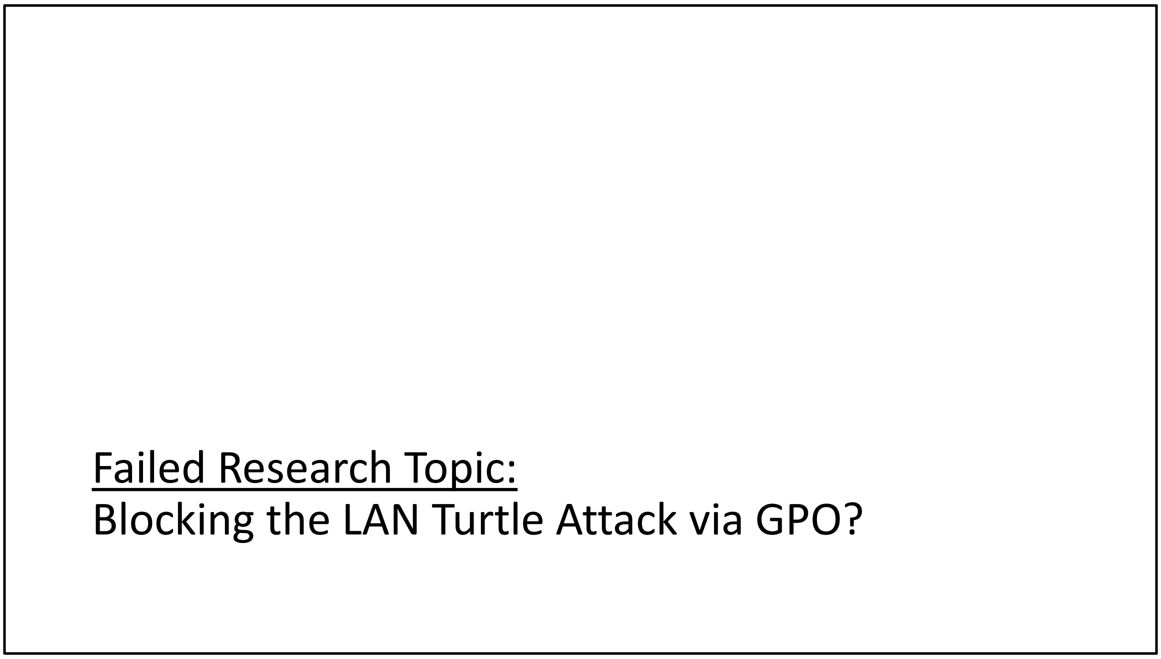


Note that without Kerberos RC4 encryption support on the Domain Controllers, this attack will not work.

In the screenshots shown in the attack scenario above, you can see the Kerberos ticket encryption type is "rc4_hmac" which means that the NTLM password hash of the associated service account is used to encrypt the ticket. Since this hash function is known, Kerberoast can use a dictionary word list file to generate NTLM password hashes and attempt to open the ticket with them until one is successful.

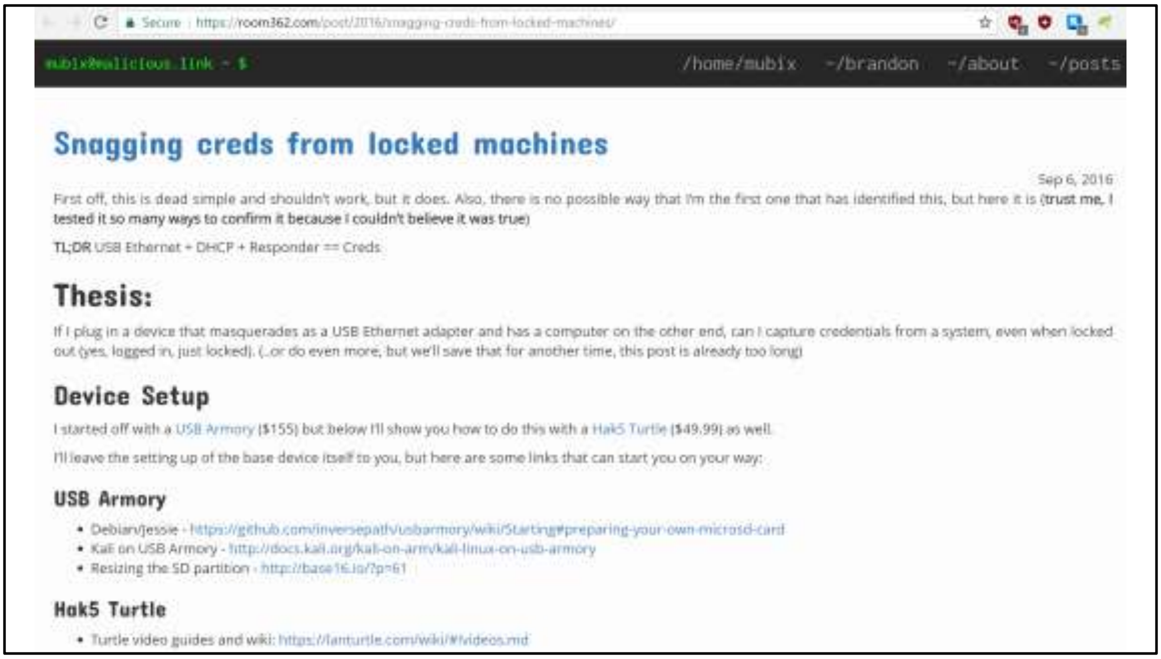
By default, RC4_HMAC_MD5 Kerberos encryption is enabled on Domain Controllers.

I even started writing the background information in an ADSecurity.org blog post that I was unable to publish since I was wrong.



Failed Research Topic:
Blocking the LAN Turtle Attack via GPO?

I can do this!



Secure | https://room362.com/post/2016/snagging-creds-from-locked-machines/
mubix@malicious.link ~ $
/home/mubix
~/brandon
~/about
~/posts

Snagging creds from locked machines

Sep 6, 2016

First off, this is dead simple and shouldn't work, but it does. Also, there is no possible way that I'm the first one that has identified this, but here it is (**trust me, I tested it so many ways to confirm it because I couldn't believe it was true**)

TL;DR USB Ethernet + DHCP + Responder == Creds

Thesis:

If I plug in a device that masquerades as a USB Ethernet adapter and has a computer on the other end, can I capture credentials from a system, even when locked out (yes, logged in, just locked). (..or do even more, but we'll save that for another time, this post is already too long)

Device Setup

I started off with a USB Armory ($155) but below I'll show you how to do this with a Hak5 Turtle ($49.99) as well.

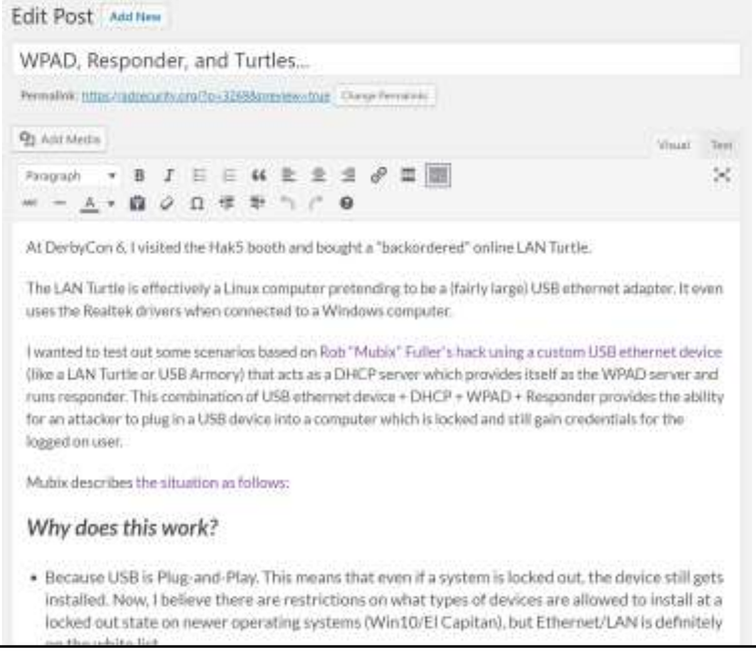
I'll leave the setting up of the base device itself to you, but here are some links that can start you on your way:

USB Armory

- Debian/Jessie - https://github.com/inversepath/usbarmory/wiki/Starting#preparing-your-own-microsd-card
- Kali on USB Armory - http://docs.kali.org/kali-on-arm/kali-linux-on-usb-armory
- Resizing the SD partition - http://base16.io/?p=61

Hak5 Turtle

- Turtle video guides and wiki: https://lanturtle.com/wiki/#!videos.md



WPAD, Responder, and Turtles…

Permalink: https://adsecurity.org/?p=3268&preview=true

At DerbyCon 6, I visited the Hak5 booth and bought a "backordered" online LAN Turtle.

The LAN Turtle is effectively a Linux computer pretending to be a (fairly large) USB ethernet adapter. It even uses the Realtek drivers when connected to a Windows computer.

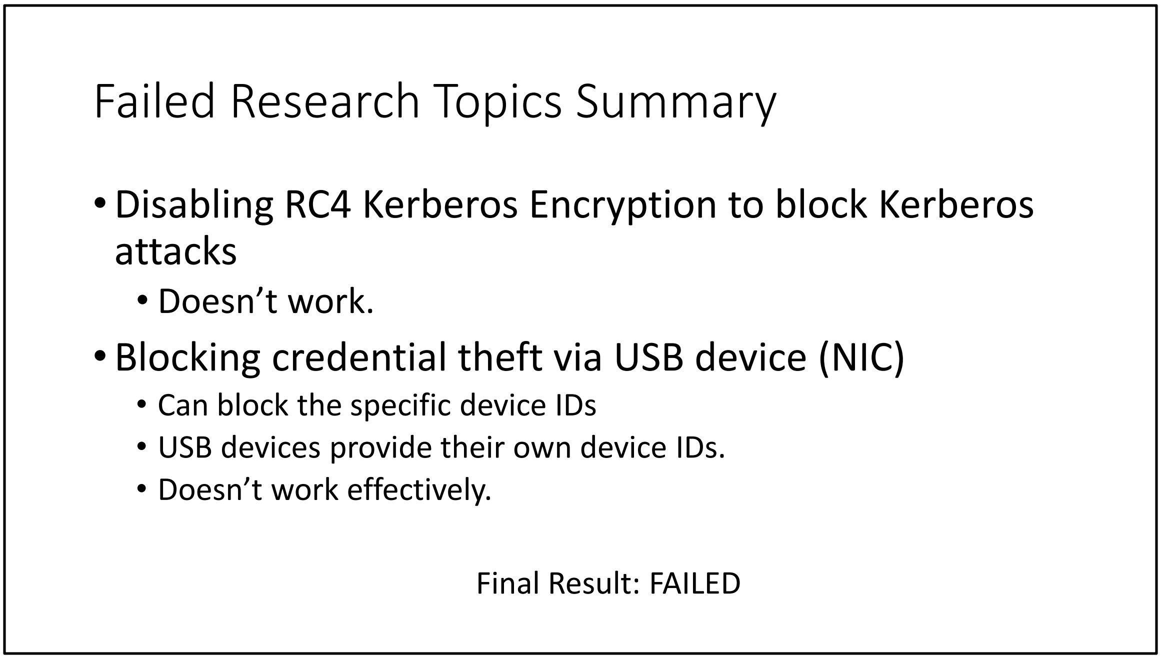
I wanted to test out some scenarios based on Rob "Mubix" Fuller's hack using a custom USB ethernet device (like a LAN Turtle or USB Armory) that acts as a DHCP server which provides itself as the WPAD server and runs responder. This combination of USB ethernet device + DHCP + WPAD + Responder provides the ability for an attacker to plug in a USB device into a computer which is locked and still gain credentials for the logged on user.

Mubix describes the situation as follows:

Why does this work?

- Because USB is Plug-and-Play. This means that even if a system is locked out, the device still gets installed. Now, I believe there are restrictions on what types of devices are allowed to install at a locked out state on newer operating systems (Win10/El Capitan), but Ethernet/LAN is definitely on the white list

I even started writing the background information in an ADSecurity.org blog post that I was unable to publish since I was wrong.
It didn't work out

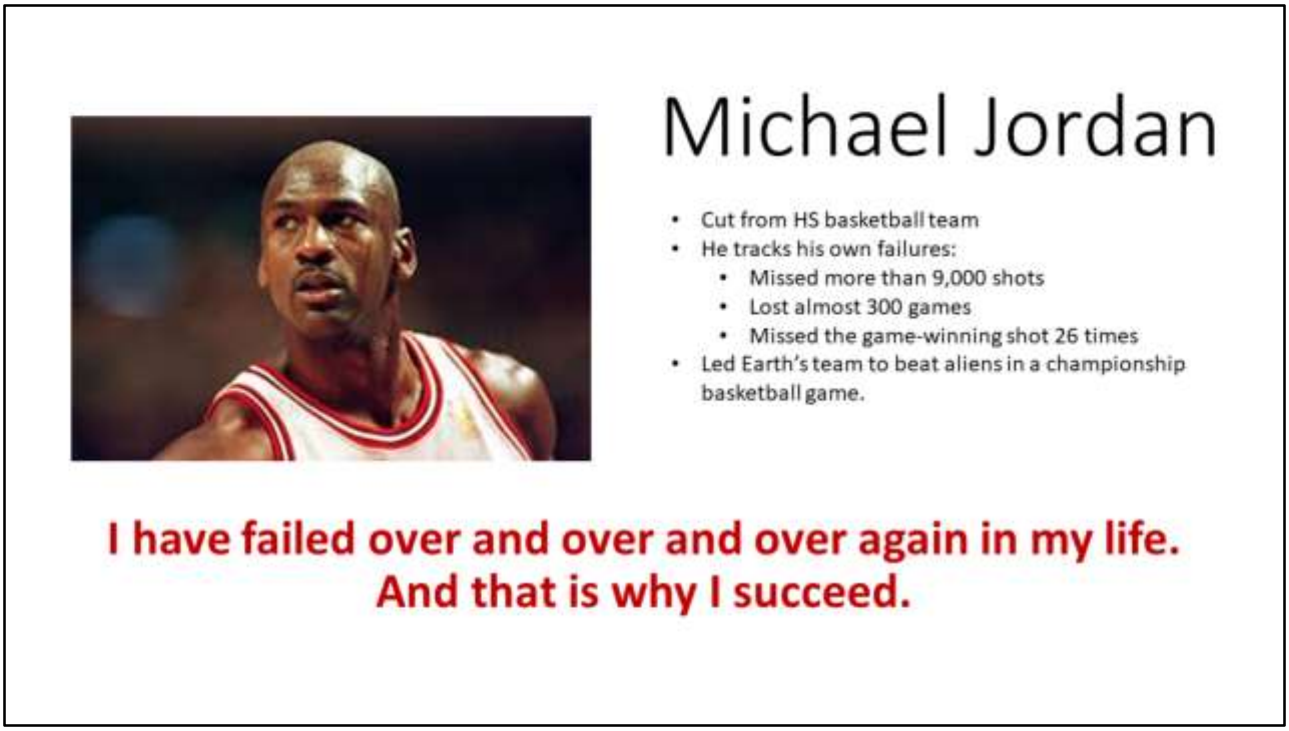


Failed Research Topics Summary

- Disabling RC4 Kerberos Encryption to block Kerberos attacks
  - Doesn’t work.
- Blocking credential theft via USB device (NIC)
  - Can block the specific device IDs
  - USB devices provide their own device IDs.
  - Doesn’t work effectively.

Final Result: FAILED

Received the MVP no more email while on vacation.

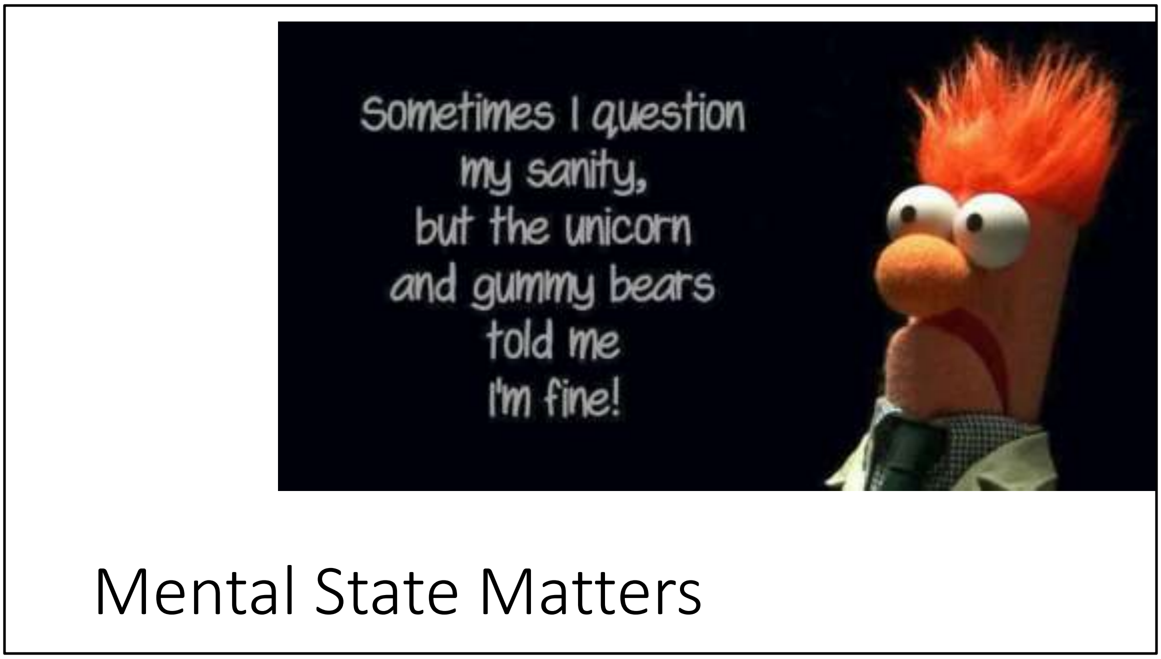


Michael Jordan

- Cut from HS basketball team
- He tracks his own failures:
  - Missed more than 9,000 shots
  - Lost almost 300 games
  - Missed the game-winning shot 26 times
- Led Earth's team to beat aliens in a championship basketball game.

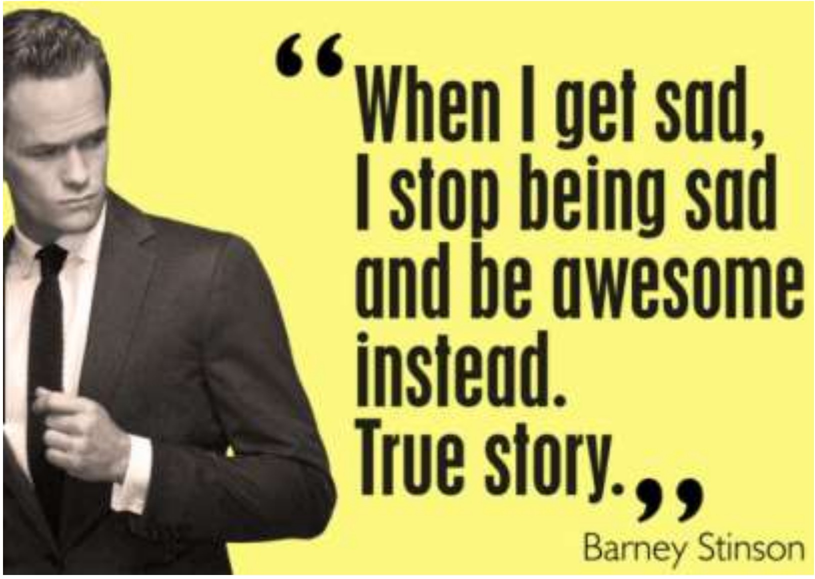
**I have failed over and over and over again in my life.
And that is why I succeed.**

Jordan was cut from his high school basketball team.
According to his own admission, he missed more than 9,000 shots, lost almost 300 games, and missed the game-winning shot 26 times.



Mental State Matters

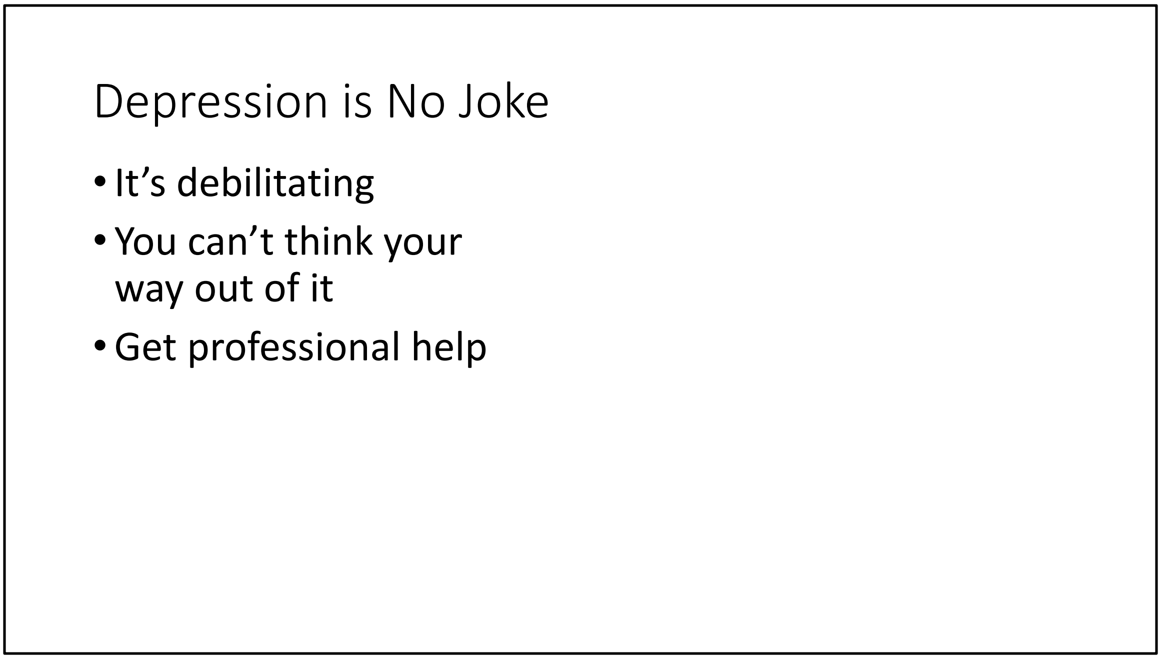
How you currently feel affects your motivation and ability.



“When I get sad, I stop being sad and be awesome instead. True story.”

Barney Stinson

Funny joke. Sometimes you are just sad and can move on.
Other times, someone may be depressed. You can’t just make a decision and move on from being depressed.



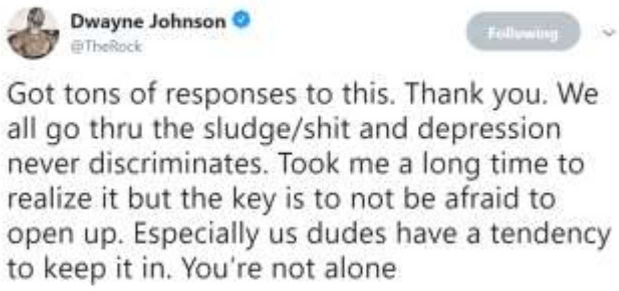
Depression is No Joke

- It’s debilitating
- You can’t think your way out of it
- Get professional help

If you are depressed, please talk to a professional and get help.

Depression is No Joke

- It’s debilitating
- You can’t think your way out of it
- Get professional help



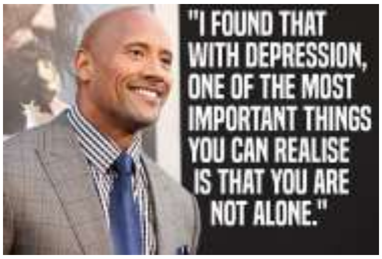
Dwayne Johnson
@TheRock

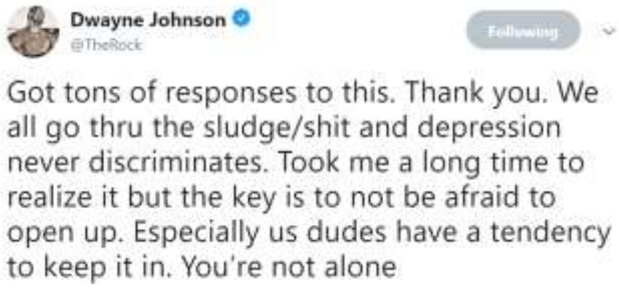
Got tons of responses to this. Thank you. We all go thru the sludge/shit and depression never discriminates. Took me a long time to realize it but the key is to not be afraid to open up. Especially us dudes have a tendency to keep it in. You're not alone

The Rock recently went to social media and discussed his struggle with depression over the years

Depression is No Joke

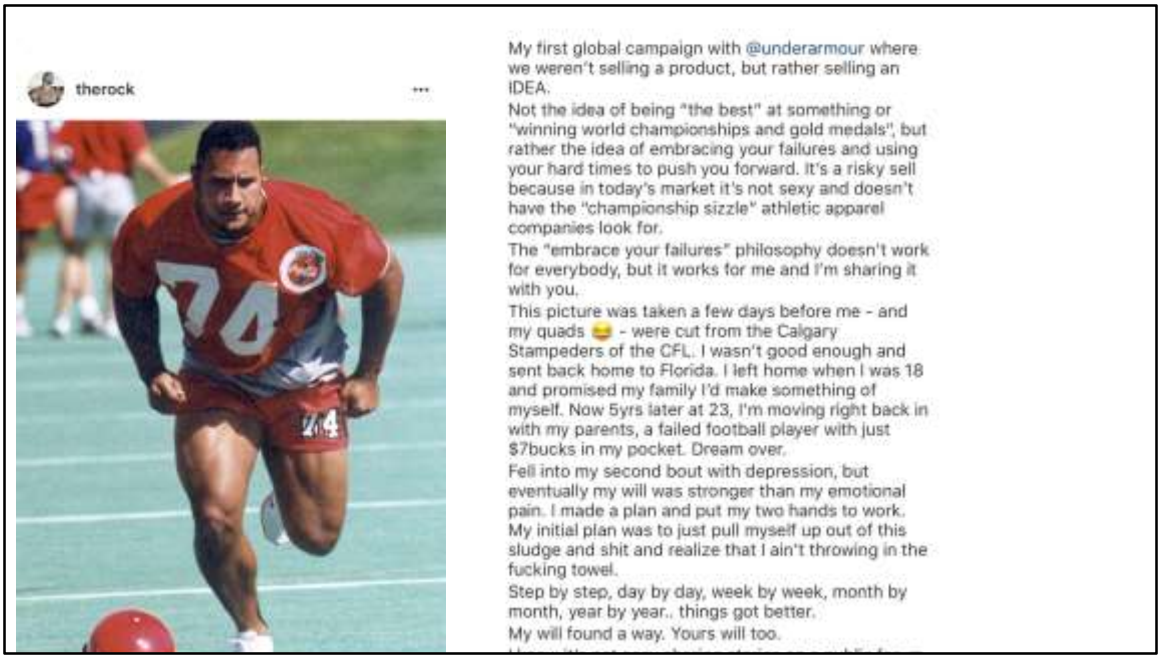
- It’s debilitating
- You can’t think your way out of it
- Get professional help


"I FOUND THAT WITH DEPRESSION, ONE OF THE MOST IMPORTANT THINGS YOU CAN REALISE IS THAT YOU ARE NOT ALONE."


Dwayne Johnson
@TheRock

Got tons of responses to this. Thank you. We all go thru the sludge/shit and depression never discriminates. Took me a long time to realize it but the key is to not be afraid to open up. Especially us dudes have a tendency to keep it in. You're not alone

You are not alone.



therock

My first global campaign with @underarmour where we weren't selling a product, but rather selling an IDEA.

Not the idea of being "the best" at something or "winning world championships and gold medals", but rather the idea of embracing your failures and using your hard times to push you forward. It's a risky sell because in today's market it's not sexy and doesn't have the "championship sizzle" athletic apparel companies look for.

The "embrace your failures" philosophy doesn't work for everybody, but it works for me and I'm sharing it with you.

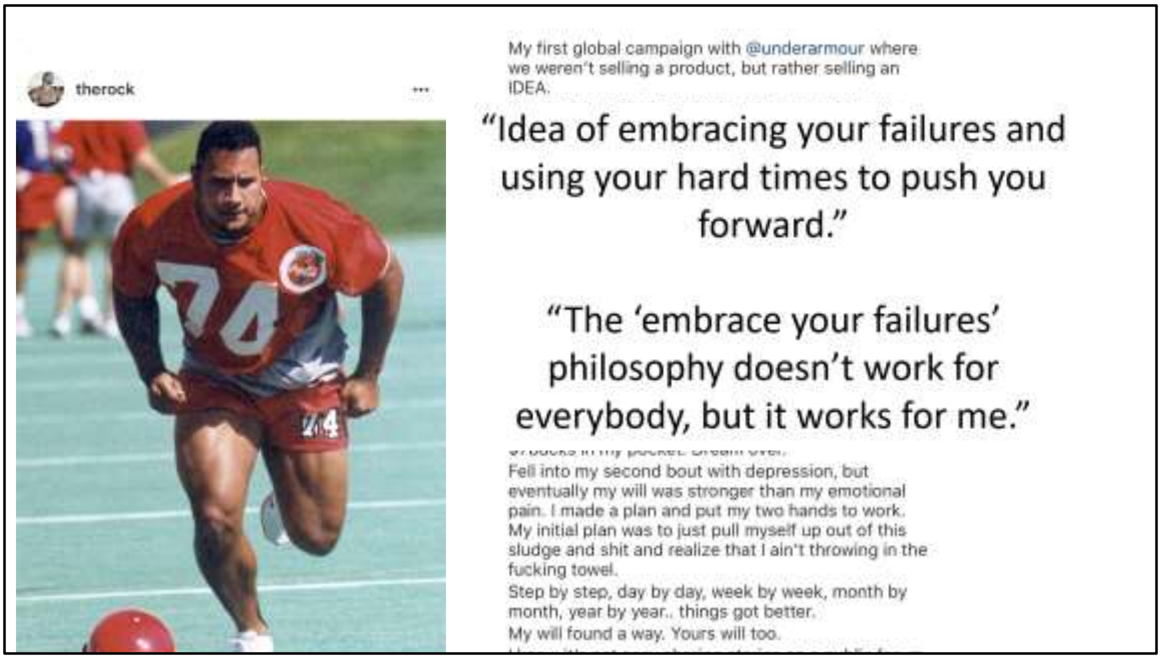
This picture was taken a few days before me - and my quads 😂 - were cut from the Calgary Stampeders of the CFL. I wasn't good enough and sent back home to Florida. I left home when I was 18 and promised my family I'd make something of myself. Now 5yrs later at 23, I'm moving right back in with my parents, a failed football player with just $7bucks in my pocket. Dream over.

Fell into my second bout with depression, but eventually my will was stronger than my emotional pain. I made a plan and put my two hands to work. My initial plan was to just pull myself up out of this sludge and shit and realize that I ain't throwing in the fucking towel.

Step by step, day by day, week by week, month by month, year by year.. things got better.

My will found a way. Yours will too.

"Idea of embracing your failures and using your hard times to push you forward."
"The 'embrace your failures' philosophy doesn't work for everybody, but it works for me."
Cut by the Calgary Stampeders (CFL) at 23 years old with $7 in his pocket.



My first global campaign with @underarmour where we weren't selling a product, but rather selling an IDEA.

“Idea of embracing your failures and using your hard times to push you forward.”

“The ‘embrace your failures’ philosophy doesn’t work for everybody, but it works for me.”

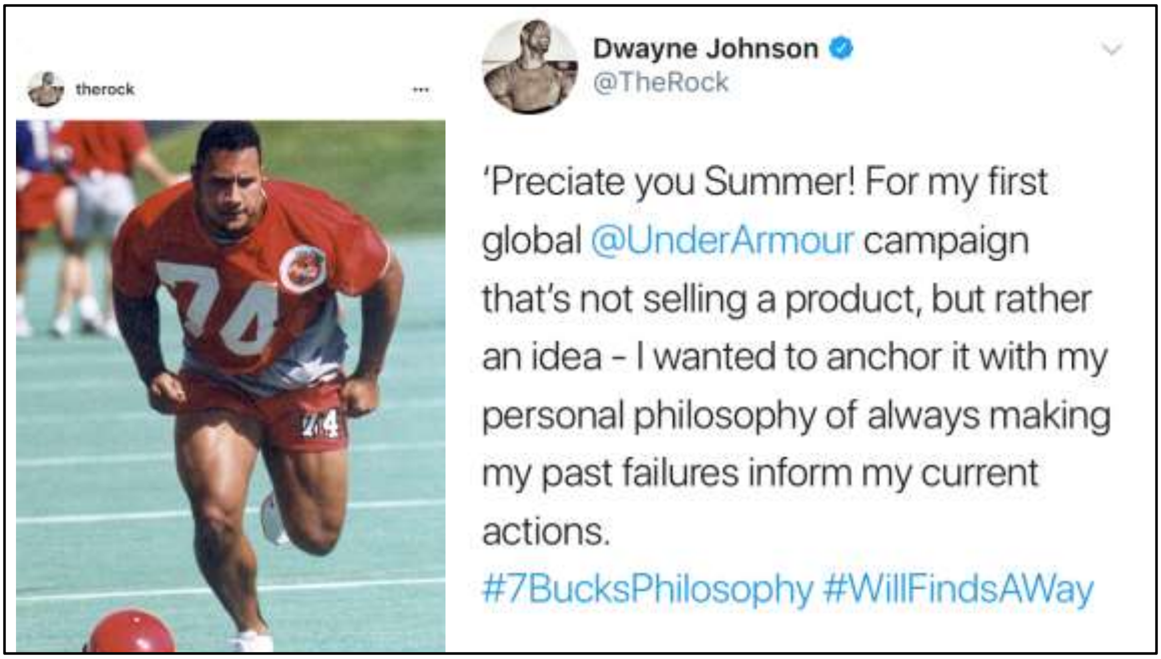
$7 bucks in my pocket. Dream over.

Fell into my second bout with depression, but eventually my will was stronger than my emotional pain. I made a plan and put my two hands to work. My initial plan was to just pull myself up out of this sludge and shit and realize that I ain't throwing in the fucking towel.

Step by step, day by day, week by week, month by month, year by year.. things got better.

My will found a way. Yours will too.

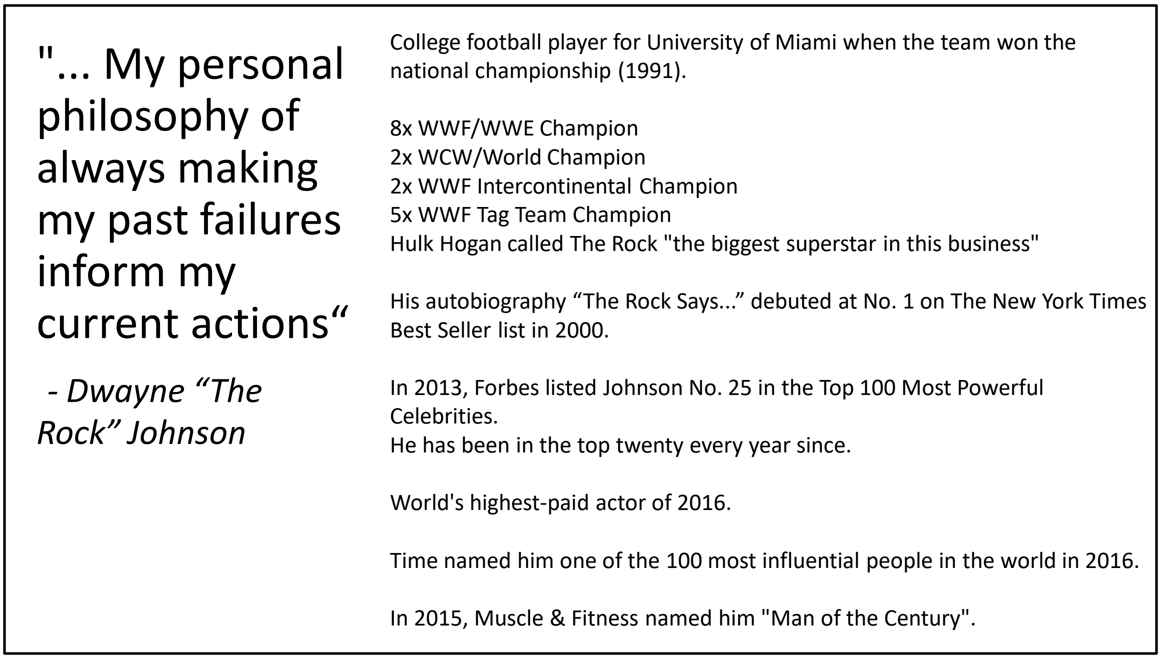
“Idea of embracing your failures and using your hard times to push you forward.”
“The ‘embrace your failures’ philosophy doesn’t work for everybody, but it works for me.”
Cut by the Calgary Stampeders (CFL) at 23 years old with $7 in his pocket.



Dwayne Johnson
@TheRock

'Preciate you Summer! For my first global @UnderArmour campaign that's not selling a product, but rather an idea - I wanted to anchor it with my personal philosophy of always making my past failures inform my current actions.
#7BucksPhilosophy #WillFindsAWay

The Rock helped me write a good part of this slide deck! ☺



"... My personal philosophy of always making my past failures inform my current actions“

- Dwayne “The Rock” Johnson

College football player for University of Miami when the team won the national championship (1991).

8x WWF/WWE Champion
2x WCW/World Champion
2x WWF Intercontinental Champion
5x WWF Tag Team Champion
Hulk Hogan called The Rock "the biggest superstar in this business"

His autobiography “The Rock Says...” debuted at No. 1 on The New York Times Best Seller list in 2000.

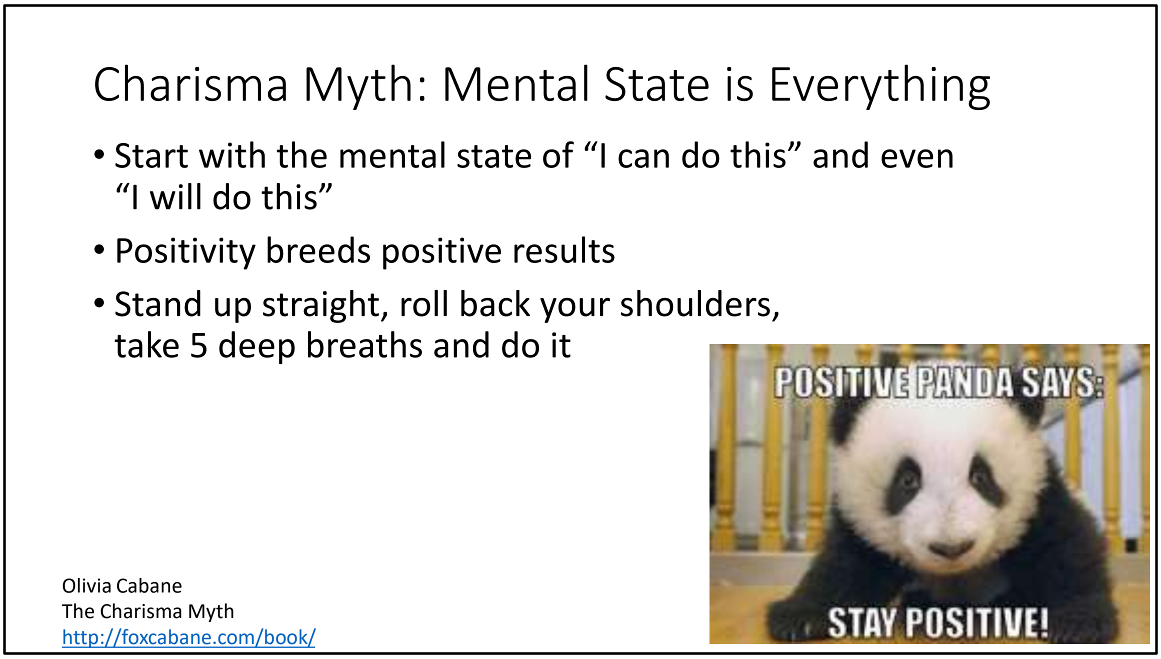
In 2013, Forbes listed Johnson No. 25 in the Top 100 Most Powerful Celebrities.
He has been in the top twenty every year since.

World's highest-paid actor of 2016.

Time named him one of the 100 most influential people in the world in 2016.

In 2015, Muscle & Fitness named him "Man of the Century".

Despite failing at 23 and struggling with depression, Dwayne Johnson has been one of the most successful entertainers in recent years.



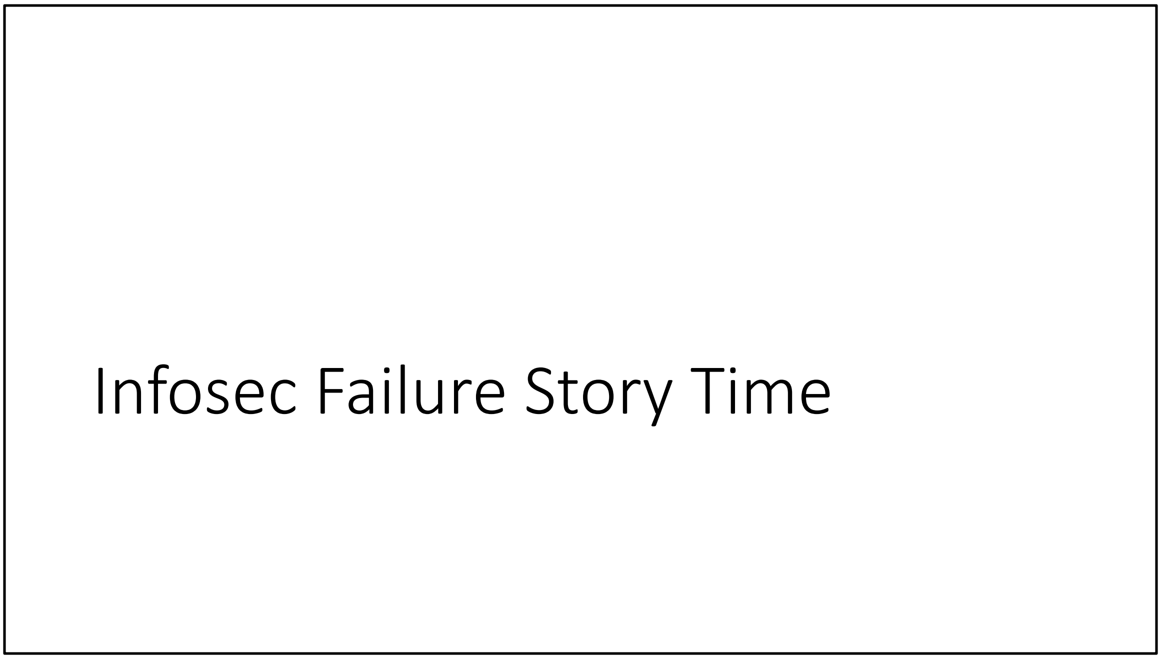
Charisma Myth: Mental State is Everything

- Start with the mental state of “I can do this” and even “I will do this”
- Positivity breeds positive results
- Stand up straight, roll back your shoulders, take 5 deep breaths and do it

POSITIVE PANDA SAYS:
STAY POSITIVE!

Olivia Cabane
The Charisma Myth
http://foxcabane.com/book/

Stay positive and think positive. It does matter.
“The Charisma Myth” by Olivia Cabane

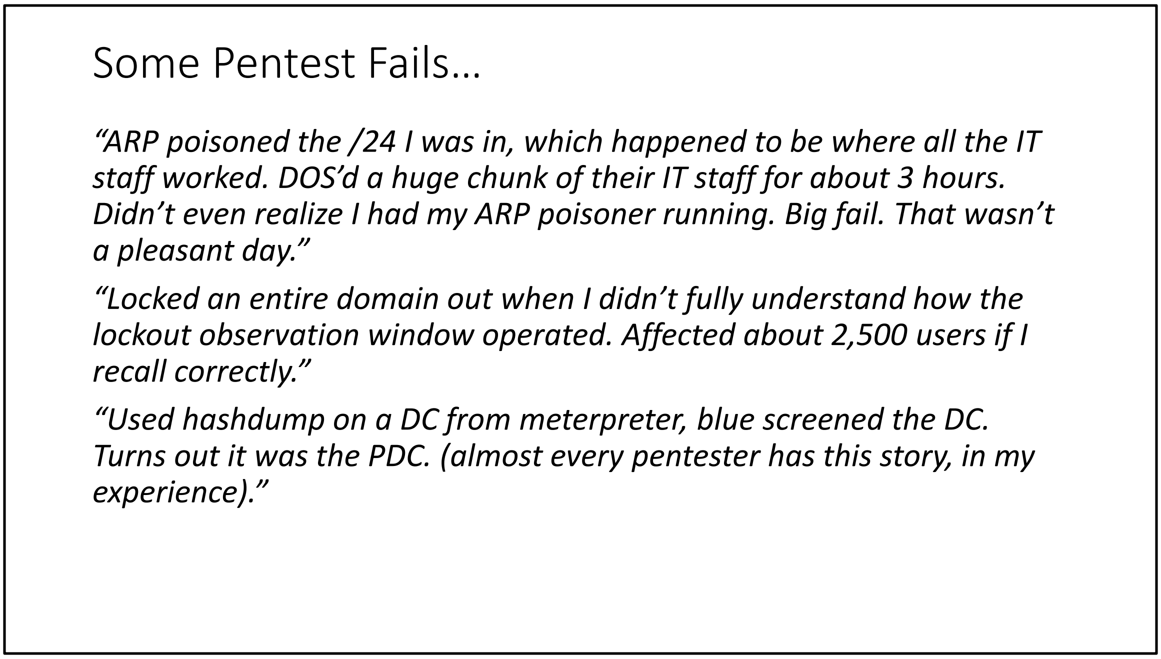


Infosec Failure Story Time

Others in the community shared their failures with me

> *“Years ago I wrote my first Snort signature. Probably my 10th Snort sig was looking for content “powershell”…that’s it. any port, any protocol, etc. for all our network devices in the world.*
>
> *I nearly brought down our backend for processing these hits (about half a million hits in 15 minutes). Got some new QA processes set up just for me.*
>
> *BUT it opened my eyes to a completely different way of looking for host-based indicators over the wire. I went on to write nearly 150 Snort sigs over the next several months based entirely on this discovery.“*

Others in the community shared their failures with me



Some Pentest Fails…

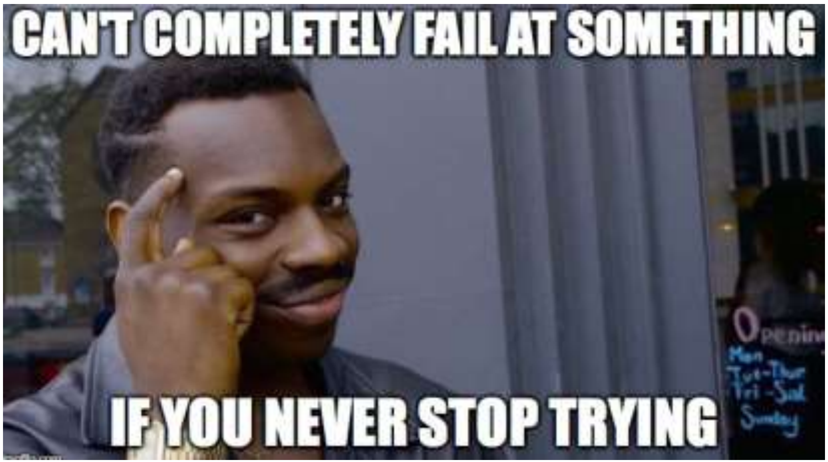
"ARP poisoned the /24 I was in, which happened to be where all the IT staff worked. DOS'd a huge chunk of their IT staff for about 3 hours. Didn't even realize I had my ARP poisoner running. Big fail. That wasn't a pleasant day."

"Locked an entire domain out when I didn't fully understand how the lockout observation window operated. Affected about 2,500 users if I recall correctly."

"Used hashdump on a DC from meterpreter, blue screened the DC. Turns out it was the PDC. (almost every pentester has this story, in my experience)."

Others in the community shared their failures with me

In conclusion…

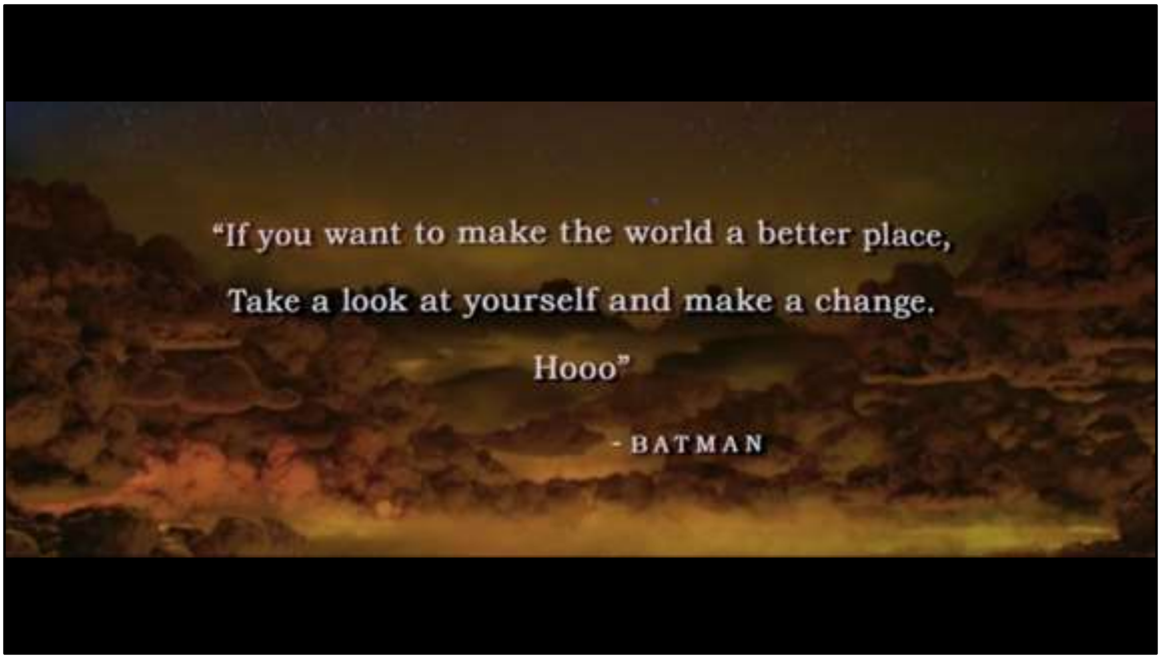


"If you want to make the world a better place,

Take a look at yourself and make a change.

Hooo"

- MICHAEL JACKSON



"If you want to make the world a better place,
Take a look at yourself and make a change.
Hooo"

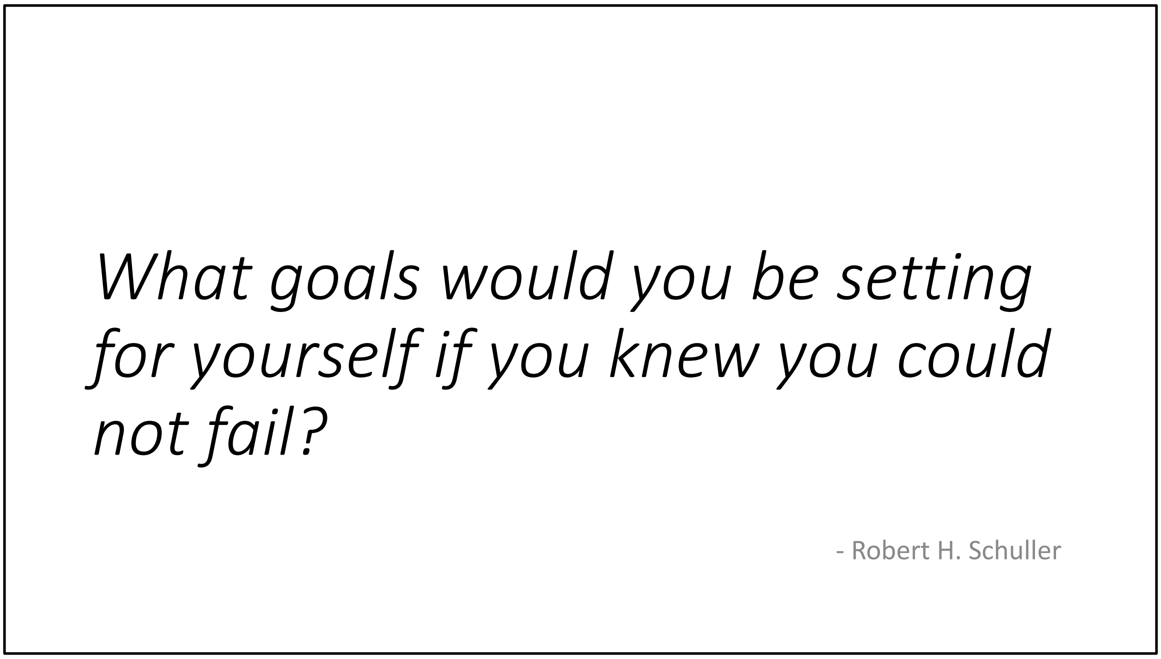
- BATMAN

“Never believe anyone who doesn't believe in you. *This is especially true of those who are closest to you. They are wrong. They will always be wrong about you & they don't deserve to be in the presence of your splendor, dragging you down.* ***Reject their reality & substitute your own.***

Give everything you have to whatever you set your mind to. *The only voice that actually has power over your actions is your own. Create your path. It will be treacherous at times, but in the end - it will be paved with your own power.*

You can punch through any obstacle if you have to. ***You can climb the unclimbable. When you look back, you'll reflect on how well you accepted the opportunities in front of you and acted upon them."***

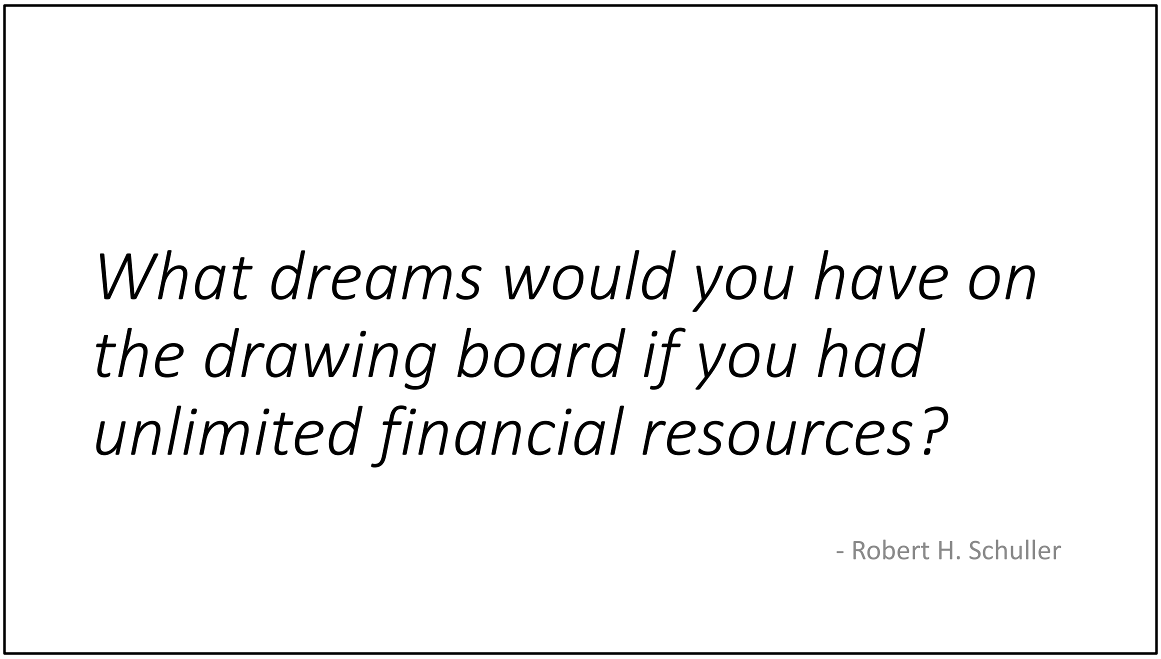
- Katie Moussouris



What goals would you be setting for yourself if you knew you could not fail?

- Robert H. Schuller

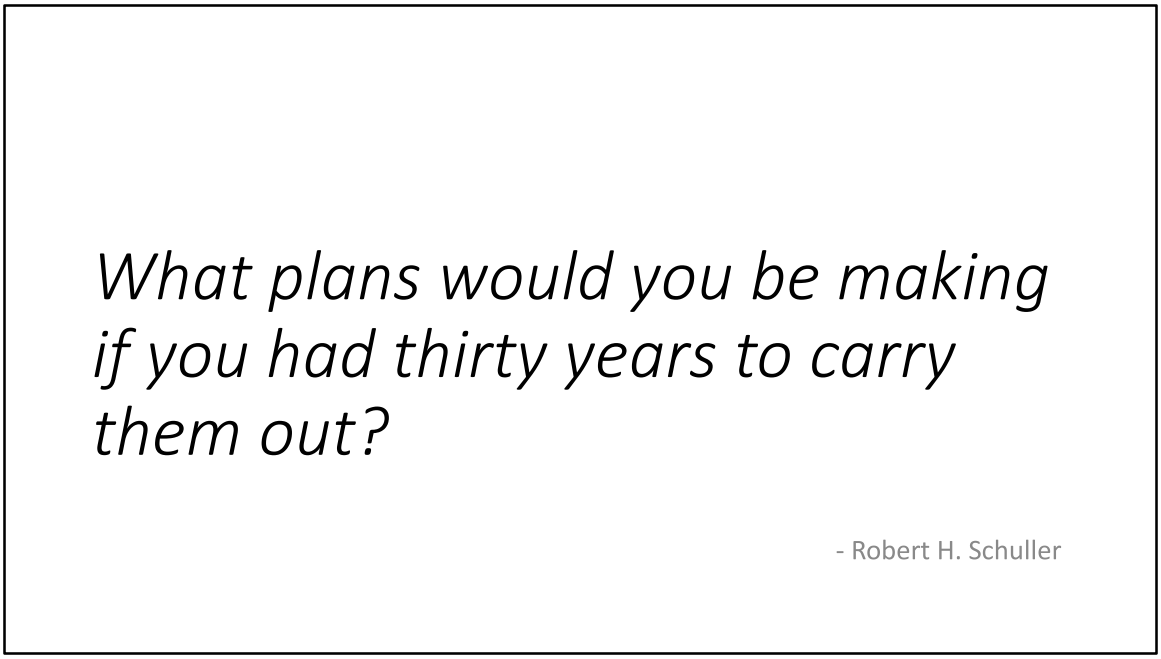
This removes failure from the equation to help you get over this fear



What dreams would you have on the drawing board if you had unlimited financial resources?

- Robert H. Schuller

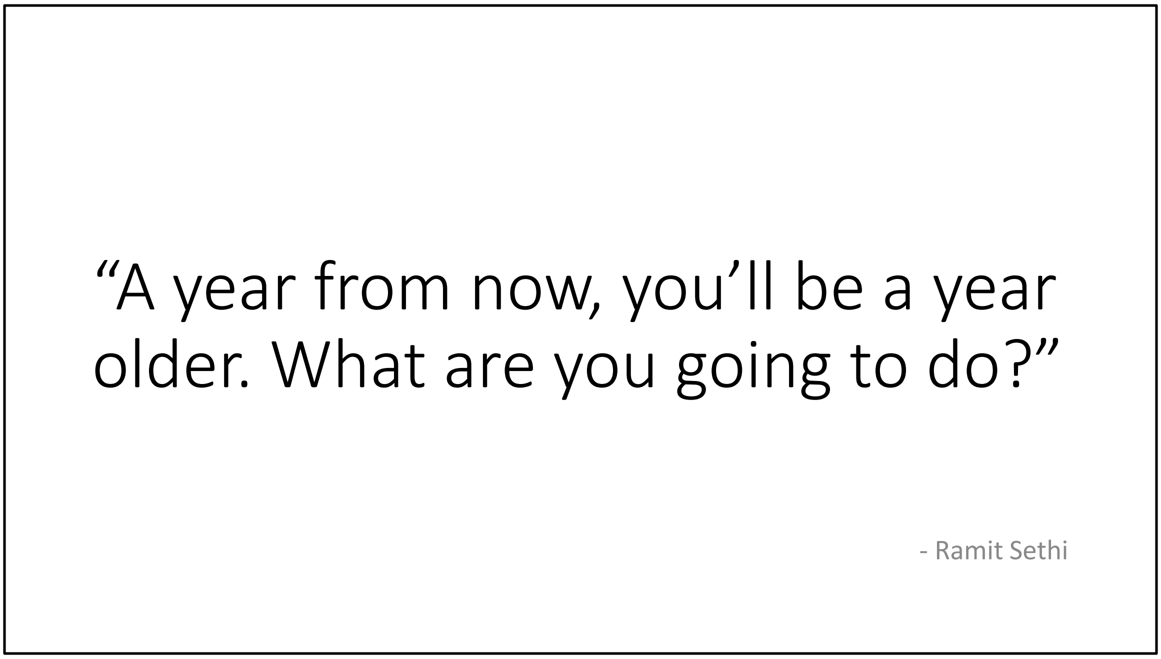
This removes money from the equation to help you get over this fear



What plans would you be making if you had thirty years to carry them out?

- Robert H. Schuller

This removes time from the equation to help you get over this fear.
You aren’t too old or two young. Just do it!



“A year from now, you’ll be a year older. What are you going to do?”

- Ramit Sethi

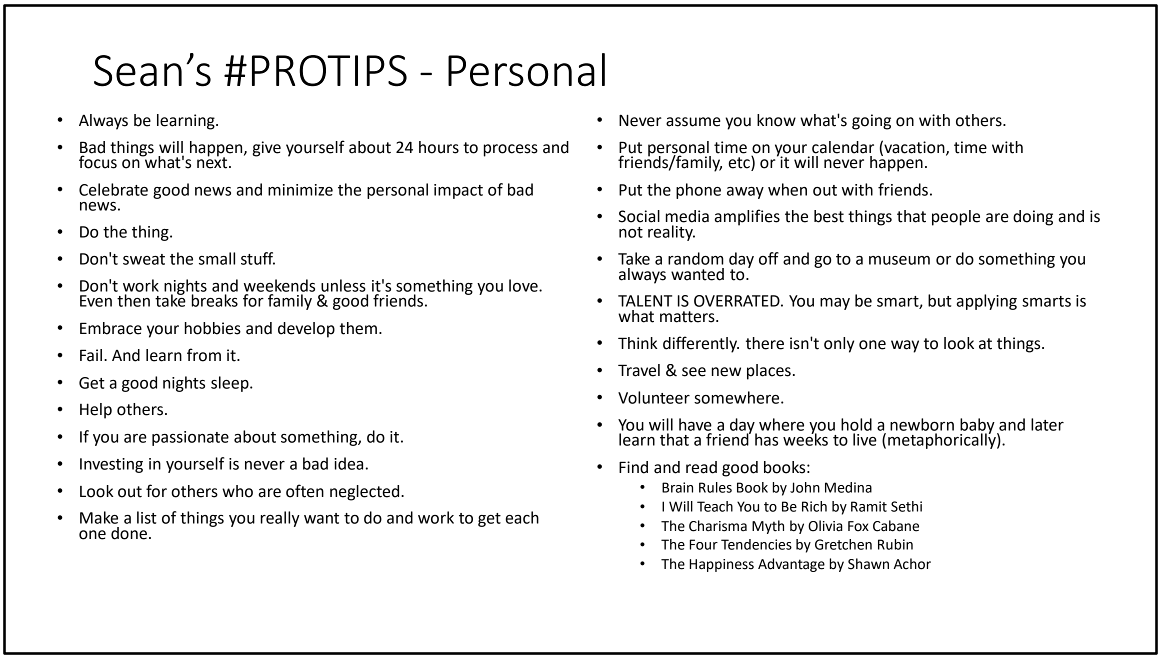
My favorite quote and the one that I focus on throughout the year.
This will by MY year to do ___________________

THANK YOU!

Fail Time

Presentations.ADSecurity.org

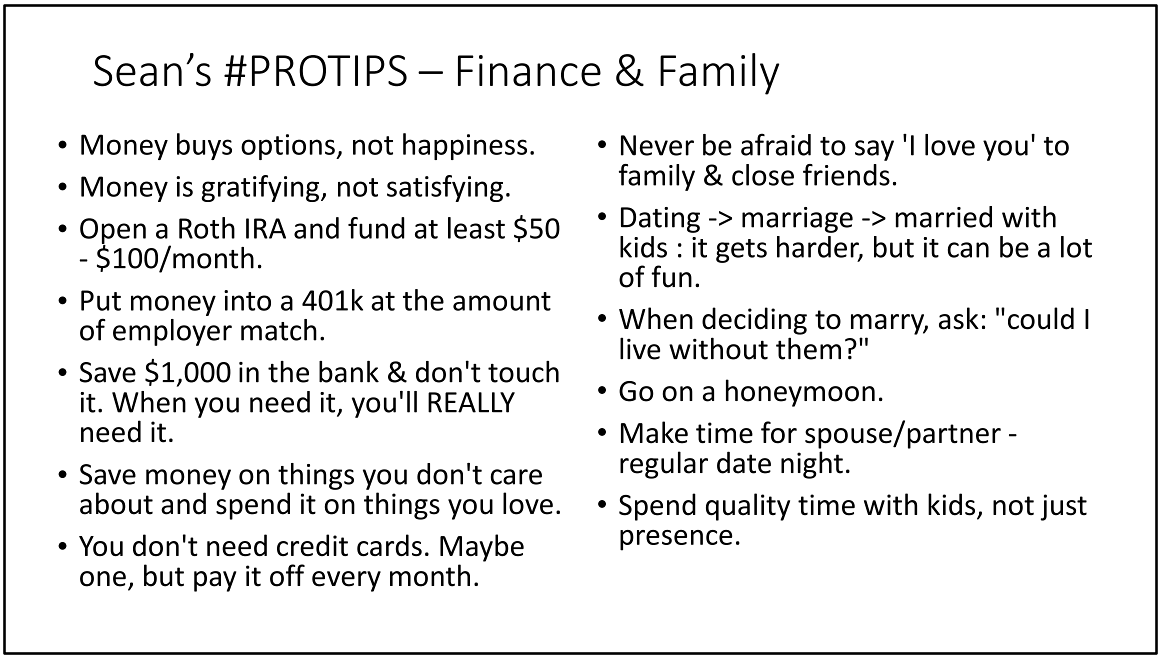
Sean Metcalf (@Pyrotek3)
sean [@] TrimarcSecurity.com
www.ADSecurity.org
TrimarcSecurity.com



Sean’s #PROTIPS - Personal

- Always be learning.
- Bad things will happen, give yourself about 24 hours to process and focus on what's next.
- Celebrate good news and minimize the personal impact of bad news.
- Do the thing.
- Don't sweat the small stuff.
- Don't work nights and weekends unless it's something you love. Even then take breaks for family & good friends.
- Embrace your hobbies and develop them.
- Fail. And learn from it.
- Get a good nights sleep.
- Help others.
- If you are passionate about something, do it.
- Investing in yourself is never a bad idea.
- Look out for others who are often neglected.
- Make a list of things you really want to do and work to get each one done.
- Never assume you know what's going on with others.
- Put personal time on your calendar (vacation, time with friends/family, etc) or it will never happen.
- Put the phone away when out with friends.
- Social media amplifies the best things that people are doing and is not reality.
- Take a random day off and go to a museum or do something you always wanted to.
- TALENT IS OVERRATED. You may be smart, but applying smarts is what matters.
- Think differently. there isn't only one way to look at things.
- Travel & see new places.
- Volunteer somewhere.
- You will have a day where you hold a newborn baby and later learn that a friend has weeks to live (metaphorically).
- Find and read good books:
  - Brain Rules Book by John Medina
  - I Will Teach You to Be Rich by Ramit Sethi
  - The Charisma Myth by Olivia Fox Cabane
  - The Four Tendencies by Gretchen Rubin
  - The Happiness Advantage by Shawn Achor

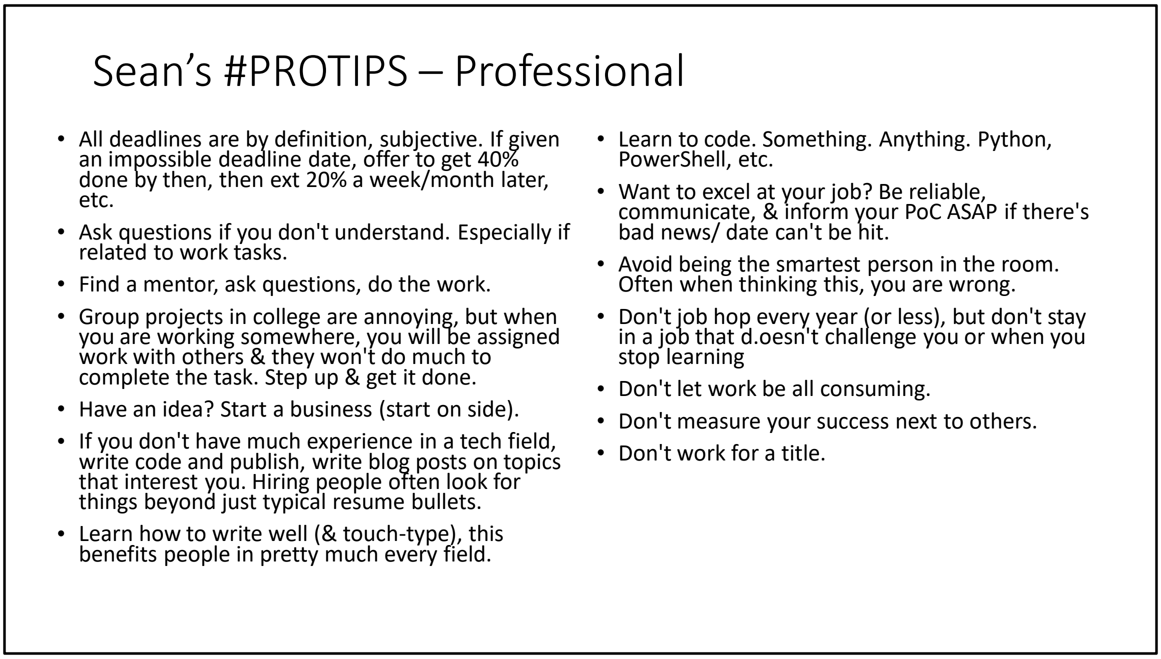
These are from a Tweet thread I wrote a month or so ago.



Sean’s #PROTIPS – Finance & Family

- Money buys options, not happiness.
- Money is gratifying, not satisfying.
- Open a Roth IRA and fund at least $50 - $100/month.
- Put money into a 401k at the amount of employer match.
- Save $1,000 in the bank & don't touch it. When you need it, you'll REALLY need it.
- Save money on things you don't care about and spend it on things you love.
- You don't need credit cards. Maybe one, but pay it off every month.
- Never be afraid to say 'I love you' to family & close friends.
- Dating -> marriage -> married with kids : it gets harder, but it can be a lot of fun.
- When deciding to marry, ask: "could I live without them?"
- Go on a honeymoon.
- Make time for spouse/partner - regular date night.
- Spend quality time with kids, not just presence.

These are from a Tweet thread I wrote a month or so ago.



Sean’s #PROTIPS – Professional

- All deadlines are by definition, subjective. If given an impossible deadline date, offer to get 40% done by then, then ext 20% a week/month later, etc.
- Ask questions if you don't understand. Especially if related to work tasks.
- Find a mentor, ask questions, do the work.
- Group projects in college are annoying, but when you are working somewhere, you will be assigned work with others & they won't do much to complete the task. Step up & get it done.
- Have an idea? Start a business (start on side).
- If you don't have much experience in a tech field, write code and publish, write blog posts on topics that interest you. Hiring people often look for things beyond just typical resume bullets.
- Learn how to write well (& touch-type), this benefits people in pretty much every field.
- Learn to code. Something. Anything. Python, PowerShell, etc.
- Want to excel at your job? Be reliable, communicate, & inform your PoC ASAP if there's bad news/ date can't be hit.
- Avoid being the smartest person in the room. Often when thinking this, you are wrong.
- Don't job hop every year (or less), but don't stay in a job that d.oesn't challenge you or when you stop learning
- Don't let work be all consuming.
- Don't measure your success next to others.
- Don't work for a title.

These are from a Tweet thread I wrote a month or so ago.