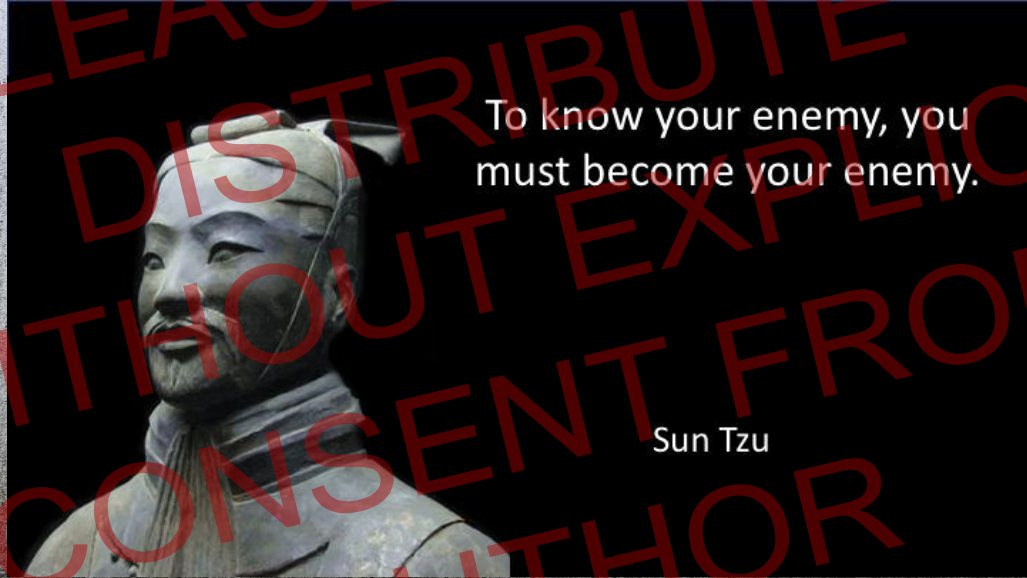


DIY APTs for your protection



To know your enemy, you
must become your enemy.

Sun Tzu

Roei Sherman

♠ Red Team @  - We do Cybe(e)r.....

♠ Co-organizer @ 

♠ OSCP, GPEN, GXPN, CCSK – SANS Advisory Board



<https://bettheadversary.com>



x_Freed0m



<https://github.com/xFreed0m>

Missing logs

- Password spraying was performed
- We know how
- WE DON'T KNOW WHO DID IT





Event Properties - Event 4625, Microsoft Windows security auditing.

General Details

An account failed to log on.

Subject:

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

Logon Type: 3

Account For Which Logon Failed:

Security ID: NULL SID
Account Name: test5
Account Domain: mutiny

Failure Information:

Failure Reason: Unknown user name or bad password.
Status: 0xC000006D
Sub Status: 0xC000006A

Process Information:

Caller Process ID: 0x0
Caller Process Name: -

Network Information:

Workstation Name: testhostname1
Source Network Address: -
Source Port: -

PLEASE DO NOT
DISTRIBUTE
WITHOUT EXPLICIT
CONSENT FROM
AUTHOR

Well I caught it



Now what?

PLEASE DO NOT
DISTRIBUTE
WITHOUT EXPLICIT
CONSENT FROM
AUTHOR

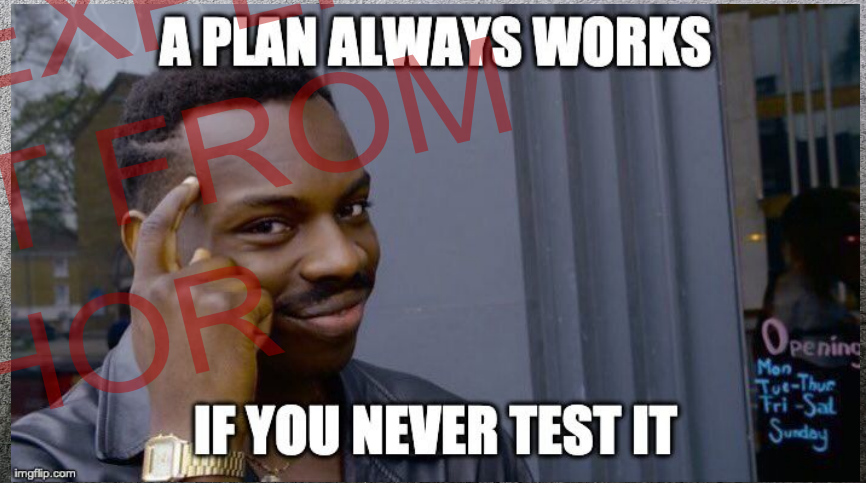
Most of us...

- Invest a lot of money in products
 - Prevention, detection
- Never really know what is working properly
- Always face new attacks

PLEASE DO NOT
DISTRIBUTE
WITHOUT EXPLICIT
CONSENT FROM
AUTHOR

Do we really need the attackers?

- Adversaries aren't planning to stop
- You won't understand the enemy without being the enemy
- Plans always work - until reality kicks in



Why consulting isn't enough

- Engagements are time framed
- External consultants aren't familiar with our roadblocks
- Consultants change often

Can defenders assess themselves?

- They know what they are after
- They know their systems
- They are THE owners to implement improvements



In-sourcing the detection coverage

- Depend on ourselves
- Test using real attacks tools
- Fast, tailormade, automated

Meet Caldera

- By MITRE
- Widely adopted - The new standard* for defense mapping
- Constantly updated matrix of TTPs

*Not official standard

Intended use cases

- Mapping organization detection
- Automate attacks*
- And everything else that you would decide

*Automation for the actions, doesn't substitute pentest.

No one-size in threats - need to DIY

- Based on our feeds - create our own adversaries
- Want to check a product we are using
- Reply attacks against our detection

Hands-on demo (standard adversary & custom adversary)

Welcome to Disruption (dedicated branch) -

[xFreed0m/Disruption: Terraform script to deploy AD-based environment on Azure](#)

