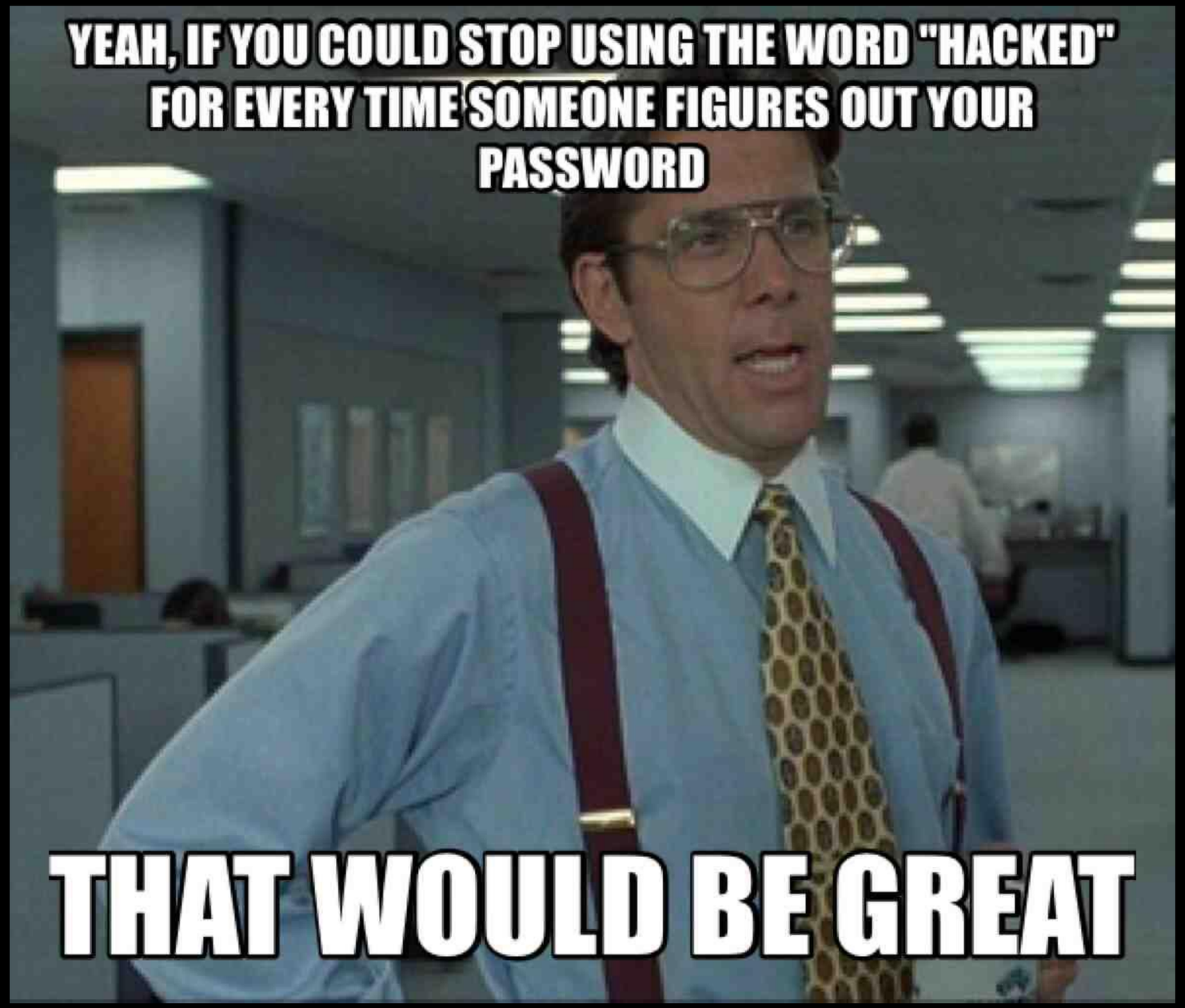
ASSUMED BREACH:
A BETTER MODEL FOR PEN TESTING

Mike Saunders
mike@redsiege.com
slides: redsiege.com/abm

ABOUT MIKE

- Principal Consultant, Red Siege
- > 20 years IT, 12 security
- Speaker
  - DerbyCon
  - BSides MSP / KC / Winnipeg
  - Wild West Hackin’ Fest
- Kayaking, fishing, musician


YEAH, IF YOU COULD STOP USING THE WORD "HACKED"
FOR EVERY TIME SOMEONE FIGURES OUT YOUR
PASSWORD
THAT WOULD BE GREAT

TWO MODELS FOR ASSUMED BREACH

- Compromised User
- Malicious Insider
- Both use standard workstation image with representative user
  - Preferably a recently terminated user account
- DA is a tool, not a destination!

MODEL – COMPROMISED USER

- Simulating a user who clicked on payload
- Execute a custom payload
- All ops take place over C2 framework
  - Pivot to remote access with credentials

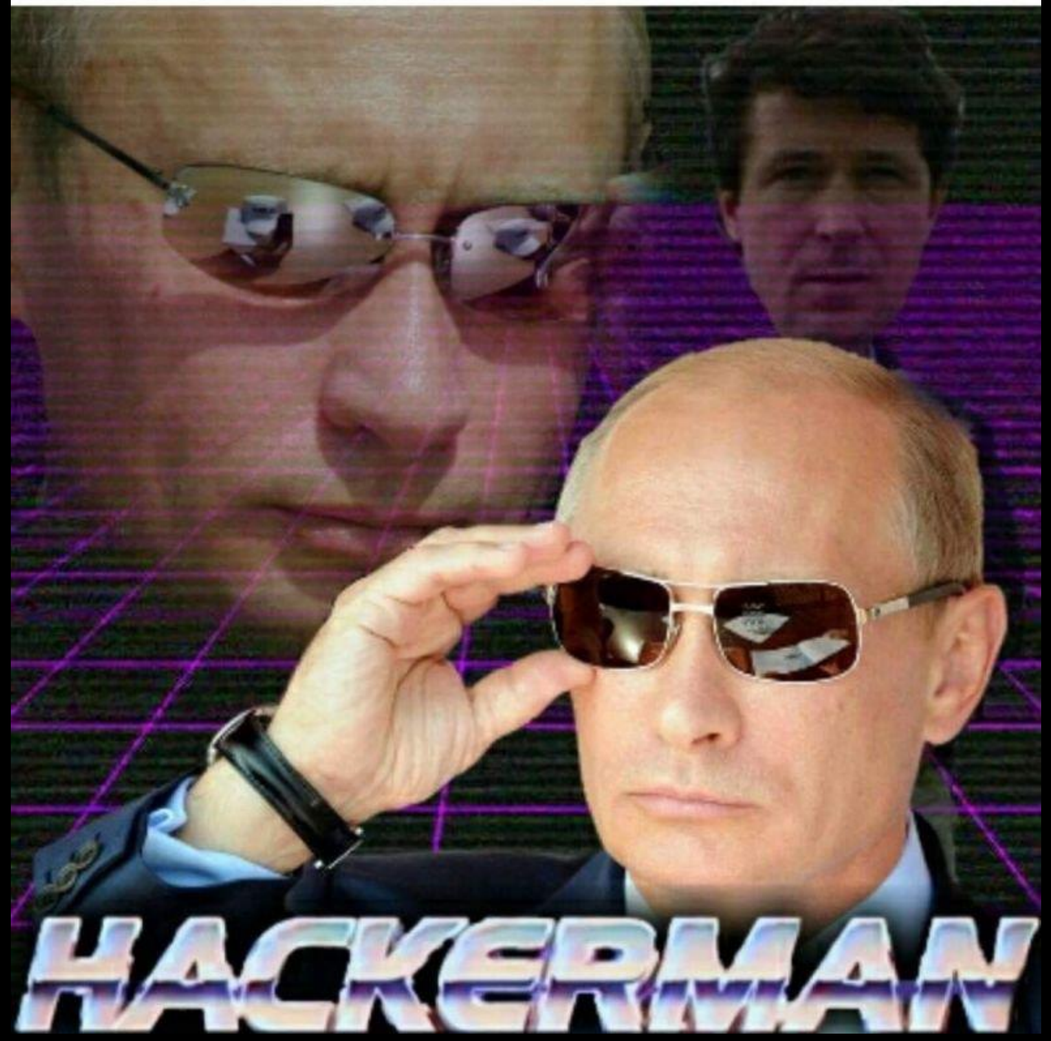
AV/EDR - DISABLE OR NOT?

- AV / EDR can be bypassed given time
- Is it worth client $$$ to spend time to bypass
- Discuss goals with client

MODEL – MALICIOUS INSIDER

- Simulates user who wants to steal / cause harm
- Test on-site or remotely through VPN to user workstation
- Testing starts with what tooling is available on workstation or can be loaded
- Standard AV / EDR configuration

When you put 'password' in the password field and it works.



REDSIEGE

REAL-WORLD TACTICS

- https://www.fireeye.com/blog/threat-research/2019/04/finding-weaknesses-before-the-attackers-do.html
- Blog lays out a likely real-world attack scenario
  - Phishing
  - Pivot internal through remote access
  - Targeted Kerberoasting => elevation of privilege
  - Access high-value targets

ASSUMED BREACH TACTICS

- Simulate payload sent via email / phishing / SE
- Search out high value targets / data
  - Kerberoasting => elevation of privilege
  - Collect credentials
  - Pivot to data
  - Access high-value targets

DOMAIN FRONTING

- Use client's own domain to blend in
- Find other domains to blend in
  - Technology companies used by client
  - Other sites likely to be used by employees
- https://github.com/rvrsh3ll/FindFrontableDomains
  - CloudFront no longer works!
- Build custom C2 profile

INITIAL ACCESS - SIMULATING PHISHING

- HTA is still effective
  - https://github.com/trustedsec/unicorn
  - https://github.com/danielbohannon/Invoke-Obfuscation
  - https://github.com/samratashok/nishang/blob/master/Client/Out-HTA.ps1
  - https://github.com/nccgroup/demiguise

INITIAL ACCESS - SIMULATING PHISHING

- Macros
- ClickOnce Executables
  - https://blog.netspi.com/all-you-need-is-one-a-clickonce-love-story/

KERBEROASTING

- Traditional tools
  - PowerView
    - Invoke-Kerberoast
  - https://raw.githubusercontent.com/fullmetalcache/tools/master/autokerberoast_nomimi_stripped.ps1
    - Invoke-AutoKerberoast -Format hashcat

KERBEROASTING

- Ideally low & slow
  - Target users in specific groups (PowerView)
  - https://www.harmj0y.net/blog/powershell/kerberoasting-without-mimikatz/
    - Get-DomainUser -SPN
    - Get-DomainSPNTicket -SPN
- Random delay
- https://adsecurity.org/?p=230

REDSIEGE

FINDING ACCOUNTS

- Password spraying (Internal or External)
  - OWA / O365
    - https://github.com/dafthack/MailSniper
      - Search email after gaining access
  - Domain accounts
    - https://github.com/dafthack/DomainPasswordSpray

MINING AD

- SharpHound via execute-assembly
  - Remember –NoSaveCache option
  - Research stealth options

- Hunt for creds in AD schema with ADExplorer
  - ADExplorer.exe –snapshot "" ad.snap –noconnectprompt
  - https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer/

REDSIEGE

HUNTING GPP CREDS

- GPP = XML config files stored in SYSVOL
  - Used to store credentials for workstation Local Admin, mapping drives, etc.
  - https://adsecurity.org/?p=2288
- PowerSploit Get-GPPPassword
- PowerSploit PowerUp Get-CachedGPPPassword

LATERAL MOVEMENT

- Find lateral movement to admin access with PowerView
  - Test-AdminAccess -ComputerName
  - Get-DomainComputer | Test-AdminAccess

FILE/SHARE TRAWLING

- Elevated account credentials (DA / sa / etc.) frequently found in files
  - PowerShell PSReadLine Logs (ConsoleHost_history.txt)
  - Source code & sensitive data
- PowerView
  - Invoke-ShareFinder -CheckAccess
  - Find-InterestingDomainShareFile
  - Find-InterestingFile

SESSION HUNTING

- Find files that can be used for lateral movement
  - SSH private keys, RDP files, FileZilla / WinSCP saved passwords, etc.
- https://github.com/Arvanaghi/SessionGopher
  - Invoke-SessionGopher -Thorough (local system)
  - Invoke-SessionGopher -Target hostxyz -Thorough
  - Invoke-SessionGopher -AllDomain -Thorough

BYOPOWERSHELL

- Code can be executed in ISE even if PS scripts execution is disabled
- Build custom PS environment
  - https://github.com/fullmetalcache/PowerLine

PROS & CONS

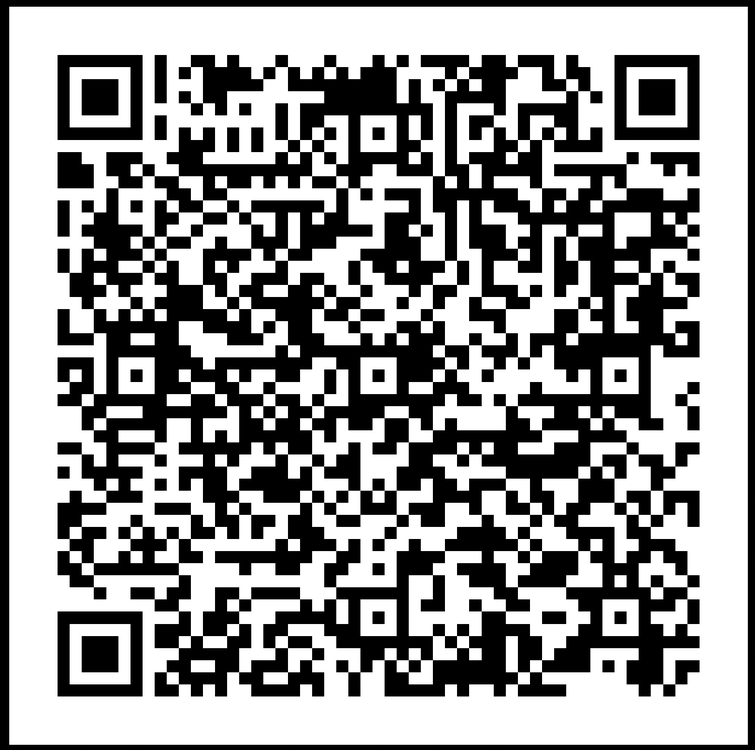
- Pro
  - Better understanding of strengths & weaknesses
  - Ability to model real-world TTPs

- Cons
  - Limited time = we have to be noisier
  - Not focused on vulnerabilities
  - Non-representative accounts or machines can negatively impact test

SUMMARY

- A better way to prepare clients for attacks they are likely to face
- Requires some maturity in client processes
  - VA & pen test cycles before client is ready
- Work with client to get good accounts & workstations
- Only showed PowerShell here, but it's not the only language

REDSIEGE



Mike Saunders
mike@redsiege.com
@hardwaterhacker
@RedSiegeInfoSec

redsiege.com/abm