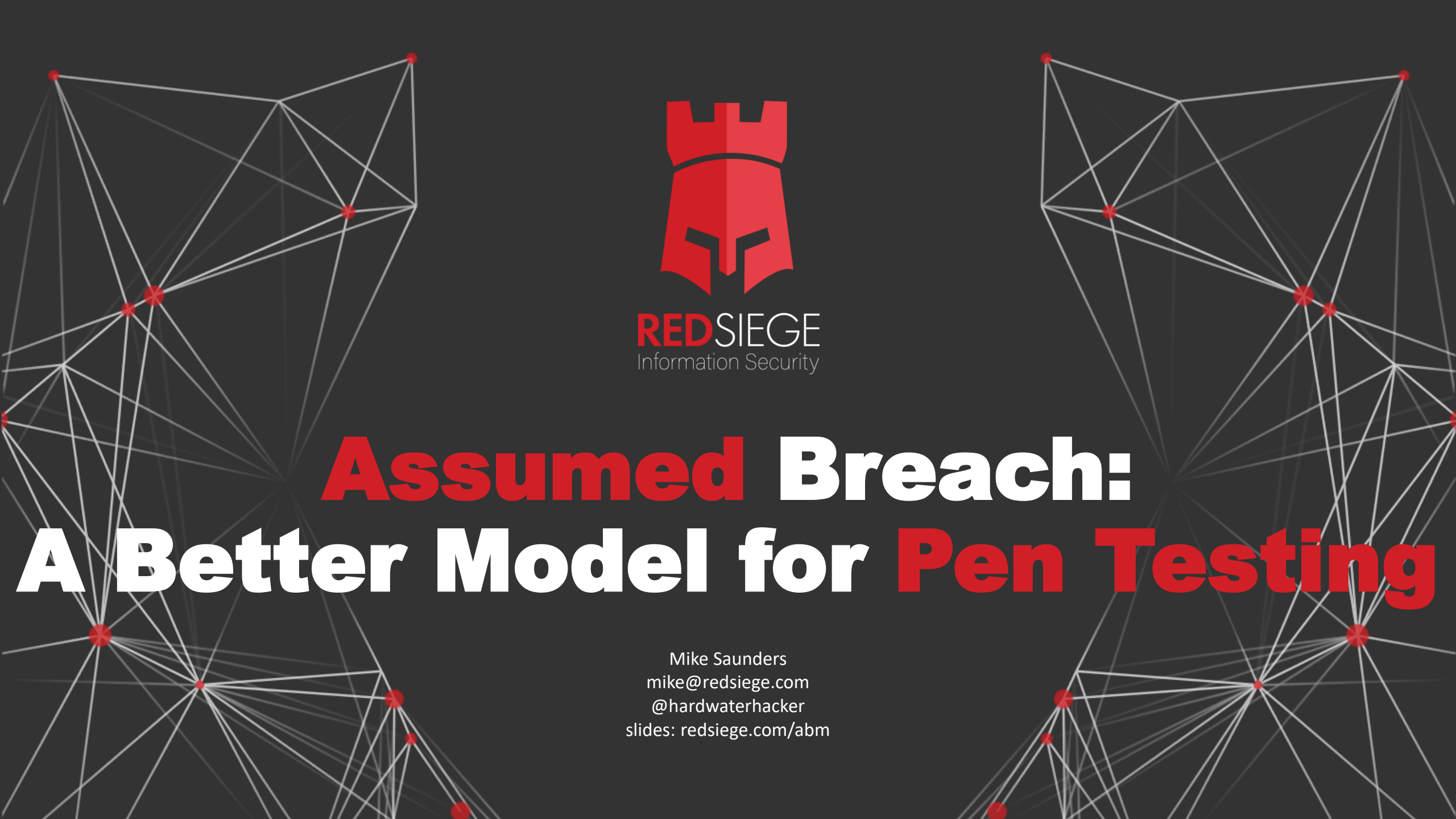

Assumed Breach: A Better Model for Pen Testing

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

ABOUT
Mike

Principal Consultant - Red Siege

> 20 years IT > 12 years security

kayaking / fishing / music / photography

Pen Testing is BROKEN

- Internal pen tests don't represent how attackers operate
  - Starting inside the network (kali or otherwise)
  - Noisy scans
  - Lobbing exploits everywhere

"I WANT A RED TEAM"

REDSIEGE

- Most customers don't need a true red team
  - Require a lot of time = expensive
  - Requires maturity in IT org.
    - Low return on investment compared to other test options

ASSUMED WHAT?

- Based on assumption endpoint is already compromised / org is breached
  - What can an attacker do with this access

AB - TWO(ish) MODELS

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

Compromised USER - PATH A

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

Compromised USER - PATH B

- Demonstrate impact of compromised user
- Operate on workstation
  - Shipped laptop / VPN + RDP / on site
- Work with tools available on desktop or what can be loaded
  - Initiate C2 if needed

AV/EDR - DISABLED?

- AV/EDR can be bypassed given time
- Is it worth client $$$ to spend time to bypass?
- Discuss goals with client
- @HackingLZ - Start with AV/EDR enabled, verify bypass or visibility of actions, then disable if needed

MALICIOUS USER

- Simulates employee who wants to steal / cause harm
- Shipped laptop / VPN + RDP / on site
- Testing starts on standard workstation
  - Whatever tooling is available on workstation
- Standard AV/EDR config

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

REAL WORLD TACTICS

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

ASSUMED BREACH TACTICS

- Simulate payload sent via email / SE
- Search out high value targets / data
  - Kerberoasting => elevation of privilege
  - Gather credentials
  - Pivot to data
  - Access high-value targets
- DA is a tool, not a destination!

DOMAIN FRONTING

- Vendors are breaking traditional fronting model
  - Some CDNs still work
- *.cloudfront.net / *.azureedge.net still works
- Build custom C2 profile
  - https://github.com/bluescreenofjeff/
    - Malleable-C2-Randomizer

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

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

FINDING ACCOUNTS

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

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

MINING AD

- SharpHound via execute-assembly
  - Research stealth options
    - --NoSaveCache is your friend
- Hunt for creds in AD schema
  - ADExplorer.exe -snapshot "" ad.snap -noconnectprompt
  - https://www.blackhillsinfosec.com/domain-goodness-learned-love-ad-explorer/

HUNTING GPP CREDS

- GPP = XML config files stored in SYSVOL
  - 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
- psexec
- wmic

TRAWLING FILES/SHARES

- Elevated account creds (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

HUNTING SESSIONS

- 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

BYO POWERSHELL

- Code can be executed in ISE even if PS script 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 means we have to be noisier
  - Not focused on vulns
  - Non-representative accounts/workstations can negatively impact test

SUMMARY

- Better way to prepare clients for attacks they're likely to face
- Requires maturity in client processes
  - VA & pen test cycles before client is ready
- Work with client to get good accounts and workstations
- PowerShell & Cobalt Strike aren't the only way - these were just examples

QUESTIONS?

Mike Saunders

Principal Consultant

mike@redsiege.com
@hardwaterhacker
@RedSiegeInfoSec

Slides: redsiege.com/abm