# HACKER AND QSA STORIES: LESSONS LEARNED FROM A YEAR OF COMPROMISES

LBMC | INFORMATION SECURITY


Speakers

Sheryl Benedict,
Manager
LBMC Information Security
QSA, PCIP, CISA, ISO 27001
Senior Lead Implementer

Daniel Nguyen,
Lead Security Consultant
LBMC Information Security
OSCP, GWAPT


March 28, 2021

# AGENDA









# BACKGROUND

# SHERYL'S BACKGROUND

- Manager at LBMC Information Security
- Cal Poly Pomona BS-CIS Application Software Development Track - Graduated in 2002
- More than 15+ years of experience in Information Security and Compliance.
- Performed various assessments and testing compliance with PCI DSS, SOC reporting, SOX, FIEL/JSOX, HIPAA, Security Risk Assessments, ACAB, IT Internal Controls and Business Process Control reviews, and e-Discovery Computer Forensics throughout several industries and Fortune 500 Global Organizations
- Holds CISA, QSA, PCIP, and ISO 27001 Senior Lead Implementer Certifications

# DANIEL'S BACKGROUND

- Lead Security Consultant at LBMC Information Security
- Former cancer research biologist
- Transitioned into penetration testing with OSCP certification
- No prior tech background
- Professional emphasis on stealthy techniques, e.g. Living off the Land (LOL), Open Source Intelligence (OSINT), misconfiguration abuse
- Led to focus on exploiting human behavior

# WHY HUMAN BEHAVIOR?

## *Benefits for Clients*

- Assesses compliance to information security frameworks
- Qualifies effectiveness of current policies and user education
- Uncovers issues undetected by vulnerability scanners

## *Benefits for Providers*

- Differentiates yourself from competition
- Provides variety on recurring assessments
- For the offensively inclined: Additional attack vectors to bypass otherwise strong technical controls

*Security is both technical and procedural*

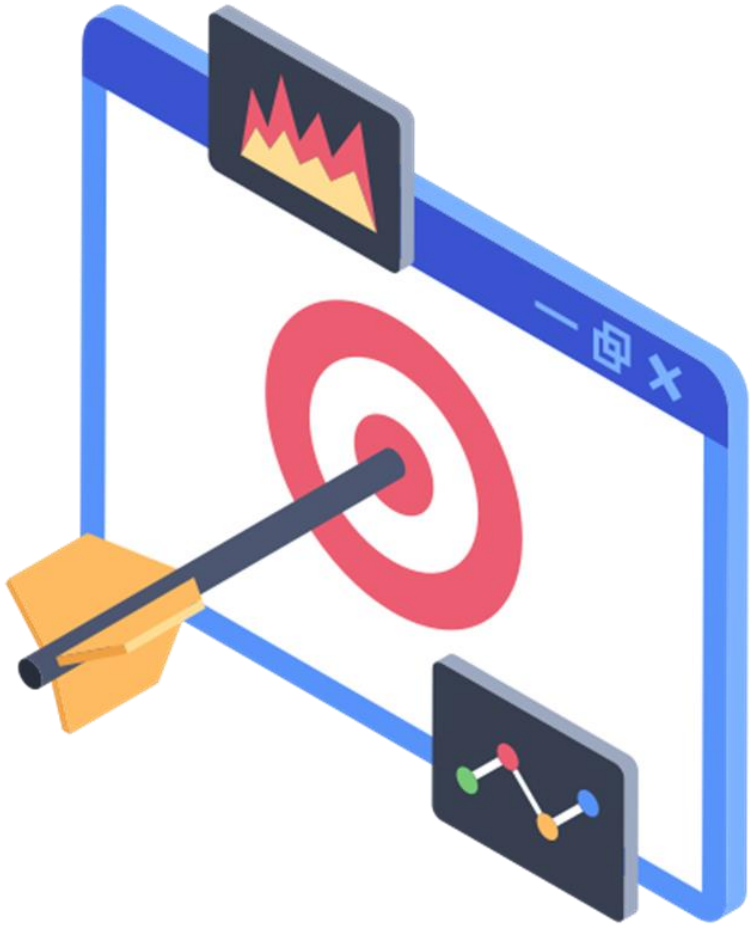
# TARGET PROFILING

*Understand Your Targets*

# TARGET PROFILING

## *Overview*

- Profiling targets helps identify good points of entry and likely successful attacks
- Get it right the first time – you might only have one chance



## *Factors*

- Field/Industry (e.g. Healthcare, Finance, Retail)
- Job Role
- Behaviors, Personality Traits
- Company Culture

# TARGET PROFILING CASE STUDY

## *Background*

- Compromised developer's account on external pentest
- Accessed external Jira and Confluence services hosted on Atlassian
- Third party services not protected by MFA

## *Compromise*

- Cleartext credentials accidentally logged in uploaded shell history file

## *Impact*

- Cleartext credentials were for user and root accounts in Card Data Environment (CDE)
- Complete compromise of CDE
- Highlights need for comprehensive MFA protection

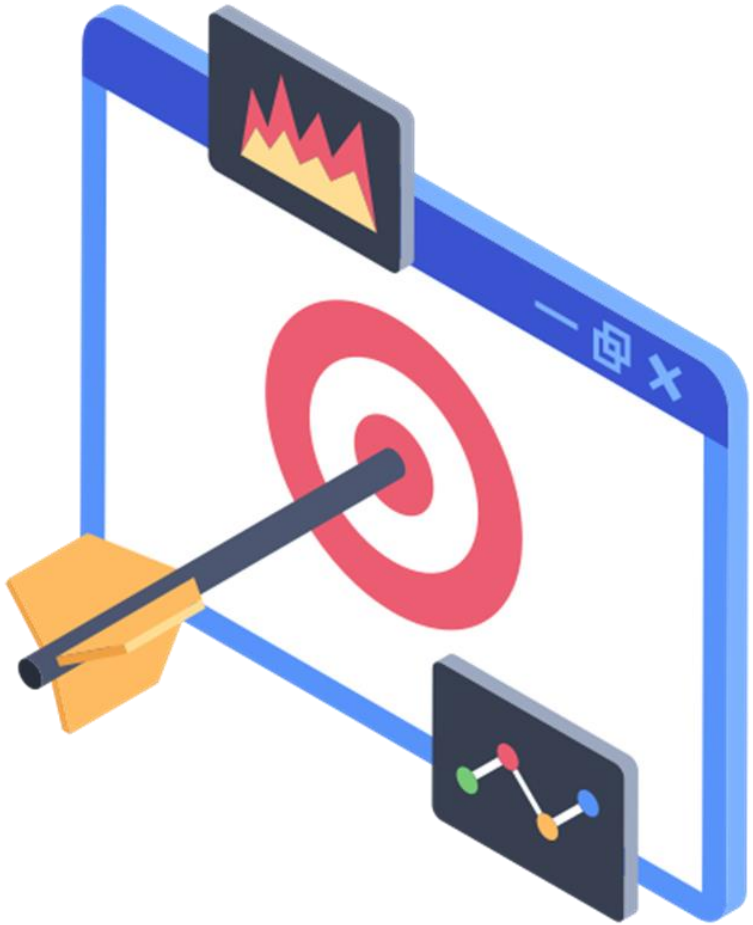
# TARGET PROFILING

## *Overview*

- Based on reconnaissance footprinting techniques

## *Compliance Protections*

- Ensure that technology information is not listed in the public domain (SQL, Oracle, AWS, Azure, etc.)
- Harden Systems
- Ensure that password controls are masked and not stored in clear text
- Enforce MFA for all external faced systems as well as systems that are accessed within the CDE
- Implement Security Awareness Training to prevent social engineering and phishing attempts to compromise PII



# ATTACK PRETEXTING

*Convince Your Targets*

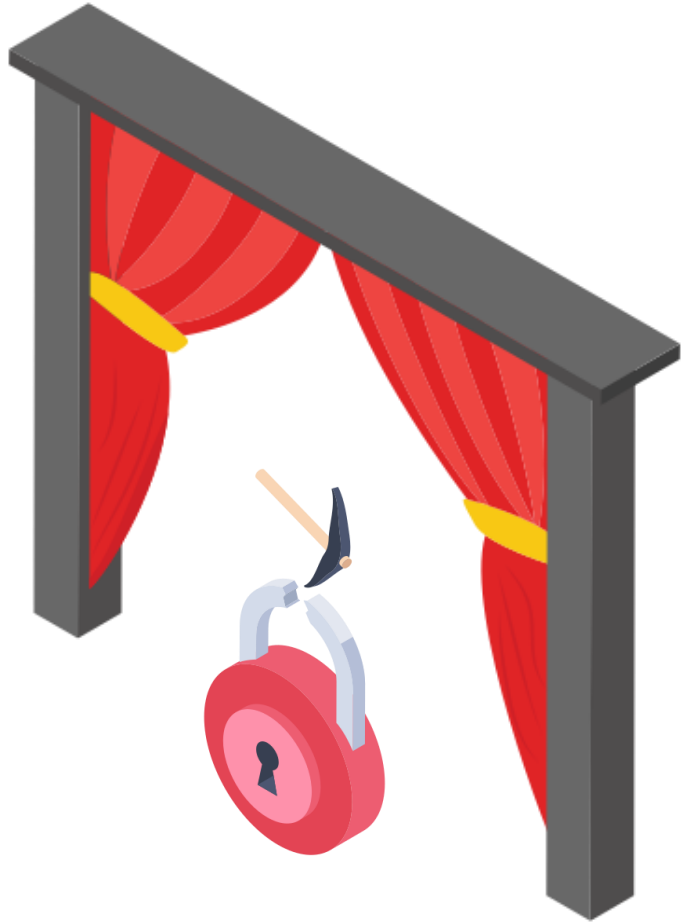
# ATTACK PRETEXTING

## *Overview*

- Contextualizing attacks increases chances of success
- Users much more likely to cooperate if attacks follow expected procedure

## *Factors*

- Standard Operating Procedure
- Daily Routine
- Likeability



# ATTACK PRETEXTING CASE STUDY

## *Background*

- Compromised multiple accounts on external pentest
- All corporate infrastructure protected by MFA
- MFA configured to allow MFA push notifications

## *Compromise*

- Sent MFA push notifications from 8AM-9AM and 12PM-1PM
- Only users with MFA push notifications were targeted

## *Impact*

- Multiple users accepted MFA push notifications
  - Access to email, internal network via VPN, SSO portal
  - External compromise of internal network via Domain Administrator access
  - MFA bypass

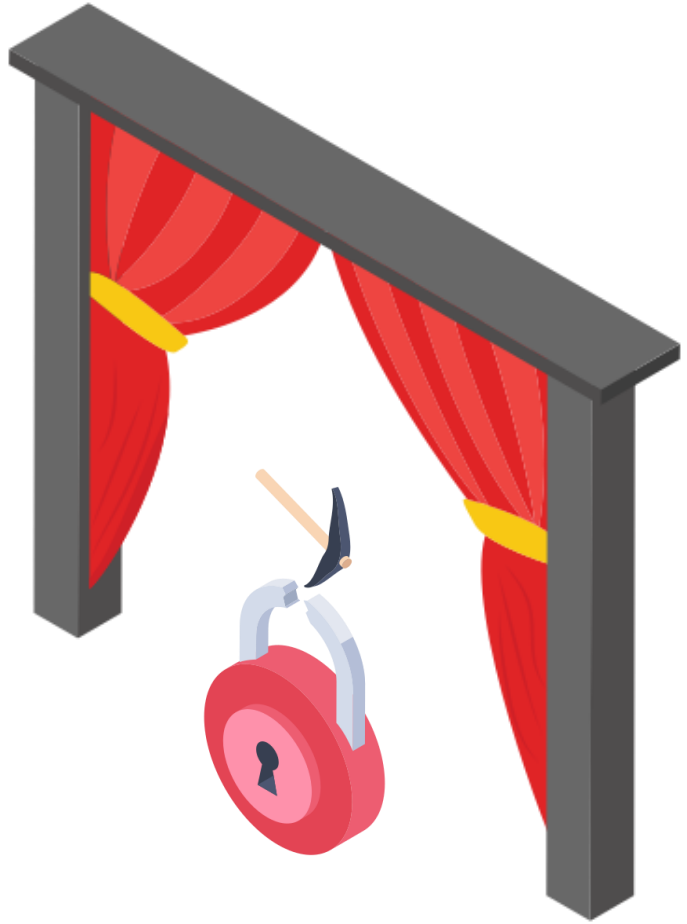
# ATTACK PRETEXTING

## *Overview*

- Based on social engineering techniques gaining trust from the target

## *Compliance Protections*

- Implement policies and procedures
- Implement MFA
- Perform Security Awareness Training (Social Engineering, Phishing, Smishing)
- Perform Regular Tests on Users, e.g. Phishing Campaigns



# PROCESS GAPS

*Divergence in Planning and Execution*

# PROCESS GAPS

## *Overview*

- The best security controls are only as effective as their implementation
- Some issues will slip through the cracks in a sufficiently complex organization

## *Factors*

- Complexity of organization
- Technical and human resources available
- Audits on effectiveness of policies
- Technical quirks, e.g. Group Policy Object Precedence

# PROCESS GAPS CASE STUDY

## *Background*

- Client is organization with decades-old Active Directory environment
- Organic turnover in IT team over the years
- Most security policies implemented since early 2010s
- Many Domain Administrators have not had password changed in 5+ years

## *Compromise*

- Backup Operator account with RDP access to Domain Controllers without password
- One Domain Controller hosting three-year-old backup file of ntds.dit

## *Impact*

- Obtained three-year-old credentials for multiple Domain Administrators
- Credentials valid for many accounts where passwords have not been changed

# PROCESS GAPS

## *Overview*

- Exploitation of weak security controls

## *Compliance Protections*

- Ensure that policies and procedures reflect current practices enforced
- Ensure that password controls reflect industry standard best practices
- Performance of periodic compliance assessments/audits against policies and procedures as well as system configurations

# ACCESS CONTROL GAPS

*One Person's Trash…*

# ACCESS CONTROL GAPS

## *Overview*

- Access control is a fundamental part of security: only grant access to users who need it
- Good access controls hinges on correct determination of appropriate access
- Controls are only as effective as their implementation
- Attackers can often find useful data that is overlooked

## *Factors*

- Proper risk evaluation
- Complexity of access policies
- Visibility into “hidden” infrastructure

# ACCESS CONTROL GAPS

## *Background*

- Found network share readable by any user containing dev environment logs
- Discovered non-sa SQL Server credentials within logs
- SQL Server databases did not contain any sensitive information

## *Compromise*

- SQL Server instance was being run under a Domain Administrator account
- TSQL command xp_dirtree can be run by any SQL Server user to list directory
- SMB poisoners can relay/capture hashes of account running SQL Server instance

## *Impact*

- Hash relaying and password cracking allowed Domain Administrator access

# ACCESS CONTROL GAPS

## *Overview*

- Exploitation of weak and/or excessive access controls

## *Compliance Protections*

- Develop access roles/responsibilities matrixes for various job positions
- Ensure assigned roles permit appropriate separation of duties
- New access requests should not mirror another user's access rights/permissions
- Perform periodic user access reviews
- Ensure terminated user's access is removed timely

# CLOSING THOUGHTS

# TECHNICAL FINAL THOUGHTS

## *Organizations are run by humans*

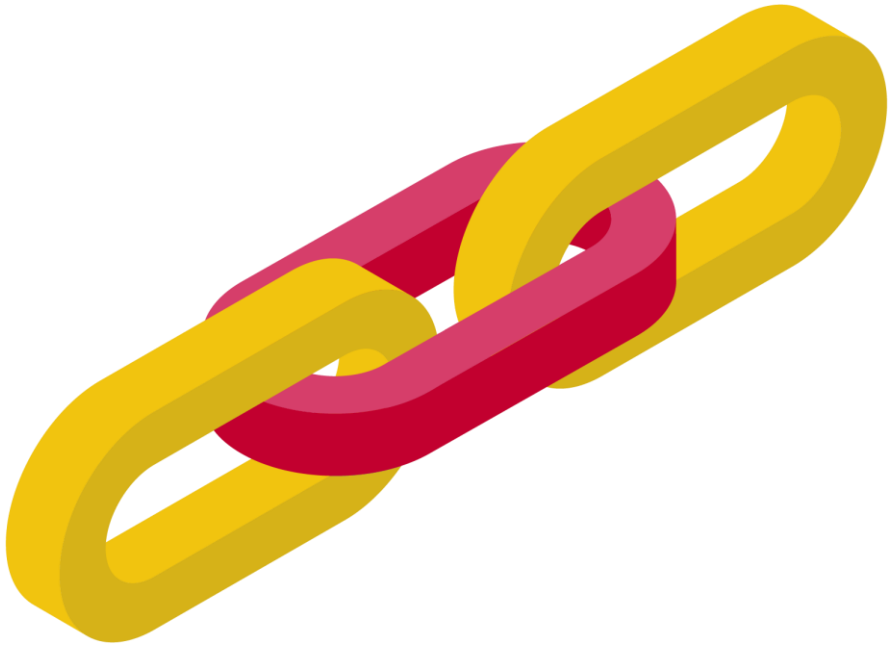
- Technical defenses are ultimately planned, implemented, and controlled by people
- Attackers can bypass technical controls by exploiting the people involved
  - MFA bypass
  - Internal network access without VPN
  - Internal network compromise without privileged account access

## *Anticipate vulnerabilities from people*

- Mitigate risk by implementing processes to counter vulnerabilities from people
  - Regular audits of organization's security
  - Regular security education for all users
  - Continuous learning on new attacks and attack vectors

## *Security is collaborative*

- Technical and process controls supplement one other
- Understanding the human component involved can greatly improve security posture
- Perform risk assessments within the organization



# COMPLIANCE FINAL THOUGHTS

## *Compliance is a requirement*

- Organizations need to implement both technical testing and compliance testing to truly secure an organization.
- Organization may face fines/penalties if not compliant with regulations/standards (i.e., PCI, HIPAA, GDPR, etc.)

## *Best Practices*

- Develop and implement organization wide Information Security Policies and Procedures
- Performance of Enterprise Risk Assessment to understand the Administrative, Physical, Technical, Organizational, Policy and Procedure safeguards required and identify the Human Threats, Technical Threats, Environmental/Physical Threats, and Natural Threats that may exist within the organization
- Implement the necessary controls and compensating controls as necessary to protect the organizations assets

## *Continuous Audit*

- Perform regular assessments/audits of organization's security posture
- Perform security awareness training upon hire and annually for all users
- Ensure users are aware of information security policies and procedures and their requirements to adhere to them
- Perform at a minimum annual penetration testing against environments (black box, gray box)

# ANY QUESTIONS?

LBMC

INFORMATION SECURITY


Sheryl Benedict

*Manager,*
*LBMC Information Security*

615.309.2285

SBenedict@LBMC.com

Daniel Nguyen

*Lead Security Consultant,*
*LBMC Information Security*

615.309.2252

Daniel.Nguyen@LBMC.com


**www.LBMCInformationSecurity.com**