Assumed Breach Assessment: Using You Against You

Don C. Weber - @cutaway
Principal Consultant, Founder

© 2019 Cutaway Security, LLC. All Rights Reserved.
Cutaway Security, LLC

• Don C. Weber - Jack of All Trades
  • Security Management
  • Incident Response
  • Penetration Testing
  • Security Assessments
  • Security Researcher
  • Instructor / Presenter
Assumed Breach Assessment Purpose

• Don’t our system controls protect us from hackers?
• Our workstations are too locked down to do anything!
• Why can’t we access the OT environment with our corporate laptop?
• Those pentesters were already on the inside, that would never work.
Agenda

• Assessment Overview
• Purpose for Assumed Breach Assessment
• Methodology
• Actionable Report
• Roadmap for Improvement
Types of Assessments

Production
- Security Assessment
- Penetration Testing
- Red Teaming

Assumed Breach Assessment

Development
- Design Review
- Architecture Review
- Security Validation

Pre-Development
- Vendor / Service Review
- Software Review
Assessment Styles

• **White Box**
• **Black Box**
• **Gray Box**
Assumed Breach Purpose

- How far can an attacker get as a user?
  - Persist on system?
  - Access file shares?
  - Access local Administrator credentials and use them to move to other systems?
  - Conduct SMB Session enumeration?

- Access to a typical user system
  - Help Desk, HR, Legal
  - Engineer, Programmer
  - Third-party consultant

- Attacker gains control of system
  - Malware / browser / software exploit
  - Physical access
  - Insider threat
Assumed Breach Is Not....

- An internal or external penetration test of the organization
- A detailed analysis of the asset's security baseline.
- Validation of complete / perfect user end-point security.

Assumed Breach Methodology

1. **Tools Required**
2. **Information Gathering**
3. **Vulnerability Analysis**
4. **Exploitation**
5. **Reporting**

Image Source: https://www.controlthings.io/
Methodology: Tools Required

- User account with specified role and permissions.
- Workstations built to the standard that would be assigned to the user.
- Local or remote network access.

Image Source: https://unsplash.com/photos/G3yLB3Fasow
Methodology: Information Gathering

- Review of User's Role and Permissions on system.
- Understand the system’s configuration, installed software, and security controls.
  - Device configuration software and files?
- Network and services reconnaissance.
  - PCAPs of software connecting to servers or devices?
Information Gathering (1)

- Monitor network communications
  - Software: tcpdump, wireshark
  - Hardware: tap, switch with span port
• Assumed Breach Config Checks - https://github.com/cutaway/assumed_breach_config_checks
• PowerSploit’s PowerUp - https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1
Methodology: Vulnerability Analysis

- System vulnerability review (limited to system due to scope).
- Manual review of custom thick clients and third-party programs.
- Vulnerability validation for privilege escalation, remote control, and persistence.
Methodology: Exploitation

- Security control evasion (limited to system due to scope).
- Access remote shares, services, systems, and networks.
Privilege Escalation

• Can attacker elevate privileges on the system or within the environment?
  • Brute Force
  • Metasploit Meterpreter – getsystem
  • Unquoted Service Paths
  • DLL Injection / Hijacking
Actions on Target

- External Control and Data Exfiltration
  - Metasploit - https://www.metasploit.com/
  - Cobalt Strike - https://www.cobaltstrike.com/
  - DNSCat2 - https://github.com/iagox86/dnscat2
  - Iodine - https://code.kryo.se/iodine/
  - Gcat / Gdog - https://github.com/maldevel/gdog

- Internal Network Information Gathering (scope dependent)
  - Powershell Empire - https://github.com/EmpireProject/Empire
  - Powersploit - https://github.com/PowerShellMafia/PowerSploit
    - Find Interesting Files
  - Etc.
Methodology: Reporting

- Executive summary of assessment.
- Detailed description about all actions: successful, blocked, and alerted.
- Risk rated findings with recommendations and validation methods.
- List of baseline configuration changes that will make attacker actions harder to accomplish.
- List of baseline configuration changes that will improve logging of user actions.
Improving Baseline Security

- Microsoft Security Compliance Toolkit 1.0

- Security Technical Implementation Guides (STIGs)
  - https://iase.disa.mil/stigs/Pages/index.aspx

  - https://adsecurity.org/?p=3299

Closing Thoughts

- Uses similar techniques as a penetration test.
- Concentrates on how corporate systems configurations protect assets.
- Focuses on common attack vectors.
Recap

- Assessment Overview
- Purpose for Assumed Breach Assessment
- Methodology
- Actionable Report
- Roadmap for Improvement
Don C. Weber - @cutaway
Principal Consultant, Founder
http://www.cutawaysecurity.com
http://linkedin.com/in/cutaway
https://www.sans.org/instructors/don-c-weber