

MANAGE CYBERSECURITY RISK

WITH PENETRATION TESTING





Lifelong tech geek

Over 20 years of experience in information security strategy and development, risk management, network administration and compliance

Previous experience as a network/security administrator and penetration tester

Holds the following certifications:

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- EC-Council Certified Ethical Hacker (CEH)

TYLER LEET Director of Risk & Compliance Services, CSI



MANAGING CYBER RISK

- Identification of vulnerabilities and security weaknesses
- Testing and validation of controls
- Simulation exercises to mimic real-world threats
- Routine exercises and check-ups
- Remediation, lessons learned and improvements





VULNERABILITY SCAN VS. ASSESSMENT

VULNERABILITY ASSESSMENT

Objective:

Adds evaluation of the risks posed and prioritization of remediate efforts

Gives context and validation to the content

VULNERABILITY SCAN

Objective:
Identifying
vulnerabilities

Only provides unvalidated content







- External/Perimeter
- Internal
- Physical
- Web application
- Wireless

Complements, not substitutes

Combining these measures offers the most protection

Vulnerability Assessment Penetration Testing

Manual and objectoriented

Identifies weaknesses and then attempts to exploit them to move throughout the network

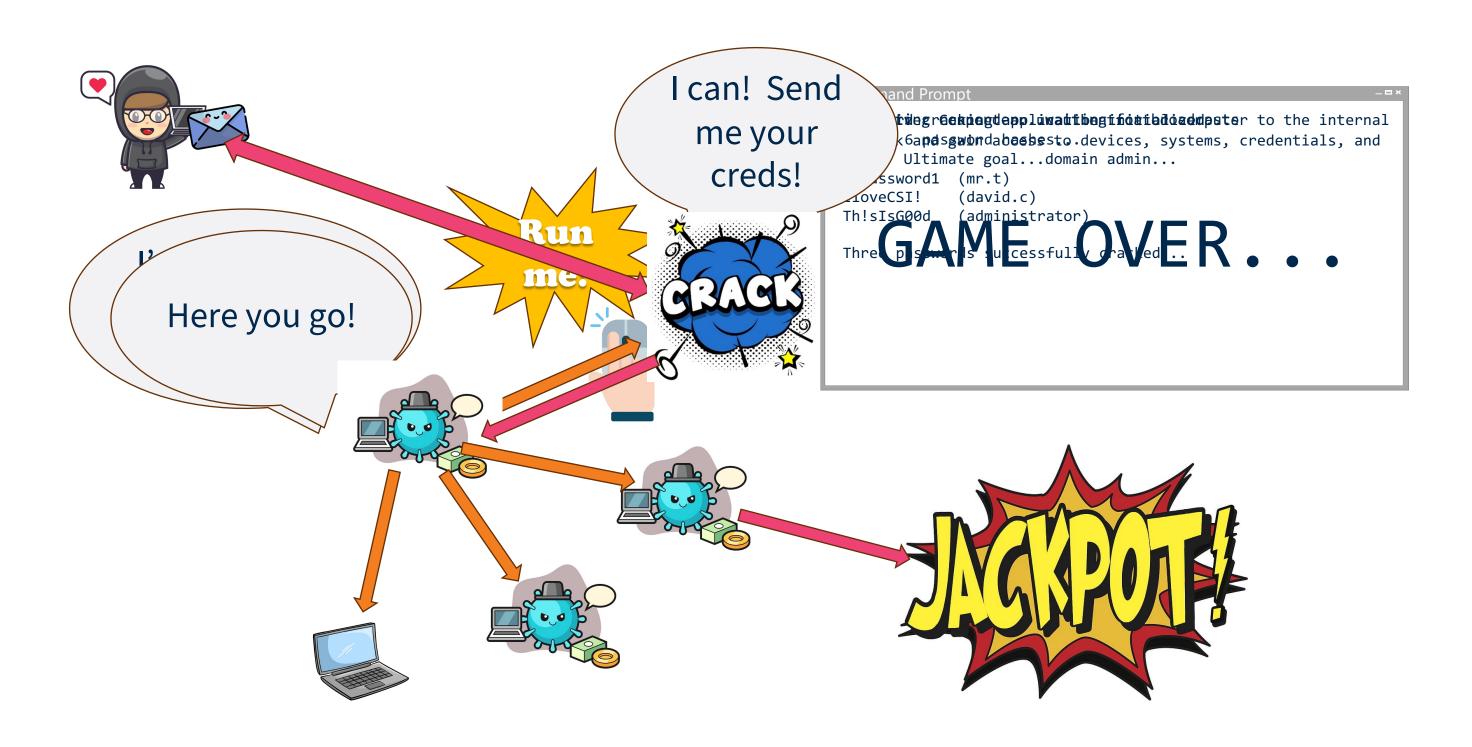
Demonstrates impacts and avenues of exploitation

A broader, generic view

Provides numerous actionable items for remediation, especially low-hanging fruit











SESSION RECAP

The importance of security testing in managing your cyber risk

Differences between the various types of tests

 How penetration testing helps you identify and mitigate cybersecurity vulnerabilities



Contact Info

Tyler Leet, Director of Risk & Compliance Services

Computer Services, Inc.

3901 Technology Drive Paducah, KY 42001

Tyler.Leet@csiweb.com



