A Primer on Penetration Testing in 2019

Presented to the 85th Annual ICUL Meeting

Justin Hall

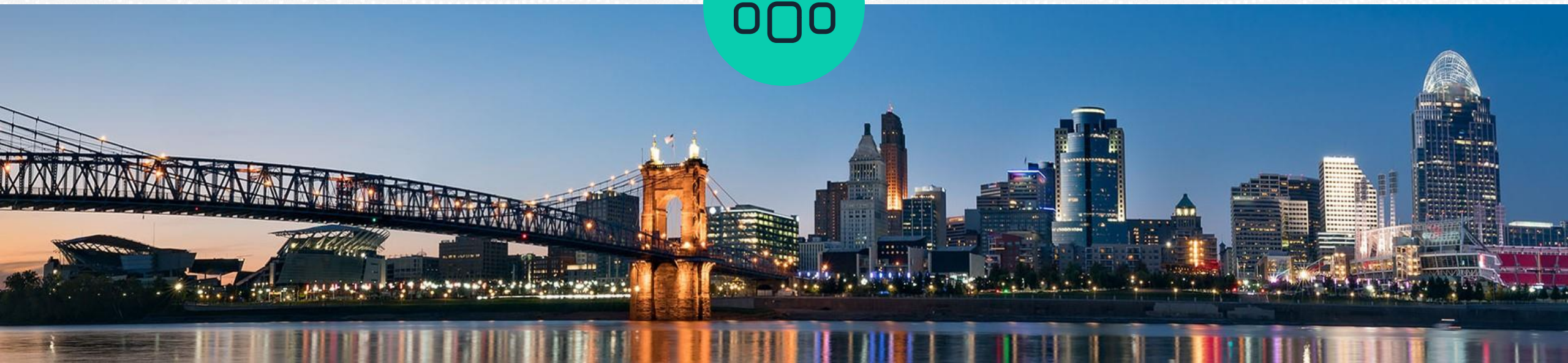
Director, Security Consulting

cbts

/usr/bin/whoami

- Cincinnati native
- Husband & dad
- 23+ years in IT
- 14+ years in security

- Director of Security Consulting at CBTS
- GCIH Gold / GCFA / GPEN
- University of Cincinnati College of Business alumnus



What is a Penetration Test?

cbts


The Engineer

Cybersecurity spending in 2018 was

$114 billion

and is likely to grow to $170 billion in 2022

Source: Gartner, Forecast Analysis: Information Security

What is penetration testing?

cbts

"Security testing in which assessors **mimic real-world attacks** to identify **methods for circumventing the security features** of an application, system, or network."

NIST 800-115 - Technical Guide To Information Security Testing And Assessment

Penetration testing is not…

Vulnerability Assessment

- Vulnerability assessment is simply **cataloguing and identifying issues** in a computing environment, Penetration testing is an **attack simulation**

- Vulnerability assessment **stops at finding vulnerabilities**, Penetration testing goes on to **exploit them**

Penetration testing is not…

Red Teaming

- A red team directs an **ongoing**, 24x7 set of **individual operations** intended on compromising a network by **any means necessary**, with the goal of exposing issues in an organization's entire security strategy

- A penetration test typically has an **explicitly defined scope** and limits on the attack vectors that can be employed to validate the controls around a particular **network segment**, **application**, **or practice**

CBTS Penetration Testing Practices

cbts

Since 2009, **20-30 delivered per year** by GIAC-certified CBTS Security Consulting team based in Ohio

Attack vectors include Network, Web Application, Mobile Application, Phishing & Social Engineering, Wireless, and Physical testing

Custom attack scenarios and **handwritten** (not auto-generated), cage free, artisan, locally-sourced, farm-to-table findings reports suitable for several audiences

Common Findings

Common Pentest Findings

From CBTS Penetration Test Services

cbts

#1 Missing Patches

Attackers will use these vulnerabilities to:

- Run their code on target systems
- Establish persistence mechanisms
- Gain information about the environment, or elevated privileges

Defenders need to:

- Have visibility into the state of the authorized assets in the environment
- Establish a strong vulnerability management program
- Test patches before install, and validate patches have been applied with scans

Common Pentest Findings

From CBTS Penetration Test Services

cbts

#2 Default or Easily Guessed Passwords

Attackers will use these vulnerabilities to:

- Gain access to applications, smart devices, appliances, OT
- Quickly gain administrative privileges
- Password-spray with known accounts

Defenders need to:

- Enforce a strong password policy for all employees and for functional accounts
- Ensure that deployment processes for all infrastructure include default password changes
- Regularly audit enterprise password strength

Common Pentest Findings

From CBTS Penetration Test Services

cbts

#3 Weak Operating System configuration

Attackers will use these vulnerabilities to:

- Intercept network sessions, such as SMB or Remote Desktop traffic, and steal credentials
- Laterally move from host to host undetected
- Grab cached Domain Admin credentials from memory

Defenders need to:

- Harden gold images of servers, workstations, and network devices so that all newly deployed machines have reduced attack surface
- Compare OS config to benchmarks and vendor best practices

Pentesting Resources

Methodology

- *NIST 800-115* – Technical Guide to Information Security Testing & Assessment
  - Official guidance from US govt
- Penetration Test Execution Standard *(PTES)*
  - Community developed
- MITRE ATT&CK Framework
  - Research institution developed

Books

- *CounterHack Reloaded* by Ed Skoudis and Tom Liston
- *Penetration Testing: A Hands-On Introduction to Hacking* by Georgia Weidman

Pentesting Resources

Tools

- Kali Linux
  - Linux distribution with commonly used tools by Offensive Security
- DVL
  - Linux distribution that contains vulnerable software for test simulation
- Samurai WTF
  - Linux distribution with commonly used web application testing tools

Training

- *SANS Institute* – SEC560, Network Penetration Testing & Ethical Hacking
- *Offensive Security* – Certified Professional (OSCP)
- *SpectreOps* – Red Team Operations

Q&A

Justin Hall, GCIH, GPEN
Justin.Hall@cbts.com
@justinhall

cbts


Thanks!
cbts
cbts.com/security