



# Penetration Testing, Vulnerability Scanning and Mitigation

Find – Test - Resolve



# Disclaimer

*The information contained herein has been prepared for general informational purposes only and is not offered as and does not constitute legal advice or legal opinions. You should not act or rely on any information contained herein without first seeking the advice of your legal counsel.*

*No copy or use of this presentation should occur without the permission of Vizo Financial. Vizo Financial retains all intellectual property interests associated with this presentation. Vizo Financial makes no claim, promise, or guarantee of any kind about the accuracy, completeness, or adequacy of the content of the presentation and expressly disclaims liability for errors and omissions in such content.*

*“Penetration Testing, Vulnerability Scanning and Mitigation” discussed in this presentation is the current version with effective date of 03/25/2025.*

*The comments today are my own and not necessarily those of Vizo Financial or the Vizo Financial membership.*

# Agenda

Vulnerability Scanning

Penetration Testing

Scanning vs. Testing

Mitigation

Questions



# What is a Vulnerability?



# Vulnerability Scanning

- ....the quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.
- It's a weakness in your defenses...
- A crack in your armor...
- A hole in your castle wall...

# Vulnerability Scanning



# Vulnerability Scanning

- Cyber Security – the process of using automated tools to identify and assess security weaknesses in
  - Systems / Networks / Software
  - Predictable Scheduled / One-Off
  - Authenticated Mode
  - Address Ranges
- Allowing organizations to proactively address potential threats before attackers can exploit them.

# Vulnerability Scanning – Why?

- Identify security risks – cannot fix what you don't know about.





# Vulnerability Scanning

- Missing Patches both OS and Third Party
- Weak, Default, or Missing Passwords
- Open Ports
- End of Life Software
- Misconfigurations



# Vulnerability Scanning

- Known Vulnerabilities – Common Vulnerabilities and Exposure
  - CVE catalog: list of known vulnerability
    - Identify one vulnerability from another
    - Define how the vulnerability works
    - Prioritize through criticality
    - Resolution
  - Zero Day – **\*\*the unknown\*\***
    - White Hat vs. Black Hat - Bug Hunters

# Vulnerability Scanning - What

- Network – Routers, Switches, other Infrastructure Devices
- Hosts – Servers, Laptops, Desktops
- Web Applications – Both the Code and Hardware
- Cloud Services – Storage, SaaS

# What is Penetration Testing?



# Penetration Testing

- ....an authorized simulated attack preformed on a computer system to evaluate its security.
- Preformed by ethical hackers attempting to gain access...
- Mimics a real-world situation to test defenses, incident response and find weaknesses...
- Tests the inside and outside of your network...

# Penetration Testing – Types

- Black / White / Gray Box
- Social Engineering
- Wireless
- Applications

# Vulnerability Scanning vs. Penetration Testing



# Scanning vs. Testing

- Vulnerability Scanning
  - Automated tools to find “known” weaknesses
- Penetration Testing
  - Begins with vulnerability scan, but then takes it further by attempting to exploit what is found



# Mitigation



# Mitigation

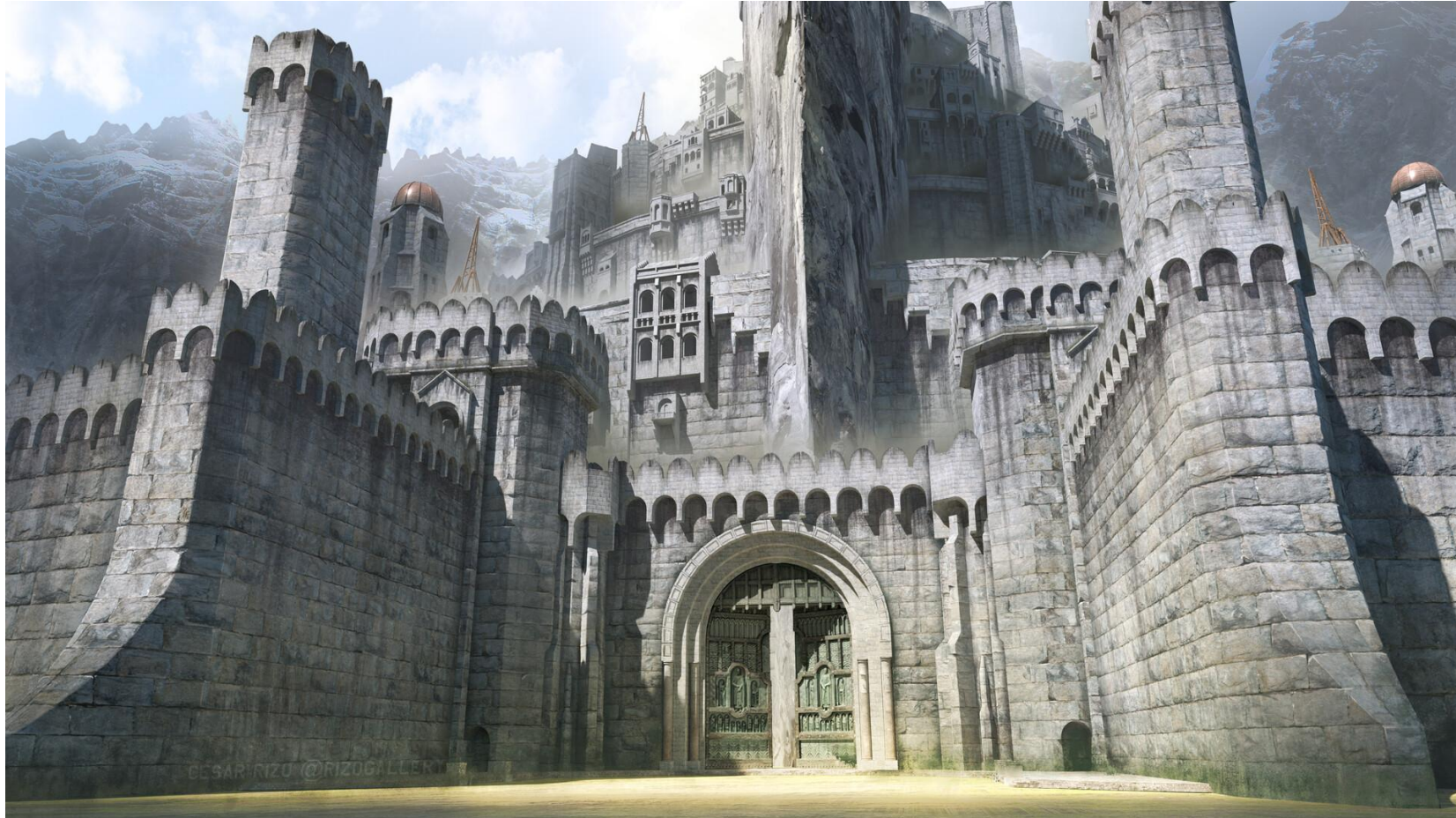
- ...process of reducing or eliminating the risk associated with a security vulnerability.
- Patching
- Security Controls
- Accept the Risk

# Mitigation





# Mitigation



# Review



Vulnerability Scanning



Penetration Testing



Risk Mitigation



www.TedNasmith.com

Green Hill Country — Copyright © Ted Nasmith. All rights reserved.



# Questions





# Contact Information

- Michael Bechtel
- Information Security Engineer
- [mbechtel@vfccu.org](mailto:mbechtel@vfccu.org)
- Toll-Free (800) 622-7494 ext. 1101
- Website:  
[www.vfccu.org/solutions\\_mobile/risk\\_management.html](http://www.vfccu.org/solutions_mobile/risk_management.html)