

3-TIER APPROACH FOR A TRUE PENETRATION TEST

PRESENTED BY: DONOVAN FARROW



WHY HAVE A PENETRATION TEST?

- **Get a Baseline for Security?**
- **Discovery of a Vulnerability?**
- **Secure your Environment?**
- **3rd Party Perspective?**
- **Make the Auditors
Leave you ALONE!?**
- **Want to Get
More?**



DISCOVERY, RECOVERY AND INTELLIGENCE

TIER-1

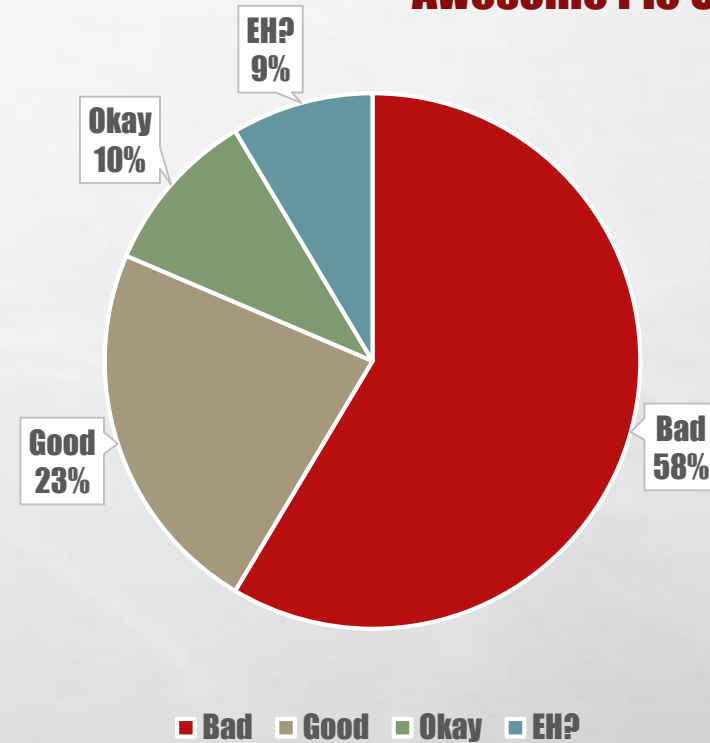
- **LINKEDIN**
 - **CISO'S BACKGROUND, CEO BACKGROUND, SECURITY PERSONAL AND THEIR TALENT SKILLS**
- **GOOGLE**
 - **FIND IP RANGES, NET WORTH, BUSINESS PARTNERS, KNOWN VULNERABILITIES**
- **PASTE SITES**
 - **LEAKED USERNAMES AND PASSWORDS, VULNERABILITY CODE, LEAKED INTERNAL NETWORK INFORMATION**
- **DARKWEB**
 - **RAT FOR SALE, LEAKED USERNAME AND PASSWORDS, BLACKMAIL MATERIAL, DARKWEB INTEL OF COMPANY**
- **FORUM / LISTERV**
 - **DISCOVER / PURCHASE DATA TO SEE WHAT IS KNOWN ABOUT A COMPANY WITH SOCK PUPPET TECHNOLOGY**

SCANNING AND VULNERABILITIES

TIER-2

- **Why do We Scan the Environment?**
- **Is one Scanner Good Enough?**
- **Vulnerability is Found. Now What?**
- **Not Practical. Single Scan Next Steps?**
- **30 Day - Return of the Hack.**

Awesome Pie Chart



GETTING EXPOSED, EDUCATED WITH A TOUCH OF INCIDENT RESPONSE

TIER-3

- **Live Scenario!**
- **We have Identified the Vulnerabilities.**
- **How does a Vulnerability Translate into a Breach?**
- **Does Your Team even know what the Breach would look like?**
- **How do we Stop the Breach!?**

TAKEAWAYS

- **Why have a Penetration Test?**
- **Discovery, Recovery and Intelligence.**
- **Scanning and Vulnerabilities.**
- **Exposed, Educate and Incident Response.**
- **Get More from a Penetration Test.**

THANK YOU

**Presented By:
Donovan Farrow**

AF
alias forensics