



# Hunt or be Hunted!!!

*Enhancing Your Enterprise doing VA and PenTesting*

---

*Ali Hadi, PhD*

[@binaryz0ne](#)



# # whoami

- University professor @PSUT by day
- DFIR researcher by night!
- PhD research in Network Security “Port Knocking”
- 14+ years of Professional Experience
- 14+ world known certificates
- Author and Speaker
- Research interests: DFIR, Network and Malware Forensic Analysis, Social Engineering

# Vulnerability Assessments

---

- Identify, quantify, and evaluate the security risks posed by identified vulnerabilities
  - Identification
  - Prioritizing

# Penetration Tests


- Simulate the tactics and behavior of an actual attacker (external and/or internal ) that aims to breach the security of the organization
  - Scope: what it is you are supposed to test
  - RoE: how testing is to occur
  - Social Engineering
  - etc

# Diff VA PT?

---

- To answer that Q, consider this goal:

**Modify Student Mark in DB**



So ...

---

## **Vulnerability Assessments**

- What are our weaknesses and how do we fix them?

## **Penetration Tests**

- Can someone break-in and what can they attain?

# Which Comes First?

- Start with VA
  - (re)-Assess, Scope, Recon, Analyze, Report, Mitigate
- Reach the required security posture
- Request and/or Perform Pen Testing

# Tools, Tools, Tools ...





# True Arsenal

---

## Your staff is the best arsenal, so:

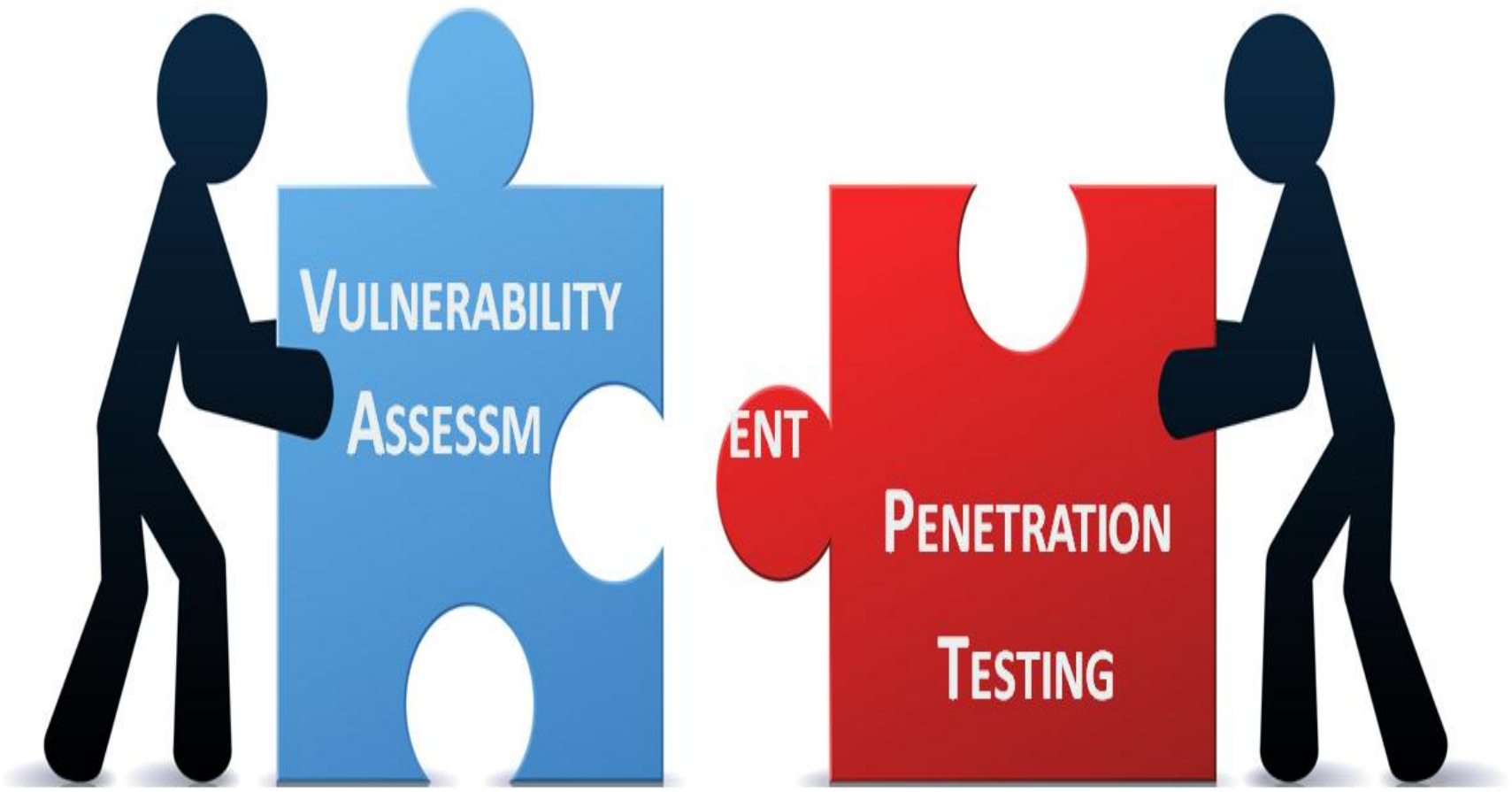
- Continuously educate them (a must)
- Hire guys with brains not certificates!
  - Getting both is perfect
  - People with perseverance
  - People that think differently
- Pay them well
  - They are the ones covering your back 😊

# Being Effective

- Understand your environment
  - Hosts
  - Applications
  - Services
  - Systems
  - Processes
  - Users and Groups
  - Privileges
  - Networks
  - Protocols
  - Connections and relationships
  - Procedures
  - etc

**It's not just  
pointing and  
clicking!!!**

# Side | Side



**Is that all you're explaining?**

---

# Need Hunting Teams?

---

- Many opaque components of the information infrastructure
- You are combating a creative and adaptive adversary
- Statistics have shown that people are compromised for years without noticing

# Hunting Teams do What?

---

- Searching for adversaries without a particular indicator !

# Benefits?

- Makes the organization proactive against attackers
- Quickly find gaps in system and application configurations
- Defenders more familiar with their own environment and infrastructure
- Documentation leads to organizational knowledge

*Highly recommend checking Andrew Case's presentation [4]*

# Real Life Scenario

- Company did a pentest “call it that way” 😊
- Was told to double check their network
- Found a 2y old vulnerability!
- Why? How?
  
- Further hunting showed that this 2y old vulnerability has lead to compromise!
  - Client had no idea he/she was compromised!



# References

---

- [1] Vulnerability Assessments Versus Penetration Tests, <http://www.secureworks.com/resources/newsletter/2006-03/>
- [2] Penetration Testing Execution Standard, [http://www.pentest-standard.org/index.php/PTES Technical Guidelines](http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines)
- [3] Effective Security Spending, <http://blog.securestate.com/prerequisites-for-pentests/>
- [4] The Need for Proactive Threat Hunting, Andrew Case, 2015, <https://www.slideshare.net/AndrewDFIR/my-keynote-from-bsidestampa-2015-video-in-description>