



# Security Scanner

---

ابوالفضل بابامحمدی [babamohamadi@cert.um.ac.ir](mailto:babamohamadi@cert.um.ac.ir)

کارشناس آزمایشگاه تخصصی آپا دانشگاه فردوسی مشهد

سازمان فناوری اطلاعات ایران - مرکز ماهر - تابستان ۱۳۹۵

(کارگاه آموزشی مدیران و کارشناسان فناوری اطلاعات و ارتباطات استان بوشهر)



# Penetration Testing

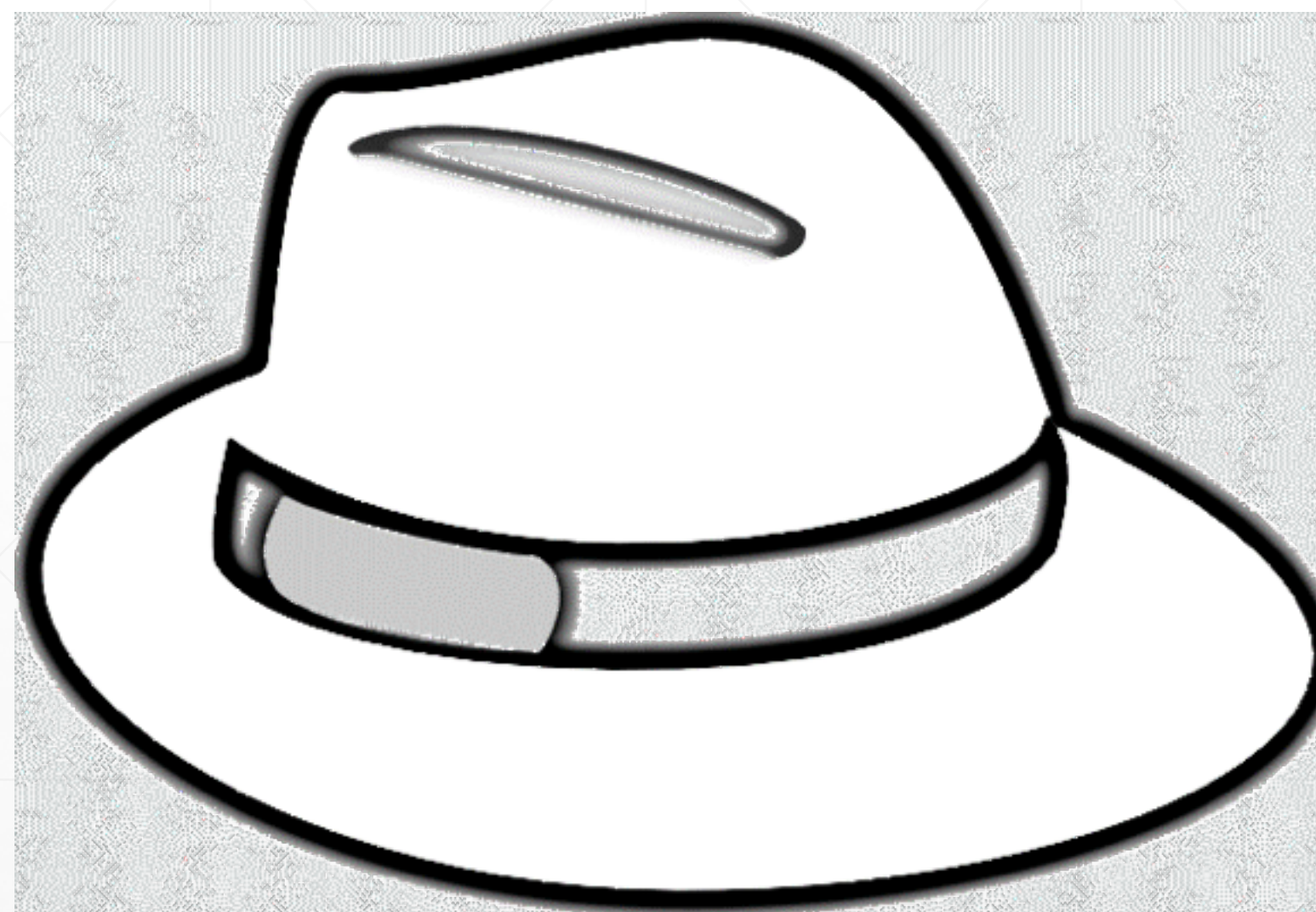
- Pen test  $\equiv$  Penetration Testing
  - A Penetration Test, occasionally pen test, is a method of evaluating the security of a computer system or network by simulating an attack from a malicious source.





# Penetration Testing

- What deferent Hackers and Penetration tester?





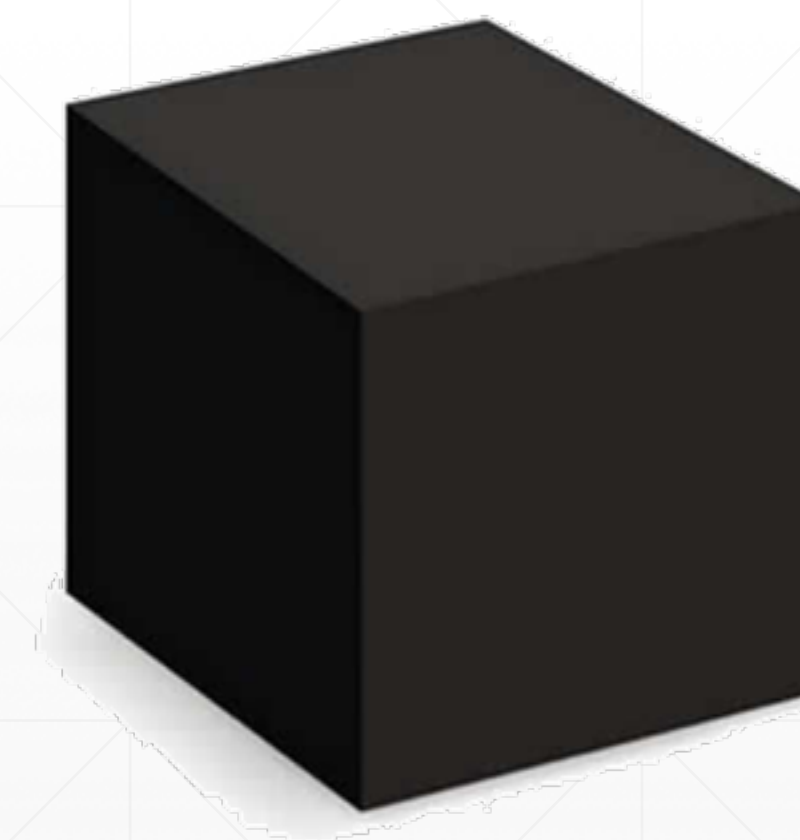
# Phase Of Pen Test

- Black Box
  - External Penetration Test
- With Box
  - Internal Penetration Test
- Grey Box



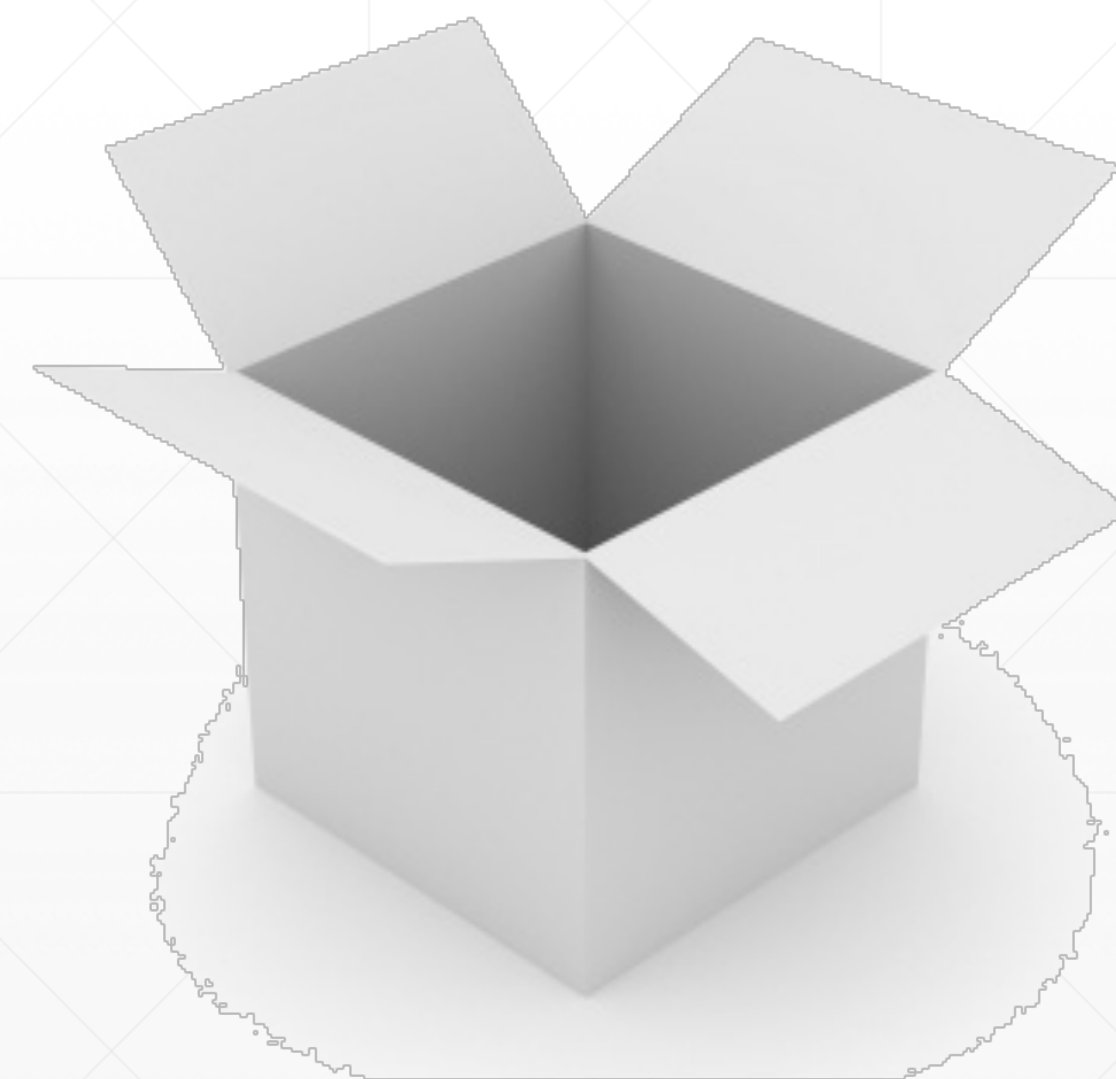
# Black Box Penetration Testing

- The first phase of Pen Test
- simulate real-world attacks
- External Pen Test
- Zero-Knowledge testing



# White Box Penetration Testing

- You Will be give Complete Knowledge of the Infrastructures that needs to be test.
- Check misconfiguration



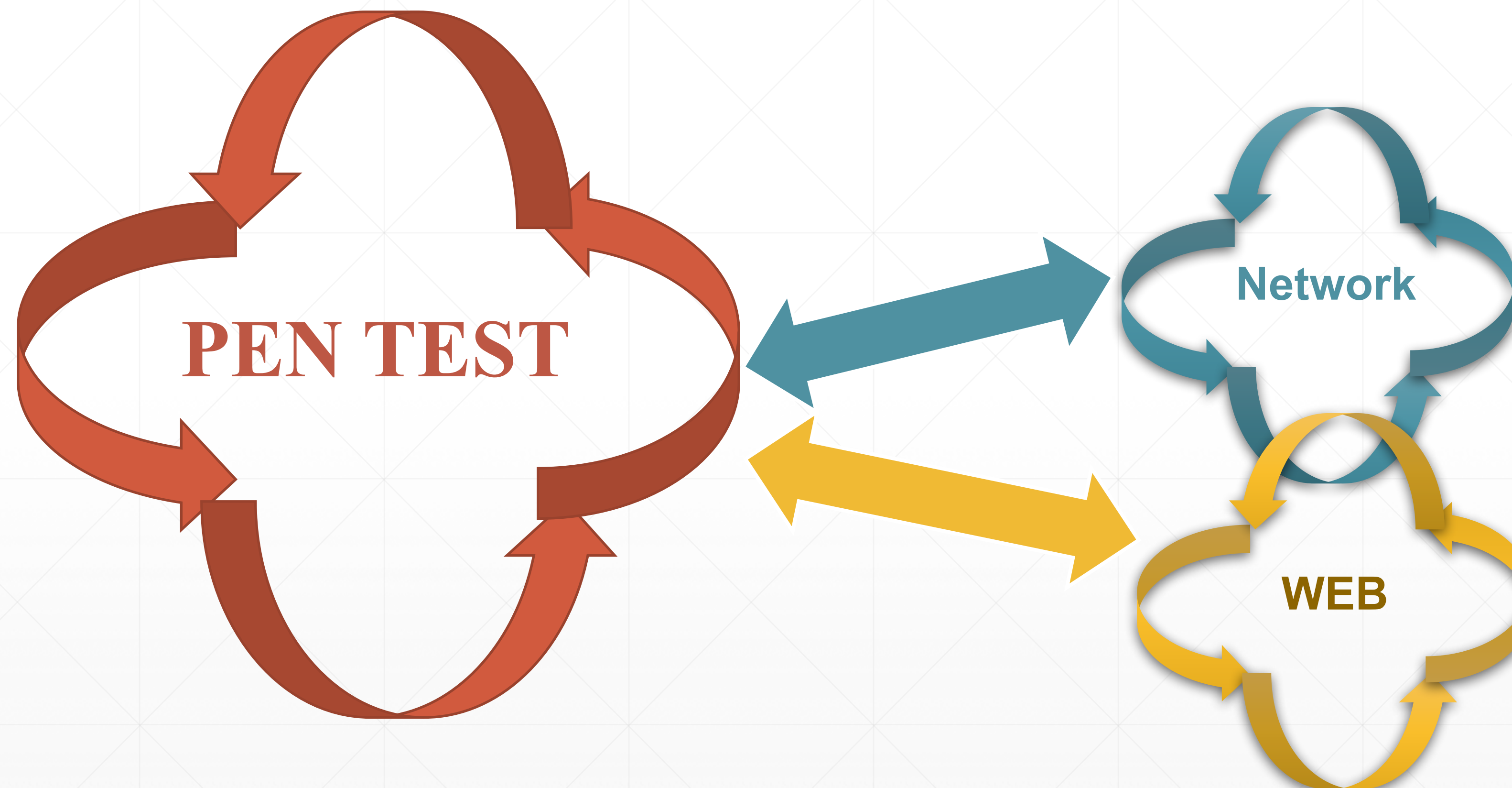


# Grey Box Penetration Testing

- The Grey Box or Crystal Box, Tester Usually has a Limit Knowledge of Information
- Authorize Hackers!



# Scope of Pen Test





# OS Penetration Testing (Timeline)

- SLAX
- Konppix
- Helix
- Blackbuntu
- Operator
- PHLAK
- F.I.R.E
- NodeZero
- Bugtraq
- WEAKERTH4N
- DEFT
- CAINE
- Matriux
- Gnack Track
- BackTrack
- **Kali**
- ...



Favorites

- 01 - Information Gathering ▶
- 02 - Vulnerability Analysis ▶
- 03 - Web Application Analysis ▶
- 04 - Database Assessment ▶
- 05 - Password Attacks ▶
- 06 - Wireless Attacks ▶
- 07 - Reverse Engineering ▶
- 08 - Exploitation Tools ▶
- 09 - Sniffing & Spoofing ▶
- 10 - Post Exploitation ▶
- 11 - Forensics ▶
- 12 - Reporting Tools ▶
- 13 - System Services ▶

Usual applications ▾

- Accessories
- Electronics
- Graphics
- Activities Overview



# Security Scanner

- Nessus
- GFI LanGard
- Acunetix
- Netsparker
- BurpSuitPro
- ...



# Questions ?

---

Thanks for your Attention