Internet Service Provider Attack Scenario

MENOG
2018

About me

Mohammad Reza Mostame

- Expert in information security

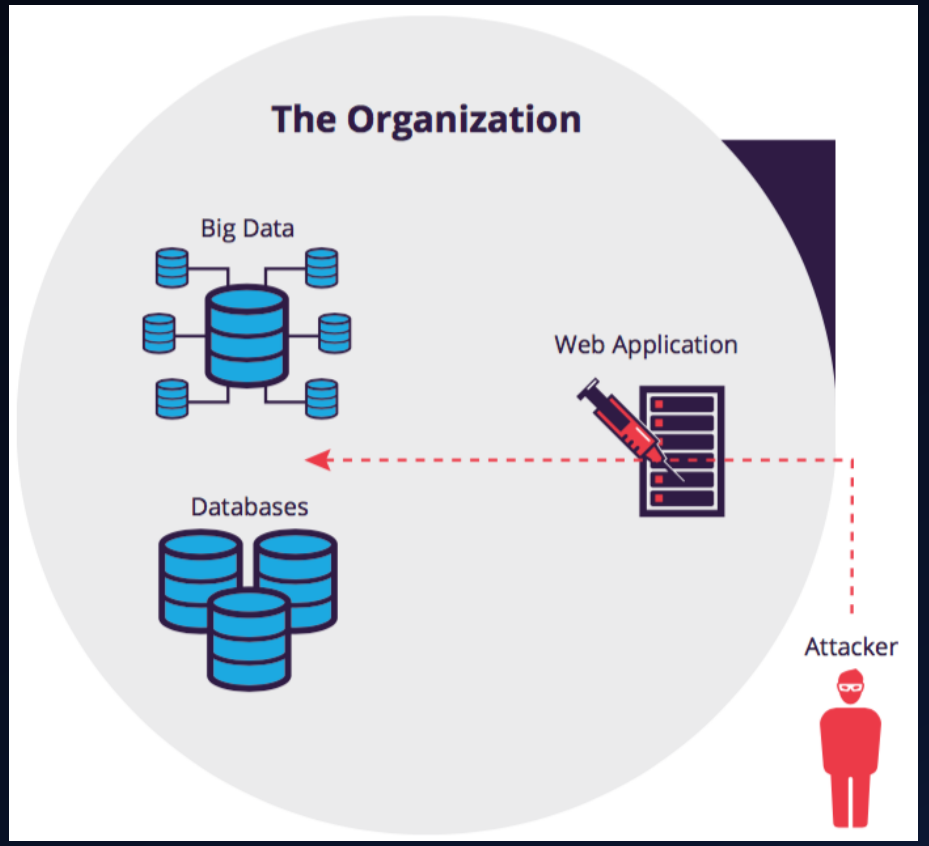
- Email: info@rnpg.ir

Internet Service Provider threats

- Service unavailability
- Data leakage
- Abuse of network resources

Network access through web applications

- Web application vulnerability
  1. SQL Injection
  2. OS access
  3. Privilege escalation
  4. Layer 2 network attack

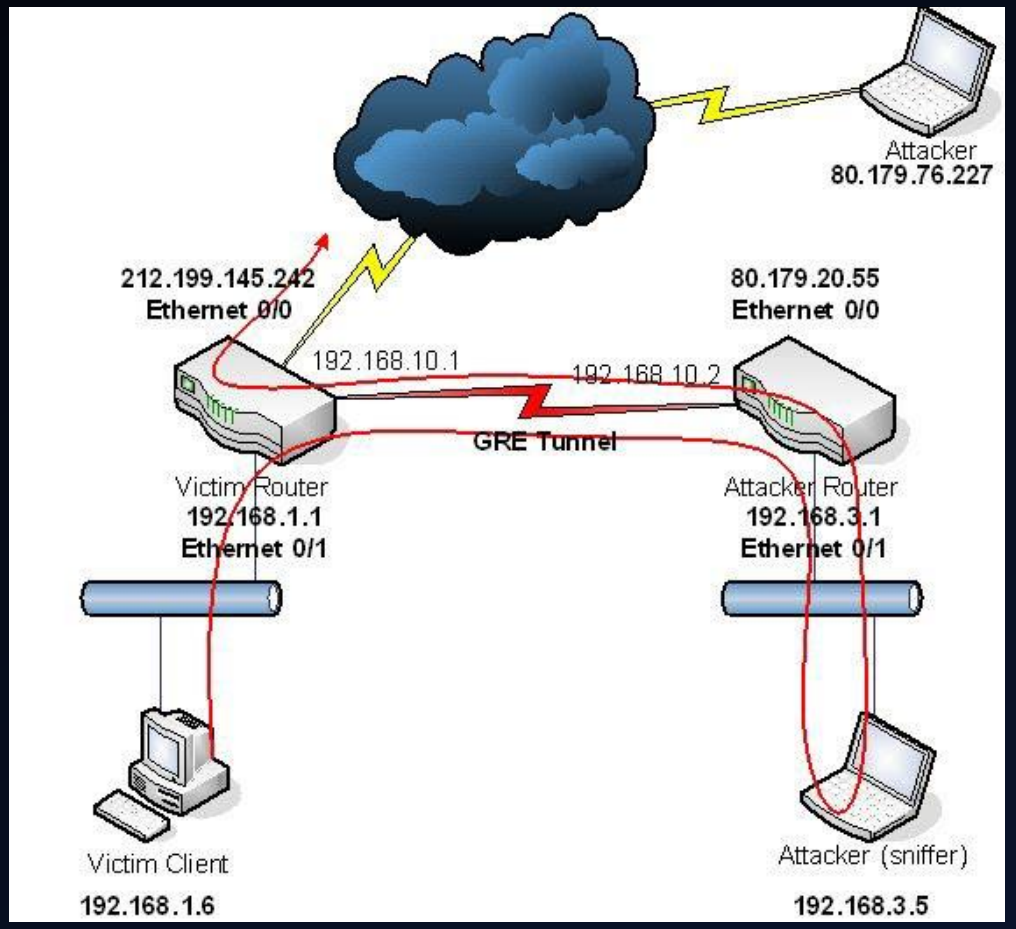


Routers access method

- monitoring software vulnerabilities
- Routers vulnerabilities
- Routers misconfigurations

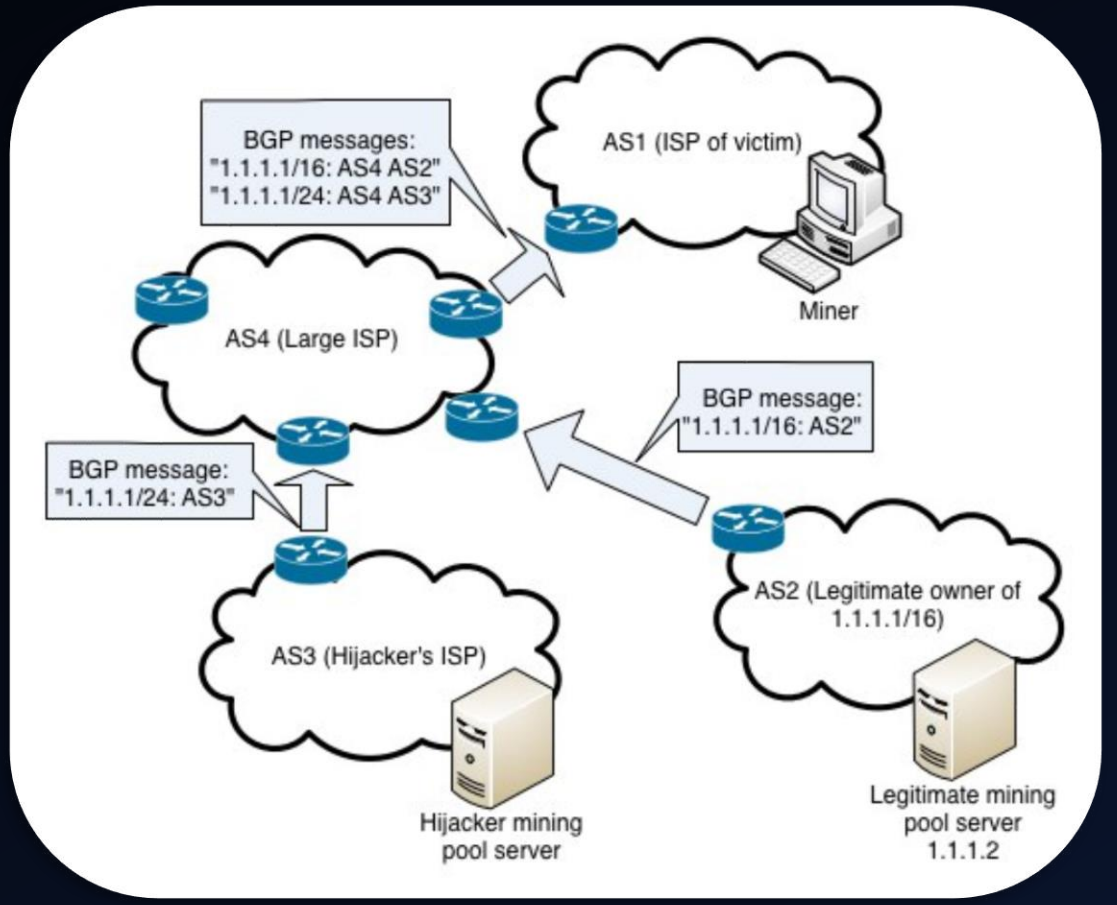
Attack scenario against Internet Service Provider

- Getting access to the routers and hijack the network traffic



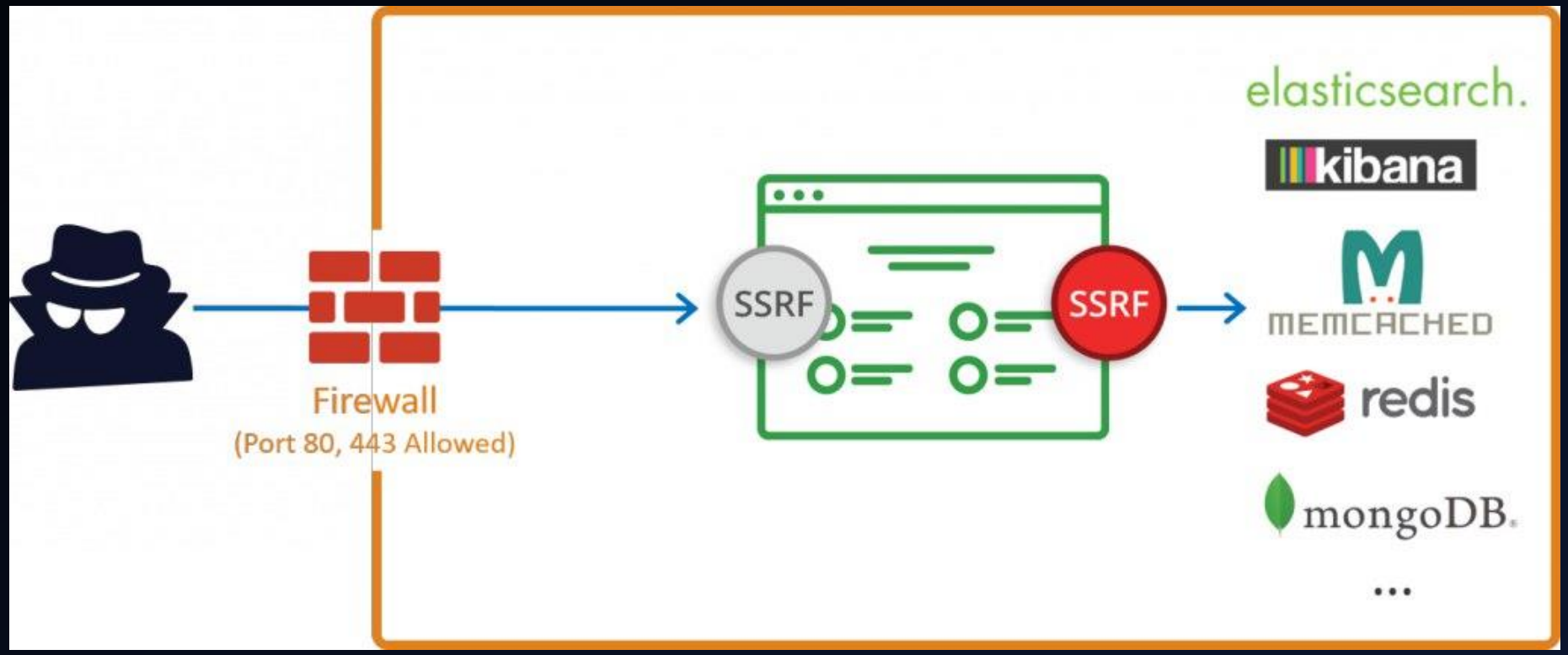
Attack scenario against Internet Service Provider

- BGP hijack



Attack scenario against Internet Service Provider

- Remote File Inclusion’s vulnerability leads to Firewall bypass



Attack scenario against Internet Service Provider

- LDAP Injection attack
- Pass The Hash vulnerability
- Escalate privileges to the administrator in Active Directory

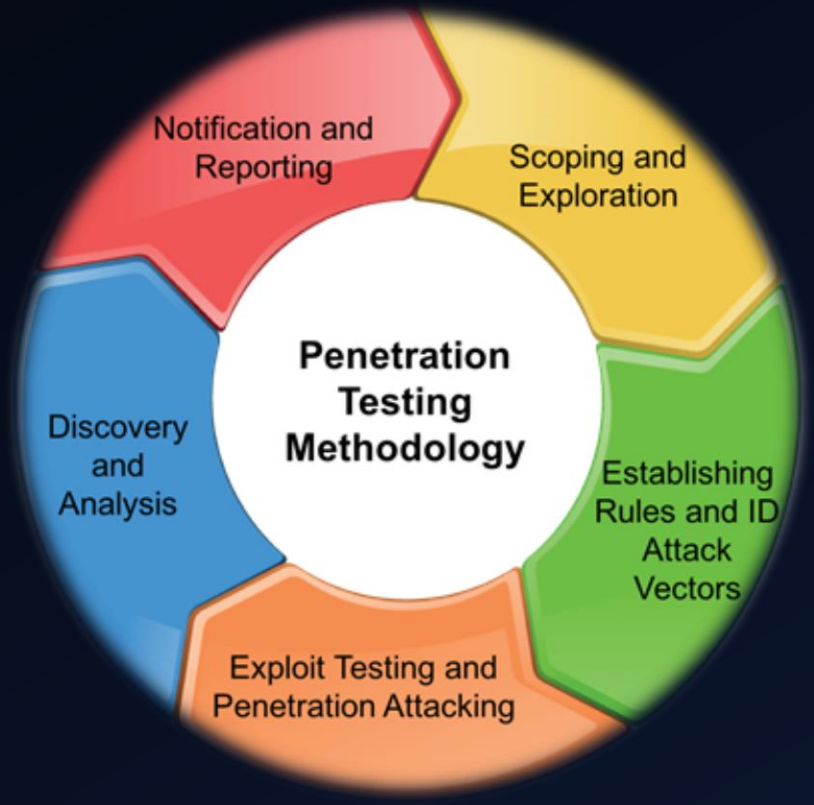
How to secure the Internet Service Provider’s infrastructure!

First: Identify threats

- Penetration testing can help us to find the threats.
- ISP’s threats divided into 4 sections
  1. Web application vulnerability and exploitation
  2. Misuse of Network resources
  3. Misuse of OS vulnerability
  4. Mobile applications threats

Penetration testing benefits

- Preventing Information Loss
- Preventing Financial Loss
- Protect Your Brand in Market
- Essential part of compliance standards or certifications for your business

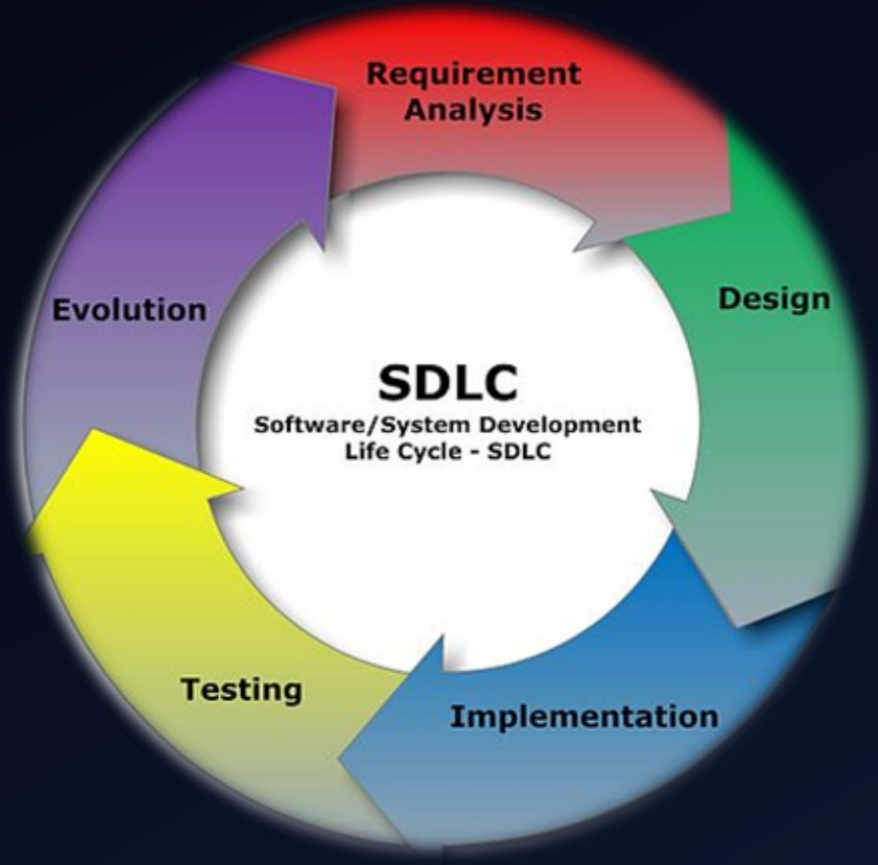


Second: Secure your business

- Web application hardening
- Network hardening
- OS hardening
- DLP

Web application hardening

- Runtime Application Self-Protection (RASP)
- Web Application Firewall (WAF)
- Secure Software Development Life Cycle (SDLC)
- Database Firewall (DBFW)

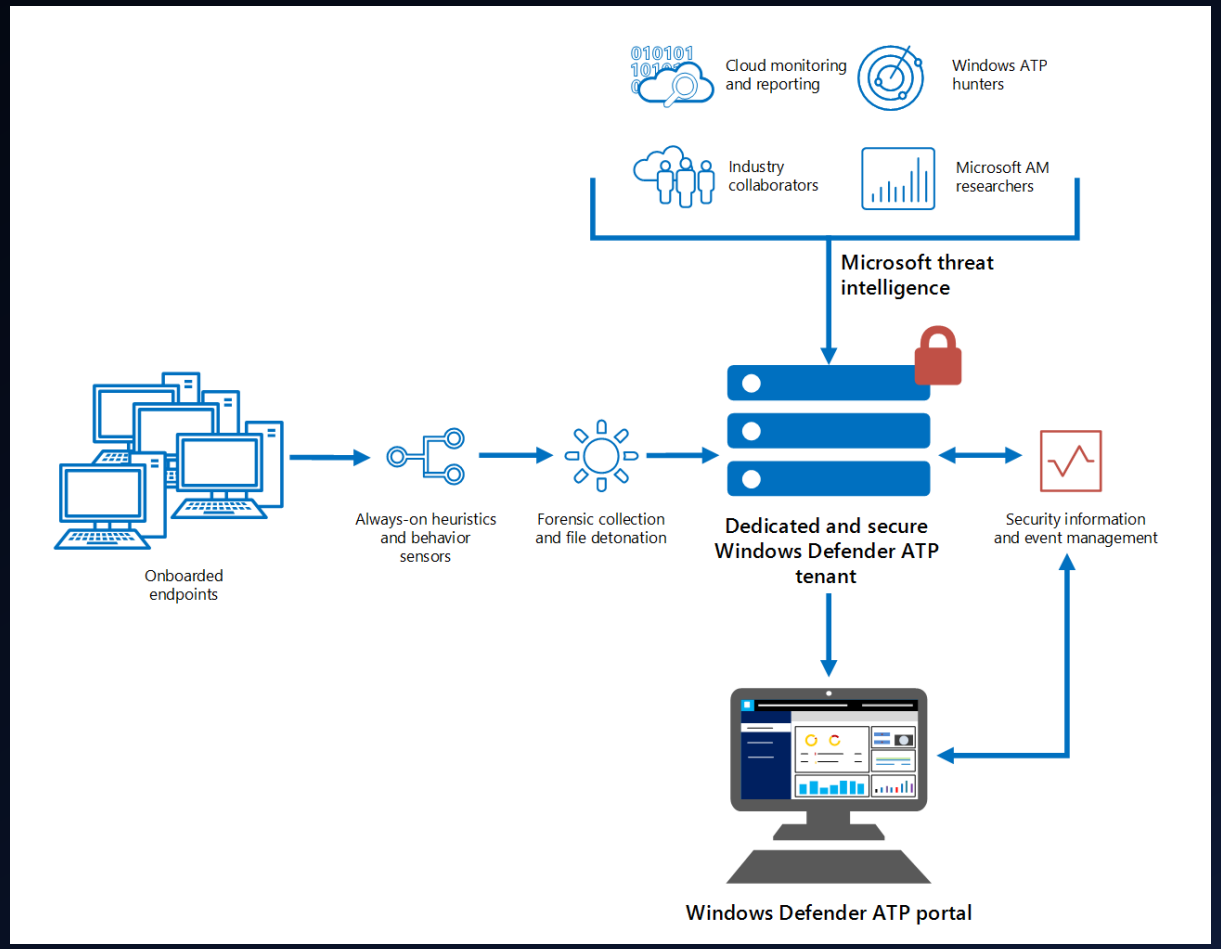


Network hardening

- Service hardening
- Device hardening
- Intrusion Prevention System & Firewall

OS hardening

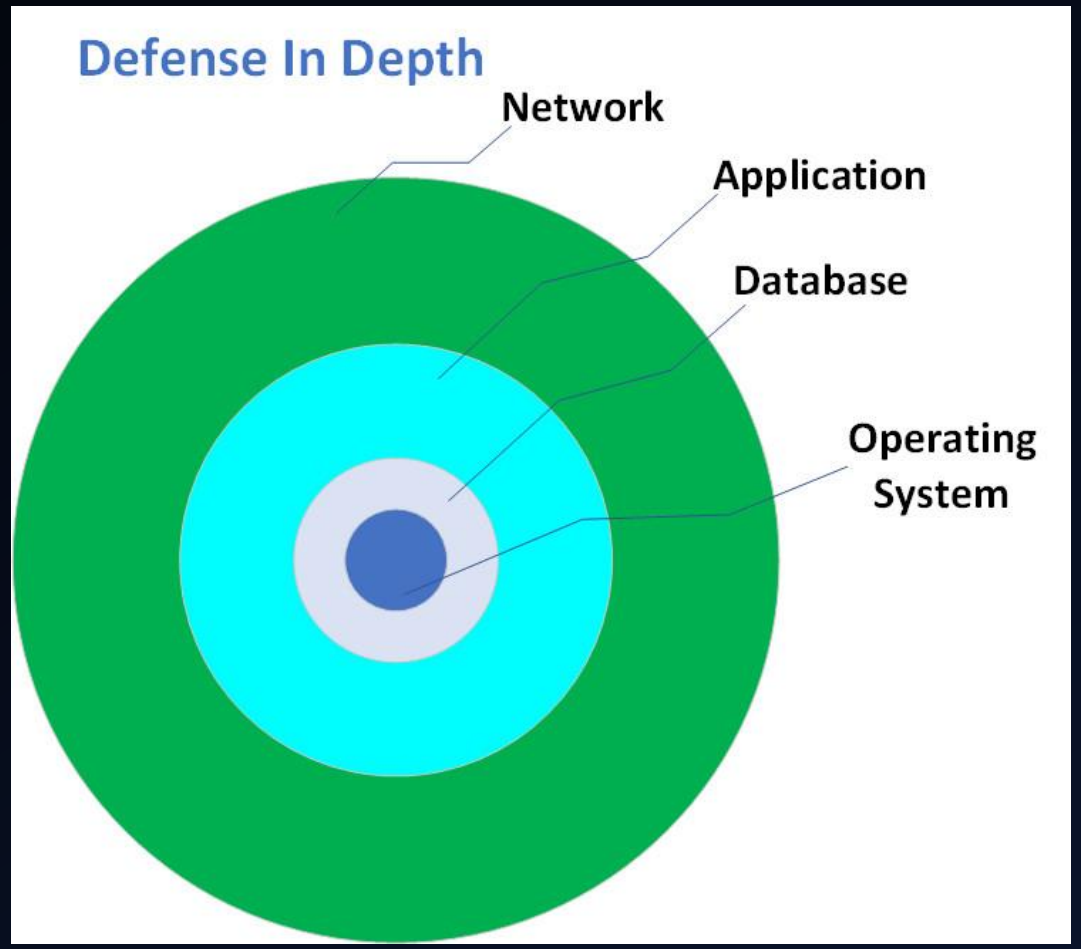
- Application hardening
- Sandbox
- Vulnerability management
- Mandatory Access Control (SE Linux)



Data Loss Prevention

- AD RMS (Active Directory Rights Management Services)
- Host Based DLP
- Network Based DLP

Defense In Depth



Questions and Answer

- Thanks

http://rnpg.ir