Misconfiguration

Objectives

- Understand what misconfiguration is
- Discuss the risks and threats around misconfiguration

What is a misconfiguration

- Misconfiguration is essentially incorrectly configuring software safeguards
- Typically web applications
- #5 on OWASP Top 10
- Can be anything else however

Examples

- Disabling default accounts - wireless
- Not setting update schedule – Windows, Linux
- Removing setup files - Wordpress
- Closing open ports - Linux
- Using insecure ports – LDAP
- Not setting a password
- Unnecessary services enabled – Linux
- Default certificates - Lenovo

Discussion

- Attackers are usually external
- Intentional or unintentional - Shodan
- Exploitability is easy since the admin “forgot” to set something up
- Can happen anywhere in the application stack
- Risks and threats vary depending on what the application has access to

Top 10 2013-A5-Security Misconfiguration Scenarios

- **Scenario #1:** The app server admin console is automatically installed and not removed. Default accounts aren't changed. Attacker discovers the standard admin pages are on your server, logs in with default passwords, and takes over.
- **Scenario #2:** Directory listing is not disabled on your server. Attacker discovers she can simply list directories to find any file. Attacker finds and downloads all your compiled Java classes, which she decompiles and reverse engineers to get all your custom code. She then finds a serious access control flaw in your application.
- **Scenario #3:** App server configuration allows stack traces to be returned to users, potentially exposing underlying flaws. Attackers love the extra information error messages provide.
- **Scenario #4:** App server comes with sample applications that are not removed from your production server. Said sample applications have well known security flaws attackers can use to compromise your server.