Security Assessment and Testing

Definitions

- War Dialing - technique to automatically scan a list of telephone numbers
- Pentesting Methodology
    - Planning
    - Reconnaissance
    - Scanning(enumeration)
    - Vulnerability Assessment
    - Exploitation
    - Reporting
- Unit Testing - low level, functions, procedures, or objects
- Installation Testing - seeing if it installs and can run
- Integration Testing - multiple components together. say there is unit test for head lights and one for turn signal. integration test would be making sure they both work at same time
- Regression Testing - testing updates, modifications, or patches
- Acceptance Testing - ensuring it meets standards and requirements
- Fuzzing - black-box testing that submits random, malformed data to see if it will crash
- Dynamic Analysis - giving program inputs to test all paths for bugs, weaknesses, vulnerabilities, etc
- Static Analysis - analyzing the source for for bugs, weaknesses, vulnerabilities, style, etc
- Risk = Threat X Vulnerability

Design and validate assessment, test, and audit strategies

Pentesting and active assessments. Once you create something, look for weaknesses or abuse cases

- Internal - usually done by checking logs, scanning internal network with vulnerability scanner, checking camera coverage, etc
- External - analyzing firewall rules, IDS/IPS, endpoint protection, fences, gates, etc
- Third-party - paying another organization to test your security for you

Conduct security control testing

- Vulnerability assessment - describes a ton of weaknesses in the system. Doesn't exploit anything
- Penetration testing - chaining together weaknesses to see what is possible. Puts theirselves in place of attackers to see what they could do
- Log reviews - manually reviewing logs or setting up log analysis tool/filter i.e. splunk
- Synthetic transactions - building scripts to simulate normal activities. this is capture a baseline and simulate traffic
- Code review and testing - manual review, static analysis, and dynamic analysis. all three should be used
- Misuse case testing - writing security tests. could write a security test to ensure the server redirects you, or that all passwords hashes used are strong
- Test coverage analysis - sees how much code you are testing or covering with dynamic analysis
- Interface testing - testing functionality of interface. ensuring user can't see any weird files, error messages, or anything unneccessary.

Collect security process data (e.g., technical and administrative)

- Account management - user accounts should be monitored, permissions checked, and passwords automatically changed
- Management review and approval - weaknesses and risk should always be taken to management before acting. determine what the best plan forward and how much risk they want to accept.
- Key performance and risk indicators - *no idea what this means*..
- Backup verification data - Information used to verify and manage should be backed up
- Training and awareness - everyone should have to take frequent awarness training and their training should be tracked
- Disaster Recovery (DR) and Business Continuity (BC) - there should be plans in place for what to do when bad things happen. Is a Hot site, cold site needed? Should everything be completely redundant?

Analyze test output and generate report

- Policies and Procedures
- Security Personel Training
- Change Management
- Architectural Reviews
- Vulnerability Reports
- Metrics reports on security
- Metrics reports on IT and remediation
- Pentest Reports

Conduct or facilitate security audits

Same thing as the first title in this section, except you are doing this for real now.

- Internal
- External
- Third-party

Home Page
To next domain! - D7 - Security Operations