АНАЛИЗ ТЕХНОЛОГИЙ ПОИСКА УЯЗВИМОСТЕЙ СОВРЕМЕННЫМИ СКАНЕРАМИ БЕЗОПАСНОСТИ

УЧЕБНЫЕ ВОПРОСЫ

- Уязвимости компьютерных систем.
- Классификация средств инструментальной проверки защищенности компьютерных систем.
- Анализ функциональных возможностей существующих сканеров безопасности и технологий, применяемых для тестирования защищенности компьютерных систем.

УЯЗВИМОСТЬ

Состояние компьютерной системы, позволяющее атакующему нарушать действующую политику безопасности компьютерной системы

Обычно различают:

- Уязвимости проектирования
- Уязвимости реализации
- Уязвимости конфигурации

КЛАССИФИКАЦИЯ СРЕДСТВ ИНСТРУМЕНТАЛЬНОЙ ПРОВЕРКИ ЗАЩИЩЕННОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

- Программы инвентаризации сетевых ресурсов
- Универсальные сканеры безопасности
- Специализированные сканеры безопасности

ПРОГРАММЫ ИНВЕНТАРИЗАЦИИ СЕТЕВЫХ РЕСУРСОВ

Предназначены для выявления доступных сетевых узлов, определения перечня запущенных на узле сетевых служб и установленного программного обеспечения

- NMAP
- AdRem NetCrunch
- Atelier Web Security Port Scanner
- MegaPing
- ScriptLogic Enterprise Security Reporter

УНИВЕРСАЛЬНЫЕ СКАНЕРЫ БЕЗОПАСНОСТИ

Как правило, включают в себя функции программ инвентаризации сетевых ресурсов, а также функции по поиску уязвимостей операционных систем и установленного программного обеспечения

- Tenable Nessus
- X-Spider
- OpenVAS
- GFI LANguard Network Security Scanner
- eEye Digital Security Retina Network Security Scanner

СПЕЦИАЛИЗИРОВАННЫЕ СКАНЕРЫ БЕЗОПАСНОСТИ

Предназначены для поиска уязвимостей в конкретных сетевых службах или программном обеспечении

- SAFETY-LAB Shadow Database Scanner
- Acunetix Web Vulnerability Scanner
- Watchfire (IBM) AppScan
- Nikto
- Atelier Web Firewall Tester

ТЕХНОЛОГИИ ПОИСКА УЯЗВИМОСТЕЙ

1. Идентификация открытых портов
2. Идентификация служб
3. Идентификация процессов
4. Анализ метаданных файлов
5. Анализ содержимого конфигурационных файлов
6. Анализ содержимого файлов
7. Анализ реестра ОС Windows
8. Идентификация установленного ПО
9. Идентификация установленных пакетов обновлений в ОС Windows
10. Анализ списка пользователей и групп ОС Windows

ТЕХНОЛОГИИ ПОИСКА УЯЗВИМОСТЕЙ

11. Анализ баннеров
12. Проверка доступности заданного CGI-сценария
13. Анализ результата обращения к заданному CGI-сценарию
14. Автоматический поиск CGI-сценариев
15. Автоматический поиск XSS-уязвимостей
16. Автоматический поиск уязвимостей SQL-инъекций
17. Автоматический поиск уязвимостей Directory Traversal
18. Автоматический поиск уязвимостей Command Injection
19. Автоматический поиск уязвимостей File Inclusion
20. Автоматический поиск уязвимостей по базам данных уязвимостей (CVE, CWE, MS BulletIn, OWASP, etc)