Вопросы по курсу

«Тестирование безопасности компьютерных систем»

Магистратура «Программное обеспечение вычислительных сетей», ***1 курс***
2020-2021 уч год

1. Сегментирование сетей на канальном уровне. Стандарт VLAN.
2. Семейство протоколов IPSec. Основные топологии.
3. Семейство протоколов IPSec. Протоколы AH и ESP.
4. Семейство протоколов IPSec. Базы данных SPD и SAD.
5. Семейство протоколов IPSec. Аутентификация сторон и обмен ключа в протоколе IKE, фаза I.
6. Семейство протоколов IPSec. Аутентификация сторон и обмен ключа bbпротоколе IKE, фаза II.
7. Семейство протоколов IPSec. Использование IPSec совместно с NAT. Способы определения сбоя противоположной стороны.
8. Способы классификации систем обнаружения вторжений (IDS).
9. Сравнение сетевых, хостовых и прикладных IDS.
10. Сравнение сигнатурных и аномальных IDS.
11. Инструментальные средства анализа уязвимостей.
12. Протокол HTTP. Типы cookies.
13. Протокол HTTP. Принцип Same-origin policy.
14. Протокол HTTP. Стандарт CSP.
15. Протокол HTTP. Стандарт CORS.
16. Последовательность действий при выполнении SQL Injection.
17. Способы обхода проверок наличия SQL Injection.
18. Способы предотвращения SQL Injection.
19. Классификация уязвимостей типа Cross-site Scripting.
20. Предотвращение уязвимостей типа Cross-site Scripting.
21. Уязвимость межсайтовой подделки запросов (Cross Site Request Forgery – CSRF) и способы ее предотвращения.
22. Уязвимость модификации пользовательского интерфейса (Clickjacking) и способы ее предотвращения.
23. Основные превентивные технологии обеспечения безопасности веб-приложений (по версии OWASP).
24. Основные возможности межсетевого экрана прикладного уровня для протокола HTTP (WAF) ModSecurity.
25. Технологии создания единого входа, стандарт SAML.
26. Протокол авторизации OAuth 2.0.
27. Способы управления доступом, дискреционный и мандатный способы управления доступом, RBAC.