Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт зачета

по дисциплине «Тестирование на проникновение», 7 семестр

1. Методика оценки

Зачет проводится в устной (письменной) форме, по билетам. Билет состоит из 2 вопросов и формируется по следующему правилу:

- первый вопрос выбирается из диапазона вопросов 1-15;
- второй вопрос из диапазона вопросов 16-30.

Таким образом, проверяются результаты обучения по дисциплине, соотнесенные с установленными в программе индикаторами достижения компетенций.

На зачете преподаватель вправе задавать студенту уточняющие и дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____
к зачету по дисциплине «Тестирование на проникновение»

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой ____ _____ должность, ФИО
(подпись)
(дата)

2. Критерии оценки результатов обучения, соотнесенных с уровнями освоения индикаторов достижения компетенций

Ответ на билет для зачета засчитывается на **продвинутом** уровне, если студент проводит сравнительный комплексный анализ материала, выявляет проблемы, предлагает механизмы их решения, представляет количественные характеристики определенных процессов, приводит конкретные примеры. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций не

содержит пробелов. Установленные в программе компетенции сформированы в полном объеме. Оценка составляет *от* 18 *до* 20 *баллов.*

Ответ на билет для зачета засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, дает характеристику процессов, явлений, проводит анализ причин, условий, способен представить количественные и качественные характеристики процессов. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит несущественные пробелы. Установленные в программе компетенции сформированы на базовом уровне. Оценка составляет *от* 1*4 до* 17 *баллов.*

Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит пробелы. Установленные в программе компетенции сформированы на пороговом уровне. Оценка составляет *от* 1*0 до* 13 *баллов.*

Ответ на билет для зачета считается **неудовлетворительным** (ниже порогового уровня), если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений. Совокупность результатов обучения по дисциплине (модулю) и соотнесенных с ними индикаторов достижения компетенций содержит существенные пробелы. Установленные в программе компетенции не сформированы. Оценка составляет *менее* 1*0 баллов.*

3. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета составляет от 10 до 20 баллов включительно. Сумма менее 10 баллов признается неудовлетворительным результатом промежуточной аттестации по дисциплине (модулю).

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, установленными в НГТУ.

4. Вопросы к зачету по дисциплине «Тестирование на проникновение»

1. Чем легальное тестирование на проникновение отличается от несанкционированного взлома с юридической точки зрения?
2. Какие документы необходимо оформить перед началом работ по тестированию на проникновение?
3. Какова юридическая ответственность пентестера при выходе за рамки согласованной области тестирования?
4. Какие этапы включает процесс организации тестирования на проникновение?
5. Что такое область тестирования и почему его четкое определение критически важно?
6. Какие роли и обязанности участников проекта по тестированию на проникновение вы знаете?
7. Какие основные методологии тестирования на проникновение существуют?
8. Чем отличаются подходы black box, white box и gray box тестирования? В каких случаях применяется каждый из них?
9. Что такое kill chain (Cyber Kill Chain) и как эта модель применяется в пентесте?
10. Какие фазы включает процесс тестирования на проникновение?
11. Чем тестирование на проникновение отличается от оценки уязвимостей и red team operations?
12. Какие компоненты входят в типичную серверно-клиентскую архитектуру веб-приложений?

13. Как взаимодействуют клиентская и серверная части в многоуровневой архитектуре?
14. Какие уязвимости характерны для клиентской части и какие для серверной?
15. Какие особенности безопасности имеют REST API и SOAP веб-сервисы? Какие уязвимости характерны для API?
16. Что такое OWASP TOP 10 и как часто обновляется этот список?
17. Опишите уязвимость A01: Broken Access Control и методы её эксплуатации.
18. Что такое криптографические сбои (A02: Cryptographic Failures) и как они проявляются?
19. Какие уязвимости инъекций (A03: Injection) вы знаете?
20. Что такое небезопасный дизайн (A04: Insecure Design) и как он отличается от ошибок реализации?
21. Опишите уязвимости конфигурации безопасности (A05: Security Misconfiguration) и методы их выявления.
22. Что такое уязвимые и устаревшие компоненты (A06: Vulnerable and Outdated Components) и как управлять зависимостями?
23. Как работают уязвимости идентификации и аутентификации (A07: Identification and Authentication Failures)?
24. Какие инструменты используются для тестирования веб-сервисов на уязвимости?
25. Как осуществляется эксплуатация SQL-инъекций в веб-приложениях?
26. Что такое APM (Application Performance Monitoring) и какие уязвимости могут быть в системах мониторинга?
27. Как происходит эскалация привилегий в Windows?
28. Как происходит эскалация привилегий в Linux?
29. Какие методы пост-эксплуатации применяются для закрепления в системе и перемещения по сети?
30. Как используется Metasploit Framework для эксплуатации уязвимостей и какие альтернативные фреймворки существуют?