



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ГЕОДЕЗИИ И КАРТОГРАФИИ
(МИИГАиК)

Факультет геоинформатики и информационной безопасности
Кафедра информационно-измерительных систем



**ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ**

Сертификат: 5387FD2AF5B17FED816FDE9A1D4973B1
Владелец: Степанченко Алексей Леонидович
Действителен: с 21.07.2025 по 14.10.2026

«УТВЕРЖДАЮ»

Проректор
А. Л. Степанченко
16 февраля 2024 г.

**ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
«Б1.В.04 ИНСТРУМЕНТЫ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ»**

Уровень высшего образования: магистратура

Направление подготовки: 10.04.01 Информационная безопасность

Направленность(профиль) подготовки: Защита информации в геоинформационных системах
и системах сбора пространственных данных

Квалификация (степень) выпускника: магистр

Форма обучения: очная

Год набора (приема на обучение): 2024

Срок получения образования: 2 года

Объем:
в зачетных единицах: 4 з.е.
в академических часах: 144 ак.ч.

Москва, 2024

Разработчики:

Преподаватель кафедры Информационно-измерительных систем
Сутягин Д. Д.

Фонд оценочных средств по дисциплине (модулю) составлен в соответствии с требованиями ФГОС ВО по направлению подготовки 10.04.01 Информационная безопасность, утвержденного приказом Минобрнауки от 26.11.2020 № 1455

Согласование и утверждение

№	Подразделение	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	факультет Геоинформатики и информационной безопасности	Председатель ученого совета факультета	Матерухин А. В.	Рассмотрено	14.12.2023, № 7-23

1. Планируемые результаты обучения, соотнесенные с планируемыми результатами освоения образовательной программы

ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)

ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности

Знать:

ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности

ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем

Уметь:

ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем

Владеть:

ПК-2.1/Нв1 навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных

Знать:

ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения

ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия

Уметь:

ПК-2.2/Ум2 выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем

Владеть:

ПК-2.2/Нв1 навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия

ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах

Знать:

ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности

Уметь:

ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

Владеть:

ПК-2.3/Нв1 навыками работы с инструментами анализа защищенности

2. Показатели и критерии оценивания компетенций

Планируемые результаты освоения программы	Уровень овладения	Критерии оценивания (перечень сформированных ИДК/ЗУВ по уровням освоения)
ПК-2 Способен проводить анализ безопасности компьютерных систем (включая выполнение научно-исследовательских работ по этой тематике)	Повышенный	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем Уметь: ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем Владеть: ПК-2.1/Нв1 навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия Уметь: ПК-2.2/Ум2 выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем Владеть: ПК-2.2/Нв1 навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности

	Уметь: ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах Владеть: ПК-2.3/Нв1 навыками работы с инструментами анализа защищенности
Базовый	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности Уметь: ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения Уметь: ПК-2.2/Ум2 выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности Уметь: ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах

	Пороговый	ИДК ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности Знать: ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ИДК ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных Знать: ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ИДК ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах Знать: ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности
--	-----------	---

3. Шкала оценивания

Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
--------	---

Отлично	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем ПК-2.1/Нв1 навыками подготовки аналитического отчета по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия ПК-2.2/Ум2 выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем ПК-2.2/Нв1 навыками анализа программно-аппаратных средств защиты с целью определения уровня обеспечиваемых ими защищенности и доверия ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Нв1 навыками работы с инструментами анализа защищенности
Хорошо	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Ум2 оценивать реальный уровень защищенности анализируемых компьютерных систем ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия ПК-2.2/Ум2 выбирать инструменты тестирования на проникновение под конкретные условия при анализе безопасности компьютерных систем

	ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности ПК-2.3/Ум1 подготавливать аналитические отчеты по результатам анализа уровня защищенности и доверия в компьютерных системах
Удовлетворительно	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности
Неудовлетворительно	Результаты обучения не сформированы на достаточном уровне
Оценка	Критерии оценивания (перечень сформированных ИДК/ЗУВ)
Зачтено	ПК-2.1 Обладает пониманием способов научного анализа применяемых методов и средств защиты информации для оценки их соответствия политике безопасности и эффективности ПК-2.1/Зн2 основные нормативные документы в области анализа безопасности компьютерных систем ПК-2.1/Зн1 способы научного анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности и оценке их эффективности ПК-2.2 Анализирует программно-аппаратные средства защиты с целью определения уровня обеспечиваемых ими защищенности и доверия при проведении научных исследований и сборе экспериментальных данных ПК-2.2/Зн3 классы инструментов тестирования на про-никновения, принципы их действия ПК-2.2/Зн2 основные методы реализации угроз безопасности информации и способы их предотвращения ПК-2.3 Подготавливает аналитические отчеты по результатам проведенного анализа уровня защищенности и доверия в компьютерных системах ПК-2.3/Зн1 методы и инструменты оценки уровня защищенности
Не зачтено	Результаты обучения не сформированы на достаточном уровне

4. Контрольные мероприятия по дисциплине

Вид контроля	Форма контроля/Оценочное средство
Текущий контроль	Тестирование
Промежуточная аттестация	Зачет Зачет с оценкой

№ п/п	Наименование раздела	Контролируемые ИДК	Вид контроля/ используемые оценочные материалы	
			Текущий	Промежут. аттестация
1	Инструменты сбора информации о системах и сетях	ПК-2.1	Тестирование	Зачет Зачет с оценкой
2	Инструменты эксплуатации систем и сетей	ПК-2.1 ПК-2.2	Тестирование	Зачет Зачет с оценкой
3	Инструменты закрепления в системе и сети	ПК-2.1 ПК-2.2	Тестирование	Зачет Зачет с оценкой
4	Инструменты эксфильтрации данных	ПК-2.1 ПК-2.2	Тестирование	Зачет Зачет с оценкой
5	Применение инструментов тестирования на проникновение в лабораторных условиях	ПК-2.1 ПК-2.2 ПК-2.3	Тестирование	Зачет Зачет с оценкой

5. Порядок проведения промежуточной аттестации

Порядок проведения промежуточной аттестации регламентируется локальными нормативными актами Университета:

- Положением о формах, периодичности, порядке текущего контроля успеваемости и промежуточной аттестации обучающихся по основным образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.6 «Организация и проведение промежуточной аттестации».
- Положением о порядке осуществления образовательного процесса, проведения текущего контроля успеваемости и промежуточной аттестации обучающихся с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет геодезии и картографии», п.8 «Проведение промежуточной аттестации с применением ЭО и ДОТ».

Промежуточная аттестация: Зачет, 3 семестр.

Зачет оценивается по следующей шкале:

- оценка «зачтено» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний; а также автоматически, когда обучающийся за промежуточную аттестацию имеет оценки «отлично»;
- оценка «не зачтено» выставляется обучающемуся в случае наличия грубых ошибок при

изложении ответа на основные вопросы программы, свидетельствующих о неправильном понимании предмета; при решении практических задач показано незнание способов их решения, материал изложен беспорядочно и неуверенно.

Промежуточная аттестация: Зачет с оценкой, 4 семестр.

Зачет оценивается по пятибалльной шкале:

- зачтено с оценкой «отлично» выставляется, если обучающийся имеет глубокие, исчерпывающие знания в объеме освоенной программы; знание основной (обязательной) литературы; дает правильные и уверенные ответы, свидетельствующие о наличии твердых знаний и навыков в использовании технических средств; полное, четкое, грамотное и логически стройное изложение материала; демонстрирует свободное применение теоретических знаний при анализе практических вопросов;
- зачтено с оценкой «хорошо» выставляется обучающемуся в случае соблюдения тех же требований, но наличии в ответе обучающегося по некоторым перечисленным показателям недостатков принципиального характера, что вызывает замечания или поправки преподавателя;
- зачтено с оценкой «удовлетворительно» выставляется обучающемуся в случае соблюдения тех же требований, но в случае наличия в ответе ошибок, необходимости существенной помощи в виде поправок и наводящих вопросов преподавателя;
- не зачтено («не удовлетворительно») – обучающийся не смог ответить на 2/3 вопросов; не справился с практическим заданием или выполнено менее 50 % практических заданий.

6. Оценочные материалы текущего контроля

Раздел 1. Инструменты сбора информации о системах и сетях

Контролируемые ИДК: ПК-2.1

Тема 1.1. Инструменты сбора информации о системах и сетях

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какие инструменты можно использовать для SYN-сканирования:
 1. nmap
 2. sqlmap
 3. acunetix
2. Выберите C2 фреймворк:
 1. nessus
 2. cobalt strike
 3. httpx
3. С какого tcp флага начинается трехэтапное tcp рукопожатие (3-way tcp handshake):
 1. syn
 2. fin
 3. rst
 4. ack
4. Каким tcp флагом сбрасывается tcp соединение:
 1. syn
 2. fin
 3. rst
 4. ack

Раздел 2. Инструменты эксплуатации систем и сетей

Контролируемые ИДК: ПК-2.1 ПК-2.2

Тема 2.1. Инструменты эксплуатации систем и сетей

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Каким tcp флагом завершается tcp соединение:
 1. syn
 2. fin
 3. rst
 4. ack
2. Что из этого не является функцией burp suite:
 1. перехватывающий прокси-сервер
 2. автоматический сбор информации об архитектуре приложения
 3. автоматическое сканирование уязвимостей
 4. сканирование сетевых портов
3. Как называется утилита Burp Suite для сбора информации об архитектуре приложения:
 1. Spider
 2. Intruder
 3. Repeater
 4. Scanner
4. Как называется утилита Burp Suite для автоматического поиска уязвимостей:
 1. Spider
 2. Intruder
 3. Repeater
 4. Scanner

Раздел 3. Инструменты закрепления в системе и сети

Контролируемые ИДК: ПК-2.1 ПК-2.2

Тема 3.1. Инструменты закрепления в системе и сети

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Как называется утилита Burp Suite для автоматической атаки, такой как, например, подбор паролей:
 1. Spider
 2. Intruder
 3. Repeater
 4. Scanner
2. Что из этого не является протоколом для подключения к удаленному рабочему столу:
 1. vnc
 2. rdp
 3. ftp
3. На каком уровне модели OSI работает протокол ICMP:
4. На каком уровне сетевой модели OSI может вести сканирование nmap:

Раздел 4. Инструменты эксфильтрации данных

Контролируемые ИДК: ПК-2.1 ПК-2.2

Тема 4.1. Инструменты эксфильтрации данных

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Какой флаг в TCP пакете отправляется при инициировании нового соединения:
2. Как называется атака, в ходе которой злоумышленник размещает на своём сервере файл шаблона Word (.dotm) с вредоносными макросами:
3. Какой инструмент может использоваться для проксирования собственного трафика (в том числе зашифрованного) с целью его исследования:
4. Какой инструмент может использоваться для автоматического поиска уязвимостей типа SQL-инъекция:

Раздел 5. Применение инструментов тестирования на проникновение в лабораторных условиях

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3

Тема 5.1. Применение инструментов тестирования на проникновение в лабораторных условиях

Форма контроля/оценочное средство: Тестирование

Вопросы/Задания:

1. Для чего используется утилита repeater в составе Burp Suite:
2. Можно ли запускать графические утилиты на удаленном сервере используя SSH:
3. Что такое meterpreter:
4. Какую технику можно применить для сокрытия полезной нагрузки от антивируса:

7. Оценочные материалы промежуточной аттестации

3 семестр, Зачет

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3

Вопросы/Задания:

1. Обзор популярных сетевых сканеров
2. Принципы работы сетевых сканеров
3. Пассивное и активное сетевое сканирование. Разница.
4. Возможные состояния сетевых хостов, портов
5. Принцип действия сетевых сканеров, направленных на сканирование большой (больше 1000 хостов) подсети
6. Типы инструментов, используемых для пассивного сканирования
7. Типы инструментов, используемых для активного сканирования
8. Ресурсы, которые можно использовать для OSINT
9. Основные источники информации в OSINT
10. Автоматизация OSINT
11. Инструменты, используемые для разведки, разрешения доменных зон, имен

12. Обзор сканеров сетевых путей
13. Принципы действия сканеров сетевых путей
14. Инструменты, используемые для веб-фаззинга
15. Автоматические сканеры уязвимостей
16. Базы данных уязвимостей
17. Инструменты для автоматической эксплуатации уязвимостей
18. Что такое PoC в терминах эксплуатации уязвимостей?
19. Использование существующих PoC
20. Написание собственных PoC к известным уязвимостям
21. Классы задач веб-эксплуатации
22. Инструменты и техники веб-эксплуатации
23. Что такое полезная нагрузка?
24. Принципы генерации полезной нагрузки
25. Инструменты автоматической генерации полезной нагрузки
26. Принципы закрепления в системах и сетях
27. Принципы действия C2 фреймворков
28. Легитимные инструменты, которые возможно использовать для закрепления в системах и сетях
29. Основные проблемы закрепления в системах и сетях, угрозы обнаружения
30. Что такое эксфильтрация данных?
31. Легитимные инструменты и каналы для эксфильтрации данных
32. Соккрытие факта эксфильтрации данных
33. Нестандартные инструменты и каналы, которые можно использовать для эксфильтрации данных

4 семестр, Зачет с оценкой

Контролируемые ИДК: ПК-2.1 ПК-2.2 ПК-2.3

Вопросы/Задания:

1. Объясните основные отличия и применения методов сбора информации из открытых источников (OSINT) в тестировании на проникновение.
2. Какие инструменты и техники используются для пассивного сканирования сетей и систем?
3. В чем состоят риски активного сканирования и как минимизировать его обнаружение?
4. Опишите этапы и инструменты активного сканирования для выявления уязвимостей.
5. Как строится и применяется PoC (Proof of Concept) в эксплуатации известных уязвимостей?
6. Какие сложности возникают при адаптации и модернизации существующих PoC для новых целей?
7. Какие инструменты являются стандартом для веб-эксплуатации уязвимостей в современных приложениях?
8. Как работает механизм генерации полезной нагрузки для дальнейшего распространения атаки?
9. Какие риски и преимущества использования автоматизированных инструментов фишинга?
10. Какие принципы лежат в основе C2 (Command and Control) фреймворков и как они используются в закреплении?
11. Сравните техники закрепления в системах Linux и Windows. Какие особенности у каждой ОС учитываются?
12. Какие инструменты применяются для сканирования систем с целью поиска уязвимостей повышения привилегий?
13. Объясните легитимные способы и инструменты эксфильтрации данных при тестировании.
14. Какие техники используются для сокрытия факта эксфильтрации данных?
15. Опишите процесс создания лабораторной среды для тестирования инструментов на проникновение.
16. Какие ключевые аспекты необходимо учитывать при применении инструментов тестирования на различных этапах проникновения?
17. Как организовать комплексное применение инструментов тестирования на проникновение при оценке безопасности систем и сетей?

18. В чем заключаются основные отличия между ручным и автоматическим тестированием на проникновение?

19. Какие стадии проверки физической безопасности включаются в тестирование на проникновение и какие инструменты для этого используются?

20. Объясните подходы к сбору и анализу данных в рамках OSINT и их влияние на последующее тестирование.

21. Каково значение нейронных сетей, например LSTM, для анализа сетевого трафика в контексте IDS и тестирования на проникновение?

22. Что такое honeypot и как он интегрируется в процесс тестирования и анализа атак?

23. Охарактеризуйте основные возможности и ограничения Metasploit Framework при эксплуатации уязвимостей.

24. Опишите алгоритмы работы сетевых сканеров, таких как Nmap, включая различные виды сканирования портов.

25. Какие методы используются для обфускации и маскировки фишинговых кампаний?

26. Какие существуют виды атак с повышением привилегий и какие инструменты им соответствуют?

27. Объясните принципы работы и применения программных средств для мониторинга и предупреждения эксфильтрации данных.

28. В чем заключаются особенности организации виртуальных лабораторий для борьбы с данным видом атак?

29. Какие проблемы возникают при использовании готовых PoC в реальной инфраструктуре?

30. Как можно интегрировать инструменты тестирования на проникновение с системами управления безопасностью предприятия?

31. Опишите основные компоненты и взаимодействия C2-фреймворка в процессе эксплуатации и закрепления.

32. Какие сетевые протоколы чаще всего используются для скрытой передачи эксфильтрованных данных?

33. Как оценить эффективность и безопасность используемых инструментов тестирования на проникновение?

34. Что такое «многоступенчатая атака» (APT), и какие инструменты применяются для её имитации и тестирования?

35. Какие законодательные и этические аспекты необходимо учитывать при проведении тестирования на проникновение?

