Муниципальное автономное общеобразовательное учреждение
Белоярского района
«Средняя общеобразовательная школа № 1 г. Белоярский»

РАССМОТРЕНО
на заседании педагогического
совета школы
Протокол № 20 от 17.12.2024 г.

УТВЕРЖДАЮ
Директор _____ Е.А.Пакулев
Приказ по СОШ №1 г.Белоярский
от 17.12.2024, №1292

Подписано цифровой подписью:
Пакулев Евгений Анатольевич
Дата: 2025.01.22 12:37:28 +05'00'

Дополнительная общеобразовательная общеразвивающая программа «Кибербезопасность и криптография»

Возраст учащихся: 16-18 лет

Срок реализации программы: 2024-2025 учебный год

город Белоярский, 2024 год

Автор программы:

Бутаков Юрий Владимирович,учитель информатики,высшая квалификационная категория, СОШ № 1 г.Белоярский

1. Пояснительная записка

Введение

О важности сохранения информации в тайне знали уже в древние времена, когда с появлением письменности появилась и опасность прочтения её нежелательными лицами. На сегодняшний день количество передаваемой информации возросло в миллионы и миллиарды раз, поэтому актуальность её защиты от несанкционированного доступа возрастает с каждым новым битом информации.

Основным содержанием данного курса является формирование умений и навыков по защите личного информационного пространства,информационно-коммуникационных систем, современных приемов шифрования информации(криптография).

1.1. Программа разработана в соответствии со следующими нормативно-правовыми актами:

- Федеральный закон РФ 273-ФЗ «Об образовании в Российской Федерации» от 29.12.2012 г.;
- Указ Президента Российской Федерации от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации» (с изменениями и дополнениями от 15 марта 2021 г.;
- Указ Президента Российской Федерации от 09.05.2017 № 203 «О
- Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»;
- Указ Президента Российской Федерации от 07.05.2024 № 309 «О национальных целях развития Российской Федерации на период до 2030 года» и на перспективу до 2036 года;
- Постановление Правительства Российской Федерации от 18 апреля 2016 г. № 317 «О реализации Национальной технологической инициативы» (в ред. от 16 мая 2022 года);

- Стратегия развития воспитания в Российской Федерации на период до 2025 года, утверждённая Распоряжением Правительства Российской Федерации от 29 мая 2015 г. № 996-р.;
- Приказ Министерства науки и высшего образования РФ и Министерства просвещения РФ от 30 июня 2020 г. № 845/369 «Об утверждении Порядка зачета организацией, осуществляющей образовательную деятельность, результатов освоения обучающимися учебных предметов, курсов, дисциплин (модулей), практики, дополнительных образовательных программ в других организациях, осуществляющих образовательную деятельность»;
- Приказ Министерства науки и высшего образования РФ и Министерства просвещения РФ от 5 августа 2020 г. № 882/391 «Об организации и осуществлении образовательной деятельности при сетевой форме реализации образовательных программ» (с изменениями и дополнениями от 1 1 февраля 2022 года);
- Приказ Министерства просвещения РФ от 27 июля 2022 г. № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;
- «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодёжи». Постановление Главного государственного санитарного врача РФ от 28 сентября 2020 года № 28 «Об утверждении санитарных правил СП 2.4.3648-20».
- Концепция развития системы дополнительного образования детей Ханты-Мансийского автономного округа - Югры до 2030 г., утвержденная распоряжением Правительства Российской Федерации от 31.03.2022 № 678-р.

1.2. Направленность: техническая.

1.3. Актуальность программы:

Актуальность данной программы состоит в том, что последнее время сообщения об атаках на информацию, о хакерах и компьютерных взломах наполнили все средства массовой информации. Дать определение этому действию

на самом деле очень сложно, поскольку информация, особенно в электронном виде, представлена сотнями различных видов.

С массовым внедрением компьютеров во все сферы деятельности человека объем информации, хранимой в электронном виде, вырос в тысячи раз. А с появлением компьютерных сетей даже отсутствие физического доступа к компьютеру перестало быть гарантией сохранности информации.

Понятие «Безопасность» охватывает широкий круг интересов, как отдельных лиц, так и целых государств. В наше мобильное время цифровых технологий, когда интернет проник во все сферы деятельности человека: начиная от пересылки SMS и заканчивая базами данных огромных предприятий и организаций, системами управления автоматизированными процессами запусками ракет и т.д., видное место отводится проблеме информационной безопасности, обеспечению защиты конфиденциальной информации.

Одним из способов защиты информации заключался в преобразовании смыслового текста в некий набор хаотических знаков (или букв алфавита). Получатель данного донесения имел возможность преобразовать его в то же самое осмысленное сообщение, если обладал ключом к его построению. Этот способ защиты информации называется криптографическим. Криптография – (от др.-греч. κρυπτός — скрытый и γράφω — пишу) - «скрыто пишу». По утверждению ряда специалистов криптография по возрасту - ровесник египетских пирамид. В документах древних цивилизаций - Индии, Египта, Месопотамии - есть сведения о системах и способах составления шифрованных писем.

Новизной и отличительной особенностью программы является формирования у будущих специалистов компетенций в области обеспечения информационной безопасности, правовых аспектов информационной безопасности, кибербезопасности, а также получения базовых знаний по криптографии и элементам сетевой безопасности, обеспечения информационной безопасности личного пространства.

Педагогическая целесообразность настоящей программы заключается в том, чтов рамках реализации дополнительной образовательной программы,

обучающиеся получать метазнания, то есть способность оперировать методами и приемами познания, и метаумения - навыки практического мышления, систематизации и обобщения, анализа информации, критического и технического мышления, а также поиска альтернативных вариантов достижения поставленных целей.

Наряду с этим использование различных инструментов развития гибких навыков обучающихся (игропрактика, командная работа) в сочетании с развитием у них предметных умений позволит сформировать у школьника целостную систему знаний, умений и навыков.

1.4. Цель программы – сформировать у обучающихся компетенций в областях:

○ обеспечение информационной безопасности;

○ правовые аспекты информационной безопасности;

○ криптография;

○ сетевая безопасность;

○ безопасность личного информационного пространства.

● обеспечение условий для профилактики негативных тенденций в развитии информационной культуры учащихся, повышения защищённости детей от информационных рисков и угроз;

● формирование навыков своевременного распознавания онлайн-рисков (технического, контентного, коммуникационного, потребительского характера

Задачи программы:

Обучающие:

● создать условия для формирования умений, необходимых для различных форм безопасной коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) с различными целями и ответственного отношения к взаимодействию в современной информационно-телекоммуникационной среде;

● дать представление о видах и способах распространения вредоносных кодов, способов защиты личных устройств;

● познакомить со способами защиты от противоправных посягательств в Интернете, защиты личных данных;

● познакомить со стандартами информационного взаимодействия систем;

● познакомить с конструкциями типичных элементов линий передачи информации;

● сформировать умения задавать базовые параметры, в том числе параметры защиты от несанкционированного доступа к операционным системам, а так же настройки конфигурации операционных систем сетевых устройств;

● познакомить с архитектурой, устройством и функционированием вычислительных систем;

● сформировать знания в области обеспечения защиты информации в вычислительных сетях и системах;

● сформировать знания в области типовых и программно-аппаратных средств защиты информации в операционных системах.

Развивающие:

- развивать мыслительные, творческие, коммуникативные способности;
- развивать творческую инициативу и самостоятельность;

Воспитательные:

- воспитывать умение работать в команде, эффективно распределять обязанности;
- воспитывать творческое отношение к выполняемой работе;
- формировать потребность в творческой деятельности, стремление к самовыражению через техническое творчество.

1.5. Отличительная особенность программы:

Программа направлена на подготовку к решению задач олимпиады НТО с использованием новейшего программного обеспечения и стендов, не имеющих аналогов, а также получения знаний сверх школьной программы.

1.6. Адресат программы:

Программа рассчитана на обучающихся 16-18 лет (10-11 классы), мотивированных на получение повышенных образовательных результатов и участие в конкурсных мероприятиях НТО.

1.7. Объем программы: 72 академических часа.

1.8. Форма и режим занятий:Занятия проводятся в очном формате - 1 раз в неделю по 2 академических часа.

Формы организации учебных занятий:

- инструктаж;
- практикум (работа в специально оборудованном помещениях и полигонах);
- компьютерный практикум;
- тренинг занятия

Формы контроля:

- практические работы;
- соревнования;
- мини-проекты.

Методы обучения:

- Познавательный (восприятие, осмысление и запоминание учащимися нового материала с привлечением наблюдения готовых примеров, моделирования, изучения иллюстраций, восприятия, анализа и обобщения демонстрируемых материалов).
- Метод проектов (при усвоении и творческом применении навыков и умений в процессе разработки собственных моделей).
- Систематизирующий (беседа по теме, составление систематизирующих таблиц, графиков, схем и т.д.).
- Контрольный метод (при выявлении качества усвоения знаний, навыков и умений и их коррекция в процессе выполнения практических заданий).

Форма организации работы обучающихся

- Групповая работа;
- Работа в парах;

- Индивидуальная работа;
- Индивидуально–групповая работа.

1.9. Уровень освоения программы: базовый

1.10. Планируемые результаты

Личностные

● сформированность основ саморазвития и самовоспитания в соответствии с общечеловеческими ценностями и идеалами гражданского общества; готовность и способность к самостоятельной, творческой и ответственной деятельности;

● толерантное сознание и поведение в поликультурном мире, готовность и способность вести диалог с другими людьми, достигать в нем взаимопонимания, находить общие цели и сотрудничать для их достижения, способность противостоять идеологии экстремизма, национализма, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам и другим негативным социальным явлениям;

● навыки сотрудничества со сверстниками, детьми младшего возраста, взрослыми в образовательной, общественно полезной, учебно-исследовательской, проектной и других видах деятельности;

● нравственное сознание и поведение на основе усвоения общечеловеческих ценностей;

● готовность и способность к образованию, в том числе самообразованию, на протяжении всей жизни; сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности;

● осознанный выбор будущей профессии и возможностей реализации собственных жизненных планов; отношение к профессиональной деятельности как возможности участия в решении личных, общественных, государственных, общенациональных проблем;

● принятие и реализацию ценностей здорового и безопасного образа жизни правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Предметные

Выпускник научится:

● безопасно использовать средства коммуникации;

● безопасно использовать ресурсы интернета;

● идентифицировать типичные инциденты;

● задавать базовые параметры, в том числе параметры защиты от несанкционированного доступа к операционным системам;

● настраивать и управлять сетевыми устройствами;

● использовать процедуры восстановления данных;

● определять точки восстановления данных;

● производить мониторинг администрируемых сетевых устройств информационно-коммуникационных систем;

● применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры;

● устанавливать и настраивать параметры сетевых протоколов, реализованных в телекоммуникационном оборудовании;

● применять программно-аппаратные средства защиты информации в операционных системах;

● применять антивирусные средства защиты информации в операционных системах;

● анализировать компьютерную систему с целью определения уровня защищенности;

● использовать типовые криптографические средства защиты информации;

● классифицировать и оценивать угрозы информационной безопасности;

● изготавливать защищенное техническое средство или систему обработки информации.

Выпускник овладеет:

● основами правовых аспектов использования компьютерных программ и работы в Интернете;

● представлениями о влиянии информационных технологий на жизнь человека в обществе;

● знаниями об "операционных системах" и основных функциях операционных систем;

● знаниями об общих принципах разработки и функционирования интернет-приложений;

● представлениями о компьютерных сетях и их роли в современном мире;

● приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

● навыками и умениями безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете;

● основными навыками и умениями использования компьютерных устройств.

Выпускник получит возможность овладеть:

● навыками инженерного мышления;

● навыками работы с реальными программно-аппаратными комплексами;

● навыками оценивания уровня безопасности компьютерных систем; навыками обеспечения информационной безопасности личного пространства;

● различными источниками информации, включая Интернет-ресурсы и другие базы данных для решения коммуникативных задач в области безопасности жизнедеятельности.

Метапредметные

● умение самостоятельно определять цели деятельности и составлять планы деятельности; самостоятельно осуществлять, контролировать и корректировать деятельность; использовать все возможные ресурсы для достижения поставленных целей и реализации планов деятельности; выбирать успешные стратегии в различных ситуациях;

● умение продуктивно общаться и взаимодействовать в процессе совместной деятельности, учитывать позиции других участников деятельности, эффективно разрешать конфликты;

● владение навыками познавательной, учебно-исследовательской и проектной деятельности, навыками разрешения проблем; способность и готовность к самостоятельному поиску методов решения практических задач, применению различных методов познания;

● готовность и способность к самостоятельной информационно-познавательной деятельности, владение навыками получения необходимой информации из словарей разных типов, умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

● умение использовать средства информационных и коммуникационных технологий (далее - ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности;

● умение определять назначение и функции различных социальных институтов;

● умение самостоятельно оценивать и принимать решения, определяющие стратегию поведения, с учетом гражданских и нравственных ценностей;

● владение языковыми средствами - умение ясно, логично и точно излагать свою точку зрения, использовать адекватные языковые средства;

● владение навыками познавательной рефлексии как осознания совершаемых действий и мыслительных процессов, их результатов и оснований, границ своего знания и незнания, новых познавательных задач и средств их достижения.

1.11. Формы контроля и подведения итогов реализации программы

В образовательном процессе будут использованы следующие виды и методы контроля успешности освоения обучающимися программы:

Входной контроль осуществляется оценка владения базовыми навыками решения математических задач и задач по информатике.

Текущий контроль с целью непрерывного отслеживания уровня усвоения материала, выполнения работ и развития мотивации обучающихся. Для реализации текущего контроля в процессе объяснения теоретического материала преподаватель обращается к обучающимся с вопросами и короткими заданиями; в процессе выполнения практических работ (задач и упражнений) преподаватель контролирует и оценивает выполненные этапы работы, обучающиеся осуществляют самоконтроль, анализ образовательных результатов.

Промежуточный контрольосуществляется в виде теста.

Итоговый контроль осуществляется в виде итогового теста.

2.Учебный план

№	Названия раздела/темы	Количество часов		
		Всего	Теория	Практика
1	Введение в профессию «Белый хакер – пентестер»	2	2	0
2	Уровень 1.Разведка во внешней инфраструктуре .	6	3	3
3	Уровень 2.Атака первичного доступа	12	6	6
4	Уровень 3.Закрепление доступа и повышение привилегий.	6	2	4
5	Уровень 4. Проброс сетевого трафика.	6	2	4

6	Уровень 5. Выход за рамки ДМЗ.	4	2	2
7	Уровень 6. Разведка в сети Windows-машин.	4	2	2
8	Уровень 7. Повышение привилегий.	6	4	2
9	Уровень 8. Захват управления инфраструктурой.	6	4	2
10	Уровень 9. Противодействие обнаружению.	5	3	2
11	Уровень 10. Социальная инженерия.	3	1	2
12	Уровень 11. Взлом веб-приложений.	8	6	2
13	Уровень 12. Противодействие обнаружению. Развитие хакера.	4	3	1
	всего	**72**	**40**	**32**

2.1. Календарный учебный график

Год обучения	Дата начала обучения по программе	Дата окончания обучения по программе	Всего учебных недель	Количество учебных часов	Режим занятий*
2025	09.01.2025	31.12.2025	36	72	очно

*занятия проводятся 1 раз в неделю по 2 академических часа

2.2 Календарно-тематический план

№ пп	Кол-во часов	Тема урока	Содержание	Дата
Введение в профессию «Белый хакер – пентестер» 2 часа.				
1	1	Введение в курс.	как устроен курс; какие необходимы начальные знания; как подготовить рабочее окружение для прохождения практических заданий.	
2	1	Белый хакинг.	необходимые подходы и техники для успешной карьеры в этой области, современные инструменты и методами работы с компьютерными системами.	
Уровень 1.Разведка во внешней инфраструктуре. 6 часов.				
3	1	Поиск доменных имен организации.	Обнаружение доменных имен, принадлежащих организации Обнаружение “живых” хостов в сети и составления списка их IP-адресов Определение актуального статуса сетевых портов узлов из списка Определение типа и версии операционной системы на исследованных машинах Определение версий ПО или служб, которые находятся на сетевых портах Сбор информации об используемых технологиях на веб-сайте	
4	1	Сканеры сети	анализировать и определить уязвимостивсети компании, а также определить, какие порты и службы открыты на каждом устройстве в сети, выявлять уязвимые места в сети и	

			предотвращать возможные кибератаки.	
5	1	Сканеры портов.	Данная техника направлена на сбор актуальной информации о сетевых портах исследуемого узла. Если бы мы занялись пассивным сканированием сетевых портов, то тогда не выдали бы факт исследования узла, но при этом не были бы полностью уверены в актуальности результата. Если важна актуальность – выбираем активное сканирование портов, а если скрытность – пассивное сканирование сетевых портов.	
6	1	Сканирование узлов сети	Сканирование сети применяется на начальном этапе сбора информации для получения информации об используемых IP-адресах в сети. Сканирование применяют при отсутствии какой-либо информации о сети и инфраструктуре.	
7	1	Практика "Разведка во внешней сети"	Задача - найти как можно больше поддоменов, связанных с этой организацией.	
8	1	Тестирование.	тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 2. Атака первичного доступа. 12 часов.				
9	1	Уязвимости обхода аутентификации	механизмы управления и защиты информации, как идентификация**,** авторизация и аутентификация**.**	
10	1	Тестирование.	тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
11	1	Уязвимости контроля доступа	Проектирование и управление контролем доступа — это сложная и динамичная проблема, которая применяет деловые, организационные и правовые ограничения	

			к технической реализации.	
12	1	Практика.	Проанализируйте защищенность механизма проверки информации о заказе в магазине курсов. Обнаружьте уязвимости контроля доступа, позволяющие исследовать содержимое заказов других пользователей.	
13	1	Тестирование.	тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
14	1	Атаки межсайтового скриптинга (XSS)	Межсайтовый скриптинг (также известный как Cross-SiteScripting, XSS) – это уязвимость веб-безопасности, позволяющая злоумышленнику скомпрометировать взаимодействие пользователей с уязвимым приложением.	
15	1	Практика.	Обнаружьте версию ПО и его наименование, постарайтесь определить наличие в данном ПО известных уязвимостей при помощи фреймворкаMetasploit	
16	1	Тестирование.	тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
17	1	Эксплуатация уязвимостей 1-го дня в сетевых сервисах.	Фреймворки эксплуатации, которые разработаны для унификации подготовки, настройки и тестирования эксплойтов.	
18	1	Поиск email-адресов сотрудников организации	Первый принцип работы данной техники заключается в том, что если нам нужно найти электронный адрес только одного сотрудника, то мы можем его поискать в различных утечках баз данных.	
19	1	Практика.	В данной практике вам предстоит работать со стендом, эмулирующим рабочую станцию сотрудника на ОС Windows.	

20	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 3.Закрепление доступа и повышение привилегий. 6 часов.				
21	1	Получение легитимного доступа к системе.	Методы закрепления доступа, позволяющие закреплять доступ к системе, не внося в систему изменения, используя существующие учетные данные и способы доступа к системе.	
22	1	Практика.	сгенерируйте нагрузку для закрепления доступа в системе при помощи утилиты pupy. Отправьте эту нагрузку на скомпрометированную систему и запустите ее там.	
23	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
24	1	Эксплуатация ошибок администрирования ОС Linux	Как устроено управление пользователями и группами Как происходит управления правами доступа к файлам Какие есть встроенные механизмы передачи и получения прав доступа	
25	1	Практика.	Обнаружьте уязвимости конфигурации настроек sudo для вашего пользователя.	
26	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 4. Проброс сетевого трафика. 6 часов.				
27	1	Использование стандартных протоколов для проброса	Удобство и простота использования. Возможность использования почти на любой ОС. Относительная надежность соединения.	

		трафика.		
28	1	Практика.	Проанализируйте защищенность панели расположенной на сайте узла jump и проэксплуатируйте найденные уязвимости, используя различные инструменты описанные в шаге (помимо gost можно воспользоваться netcat и т.д.).	
29	1	Обнаружение Windows-машин в сети	браузер в машине Windows использует эту технологию для отправки локальному DHCP-серверу DHCPINFORM-запроса и использует полученный URL из WPAD-опции ответа сервера. Если DHCP-сервер не может предоставить требуемую информацию, то используется DNS.	
30	1	Компрометация Windows-машин в сети	Применение эксплойтов к известным уязвимостям Windows машин. Применение атак методом перебора. Перехват трафика и атаки MitM.	
31	1	Практика.	Проанализируйте защищенность узла, развернутого вами в виртуальном стенде, определите версию ПО и попытайтесь определить известные уязвимости данной операционной системы.	
32	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 5. Выход за рамки ДМЗ. 4 часа.				
33	1	Сканирование сети	Для обнаружения лазеек достаточно просканировать диапазон локальной сети на доступность узлов или отдельных портов и протоколов при помощи *nmap* или *masscan*. Обычно локальные сети компаний используют адресацию: 10.0.0.0/8,	

			172.16.0.0/12, 192.168.0.0/16 Мы можем проверить доступность отдельных портов TCP/UDP или целых узлов сети	
34	1	Анализ трафика сети ДМЗ	Широковещательные и мультикаст-пакеты протоколов: mDNS, DHCP, LLMNR, NBT-NS, NDP for IPv6, RTP Протоколы, которые впоследствии могут быть использованы для атак: DTP,STP,CDP, и пр. Сетевые соединения скомпрометированного узла с узлами остальной сети	
35	1	Практика.	Необходимо скачать образ виртуальной машины по ссылке: Mikrotik.ova (зеркала: Яндекс.Диск и OneDrive) Импортировать виртуальную машину Mikrotik двойным нажатием на файл `Mikrotik.ova`. После импорта виртуальной машины, запустить ее и войти под пользователем `admin` с паролем `password` для инициализации сети ОС.	
36	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 6. Разведка в сетиWindows – машин. 4 часа.				
37	1	Обнаружение Windows-машин в сети	Сканирование портов, принадлежащих Windows машинам	
38	1	Компрометация Windows-машин в сети	**Атаки первичного доступа на Windows машины** могут быть предприняты после их обнаружения и использовать следующие способы атак:	

			Применение эксплойтов к известным уязвимостям Windows машин. Применение атак методом перебора. Перехват трафика и атаки MitM.	
39	1	Практика.	На вашей операционной системе должно быть установлено программное обеспечение VirtualBox. Поддерживаемые ОС: Linux,Windows, MacOS (x64). MacOS с архитектурой arm (m1/m2/…) не поддерживаются.	
40	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 7. Повышение привилегий. 6 часов.				
41	1	Извлечение секретов и учетных данных	Взлом менеджеров паролей пользователей по причине небезопасной конфигурации. Обнаружение секретов и учетных данных в логах и истории команд. Извлечение учетных данных из оперативной памяти. Доступ к файлу, хранящему хеши пользовательских паролей. Извлечение учетных данных из конфигурации Групповых Политик.	
42	1	Эксплуатация уязвимостей конфигурации ОС Windows	Повышение привилегий через права на создание резервных копий (SeBackupPrivilege) Повышение привилегий через перехват сервиса (WeakServicesPermission) Повышение привилегий через имперсонификацию (выдачу себя за другого) SeImpersonatePrivilege (JyicyPotato) Повышение привилегий через права на установку ПО (AlwaysInstallElevated) Повышение привилегий через изменение пути бинарного файла сервиса (ServiceBinaryPath) Повышение привилегий через подмену DLL библиотек (DLL Hijacking) Повышение привилегий через неэкранированные пути сервисов (UnquotedServicePaths)	

43	1	Эксплуатация известных уязвимостей ОС Windows	Уязвимостьвустановщике Windows (InstallerFileTakeOver (0day) Уязвимостьв Windows Print Spooler (PrintNightmare) Уязвимость в планировщике задач Windows (MS10-092) Уязвимость в ядре Windows (MS16_014) Обработка вторичного входа в систему (MS16-032)	
44	1	Горизонтальное (“боковое”) перемещение	Боковое перемещение — это одновременное сочетание **2 техник:** Извлечение секретной информации после получения доступа. Аутентифицированное удаленное выполне ния кода.	
45	1	Практика.	На вашей операционной системе должно быть установлено программное обеспечение *VirtualBox***.** Поддерживаемые ОС: Linux,Windows, MacOS (x64). MacOS с архитектурой arm (m1/m2/…) не поддерживаются.	
46	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 8. Захват управления инфраструктурой. 6 часов.				
47	1	Эксплуатация уязвимостей узла контроллера домена	Рассмотрим эксплуатацию одной из самых ярких уязвимостей в контроллере домена. **Zerologon** — это название уязвимости с идентификатором CVE-2020-1472. Ее так назвали из-за изъяна процесса Netlogon: вектор инициализации (IV), который должен был бы представлять собой случайное число, всегда состоит из одних нулей.	
48	1	Кража учетных данных, токенов и сессий привилегированных УЗ	Данный подход — один из наиболее распространенных в сетях, **незрелых с точки зрения ИБ заказчиков.** Он	

			подразумевает отсутствие серьезных препятствий на пути пентестера в виде разграничения доступа в сети, Tier-модели Майкрософт, механизмов CredentialsGuard и пр.	
49	1	Сбор информации об объектах в домене	При выборе такого подхода к компрометации домена ваше основное время уйдет **на разведку в домене и энумерацию учетных записей.**	
50	1	Эксплуатация мисконфигураций сервисов в AD	Доменная инфраструктура и конкретно инфраструктура MicrosoftActiveDirectory настолько сложна, наполнена зависимостями и наследием, что в своих имплементациях содержит десятки и сотни возможных проблем конфигурации, за которыми сложно или почти невозможно уследить.	
51	1	Практика.	Проанализируйте защищенность узла, развернутого вами в виртуальном стенде, определите версию ПО и попытайтесь определить известные уязвимости данной операционной системы. Обнаружьте известную уязвимость, которой подвержена данная операционная система и проэксплуатируйте ее при помощи фреймворкаmetasploit.	
52	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 9. Противодействие обнаружению. 5 часов.				
53	1	Снижение активности в сети	Этот принцип — один из самых простых с точки зрения технического исполнения, но в то же время является сложным из-за необходимости проявить креативность. Наша максимальная задача в этом процессе	

			— не оставить возможности детектирования наших действий активными средствами защиты.	
54	1	Использование шифрованных каналов связи	Для того, чтобы активные средства защиты не могли обнаружить атакующий трафик и определить опасные конструкции в нем по сигнатурам, необходимо постоянно заботиться о том, чтобы наш трафик эксплойтов или команд невозможно было расшифровать.	
55	1	Подготовка нагрузок. Принципы противодействия обнаружению	При подготовке нагрузок есть необходимость использовать нагрузки и обертки для них с целью обхода их детектирования системами EPP и EDR, которые обнаруживают такие вредоносные программы и не дают им возможности запуститься.	
56	1	Использование инструментов смены IP	Процесс ротации (смены) IP адресов необходим в работе пентестера, так как постоянная работа с активным анализом инфраструктуры приводит случаям блокирования вашего узла сети. Из-за этого приходится менять IP адрес, с которого вы выполняете активные действия.	
57	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 10. Социальная инженерия. 3 часа.				
58	1	Поиск email-адресов сотрудников организации	Первый принцип работы данной техники заключается в том, что если нам нужно найти электронный адрес только одного сотрудника, то мы можем его поискать в различных утечках баз данных. Или, зная маску корпоративной почты сотрудников организации, мы можем подобрать адрес	

			нужной нам электронной почты с помощью генератора email-адресов.	
59	1	Практика.	В данной практике вам предстоит работать со стендом, эмулирующим рабочую станцию сотрудника на ОС Windows.	
60	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 11. Взлом веб-приложений. 8 часов.				
61	1	Уязвимости обхода аутентификации	**Классифицировать различные типы проверки подлинности можно по трем факторам:** **Знание**, например, пароль или ответ на вопрос безопасности, одноразовый код. Их иногда называют *факторами знаний.* **Обладание**, то есть физический объект, такой как мобильный телефон или маркер безопасности - магнитная карта. Их иногда называют *факторами владения*. **Биометрия**, например, персональные данные или модели поведения - конфиденциальная информация. Их иногда называют *факторами согласованности*.	
62	1	Уязвимости инъекции команд ОС	Инъекция команд ОС (также известная как shell инъекция) является уязвимостью веб-приложений, которая позволяет злоумышленнику выполнять произвольные команды операционной системы (ОС) на сервере, на котором запущено приложение, и, как правило, дает возможность полностью скомпрометировать приложение и все его данные	
63	1	Уязвимости контроля доступа.	Аутентификация идентифицирует пользователя и подтверждает, что он является тем, за кого себя выдает. Управление сеансом идентифицирует, какие последующие HTTP-запросы выполняются тем же самым пользователем. Управление доступом определяет, разрешено ли пользователю выполнять	

			действия, которые он пытается выполнить.	
64	1	Уязвимости разграничения доступа к каталогам	Обход файловых путей (англ. **PathTraversal** или **DirectoryTraversal**) – это уязвимость веб-безопасности, позволяющая злоумышленнику читать произвольные файлы на сервере, на котором запущено приложение.	
65	1	Уязвимости SQL-инъекции	SQL-инъекция – это уязвимость веб-приложений, позволяющая злоумышленнику вмешиваться в запросы, которые приложение делает к своей базе данных. Она позволяет злоумышленнику просматривать данные, которые он, как правило, не может получить.	
66	1	Уязвимости внедрения внешних сущностей XML	Некоторые приложения используют формат XML для передачи данных между браузером и сервером. Приложения, которые это делают, практически всегда используют стандартную библиотеку или платформенный API для обработки XML-данных на сервере.	
67	1	Атаки межсайтового скриптинга (XSS)	**Межсайтовый скриптинг (также известный как Cross-SiteScripting, XSS)** – это уязвимость веб-безопасности, позволяющая злоумышленнику скомпрометировать взаимодействие пользователей с уязвимым приложением.	
68	1	Тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Уровень 12.Противодействие обнаружению. Развитие хакера. 4 часа.				
69	1	Направления развития.	В нашей сегодняшней реальности есть конкретные наборы популярных областей и направлений развития хакеров и в особенности профессиональных хакеров	

			— **пентестеров.** Пентестеры работают по заказу компаний и легально взламывают информационные системы, с целью сделать их защищеннее. В связи с этим, появляется все больше хакеров, которые специализируются на исследовании определенных типов информационных систем.	
70	1	Этика.	Абсолютное большинство российского сообщества живет в Телеграмм. Это публичные каналы и чаты, а также приватные группы для интересных собеседников с богатым опытом, которые не разбавляются новичками. Огромное количество знаний проходят через них, и вы можете к ним присоединиться	
71	1	Практика.	Материалы для самостоятельного изучения:	
72	1	Итоговое тестирование.	Тестирование по изученному материалу, чтобы закрепить и систематизировать полученные знания.	
Всего: 72 часа				

2.3Содержание курса

Раздел 1. Введение в профессию «Белый хакинг»

Вводное занятие.

Теория:

Одним из необходимых навыков в современном мире является поиск информации в Интернете.

Для пентестера этот навык является ключевым, так как такому специалисту необходимо не только постоянно совершенствовать свои знания и осваивать новые рабочие инструменты, но и следить за новыми тенденциями в мире кибербезопасности, а также своевременно разобраться в новых техниках и тактиках злоумышленников.

Практика:

1. Потребуется регистрация на платформе.
2. Даже если сдали флаг в облачной платфоме, потребуется сдать его ещё и в stepik'e.
3. Для доступа к некоторым стендам потребуется воспользоваться openVPN.
4. Выполнять задания через ОС KaliLinux удобнее, поэтому всё равно она потребуется и желательно развернуть ОС локально (обычно это делается через VirtualBox).

Профессия «Белый хакинг»

Теория:

Введение в профессию.

В курсе "Профессия — Белый Хакер" вы узнаете все необходимые подходы и техники для успешной карьеры в этой области, а также познакомитесь с самыми современными инструментами и методами работы с компьютерными системами.

В настоящее время количество вакансий в области кибербезопасности растет с каждым годом — пропорционально росту угроз и кибератак. Большинство компаний нуждаются в квалифицированных специалистах, которые могут помочь им защитить свои данные и устройства. Белые хакеры занимаются исследованием уязвимостей компьютерных систем и помогают компаниям защитить свои данные и предотвратить атаки со стороны злоумышленников.

Раздел 2.Уровень 1. Разведка в сети.

Теория:

Разведка в сети – это процесс сбора информации об объекте или цели в интернете. Это может быть любая информация, которая может помочь в осуществлении дальнейших действий по отношению к объекту. Например, определение уязвимостей или сбор данных для атаки.

Инфраструктура компании — это совокупность аппаратных, программных и сетевых средств, используемых для поддержания бизнес-процессов и обеспечения безопасности информации, находящейся в распоряжении компании. Она включает в себя серверы, сетевые устройства, базы данных, приложения и другие компоненты, используемые для обработки, хранения и передачи данных. Эффективная инфраструктура компании должна быть разработана с учетом требований к безопасности и включать в себя меры защиты, которые обеспечат целостность, конфиденциальность и доступность информации в пределах организации.

Сетевой сканер — это программа, предназначенная для сканирования компьютерных сетей и обнаружения устройств, портов и служб, работающих на этих устройствах. Они используются для проверки безопасности сетей, выявления уязвимостей и проверки соответствия настроек безопасности определенным стандартам.

Доменное имя – это уникальное текстовое имя, которое используется для идентификации адреса ресурса в Интернете.

Практика:

Основной домен организации `cyber-ed.ru`. Задача постараться найти как можно больше поддоменов, связанных с этой организацией.

Некоторые поддомены в TXT-записи DNS-сервера содержат различные флаги. В одном из поддоменов (кстати, его имя будет логически связано с заданием) будет

TXT-запись с флагом в формате: `FLAG=значение_флага`, где "значение_флага" — это смесь из 32 произвольных букв и цифр. Необходимо найти этот флаг и предоставить его значение в текстовое поле ниже.

Раздел 3. Уровень 2. Атака первичного доступа.

Теория:

Атака первичного доступа (англ. InitialAccessAttack) — это попытка несанкционированного доступа к системе, сети или приложению, с целью получить начальный уровень доступа и проникнуть в них.

Уязвимости — это слабые места в системе или приложении, которые могут быть использованы злоумышленниками для проведения атак.

Фишинг (Phishing) — это метод социальной инженерии, при котором злоумышленник пытается получить доступ к чужой информации, обманывая пользователей с помощью поддельных веб-сайтов, электронных писем или сообщений.

Фишинговый сервис — это специальный инструмент, который используется для проведения фишинг-атак.

Отказ в обслуживании (англ. *denial-of-service attack (DoS)*) — атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

Атака «человек посередине» (англ. Maninthemiddle (MiTM)) — вид атаки в компьютерной безопасности, когда злоумышленник тайно ретранслирует и при

необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Практика:

Проанализируйте веб-приложение, развернутое по адресу http://localhost:1337. Обнаружить версию ПО и его наименование, определить наличие в данном ПО известных уязвимостей при помощи фреймворкаMetasploit. Проэксплуатировать известную уязвимость, имеющуюся в используемом приложением фреймворке.

Раздел 4. Уровень 3.Закрепление доступа и повышение привилегий.

Теория:

Закрепление доступа — это набор методов, которые атакующие используют для сохранения доступа к системам после
перезагрузки, изменения учетных данных и других изменений, которые могли бы прервать их доступ.

Backdoor *(англ. Тайная дверь)* — Backdoor - это скрытый способ доступа к системе, приложению или устройству, который обычно используется для обхода стандартных механизмов аутентификации и безопасности.

MITRE ATT&CK *(AdversarialTactics, Techniques, andCommonKnowledge)* - матрица для описания тактик, техник и процедур, которые могут использоваться киберпреступниками для осуществления кибератак на организации и компании. MITRE ATT&CK описывает более 200 тактик и приемов, которые могут использоваться киберпреступниками на разных этапах кибератаки: от получения доступа к сети до уничтожения данных и скрытия следов своей деятельности.

Практика:

Проэксплуатировать уже известные вам уязвимости приложения развернутого по адресу http://localhost:1337. Теперь, после эксплуатации уязвимостей сгенерировать нагрузку для закрепления доступа в системе при помощи утилиты pupy. Отправить эту нагрузку на скомпрометированную систему и запустить ее там.

В качестве подтверждения успешной эксплуатации предоставить информацию, которую выводит сгенерированная и запущенная в уязвимой системе нагрузка при помощи команды `info`.

Раздел 5. Уровень 4. Проброс сетевого трафика.

Теория:

Pivoting (англ. Pivot – “точка опоры”) – набор техник, с помощью которых организовывается доступ к тем сетям, к которым нет доступа при обычных обстоятельствах. При этом доступ получен с использованием скомпрометированных компьютеров.

Прокси-сервер (англ. “Proxy”) — промежуточный сервер в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером, позволяющий клиентам как выполнять косвенные запросы к другим сетевым службам, так и получать ответы.

Туннелирование в компьютерных сетях (англ. “Tunneling”) — процесс, в ходе которого создается логическое соединение между двумя конечными точками посредством инкапсуляции различных протоколов.

Переадресация портов (англ. “PortForwarding”) — проброс портов, который также иногда называемый перенаправлением портов или туннелированием, – это

процесс пересылки трафика, адресованного конкретному сетевому порту с одного сетевого узла на другой.
Port2Port (также известный как P2P) — это техника перенаправления сетевого трафика между двумя различными портами на одном и том же компьютере или между двумя разными компьютерами.

Port2Hostnet — это техника перенаправления сетевого трафика через порт в сеть удаленного узла.

Практика:

В этой задаче присутствует два узла и два веб-сервера. Назовем их *jump* и *target*.

Вам предоставлен доступ к веб-приложению на узле *jump*. Он откроется у вас по адресу `localhost:1337`.

Также доступен порт *1338*.

Проанализируйте защищенность панели расположенной на сайте узла jump и проэксплуатируйте найденные уязвимости, используя различные инструменты описанные в шаге (помимо gost можно воспользоваться netcat и т.д.). Обнаружьте узел *target* в той же сети, где находится jump узел (узел target недоступен вам на прямую). Когда найдете узел *target*, проанализируйте веб-приложение target и найдите в нем файлы опубликованные в веб-сервере. Для этого научитесь пробрасывать трафик для сканирования через узел *jump* на узел *target*.

В качестве подтверждения успешной эксплуатации предоставьте флаг (секретную строку в формате 32 букв и цифр) из кода специальной скрытой страницы на узле *target*.

Раздел 6. Уровень 5. Выход за рамки ДМЗ.

Теория.

Сегмент сети — логически или физически обособленная часть сети. Разбиение сети на сегменты осуществляется с целью оптимизации сетевого трафика и/или повышения безопасности сети в целом.

Атака «человек посередине» (англ. Maninthemiddle (MitM)) — вид атаки в компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.

Практика.

Проанализируйте защищенность узла, развернутого вами в виртуальном стенде, определите версию ПО и попытайтесь определить известные уязвимости данной операционной системы. Обнаружьте известную уязвимость, позволяющую извлекать историю паролей учетных записей роутера, и проэксплуатируйте ее при помощи фреймворкаmetasploit.

В качестве подтверждения успешной эксплуатации предоставьте флаг *(пароль учетной записи администратора, который предшествовал паролю, который вы указывали когда инициализировали роутер, в формате 9 букв, цифр и спецсимволов).*

Раздел 7. Уровень 6. Разведка в сети Windows – машин.

Теория.

NBT (NetBIOSover TCP/IP) — механизм отображения запросов NetBIOS на TCP/IP.

Служба имен NetBIOS (NBT-NS) — это протокол Windows, который используется для преобразования имен NetBIOS в IP-адреса в локальной сети.

LLMNR, англ. Link-LocalMulticastNameResolution — протокол стека TCP/IP, основанный на формате пакета данных DNS,

который позволяет компьютерам выполнять разрешение имен хостов в локальной сети.

MS17-010 — обновление безопасности, устраняющее уязвимости в MicrosoftWindows. Наиболее серьезная из уязвимостей может позволить удаленное выполнение кода, если злоумышленник отправит специально созданные сообщения на сервер MicrosoftServerMessageBlock 1.0 (SMBv1).

Практика.

Проанализируйте защищенность узла, развернутого вами в виртуальном стенде, определите версию ПО и попытайтесь определить известные уязвимости данной операционной системы. Обнаружьте известную уязвимость, которой подвержена данная операционная система и проэксплуатируйте ее при помощи фреймворкаmetasploit.

В качестве подтверждения успешной эксплуатации предоставьте флаг (секретную строку в формате 26 букв и цифр) из файла root.txt, расположенного в папке рабочего стола пользователя *Kevin*.

Раздел 8. Уровень 7. Повышение привилегий.

Теория.

Горизонтальное перемещение (lateralmovement) — один из этапов атаки на организацию, во время которого злоумышленник, уже сумевший проникнуть внутрь корпоративной инфраструктуры и закрепиться в ней, начинает продвигаться по сети от точки входа (например, скомпрометированного устройства или аккаунта) к другим объектам.

Домен – это основная административная единица в сетевой инфраструктуре предприятия, в которую входят все сетевые объекты, такие как пользователи, компьютеры, принтеры, общие ресурсы и т.д. Совокупность (иерархия) доменов называется **лесом.** У каждой компании могут быть внешние и внутренние домены.

Контроллер домена (domaincontroller) — сервер, управляющий доступом к сетевым ресурсам в рамках одного домена (группы сетей или хостов, объединенных общими политиками безопасности). Контроллер домена осуществляет аутентификацию пользователя в домене, то есть позволяет ему входить в сеть с помощью одной и той же пары логин/пароль с любого включенного в домен компьютера, на котором это не запрещено политиками безопасности или локальными настройками.

Практика.

Проанализируйте защищенность узла. Воспользуйтесь опубликованным на узле SSH сервисом, чтобы подобрать пароль пользователя John с использование словаря rockyou.

После получения доступа к SSH (в предыдущем задании) обнаружьте уязвимости, позволяющие вам повысить свои привилегии и проэксплуатируйте их.

Раздел 9. Уровень 8. Захват управления инфраструктурой.

Теория.

Каталог (Directory, хранилище данных) — в контексте компьютерной сети, иерархическая структура, хранящая информацию об объектах в сети. Объекты - это серверы, общие тома и принтеры, учетные записи пользователей, рабочие станции, а также домены, приложения, службы, политики безопасности и почти все остальное в вашей сети.

Служба каталогов (DirectoryService) — является как источником информации каталога, так и службой, делающей информацию доступной и полезной для администраторов, пользователей, сетевых служб и приложений. ActiveDirectory™, служба каталогов, которая хранит информацию о сетевых объектах, а также реализует службы, которые делают эту информацию доступной и полезной для пользователей, компьютеров и приложений.

Объекты (Objects) — это сущности, составляющие сеть. **Объект** — это отдельный именованный набор атрибутов, представляющий что-то конкретное, например, пользователя, принтер или приложение.

Схема (Schema) — это описание классов объектов (различных типов объектов) и атрибутов для этих классов объектов. Для каждого класса объектов схема определяет атрибуты, которые должен иметь этот класс объектов, дополнительные атрибуты, которые он может иметь, и класс объектов, который может быть его родителем. Каждый объект ActiveDirectory является экземпляром класса объекта. Каждый атрибут определяется только один раз и может использоваться в нескольких классах. Например, атрибут Description определяется один раз, но используется во многих различных классах.

Домены — это объекты-контейнеры, или набор административно определенных объектов, которые имеют общую базу данных каталога, политики безопасности и доверительные отношения с другими доменами. Таким образом, каждый домен является административной границей для объектов. Один домен может охватывать несколько физических мест или сайтов, и содержать миллионы объектов.

Дерево домена (DomainTree) — состоит из нескольких доменов, которые имеют общую схему и конфигурацию, образуя непрерывное пространство имен. Домены в дереве также связаны между собой доверительными отношениями. ActiveDirectory представляет собой набор из одного или нескольких деревьев.

Лес (Forest) — это набор из одного или нескольких деревьев доменов, которые не образуют непрерывное пространство имен. Все деревья в лесу имеют общую схему, конфигурацию и глобальный каталог. Все деревья в данном лесу обмениваются доверием в соответствии с транзитивными иерархическими отношениями доверия Kerberos. В отличие от деревьев, лес не требует отдельного имени. Лес существует как набор объектов перекрестных ссылок и доверительных отношений Kerberos, распознаваемых входящими в него деревьями. Деревья в

лесу образуют иерархию для целей доверия Kerberos. Имя дерева в корне дерева доверия относится к данному лесу.

Доверительные отношения (TrustRelationship) — это отношения, установленные между двумя доменами, которые позволяют пользователям одного домена быть распознанными контроллером домена в другом домене. Доверительные отношения позволяют пользователям получать доступ к ресурсам в другом домене, а также позволяют администраторам управлять правами пользователей в другом домене. На уровне леса доверительные отношения создаются автоматически между корневым доменом леса и корневым доменом каждого дерева доменов, добавленного в лес, в результате чего между всеми доменами в лесу ActiveDirectory существует полное доверие.

Практика.

Проанализируйте защищенность узла, развернутого вами в виртуальном стенде, определите версию ПО и попытайтесь определить известные уязвимости данной операционной системы. Обнаружьте известную уязвимость, которой подвержена данная операционная система и проэксплуатируйте ее при помощи фреймворкаmetasploit.

Соберите информацию о домене при помощи утилит ldapdomaindump или BloodHound и найдите в домене пользователя, у которого в комментарии указан секретный флаг в формате: `Flag{ПРОИЗВОЛЬНЫЕ ЦИФРЫ И БУКВЫ}`

Раздел 10. Уровень 9. Противодействие обнаружению.

Теория.

EndpointDetection&Response (EDR) — класс решений для обнаружения и изучения вредоносной активности на конечных точках, подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее. В отличие от антивирусов, задача которых бороться с типовыми и массовыми угрозами, EDR-решения ориентированы на выявление целевых атак и сложных угроз. При

этом EDR-решения не могут полностью заменить антивирусы (EPP), поскольку эти две технологии решают разные задачи.

EndpointProtectionPlatform (EPP) — комплексные защитные решения для конечных точек, в которые входит антивирус, технологии шифрования данных, технологии для отслеживания и устранения уязвимостей, контроля приложений и устройств и т.д.

SecurityInformationandEventManagement (SIEM) — решения для сбора и автоматического анализа информации о событиях безопасности.

NextGenerationFirewall, межсетевой экран нового поколения (NGFW) — межсетевой экран для глубокой фильтрации трафика, интегрированный с IDS (IntrusionDetectionSystem, система обнаружения вторжений) или IPS (IntrusionPreventionSystem, система предотвращения вторжений), и обладающий возможностью контролировать и блокировать трафик на уровне приложений.

IntrusionDetectionSystem (IDS) — система обнаружения вторжений, программный продукт или устройство, предназначенные для выявления несанкционированной и вредоносной активности в компьютерной сети или на отдельном хосте. Задача IDS — обнаружить проникновение киберпреступников в инфраструктуру и сформировать оповещение безопасности (функций реагирования, например блокировки нежелательной активности, в таких системах нет), которое будет передано в SIEM-систему для дальнейшей обработки.

Песочница — специально выделенная (изолированная) среда для безопасного исполнения компьютерных программ.

Практика.

Процесс ротации (смены) IP адресов необходим в работе пентестера, так как постоянная работа с активным анализом инфраструктуры приводит случаям

блокирования вашего узла сети. Из-за этого приходится менять IP адрес, с которого вы выполняете активные действия.

Раздел 11. Уровень 10. Социальная инженерия.

Теория. **Социальная инженерия (атака)** — обман, манипулирование и мошенничество с использованием социальных и психологических аспектов человеческой жизни.

Разведка по открытым источникам (OpenSourceIntelligence, OSINT) — разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ.

Практика.В стенде имеется почтовый сервер, работающий в домене `sandbox.local`.

У пользователя `Mike` запущен бот, который раз в 30 секунд читает все ранее не прочитанные письма и, при наличии в них вложений запускает их (тем самым эмулируя действия неграмотного сотрудника).

Ваша задача воспользоваться данной уязвимостью и получить доступ к секретному содержимому файла `root.txt`, расположенного на рабочем столе пользователя `Mike`.

Раздел 12. Уровень 11. Взлом веб – приложений.

Теория.

Веб-приложение (Webapplication) — клиент-серверное приложение, в котором клиент взаимодействует с веб-сервером при помощи браузера. Уязвимости веб-приложений возникают, когда разработчики допускают ошибки в коде. Это может происходить как на этапе разработки, так и на этапе

доработки или исправления найденных ранее уязвимостей. Также при разработке веб-сервиса может использоваться сторонний код, проверка которого требует отдельного внимания разработчиков. Существуют и другие причины небезопасных веб-приложений, некоторые из которых мы коснемся в курсе.

Идентификация (Identification)— это процедура определения и подтверждения субъекта идентификации (пользователя) через его идентификатор, однозначно определяющий его на основе предоставленных им данных, таких как: имя, адрес электронной почты или номер телефона. Идентификация часто используется вместе с аутентификацией для подтверждения подлинности пользователя.

Аутентификация (Authentication) — это процедура проверки подлинности идентификационных данных пользователя, таких как: логин и пароль. Чтобы убедиться, что он является тем, за кого себя выдает. По сути, процесс проверки конкретного пользователя или клиента путем сравнения введенного им пароля с паролем, сохраненным в базе данных.

Авторизация (Authorization) — это процесс проверки прав пользователя на выполнение определенных действий или доступ к определенным ресурсам системы. Пользователь может быть аутентифицирован, но не авторизован на выполнение определенной операции, если у него нет необходимых прав.

Атака грубой силы (Bruteforce) — это метод криптоанализа, при котором злоумышленник пытается взломать пароль или зашифрованные данные путем перебора возможных комбинаций до тех пор, пока не будет найдено правильное сочетание. Атака грубой силы может быть эффективной, если пароль короткий или используется слабый алгоритм шифрования, однако, при достаточной длине и сложности пароля, такая атака может занять слишком много времени или быть совсем неэффективной.

Инъекция команд ОС (OS CommandInjection) (также известная как shell инъекция) — уязвимость веб-приложений, которая позволяет злоумышленнику выполнять произвольные команды операционной системы (ОС) на сервере, на котором запущено приложение, и, как правило, дает возможность полностью скомпрометировать приложение и все его данные.

Практика.

Для компрометации веб-приложений используются уязвимости, как правило, возникающие в различных механизмах данного приложения из-за допущенных ошибок при разработке (ошибки в коде, использование уязвимых библиотек и др.). Такие ошибки часто складываются в целые группы типовых уязвимостей.

Раздел 13. Уровень 12. Противодействие обнаружению. Развитие хакера.

Теория:

EndpointDetection&Response (EDR) — класс решений для обнаружения и изучения вредоносной активности на конечных точках, подключенных к сети рабочих станциях, серверах, устройствах Интернета вещей и так далее. В отличие от антивирусов, задача которых бороться с типовыми и массовыми угрозами, EDR-решения ориентированы на выявление целевых атак и сложных угроз. При этом EDR-решения не могут полностью заменить антивирусы (EPP), поскольку эти две технологии решают разные задачи.

EndpointProtectionPlatform (EPP) — комплексные защитные решения для конечных точек, в которые входит антивирус, технологии шифрования данных, технологии для отслеживания и устранения уязвимостей, контроля приложений и устройств и т.д.

SecurityInformationandEventManagement (SIEM) — решения для сбора и автоматического анализа информации о событиях безопасности.

NextGenerationFirewall, межсетевой экран нового поколения (NGFW) — межсетевой экран для глубокой фильтрации трафика, интегрированный с IDS

(IntrusionDetectionSystem, система обнаружения вторжений) или IPS (IntrusionPreventionSystem, система предотвращения вторжений), и обладающий возможностью контролировать и блокировать трафик на уровне приложений.

IntrusionDetectionSystem (IDS) — система обнаружения вторжений, программный продукт или устройство, предназначенные для выявления несанкционированной и вредоносной активности в компьютерной сети или на отдельном хосте. Задача IDS — обнаружить проникновение киберпреступников в инфраструктуру и сформировать оповещение безопасности (функций реагирования, например блокировки нежелательной активности, в таких системах нет), которое будет передано в SIEM-систему для дальнейшей обработки.

Песочница — специально выделенная (изолированная) среда для безопасного исполнения компьютерных программ.

"Белые шляпы" (или "белые хакеры") — это специалисты по информационной безопасности, которые используют свои навыки и знания, чтобы обнаруживать уязвимости и слабые места в системах безопасности компьютеров и сетей, чтобы предотвращать кибератаки и другие виды злоупотреблений с целью защиты компаний, организаций и пользователей от потенциальных угроз.

"Черные шляпы" (или "нелегальные хакеры") — это хакеры, которые нарушают законы, взламывая системы безопасности компьютеров и сетей с целью получения несанкционированного доступа к чужим данным, финансовым ресурсам или другой ценной информации. Они используют свои навыки для получения выгоды, нанесения вреда или реализации других криминальных действий.

Практика:

Процесс ротации (смены) IP адресов необходим в работе пентестера, так как постоянная работа с активным анализом инфраструктуры приводит случаям

блокирования вашего узла сети. Из-за этого приходится менять IP адрес, с которого вы выполняете активные действия.

3. Организационно-педагогические условия реализации программы.

3.1. Материально-техническое обеспечение:

- Класс с проектором, интерактивной доской, возможностью выхода в интернет, класс для практических занятий (на 12-15 чел.) с проектором, возможностью выхода в интернет;

- Кабинеты СОШ №1 г.Белоярский, ул. Школьная д.6.

3.2. Оборудование:

Продуктивность работы во многом зависит от качества материально-технического оснащения процесса, инфраструктуры организации и иных условий. Для успешного проведения занятий и выполнения Программы в полном объеме необходимы:

- Компьютеры с необходимым оборудованием и ПО.
- Киберполигон.

3.3. Кадровое обеспечение:

Бутаков Юрий Владимирович, учитель информатики, высшая квалификационная категория, СОШ №1 г.Белоярский.

3.4. Информационное обеспечение:

Сайт Регионального модельного центра дополнительного образования детей –

https://stepik.org/course/169003/promo

3.5. Методическое обеспечение программы

Методы обучения, используемые в программе: словесные (устное объяснение материала), наглядные (презентация), аналитические. С целью вовлечения в продуктивную и творческую деятельность обучающихся будут использованы:

- информационно аналитический метод;
- логический метод;

- метод системного анализа;
- метод моделирования;
- технико- и тактико-криминалистические методы.

3.6. Программное обеспечение

ОС LinuxAstra 1.7-1.8

VirtualBox

ОС KaliLinux для виртуальной машины

CyberEDlabs

3.7. Информационные источники

https://ctfnews.ru/literature/

https://linux.die.net/man/1/gdb

https://stepik.org/course/762/info

https://www.asozykin.ru/courses/networks_online