Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 1

Введение в этичный хакинг

Преподаватель: **Батыргалиев Асхат Болатканович, PhD, ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»**

askhat.b.b@gmail.com

Содержание

1. Основные термины
2. Понятие слова хакер
3. Виды хакеров
4. Основные области хакинга
5. Виды киберпреступлений
6. Виды компьютерных преступлений

По завершению урока Вы будете знать:

1. Основную терминологию этичного хакинга
2. Понятие слова хакер и виды хакеров
3. Основные области хакинга
4. Виды киберпреступлений

Основные термины и определения

- **Взлом** – выявление слабых мест в компьютерных системах или сетях, чтобы использовать их слабости для получения доступа.
- **Хакер** - человек, который находит и использует слабость компьютерных систем и/или сети для получения доступа. Хакеры – это обычно опытные программисты, обладающие знаниями в области компьютерной безопасности.
- **Взлом программного обеспечения** (cracking) – действия, направленные на устранение защиты программного обеспечения, встроенной разработчиками для ограничения функциональных возможностей.
- **Крэк** (crack) – программа, позволяющая осуществить взлом программного обеспечения.
- **Фрикинг** (phreaking) – взлом телефонных автоматов, телефонных сетей и сетей мобильной связи, с использованием скрытых от пользователя или недокументированных функций.
- **Компьютерный терроризм (кибертерроризм)** - использование компьютерных и телекоммуникационных технологий (прежде всего, Интернета) в террористических целях.
- **Киберпреступность** – незаконные, противоправные действия, которые осуществляются людьми, использующими информационно-телекоммуникационные технологии, компьютеры и компьютерные сети для преступных целей.

Основные термины и определения

- **Хактивизм** – использование незаконными способами компьютеров и компьютерных сетей для продвижения политических идей, свободы слова, защиты прав человека и обеспечения свободы информации.
- **«Анонимус»** – современная международная сеть активистов и хактивистов, отдельные узлы которой слабо связаны между собой.
- **Этичный хакер** (белый хакер, белая шляпа) – специалист по компьютерной безопасности, который специализируется на тестировании безопасности компьютерных систем. В отличие от чёрных шляп (чёрных хакеров), белые хакеры ищут уязвимости на добровольной основе или за плату с целью помочь разработчикам сделать их продукт более защищённым.
- **Компьютерный вирус** – вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.
- **Троянская вирусная программа (троян)** – разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно.

Основные термины и определения

- **Сетевой червь** – разновидность вредоносной программы, самостоятельно распространяющейся через локальные и глобальные (Интернет) компьютерные сети.
- **Анализатор трафика (сниффер)** – программа или устройство для перехвата и анализа сетевого трафика (своего и/или чужого).
- **Руткит (rootkit, «набор root-а»)** – набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), обеспечивающих: маскировку объектов (процессов, файлов, каталогов, драйверов); управление (событиями, происходящими в системе); сбор данных (параметров системы).
- **IP-спуфинг (spoofing)** – вид хакерской атаки, заключающийся в использовании чужого IP-адреса источника с целью обмана системы безопасности.
- **Атака посредника** (атака «человек посередине», Man in the middle (MITM)) – вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.
- **SQL-инъекция** (внедрение SQL-кода, SQL injection / SQLi) – атака, в ходе которой изменяются параметры SQL-запросов к базе данных, один из распространённых способов взлома сайтов и программ, работающих с базами данных, основанный на внедрении в запрос произвольного SQL-кода.

Основные термины и определения

- **PHP-инъекция (PHP injection)** – один из способов взлома веб-сайтов, работающих на PHP, заключающийся в выполнении постороннего кода на серверной стороне.
- **Межсайтовый скриптинг (XSS, Cross-Site Scripting)** – тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода (который будет выполнен на компьютере пользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника.
- **XPath-инъекция** – вид уязвимостей, который заключается во внедрении XPath-выражений в оригинальный запрос к базе данных XML.
- **Автозалив** – веб-инъекция, действующая по принципу троянских программ, основная цель которой заключается во внедрении в аккаунт пользователя в платежной системе, незаметной подмене данных транзакции путём модификации HTML-кода и переводе средств пользователя на счёт злоумышленника.
- **Социальная инженерия (social engineering)** – использование некомпетентности, непрофессионализма или небрежности персонала для получения доступа к информации.
- **DoS (Denial of Service, «отказ в обслуживании»)** – хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.

Хакер

- Человек, увлекающийся исследованием подробностей (деталей) программируемых систем, изучением вопроса повышения их возможностей, в противоположность большинству пользователей, которые предпочитают ограничиваться изучением необходимого минимума.
- Кто-либо, программирующий с энтузиазмом (даже одержимо) или любящий программировать, а не просто теоретизировать о программировании.
- Человек, который силён в быстром программировании.
- Эксперт по отношению к определённой компьютерной программе или кто-либо часто работающий с ней.
- Злоумышленник, добывающий конфиденциальную информацию в обход систем защиты (например, «хакер паролей», «сетевой хакер»).
- Эксперт в компьютерной безопасности, ищущий слабые места в системе, который либо их исправляет, либо использует в своих корыстных целях.

Виды хакеров

Хакеры классифицируются в соответствии с целью их действий.
Следующий список классифицирует хакеров в соответствии с их намерением.

Символ	Описание
	**Ethical Hacker (Белая шляпа):** специалисты, обладающие глубокими знаниями в области ИТ и использующие их для защиты систем. Они также могут выполнять тестирование на проникновение и оценку уязвимости.
	**Взломщик (черная шляпа):** специалисты, обладающие глубокими знаниями в области ИТ и использующие их для осуществления незаконной, вредоносной и деструктивной деятельности
	**Серая шляпа:** специалисты, использующие свои знания и навыки в области ИТ и хакерских техник как в легальных, так и незаконных целях.

Виды хакеров

Символ	Описание
	**Script kiddies:** низкоквалифицированные люди, которые пытаются взламывать системы путем использования готовых скриптов и утилит не понимая принципов их работы.
	**Хактивист:** хакеры, использующие свои умения и навыки для продвижения политических идей, свободы слова, защиты прав и др.
	**Фрикер:** люди, которые выявляют и используют слабые места в телекоммуникационных сетях операторов связи.

Виды хакеров

Символ	Описание
	**Кибертеррористы:** хакеры, использующие свои умения и навыки в террористических целях (взлом критически важных систем, пропаганды идей и ценностей терроризма).
	**Хакеры, спонсируемые государством:** хакеры, использующие свои умения и навыки в интересах и под контролем государства.
	**Хакеры-суизидники (по Ec-Council CEH):** хакеры, ставящие своей целью причинение огромного ущерба без каких-либо на то целей, не заботящиеся о сокрытии своих действий и не боящиеся наказания.

Основные области хакинга

- **Web-Hacking** - взлом сайтов и все что с этим связано
- **Network Hacking** - взлом сетей и всего сетевого
- **OSINT** (open source intelligence) - разведывательная дисциплина и комплекс мероприятий, инструментов и методов для получения и анализа информации из открытых источников.
- **Forensic** - цифровая (компьютерная) криминалистика, прикладная наука о раскрытии преступлений, связанных с компьютерной информацией, об исследовании цифровых доказательств, методах поиска, получения и закрепления таких доказательств.
- **Anonymity** – сокрытие истинной личности в сети, настройка безопасной машины, VPS, подмена ip и др.
- **Reverse Engineering** или обратная разработка (обратное проектирование, обратный инжиниринг, реверс-инжиниринг) - исследование некоторого готового устройства или программы, а также документации на него с целью понять принцип его работы; например, чтобы обнаружить недокументированные возможности (в том числе программные закладки), сделать изменение или воспроизвести устройство, программу или иной объект с аналогичными функциями, но без прямого копирования.
- **Application Security** (безопасность приложения) - включает в себя меры, принимаемые для повышения безопасности приложения, часто путем обнаружения, исправления и предотвращения уязвимостей в безопасности.

Основные области хакинга

- **Социальная инженерия** - психологическое манипулирование людьми с целью совершения определенных действий или разглашения конфиденциальной информации, совокупность уловок с целью сбора информации, подделки или несанкционированного доступа от традиционного «мошенничества» отличается тем, что часто является одним из многих шагов в более сложной схеме мошенничества .
- **Тестирование на проникновение (пентест)** - метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника. Процесс включает в себя активный анализ системы на наличие потенциальных уязвимостей, которые могут спровоцировать некорректную работу целевой системы, либо полный отказ в обслуживании. Анализ ведётся с позиции потенциального атакующего и может включать в себя активное использование уязвимостей системы. Результатом работы является отчёт, содержащий в себе все найденные уязвимости системы безопасности, а также может содержать рекомендации по их устранению. Цель испытаний на проникновение — оценить возможность его осуществления и спрогнозировать экономические потери в результате успешного осуществления атаки.
- **Wi-FI Hacking** - взлом беспроводных сетей.
- **Coding** (компьютерное программирование) - набор определенных инструкций которые передаются электронному устройства для выполнения задания/действия, используя язык который понятен этому устройству, написание скриптов, программ для взлома.

Виды киберпреступлений

- **Компьютерное мошенничество:** преднамеренный обман для личной выгоды с использованием компьютерных систем.
- **Нарушение конфиденциальности:** раскрытие личной информации, такой как адреса электронной почты, номера телефонов, данных учетной записи и т.д. в социальных сетях, на веб-сайтах и др. ресурсах.
- **Кража личных данных:** кража личной информации и выдача себя за этого человека.
- **Нарушения авторского права и смежных прав:** распространение защищенных авторскими правами файлов, таких как электронные книги, компьютерные программы и т. Д.
- **Электронный перевод средств:** получение несанкционированного доступа к банковским компьютерным сетям и незаконные переводы средств.
- **Отмывание электронных денег:** использование компьютера для отмывания денег.

Виды киберпреступлений

- **Мошенничество с банкоматом:** перехват данных банковской карты, таких как номер счета и PIN-коды. Эти данные затем используются для снятия средств с перехваченных счетов.
- **Атаки отказа в обслуживании:** использование компьютеров в нескольких местах для атаки на серверы с целью их отключения.
- **Спам:** отправка несанкционированных писем, как правило, содержащих рекламную информацию.
- **Распространение противоправной информации**: клевета, порнографические материалы, реклама наркотиков, распространение идей терроризма, экстремизма и сепаратизма, призывы к насилию, свержению власти, расовой, сословной, религиозной и иной розни.
- **Распространение вредоносных программ и вирусов**

Виды компьютерных преступлений

В соответствии с Главой 7 **Уголовного кодекса Республики Казахстан** от 3 июля 2014 года № 226-V ЗРК к уголовным правонарушениям в сфере информатизации и связи относятся:

- неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций (статья 205);
- неправомерные уничтожение или модификация информации (статья 206);
- нарушение работы информационной системы или сетей телекоммуникаций (статья 207);
- неправомерное завладение информацией (статья 208);
- принуждение к передаче информации (статья 209);
- создание, использование или распространение вредоносных компьютерных программ и программных продуктов (статья 210);
- неправомерное распространение электронных информационных ресурсов ограниченного доступа (статья 211);
- предоставление услуг для размещения интернет-ресурсов, преследующих противоправные цели (статья 212);
- неправомерные изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства (статья 213).