Кибербезопасность и примеры атак

Дисклеймер: презентация не призывает кого-то взламывать, всё исключительно в познавательных целях для вашей же безопасности.

Статья 361. Незаконное вмешательство в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей, которое привело к искажению или уничтожению компьютерной информации или носителей такой информации, а также распространение компьютерного вируса путем применения программных и технических средств, предназначенных для незаконного проникновения в эти машины, системы или компьютерные сети и способных повлечь искажение или уничтожение компьютерной информации носил такой информации, -
наказываются штрафом до семидесяти необлагаемых минимумов доходов граждан или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

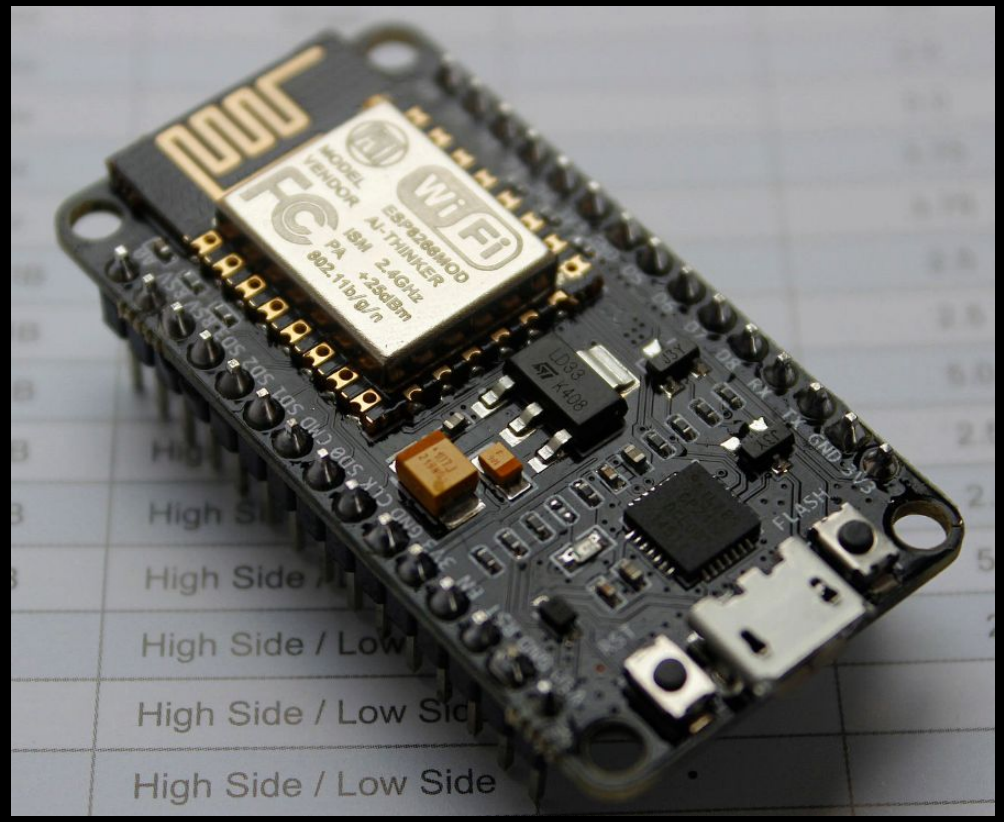
Что такое кибербезопасность?

Кибербезопасность – это реализация мер по защите систем, сетей и программных приложений от цифровых атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, на вымогательство у пользователей денег или на нарушение нормальной работы компаний.

Реализация мер эффективной кибербезопасности в настоящее время является достаточно сложной задачей, так как сегодня существует гораздо больше устройств, чем людей, а злоумышленники становятся все более изобретательными.

Почему кибербезопасность так важна?

В современном «подключенном» мире программы расширенной киберзащиты служат на благо каждого пользователя. На индивидуальном уровне атака со взломом киберзащиты может привести к разнообразным последствиям, начиная с кражи личной информации и заканчивая вымогательством денег или потерей ценных данных, например, семейных фотоснимков. Все зависят от критически важной инфраструктуры, например, электростанций, больниц и компаний, предоставляющих финансовые услуги. Защита этих и других организаций важна для поддержания жизнедеятельности нашего общества.



ESP8266 - микроконтроллер китайского производителя Espressif с интерфейсом Wi-Fi

80 MHz 32-bit процессор Tensilica Xtensa L106. Возможен негарантированный разгон до 160 МГц.
IEEE 802.11 Wi-Fi. Поддерживается WEP и WPA/WPA2.
14 портов ввода-вывода(из них возможно использовать 11)

Питание 2,2…3,6 В. Потребление до 215 мА в режиме передачи, 100 мА в режиме приема, 70 мА в режиме ожидания. Поддерживаются три режима пониженного потребления, все без сохранения соединения с точкой доступа: Modem sleep (15 мА), Light sleep (0.4 мА), Deep sleep (15 мкА).



Мини-компьютер Orange Pi Zero - это миниатюрный одноплатный компьютер на процессоре Allwinner H2+, в который входят четыре вычислительных ядра Cortex A7 с тактовой частотой до 1,2 ГГц. с открытым исходным кодом. Он может работать под управлением Android 4.4, Ubuntu, Debian. Он имеет 256 МБ DDR3 оперативной памяти SDRAM. Также этот мини-компьютер оснащен графическим ускорителем Mali-400MP2, который позволяет декодировать 4К-видео формата H.265/HEVC с частотой воспроизведения до 30 кадров в секунду и поддерживает microSD карты памяти ёмкостью до 64 гигабайт.

Атака MITM с помощью ESP8266

Атака MITM – Man In The Middle (Человек посередние). Вид атаки в криптографии, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом. Является методом компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

нагрузки на устройство жертвы с помощью перепрошитого Orange Pi Zero

Metasploit Framework — удобная платформа для создания и отладки эксплойтов.

Эксплоит (англ. exploit, эксплуатировать) — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программно обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой (повышение привилегий), так и нарушение её функционирования

DDOS атака

DDoS-атака (Distributed Denial of Service attack) - комплекс действий, способный полностью или частично вывести из строя интернет-ресурс.

1. Проведём ddos-test сайта нашего университета : https://e-u.in.ua
2. Проведём ddos-test wifi сети “European university”.

Важно знать!

Простым пользователям важно запомнить и выполнять пять простых и действенных правил защиты. А главное, не бояться сразу сообщать специалисту по кибербезопасности о возможной угрозе. Вы можете думать, что угроза миновала и с компьютером ничего не произошло, но malware достаточно клика, чтобы оказаться внутри сети.

- Не заходите на скомпрометированные или подозрительные интернет-ресурсы
- Не открывайте неизвестные e-mail, а тем более вложения в них, если вы не уверены, от кого именно пришло письмо. Проверяйте адрес, с которого пришло письмо
- Если вы все же открыли вложение и увидели, что файл выглядит как спам, содержит информацию, которая вас не касается и т.п., обязательно сообщите об этом специалисту по безопасности информационных систем
- Используйте сложные пароли и регулярно их меняйте
- Не поднимайте незнакомые флешки

Спасибо за внимание!