ВАРИАНТ 1

Организация VPN

- Проанализируйте существующие средства, применяемые для организации виртуальных частных сетей.
- Выберите для реализации какой-либо набор программных средств, из числа свободно распространяемых, например, OpenVPN.

Материалы по теме можно посмотреть, например, на таких ресурсах как:

https://www.opennet.ru/base/net/openvpn_office.txt.html
https://www.youtube.com/watch?v=XcsQdtsCS1U
https://eax.me/openvpn/
https://www.youtube.com/watch?v=BU4kTgnjzj4

- Организуйте VPN (виртуальную частную сеть) программными средствами OpenVPN или другими.
- Снифером Wireshark проанализируйте трафик в VPN туннеле при различных настройках конфигурации.
- Сравните другие возможные решения.
- По результатам работы составьте отчет и подготовьте выступление (на 8 -10 мин.) на защите проекта.

ВАРИАНТ 2

Распознавание подозрительного трафика

Материалы по теме можно посмотреть, например, на таких ресурсах как:

Finding Suspicious Traffic in Protocol Hierarchy
https://www.youtube.com/watch?v=OwQmwbD1uIs
Wireshark and Recognizing Exploits
https://www.youtube.com/watch?v=7iguG7va4l8

- Проанализируйте существующие средства и системы, применяемые для распознавания подозрительного трафика.
- Выберите, по возможности, какой-либо набор программных средств, из числа свободно распространяемых, для демонстрации.
- Сравните различные возможные решения.
- По результатам работы составьте отчет и подготовьте выступление (на 8 -10 мин.) на защите проекта.

ВАРИАНТ 3

L2 L3 Sockets spoofing

- Исследуйте возможности RAW-сокетов предоставляющих доступ к полям заголовков сообщений протоколов уровней L2 и L3 модели OSI.
Информацию по "сырым" сокетам можно найти, например, на таких ресурсах, как:

https://www.opensourceforu.com/2015/03/a-guide-to-using-raw-sockets/
https://www.binarytides.com/raw-sockets-c-code-linux/
http://www.kernel.org/doc/man-pages/online/pages/man7/packet.7.html
https://sock-raw.org/papers/sock_raw

или, воспользуйтесь множеством других источников.

- Разработайте и отладьте консольное приложение, обладающее возможностями спуфера пакетов, используя технологию RAW-сокетов. При отладке данного сетевого приложения используйте тестовые сегменты сети. Не допускайте исход модифицированных вашим приложением пакетов в публичную сеть.
- Продемонстрируйте возможности модификации полей заголовка, выбранного протокола с помощью разработанного приложения.
- По результатам работы составьте отчет и подготовьте выступление (на 8 -10 мин.) на защите проекта.

ВАРИАНТ 4

Intrusion Detection Systems

- Проанализируйте существующие средства и системы, применяемые для обнаружения вторжений.
- Выберите, по возможности, какой-либо набор программных средств, из числа свободно распространяемых (например, Snort), для демонстрации.
- Сравните различные возможные решения.
- По результатам работы составьте отчет и подготовьте выступление (на 8 -10 мин.) на защите проекта.

ВАРИАНТ 5

Аудит Wi-Fi сетей

- Проанализируйте существующие средства, применяемые с целью аудита и выработки рекомендаций по безопасности сетей Wi-Fi.
- Выберите какой-либо набор программных средств, из числа свободно распространяемых, например:

airodump (снифер для сетей стандарта 802.11),
aireplay (для инжекции Wi-Fi фреймов),
aircrack (взлом WEP и брутфорс WPA-PSK),
airdecap (декодирование перехваченных WEP/WPA файлов).

Набор средств может быть выбран и любым другим, платформа для установки и проведения исследования, также не лимитируется (Win/Lin/Mac).

- С помощью выбранных средств оцените уязвимость тестовой отдельной сети Wi-Fi. Испытайте сети Wi-Fi с различными существующими типами защиты.
- По результатам работы составьте отчет и подготовьте выступление (на 8 -10 мин.) на защите проекта.

ТРЕБОВАНИЯ К ОТЧЕТУ

По результатам курсового проектирования составляется отдельный (от лабораторных работ) отчет. Отчет должен быть оформлен с титульным листом с названием университета, института и высшей школы. На титульном листе указывается ф.и.о. студента исполнителя работы, номер студенческой группы и ф.и.о. преподавателя.

В отчете приводится аналитическая информация, скриншоты, таблицы, гистограммы, схемы, скрипты, исходные тексты и др., удостоверяющие раскрытие выбранной темы.

Защита курсового проекта происходит по предъявлению оформленного отчета и сопровождается демонстрацией исполнения программ, командных файлов, ответами на вопросы преподавателя, обсуждениями и т.д.

Файл отчета предпочтительно предоставлять в *pdf*-формате. Страницы пронумеруйте, укажите вашу фамилию и имя в названии файла.