

25.10.2023

Курс:

Практическая работа к уроку № Lesson_1

--

Введение в анализ сетевого трафика

Задание_1:

Ознакомиться с кодировкой **base64**.

Base64 — стандарт кодирования двоичных данных при помощи только 64 символов [ASCII](#). [Алфавит кодирования](#) содержит [латинские символы](#) A-Z, a-z, цифры 0-9 (всего 62 знака) и 2 дополнительных символа, зависящих от системы реализации. Каждые 3 исходных байта кодируются четырьмя символами

Исходный текст	M									a								n		
Коды ASCII	77 (0x4d)									97 (0x61)								110 (0x6e)		
Двоичный вид	0	1	0	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	
Полученный индекс в Base64	19							22						5					46	
Конечный результат в Base64	T							W						F					u	

Задание_2:

Провести аудит сетевого трафика:

- Скачать дамп .pcap, приложенный к уроку;
- Проанализировать трафик, найти секретное послание;
- Отчет приложить к домашнему заданию*.
- Задание сложное, совместная работа не возбраняется.

Задание_3:

Ознакомиться со статьями 28, 272, 273, 274 Уголовного кодекса по ссылке «УК с комментариями» в «Дополнительных материалах». Грань между легальным и нелегальным применением инструментов очень тонкая.

УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

- [Статья 272. Неправомерный доступ к компьютерной информации](#)
- [Статья 273. Создание, использование и распространение вредоносных компьютерных программ](#)
- [Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей](#)
- [Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации](#)
- [Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования](#)

[Неправомерный доступ](#) к охраняемой законом компьютерной информации, если это деяние повлекло [уничтожение](#), [блокирование](#), [модификацию](#) либо [копирование](#) компьютерной информации,

- наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.
- наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

Выводы:

Ссылки / дополнительные материалы

Вся информация в данной работе представлена исключительно в ознакомительных целях!
Любое использование на практике без согласования тестирования подпадает под действие УК РФ.

- <https://gb.ru>

Выполнил: AndreiM