ООО «НТЦ СОТСБИ»
191028, Россия, г. Санкт-Петербург, ул. Пестеля,
д. 7, литер А, помещение 14Н офис А
Тел.: (812) 273-78-27,
Факс: (812) 273-78-27, доб. 217
E-mail: info@sotsbi.ru
http://www.sotsbi.ru

НАСТОЛЬНЫЙ СЕТЕВОЙ ТРЕНАЖЕР НаСТя

I. Перечень тем лабораторных работ по направлению обучения «Инфокоммуникационные технологии»:

1. Визуальное знакомство с тренажером
2. Программное знакомство с тренажером
3. Основные аспекты работы в консоли
4. Работа с файлами
5. Управление процессами
6. Права доступа
7. Создание учетной записи пользователя
8. Изучение передаваемой информации в IP-сети
9. Изучение уровней модели TCP/IP
10. Добавление персонального компьютера (ПК) в сеть в ручном режиме (статическая адресация)
11. Добавление ПК в сеть в автоматическом режиме (DHCP)
12. Настройка соединения между маршрутизатором и сервером тренажера
13. Маршрутизация ПК тренажера (статическая)
14. Подключение ПК тренажера по беспроводной сети к маршрутизатору
15. Настройка беспроводной сети на маршрутизаторе тренажера
16. Проводное соединение между маршрутизаторами двух настольных сетевых тренажеров
17. Беспроводное соединение между маршрутизаторами двух настольных сетевых тренажеров
18. Беспроводное подключение ПК одного тренажера к серверу другого тренажера через его маршрутизатор
19. Беспроводное подключение смартфона к маршрутизатору
20. Организация точки доступа Wi-Fi на смартфоне
21. Удаленный доступ к компьютеру со смартфона по Wi-Fi сети
22. Подключение к персональным устройствам с компьютера по Bluetooth
23. Применение Bluetooth

II. Перечень тем лабораторных работ по направлению обучения «Информационная безопасность»:

1. Команды и утилиты для работы с сетью
2. Управление доступом
3. Telnet и SSH
4. Введение в криптоанализ
5. HTTPS
6. Защита от флуда (Flood):

Защита от флуда запросами протокола FTP на получение файла (FTP downloadflood)
Защита от флуда запросами протокола HTTP (HTTP flood)

Защита от флуда запросами протокола ICMP (ICMP flood)
Защита от флуда SYN-запросами протокола TCP (TCP-SYN flood)
Защита от загружающего канал потока данных протокола UDP (UDP flood)

7. Защита от атак направленных на отказ в обслуживании (DoS)

Защита веб-сервера от атаки запросами протокола HTTP (HTTP DoS)
Защита от атаки SYN-запросами протокола TCP (TCP-SYN DoS)
Защита от атаки FIN-запросами протокола TCP (TCP-FIN DoS)

8. Защита от распределенных атак (DDoS)

Защита от DDoS SYN-запросами протокола TCP (TCP-SYN DDoS)
Защита от DDoS FIN-запросами протокола TCP (TCP-FIN DDoS)
Защита от распределенного потока данных протокола UDP для загрузки канала (UDP DDoS)

9. Защита от нарушения конфиденциальности.

Защита от подбора паролей (Brute-force)

10. Защита от исследования сети.

Защита от сканирования сети запросами ICMP (ICMP IP sweep)
Защита от сканирования сети запросами TCP (TCP IP sweep)
Защита от сканирования транспортных TCP-портов.
Защита сканирования транспортных UDP-портов.