QBF

ЗАЩИТА ОТ КОНКУРЕНТНОЙ РАЗВЕДКИ ИЛИ КАК НАЙТИ ИНСАЙДЕРА

ИВАН АВГУСТОН

ДИРЕКТОР ДЕПАРТАМЕНТА ИТ

e-mail: it@qbfin.ru

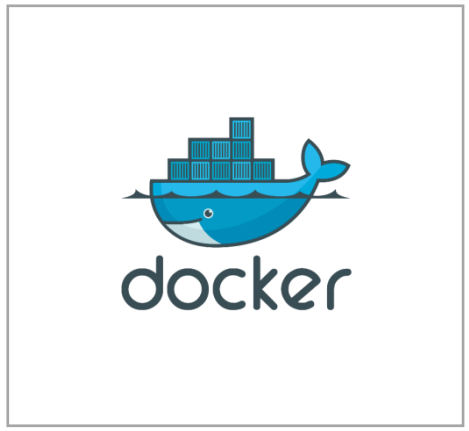
tel: 8(903)100-62-86

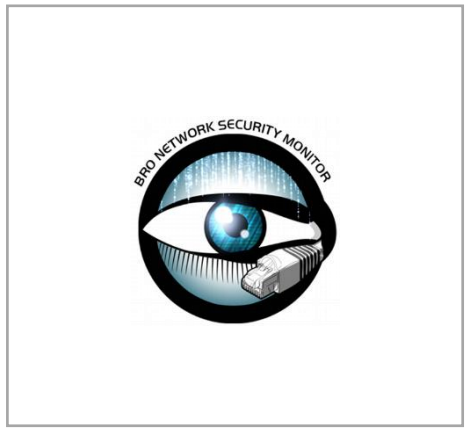
2017

Защита от конкурентной разведки или как найти инсайдера

- Правовая основа защиты (КТ, ПДн, регламенты)
- Сотрудник ИБ в роли инсайдера
- Подозрительные действия - маркеры инсайдеров
- Найти и отследить
- DLP, как избавиться от рутины

QBF Программы:





QBF Оборудование

QBF Подготовка

Защита сети

- Сегментация на подсети
- Контроль трафика между сегментами
- Токены доступа к АРМ и орг. Технике
- СКУД и Видеонаблюдение
- Контроль мессенджеров и электронной почты
- Контроль доступа съёмных устройств
- Контроль доступа к локальной сети
- Противодействие угону учетных записей и паролей

Регламенты и положения

- ПДн
- КТ
- Регламент на использование КТО
- Изменения в должностные инструкции

QBF Планирование атаки

Дано

- Права сотрудника клиентского офиса
- Перечь ценной информации и КТ
- Доступ в CRM

Задача

Совершить любое из следующих действий:

- Получить доступ к информации за рамками доступа учетной записи
- Получить доступ к БД
- Доступ к серверам CRM
- Доступ к охранным системам видеонаблюдения, СКУД
- Получить карту сети
- Нарушить работу сети путем:
  - MITM,
  - Broadcast шторма,
  - Манипулирования BPDU – пакетами,
  - Подключение своего DHCP, DNS серверов
- Использования утилит для повышения привилегий и получения паролей.

QBF История эксперимента

QBF Итоги эксперемента

- Взлом через локального администратора
- Взлом через почту
- Несанкционированное подключение устройства
- Проникновение через Wi-Fi
- Манипулирование пакетами с целью нарушения работы сети
- MITM атаки: ARP-spoofing; SMB Hijacking

QBF Что ищут инсайдеры?

Принято считать, что в основном инсайдеры действуют исключительно из-за желания заработать на продаже корпоративных секретов.

К сожалению, не всё так просто – очень часто оказывается, что корпоративными секретами делятся те, кого работодатель и так не обижал в финансовом плане, не получая при этом никакой материальной выгоды.

Мотивация инсайдера – один из основных ключей к его выявлению и обезвреживанию. Фактически, без понимания причин того, почему тот или иной сотрудник распространяет закрытую корпоративную информацию, достаточно трудно вывести его «на чистую воду» в сжатые сроки.

http://dehack.ru/arts/kak_raspoznat_insajdera_/

QBF Маркеры подозрительной активности

- Логи сервера БД с неправильным паролем
- Трафик запроса 404 страницы
- Прямая разведка сети, сетевые карты в неразборчивом режиме
- Рост трафика deny на маршрутизаторе локальной сети
- SNMP запросы
- Анализ лога прокси и поиск фраз в поиске «как взломать сайт»
- Подозрительный трафик на стандартных портах 80 443 25 993 135 445
- Заторможенность в работе рабочих станций и серверов, а также не стандартные процессы, сервисы
- Рассылка писем с доверенных адресов, содержащие файлы, либо ссылку с неявным призывом перейти, либо запустить файл (DLP)

СПАСИБО ЗА ВНИМАНИЕ!

QBF

ИВАН АВГУСТОН
ДИРЕКТОР ДЕПАРТАМЕНТА ИТ
e-mail: it@qbfin.ru
tel: 8(903)100-62-86