HACKBOX

CYBER SECURITY COMPETITION

- ИСТОРИЯ
- ПРАВИЛА
- МЕРОПРИЯТИЯ
- ТЕХНОЛОГИЯ
- ПЛАНЫ

ИСТОРИЯ

У истоков создания **Hackbox** стояли Илья Зеленчук и Максим Баклановский. Было известно, что хакеры, зачастую, люди не коллективные и не командные, в следствии этого Максимом Баклановским была предложена идея профессионального соревнования в личном зачете.

В 2009 году совместно с Виктором Мининым была сформирована идея создания **Hackbox**, соревнований, включающих в себя комплекс знаний и техник атак на компьютер оппонента. CTF, по большей части, направлена на решение определенных задач в области защиты информации, не часто встречающихся в реальных условиях. Предложенная идея **Hackbox** подразумевает под собой знания в области публичного тестирования на проникновение и эксплуатации уязвимостей, встречающихся в реальности.

В 2010 – 2011 году была составлена первая концепция этого соревнования. В это же время, организация “АРСИБ” начала активную поддержку и развитие данного проекта. В дальнейшем к проекту присоединился Артур Ханов и позже уже сформировался проект в текущем виде. Так же и возник другой вопрос, если с CTF все просто в этическом плане и это легко объяснить, что это не криминал, то в **Hackbox** применяются серьезные профессиональные знания, которые зачастую связаны с теневым сектором, и возникает тонкая грань отличия от криминала. Но в отличии от криминала, в таких соревнованиях отсутствует важная часть – невидимость она же анонимность. Поэтому **Hackbox** выступает в своем роде буфером для тех, кто уже прошел CTF и накопил необходимые техники и тем, кто уже способен использовать комплексные знания сам, без своей команды.

В 2017 году состоялась первая реализация **Hackbox** в рамках Кубка CTF России. Данный проект реализовал Усков Александр при поддержке "АРСИБ", Артура Ханова, Максима Баклановского, Евгения Егоренко. В дальнейшем надеемся на развитие и привлечение новых заинтересованных лиц в проект.Таким образом авторство стоит за упомянутыми выше людьми и организациями.

ПРАВИЛА

Участие – индивидуальное.

Каждому участнику выдается компьютер с предустановленным подмножеством программ и сервисов из рабочего набора. Рабочий набор представляет собой список ОС и программ.

В качестве условия победы считается доведение компьютера противника до неспособности выполнять функции. Например, отключение компьютера, BSOD, Kernel Panic, также получение доступа, замена картинки рабочего стола. Перезагрузка компьютера более 3 раз.

Разрешается использовать флешку с набором необходимых инструментов.

На действия участников будет накладываться минимум ограничений – для победы над компьютером противника будет разрешено использовать абсолютно любые средства, кроме следующих пунктов:
– полностью запрещён физический контакт участников с инфраструктурой и компьютером противника.
– запрещены целенаправленные атаки на сетевую инфраструктуру, обеспечивающую функционирование соревнований.
– запрещено физическое воздействие на оппонента.
– запрещена порча турнирного оборудования.

МЕРОПРИЯТИЯ

HACKBOX

- 3 игровых часа
- ~30 минут на сессию
- единый для всех уязвимый образ
- трансляция действий участников в прямом эфире
- впервые представлен на Кубке CTF России, который проходил с 8 по 9 декабря 2017 года в Сколково. https://ctfcup.ru

СТАТИСТИКА

8	>15	16	4
КОМПЬЮТЕРОВ	УЯЗВИМОСТЕЙ	УЧАСТНИКОВ	УЯЗВИМЫХ СЕРВИСА

ТЕХНОЛОГИЯ

ВИРТУАЛЬНЫЙ ОБРАЗ

В первой версии использовался набор: виртуальный образ OS Windows XP с запущенным сервисом IIS, службой telnet, ssh и 3 дополнительными уязвимыми сервисами.
Все это управлялось средством виртуализации Oracle VirtualBox.
Каждый набор был идентичен для каждого участника, тем самым найдя уязвимости в своей системе, участник мог эксплуатировать это на машине оппонента.

ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Использование системы виртуализации Vmware/Vbox.
Процессор не ниже Intel core i5 или аналог AMD с поддержкой процессором технологии виртуализации Intel-VT/AMD virtualization.
Не менее 8 GB оперативной памяти.
Возможность использования программ для захвата экрана при проведении трансляции.
Настройка VLAN для изоляции от других участников (видно только оппонента).
Настройка snapshot для быстрого восстановления исходного состояния VM.
Установка необходимого софта.

УЯЗВИМЫЕ СЕРВИСЫ

- IIS
- Syncbreez
- Diskboss
- MiniMail

ТИПЫ УЯЗВИМОСТЕЙ

- DoS
- RCE
- Подбор паролей(windows, telnet, ssh)
- Smb атаки
- Переполнение буфера

ПЛАНЫ

Отойти от использования виртуальных машин и перейти на реальное железо. Использовать ноутбуки прошлых лет с совместимыми версиями ОС.

Разработка различных сервисов для эсплуатации уязвимостей на них.

Логгирование всех событий.

Визуализация и трансляция.

Для предложений и получения подробной информации uas@aciso.ru