Техническое задание
на оказание услуг по проверке устойчивости внешней инфраструктуры
АО БАНК «СНГБ» к DDoS-атакам.

Срок предоставления ТКП	**07.05.2020**
Адрес направления ТКП	**obit@sngb.ru,** дополнительный **fiv@sngb.ru**
Контакты	+7 (3462) 39-88-88 доб. 2107

1.1. Исполнитель не имеет права привлекать внешних исполнителей.

1.2. Обязательное наличие лицензии ФСТЭК России на деятельность по технической защите конфиденциальной информации, предусмотренных подпунктами «б», «д» или «е» пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации №79.

1.3. Срок исполнения всех обязательств: **не позднее 01.06.2020г,**;

1.4. Опыт работы с банками не менее 3 (трех) лет, просим участников подтвердить рекомендательными письмами.

1.5. Условия по оплате, с указанием отдельно стоимости НДС: 100% оплата поэтапная по факту выполнения работ каждого этапа. Стоимость командировочных расходов указывается отдельной позицией. Необходимо предоставить стоимость по каждому этапу с указанием объема и формы предоставления услуги.

1.6. Обязательное указание в ТКП сроков и стоимости по каждому этапу работ;

1.7. Отсутствие Исполнителя в санкционном списке: https://sanctionssearch.ofac.treas.gov/.

1.8. Исполнитель гарантирует выполнение взятых на себя обязательств по Договору в случае попадания в санкционные списки.

1.9. Результатом является подробный отчет с описанием хода тестирования, выявленных нарушения функционирования и экспертными рекомендациями по их устранению.

Обязательно получите подтверждение о принятии Вашего ТКП представителем Банка в работу.

С целью проведения проверки по устойчивости внешней инфраструктуры АО БАНК «СНГБ» к DDoS-атакам, прошу выставить коммерческое предложение по нагрузочному тестированию имитирующего проведение DDoS-атаки.

Проведение проверки устойчивости к DDoS-атакам

Примечание

- Специалисты исполнителя должны быть доступны в режиме онлайн для связи.
- На первом этапе атака проводится на инфраструктуру как есть, на втором этапе на каждый канал после переключения.
- Исполнитель не имеет право привлекать внешних исполнителей.
- Обязателен опыт проведения подобных работ не менее трех лет для организаций финансового сектора.
- Готовность проводить работы совместно со специалистами Заказчика во внерабочее время (праздничные и выходные дни, в том числе в ночные часы).

Описание

Специалистами Исполнителя эмулируются основные типовые атаки на отказ в обслуживании (распределенные и нераспределенные), которыми пользуются злоумышленники. Тестирование проводится на различных уровнях сетевой модели OSI. Работы проводятся поэтапно, с **постепенным возрастанием силы атаки.**

a. UDP/TCP-connect flood (Атака на канал)

Тестирование производится путем генерации большого объема входящего трафика UDP или TCP с множества удаленных хостов, расположенных в сети Интернет. Атака направлена на исчерпание пропускной способности канала, что приводит к невозможности использования его в легитимных целях. Проверяется устойчивость к высоким нагрузкам пограничного сетевого оборудования, образующего внешний периметр корпоративной инфраструктуры.

b. TCP-SYN flood (Атака на исчерпание ресурсов ОС)

Тестирование производится посредством инициализации большого количества одновременных полуоткрытых TCP-соединений с множества удаленных хостов, расположенных в сети Интернет. При этом на атакуемой системе возможно переполнение очереди на подключения, что приводит к невозможности установления легитимных подключений.

c. Атаки прикладного уровня (Атака на исчерпание ресурсов ОС или сервиса)

Тестирование производится путем эксплуатации специфических для конкретного серверного программного обеспечения слабостей, приводящих к исчерпанию системных ресурсов либо мгновенному отказу в обслуживании. При этом генерируется небольшое количество сетевого трафика, что представляет собой дополнительную сложность при обнаружении подобных атак. В частности, производится тестирование на устойчивость к таким типам атак, как Slow Read, Slow POST, Slowloris, Hash Collision, SSL Renegotiation и т.д.

Параметры приведены в таблице 1 к техническому заданию.

IP-адреса: 91.209.17.0/24 (16 шт.)

Количество каналов: 3шт., суммарная 230 Мбит/с

Время эмуляции DDOS-атаки: не более 6 часов.

Эмулирования DDoS-атаки: до 5 Гбит/с

Методология проверки устойчивости к DDoS-атакам

Этап 0: согласование работ.

Перед началом работ, заказчик предоставляет специалистам набор IP-адресов и доменов, определяющих инфраструктуру сети, которая будет подвергнута тестированию на устойчивость к DDoS-атакам. Кроме того, согласуются временные рамки атаки, какие параметры будут измерены на *стороне атакующего и на стороне атакуемого*, каким образом будет проводится анализ приложений (для проведения атаки на прикладном уровне).

Этап 1: изучение атакуемой инфраструктуры и определение слабых мест.

На первом этапе специалисты Исполнителя исследуют инфраструктуру сети, которая будет подвержена DDoS-атаке. При этом исследование может быть (в зависимости от заключенного договора и определенного технического задания) как методом “черного”, так и методом “белого” ящика. В процессе исследования определяются характеристики серверов, состав и версии ПО, доступного извне. Кроме того, выявляются слабые места доступных извне приложений (например, Web-страницы, которые позволяют инициировать время- и ресурсо- затратные запросы к серверной (backend) части инфраструктуры).

Этап 2: проведение тестирования.

На этом этапе непосредственно проводится тестирование и измеряются статистические показатели. Тестирование разбито на несколько пунктов: нагрузочное тестирование серверных приложений, нагрузочное тестирование канала, атаки DoS на серверные приложения, атаки на backend. В процессе каждого пункта, происходит постепенное увеличение нагрузки (например, на этапе атаки на канал, тестирование может начаться с 20Mbps и, при возможности, продолжаться до заполнения всей полосы пропускания канала тестируемой инфраструктуры).

2.1. Нагрузочное тестирование серверных приложений представляет из себя эксплуатацию специфических для конкретного серверного программного обеспечения слабостей, приводящих к исчерпанию системных ресурсов либо мгновенному отказу в обслуживании. В зависимости от серверного ПО, содержание этого пункта может изменяться, но обычно проводятся следующие атаки:

- Большое количество одновременных соединений (исчерпание памяти, процессорного времени или количества файловых дескрипторов приложения или операционной системы);
- Атаки Slow HTTP Read/Slow HTTP POST (исчерпание памяти, файловых дескрипторов или числа потоков-обработчиков);
- Атаки чтения малым размером TCP-окна для протоколов, отличных от HTTP;
- SSL Renegotiation (исчерпание процессорного времени или числа потоков-обработчиков);
- Hash collision.

2.2. Эксплуатация уязвимостей Denial of Service в серверном или backend- ПО. В случае наличия уязвимостей отказа в доступе в установленном в инфраструктуре ПО, специалисты пытаются их проэксплуатировать и таким образом нарушить работу ПО. Атаки такого рода могут вообще не занимать канал, но приводить к полной неработоспособности инфраструктуры.

2.3. Атаки на приложения. Проводятся, если на этапе 1 были выявлены уязвимости функционала в backend-приложениях, которые могут вызвать высокую степень потребления различных ресурсов инфраструктуры (памяти, дискового пространства, процессорного времени и.т.д.).

2.4. Нагрузочное тестирование канала. При помощи ПО Mausezahn, тестовые сервера начинают генерировать большой объем трафика (TCP SYN или UDP-пакетов), достигающий нескольких Гбит/с. Атака такого рода рассчитана на исчерпание пропускной способности входящего канала инфраструктуры. Кроме того, проверяется устойчивость пограничного сетевого оборудования (маршрутизаторов, файрволлов и т.п.) к высоким показателям bps (бит в секунду) и pps (пакетов в секунду).

В процессе проведения тестирования, заказчик может (при желании) измерять различные показатели нагрузки своей инфраструктуры, такие как:

- Потребление ресурсов центрального процессора, %;
- Потребление оперативной памяти, Мб;
- Количество свободных дескрипторов;
- Количество запущенных процессов;
- Работа с дисковой подсистемой;
- Время обработки запроса, мс.;
- Количество открытых соединений;
- Занятая полоса пропускания канала (входная и выходная), бит/с.

Этап 3: анализ результатов.

По окончанию тестирования проводится анализ результатов с учетом временных интервалов доступности инфраструктуры и параметров, измеренных на стороне заказчика (см. этап 2). По окончанию анализа специалисты составляют отчет о проведенном тестирования и вырабатывают общие рекомендации по повышению устойчивости к DDoS-атакам. При необходимости, согласовываются сроки проведения повторного (ых) тестирования.

Таблица 1 – Ресурсы для DDOS

№ п/п	Наименование	Сценарий 1	Сценарий 2	Сценарий 3	Сценарий 4	Всего
	Количество IP участвующих в сценарии	16	10	15	10	16

Сценарий.1. Атака на израсходование пропускной способности канала связи
Сценарий.2. Атака, направленная на израсходование ресурсов веб-сервера Системы
Сценарий.3. Атака, направленная на израсходование ресурсов компонента Системы
Сценарий.4. Атака, направленная на израсходование ресурсов компонента Системы через веб-запросы