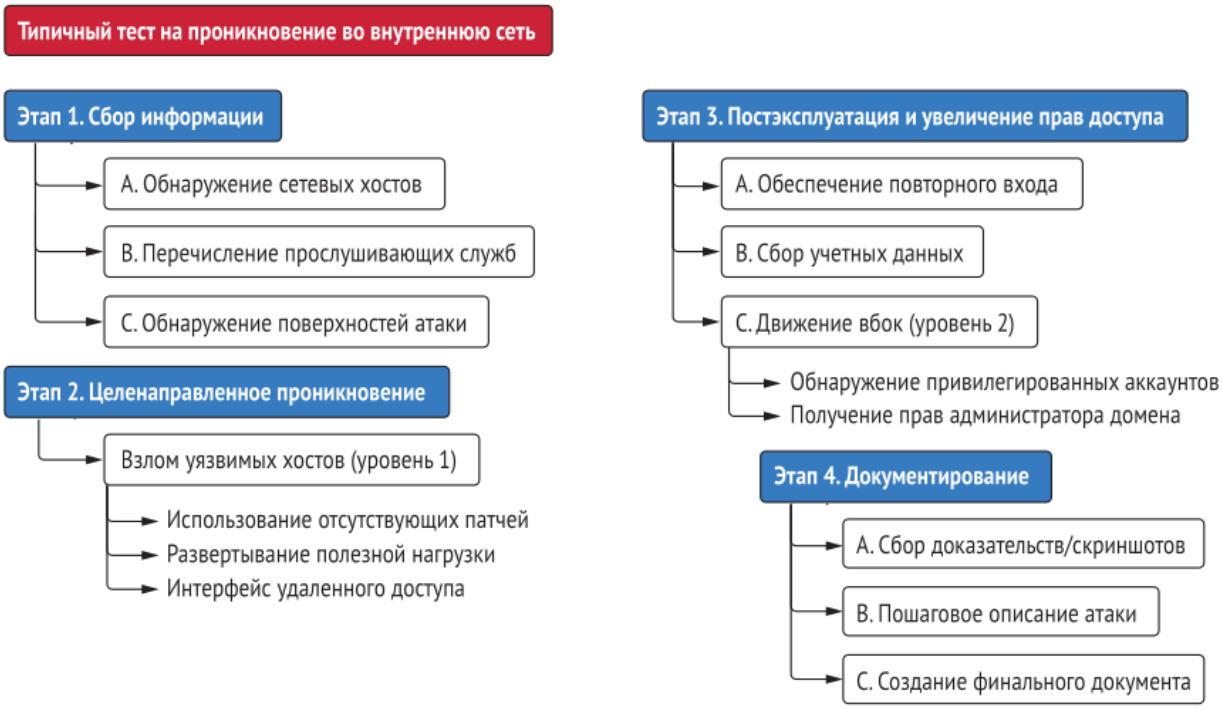
Основные этапы тестирования. – Telegraph

telegra.ph/Osnovnye-ehtapy-testirovaniya-06-21

Life-Hack - Linux/Хакинг/Хакер/ИБ/Osint June 21, 2024

Стандартная процедура тестирования на проникновение включает в себя четыре этапа, выполняемых по порядку, как показано на рисунке ниже. Называть каждый этап можно по-разному, не обязательно придерживаться имеющихся терминов. Например, часто применяется слово "разведка", вместо "сбора информации", или термин "доклад" вместо "документации". Несмотря на различия в названиях этапов, большинство специалистов в данной области придерживаются одинакового перечня задач на каждой стадии тестирования.



Этап 1 – сбор информации:

a) составление карты сети;

b) определение возможных целей;

c) перечисление слабых мест в службах, работающих на этих целях.

Этап 2 – целенаправленное проникновение:

a) взлом уязвимых сервисов (получение к ним несанкционированного доступа).

Этап 3 – постэксплуатация и повышение привилегий:

a) сбор информации о скомпрометированных системах, которая может быть использована для дальнейшего доступа (закрепления в системе);

b) поднятие привилегий до самого высокого уровня доступа, фактически стать системным администратором компании;

Этап 4 – документирование:

a) сбор доказательств проникновения;

b) составление окончательного отчета.

После выполнения первых трех этапов, пентестер мысленно покидает позиции злоумышленника и превращается в консультанта. Оставшееся время он посвящает составлению максимально подробного отчета. Этот отчет содержит детальное описание всех способов, которыми удалось взломать сеть и обойти меры безопасности, а также предложение мер, которые компания может предпринять,

чтобы закрыть эти выявленные бреши и гарантировать, что они больше не будут использованы кем-либо еще. Процесс составления отчета обычно занимает около 40 часов в 9 из 10 случаев, однако необходимое время может варьироваться в зависимости от размера организации.