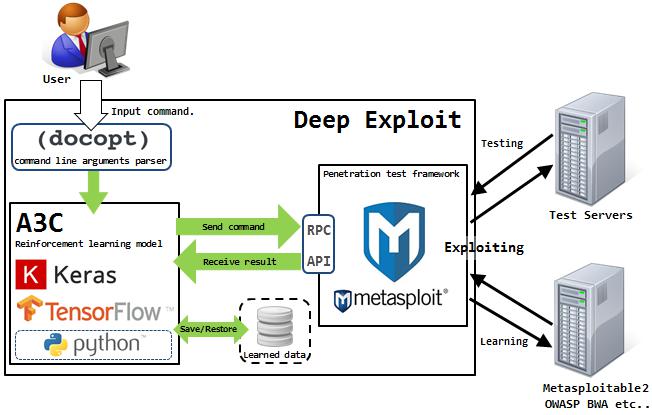
В хэш файлов с дз6 и дз7 полностью совпадает, значит схема точно таже. Описание прошлой схемы в файле 8. При использовании Big Data в сети DMZ на Postgre SQL нам необходимо использовать эффективные алгоритмы по обработке данных, а так же следить за расходуемой памятью, иначе может возникнуть DOS – отказ в обслужовании. При масштабировании Big Data необходимо это учитывать при настройке серверов. Использовать Big Data Security and Privacy Handbook. Так же необходимо защититься от 5 угроз

* Риск нарушения конфиденциальности.
* Риск потери данных.
* Риск снижения эффективности при формировании набора данных.
* Риск ошибок данных и ошибок бизнес-модели.
* Риск мошенничества.

При использовании NN стоит создать как минимум 2 сети одна будет учиться атаковать, а другая отражать атаки. Подобные практики использует яндекс. Пример NN для атаки был в методичке.



На ней видно как пользователь командами тренерует сеть через Metasploit и Metasploitable.

Нейросети поставить на стыке Интернета и DMZ.

Установить AI на стыке интернета и DMZ, а так же AI внутри inside сети. Регулярно давать задачи на решение искусственному интеллекту и проверять на атаки (пентест, red team).

Альтернативый вариант можно перенести базу данных на облачные технологии google или яндекс, но тогда внутренние злоумышленники таких компаний смогут ее похитить, что тоже плохо. Но с другой стороны файлы на таких серверах защищены хорошо. Так же можно использовать облачные технологии для создания backup.

Web сервер NGINX можно запустить на виртуальной машине и в случае компрометации у злоумышленника будет меньше шансов получить права админа в основной системе. Но следует пробросить подключение к базе данных, которая будет на основной системе. Все остальные сервисы можно запустить в контейнерах, которые лучше всего самим собрать, или скачать с доверенных репозиториев и проверить хэш суммы на подлинность. Самая большая уязвимость контейнеров в том, что они используют одно ядро, и если у нас windows 7 с eternal blue, то мы имеем серьезную уязвимость.