## Лекция 2.5. Инструменты обработки сетевых пакетов на Python

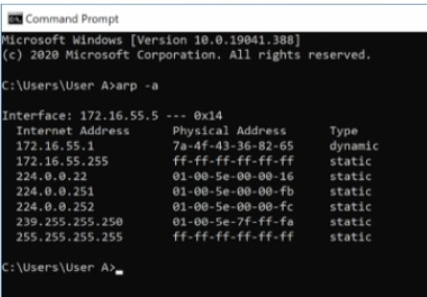
В ходе лекции будут рассмотрены:  
1. ARP-спуфинг.  
2. Этапы и типы атак.  
3. Цель отравления ARP.  
4. Методы предотвращения отравления ARP.

### Глава 1. Инструменты обработки сетевых пакетов на Python

С помощью Python можно создавать приложения для захвата, анализа и модификации сетевых пакетов на низком уровне, а также для разработки высокоуровневых сетевых протоколов и сервисов.  
Python представляет собой мощный инструмент для обработки сетевых пакетов и разработки сетевых приложений, который может быть использован для выполнения широкого спектра задач, связанных с сетевой безопасностью, мониторингом и администрированием.  
1. «Scapy» —это библиотека Python для создания и отправки сетевых пакетов.  
2. «Pyshark» — это Python-обертка для Wireshark, популярной программы для анализа сетевого трафика.  
3. «Dpkt» —это библиотека Python для работы с сетевыми пакетами.  
4. «Pcapy» —это библиотека Python для работы с сетевыми интерфейсами и захватом сетевого трафика.  
5. «Socket» —это встроенный модуль Python для работы с сокетами.  
Отравление ARP: что это такое и как предотвратить ARP-спуфинг  
Что такое ARP?  
ARP предназначен для определения MAC-адреса по IP-адресу другого компьютера. ARP позволяет подключённым к сети устройствам запрашивать, какому устройству в настоящее время назначен конкретный IP-адрес. Устройства также могут сообщать об этом назначении остальной части сети без запроса. В целях эффективности устройства обычно кэшируют эти ответы и создают список текущих назначений MAC-IP.  
Что такое отравление ARP?  
«Отравление» (подмена) ARP заключается в использовании слабых сторон ARP для нарушения назначений MAC-IP для других устройств в сети.  
Этапы отравления ARP могут различаться, но обычно их минимальный перечень таков:  
1. Злоумышленник выбирает машину или машины жертвы.  
2. Злоумышленник запускает инструменты и начинает атаку.  
3. Злоумышленник выполняет определённые действия с некорректно направленным трафиком.  
Типы атак ARP Poisoning  
Имеется два основных способа отравления ARP: злоумышленник может либо дождаться запроса ARP в отношении конкретной цели и дать на него ответ, либо использовать самообращённые запросы (gratuitous ARP). Первый вариант ответа будет менее заметен в сети, но его потенциальное влияние также будет меньшим. Самообращённые запросы ARP могут быть более эффективными и затронуть большее количество жертв, но они имеют обратную сторону — генерирование большого объёма сетевого трафика.  
При любом подходе повреждённый кэш ARP на устройствах-жертвах может быть использован для дальнейших целей:  
1. Атаки Man-in-the-Middle. Атаки MiTM, вероятно, являются наиболее распространенной и потенциально наиболее опасной целью отравления ARP.  
2. Отказ в обслуживании (Denial of Service, DoS). DoS-атака заключается в том, что одной или нескольким жертвам отказывается в доступе к сетевым ресурсам.  
3. Перехват сеанса. Перехват сеанса по своей природе похож на MiTM за исключением того, что злоумышленник не будет напрямую перенаправлять трафик с машины жертвы на целевое устройство. Вместо этого он захватывает подлинный порядковый номер TCP или файл cookie жертвы и использует его, чтобы выдавать себя за жертву.

### Глава 2. Инструменты обработки сетевых пакетов на Python

У хакеров всегда самые разные мотивы, в том числе при осуществлении отравления ARP, начиная от шпионажа высокого уровня и заканчивая азартом создания хаоса в сети. В одном из возможных сценариев злоумышленник может использовать ложные сообщения ARP, чтобы взять на себя роль шлюза по умолчанию для данной подсети, эффективно направляя весь трафик на своё устройство вместо локального маршрутизатора. Затем он может следить за трафиком, изменять или сбрасывать его. Такие атаки являются «громкими», поскольку оставляют за собой улики, но при этом необязательно влияют на работу сети. Если целью атаки является шпионаж, машина злоумышленника просто перенаправляет трафик изначальному адресату, не давая ему оснований подозревать, что что-то изменилось.  
Другой целью может быть значительное нарушение работы сети. Например, довольно часто DoS-атаки выполняются не очень опытными хакерами просто для получения удовольствия от созданных проблем.  
Опасным типом отравления ARP являются инсайдерские атаки. Поддельные сообщения ARP не выходят за пределы локальной сети, поэтому атака должна исходить от локального устройства. Внешнее устройство также потенциально может инициировать ARP-атаку, но сначала ему нужно удалённо скомпрометировать локальную систему другими способами, в то время как инсайдеру требуется только подключение к сети и некоторые легкодоступные инструменты.



Существует множество платных программ и программ с открытым исходным кодом для обнаружения отравления кэша ARP, однако проверить ARP-таблицы на своём компьютере можно даже без установки специального ПО. В большинстве систем Windows, Mac и Linux ввод команды arp-a в терминале или командной строке отобразит текущие назначения IP-адресов и MAC-адресов машины.  
Такие инструменты, как arpwatch и X-ARP, позволяют осуществлять непрерывный мониторинг сети и могут предупредить администратора о выявлении признаков отравления кэша ARP. Однако достаточно высока вероятность ложных срабатываний.

1. Как называется опасная техника атаки, при которой злоумышленник подменяет отправляемые или получаемые запросы, чтобы получить несанкционированный доступ к данным или провести манипуляции в сети?
   1. Оба ответа верны
   2. Подмена запросов
   3. Спуфинг
2. Какого типа атак спуфинга не существует?
   1. ARP-подмена
   2. IP-подмена
   3. URL-подмена
   4. DNS-подмена
   5. HTML-подмена
3. Во время какого типа атаки злоумышленник изменяет DNS-записи, чтобы перенаправить пользователей на фальшивые веб-сайты или серверы?
   1. ARP-подмена
   2. IP-подмена
   3. URL-подмена
   4. DNS-подмена
4. Во время какого типа атака злоумышленник подделывает свой IP-адрес, чтобы выглядеть как другой узел или клиент?
   1. ARP-подмена
   2. IP-подмена
   3. URL-подмена
   4. DNS-подмена
5. Во время какой атаки злоумышленник изменяет таблицы Address Resolution Protocol на сетевых устройствах, чтобы перехватывать или перенаправлять сетевой трафик?
   1. ARP-подмена
   2. IP-подмена
   3. URL-подмена
   4. DNS-подмена
6. Во время какого типа атаки злоумышленник подделывает URL-адреса, чтобы пользователи были перенаправлены на фальшивые или опасные веб-сайты?
   1. ARP-подмена
   2. IP-подмена
   3. URL-подмена
   4. DNS-подмена
7. Укажите правильный порядок этапов процесса подмены запросов:
   1. Перехват запроса, изменение данных, перенаправление запроса
   2. Перехват запроса, перенаправление запроса, изменение данных
   3. Перенаправление запроса, перехват запроса, изменение данных
   4. Изменение данных, перехват запроса, перенаправление запроса