УЯЗВИМОСТИ ARP И DNS В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Аблецов А.М

Белоусова Е.С – к.т.н., доцент

В работе рассматриваются уязвимости протоколов ARP и DNS в локальных вычислительных сетях. Для практической реализации атак использовалась утилита Ettercap. Также представлены рекомендации для исключения выявленных уязвимостей в локальных вычислительных сетях.

Локальная вычислительная сеть (англ. Local Area Network, LAN) – сеть, соединяющая оконечные устройства, расположенные на относительно небольшом расстоянии друг от друга (дом, офис, административное здание), с целью повышение эффективности работы оконечных устройств за счет совместного использования ресурсов, а также для доступа в глобальную вычислительную сеть (англ. Wide Area Network, WAN).

Сетевые протоколы, используемые для связи устройств в LAN и WAN были разработаны в конце XX, так например протокол ARP был внедрен в 1982 г., DNS – в 1983 г., DHCP – в 1990 г. Основными требованиями для данных протоколов были производительность и эффективность. Вопросам защиты информации уделялось незначительное внимание. Из этого следует, что сетевые протоколы обладают рядом уязвимостей.

Для демонстрации уязвимостей была использована схема, представленная на рисунке 1, которая реализует атаку «Человек по середине» (англ. Man In The Middle, MITM).

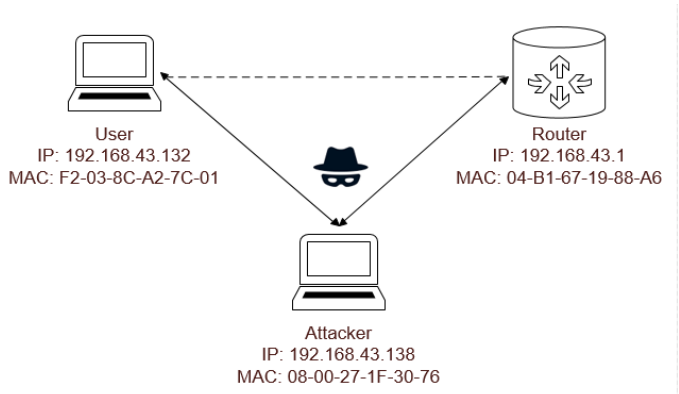

Рисунок 1 – Схема построения сети для демонстрации атаки MITM

Одним из основных протоколов LAN является ARP, предназначенный для сопоставления IP-адресам MAC-адресов. Информация об этих сопоставлениях хранится в оперативной памяти оконечных устройств (ARP-кэш). Протокол не предполагает какой-либо аутентификации. Следовательно, злоумышленник, инициализируя заведомо ложные ARP фреймы, способен изменить ARP-кэш устройств, находящихся с ним в пределах одной LAN, что используется для перенаправления трафика и реализации атаки MITM.

Для использования данной уязвимости злоумышленник (Attacker) с помощью утилиты Ettercap [1] изменил ARP-кэш на устройстве пользователя (User). На рисунке 2 представлен ARP-кэш до и после проведения атаки на устройстве User. Теперь весь трафик, направляемый в WAN от устройства User, проходит через устройство Attacker

```
C:\Users\admin>arp -a

Interface: 192.168.43.132 --- 0x2
  Internet Address      Physical Address      Type
  192.168.43.1          04-b1-67-19-88-a6     dynamic
  192.168.43.138        08-00-27-1f-30-76     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
```

```
C:\Users\admin>arp -a

Interface: 192.168.43.132 --- 0x2
  Internet Address      Physical Address      Type
  192.168.43.1          08-00-27-1f-30-76     dynamic
  192.168.43.138        08-00-27-1f-30-76     dynamic
  192.168.43.255        ff-ff-ff-ff-ff-ff     static
```

Рисунок 2 – ARP кэш на устройстве User до и во время проведения атаки соответственно

На рисунке 3 представлен процесс формирование устройством Attacker ложных ARP фреймов, который может быть отслежен с помощью сетевого анализатора Wireshark.

No.	Time	Source	Destination	Protocol	Length	Info
35	1.850110014	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76
36	1.850184590	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
37	1.860383541	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
38	1.860434579	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76
39	11.870838430	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76
40	11.870892220	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
41	11.881087308	PcsCompu_1f:30:76	XiaomiCo_19:88:a6	ARP	42	192.168.43.132 is at 08:00:27:1f:30:76 (duplicate use…
42	11.881126702	PcsCompu_1f:30:76	f2:03:27:a2:08:3e	ARP	42	192.168.43.1 is at 08:00:27:1f:30:76

Рисунок 3 – Формирование ложных ARP фреймов злоумышленником

В качестве примера было организовано HTTP соединение устройства User с интернет ресурсом, а также аутентификация пользователя. С помощью сетевого анализатора Wireshark, устройство Attacker просматривает содержимое перенаправленного трафика. Результат перехвата логина и пароля пользователя представлены на рисунке 4.

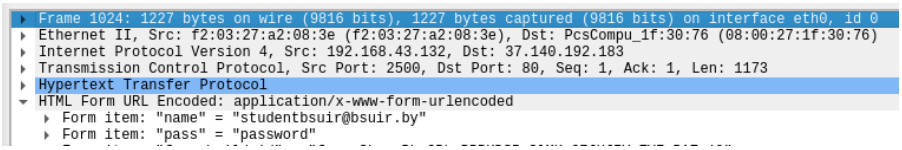

Рисунок 4. Результат перехвата пароля пользователя

Также с помощью уязвимости протокола ARP злоумышленник имеет возможность провести DNS-атаку. Протокол DNS предназначен для сопоставления IP-адресам доменных имен. Информация об этих сопоставлениях хранится в виде DNS-кэша на оконечных устройствах. Изменяя DNS-кэш, злоумышленник может перенаправить запрос пользователя на заведомо ложный IP-адрес.

Для проведения данной атаки устройство Attacker, с помощью утилиты Ettercap изменяет ARP-кэш на устройстве User. Затем, выступая в роли DNS-сервера, сопоставляет свой IP-адрес доменному имени, введенному на устройстве User. Таким образом, DNS-атака может применятся с целью вымогания денег, а также в качестве атаки «Отказ в обслуживании». На рисунке 5 представлены неудачные попытки устройства User получить доступ к интернет ресурсам.

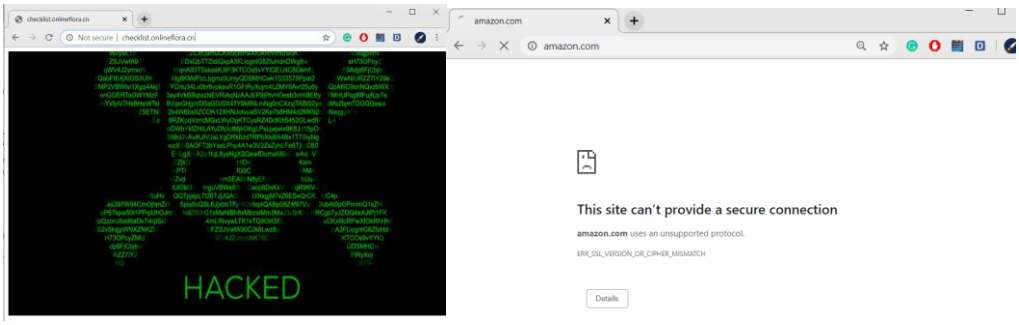

Рис 5. Попытки устройства User получить доступ к интернет ресурсам.

Для защиты от уязвимости ARP рекомендуется организовывать статическое заполнение ARP таблицы на оконечных устройствах, а также осуществлять разделение сети на VLAN. На рисунке 6 представлен фрагмент формирования статической таблицы ARP

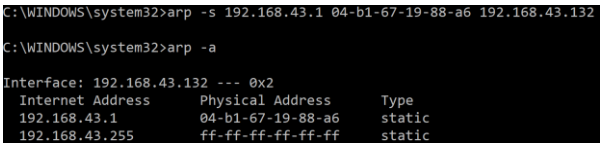

Рис 6. Формирования статической таблицы ARP

Список использованных источников:

Ettrecap manual [Электронный ресурс]. – Режим доступа: https://github.com/Ettercap/ettercap – Дата доступа: 25.03.2020