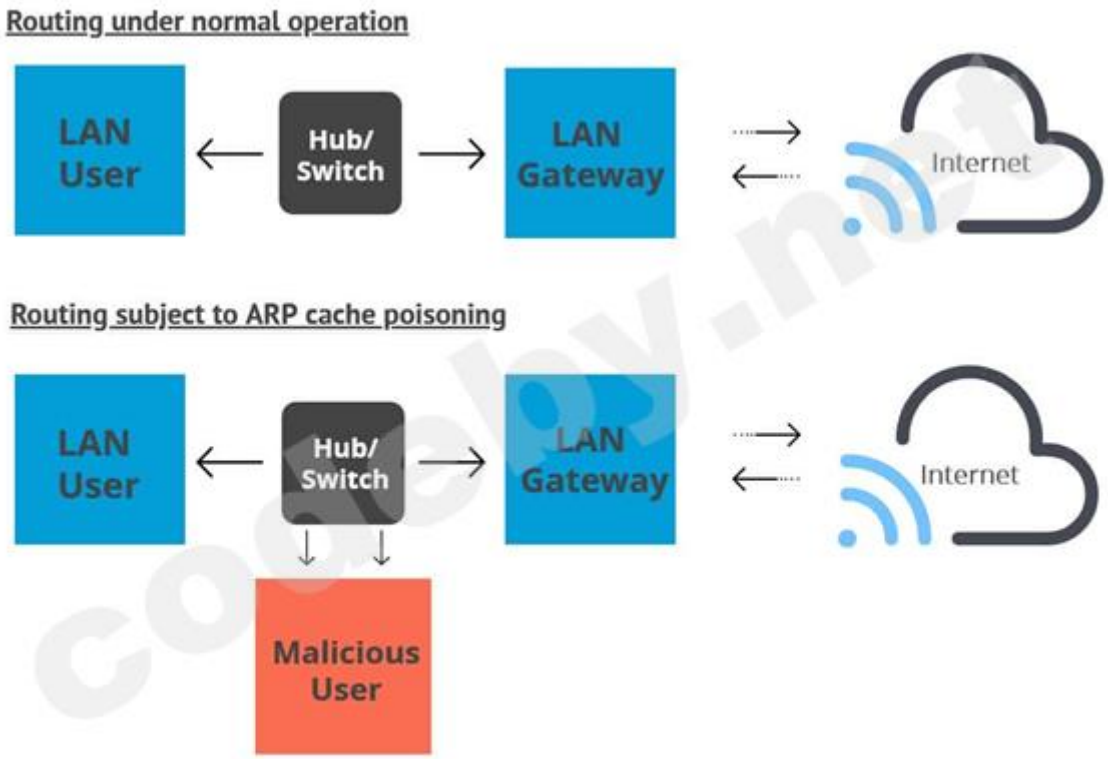
**Практикалық сабақ №12**:Address Spoofing шабуылынан қорғау




**Мекен-жайларды шешу протоколының залалдануы (Address Resolution Protocol (ARP))** - бұл жергілікті желі арқылы жалған ARP хабарламаларын жіберуді қамтитын шабуыл. Ол сондай-ақ **ARP спуфинг**, **ARP улану/жұқтыру** ретінде белгілі.

Бұл шабуылдар трафикті бастапқы жоспарланған хосттан шабуылдаушыға бағыттауға тырысады. ARP улану мұны шабуылдаушының **Media Access Control (MAC)** мекенжайын мақсатты IP-мекен-жайымен байланыстыру арқылы жасайды. Бұл тек ARP қолданатын желілерге қарсы жұмыс істейді.

ARP улану-бұл желілік трафикті тоқтату, оны өзгерту немесе ұстап алу үшін қолдануға болатын "ортадағы адам" *(man-in-the-middle)* шабуылының бір түрі. Бұл әдіс көбінесе сеансты ұстап алу немесе *DoS* шабуыл (denial-of-service) сияқты одан әрі шабуылдау әрекеттерін бастау үшін қолданылады.

## Адресті шешу протоколы (AddressResolutionProtocol (ARP)) дегеніміз не?

ARP-бұл IP мекенжайын тиісті физикалық машинаның арна деңгейінің мекен-жайымен байланыстыратын протокол.

ARP әдетте 32 биттік IPv4 мекенжайлары мен 48 биттік MAC мекенжайлары арасындағы алшақтықты жояды. Ол екі бағытта да жұмыс істейді.

MAC мекенжайы мен оның IP мекенжайы арасындағы байланыс ARP кэші деп аталатын кестеде сақталады. Түйінге бағытталған пакет шлюзге кіргенде, шлюз MAC мекенжайын немесе түйіннің физикалық мекенжайын корреляциялық IP мекен-жайымен байланыстыру үшін ARP қолданады.

Содан кейін хост өзінің ARP кэшінде іздейді. Егер ол тиісті мекенжайды тапса, онда мекен-жай пакеттің пішімі мен ұзындығын түрлендіру үшін қолданылады. Егер дұрыс мекен-жай табылмаса, ARP жергілікті желідегі басқа машиналардың дұрыс мекен-жайын білетіндігін сұрайтын сұрау пакетін жібереді. Егер машина мекен-жай арқылы жауап берсе, онда ARP кэші сол көзден болашақ сұраулар туындаған жағдайда жаңартылады.

## ARP улану / жұқтыру дегеніміз не?

ARP протоколы тиімді және жеткілікті жұмыс істеуге арналғанмен, бұл оның құрылымында қауіпсіздіктің айтарлықтай жетіспеуіне әкелді. Бұл, егер зиянкес өз мақсаттарының жергілікті желісіне қол жеткізе алса, шабуылдарды салыстырмалы түрде жеңілдетеді.

ARP улану жергілікті желі арқылы шлюзге жалған ARP жауап пакеттерін жіберуді қамтиды. Зиянкестер әдетте жұмысты жеңілдету үшін Arpspoof немесе Arppoison сияқты спуфинг құралдарын пайдаланады. Олар құралдың IP мекенжайын мақсатының мекен-жайына сәйкес орнатады. Содан кейін құрал мақсатты жергілікті желіні хосттардың IP және MAC мекен-жайлары үшін сканерлейді.

Шабуылдаушы хост мекен-жайларын алғаннан кейін, ол жалған ARP пакеттерін жергілікті желі арқылы хосттарға жібере бастайды. Алаяқтық хабарламалар алушыларға шабуылдаушының MAC мекен-жайы ол бағытталған машинаның IP-мекен-жайымен байланысты болуы керек екенін білуге тырысады.

Бұл алушыларға ARP кэшін шабуылдаушының мекен-жайы арқылы жаңартуға әкеледі. Болашақта алушылар сөйлескен кезде олардың хабарламалары шабуылдаушыға жіберіледі.

Бұл кезде шабуылдаушы жасырын түрде байланыс орталығында болады және трафикті оқу және деректерді ұрлау үшін осы позицияны қолдана алады.

Сондай-ақ, шабуылдаушы хабарламаларды мақсатқа жетпес бұрын өзгерте алады немесе тіпті байланысты толығымен тоқтата алады.

Зиянкестер бұл ақпаратты DoS шабуылдары (denial-of-service) немесе сеансты түсіру (sessionhijacking) сияқты қосымша шабуылдарды ұйымдастыру үшін пайдалана алады:

DoS шабуылы-бұл шабуылдар бірнеше жеке IP мекенжайларын мақсатты MAC мекен-жайымен байланыстыра алады. Егер мекен-жайлардың жеткілікті саны нысанаға сұрау жіберсе, онда ол трафикпен толып кетуі мүмкін, бұл оның қызметтерін бұзады және оны жарамсыз етеді.

SessionHijacking (сеансты ұстау) – ARP спуфингін хакерлер жүйелер мен есептік жазбаларға кіру үшін пайдаланатын сеанс идентификаторларын ұрлау үшін пайдалануға болады. Қол жеткізгеннен кейін олар өз мақсаттарына зиян келтіруі мүмкін.

## ARP залалдануын қалай анықтауға болады

ARP улану / залалдануды бірнеше түрлі жолмен анықтауға болады. Мысалы Windows пәрмен жолын, ашық бастапқы пакеттік анализаторды пайдалануға болады.

**Командалық жол**

Егер сіз ARP улануынан зардап шегуіңіз мүмкін деп күдіктенсеңіз, оны пәрмен жолында тексере аласыз. Алдымен әкімші ретінде пәрмен жолын(командная строка) ашыңыз.

Ең оңай жолы - Бастау мәзірін ашу үшін Windows пернесін басу. "Cmd" теріңіз, содан кейін Crtl, Shift және Enter пернелерін бір уақытта басыңыз.

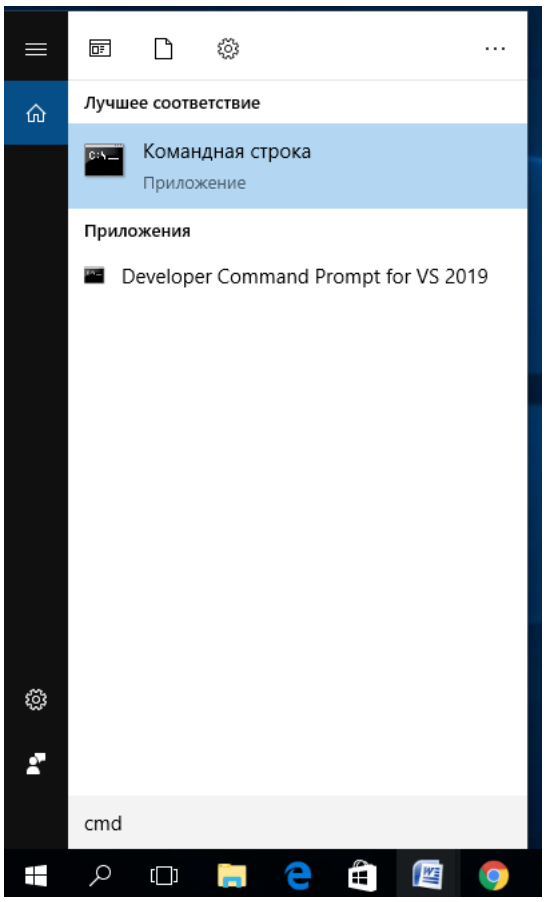
Бұл пәрмен жолын ашады, дегенмен бағдарламаға өзгерістер енгізуге рұқсат беру үшін "Иә" түймесін басу қажет болуы мүмкін.

Пәрмен жолына енгізіңіз:

Код:

*arp -1*

Бұл сізге ARP кестесін көрсетеді:




Ctrl+Shift+Enter

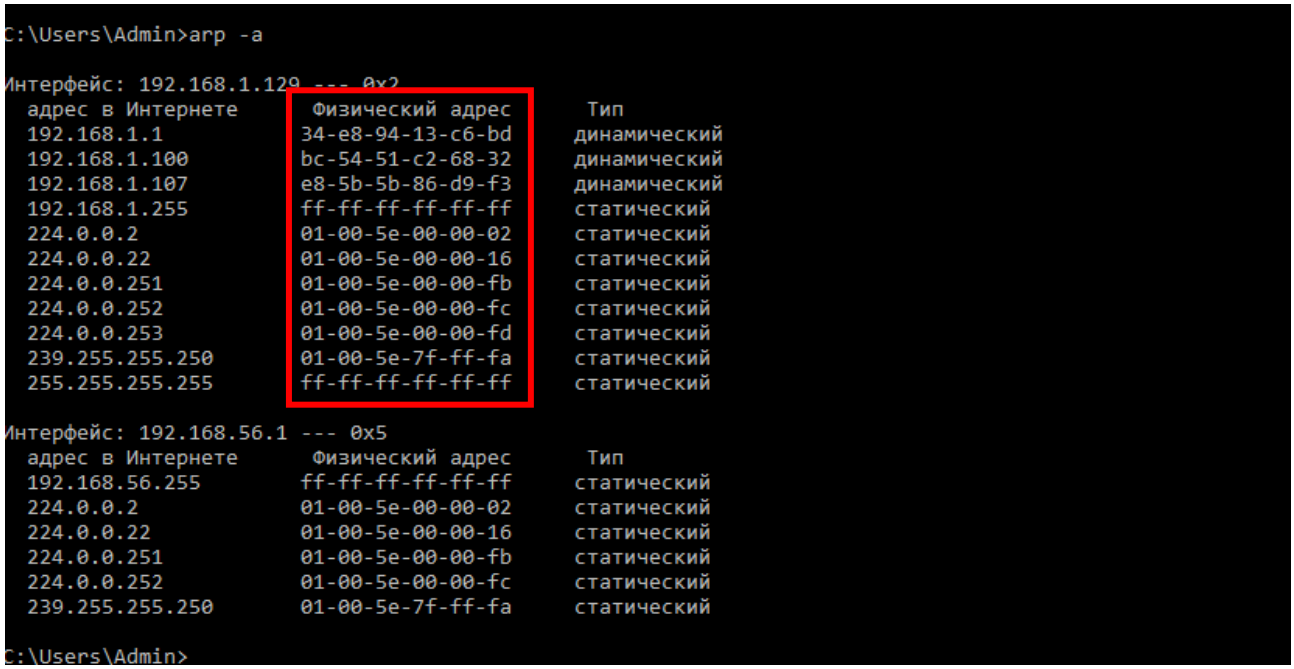
```
C:\Users\Admin>arp -1

Отображение и изменение таблиц преобразования IP-адресов в физические,
используемые протоколом разрешения адресов (ARP).

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr] [-v]

  -a            Отображает текущие ARP-записи, опрашивая текущие данные
                протокола. Если задан inet_addr, то будут отображены IP и
                физический адреса только для заданного компьютера. Если
                ARP используют более одного сетевого интерфейса, то будут
                отображаться записи для каждой таблицы.
  -g            То же, что и параметр -a.
  -v            Отображает текущие ARP-записи в режиме подробного
                протоколирования. Все недопустимые записи и записи в
                интерфейсе обратной связи будут отображаться.
  inet_addr     Определяет IP-адрес.
  -N if_addr    Отображает ARP-записи для заданного в if_addr сетевого
                интерфейса.
  -d            Удаляет узел, задаваемый inet_addr. Параметр inet_addr может
                содержать знак шаблона * для удаления всех узлов.
  -s            Добавляет узел и связывает адрес в Интернете inet_addr
                с физическим адресом eth_addr.  Физический адрес задается
                6 байтами (в шестнадцатеричном виде), разделенных дефисом.
                Эта связь является постоянной
  eth_addr      Определяет физический адрес.
  if_addr       Если параметр задан, он определяет адрес интерфейса в
                Интернете, чья таблица преобразования адресов должна
                измениться. Если параметр не задан, будет использован
                первый доступный интерфейс.
```

```
Пример:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09  .. Добавляет статическую запись.
  > arp -a                                    .. Выводит ARP-таблицу.
```




Кестеде сол жақ бағандағы IP мекенжайлары және ортасында MAC мекенжайлары көрсетілген. Егер кестеде бірдей MAC мекен-жайы бар екі түрлі IP болса, онда сіз ARP улану шабуылына ұшырауыңыз мүмкін.

Мысал ретінде сіздің ARP кестеңізде бірнеше түрлі мекен-жайлар бар делік. Сіз оны қараған кезде екі IP мекенжайының бірдей физикалық мекен-жайы бар екенін байқауыңыз мүмкін. Егер сіз осындай шабуылға тап болсаңыз, ARP кестесінде осындай нәрсені көре аласыз:

```
Интернет адрес Физикалық адрес

Код:

192.168.0.1 00-17-31-dc-39-ab
192.168.0.105 40-d4-48-cr-29-b2
192.168.0.106 00-17-31-dc-39-ab
```

Көріп отырғаныңыздай, бірінші және үшінші MAC мекенжайлары бірдей. Бұл 192.168.0.106 IP мекен-жайының иесі шабуылдаушы болуы мүмкін екенін көрсетеді.

## Басқа нұсқалар

Wireshark-ті ARP улануын пакеттерді талдау арқылы анықтау үшін қолдануға болады, дегенмен бұл қадамдар осы нұсқаулықтан асып түседі және оларды бағдарламамен тәжірибесі бар адамдарға қалдырған дұрыс.

XARP сияқты коммерциялық ARP улану детекторлары процесті жеңілдетеді. Олар ARP инфекциясы басталған кезде сізге ескерту жасай алады, яғни шабуылдар ертерек анықталады және зақым азайтылуы мүмкін.

## ARP улану / залалданудың қалай алдын алуға болады

Сіз ARP улануының алдын алу үшін бірнеше әдісті қолдана аласыз, олардың әрқайсысының оң және теріс жақтары бар. Оларға статикалық ARP жазбалары, шифрлау, VPN және пакеттік талдау кіреді.

### Статикалық ARP жазбалары

Бұл шешім Үлкен әкімшілік шығындарға байланысты және тек шағын желілер үшін ұсынылады. Ол желідегі әр компьютерге әр жеке компьютерге ARP жазбасын қосуды қамтиды.

Компьютерлерді статикалық IP және MAC мекенжайларының жиынтығымен сәйкестендіру спуфингтік шабуылдардың (spoofing attacks) алдын алуға көмектеседі, өйткені компьютерлер ARP жауаптарын елемеуі мүмкін. Өкінішке орай, бұл шешім сізді қарапайым шабуылдардан ғана қорғайды.

### Шифрлау

HTTPS және SSH сияқты протоколдар ARP улану шабуылының сәтті болу мүмкіндігін азайтуға ткөмектеседі. Трафик шифрланған кезде, шабуылдаушы мақсатты шолғышты алдау және оны заңсыз сертификатты қабылдауға мәжбүрлеу үшін қосымша қадам жасауы керек. Алайда, осы хаттамалардан тыс кез-келген деректер әлі де осал болады.

### ВИРТУАЛДЫ ЖЕКЕ ЖЕЛІ (VPN)

Бұл жеке тұлғалар үшін ақылға қонымды қорғаныс болуы мүмкін, бірақ бұл опция әдетте ірі ұйымдар үшін жарамайды. Егер тек бір адам ықтимал қауіпті қосылымды орнатса, мысалы, әуежайда Интернетке қоғамдық сымсыз қосылуды пайдаланса, онда VPN арқылы клиент пен шығу сервері арасында берілетін барлық деректерді шифрлайды. Бұл олардың қауіпсіздігін қамтамасыз етуге көмектеседі, өйткені шабуылдаушы тек шифрланған мәтінді көре алады.

Алайда, бұл ұйымдастырушылық деңгейде мүмкін емес шешім, өйткені әр компьютер мен әр сервер арасында VPN қосылымдары орнатылуы керек. Орнату және сақтау қиындығы ғана емес, сонымен қатар осындай масштабта шифрлау және дешифрлау желінің жұмысына әсер етеді.

## Пакет сүзгілері

Бұл сүзгілер желі арқылы жіберілген әрбір пакетті талдайды. Олар зиянды пакеттерді, сондай-ақ IP мекенжайлары күдікті пакеттерді сүзіп, бұғаттай алады. Пакет сүзгілері сонымен қатар пакеттің сырттан келген кезде ішкі желіден шығатындығы туралы есеп бере алады, бұл өз кезегінде шабуылдың сәтті болу мүмкіндігін азайтуға көмектеседі.

## Желіні улану / ARP залалдануынан қорғаңыз

Егер сіз өзіңіздің желіңізді ARP улану қаупінен қорғағыңыз келсе, сіз үшін ең жақсы нұсқа - жоғарыда аталған алдын-алу және анықтау құралдарының жиынтығы. *Алдын алу әдістері белгілі бір жағдайларда кемшіліктерге ие болады*, сондықтан тіпті ең қауіпсіз ортаға қауіп төнуі мүмкін.

Егер сізде белсенді анықтау құралдары болса, сіз ARP улану туралы ол басталғаннан кейін бірден білесіз. Егер сіздің желілік әкімшіңіз ескерту алғаннан кейін тез әрекет етсе, *сіз үлкен зиян келтірмес бұрын осы шабуылдарды батыл түрде тоқтата аласыз*.