?????????? Windows ?????

Поиск по сервисам

Распространенные сервисы Windows:

- 88 - kerberos (Kerberos Key Distribution Center) — наличие этого порта помогает определить контроллер домена в сети.
- 135 - MSRPC (Microsoft RPC[6]) — используется в приложениях «клиент-сервер» Microsoft (например, Exchange), позволяет выполнять различные операции в OS при наличии учетных данных.
- 137 - NETBIOS-NS (NetBIOS Name Service) — позволяет узнать доменное имя машины и ее MAC адрес.
- 389 - LDAP (Lightweight Directory Access Protocol) — этот порт может дать различные возможности, как по подбору учетных данных, так и по получению доступа к LDAP через эксплуатацию уязвимостей (пример тут).
- 445 - SMB (Server Message Blocks over IP) — протокол SMB имеет ряд уязвимостей и недостатков в различных версиях, которые могут приводить к выполнению кода, захвату пользовательской сессии, получению доступа к данным на файловых серверах.
- 1433 - MSSQL (Microsoft SQL Server) — сервис MSSQL позволяет получить доступ к управлению БД и, что более важно, выполнить произвольный код на машине Windows, если у нас есть аккаунт для доступа к БД.
- 3389 - RDP (Remote Desktop Protocol) — служба удаленных рабочих столов также имеет в истории различные уязвимости, приводящие к выполнению произвольного кода (BlueKeep), и уязвима по отношению к атакам MitM, позволяющим получить доступ к службе от имени жертвы.

Список публичных сервисов.

Пример команды для обнаружения узлов с ОС Windows:

```
nmap -Pn -n -sT -p 88,135,137,389,445,1433,3389 -sV -sC --open -iL list-of-machines.txt
```

Анализ трафика широковещательных запросов

Машины Windows активно используют протоколы WPAD, LLMNR, NBT-NS, позволяющие определить, что с высокой долей
вероятности именно машины Windows воспользовались данным протоколом.

Web Proxy Auto-Discovery Protocol (WPAD) (протокол автоматической настройки прокси) — метод, используемый клиентами

для определения места (URL) расположения конфигурационного файла с использованием технологий DHCP и/или DNS.

Служба имен NetBIOS (NBT-NS) — это протокол Windows, который используется для преобразования имен NetBIOS в IP-адреса
в локальной сети.

Link-Local Multicast Name Resolution (LLMNR) — протокол стека TCP/IP, основанный на формате пакета данных DNS, который
позволяет компьютерам выполнять разрешение имен хостов в локальной сети.

Широковещательные запросы NBNS, LLMNR:

Протокол WPAD нужен для того, чтобы автоматически настроить все браузеры в организации без ручного конфигурирования
каждого. WPAD-стандарт описывает 2 альтернативных метода распространения информации о расположении файла конфигурации для системных администраторов: с использованием Dynamic Host Configuration Protocol (DHCP) или Domain Name System (DNS).

Для поиска Windows машин мы можем исследовать трафик с использованием Wireshark и фильтром: nbns || llmnr || mdns

Для автоконфигурации клиент пытается обнаружить URL-адрес с расположением файла конфигурации, указывающим на Proxy-сервер.

До того, как будет загружена первая страница, браузер в машине Windows использует эту технологию для отправки локальному DHCP-серверу DHCPINFORM-запроса и использует полученный URL из WPAD-опции ответа сервера. Если DHCP-сервер не может предоставить требуемую информацию, то используется DNS.

Если, DNS-имя компьютера pc-hostname.subname.local-domain-name.ru, браузер попытается обратиться к следующим URL для поиска конфигурационного файла:

- http://wpad.subname.local-domain-name.ru/wpad.dat
- http://wpad.local-domain-name.ru/wpad.dat
- http://wpad.com/wpad.dat

Проблемы:

Так как какого-то имени в сети действительно нет, клиент выполняет поиск DNS имен через следующие этапы:

- Проверяет файл hosts для получения информации о системе и ее конфигурации
- Проверяет локальный кэш DNS
- Отправляет запрос к DNS
- Отправляет запрос LLMNR

- Отправляет запрос NBT-NS
- Отправляет запрос MDNS

Если мы сможем сообщить клиенту о том, что файл wpad.dat находится у нас, мы можем попытаться запросить у клиента учетные данные для аутентификации или дать клиенту настройки прокси с адресом своего узла и прослушивать весь
трафик, который будет идти через наш прокси сервер.

Revision #1
Created 9 October 2025 17:56:37 by Admin
Updated 9 October 2025 18:06:23 by Admin