АТАКА ОТРАВЛЕНИЯ ПРОТОКОЛОВ LLMNR/NBT-NS И ПРОТИВОДЕЙСТВИЕ ЕЙ

Е.А. Шитик

Учреждение образования «Гродненский государственный университет имени Янки Купалы, Гродно, Беларусь

LLMNR и NTB-NS – это протоколы, которые используются Windows, чтобы искать хосты по DNS-имени при сбое DNS-запросов в сети. Например, при необходимости идентификации определенного хоста, компьютер обращается к другим устройствам в сети с запросом, знают ли они этот хост, используя протокол LLMNR. Этот протокол по умолчанию активирован в Active Directory, хоть это и небезопасно, так как на запрос может ответить устройство, скомпрометированное злоумышленником. Приоритет способов разрешения имен в Windows: localhosts, Hosts, DNS, LLMNR, MDNS, NBT-NS. Протоколы LLMNR и NBT-NS предназначены для определения адресов хостов путем отправки мультикастных или широковещательных запросов по сети. Во время такой активности и возможна атака. С помощью таких инструментов, как Responder, злоумышленники могут наблюдать за сетевым трафиком, выявляя запросы LLMNR и NBT-NS, и отвечать на них, маскируясь под требуемый хост. В результате устройство, отправившее запрос, будет полагать, что нашло нужный хост, и попытается установить с ним соединение через SMB, при этом отправив хеш-пароля пользователя.

В докладе проводится анализа возможностей злоумышленника по организации атака отравления протоколов LLMNR и NBT-NS. Представлены методы, позволяющие детектировать проявления атаки на элементы сетевой инфраструктуры. Также представлены рекомендации по созданию базовых конфигураций для противодействия атакам отравления протоколов LLMNR и NBT-NS. Атаки с отравлением LLMNR и NBT-NS представляют значительные угрозы для сетевой безопасности. Внедряя рекомендации, изложенные в этой статье, вы можете защитить свою сеть от этих типов атак. Для защиты от отравления LLMNR, вы можете отключить LLMNR для всех компьютеров в домене, используя групповые политики. Для защиты от отравления NBT-NS, вы можете вручную отключить NBT-NS для каждого сетевого адаптера.

Список литературы

1. PoisonedCredentials – разбор задания с платформы CyberDefenders [Электронный ресурс]. – Режим доступа: https://habr.com/ru/articles/775414/. – Дата доступа: 04.05.2024.

2. How To Protect Against LLMNR And NBT-NS Poisoning / informer.io [Электронный ресурс]. – Режим доступа: https://informer.io/resources/llmnr-and-nbt-ns-poisoning. – Дата доступа: 04.05.2024.