УДК 004.056.53

ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ АТАК ТИПА «ЧЕЛОВЕК ПОСЕРЕДИНЕ»

А.В. Денисов, студент факультета компьютерных наук и электроники специальности «Компьютерная физика»,
П.Н. Солдатенко, ст. преподаватель кафедры физики,
Полоцкий государственный университет имени Евфросинии Полоцкой, Новополоцк, Беларусь

Проанализирован тип атаки Man in the middle, способы проведения атаки, возможности мониторинга параметров сети с целью обнаружения угроз и их предотвращения.

Ключевые слова: *информационная безопасность, человек посередине, перехват сигнала, спуфинг.*

Повсеместное проникновение интернета в жизнедеятельность современного общества несет несомненные преимущества в повышение качества жизни каждого его члена. Информационно-коммуникационные технологии охватывают практически каждую область жизни человека. Однако подобные процессы приводят к появлению существенных угроз внедрения в сферу личных критически важных данных сведений о пользователе информационных сетевых систем [1–4]. Большинство людей во время использования мессенджеров, информационных ресурсов и социальных сетей даже не задумываются о том, что они могут быть не единственными, кто видит их транзакции либо активности в интернете.

Одной из опасных и часто используемых атак, направленной на перехват связи между двумя системами, является атака типа Man in the middle (MITM) [1–3]. Наличие подобных угроз требует нового подхода к обеспечению личной информационной безопасности. В настоящей работе проанализирован методы обнаружения и предотвращения атак типа MITM.

Целью MITM атаки зачастую является получения конфиденциальных данных пользователя, примером таких данных является: учётные данные пользователя, данные банковского счёта, номер банковской карты и т.д.

Злоумышленник имеет в арсенале несколько способов проведения MITM атаки.

Типы проведения атаки:

– Подмена IP-адреса

Каждое устройство, подключенное к интернету, имеет свой интернет-протокол. Злоумышленник, подменив IP-адрес заставляет жертву думать, что она взаимодействует с интернет-ресурсом, но на деле не обменивается никакими данными с сервером, а отправляет данные злоумышленнику.

– Спуфинг DNS

Во время подмены DNS злоумышленник получает полное управление над запросами пользователя и может перенаправлять его на поддельные веб-страницы и сайты.

– Спуфинг ARP

Злоумышленник, отправляет жертве поддельные ARP-ответы с информацией что поддельный MAC-адрес совпадает с настоящим IP-адресом маршрутизатора.

– Фальшивый Wi-Fi

Создаётся фальшивая точка доступа в общедоступных сетях при подключении к который злоумышленник отслеживает все действия пользователя сети.

Пример атаки с использованием APR спуфинга:

1. Атакующий узнаёт IP-адрес сетевого интерфейса.
2. С помощью утилиты netdiscover обнаруживает узлы в сети.
3. Выбирает жертву.
4. Запускает arpspoof.

```
┌──(root㉿LEGION)-[/home/kakto]
└─# arpspoof -i wlan0 -t 192.168.100.4 192.168.100.1
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
f0:a6:54:cf:eb:9b 14:d4:24:90:4a:b 0806 42: arp reply 192.168.100.1 is-at f0:a6:54:cf:eb:9b
```

Рисунок 1. – Переход трафика жертвы через злоумышленника

Жертва всё так же может пользоваться интернетом, но теперь весь трафик идёт через злоумышленника.

Признаки атаки MITM:

1. Частые разрывы и переподключения к сети.
2. Изменение MAC-адреса точки доступа.
3. Несколько точек доступа с одинаковым SSID.
4. Задержки при отправке запроса.
5. Неизвестные устройства в сети.

Обнаружение и предотвращение атаки. Для обнаружения MITM атаки используется Arduino UNO и Wi-Fi модуль ESP32, при помощи модуля можно осуществлять мониторинг различных параметров сети, что приведёт к дальнейшему обнаружение атаки. Преимущества использования микроконтроллера заключается в простоте внедрения этого устройства в интернет вещей.

– Проверка изменений MAC-адреса точки доступа

Обнаружение нескольких точек доступа с одинаковыми SSID, но с другим MAC-адресом. Можно обнаружить атаку если мониторить MAC-адрес точки доступа и реагировать на его изменение.

– Сканирование сети и поиск дублей SSID

Обнаружение нескольких точек доступа с одинаковыми SSID, может свидетельствовать об попытке подмены сети.

– Анализ уровня сигнала

Поддельная точка доступа имеет другой уровень сигнала в отличие от настоящей. Если уровень сигнала резко изменился это может свидетельствовать о атаке.

– Мониторинг переподключения и сбоев соединения

Частые разрывы и переподключения к сети Wi-Fi могут быть признаком атаки. Злоумышленник может пытаться перебросить устройство на поддельную точку доступа путём искусственных сбоев соединения.

Пример обнаружения APR атаки при помощи утилиты Wireshark представлен на рисунке 2.

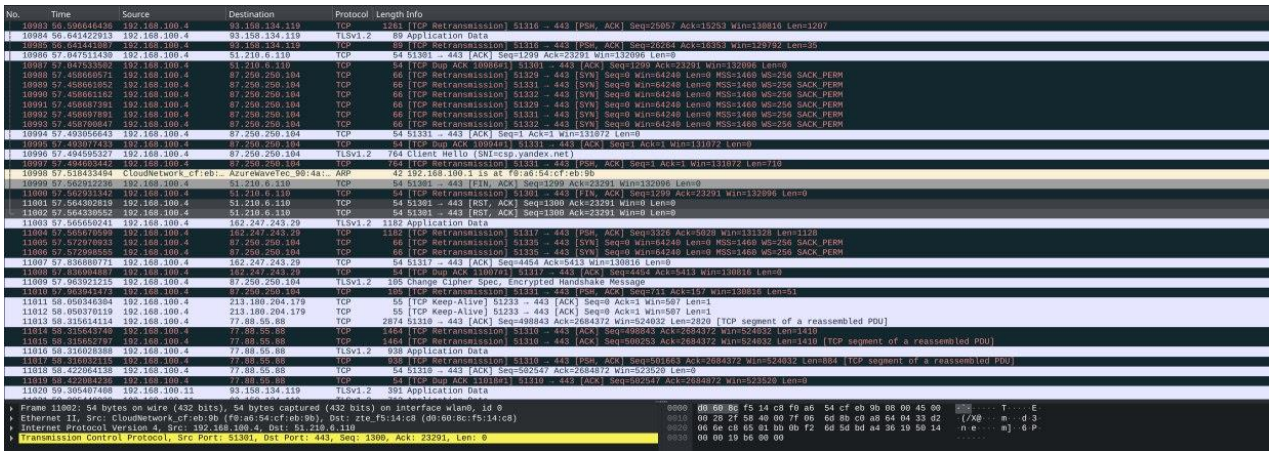

Рисунок 2. Анализ трафика через утилиту Wireshark

Жёлтым цветом помечена аномалия, на которую нужно обратить внимание и предпринять действия по исключению угрозы.

Таким образом, представленный в работе способ обнаружения MITM атаки с использованием Arduino UNO и Wi-Fi модуля ESP32 может быть применен для осуществления эффективного мониторинга различных параметров сети, что, в свою очередь, сократит количество успешных атак.

ЛИТЕРАТУРА

1. Man-in-the-Middle: советы по обнаружению и предотвращению https://www.securitylab.ru/news/553281.php(19.10.2024).
2. Brijith A. (2024) Man-in-the-Middle Attack, Insights2Techinfo, pp.1 https://insights2techinfo.com/man-in-the-middle-attack-2/(20.10.2024)
3. Copyright © 2000-2002 <Alberto Ornaghi, Marco Valleri> (GNU/FDL License) This article is under the GNU Free Documentation License, http://www.gnu.org/copyleft/fdl.html(21.10.2024).
4. Грэм Дэниел Г. Этичный хакинг. Практическое руководство по взлому. – СПб.: Питер, 2022. – 384 с.: ил. – (Серия «Библиотека программиста»). – С. 44–72.