Секция V.
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

УДК 004.056.5

МАКЕТ ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ PNETLAB ДЛЯ ИЗУЧЕНИЯ КИБЕРАТАКИ VLAN HOPPING

А.П. Иванов, А.В. Кисель, студенты гр.161402,
Е.С. Белоусова, канд. техн. наук, доц., доц. кафедры защиты информации
Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь

В материалах доклада представлены результаты реализация кибератаки VLAN Hopping в смоделированной локальной сети в виртуальной лаборатории PnetLAB. Разработанный макет виртуальной лаборатории предлагается использовать для развития знаний и навыков в области информационной безопасности корпоративных сетей у студентов разных специальностей, в том числе 1-98 01 02 «Защита информации в телекоммуникациях».

Ключевые слова: *сетевые кибератаки, VLAN Hopping, PnetLab.*

Введение. VLAN (Virtual Local Area Network) – это технология, которая позволяет логически разделять устройства в одной физической сети на различные виртуальные сегменты, обеспечивая гибкость и безопасность в управлении сетевыми ресурсами. Тем не менее, данная технология имеет уязвимости, которые могут быть эксплуатированы нарушителями посредством реализации кибератаки VLAN hopping. Эта кибератака позволяет нарушителю обойти ограничения сегментации и получить доступ к данным, передаваемым в других VLAN.

Кибератака VLAN hopping стала объектом повышенного внимания в контексте внедрения технологии сегментации в корпоративные сети современных организаций для защиты конфиденциальной информации и управления трафиком. В условиях постоянного увеличения масштабов использования VLAN в корпоративных и государственных сетях, угроза VLAN hopping может привести к перехвату данных и несанкционированному доступу.

Цель данной научной работы заключается в изучении техники кибератаки VLAN hopping и реализации методов защиты, которые обеспечат безопасность сетевых сегментов. Результаты исследования будут способствовать повышению защищенности локальных сетей, использующих технологию VLAN, и минимизации риска компрометации информации.

Основная часть. Для изучения кибератаки была создана топология локальной сети в виртуальной лаборатории PnetLab. Лаборатория PnetLab предоставляет возможности

проектирования локальных сетей на базе устройств различных производителей в режиме реального времени.

Построенная топология локальной сети в виртуальной лаборатории PnetLab приведена на рисунке 1. В нее входит следующее оборудование:

- шлюз подключения к внешней сети (Network);
- маршрутизатор Mikrotic (Router);
- коммутатор Cisco IOS L2 (Switch);
- компьютер нарушителя с ОС Linux (Killer);
- компьютер жертвы с ОС Linux (Ubuntu_work);
- компьютер с ограниченной ОС (VPC).

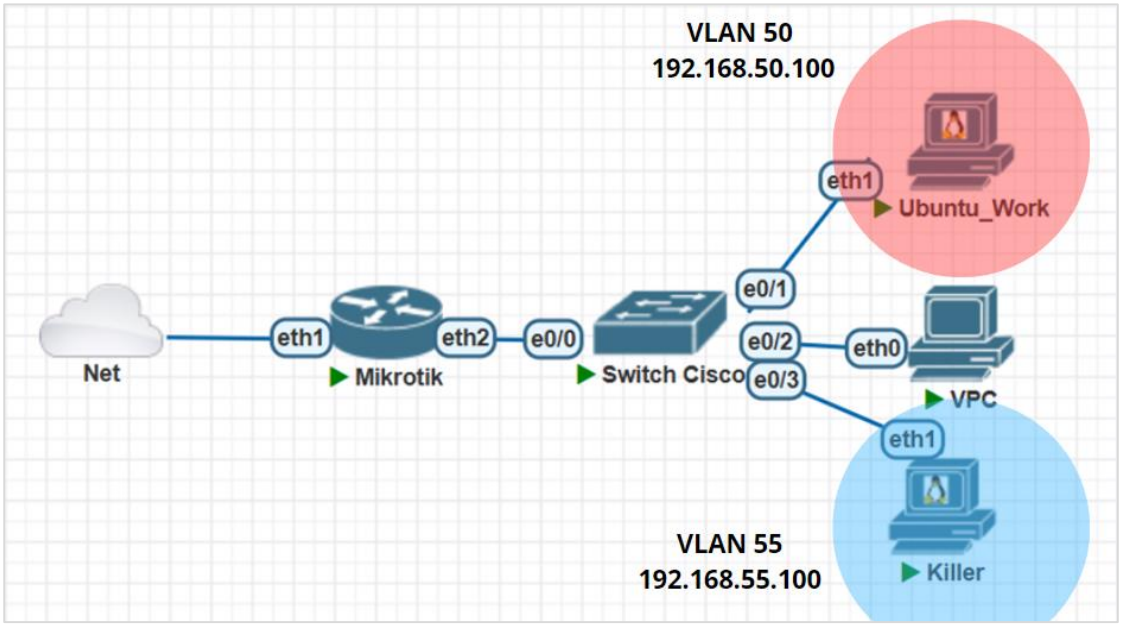


Рисунок 1. – Топология локальной сети в виртуальной лаборатории PnetLab

В данной работе будет реализована кибератака, которая описана в рамках MITRE ATT&CK под идентификатором T1040 Network Sniffing. Этот тип атаки направлен на перехват сетевого трафика между сегментами VLAN, что становится возможным при эксплуатации уязвимостей в технологии VLAN. В частности, будет применена кибератака VLAN hopping с использованием уязвимостей протокола DTP (Dynamic Trunking Protocol), который управляет автоматической конфигурацией транковых портов на коммутаторах.

На рисунке 2 представлен вектор кибератаки, составленный в соответствии с моделью Cyber Kill Chain, который демонстрирует все этапы, начиная с разведки сети и сканирования VLAN, до успешного перехвата трафика между сегментами.

Использование уязвимостей протокола DTP в кибератаке VLAN hopping позволяет нарушителю превратить порт коммутатора, который должен быть в режиме доступа, в транковый порт. Это дает возможность передавать кадры в другие VLAN, устанавливая связь между виртуальными сегментами сети и получая возможность перехвата трафика.

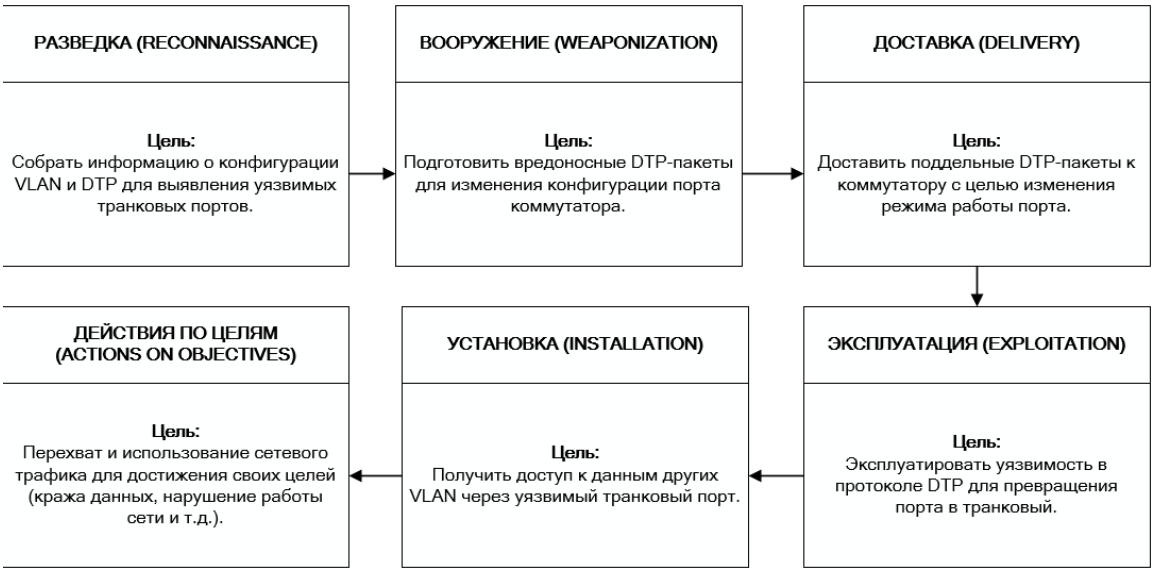


Рисунок 2. – Вектор реализации кибератаки VLAN hopping

В топологии локальной сети в виртуальной лаборатории PnetLab (рисунок 1) устройство Ubuntu_work находится в VLAN 50, а устройство Killer находится в VLAN 55. Кроме этого порт коммутатора, который подключен к устройство Killer изначально имеет статус dynamic desirable, что позволяет автоматически настраивать транковое соединение при взаимодействии с другим устройством, поддерживающим DTP.

Для реализации атаки VLAN hopping с использованием протокола DTP была выбрана утилита Yersinia, которая предоставляет инструменты для проведения атак на сетевые протоколы. В Yersinia был выбран протокол DTP, после чего были сформированы и отправлены поддельные DTP-пакеты на коммутатор, к которому подключено устройство Killer (рисунок 3). В итоге было установлено, что порт коммутатора имеет статус TRUNK/DESIRABLE, который указывает на то, что порт настроен на автоматическое установление транкового соединения и готов к передаче трафика из нескольких VLAN. Таким образом, были реализованы три этапа вектора кибератаки VLAN hopping (рисунок 2).

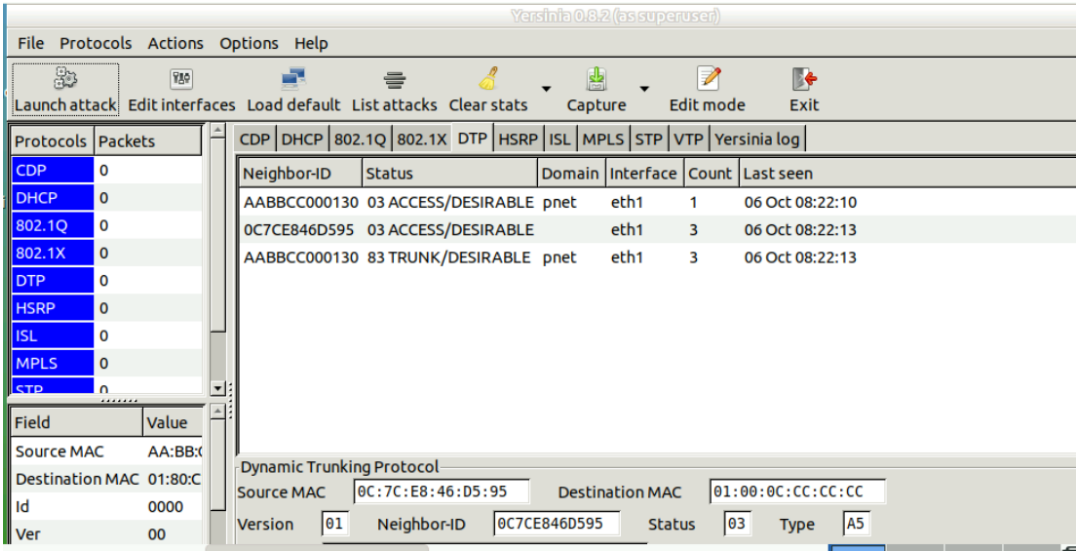
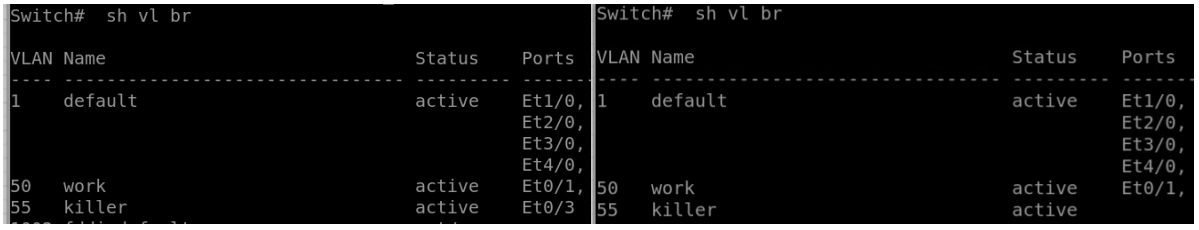


Рисунок 3. – Результат использования утилиты Yersinia

Также, для того чтобы убедиться в успешности реализации первого этапа кибератаки VLAN hopping, произведено сравнение принадлежности к VLAN до и после проведения атаки (рисунок 4).



а *б*

Рисунок 4. – Содержимое таблицы VLAN на коммутаторе до (*а*) и после (*б*) реализации кибератаки VLAN Hopping

Изменение статуса порта коммутатора позволяет нарушителю (Killer) передавать и получать трафик из других VLAN, включая VLAN 50, к которому принадлежит устройство Ubuntu_work. Следовательно, нарушитель может перейти к реализации четвертого этапа вектора кибератаки VLAN hopping (рисунок 2). Таким образом, кибератака нарушила ограничение доступа между сегментами сети.

Кроме этого, на устройстве Killer был создан новый интерфейс VLAN с идентификатором 50, который соответствует VLAN 50, посредством команд:

root@Killer:/home/admin# vconfig add eth1 50

root@Killer:/home/admin# ifconfig eth1.50 up

root@Killer:/home/admin# ifconfig eth1.50 192.168.50.50 up

Таким образом, были реализованы 4–5 этап вектора кибератаки VLAN hopping (рисунок 2), что позволило устройству Killer непосредственно подключиться к VLAN, в которой находится устройство Ubuntu_work (рисунок 5).

Теперь устройство Killer может обмениваться данными с Ubuntu_work и другими устройствами в VLAN 50, а также выполнять атаки типа «человек посередине», модифицируя или подменяя пакеты данных, что позволяет ему вмешиваться в сетевое взаимодействие.

```
admin@Killer:~$ ping 192.168.50.100
PING 192.168.50.100 (192.168.50.100) 56(84) bytes of data.
64 bytes from 192.168.50.100: icmp_seq=1 ttl=64 time=0.822 ms
64 bytes from 192.168.50.100: icmp_seq=2 ttl=64 time=0.562 ms
64 bytes from 192.168.50.100: icmp_seq=3 ttl=64 time=0.641 ms
```

Рисунок 5. – Результат доступности Ubuntu_work для Killer

Рассмотрим последний и ключевой этап вектора кибератаки VLAN hopping (рисунок 2), в котором нарушитель получает возможность к перехвату трафика с устройства Ubuntu_work.

Для проверки использовалась программа Wireshark, установленная на компьютере Killer (рисунок 6). Перехват ICMP-запросов с устройства Ubuntu_work подтверждает успешное выполнение реализации кибератаки и последнего этапа модели Cyber Kill Chain.

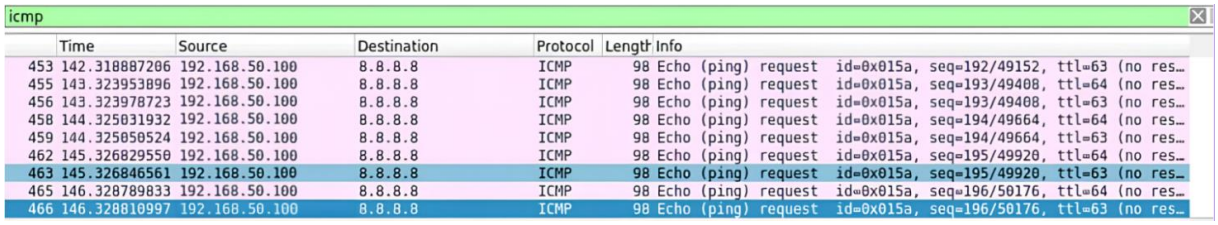


Рисунок 6. – Результат перехват трафика с компьютера Ubuntu_work

На основе полученных результатов можно сделать вывод, что, несмотря на важность сегментации сети с использованием VLAN в современных локальных сетях, протокол DTP может быть использован нарушителями для реализации кибератак VLAN hopping и перенаправления трафика между различными сегментами сети. Это подчеркивает необходимость применения необходимых мер защиты на сетевом оборудовании, для предотвращения несанкционированного доступа и обеспечения безопасность сетевой инфраструктуры.

Возможны несколько вариантов защиты от кибератаки VLAN Hopping:

1. Отключение протокола DTP.
2. Отказ от использования VLAN 1.
3. Перемещение всех неиспользуемых портов в отдельный VLAN и их отключение.

Заключение. На основе проведенных исследований предлагается реализовать макет виртуальной лаборатории на основе платформы PnetLab для изучения и реализации кибератаки VLAN Hopping, конфигурации функций сетевого оборудования для предотвращения подобных кибератак.

Такой макет позволит развивать знания и навыки у студентов разных специальностей, в том числе 1-98 01 02 «Защита информации в телекоммуникациях».

ЛИТЕРАТУРА

1. Переход в соседний VLAN: Атака VLAN Hopping [Электронный ресурс]. – Режим доступа: https://www.securitylab.ru/analytics/495927.php/. – Дата доступа: 12.09.2024.
2. Exploiting VLAN Double Tagging [Электронный ресурс]. – Режим доступа: https://www.claranet.com/us/blog/2020-1030exploiting-vlan-double-tagging/. – Дата доступа: 14.09.2024.
3. Virtual local area network hopping (VLAN hopping) [Электронный ресурс]. – Режим доступа: https://www.claranet.com/us/blog/2020-10-30exploiting-vlan-double-tagging/. – Дата доступа: 14.09.2024.