АНАЛИЗ БЕЗОПАСНОСТИ СЕТЕВЫХ ПРОТОКОЛОВ, ИСПОЛЬЗУЕМЫХ В ОБОРУДОВАНИИ CISCO

Сайжанов Исмаил
студент
Нукусский филиала Ташкентского университета информационных технологий имени Мухаммада аль-Хорезми

Аннотация: *В данной статье проводится анализ безопасности сетевых протоколов Cisco позволяет выявить потенциальные уязвимости, угрозы и риски, с которыми может столкнуться сетевая инфраструктура. Это включает в себя изучение протоколов маршрутизации (например, OSPF, EIGRP), протоколов коммутации (например, VLAN, STP), протоколов безопасности (например, IPsec, SSL/TLS), а также механизмов аутентификации и авторизации (например, TACACS+, RADIUS).*

Ключевые слова: *Сетевые протоколы, Cisco, информационная безопасность, компьютерные сети, топология сети, протоколы TCP/IP, UDP, SNMP и SSH.*

Компьютерная сеть – совокупность оборудования (компьютеры, серверы, средств коммутации и др.), соединенная каналами связи, представляющая единую систему для обмена информацией. Сеть можно представить в виде графа, в котором узлы играют роль сетевого оборудования, а ребра, соединяющие узлы – каналы связи. Узлы могут быть оконечными, промежуточными или смежными. Оборудование может быть соединено друг с другом различными способами.

Анализ безопасности сетевых протоколов Cisco — это процесс исследования и оценки уязвимостей, рисков и возможных угроз, связанных с применением протоколов и технологий Cisco в компьютерных сетях.

Transmission Control Protocol (TCP), в таблице 1 приведен анализ протокола:

- Управление соединением: TCP обеспечивает установку, поддержание и завершение соединений между узлами в сети. Это происходит через процессы "тройного рукопожатия" для установки соединения и последующие сегменты для поддержания связи.
- Контроль потока и надежность: TCP обеспечивает контроль потока данных и обнаружение, и восстановление потерянных или поврежденных сегментов, что делает его надежным протоколом для передачи данных в сети.

Internet Protocol (IP):

- Маршрутизация пакетов: IP отвечает за маршрутизацию пакетов данных в сети, определяя путь и направление передачи данных от отправителя к получателю.
- Адресация и фрагментация: IP использует IP-адреса для идентификации узлов в сети и обеспечивает фрагментацию и сборку пакетов для передачи данных через сети с различными MTU (Maximum Transmission Unit).

Критерий	Оценка	Комментарий
Аутентификация и авторизация	Средняя	Протокол TCP/IP не предоставляет встроенных механизмов аутентификации, но может быть использован совместно с протоколами уровня приложения, такими как TLS/SSL.
Шифрование данных	Средняя	Шифрование на уровне приложения с использованием SSL/TLS возможно, но не всегда реализуется.
Защита от атак	Высокая	Протокол TCP/IP не обеспечивает защиту от атак, но сетевые устройства могут применять механизмы защиты, такие как брандмауэры и IDS/IPS.
Контроль доступа	Средняя	Использование ACL на маршрутизаторах и коммутаторах для ограничения доступа к сетевым ресурсам.
Аудит безопасности	Низкая	Отсутствуют стандартные механизмы аудита безопасности на уровне протокола TCP/IP.
Обновления и уязвимости	Высокая	Постоянные обновления и устранение уязвимостей в реализации протоколов и сетевых устройствах.
Соблюдение стандартов и регулирований	Средняя	Протокол TCP/IP не обеспечивает непосредственно соблюдение стандартов безопасности и регулирований, но может быть настроен в соответствии с ними.
Мониторинг и обнаружение инцидентов	Средняя	Необходимы системы мониторинга сетевого трафика и обнаружения аномального поведения для обеспечения безопасности на уровне TCP/IP.
Управление идентификацией	Низкая	Протокол TCP/IP не предоставляет встроенных средств управления идентификацией.

Таблица 1. Общий анализ критериев протокола TCP/IP

Угрозы и уязвимости:

Атаки DoS/DDoS: TCP уязвим к атакам на основе отказа в обслуживании, таким как атаки на переполнение буфера или избыточные запросы, что может привести к отказу в обслуживании или перегрузке сетевых ресурсов.

Перехват и подмена данных: Незащищенные соединения TCP могут подвергаться риску перехвата и подмены данных, что может привести к утечке конфиденциальной информации или выполнению атак посередине.

Отказ в сегментации пакетов: Атаки на основе перегрузки сегментов могут привести к отказу в обслуживании или снижению производительности сети.

User Datagram Protocol (UDP):

- Отсутствие управления соединением: UDP является протоколом без установления соединения, что означает отсутствие процесса установки и поддержания соединения между отправителем и получателем.
- Отсутствие контроля потока и надежности: UDP не обеспечивает контроля потока данных и не гарантирует доставку данных в правильной последовательности. Также он не обнаруживает и не восстанавливает потерянные или поврежденные пакеты.

Угрозы и уязвимости UDP: Отказ в обслуживании (DoS/DDoS): UDP уязвим к атакам на основе отказа в обслуживании, включая атаки на перегрузку сетевых ресурсов и использование уязвимостей в обработке UDP-пакетов.

Перехват и подмена данных: Из-за отсутствия механизмов аутентификации и проверки целостности данных, UDP-пакеты могут быть подвергнуты риску перехвата, подмены и изменения злоумышленниками.

SNMP (Simple Network Management Protocol) представляет собой стандартный протокол сетевого управления, используемый для мониторинга и управления

сетевыми устройствами, такими как маршрутизаторы, коммутаторы, серверы и другие сетевые устройства. Давайте проведем анализ SNMP:

Основные функции SNMP:

Сбор информации о состоянии сети: SNMP позволяет собирать данные о состоянии и работе сетевых устройств, таких как загрузка ЦП, использование памяти, количество переданных данных и т. д.

Управление сетевыми устройствами: SNMP позволяет управлять сетевыми устройствами, например, изменять конфигурацию устройств, перезапускать их или выполнять другие административные действия.

Компоненты SNMP:

Управляемые устройства (Agents): Управляемые устройства, такие как маршрутизаторы или коммутаторы, имеют программное обеспечение, поддерживающее SNMP и предоставляющее информацию для мониторинга и управления.

Сетевые менеджеры (Managers): Сетевые менеджеры, такие как системы мониторинга сети, используют протокол SNMP для сбора данных о состоянии сети и управления устройствами.

MIB (Management Information Base): MIB представляет собой базу данных, содержащую описания управляемых объектов на устройствах, которые могут быть доступны через SNMP. MIB определяет структуру и синтаксис данных, доступных по протоколу SNMP.

Угрозы и уязвимости SNMP:

Перехват информации: Использование нешифрованного SNMP может привести к перехвату конфиденциальной информации о сети, такой как пароли или данные конфигурации устройств.

Атаки на подмену данных: Злоумышленники могут попытаться подменить данные, передаваемые по SNMP, чтобы изменить конфигурацию устройств или ввести сеть в нежелательное состояние.

Отказ в обслуживании (DoS): Атаки на основе DoS могут быть направлены на SNMP-устройства для перегрузки ресурсов или нарушения их работы.

SSH (Secure Shell) - это криптографический протокол для обеспечения безопасной передачи данных через незащищенную сеть, обеспечивающий безопасное удаленное управление и обмен файлами между компьютерами. Давайте проведем анализ SSH:

Шифрование и аутентификация:

Шифрование данных: SSH шифрует все данные, передаваемые между клиентом и сервером, предотвращая перехват и чтение конфиденциальной информации.

Аутентификация: SSH использует различные методы аутентификации, включая пароль, ключи RSA или ключи PKI (Public Key Infrastructure), для проверки подлинности клиента и сервера.

Безопасность:

Избежание подмены и атак посередине: SSH использует механизмы проверки целостности данных, такие как HMAC (Hash-based Message Authentication Code), чтобы предотвратить подмену данных и атаки посередине.

Защита от атак перебором паролей: SSH предотвращает атаки перебором паролей с помощью функций ограничения попыток входа и блокирования учетных записей после нескольких неудачных попыток.

Портативность и гибкость:

Кросс-платформенность: SSH поддерживается на большинстве операционных систем, включая Unix, Linux, macOS и Windows, что делает его универсальным инструментом для удаленного доступа и управления.

Поддержка различных приложений: SSH может использоваться для различных целей, включая удаленное управление командной строкой, передачу файлов через SCP (Secure Copy) и сетевые туннели для безопасного доступа к удаленным ресурсам.

Управление ключами: Использование ключей SSH: Вместо паролей SSH также позволяет использовать асимметричные ключи для аутентификации, что обеспечивает более высокий уровень безопасности и удобства в использовании.

Меры по обеспечению безопасности SSH:

Обновление и конфигурация: Регулярное обновление SSH-серверов и настройка безопасных параметров аутентификации и шифрования.

Использование ключей: Предпочтительно использовать ключи SSH вместо паролей для аутентификации, так как они обеспечивают более высокий уровень безопасности.

Мониторинг и журналирование: Ведение журналов аутентификационных событий и мониторинг необычной активности для быстрого обнаружения возможных атак.

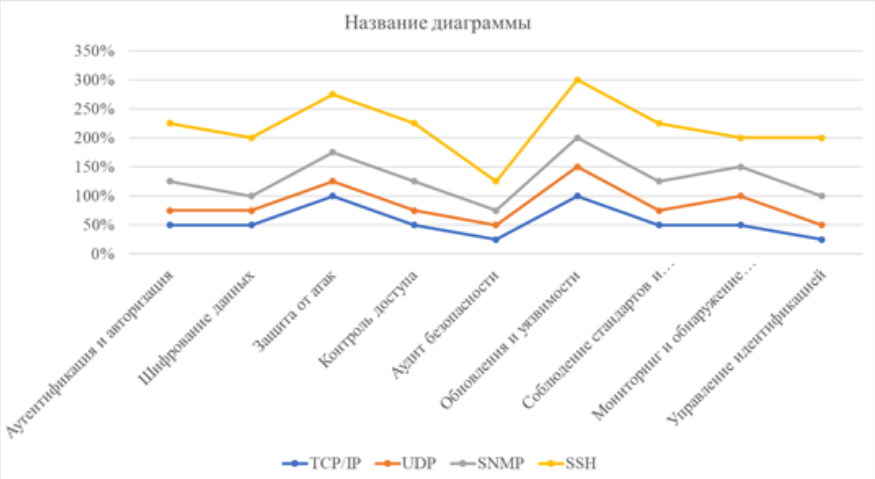

Рис.4. Сравнительный график четырех протоколов TCP/IP, UDP, SNMP и SSH

SH является основным инструментом для безопасного удаленного доступа и управления сетевыми ресурсами. Правильная настройка и использование SSH помогают обеспечить конфиденциальность, целостность и доступность данных и ресурсов в сети.

Общий сравнительный график четырех протоколов показан на рис.4.

В процессе исследования были рассмотрены основные сетевые протоколы, используемые на оборудовании Cisco, включая протоколы маршрутизации, протоколы управления сетью и протоколы безопасности. Были выявлены потенциальные уязвимости и угрозы безопасности, связанные с каждым из этих протоколов, а также проанализированы методы защиты и средства обеспечения безопасности, предоставляемые Cisco.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Seitnazarov K.K. Integration of gis technology for fuzzy deterministic simulation of conditions of operation and maintenance Kegeyli groundwater is abstracted// «IJRET» Volum 4 Issue 2. – Indiya, 2015. – P.727-735. eISSN: 2319-1163/pISSN: 2321-7308.
2. Усманов Р.Н., Сеитназаров К.К. Об организации параллельных вычислений в процессе решения геофильтрационных задач // Вестник ТУИТ. – Ташкент, 2014. - № 1. – С. 101-106. ISSN 2010-9857
3. Usmanov R.N., Seitnazarov K.K. The problem of information model development for the relationship between hydrogeological object and its fuzzy-deterministic model// The Advanced Science Journal. USA, 2014 –№7. – С.67-73. ISSN 2219-746X.
4. Усманов Р.Н., Сеитназаров К.К. Программный комплекс нечетко-детерминированного моделирования гидрогеологических объектов // Автоматика и программная инженерия. – Новосибирск, 2014. – № 1. – С. 29-34. ISSN 2312-4997.
5. Усманов Р.Н., Сеитназаров К.К. Нечетко-детерминированные математические модели процессов восстановления запасов и качества подземных вод // Наука и мир. – Волгоград, №5(21), 2015 – С. 102-104. ISSN 2308-4804.
6. К.К.Сеитназаров, Б.К.Туремуратова. Разница Между Глубоким И Машинным Обучением // Periodica Journal of Modern Philosophy, Social ..., 2022
7. К.К.Сеитназаров, Б.К.Туремуратова. ПРИМЕНЕНИЕ ТЕХНОЛОГИИ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СИСТЕМЕ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ// Новости образования: исследование в XXI веке, 2022.
8. К.К. Сеитназаров, Д.Х. Турдышов, Б.К. Туремуратова. ОБЗОР МЕТОДОВ ПОЛУЧЕНИЯ КОСМИЧЕСКИХ ИЗОБРАЖЕНИЙ С ВЫСОКИМ РАЗРЕШЕНИЕМ// НАУКА и ОБЩЕСТВО
9. K. Seitnazarov, D. Turdishov, A. Dosimbetov. Knowledge base of algorithmic software complex for providing agricultural fields with water resources// AIP Conference Proceedings, 2024.
10. K.K. SEITNAZAROV, B.M. MAMBETKARIMOV. DEVELOPMENT AND APPLICATION OF A DIGITAL EDUCATIONAL RESOURCE FOR TEACHING PROGRAMMING IN HIGHER EDUCATION INSTITUTIONS// Mental Enlightenment Scientific-Methodological ..., 2024.

11. K.K. Seitnazarov, A.K. Bazarbaeva.METHODOLOGY FOR ASSESSING THE ECTS CREDIT SYSTEM IN HIGHER EDUCATIONAL INSTITUTIONS IN WESTERN EUROPE//Modern Science and Research 3 (2), 728-731.

12. К.К. Сеитназаров, Н.С. Мухиятдинов, М.М. Урынбаева. Искусственный интеллект и его применение в принятии решений: методы, алгоритмы и перспективы// Journal of Universal Science Research, 2023.

13. Seitnazarov K.K. Dosımbetov A.M., Aytanov A.K., Omaraov X./ Software Principles for Mapping the Relative State of Groundwater/ European Journal of Molecular & Clinical Medicine ISSN 2515-8260 Volume 7, Issue 11, 2020. – P 319-323.

14. Seitnazarov K.K. Dosımbetov A.M., Aytanov A.K/ Strategy for Organization of Computational Experiments of the Functioning of Underground Water Inlets Using a Fuzzy Multiple Approach/ 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2020, pp. 1-4.

15. Seitnazarov K.K. Aytanov A.K.., Kojametov E., Asenbaev N./ 2021 International Conference on Information Science and Communications Technologies (ICISCT)./ Hydrogeological-Mathematical Model of Formation and Management of Resources and Quality of Fresh Underground Water of the Karakalpak Artesian Basin.