ИССЛЕДОВАНИЕ УЯЗВИМОСТЕЙ СРЕДСТВ IP-ТЕЛЕФОНИИ С ПОМОЩЬЮ ОБЩЕДОСТУПНЫХ ПРОГРАММНЫХ СРЕДСТВ

Макатерчик А.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Маликов В.В. – канд. тех. наук

Аннотация. Актуальным вопросом развития инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь является оценка новых средств связи на предмет наличия уязвимостей информационной безопасности. Знание имеющихся уязвимостей позволит оперативно оценивать состояние системы защиты информации, а также принимать необходимые меры по снижению рисков, связанных с создаваемыми данными уязвимостями угрозами.

Объектом исследования были выбраны стоящие на вооружении и допущенные к использованию в Вооруженных Силах IP-телефоны.

ТА-10 – цифровой телефонный аппарат, предназначенный для обеспечения телефонной связи по IP-сетям и сетям автоматической телефонной связи в стационарных и подвижных пунктах управления Вооруженных Сил.

В качестве инструментов исследования выбраны сканеры уязвимостей: Nmap, XSpider 7.7.

В ходе сканирования были обнаружены открытые порты на устройстве. Открытые порты могут нести опасность, если за ними стоит какая-либо служба, которой может воспользоваться злоумышленник для атаки.

Обе программы показали, что порты 23 и 111 открыты, а расширенное сканирование программы Nmap также показало, что открыты порты 5038 и 5060.

Порт 23 порт используется для службы TELNET. Порт 111 порт используется для службы SUNRPC (Sun Remote Procedure Call). Порты 5038 и 5060 не используются какими-либо распространенными службами, что ставит определенный вопрос к разработчикам о необходимости их использования. Однако, также затрудняют злоумышленнику процесс поиска уязвимостей и их последующей эксплуатации.

Найденные открытые порты можно использовать для несанкционированного доступа к устройству. Например, через порт 23, использующийся для службы TELNET, злоумышленник может подключится к терминалу устройства, зная логин и пароль. Есть несколько способов, которыми может воспользоваться злоумышленник, чтобы узнать пароль: брутфорс, расшифровка хешей, вредоносное ПО.

В рамках исследования оценены возможности реализации брутфорса. Использованы следующие инструменты: операционная система Kali Linux; программное обеспечение Hydra; словари часто используемых логинов и паролей.

Для реализации использована команда из ПО Hydra

hydra -l '/media/root/KALI LIVE/взлом ТА10/logins.txt' -P '/media/root/KALI LIVE/взлом ТА10/passwords.txt' 10.0.0.5 -t 5 telnet -V

После выполнения команды осуществлялся последовательный перебор логинов из файла logins.txt, паролей из файла passwords.txt и попытка входа под полученной парой значений. Ход выполнения программы представлен на рисунках 1 и 2.

По окончанию работы, показан полученный результат: количество целей брутфорса и количество комбинаций логинов и паролей, с которыми получился вход в систему.

Как видно из результатов, защита от брутфорса в данном телефонном аппарате не реализована по умолчанию.

В ходе исследования установлено, что поиск уязвимостей устройств IP-телефонии с помощью общедоступных программных средств для сканирования сетевых уязвимостей таких как Nmap и XSpider 7.7 осуществим и не представляет сложностей ни для специалистов по информационной безопасности, ни для злоумышленников.

С помощью выбранных инструментов было обнаружено, что устройство ТА-10 использует протокол TELNET, к которому может быть осуществлен удаленный доступ. А также проверена возможность реализации атаки подбора данных для входа «брутфорс».

Используемого словаря было недостаточно, доступ к устройству не получен. Что свидетельствует скорее о низком качестве словаря, чем о надежности пароля.

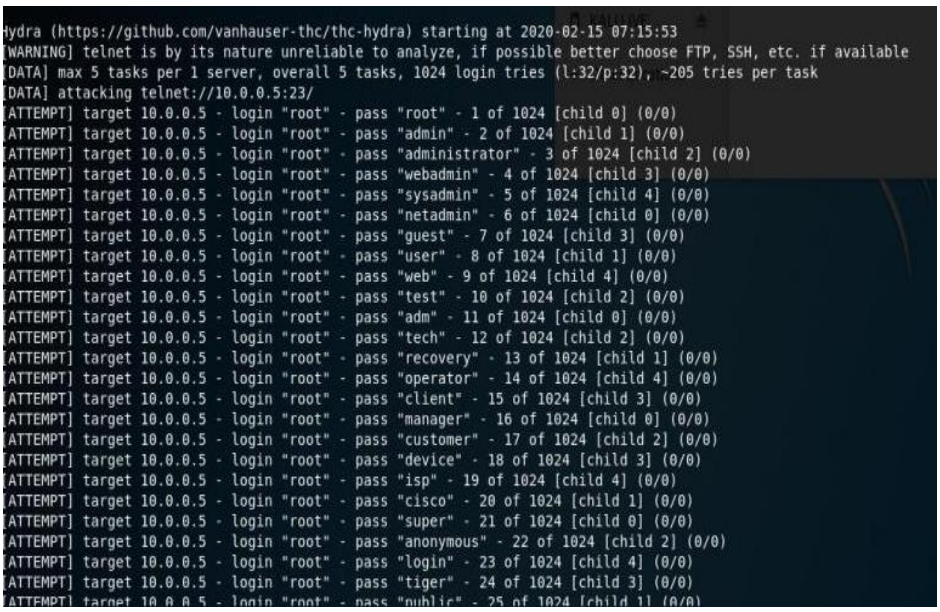

Рисунок 1 – Подбор пароля ТА-10

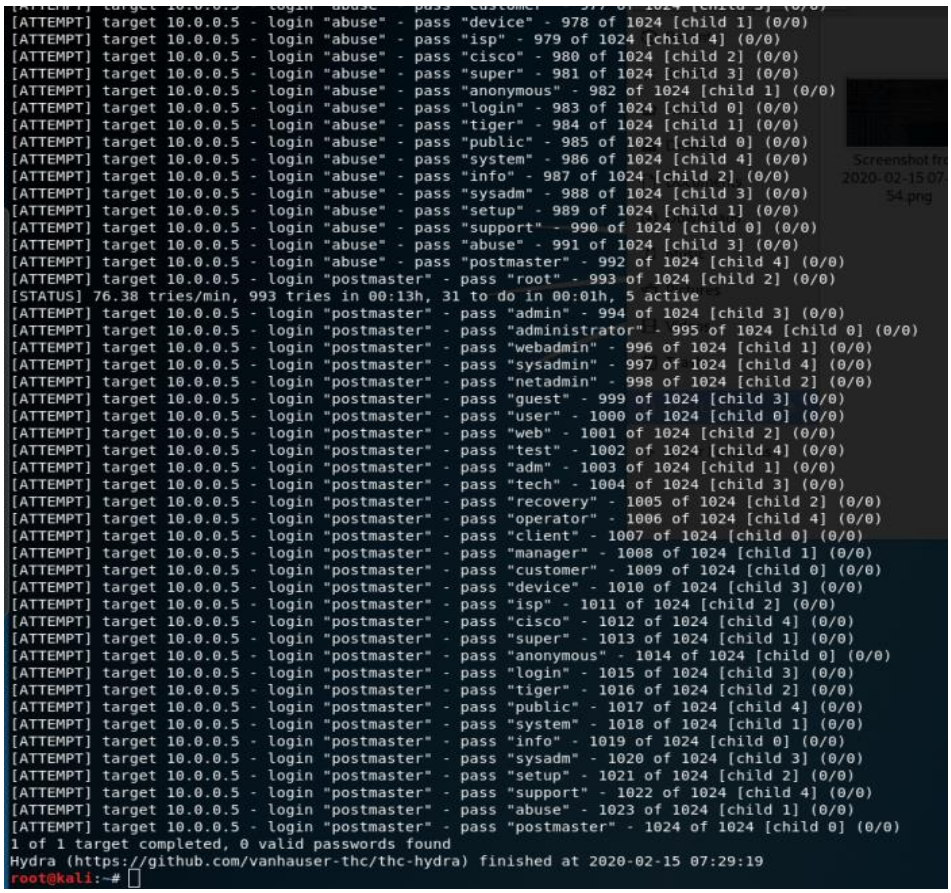

Рисунок 2 – Подбор пароля ТА-10

Брутфорс - один из самых распространенных способов получения несанкционированного доступа к слабо защищенным системам. Следовательно, установка сложных паролей и регулярная их замена является основополагающим способом защиты от взлома.

Использование стандартной конфигурации, может также привести к взлому, так как обычно используются распространенные пары логинов и паролей (admin, root и т.д.), которые в первую очередь злоумышленник проверяет при попытке взлома. А также отсутствие в стандартных установках реализации защиты от атак типа «брутфорс», например, ограничение числа попыток ввода и временная блокировка.