|  |  |
| --- | --- |
| ДИСЦИПЛИНА | Администрирование отечественных операционных систем |
| ИНСТИТУТ | Институт перспективных технологий и индустриального программирования |
| КАФЕДРА | Цифровая кафедра |
| ВИД УЧЕБНОГО МАТЕРИАЛА | Практическая работа |
| ПРЕПОДАВАТЕЛЬ | Макиевский Станислав Евгеньевич |
| СЕМЕСТР | 1 семестр, 2023-2024 |

**Цель работы:** получить навыки работы по следующим направлениям:

- устанавливать сервер и клиент FreeIPA;

- вводить клиента в домен FreeIPA;

- управлять учетными записями пользователей и групп с учетом наличия мандатного доступа;

- настраивать правила на основе узла (хоста);

- настраивать аутентификацию сетевых служб во FreeIPA.

**Задание:**

**0. Подготовка сервера и клиента**

1) Необходимо настроить hostname на сервере и клиента вида:

server1.astra.test

client1.astra.test

2) Убедитесь, что на сервере и клиенте назначены статические IP-адреса.

3) Убедитесь, что разрешаются имена server1 и client1 для команды nslookup.

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

**1. Установка сервера**

1.1. Установите серверное и клиентское программное обеспечение FreeIPA на server1.

sudo apt install fly-admin-freeipa-server

sudo apt install fly-admin-freeipa-client

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

1.2. Запустите сервер FreeIPA (выбрать сетевой интерфейс из внутренней сети и задать пароль для доменной учетной записи admin). Далее перезагрузите ВМ.

sudo fly-admin-freeipa-server -d astra.test -n server1 -o

Примечание: также это можно сделать через графический интерфейс (Панель управления 🡪 Сеть).

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

1.3. Проверьте статус служб FreeIPA командой ipactl.

ipactl status

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

1.4. Проверьте доступность административной веб-консоли FreeIPA через браузер Firefox (пользователь: admin, пароль был введен во время запуска сервера FreeIPA)

https://server1.astra.test

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

1.5. Запустите службу ssh и включите ее в автозагрузку (если не было настроено ранее).

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

**2. Установка клиента и ввод клиента в домен**

2.1. Установите клиентское программное обеспечение FreeIPA на client1.

sudo apt install fly-admin-freeipa-client

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

2.2. Запустите клиент FreeIPA и перезапустите ВМ.

sudo astra-freeipa-client -d astra.test

Примечание: также это можно сделать через графический интерфейс (Панель управления 🡪 Сеть).

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

2.3. На сервере FreeIPA server1.astra.test проверить, что хост client1.astra.test добавлен в домен.

kinit admin

ipa host-show client1.astra.test

или

в веб-консоли https://server1.astra.test Идентификация→Узлы.

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

**3. Управление учетными записями пользователей**

3.1. Создайте учетную запись доменного пользователя ipauser1 из веб-консоли (мин. уровень конфиденциальности – 0, макс. – 1):

Идентификация→Пользователи →+Добавить (заполнить обязательные поля и задать пароль).

Щелкнуть по имени добавленной учетной записи. В Параметрах идентификации задать минимальный (0) и максимальные уровни конфиденциальности (1).

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

3.2. Создайте учетную запись пользователя ipauser2 и задайте пароль из командной строки с помощью утилиты ipa (мин. уровень конфиденциальности – 0, макс. – 2).

kinit admin

ipa user-add --first=IPA --last=User2 ipauser2

ipa user-mod ipauser2 --macmin=0 --macmax=2

ipa passwd ipauser2

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

3.3. На клиенте зайдите под учетными записями ipauser1 и ipauser2 с разными уровнями конфиденциальности.

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

**4. Управление доступом на основе узла**

Выполняется с помощью утилиты ipa в командной строке на сервере FreeIPA (может быть также выполнено в веб-консоли).

4.1. Просмотрите информацию о всех настроенных службах из командной строки и проверьте, есть ли в списке служба fly-dm.

kinit admin

ipa hbacsvc-find --all

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

4.2. Создайте правило, которое разрешает доменному пользователю ipauser2 графический вход в систему на хосте client1.astra.test:

1) На сервере FreeIPA добавьте службу fly-dm.

ipa hbacsvc-add fly-dm --desc="Fly Display Manager"

2) Создайте «пустое» правило с именем flydm.

ipa hbacrule-add flydm

3) Добавьте в правило flydm учетную запись пользователя ipauser2.

ipa hbacrule-add-user flydm --users=ipauser2

4) Добавьте в правило flydm хост client1.astra.test.

ipa hbacrule-add-host flydm --hosts=client1.astra.test

5) Добавьте в правило flydm службу fly-dm.

ipa hbacrule-add-service flydm --hbacsvcs=fly-dm

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

4.3. Просмотрите правило flydm.

ipa hbacrule-show flydm

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

4.4. Протестируйте правило flydm для пользователей ipauser1 и ipauser2 с помощью утилиты ipa hbactest.

ipa hbactest --user=ipauser1 --host=client1.astra.test --service=fly-dm

ipa hbactest --user=ipauser2 --host=client1.astra.test --service=fly-dm

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

4.5. Отключите правило allow\_all и снова протестировать правило flydm.

ipa hbacrule-disable allow\_all

ipa hbactest --user=ipauser2 --host=client1.astra.test --service=fly-dm

ipa hbactest --user=ipauser1 --host=client1.astra.test --service=fly-dm

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

4.6. Зайдите под учетными записями ipauser1 и ipauser2 на хостах client1.astra.test через графический вход.

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

4.7. Попробуйте зайти пользователем ipauser2 в client1.astra.test через виртуальный терминал (вход не должен быть разрешен).

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

4.8. Включите правило allow\_all.

ipa hbacrule-enable allow\_all

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

**5. Настройка аутентификации сетевых служб**

Перед выполнением данного пункта обязательно нужно сделать снепшот ВМ server1. Могут наблюдаться проблемы с дальнейшим входом в графический интерфейс FreeIPA.

В данном пункте будет использоваться сервер server1 в качестве кэширующего DNS-сервера (в реальных ситуациях DNS-сервер будет представлять из себя отдельную машину). Для отдельной машины необходимо проделать те же действия по подготовке, что и для клиента.

5.1. Перейдите в веб-консоль и выберите «Сетевые службы» 🡪 DNS 🡪 Глобальная конфигурация DNS 🡪 Глобальные перенаправители, далее введите 192.168.1.10 🡪 Сохранить.

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.2. Зарегистрируйте службу squid в домене (должна быть зарегистрирована, т.к. SQUID работает на данном сервере).

sudo kinit admin

sudo ipa service-add HTTP/server1.astra.test

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.3. Создайте файл /etc/squid/krb5.keytab с ключом для службы squid.

sudo kinit admin

sudo ipa-getkeytab -s server1.astra.test -p HTTP/server1.astra.test -k /etc/squid/krb5.keytab

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.4. Назначьте на файл /etc/squid/krb5.keytab владельца proxy и группу-владельца proxy, задайте права доступа 640.

sudo chown proxy:proxy /etc/squid/krb5.keytab

sudo chmod 640 /etc/squid/krb5.keytab

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.5. Внести информацию о keytab-файле в сценарий, запускающий службу SQUID. Для этого в файл /etc/init.d/squid добавить строки после DESC="Squid HTTP Proxy":

KRB5\_KTNAME=/etc/squid/krb5.keytab

export KRB5\_KTNAME

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

В файле /etc/squid/squid.conf настройте аутентификацию SQUID через Kerberos:

1) закомментируйте строки, содержащие разрешающие правила для localnet

#http\_access allow localhost

#http\_access allow localnet

2) закомментируйте или удалите строки с настройками других видов аутентификации (например, аутентификации NCSA, которая настраивалась в предыдущей практической работе «Прокси-сервер SQUID»).

3) перед последним правилом http\_access deny all и после всех acl-листов добавите строки, которые разрешают использовать SQUID только доменным пользователям (настроить аутентификацию SQUID через Kerberos).

auth\_param negotiate program \

/usr/lib/squid/negotiate\_kerberos\_auth -d –s \

HTTP/server1.astra.test –k /etc/squid/krb5.keytab

auth\_param negotiate children 10

auth\_param negotiate keep\_alive on

acl auth\_users proxy\_auth REQUIRED

http\_access deny !auth\_users

http\_access allow auth\_users

4) перезапустите systemd и службу squid (может занять продолжительное время) и убедиться, что служба squid была запущена успешно.

sudo systemctl daemon-reload

sudo systemctl restart squid

sudo systemctl status squid

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.6. На хосте client1.astra.test выполнить следующие действия:

1) Зайдите администратором.

2) Проверите, что внешние DNS имена и имена из домена astra.test разрешаются.

nslookup www.astralinux.ru

nslookup server1.astra.test

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.7. В браузере Firefox настройте прокси для доступа в Интернет (ручная настройка прокси): server1.astra.test, порт 3128, установите параметр «Также использовать этот прокси для FTP и HTTPS».

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.8. В адресной строке браузера Firefox введите www.astralinux.ru и зайдите на сайт. Можно одновременно на хосте server1.astra.test ввести команду sudo tail -f /var/log/squid/access.log и отслеживать процесс обращения к Интернет-ресурсам через прокси.

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |

5.9. Зайдите под доменной учетной записью ipauser1 с нулевым уровнем конфиденциальности. Настройте в браузере Firefox прокси и зайдите на сайт www.astralinux.ru. На хосте server1.astra.test проверьте поступающую в файл /var/log/squid/access.log информацию.

Примечание: чтобы починить веб-интерфейс, необходимо прописать команду:

ipa-getkeytab -s server1.astra.test -p HTTP/server1.astra.test -k /var/lib/ipa/gssproxy/http.keytab

|  |  |
| --- | --- |
|  | student@prac-work-question:~#Предоставьте ответ в виде скриншота(-ов), где каждый шаг (действие) сопровождается письменным описанием.  Если необходимо предоставить скрипт, то ответ может содержать ссылку на скрипт решения (только git): |
|  | |
|  | |