Заданиѧ муниципального этапа ВсОШ по информатике
(направление «Информационная безопасность»)
для 11 класса (I вариант)
2025/26 учебный год
Максимальное количество баллов — 34

Задание № 1

Условие:
Выберите два параметра, которые можно настроить через BIOS:

Ответ:
- ○ Загрузчик операционной системы
- ○ Версия ядра операционной системы
- ○ Разрешённые ключи для подписи доверенного платформенного ПО
- ○ Имя узла (host) системы
- ○ Открытые/закрытые порты подключения к узлу
- ○ Перечень установленных на платформе компонентов операционной системы

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 2

Условие:
С помощью какой команды выполняется добавление пользователя с именем «ivan» в группу «wheel»?

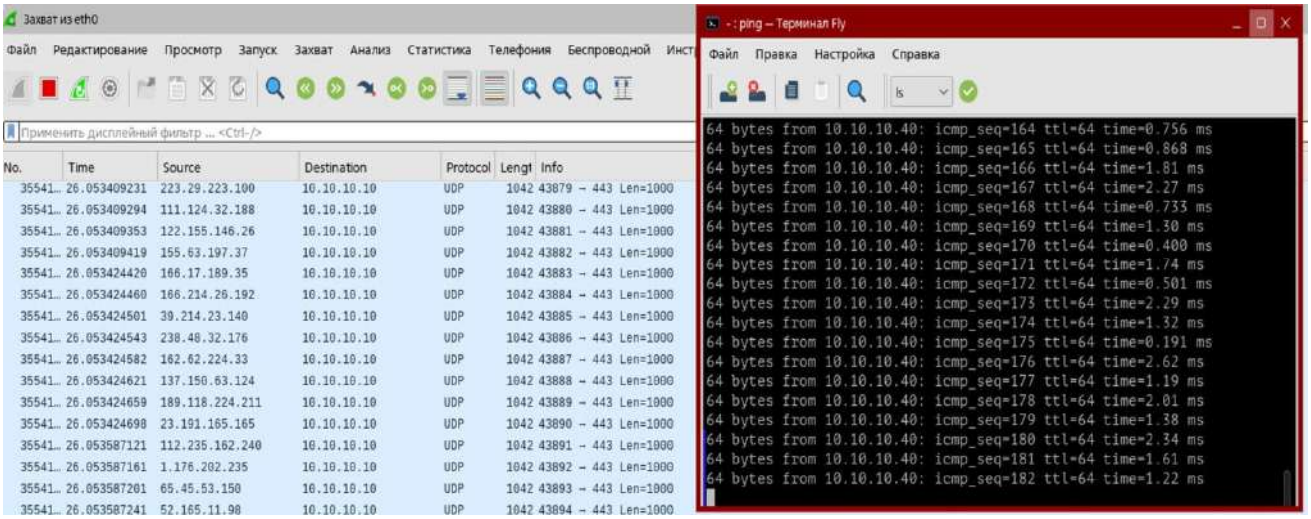
Ответ:
- ○ usermod -aG wheel ivan
- ○ groupadd ivan wheel
- ○ useradd ivan wheel
- ○ passwd -G wheel ivan

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 3

Условие:

Какая атака приведёт к подобному результату?



Ответ:

- UDP Sequence Prediction
- UDP Flood
- TCP Session Hijacking
- Port Scanning UDP

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 4

Условие:

Какой механизм в рамках технологии DHCP-Snooping применяется для усиления защиты от атаки ARP-spoofing?

Ответ:

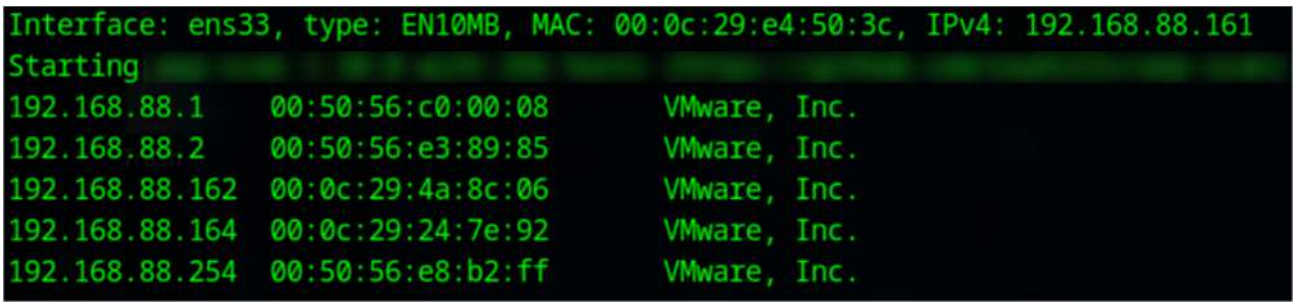
- Настройка автоматического обновления на сетевых устройствах L2
-
-
- Создание базы доверенных сопоставлений IP-адресов и MAC-адресов

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 5

Условие:

Какую команду использовал злоумышленник для получения сведений в изображённой форме?



Ответ:

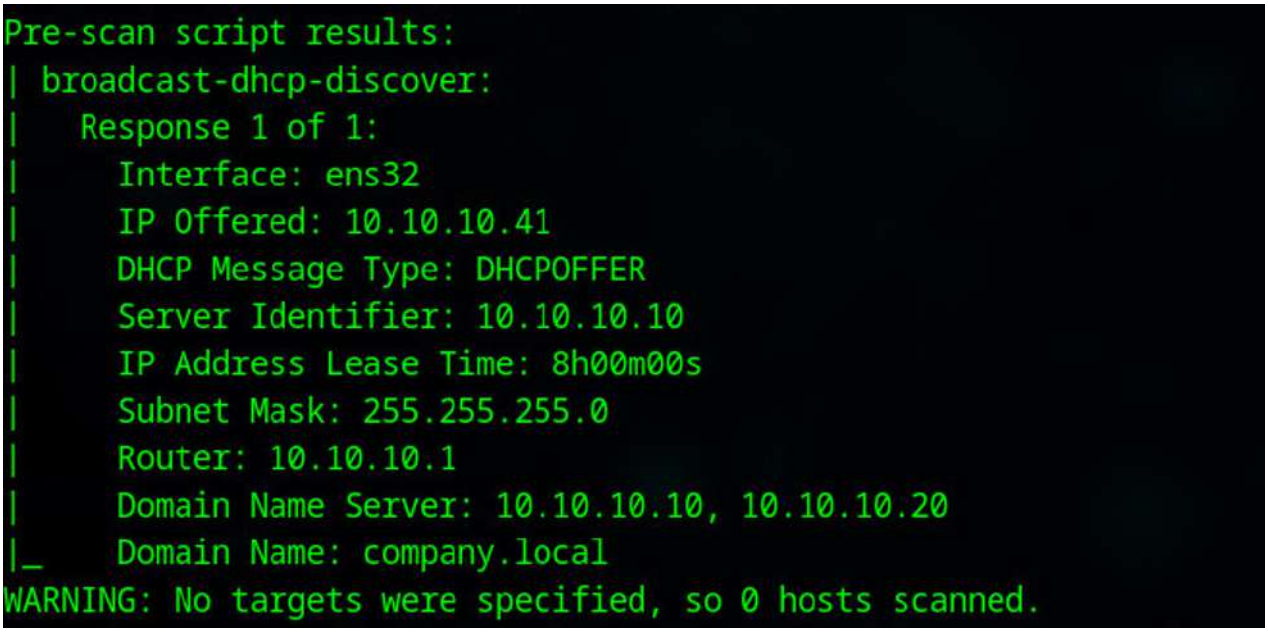
- nmap 192.168.88.0/24
- arp-scan -l
- netdiscover -r 192.168.88.0/24
- arp –a

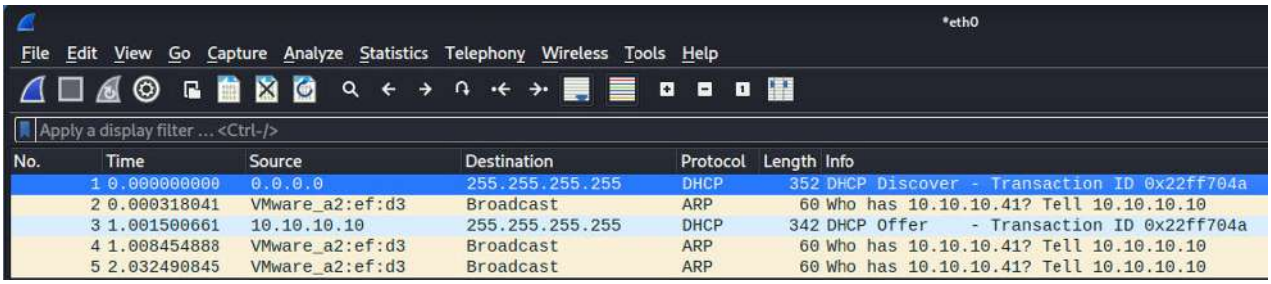
Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 6

Условие:

Какая команда приведёт к изображённому результату?





Ответ:

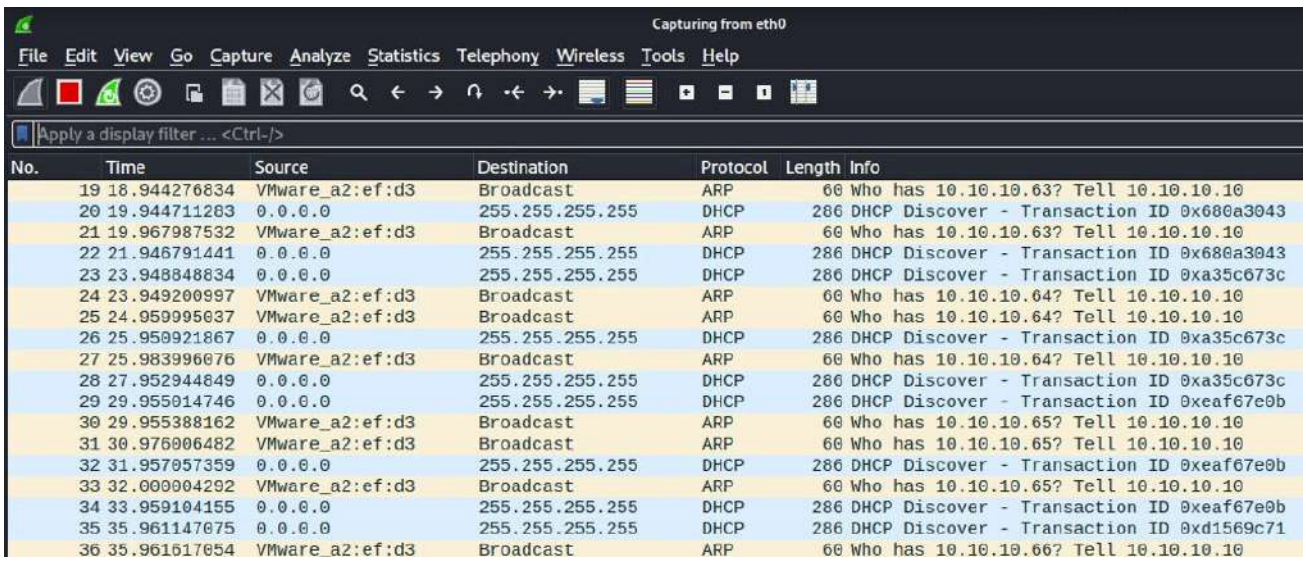
- tcpdump -i ens33 -n port 67 or port 68 -v
- nmap --script broadcast-dhcp-discover
- dhclient -v
- dhcpdump -i eth0

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 7

Условие:
Администратор обнаружил аномальную активность и приступил к анализу лога DHCP-сервера.

```
root@machine:~# tail -f /var/log/syslog | grep -i dhcp
Oct 31 02:03:55 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:7b:c0:d7 via eth0
Oct 31 02:03:56 machine dhcpd[19310]: DHCPOFFER on 10.10.10.42 to 00:16:36:7b:c0:d7 via eth0
Oct 31 02:03:57 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:7b:c0:d7 via eth0
Oct 31 02:03:57 machine dhcpd[19310]: DHCPOFFER on 10.10.10.42 to 00:16:36:7b:c0:d7 via eth0
Oct 31 02:03:59 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:7b:c0:d7 via eth0
Oct 31 02:03:59 machine dhcpd[19310]: DHCPOFFER on 10.10.10.42 to 00:16:36:7b:c0:d7 via eth0
Oct 31 02:04:01 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:ac:00:42 via eth0
Oct 31 02:04:02 machine dhcpd[19310]: DHCPOFFER on 10.10.10.43 to 00:16:36:ac:00:42 via eth0
Oct 31 02:04:03 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:ac:00:42 via eth0
Oct 31 02:04:03 machine dhcpd[19310]: DHCPOFFER on 10.10.10.43 to 00:16:36:ac:00:42 via eth0
Oct 31 02:04:05 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:ac:00:42 via eth0
Oct 31 02:04:05 machine dhcpd[19310]: DHCPOFFER on 10.10.10.43 to 00:16:36:ac:00:42 via eth0
Oct 31 02:04:07 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:2d:26:a9 via eth0
Oct 31 02:04:08 machine dhcpd[19310]: DHCPOFFER on 10.10.10.44 to 00:16:36:2d:26:a9 via eth0
Oct 31 02:04:09 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:2d:26:a9 via eth0
Oct 31 02:04:09 machine dhcpd[19310]: DHCPOFFER on 10.10.10.44 to 00:16:36:2d:26:a9 via eth0
Oct 31 02:04:11 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:2d:26:a9 via eth0
Oct 31 02:04:11 machine dhcpd[19310]: DHCPOFFER on 10.10.10.44 to 00:16:36:2d:26:a9 via eth0
Oct 31 02:04:13 machine dhcpd[19310]: DHCPDISCOVER from 00:16:36:41:c9:20 via eth0
Oct 31 02:04:14 machine dhcpd[19310]: DHCPOFFER on 10.10.10.45 to 00:16:36:41:c9:20 via eth0
```



Используя изображённые результаты анализа, определите тип атаки:

Ответ:

- DHCP Hijacking
-
- DHCP Starvation
- DNS Injection
- ARP Spoofing
- ARP Poisining

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Задание № 8

Условие:

Какие системные файлы подвергаются модификации при выполнении useradd?

Ответ:

- /etc/passwd
- /etc/shadow
- /etc/group
- /home/username/

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Задание № 9

Условие:

Администратору сети необходимо из локальной файловой (/usr/file) системы скопировать файл по защищённому каналу в удаленный хост с IP-адресом 192.168.4.46. При помощи какой команды администратор выполнит данное действие?

Ответ:

- ssh-copy-id user@192.168.4.46
- scp /usr/file user@192.168.4.46:/path/
- sftp get /usr/file.txt
-

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

Задание № 10

Условие:

Небольшой фрагмент исполняемого машинного кода, который используется злоумышленниками как «полезная нагрузка» при эксплуатации уязвимостей, чтобы запустить командную оболочку, называется

Ответ:

- шелл-код
- реверс-шелл
- переполнение стека
- реверс-инжиниринг

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 11

Условие:

Какая команда была использована администратором для получения следующих сведений?

```
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.1  0.2 168636 11340 ?        Ss   06:25   0:02 /sbin/init
root           2  0.0  0.0      0     0 ?        S    06:25   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   06:25   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   06:25   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   06:25   0:00 [kworker/0:0H-events_highpri]
root           9  0.0  0.0      0     0 ?        I<   06:25   0:00 [mm_percpu_wq]
root          10  0.0  0.0      0     0 ?        S    06:25   0:00 [rcu_tasks_rude_]
root          11  0.0  0.0      0     0 ?        S    06:25   0:00 [rcu_tasks_trace]
root          12  0.0  0.0      0     0 ?        S    06:25   0:00 [ksoftirqd/0]
root          13  0.0  0.0      0     0 ?        I    06:25   0:01 [rcu_sched]
root          14  0.0  0.0      0     0 ?        S    06:25   0:00 [migration/0]
```

Ответ:

- ps -ef
- ps aux
- ps lax
- ps –elf

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 12

Условие:
Что делает команда find / -name passwd -perm 4000?

Ответ:

- Ищет файл с именем passwd, у которого установлен SUID
- Ищет файл с именем passwd в домашней директории
- Ищет файл с именем passwd и правами на чтение только для владельца
-

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 13

Условие:
Какой технологии принадлежит данная запись?

```
- name: Сохраняем
  delegate_to: localhost
  copy:
    content: |
      computer_name: "{{ computer_name }}"
      vim_version: "{{ vim_output.stdout | default('Программа не установлена') }}"
      chromium_version: "{{ chromium_output.stdout | default('Программа не установлена') }}"
      ip_address: "{{ ip_address }}"
    dest: "/etc/ansible/PC_INFO/{{ computer_name }}_info.yml"
```

Ответ:

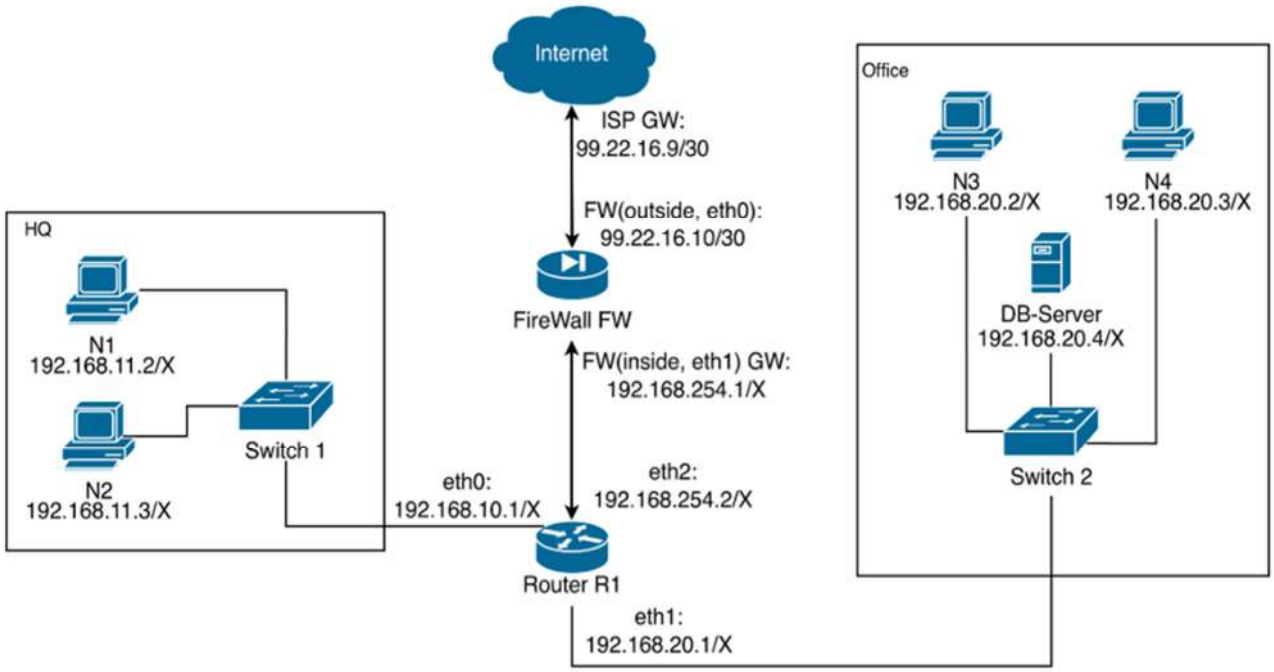
- ansible
-
- dhcp
- terraform
- bash

Точное совпадение ответа — 1 балл
Максимальный балл за задание — 1

Задание № 14

Условие:

Широковещательный (broadcast) адрес сети — это специальный зарезервированный адрес, который используется для одновременной отправки сетевого пакета всем устройствам в пределах одного сегмента локальной сети (подсети).



Определите широковещательный адрес в сети 192.168.254.0/30.

Ответ:

Точное совпадение ответа — 1 балл

Какие адреса **НЕ** могут быть назначены интерфейсам в сети 99.22.16.8/30?

Ответ:

- 99.22.16.8
- 99.22.16.9
- 99.22.16.10
- 99.22.16.11

За каждый верный ответ — 0.5 балла. Количество выбранных ответов, не более 2. Всего 1 балл.

Какую максимальную длину префикса сети можно задать для подсети Office, чтобы все её узлы оставались в одной подсети?

Ответ:
Точное совпадение ответа — 2 балла

Устройство N1 должно иметь доступ к базе данных PostgreSQL на DB-Server. Какое правило iptables в цепи FORWARD нужно добавить на R1?

Ответ:

За каждый верный ответ — 0.5 балла. Всего 2 балла.

Администратор хочет создать одну суммарную сеть вместо отдельных подсетей HQ и Office. Какую минимальную по размеру сеть он может использовать, чтобы обе подсети гарантированно в неё входили?

Ответ:

- 192.168.0.0/16
- 192.168.0.0/18
- 192.168.0.0/19
- 192.168.8.0/21

Точное совпадение ответа — 1 балл

Нужно разрешить пользователям из сети Office (192.168.20.0/29) выход в Интернет по протоколам HTTP и HTTPS через межсетевой экран FW. На FW политика по умолчанию в цепи FORWARD — DROP. Какое правило iptables в цепи FORWARD нужно добавить на FW?

Ответ:

За каждый верный ответ — 0.5 балла. Всего 2 балла.

Максимальный балл за задание — 9

Задание № 15
«Протокол безопасности «Коллектив 2.0»

Условие:
Рекомендуемые утилиты: python
Файл: **reverse_11_1.cpp**
Агент П-3, вам необходимо восстановить пароль доступа к терминалу, проанализировав алгоритм обработки полимерного потока данных.

Ответ:
Точное совпадение ответа — 3 балла

Максимальный балл за задание — 3

Пример решения на Python:

```
target = [35, 70, 60, 69, 65, 48, 13, 110, 18, 62, 45, 62, 59, 85, 72, 33, 77, 28, 70, 49]
res = []
for i in range(9, -1, -1):
    new_beta = target.pop(); new_alpha = target.pop()
    beta = (new_beta + 10) ^ new_alpha
    alpha = (new_alpha - i * 2) ^ 0x55
    res = [alpha, beta] + res
print("".join(chr(x) for x in res))
```

Задание № 16
«Сетевая аномалия»

Условие:
Рекомендуемые утилиты: Wireshark
Файл: **traffic_11_1.pcap**
Товарищ, в наших информационных сетях обнаружена серьёзная аномалия. Злоумышленник провёл сложную многоступенчатую атаку на внутреннюю инфраструктуру. Требуется детальное расследование.

Какой тип атаки был применён?

Ответ:

- SQL injection
- LDAP injection
- Command injection (OS)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- Server-Side Request Forgery (SSRF)
- XML External Entity (XXE)
- Directory Traversal (LFI/RFI)
- Insecure Deserialization
- Broken Access Control (IDOR)
- ARP Spoofing
- No attack (valid creds)

Точное совпадение ответа — 1 балл

Определите IP-адрес атакующего.

Ответ:
Точное совпадение ответа — 1 балл

К какому внутреннему сервису получил доступ злоумышленник? Ответ запишите в формате host:port.

Ответ:
Точное совпадение ответа — 2 балла

Определите переданный флаг.

Ответ:

Точное совпадение ответа — 2 балла

Максимальный балл за задание — 6

Задание № 17
«Полимерный контейнер»

Условие:
Рекомендуемые утилиты: python, CyberChef
Файл: **rdecode_11_1**
В лабораториях комплекса «Завод-3826» найден подозрительный файл с ключом к роботу-кодировщику. Исследователи подозревают, что данные были хитро закодированы необычным способом; возможно, кратность длины кодирования имеет значение. Ваша задача — извлечь секретную информацию.

Ответ:
Точное совпадение ответа — 3 балла

Максимальный балл за задание — 3

Пример решения на Python:

```
import base64, tarfile, io
data = "..."
for _ in range(12):
    data = base64.b85decode(data)
with tarfile.open(fileobj=io.BytesIO(data)) as tar:
    print(tar.extractfile('secret/flag.txt').read())
```