

**Задания 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?

The screenshot shows two windows. The left window is Wireshark, displaying a packet capture on the 'eth0' interface. The filter is 'Применить дисплейный фильтр ... <Ctrl-F>'. The packet list shows a series of UDP packets from various source IP addresses to 10.10.10.10, all with a length of 1000 bytes. The right window is a terminal titled 'ping - Терминал Fly', showing the output of a continuous ping command to 10.10.10.40. The output shows a series of '64 bytes from 10.10.10.40: icmp_seq=...' messages with increasing sequence numbers and response times, indicating a successful ping test despite the flood.

No.	Time	Source	Destination	Protocol	Length	Info
35541	26.053409231	223.29.223.100	10.10.10.10	UDP	1042	43879 → 443 Len=1000
35541	26.053409294	111.124.32.188	10.10.10.10	UDP	1042	43880 → 443 Len=1000
35541	26.053409353	122.155.146.26	10.10.10.10	UDP	1042	43881 → 443 Len=1000
35541	26.053409419	155.63.197.37	10.10.10.10	UDP	1042	43882 → 443 Len=1000
35541	26.053424420	166.17.189.35	10.10.10.10	UDP	1042	43883 → 443 Len=1000
35541	26.053424460	166.214.26.192	10.10.10.10	UDP	1042	43884 → 443 Len=1000
35541	26.053424501	39.214.23.140	10.10.10.10	UDP	1042	43885 → 443 Len=1000
35541	26.053424543	238.48.32.176	10.10.10.10	UDP	1042	43886 → 443 Len=1000
35541	26.053424582	162.62.224.33	10.10.10.10	UDP	1042	43887 → 443 Len=1000
35541	26.053424621	137.150.63.124	10.10.10.10	UDP	1042	43888 → 443 Len=1000
35541	26.053424659	189.118.224.211	10.10.10.10	UDP	1042	43889 → 443 Len=1000
35541	26.053424690	23.191.165.165	10.10.10.10	UDP	1042	43890 → 443 Len=1000
35541	26.053587121	112.235.162.240	10.10.10.10	UDP	1042	43891 → 443 Len=1000
35541	26.053587161	1.176.202.235	10.10.10.10	UDP	1042	43892 → 443 Len=1000
35541	26.053587201	65.45.53.150	10.10.10.10	UDP	1042	43893 → 443 Len=1000
35541	26.053587241	52.165.11.98	10.10.10.10	UDP	1042	43894 → 443 Len=1000

```
64 bytes from 10.10.10.40: icmp_seq=164 ttl=64 time=0.756 ms
64 bytes from 10.10.10.40: icmp_seq=165 ttl=64 time=0.868 ms
64 bytes from 10.10.10.40: icmp_seq=166 ttl=64 time=1.81 ms
64 bytes from 10.10.10.40: icmp_seq=167 ttl=64 time=2.27 ms
64 bytes from 10.10.10.40: icmp_seq=168 ttl=64 time=0.733 ms
64 bytes from 10.10.10.40: icmp_seq=169 ttl=64 time=1.30 ms
64 bytes from 10.10.10.40: icmp_seq=170 ttl=64 time=0.400 ms
64 bytes from 10.10.10.40: icmp_seq=171 ttl=64 time=1.74 ms
64 bytes from 10.10.10.40: icmp_seq=172 ttl=64 time=0.501 ms
64 bytes from 10.10.10.40: icmp_seq=173 ttl=64 time=2.29 ms
64 bytes from 10.10.10.40: icmp_seq=174 ttl=64 time=1.32 ms
64 bytes from 10.10.10.40: icmp_seq=175 ttl=64 time=0.191 ms
64 bytes from 10.10.10.40: icmp_seq=176 ttl=64 time=2.62 ms
64 bytes from 10.10.10.40: icmp_seq=177 ttl=64 time=1.19 ms
64 bytes from 10.10.10.40: icmp_seq=178 ttl=64 time=2.01 ms
64 bytes from 10.10.10.40: icmp_seq=179 ttl=64 time=1.38 ms
64 bytes from 10.10.10.40: icmp_seq=180 ttl=64 time=2.34 ms
64 bytes from 10.10.10.40: icmp_seq=181 ttl=64 time=1.61 ms
64 bytes from 10.10.10.40: icmp_seq=182 ttl=64 time=1.22 ms
```

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?

```
Interface: ens33, type: EN10MB, MAC: 00:0c:29:e4:50:3c, IPv4: 192.168.88.161
Starting
192.168.88.1    00:50:56:c0:00:08    VMware, Inc.
192.168.88.2    00:50:56:e3:89:85    VMware, Inc.
192.168.88.162  00:0c:29:4a:8c:06    VMware, Inc.
192.168.88.164  00:0c:29:24:7e:92    VMware, Inc.
192.168.88.254  00:50:56:e8:b2:ff    VMware, Inc.
```

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 изобраённому результату?

```
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: ens32
|     IP Offered: 10.10.10.41
|     DHCP Message Type: DHCPOFFER
|     Server Identifier: 10.10.10.10
|     IP Address Lease Time: 8h00m00s
|     Subnet Mask: 255.255.255.0
|     Router: 10.10.10.1
|     Domain Name Server: 10.10.10.10, 10.10.10.20
|_    Domain Name: company.local
WARNING: No targets were specified, so 0 hosts scanned.
```

*eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	0.0.0.0	255.255.255.255	DHCP	352	DHCP Discover - Transaction ID 0x22ff704a
2	0.000318041	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.41? Tell 10.10.10.10
3	1.001500661	10.10.10.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x22ff704a
4	1.008454888	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.41? Tell 10.10.10.10
5	2.032490845	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.41? Tell 10.10.10.10

Ответ:

- tcpdump -i ens33 -n port 67 or port 68 -v
- nmap --script broadcast-dhcp-discover
- dhclient -v
- dhcpcdump -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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER 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]: DHCPDISCOVER on 10.10.10.45 to 00:16:36:41:c9:20 via eth0
```

Capturing from eth0						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
19	18.944276834	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.63? Tell 10.10.10.10
20	19.944711283	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xa680a3043
21	19.967987532	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.63? Tell 10.10.10.10
22	21.946791441	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xa680a3043
23	23.948848834	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xa35c673c
24	23.949200997	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.64? Tell 10.10.10.10
25	24.959995637	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.64? Tell 10.10.10.10
26	25.950921867	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xa35c673c
27	25.983996076	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.64? Tell 10.10.10.10
28	27.952944849	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xa35c673c
29	29.955014746	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xeaf67e9b
30	29.955388162	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.65? Tell 10.10.10.10
31	30.976906482	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.65? Tell 10.10.10.10
32	31.957957359	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xeaf67e9b
33	32.000004292	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.65? Tell 10.10.10.10
34	33.959104155	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xeaf67e9b
35	35.961147675	0.0.0.0	255.255.255.255	DHCP	286	DHCP Discover - Transaction ID 0xd1569c71
36	35.961617654	VMware_a2:ef:d3	Broadcast	ARP	60	Who has 10.10.10.66? Tell 10.10.10.10

Используя изображённые результаты анализа, определите тип атаки:

Ответ:

- ☐ DHCP Hijacking
- ☐
- ☐ DHCP Starvation
- ☐ DNS Injection
- ☐ ARP Spoofing
- ☐ ARP Poisoning

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	11348	?	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

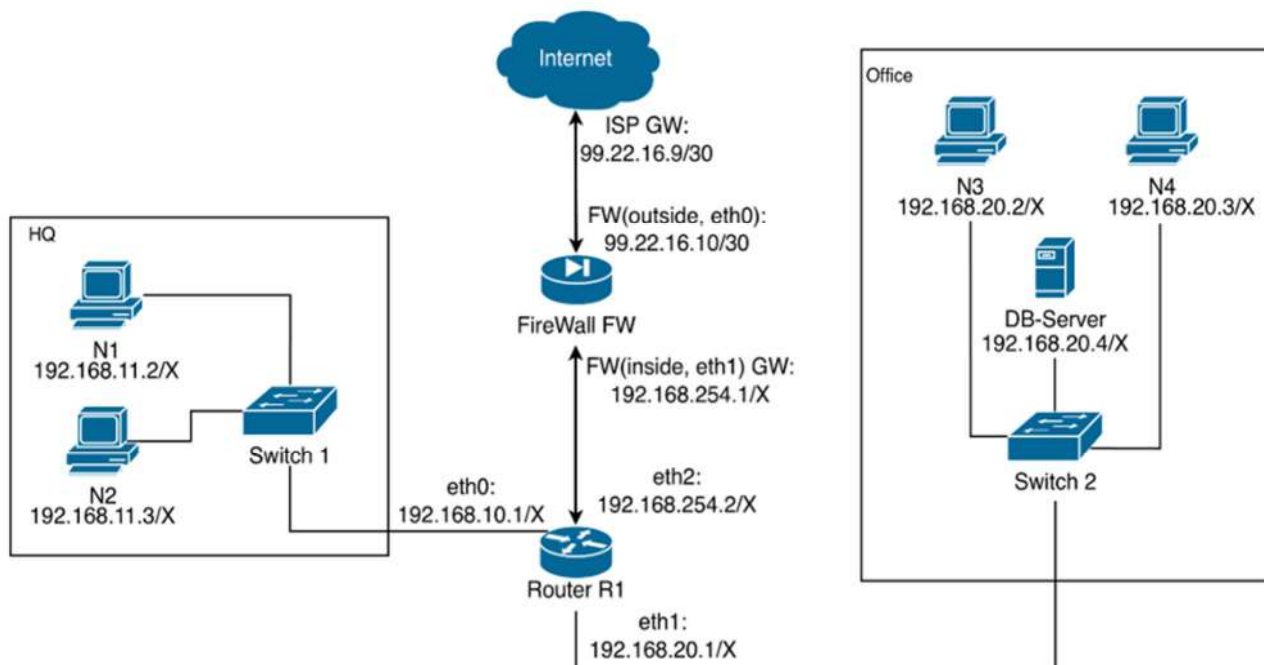
Точное совпадение ответа — 1 балл

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())
```