

**Разбор заданий 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**

**Решение:**

Через современный BIOS/UEFI можно управлять загрузкой (выбор/приоритет загрузочных записей/загрузчика) и хранить/настраивать ключи, используемые для проверки доверенного ПО (Secure Boot).

**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**

**Решение:**

Команда `usermod -aG wheel ivan` добавляет пользователя `ivan` в дополнительную группу `wheel` (через `-a`), не убирая его из уже существующих групп (опция `-G`). Особенностью команды `usermod` является то, что параметр `a` используется обычно только с `G`.

### Задание № 3

#### Условие:

Какая атака приведёт к подобному результату?

The screenshot shows two windows. The left window is Wireshark, titled 'Захват из eth0'. It displays a list of captured packets, all of which are UDP packets from various source IP addresses to the destination 10.10.10.10. The right window is a terminal titled 'ping - Терминал Fly', showing the output of a continuous ping command to 10.10.10.40. The ping results show a consistent response time of approximately 0.756 ms, indicating that the target is reachable despite the flood of UDP packets.

| 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

#### Решение:

На скриншоте виден перечень UDP-портов и их состояние для множества узлов, что характерно для UDP-сканирования, а не для захвата сессии или DDoS-флуда.

## 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
- Полное шифрование ARP-трафика
- Блокировка всех ARP-Reply сообщений
- ✓ Создание базы доверенных сопоставлений IP-адресов и MAC-адресов

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

### Решение:

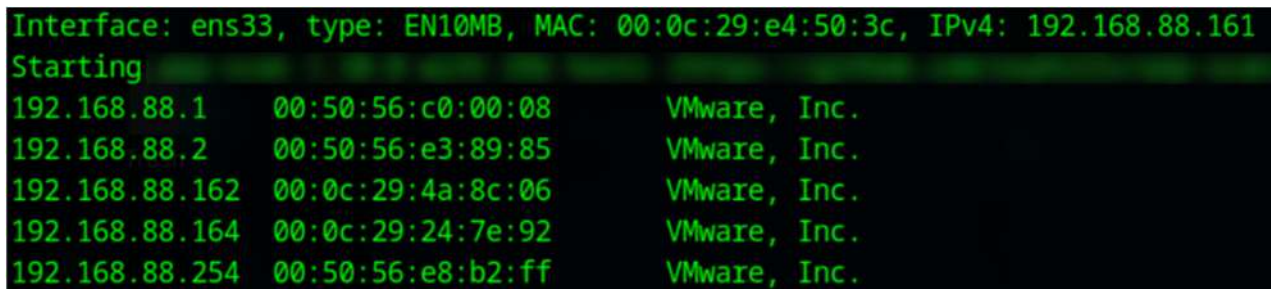
DHCP Snooping ведёт базу «доверенных» соответствий IP-адресов и MAC-адресов, что позволяет фильтровать ARP-ответы, которые не совпадают с этими связками, тем самым уменьшая риск ARP-подмены.

## 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

### Решение:

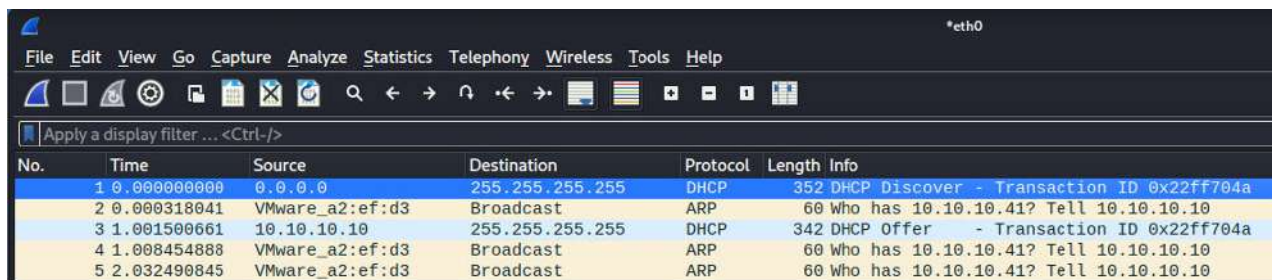
Используется команда arp-scan -l специально для сканирования локальной сети.

## Задание № 6

### Условие:

Какая команда приведёт к изображённому результату?

```
Pre-scan script results:
| broadcast-dhcp-discover:
|   Response 1 of 1:
|     Interface: ens32
|     IP Offered: 10.10.10.41
|     DHCP Message Type: DHCP OFFER
|     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.
```



The image shows a Wireshark packet capture on the eth0 interface. The packet list table contains the following data:

| 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
- ☐ dhcpdump -i eth0

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

### Решение:

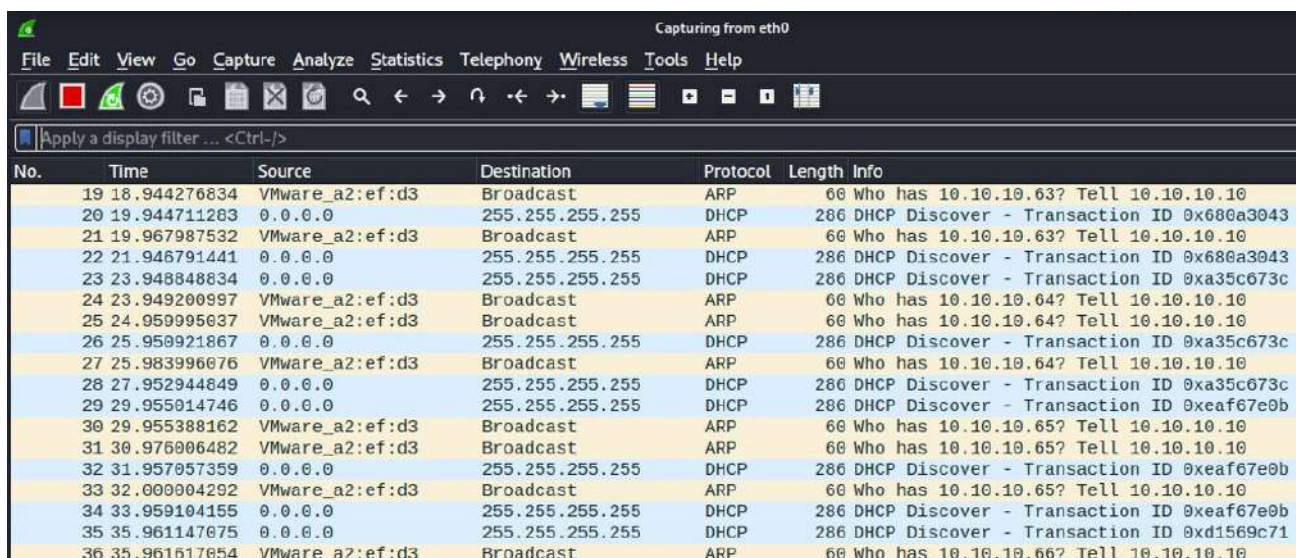
Скрипт `broadcast-dhcp-discover` в составе `nmap` рассылает `DHCPDISCOVER` в широковещательный адрес и получает ответы серверов.

## 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
```



| 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 0x680a3043 |
| 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 0x680a3043 |
| 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  | 24.959995037 | 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 0xeaf67e0b |
| 30  | 29.955388162 | VMware_a2:ef:d3 | Broadcast       | ARP      | 60     | Who has 10.10.10.65? Tell 10.10.10.10     |
| 31  | 30.976006482 | VMware_a2:ef:d3 | Broadcast       | ARP      | 60     | Who has 10.10.10.65? Tell 10.10.10.10     |
| 32  | 31.957057359 | 0.0.0.0         | 255.255.255.255 | DHCP     | 286    | DHCP Discover - Transaction ID 0xeaf67e0b |
| 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 0xeaf67e0b |
| 35  | 35.961147075 | 0.0.0.0         | 255.255.255.255 | DHCP     | 286    | DHCP Discover - Transaction ID 0xd1569c71 |
| 36  | 35.961517054 | 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 Replay
- ☒ DHCP Starvation
- ☐ DNS Injection
- ☐ ARP Spoofing
- ☐ ARP Poisoning

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

### Решение:

В логах DHCP при атаке Starvation видно множество запросов за короткий промежуток времени от разных (возможно поддельных) MAC-адресов, из-за чего быстро заканчивается пул свободных IP-адресов. Собственно, в этом и суть атаки «голода» (Starvation) IP адресов – у DHCP сервера заканчиваются свободные адреса для выдачи.

## 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**

### Решение:

При создании пользователя `useradd` добавляет запись в `/etc/passwd`, хеш пароля в `/etc/shadow` и обновляет группы в `/etc/group`; домашний каталог создаётся отдельно и не является «системным файлом» в этом смысле.

## 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**

### Решение:

Команда `scp /usr/file user@192.168.4.46:/path/` использует SSH для шифрования трафика при копировании файла, обеспечивая защищённый перенос данных.

## 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

### Решение:

Shellcode — это машинный код, который выполняется после эксплуатации уязвимости и обычно запускает командную оболочку для дальнейшего управления системой.

## 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**

**Решение:**

Форма ps аих традиционно показывает список всех процессов для всех пользователей с параметрами работы (объём памяти, загрузка процессора и т.п.) т.е. колонками USER, PID, %CPU, %MEM, VSZ, STAT и т. д., что и видно на подобных скриншотах.

---

**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**

**Решение:**

Ключ `-name passwd` отбирает файлы с именем passwd, а `-perm 4000` ищет только те, у которых установлен бит SUID (четвёрка в старшем разряде прав).

## 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
- ☐ docker
- ☐ dhcp
- ☐ terraform
- ☐ bash

Точное совпадение ответа — 1 балл

Максимальный балл за задание — 1

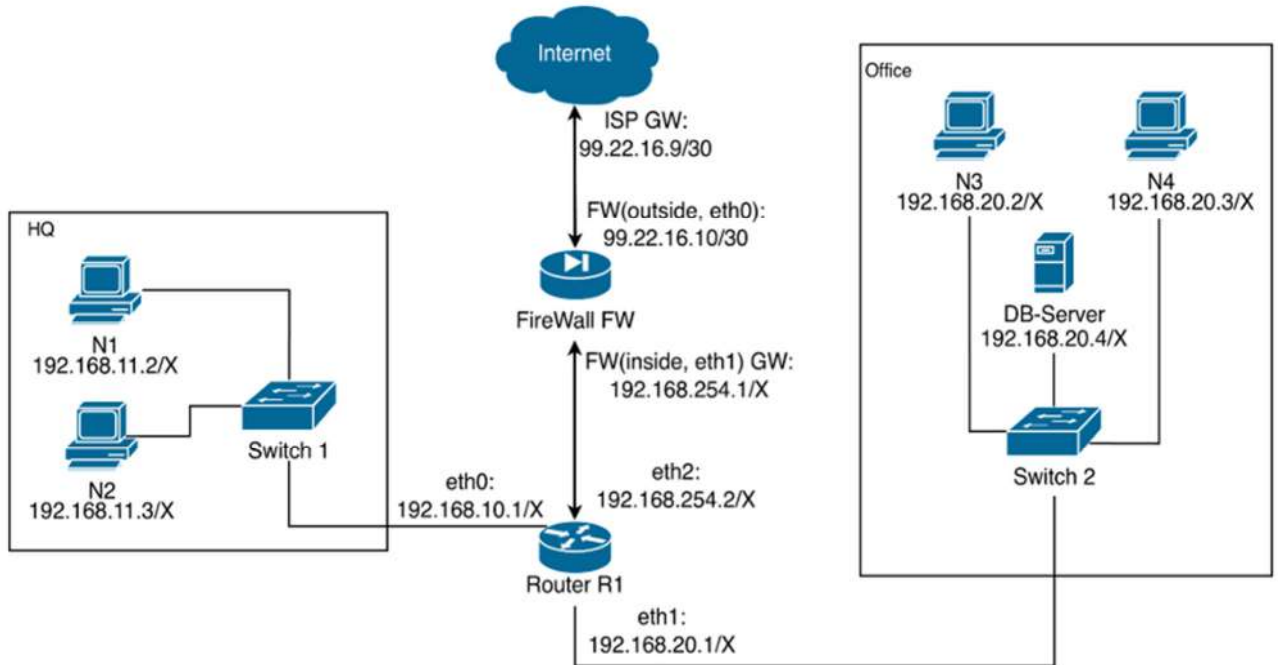
### Решение:

Отрывок в стиле YAML с описанием «tasks», «hosts» и модулей (например, copy, package) характерен для плейбуков Ansible, а не для Docker, DHCP или Terraform.

## 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:** 192.168.254.3

**Точное совпадение ответа — 1 балл**

### Решение:

Для /30 блок из четырёх адресов: сетевой (.0), два хоста (.1 и .2) и широковещательный (.3), поэтому broadcast — 192.168.254.3.

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.

**Решение:**

.8 — адрес сети, .11 — broadcast, поэтому эти два адреса недопустимы для интерфейсов.

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

**Ответ:** 29

**Точное совпадение ответа — 2 балла**

**Решение:**

Подсеть Office содержит несколько узлов, и /29 — самый «узкий» префикс, который всё ещё даёт достаточно рабочих IP (6), не разрывая сеть на части.

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

**Ответ:** iptables -A FORWARD -i eth0 -o eth1 -s 192.168.10.0/24 -d 192.168.20.4 -p tcp --dport 443 5432 -j ACCEPT

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

**Решение:**

Используем FORWARD, потому что пакет идёт через R1 между сетями HQ и Office, а не к самому маршрутизатору. Поля -s/-d фиксируют сеть-источник и конкретный IP сервера, -p tcp --dport 5432 отбирают только соединения PostgreSQL, а -i/-o задают правильное направление интерфейсов.

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**

**Решение:**

Подсети 192.168.10.0/24 и 192.168.20.0/24 попадают в диапазон 192.168.0.0–192.168.31.255, который описывает сеть /19; более узкие префиксы (например, /20) уже не вместили бы обе.

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:** iptables -A FORWARD -s 192.168.20.0/29 -o eth0 -p tcp -m multiport --dports 80,443 -j ACCEPT

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

**Решение:**

Ставим правило в FORWARD, потому что через этот узел трафик просто проходит наружу. -s 192.168.20.0/29 ограничивает источник маленькой подсетью Office, -o eth0 выбирает внешний интерфейс, а -m multiport --dports 80,443 пропускает только HTTP/HTTPS по TCP.

**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:** vsosh{Ru\_Zvezdochka}

**Точное совпадение ответа — 3 балла**

**Максимальный балл за задание — 3**

**Решение:**

Программа на C++ имитирует "полимерный поток". Ввод длиной 20 символов обрабатывается парами через очередь. Операции:  $\text{new\_alpha} = (\text{alpha} \wedge 0x55) + (i * 2)$ ,  $\text{new\_beta} = (\text{beta} \wedge \text{new\_alpha}) - 10$ . Для решения нужно обратить эти операции для каждой из 10 пар в обратном порядке.

Ответ: ``vsosh{Ru_Zvezdochka}``

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:** 10.20.30.99

**Точное совпадение ответа — 1 балл**

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

**Ответ:** 172.16.0.5:8500

**Точное совпадение ответа — 2 балла**

Определите переданный флаг.

**Ответ:** vsosh{ssrf\_ch41n\_1nt3rn4l}

**Точное совпадение ответа — 2 балла**

**Максимальный балл за задание — 6**

**Решение:**

Атака SSRF, где через один уязвимый сервис атакуется другой внутренний сервис (Consul на порту 8500). Нужно отследить цепочку запросов от атакующего (IP 10.20.30.99).

Целевые пакеты: 271, 308, 312, 316, 320, 324.

Тип атаки: Server-Side Request Forgery (SSRF)

IP атакующего: 10.20.30.99

Внутренний сервис: 172.16.0.5:8500

Флаг: `vsosh{ssrf_ch41n_1nt3rn4l}`

**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; кратность длины кодирования имеет значение. Ваша задача — извлечь секретную информацию.

**Ответ:** `vsosh{b4s3_85_4nd_t4r_f0r_fun}`

**Точное совпадение ответа — 3 балла**

**Максимальный балл за задание — 3**

**Решение:**

Используется "нестандартная база" и "архив". Анализ длины и символов указывает на Base85. После 12 итераций декодирования Base85 получается Tar-архив. Внутри архива в папке ``secret/`` лежит файл ``flag.txt`` с флагом ``vsosh{b4s3_85_4nd_t4r_f0r_fun}``.

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())
```