ИНТЕЛЛЕКТУАЛЬНЫЙ МЕГАПОЛИС

ЗАДАЧНИК

ИТ-класс

в московской школе

НАПРАВЛЕНИЕ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ТЕХНОЛОГИИ СВЯЗИ

ПРАКТИЧЕСКИЙ ЭТАП

МОСКВА
2025

ИНТЕЛЛЕКТУАЛЬНЫЙ МЕГАПОЛИС

ЗАДАЧНИК РАЗРАБОТАН:

Подлесных Дмитрием Артуровичем, старшим преподавателем кафедры информатики и вычислительной математики МФТИ, тренером Центра развития ИТ-образования МФТИ

Колыбельниковым Александром Ивановичем, старшим преподавателем кафедры логистических систем и технологий МФТИ, старшим преподавателем Центра образовательных программ ФРКТ МФТИ, старшим преподавателем Центра образовательных программ топ-уровня по информационным технологиям МФТИ

МОСКВА
2025

ВАРИАНТЫ ЗАДАЧ 4,5,6

ВАРИАНТ 1 4

ВАРИАНТ 2 9

ВАРИАНТ 3 12

ВАРИАНТ 4 15

ВАРИАНТ 5 18

ВАРИАНТ 6 21

ВАРИАНТ 7 25

ВАРИАНТ 8 28

ВАРИАНТ 9 31

ВАРИАНТ 10 35

ВАРИАНТ 11 38

ВАРИАНТ 12 42

ВАРИАНТ 13 45

ВАРИАНТ 14 48

ВАРИАНТ 15 51

ВАРИАНТ 16 54

ВАРИАНТ 17 57

ВАРИАНТ 18 60

ВАРИАНТ 19 64

ВАРИАНТ 20 68

ВАРИАНТ 21 71

ВАРИАНТ 22 74

ВАРИАНТ 23 78

ВАРИАНТ 24 82

ВАРИАНТ 25 86

ВАРИАНТ 26 89

ВАРИАНТ 27 92

ВАРИАНТ 28 95

ВАРИАНТЫ ЗАДАЧ 4,5,6

ВАРИАНТ 1

ЗАДАЧА 4.

Как называется метод взлома, использующий уязвимости человеческого фактора? Допускается ответ на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: социнженерия, соц. инженерия, социальная инженерия, social engineering)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует	**0**

Ответ:
социальная инженерия/ social engineering.

ЗАДАЧА 5.

В организации виртуальный сервер с 100-гигабайтным жёстким диском стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/nvme0n1p7   95G   95G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/nvme0n1p7 on / type ext3 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G80G /*home/vasya/proof_of_storage*

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только nvme0n1p7	1	
Учащийся определил, что proof_of_storage, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок.	1	
Смонтирован накопитель для резервного копирования	1	
Каталог proof_of_storage перемещён на резервный накопитель	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Видим, что закончилось место на 100-гигабайтном жёстком диске, но видим только 95 Гб на файловой системе ext3. Значит, есть стандартные 5 Гб, зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге proof_of_storage. Это сразу наводит на подозрения, что это - майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/nvme0n1p7Смонтируем резервный накопитель, перенесём на него proof_of_storage, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Пользователю vasya@shkola.su пришло письмо с весьма заманчивым предложением работы с зарплатой в размере 100 000 биткоинов в наносекунду. Согласно тексту письма, на работу приглашает сам генсек ООН.

Received: from relay1.ele-ele.com (91.215.42.222) by relay2.ele-ele.com (proof_of_storagetfix) with SMTP id 29467120A4F for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>

Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)

From: gensec@un.org

Вася стал исследовать:*dig TXT un.org*

; <<>> DiG 9.16.20 <<>> un.org;; global options: +cmd;; Got answer:;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32514;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1;; OPT PSEUDOSECTION:; EDNS: version: 0, flags:; udp: 1232;; QUESTION SECTION:;un.org. IN A;; ANSWER SECTION:un.org. 600 IN A 157.150.185.92un.org. 600 IN A 157.150.185.49;; Query time: 176 msec;; SERVER: 192.168.8.1#53(192.168.8.1);; WHEN: Thu Jul 10 22:51:42 MSK 2025;; MSG SIZE rcvd: 67

;dig TXT un.org

; <<>> DiG 9.16.20 <<>> TXT un.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 23566
;; flags: qr rd ra; QUERY: 1, ANSWER: 23, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;un.org. IN TXT

;; ANSWER SECTION:
un.org. 3600 IN TXT "56a37f487f3361c43f8c285de2f7f60839ac3a7f1bd37b37353ecd343c995fa2"
un.org. 3600 IN TXT "sendinblue-code:c80931e2ffea8fadc62c1bfb5141f449"
un.org. 3600 IN TXT "cisco-ci-domain-verification=71023db9cebccd164d6c6916b649179c4109a8bf4a53206db808dc9c778dd271"
un.org. 3600 IN TXT "d365mktkey=GU4x93TE2dUlhH2NSdB6v7gbxcKnvDje0eF8WD0rNnUx"
un.org. 3600 IN TXT "iContact1651565"
un.org. 3600 IN TXT "mandrill_verify.J6D4EK4DxGiLqR1nMTfHSA"
un.org. 3600 IN TXT "cisco-ci-domain-verification=3be0a328c387dcfe19bfab64b24e33f04b04e2065771adbc4043b754f65d8392"
un.org. 3600 IN TXT "rij4mb6stfqk9nqp6db054r4se"
un.org. 3600 IN TXT "teamviewer-sso-

```
verification=fde5c90fdb764da199caa79160aef58b"
un.org.          3600    IN      TXT     "atlassian-domain-
verification=1rY0mwP3xqUqI0Z6SVEdrrPHJ4hquQL28GrmRTVZ6/IZMKDmPspPa9jE7fXrIY
Mj"
un.org.          3600    IN      TXT
   "webexdomainverification.4C675B882DC2B136E053AB06FC0A3F65=6652b0a5-c301-4a9f-
8629-d7e156da37b8"
un.org.          3600    IN      TXT     "apple-domain-verification=yaMAnI0GjK2mwjBL"
un.org.          3600    IN      TXT     "brevo-code:0502b29d26710cfe3a7f5a6713f7b141"
un.org.          3600    IN      TXT     "brevo-code:4258a8aaff2c4cc4d4f46631ee3f416d"
un.org.          3600    IN      TXT     "atlassian-sending-domain-verification=030cf619-e1ff-
4c61-b2ff-0b8bf31422e8"
un.org.          3600    IN      TXT     "MS=ms26002463"
un.org.          3600    IN      TXT
   "xrqyoOBvFUFgFNdafNF3eo+zN4SEGAc+1gcHkfcbobjGa/UFAkMc/rCWUxywPjgWU1yMI
YtuFAnHfLXdgFbRLQ=="
un.org.          3600    IN      TXT
   "FOhfWhsJtJ/FZcqQdLjqBNwOqynP/KX4ozWsJFw+k50mDbWjv05zbvEonHMzMIKP9XSZ7
7kWWuilSHT/t7BQ8w=="
un.org.          3600    IN      TXT     "atlassian-domain-
verification=4qBZ2F7TUigBgD7l6Ate/ExncM2HVQU855IzHmcHurVkPVGUU6H2ATvyZFEnn
k9N"
un.org.          3600    IN      TXT
   "amazonses:cq717whOBbl30dhYr9HtG5aBpZfmtVwZ8/8TyeUrXh8="
un.org.          3600    IN      TXT     "v=spf1 include:_netblocks.un.org
include:_netblocks2.un.org -all"
un.org.          3600    IN      TXT     "atlassian-sending-domain-verification=b818d67b-c504-
4b82-a2ac-fb1ffa5dd99e"
un.org.          3600    IN      TXT
   "j9lgbXbR0aOn/a3/tHAIQ1aK4uhUriBVu4/6I88jmBK0NyrCV36RIyrHwXouU3F0uQSEK0EP
j6eBZ/Tc1odW4w=="

;; Query time: 576 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Thu Jul 10 22:53:07 MSK 2025
;; MSG SIZE  rcvd: 1778

 dig MX  un.org

; <<>> DiG 9.16.20 <<>> MX un.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36422
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
```

;; QUESTION SECTION:
;un.org. *IN* *MX*

;; ANSWER SECTION:
un.org. *600* *IN* *MX* *0 un-org.mail.protection.outlook.com.*

;; Query time: 116 msec
;; SERVER: 192.168.8.1#53(192.168.8.1)
;; WHEN: Thu Jul 10 22:53:22 MSK 2025

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе приведённых данных по биткоинам в связке с наносекундами и информации об адресе отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как невозможную или нереалистичную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес отправителя не соответствует SPF записи	**5**
ИТОГО	**10**

Ответ:
Всего может быть 21 миллион биткоинов. При зарплате 100 000 биткоинов в наносекунду они исчерпаются за 210 наносекунд. Адрес отправителя не соответствует SPF записи домена un.org.

ВАРИАНТ 2

ЗАДАЧА 4.

Как называется метод взлома, использующий полный перебор отправляемых данных? Допускается ответ на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: метод грубой силы, brute force, bruteforce,bruteforcing, брутфорс)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует	**0**

Ответ:
брутфорсинг/метод грубой силы/bruteforce/ brute force/bruteforcing/брутфорс.

ЗАДАЧА 5.

В организации виртуальный сервер с 16 ядрами стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): **200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	1600.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
14	root	20	0	0	0	0	S	0.0	0.0	0:23.83	ksoftir+
15	root	20	0	0	0	0	I	0.0	0.0	11:22.93	rcu_pre+

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (16 ядер из 16 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в

контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Пользователь vasya@itclass.su получил сообщение от владельцев сервера t.me с его аккаунтом. Вымогатель требует 120 ETH, угрожая опубликовать 100 500 кветтабайт переписки Васи, в которой он обсуждает действия, описываемые главой 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной безопасности».
Received: from relay1.ele-ele.com (92.225.42.222) by relay2.ele-ele.com (Postfix) with SMTP id 29467120A4F for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>
Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)
From: interpol@t.me

Вася стал исследовать:dig TXT t.mevk.cc. 889 IN TXT "v=spf1 -all"

Задание:

Можно ли доверять вымогателю? Ответ обоснуйте на основе анализа объёма информации и адреса отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как невозможную или нереалистичную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес отправителя не соответствует SPF записи	**5**
ИТОГО	**10**

Ответ:

1. 100500 * 10^{30} байтов — нереалистичный объём информации.
2. Для t.me SPF записи пустые.

ВАРИАНТ 3

ЗАДАЧА 4.

Какая уязвимость позволяет пользователю забрать любой файл с сервера? Ответ дайте в аббревиатуре.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: LFI, Local File Inclusion)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует	**0**

Ответ:
LFI.

ЗАДАЧА 5.

В организации виртуальный сервер с 100-гигабайтным жёстким диском стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/sda7        90G   90G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/sda7 on / type ext4 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G80G /*home/vasya/PoS*

Задание:

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только sda7	1	
Учащийся определил, что PoS, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/sda7 Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок	1	
Смонтирован накопитель для резервного копирования	1	
Каталог PoS перемещён на резервный накопитель	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
ИТОГО		**15**

Ответ:

Видим, что закончилось место на 100-гигабайтном жёстком диске, но видим только 90 Гб на файловой системе ext4. Значит, есть 10 Гб, зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге PoS. Это сразу наводит на подозрения, что это –майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/sda7Смонтируем резервный накопитель, перенесём на него PoS, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Пользователю vasya@itclass.su пришло письмо с весьма заманчивым предложением работы с зарплатой в размере 100 500 биткоинов в наносекунду. Согласно тексту письма, на работу приглашает сам руководитель «Технокубка».

Received: from relay1.ele-ele.com (91.215.42.222) by relay2.ele-ele.com (Postfix) with SMTP id 29467120A4F for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>
Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)
From: president@techno-cup.ru

Вася стал исследовать:*dig TXT techno-cup.ru*

v=spf1 ip4:176.112.170.0/31 ip4:89.221.228.76/31" " redirect=_spf.mail.ru"

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе приведённых данных по биткоинам в связанности с наносекундами и информации в части адреса отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как невозможную или нереалистичную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес отправителя не соответствует SPF записи	**5**
ИТОГО	**10**

Ответ:

1. Всего может быть 21 миллион биткоинов. При зарплате 100 500 биткоинов в наносекунду они исчерпаются за 209 наносекунд.
2. Адрес отправителя не соответствует SPF записи домена techno-cup.ru.

ВАРИАНТ 4

ЗАДАЧА 4.

Какой User ID у самого главного пользователя в операционной системе Linux?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ (0)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка (root)	**3**
Ответ неправильный, либо отсутствует	**0**

Ответ:
0.

ЗАДАЧА 5.

В организации виртуальный сервер с 8 ядрами стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): **200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1234	vasya	20	0	169652	14136	9084	S	800.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
14	root	20	0	0	0	0	S	0.0	0.0	0:23.83	ksoftir+
15	root	20	0	0	0	0	I	0.0	0.0	11:22.93	rcu_pre+

Задание:

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
ИТОГО		**15**

Ответ:
Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (2 ядра из 2 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al /proc/1234/executable), убьём процесс (kill -9 1234), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Пользователь vasya@itclass.su получил сообщение от владельцев сервера vc.cc с его аккаунтом. Вымогатель требует 120 ETH, угрожая опубликовать 100 500 кветтабайт переписки Васи, в которой он обсуждает действия, описываемые главой 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной безопасности».

Received: from relay1.ele-ele.com (92.225.42.222) by relay2.ele-ele.com (Postfix) with SMTP id 29467120A4F for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>
Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)
From: interpol@vc.cc

Вася стал исследовать: dig TXT vc.ccvk.cc. 889 IN TXT "v=spf1 -all"

Задание:

Можно ли доверять вымогателю? Ответ обоснуйте на основе анализа объёма информации и адреса отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как невозможную или нереалистичную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес отправителя не соответствует SPF записи	**5**
ИТОГО	**10**

Ответ:

1. $100500 * 10^{30}$ байтов — нереалистичный объём информации.
2. Для vc.cc SPF записи пустые.

ВАРИАНТ 5

ЗАДАЧА 4.

Какая технология позволяет создать отказоустойчивый массив независимых дисков? Ответ дайте в виде аббревиатуры.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре RAID, Redundant Array of Independent Disks)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует	**0**

Ответ:
RAID.

ЗАДАЧА 5.

В организации виртуальный сервер с 100-гигабайтным жёстким диском стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/sda7        95G   95G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/sda7 on / type ext4 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G80G /*home/kolya/PoS*

Задание:

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только sda7	1	
Учащийся определил, что PoS, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/sda7 Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок	1	
Смонтирован накопитель для резервного копирования	1	
Каталог PoS перемещён на резервный накопитель	1	
Заблокирован вход пользователю kolya по паролю	1	
Удалены авторизованные ключи пользователя kolya	1	
Удалены задачи пользователя kolya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Скомпрометированная система восстановлена из резервной копии	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
ИТОГО		**15**

Ответ:

Видим, что закончилось место на 100-гигабайтном жёстком диске, но видим только 95 Гб на файловой системе ext4. Значит, есть стандартные 5 Гб, зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь kolya, причём в каталоге PoS. Это сразу наводит на подозрения, что это – майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/sda7Смонтируем резервный накопитель, перенесём на него PoS, поинтересуемся у Коли, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю kolya вход по паролю (passwd -L kolya), переименуем его авторизованные ключи (cp -p /home/kolya/.ssh/authorized_keys /tmp/kolya_kswapd_keys, rm /home/kolya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u kolya, crontab -r -u kolya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Пользователю kolya@itclass.su пришло письмо с весьма заманчивым предложением работы с зарплатой в размере 100 500 биткоинов в наносекунду. Согласно тексту письма, на работу приглашает сам ректор Воронежского университета.

Received: from relay1.ele-ele.com (191.215.42.222) by relay2.ele-ele.com (Postfix) with SMTP id 29467120A4F for <kolya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>
Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)
From: rector@webhost.vsu.ru

Коля стал исследовать:*dig TXT webhost.vsu.ru 2385 IN TXT "v=spf1 a:relay1.vsu.ru -all"*

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе приведённых данных по биткоинам в связке с наносекундами и информации об адресе отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как невозможную или нереалистичную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес отправителя не соответствует SPF записи	**5**
ИТОГО	**10**

Ответ:

1. Всего может быть 21 миллион биткоинов. При зарплате 100 500 биткоинов в наносекунду они исчерпаются за 209 наносекунд.
2. Адрес отправителя не соответствует SPF записи домена webhost.vsu.ru.

ВАРИАНТ 6

ЗАДАЧА 4.

Назовите уязвимость, позволяющую пользователю отправлять запросы от имени сервера. Допускается ответ на русском или английском языке.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ (без орфографических ошибок, в верхнем или нижнем регистре допустимо: Server-Side Request Forgery (SSRF)/ подделка запросов со стороны сервера)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует	**0**

Ответ:
Server-Side Request Forgery (SSRF)/ подделка запросов со стороны сервера.

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами стал работать с перебоями.

Команда top вывела:top - 23:02:45 up 52 days, 15:04, 3 users, load average: 0.00, 0.00, 0.00
Tasks: **1901** total, **1** running, **1900** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): **200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1234	petya	20	0	169652	14136	9084	S	3200.0	20.0	1:44.60	kswapd
2	petya	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
14	root	20	0	0	0	0	S	0.0	0.0	0:23.83	ksoftir+

15 root 20 0 0 0 0 I 0.0 0.0 11:22.93 rcu_pre+

Задание:

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd и kthreadd должен быть запущен от root'а, запуск от пользователя petya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю petya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя petya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
ИТОГО		**15**

Ответ:
Процессы kswapd и ktrheadd должны быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (32 ядра из 32 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al /proc/1234/executable), убьём процесс (kill -9 1234), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/petya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u petya, crontab -r -u petya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети

(или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux или AppArmour.

ЗАДАЧА 6.

Пользователь vasya@itclass.su получил сообщение от владельцев сервера w3.org с его аккаунтом. Вымогатель требует 120 ETH, угрожая опубликовать 100 500 кветтабайт переписки Васи, в которой он обсуждает действия, описываемые главой 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной безопасности».
Received: from relay1.ele-ele.com (91.215.52.222) by relay2.ele-ele.com (Postfix) with SMTP id 29467120A4F for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>
Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)
From: interpol@w3.org

Вася стал исследовать:dig TXT w3.org; <<>> DiG 9.11.4-P2-RedHat-9.11.4-16.P2.el7_8.6 <<>> TXT w3.org;; global options: +cmd;; Got answer:;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 48032;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 13, ADDITIONAL: 1;; OPT PSEUDOSECTION:; EDNS: version: 0, flags:; udp: 4096;; QUESTION SECTION:;w3.org. IN TXT;; ANSWER SECTION:w3.org. 300 IN TXT "v=spf1 mx ip4:34.238.48.92 ip4:34.199.101.240 ip6:2600:1f18:7d7a:2700::/56 include:_spf.google.com ~all"w3.org. 300 IN TXT "853C844562"w3.org.
300 IN TXT "ca3-d6556337888945edac9c159a068c46a2"w3.org.
300 IN TXT "google-site-verification=CZkSL9bXgKDxRmeDnAQorwhaQy3Ji1vTn36bBn5rL-E"w3.org.
300 IN TXT "google-site-verification=cu9dn6ytlndLOV87MLxedTHxoKTRKk0dUf_jXK8OsTc"w3.org.
300 IN TXT "google-site-verification=5TpwKtmzdpa5fntQgKHY96mTJ3FiSn9fGp07XKxFsMk"w3.org.
300 IN TXT "google-site-verification=dS4IjfXgopxupUFDAqg3wk94IIZ2GuQ-jW4wiLm69Rg"

Задание:

Можно ли доверять вымогателю? Ответ обоснуйте на основе анализа объёма информации и адреса отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как невозможную или нереалистичную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес отправителя не соответствует SPF записи	**5**
ИТОГО	**10**

Ответ:

1. 100500 * 10^{30} байтов — нереалистичный объём информации.
2. IP 91.215.52.222 не соответствует spf1-записи для w3.org“v=spf1 mx ip4:34.238.48.92 ip4:34.199.101.240”.

ВАРИАНТ 7

ЗАДАЧА 4.

Какие возможности даёт атакующему уязвимость типа «инъекция»?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть уязвимости типа инъекции, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: инъекция – это класс уязвимостей, при котором злоумышленник передаёт в приложение неочищённые внешние данные, которые интерпретируются системой как команды или инструкции, что позволяет нарушить нормальную работу системы, получить несанкционированный доступ к данным или выполнить нежелательные действия	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует. Общие фразы вроде «взлом через ввод» или «вредоносный ввод» без указания на интерпретацию как команд не засчитываются	**0**

Ответ:
запуск любого кода на сервере, в том числе вредоносного.

ЗАДАЧА 5.

В организации виртуальный сервер с 1000-гигабайтным жёстким диском стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/sda7       950G   950G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/sda7 on / type ext4 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G80G /*home/vasya/PoS*

Задание:

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только sda7	1	
Учащийся определил, что PoS, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/sda7 Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок	1	
Смонтирован накопитель для резервного копирования	1	
Каталог PoS перемещён на резервный накопитель	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры или виртуальные машины с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Видим, что закончилось место на 1000-гигабайтном жёстком диске, но видим только 950 Гб на файловой системе ext4. Значит, есть стандартные 50 Гб, зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге PoS. Это сразу наводит на подозрения, что это – майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/sda7Смонтируем резервный накопитель, перенесём на него PoS, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически

запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры или виртуальные машины с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Пользователю vasya@itclass.su пришло письмо с весьма заманчивым предложением работы с зарплатой в размере 100 500 биткоинов в наносекунду. Согласно тексту письма, на работу приглашает сам руководитель ВКонтакте.

Received: from relay1.ele-ele.com (91.215.42.232) by relay2.ele-ele.com (Postfix) with SMTP id 29467120A4F for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>
Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)
From: president@vk.com

Вася стал исследовать:*dig TXT vk.com;vk.com. IN TXT;; ANSWER SECTION:vk.com. 900 IN TXT "yandex-verification: 0bb3aeafaf40a3fa"vk.com. 900 IN TXT "wmail-verification: 646ff42e916a2be1aa86be6d3c742949"vk.com. 900 IN TXT "LD6VaYCKete4UB5FIx7snCoJ8bt1nGdeCWe4my5HH5psRaTl" "zAmvc"vk.com. 900 IN TXT "v=spf1 ip4:93.186.224.0/20 ip4:87.240.128.0/18 i" "p4:95.142.192.0/21 mx include:_spf.google.com in" "clude:_spf.mail.ru ~all"vk.com. 900 IN TXT "_globalsign-domain-verification=YM9xQ7VIOTNzoxGpxAE1kwy28slNTGWXflmZgt73D9"vk.com. 900 IN TXT "google-site-verification=bQE4SQUYC7KTvk4XCaMdwF0e_tj-O-6ZXMfXW2a8mHY"vk.com. 900 IN TXT "HARICA-fLc9OEonBmci43ogW3C"*

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе приведённых данных по биткоинам в связанности с наносекундами и информации в части адреса отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как невозможную или нереалистичную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес отправителя не соответствует SPF записи	**5**
ИТОГО	**10**

Ответ:

1. Всего может быть 21 миллион биткоинов. При зарплате 100 500 биткоинов в наносекунду они исчерпаются за 209 наносекунд.
2. Адрес отправителя не соответствует SPF записи домена vk.com.

ВАРИАНТ 8

ЗАДАЧА 4.

Какие методы можно применить для защиты от инъекций? Приведите как минимум один ВАРИАНТ метода.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть метода защиты от уязвимости типа инъекции, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: предварительно сгенерированный запрос/ библиотеки для работы с пользовательскими данными со встроенной защитой	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует. Общие фразы вроде «фильтрация ввода» или «анализ ввода» без указания на методы анализа инъекций не засчитываются	**0**

Ответ:
предварительно сгенерированный запрос/ библиотеки для работы с пользовательскими данными со встроенной защитой.

ЗАДАЧА 5.

В организации виртуальный сервер с 200-гигабайтным жёстким диском на базе OpenSuSE стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/nvme0n1p7           190G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/nvme0n1p7 on / type ext3 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G160G /*home/vasya/proof_of_storage*

Задание:
Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только nvme0n1p7	1	
Учащийся определил, что proof_of_storage, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/nvme0n1p7. Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок	1	
Смонтирован накопитель для резервного копирования	1	
Каталог proof_of_storage перемещён на резервный накопитель	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Видим, что закончилось место на 200-гигабайтном жёстком диске, но видим только 190 Гб на файловой системе ext3. Значит, есть стандартные 10 Гб (5%), зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге proof_of_storage. Это сразу наводит на подозрения, что это – майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/nvme0n1p7Смонтируем резервный накопитель, перенесём на него proof_of_storage, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим AppArmour (т. к. OpenSuSE)

ЗАДАЧА 6.

Пользователю vasya@shkola.su пришло письмо. Отправитель представился космонавтом, которого забыли на МКС, а его работа — поставлять кислород на Солнце, чтобы оно продолжало гореть. Ему не хватает 150 миллионов рублей, чтобы отправить ракету с недостающим кислородом.

Received: from iss.space by relay2.ele-ele.com (10.55.24.78) with SMTP id 29467120A4F for <vasya@itclass.su>; Tue, 30 Apr 2025 18:26:20 +0300 (MSK)Message-Id: <202504130152728.01AA81207D9@relay1.ele-ele.com>

Date: Tue, 30 Apr 2025 18:27:28 +0300 (MSK)

From: oxygen@iss.space

Вася стал исследовать: *host iss.space*

Host iss.space not found: 3(NXDOMAIN)

Задание:

Можно ли доверять отправителю? Ответ обоснуйте, опираясь на данные доменного имени.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как вызывающую сомнения и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Судя по выводу команды, доменного имени iss.space не существует	**5**
ИТОГО	**10**

Ответ:

1. Письмо, отправленное по адресу vasya@itclass.su, пришло на адрес электронной почты vasya@shkola.su. Адреса не совпадают, что похоже на массовую спам-рассылку с использованием поля в заголовке письма BCC (Blind Carbon Copy).
2. Судя по выводу команды, доменного имени iss.space не существует.

ВАРИАНТ 9

ЗАДАЧА 4.

Каким образом злоумышленник может получить пароль от не принадлежащего ему аккаунта? Приведите как минимум один ВАРИАНТ.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий возможные атаки на пароли, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: пользователь использует слишком простые пароли/ нет защиты от брутфорсинга/ произошла утечка паролей/фишинг/социальная инженерия/ вредоносное ПО	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует. Общие фразы вроде «подбор пароля» или «перебор» без указания на свойства паролей или детализации атак не учитываются	**0**

Ответ:
пользователь использует слишком простые пароли/ нет защиты от брутфорсинга/ произошла утечка паролей/фишинг/социальная инженерия/ вредоносное ПО.

ЗАДАЧА 5.

В организации виртуальный сервер с 400-гигабайтным жёстким диском на базе AstraLinux стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/nvme0n1p7       380G   95G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/nvme0n1p7 on / type ext3 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G80G /*home/vasya/proof_of_storage*

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только nvme0n1p7	1	
Учащийся определил, что proof_of_storage, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/nvme0n1p7. Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок	1	
Смонтирован накопитель для резервного копирования	1	
Каталог proof_of_storage перемещён на резервный накопитель	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Видим, что закончилось место на 400-гигабайтном жёстком диске, но видим только 380 Гб на файловой системе ext3. Значит, есть стандартные 20 Гб (5%), зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге proof_of_storage. Это сразу наводит на подозрения, что это – майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/nvme0n1p7Смонтируем резервный накопитель, перенесём на него proof_of_storage, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени

модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим мандатный контроль доступа (т.к. AstraLinux).

ЗАДАЧА 6.

Пользователю vasya@shkola.su пришло письмо. Отправитель представился куратором школы и сообщил о необходимости срочно пройти предварительное тестирование для сдачи предпрофессионального экзамена на сайте конкурса «Интеллектуальный мегаполис. Потенциал» по адресу http://95.165.216.52/.

Вася стал исследовать:dig A im.mcko.ru

```
; <<>> DiG 9.16.20 <<>> A im.mcko.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26956
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 13, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;im.mcko.ru.                IN      A

;; ANSWER SECTION:
im.mcko.ru.         6905    IN      A       95.165.216.51

;; AUTHORITY SECTION:
.                   1660    IN      NS      c.root-servers.net.
.                   1660    IN      NS      k.root-servers.net.
.                   1660    IN      NS      f.root-servers.net.
.                   1660    IN      NS      g.root-servers.net.
.                   1660    IN      NS      d.root-servers.net.
.                   1660    IN      NS      j.root-servers.net.
.                   1660    IN      NS      m.root-servers.net.
.                   1660    IN      NS      l.root-servers.net.
.                   1660    IN      NS      a.root-servers.net.
.                   1660    IN      NS      b.root-servers.net.
.                   1660    IN      NS      e.root-servers.net.
.                   1660    IN      NS      h.root-servers.net.
.                   1660    IN      NS      i.root-servers.net.

;; Query time: 0 msec
;; SERVER: 93.175.30.74#53(93.175.30.74)
;; WHEN: Thu Oct 09 13:49:39 MSK 2025
;; MSG SIZE  rcvd: 266
```

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе приведённого URL и информации об адресе отправителя.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как потенциально небезопасную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
IP-адрес отличается от официального адреса конкурса im.mcko.ru	**5**
ИТОГО	**10**

Ответ:

1. Отправителем письма предлагается открыть web-ссылку, используя протокол http, а не https, что является небезопасным и снижает доверие к источнику запроса.
2. IP-адрес отличается от официального адреса конкурса im.mcko.ru.

ВАРИАНТ 10

ЗАДАЧА 4.

В чём заключается опасность последовательной проверки пароля по частям?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть атаки на подбор пароля по частям, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: можно провести time-attack (атаку по времени)/ можно подбирать пароль по частям, измеряя время ответа системы и по его увеличению определять, сколько символов подбираемого пароля уже совпало с реальным	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует. Общие фразы вроде «система скажет, что часть пароля не правильная» или «анализ времени ввода» без указания на методы подбора паролей не засчитываются	**0**

Ответ:
можно провести time-attack (атаку по времени)/ можно подбирать
пароль по частям, измеряя время ответа системы и по его увеличению определять, сколько символов подбираемого пароля уже совпало с реальным.

ЗАДАЧА 5.

В организации виртуальный сервер с 1000-гигабайтным жёстким диском стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/nvme0n1p7        950G   950G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/nvme0n1p7 on / type ext3 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G80G /*home/vasya/proof_of_storage*

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что закончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только nvme0n1p7	1	
Учащийся определил, что proof_of_storage, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/nvme0n1p7. Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок	1	
Смонтирован накопитель для резервного копирования	1	
Каталог proof_of_storage перемещён на резервный накопитель	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Видим, что закончилось место на 1000-гигабайтном жёстком диске, но видим только 950 Гб на файловой системе ext3. Значит, есть стандартные 50 Гб (5%), зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге proof_of_storage. Это сразу наводит на подозрения, что это – майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/nvme0n1p7Смонтируем резервный накопитель, перенесём на него proof_of_storage, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с

ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Вася устал от писем мошенников, поступающих на электронную почту, и перешёл на открытый протокол Jabber. К сожалению, сообщения от пользователей сервера daywave.ru не доходили.

Вася стал исследовать.

Команда dig вывела:dig +short SRV _xmpp-server._tcp.daywave.ru
30 10 5270 jabber.daywave.ru.

Задание:

Определите адрес сервера для работы по протоколу XMPP в домене daywave.ru. В чём выражается нетипичный характер его настройки?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определён адрес сервера	**5**
Верно определено, почему не приходят сообщения от пользователей указанного сервера	**5**
ИТОГО	**10**

Ответ:

1. Судя по ответу, выданному dig, у сервера доменное имя jabber.daywave.ru.
2. Выданная информация демонстрирует, что для подключения к серверу по протоколу XMPP используется порт 5270, отличающийся от стандартного 5269. Это мешает получать сообщения с сервера, так как сервер Васи ждёт сообщения на порту 5270, а ему их шлют на порт 5269.

ВАРИАНТ 11

ЗАДАЧА 4.

За что отвечает файл cookie и что в нём хранится?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть файлов cookie, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: - файл cookie – это небольшой фрагмент данных, который сервер отправляет в браузер клиента с целью сохранения состояния сессии и пользовательских предпочтений между запросами; - может хранить: идентификатор сессии (session ID); параметры пользователя (например, theme=dark, lang=ru); токены аутентификации (при соблюдении мер безопасности); информацию для трекеров (идентификаторы рекламных платформ и т.п.)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «часть сайта» или «часть браузера» без указания содержание и назначение файла не засчитываются	**0**

Ответ:

Файл cookie – это небольшой фрагмент данных, который сервер отправляет в браузер клиента с целью сохранения состояния сессии и пользовательских предпочтений между запросами. Может хранить: идентификатор сессии (session ID); параметры пользователя (например, theme=dark, lang=ru); токены аутентификации (при соблюдении мер безопасности); информацию для трекеров (идентификаторы рекламных платформ и т.п.).

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами на OpenSuSE стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00

Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie

top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00

Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie

%Cpu(s): **3200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st

MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache

MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	3200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+

```
  5 root      0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_fl+
  6 root      0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
  8 root      0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker+
 10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_perc+
 11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
 12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
 13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
 14 root      20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
 15 root      20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:
Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (32 ядра из 32 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al

/proc/12345/executable), убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим AppArmour (т. к. дистрибутив OpenSuSE).

ЗАДАЧА 6.

Борис проводит открытую олимпиаду по программированию sngcode. Открыв доступ к IP сервера, он заметил, что страничка открывается не во всех браузерах, а только в Яндекс браузере и Chromium GOST, а браузер Chrome предлагает только http подключение и выдает предупреждение о незащищенном подключении.

Борис стал исследовать:dig TXT sngcode.su

```
; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> TXT sngcode.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52614
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sngcode.su.                    IN      TXT

;; ANSWER SECTION:
sngcode.su              3600    IN      TXT     "MS=E8A668AA93DA3566440B5D30932F42417C65D045"
sngcode.su              3600    IN      TXT     "v=spf1 ip4:181.5.91.6 ip4:82.5.91.10 ip4:81.6.91.71
ip4:81.5.92.85 mx -all"
sngcode.su              3600    IN      TXT     "
nuc_gost2025_d8485616c8db8142950c7c928bea37e711a5bdea
=00b97f6db4bc762418eec75e317a1df01d683d4cde "
```

Задание:

Определите причину произошедшего. Что необходимо предпринять, чтобы подключаться к сайту по https?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определена причина произошедшего	**5**
Предложена верная рекомендация	**5**
ИТОГО	**10**

Ответ:

1. На сайте установлен сертификат с поддержкой российской криптографии в протоколе TLS, факт чего можно определить из имени сертификата nuc_gost2025.
2. Нужно использовать браузеры с поддержкой российской криптографии в протоколе TLS или заменить сертификат сайта на международный.

ВАРИАНТ 12

ЗАДАЧА 4.

При каких обстоятельствах атакующий может получить доступ к зашифрованным данным?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть атаки на криптосистему и/или зашифрованные файлы, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: атакующий может получить доступ к зашифрованным данным, если: - скомпрометирован ключ шифрования (утечка, слабая генерация); - используются устаревшие или небезопасные алгоритмы шифрования; - есть ошибки в реализации; - применены побочные каналы (например, атака по времени); - нарушена конфигурация системы или произошла утечка через социальную инженерию	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «взломать шифрование» или «раскодировать шифр» без указания содержание и назначение файла не засчитываются	**0**

Ответ:

Атакующий может получить доступ к зашифрованным данным, если: скомпрометирован ключ шифрования (утечка, слабая генерация); используются устаревшие или небезопасные алгоритмы шифрования; есть ошибки в реализации; применены побочные каналы (например, атака по времени); нарушена конфигурация системы или произошла утечка через социальную инженерию.

ЗАДАЧА 5.

В организации виртуальный сервер с 64 ядрами на AstraLinux стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00

Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie

top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00

Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie

%Cpu(s): **6400.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st

MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache

MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	6400.0	20.0	1:44.60	kswapd

```
    2 root      20   0       0      0      0 S   0.0   0.0   0:00.43 kthreadd
    3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par+
    5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_fl+
    6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker+
   10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_perc+
   11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   14 root      20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
   15 root      20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root’а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:
Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же,

настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (64 ядра из 64 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим мандатный контроль доступа (т. к. дистрибутив AstraLinux).

ЗАДАЧА 6.

Васе в Jabber написал неизвестный и попросил срочно пройти тестирование на сайте АРСИБ по адресу http://92.53.96.13/ Вася начал исследовать:

```
nslookup aciso.ru
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   aciso.ru
Address: 92.53.96.12
```

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе запроса и информации об адресе сервера.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как потенциально небезопасную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Адрес сервера неверный	**5**
ИТОГО	**10**

Ответ:

1. Неизвестным рекомендуется протокол http, а не https, что является небезопасным и снижает доверие к источнику запроса. 2. IP-адрес не совпадает с адресом АРСИБ (отличается в последнем бите).

ВАРИАНТ 13

ЗАДАЧА 4.

Как называется атака, позволяющая перехватывать данные, которыми обмениваются 2 клиента сети? Ответ можно дать на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть атаки человек посередине, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл ответа соответствует смыслу «man in the middle/ «человек посередине»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «перехват» или «социальная инженерия» без указания содержание и назначение файла не засчитываются	**0**

Ответ:
man in the middle/ «человек посередине».

ЗАДАЧА 5.

В организации виртуальный сервер с 128 ядрами на базе RHEL стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): **12800.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	12800.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
14	root	20	0	0	0	0	S	0.0	0.0	0:23.83	ksoftir+

15 root 20 0 0 0 0 I 0.0 0.0 11:22.93 rcu_pre+

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:
Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (128 ядер из 128 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого

раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux (т.к дистрибутив Red Hat).

ЗАДАЧА 6.

Васе в мессенджере MAX написал неизвестный и попросил срочно пройти тестирование на сайте http://93.175.29.143. Вася решил подключиться к указанному адресу по другому протоколу и при соединении получил сертификат, действительный для сайта с адресом openpm.mipt.ru.

Вася начал исследовать: nslookup 93.175.29.143143.29.175.93.in-addr.arpa name = openmp.mipt.ru.

Задание:

Можно ли доверять отправителю? Ответ обоснуйте на основе собранных данных.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник корректно идентифицирует ситуацию как потенциально небезопасную и приводит обоснованные аргументы, опираясь на факты, логику или количественный анализ	**5**
Сертификат действителен для openpm.mipt.ru, а не openmp.mipt.ru	**5**
ИТОГО	**10**

Ответ:

1. Неизвестный предлагает подключиться по протоколу http, а не https, что является небезопасным и снижает доверие к источнику запроса.
2. Web-адрес, указанный в сертификате, действителен для другого сайта и отличается порядком букв. Сертификат похож на специально подделанный и решающий задачу снижения рисков обнаружить факт подделки.

ВАРИАНТ 14

ЗАДАЧА 4.

В чём различие протоколов HTTP и HTTPS в части обеспечения безопасности соединения?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий факт наличия TLS в протоколе HTTPS, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: https шифрует передаваемые данные с помощью технологии TLS, что делает его более безопасным	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «более современный» или «социальная инженерия» без указания содержание и назначение файла не засчитываются	**0**

Ответ:
https шифрует передаваемые данные с помощью технологии TLS, что делает его более безопасным.

ЗАДАЧА 5.

В организации виртуальный сервер на базе OpenSuSE стал работать нестабильно. Курьер Вася решил помочь администратору: под своей учётной записью подключился к серверу и начал диагностику.

Команда docker top вывела: docker top 169777379e8e

UID	PID	PPID	C	STIME	TTY	TIME	CMD
vasya	12345	12344	29	Oct08	?	95:41:04	./kswapd

Команда cat /proc/swaps вывела:cat /proc/swaps Filename Type Size Used Priority /dev/sda3 partition 4194300 0 -2

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (большое количество потраченного процессорного времени) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим AppArmour (т.к. дистрибутив OpenSuSE).

ЗАДАЧА 6.

Васе на электронную почту поступил файл nalog_2024.doc с требованием заплатить налоги на недвижимость. К письму также был прикреплен файл электронной подписи.

Вася решил проверить подпись файла на сайте e-trust.gosuslugi.ru и обнаружил, что сертификат открытого ключа электронной подписи самоподписанный.
Задание:

Укажите на то, что вызвало Ваши подозрения.Укажите, пройдёт ли проверку такая электронная подпись.Укажите, почему Вася не должен был открывать данное письмо.Какой признак указывает на то, что сертификат был самоподписанный?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Участник корректно идентифицирует ситуацию как потенциально не безопасную и приводит обоснованные аргументы, опираясь на факты, логику	**2**
Участник обращает внимание на то, что самоподписанные сертификаты не применяются для юридически значимого документооборота и могут быть созданы любым человеком	**3**
Участник обращает внимание на устаревший формат файла	**3**
Участник знает, как отличать самоподписанные сертификаты от сертификатов, выданных доверенным удостоверяющим центром	**2**
ИТОГО	**10**

Ответ:
Все государственные ведомства обмениваются с гражданами электронными файлами только в формате pdf. Файлы формата *.doc устарели и практически не применяются.В инфраструктуре открытых ключей РФ самоподписанные сертификаты используются только головным удостоверяющим центром для аккредитации удостоверяющих центров и не могут использоваться для формирования электронных подписей. Самоподписанные сертификаты для электронной подписи документов используют мошенники.Открывать файл формата *.doc, полученный из сети интернет от неизвестного источника, небезопаносно.Поле «Владелец сертификата» (Subject) и поле «Издатель сертификата» (issuer) совпадут.

ВАРИАНТ 15

ЗАДАЧА 4.

Как обнаружить уязвимость типа инъекция?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть методов обнаружения уязвимости типа инъекции, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: «Уязвимость типа «инъекция» можно обнаружить, если в поле ввода на сайте (например, логин, поиск, форма заказа) ввести необычные символы, нарушающие нормальный синтаксис, и посмотреть, как отреагирует система. Например, одинарная кавычка «‘» может вызвать ошибку базы данных, что указывает на возможную SQL-инъекцию; символы вроде «;, |, &» могут использоваться для командных инъекций; задержки ответа или неожиданное поведение также является признаком уязвимости»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «ввести странные символы» или «послать на сайт всякий мусор» без указания на методы анализа инъекций не засчитываются	**0**

Ответ:

Уязвимость типа «инъекция» можно обнаружить, если в поле ввода на сайте (например, логин, поиск, форма заказа) ввести необычные символы, нарушающие нормальный синтаксис, и посмотреть, как отреагирует система. Например, одинарная кавычка «‘» может вызвать ошибку базы данных, что указывает на возможную SQL-инъекцию; символы вроде «;, |, &» могут использоваться для командных инъекций; задержки ответа или неожиданное поведение также является признаком уязвимости.

ЗАДАЧА 5.

В организации виртуальный сервер на базе RHEL стал работать нестабильно.

Команда docker top вывела: docker top 169777379e8e UID PID PPID C STIME TTY TIME CMD
vasya 12345 12344 29 Oct08 ? 95:41:04 ./kswapd

Команда cat /proc/swaps вывела:cat /proc/swaps Filename Type Size Used Priority /dev/sda3 partition 4194300 0 -2

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Большое количество потраченного процессорного времени наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения

отдельным пользователям. Обновим систему, включим SELinux (т.к. дистрибутив Red Hat).

ЗАДАЧА 6.

Вася зарегистрировал свой домен vasyacontact.com, но 22 сентября 2025 года он не резолвился.

```
$ dig +trace vasyacontact.tld
.82789 IN NS l.root-servers.net.
;; Received ... bytes from 127.0.0.53#53(127.0.0.53) in ... ms
* com. 172800 IN NS a.gtld-servers.net.
 ...
 ;; Received ... bytes from 199.7.83.42#53(l.root-servers.net) in ... ms
 vasyacontact.com. 172800 IN NS ns4.vasyacontact.com.
 vasyacontact.com. 172800 IN NS ns3.vasyacontact.com.
vasyacontact.com. 172800 IN NS ns2.vasyacontact.com.
vasyacontact.com. 172800 IN NS ns1.vasyacontact.com.
 ;; Received ... bytes from 192.5.6.30#53(a.gtld-servers.net.) in ... ms
 coudln't get address for 'ns4.vasyacontact.com': not found
 coudln't get address for 'ns3.vasyacontact.com': not found
 coudln't get address for 'ns2.vasyacontact.com': not found
 coudln't get address for 'ns1.vasyacontact.com': not found
```

Задание:

По выводу команды dig определите, на каком этапе и что именно сломалось в цепочке резолва. Приведите два доказательства.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Потеряли NS в зоне vasyacontact.com	**5**
Потеряли glue NS в зоне com	**5**
ИТОГО	**10**

Ответ:
1. Для анализа проблемы с резолвом DNS по выводу команды dig, необходимо:1.1. Проанализировать статус ответа (flags, status code).1.
2. Проверить наличие необходимых записей в ответе.1.
3. Оценить время отклика.1.
4. Изучить цепочку рекурсии. Из перечисленного не выполняется пункт 1.2, а именно исчезла NS-запись авторитетных серверов для сайта vasyatcontact.com2. Потеряли glue NS записи для зоны com.

ВАРИАНТ 16

ЗАДАЧА 4.

Как проверить устойчивость системы ввода пароля к time-attack?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть атаки на подбор пароля по частям, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: «можно провести time-attack (атаку по времени)/ можно подбирать пароль по частям, измеряя время ответа системы и по его увеличению определять, сколько символов подбираемого пароля уже совпало с реальным»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «система скажет, что часть пароля не правильная» или «анализ времени ввода» без указания на методы подбора паролей не засчитываются	**0**

Ответ:
ввести множество паролей, отличающихся только первыми символами,
и посмотреть на разницу по времени их обработки.

ЗАДАЧА 5.

В организации виртуальный сервер на базе AstraLinux стал работать нестабильно.

Команда docker top вывела:

```
docker top 169777379e8e
UID     PID     PPID     C     STIME     TTY     TIME     CMD
vasya   12345   12344    29    Oct08     ?       95:41:04 ./kswapd
```

Команда cat /proc/swaps вывела:

```
cat /proc/swaps  Filename                Type        Size        Used        Priority
/dev/sda3                    partition   4194300     0           -2
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root’а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
ИТОГО		**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Большое количество потраченного процессорного времени наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим мандатный контроль доступа (т.к. дистрибутив AstraLinux).

ЗАДАЧА 6.

Студент первого курса Василий заметил, что на студенческом форуме в постах всех его однокурсников адреса отображаются в виде routervendorname12345.campus.vas-gu.net. Он решил использовать это для размещения сайта в Интернете.
Однако, вернувшись домой на каникулы, он не смог подключиться к своему сайту.

Задание:

Назовите протокол, поддерживающий работу с адресами такого вида. Назовите причину невозможности подключения к этому сайту из сети интернет.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определён протокол и его настройки	**5**
Верно определена причина невозможности обращения к этому сайту из сети интернет	**5**
ИТОГО	**10**

Ответ:

1. Адреса выдаются на основе DHCP-запросов (опция hostname).
2. Адреса выдаются только в локальной сети.

ВАРИАНТ 17

ЗАДАЧА 4.

Злоумышленник получил пароль пользователя из утечки данных одного ресурса и пытается использовать его для входа в другие сервисы. Как называется такая атака?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть атаки «вброс учётных данных» или «подстановка учётных данных», без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: такая атака называется credential stuffing («вброс учётных данных» или «подстановка учётных данных»)	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «подбор пароля» или «анализ времени ввода» без указания на методы подбора паролей не засчитываются	**0**

Ответ:
Такая атака называется credential stuffing («вброс учётных данных» или «подстановка учётных данных»).

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): 3**200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	3200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+

```
   12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   14 root      20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
   15 root      20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
netstat -lnptux | head
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599         0.0.0.0:*               LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Загруженный процессор (32 ядра из 32 имеющихся) наводит на мысль, что это – майнер. Также процесс слушает сетевые соединения (получает команды

извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.

Вася настроил на домашнем компьютере почтовый сервер, но публичные почтовые сервисы почему-то отправляли его письма в папку «Спам». При проверке с помощью сервиса отладки SMTP он увидел предупреждение: "record broadband-192-0-2-10.balagan-telecom.net does not match vasily.example.com"

Задание:

Назовите основную причину попадания писем в папку со спамом. Что необходимо предпринять, чтобы письма доходили до адресатов?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определена основная причина попадания писем в спам	**5**
Предложена верная рекомендация сетевых настроек	**5**
ИТОГО	**10**

Ответ:

1. PTR запись для ipv4 не совпадает с доменом отправителя.
2. Завести в реверс зоне запись на домен Васи.

ВАРИАНТ 18

ЗАДАЧА 4.

Как называется атака по срыву питания? Допускается ответ на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть атаки глитчинг/ power glitching/ glitching, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: «Это метод аппаратной атаки, при котором в питание устройства искусственно вносятся сбои, чтобы изменить его поведение. Цель — получить доступ к защищённым данным, обойти проверки или вызвать ошибки в логике исполнения»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «выключение из розетки» или «подергать провод питания» без указания на методы атаки	**0**

Ответ:
глитчинг/ power glitching/ glitching.

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами на OpenSuSE стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): 3**200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	3200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+

```
   12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   14 root      20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
   15 root      20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
netstat -lnptux | head
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599         0.0.0.0:*               LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Загруженный процессор (32 ядра из 32 имеющихся) наводит на мысль, что это – майнер. Также процесс слушает сетевые соединения (получает команды

извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим AppArmour (т. к. дистрибутив OpenSuSE).

ЗАДАЧА 6.

Вася стал разбираться в системе доменных имён и получил список DNS записей нескольких серверов.

1)```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME alpha2.example.net.
alpha2.example.net. IN CNAME beta3.corp.example.org.
beta3.corp.example.org. IN CNAME gamma4.example.io.
gamma4.example.io. IN CNAME delta5.example.dev.
delta5.example.dev. IN CNAME beta3.corp.example.org.

delta5.example.dev. IN A 198.51.100.55
dead.example.com. IN A 192.0.2.9
```

2)```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME server2.example.net.
server2.example.net. IN CNAME app3.corp.example.org.
app3.corp.example.org. IN CNAME web4.example.io.
web4.example.io. IN CNAME api5.example.dev.

api5.example.dev. IN A 203.0.113.50

api5.example.dev. IN AAAA 2001:db8::50
foo.example.com. IN TXT "goida"
bar.example.com. IN MX 10 mail.example.com.
x.example.com. IN SRV 0 0 443 svc.example.com.
```

3)```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME node2.example.net.
node2.example.net. IN CNAME host3.lab.example.org.
host3.lab.example.org. IN CNAME service4.example.io.
service4.example.io. IN CNAME final5.example.dev.

final5.example.dev. IN TXT "goida"
final5.example.dev. IN MX 10 mail.example.com.

host3.lab.example.org. IN A 198.51.100.33
service4.example.io. IN A 198.51.100.44
```

**Задание:**

Какая из конфигураций работает, то есть вернёт IPv4 адрес? Какой IPv4 адрес вернётся при запросе к `1.example.ru`?

**Критерии оценивания:**

Максимальное количество баллов за задание – 10.

| | |
|---|---|
| Выбрана верная конфигурация | **5** |
| Выбран верный IP | **5** |
| **ИТОГО** | **10** |

Ответ:
1. Вторая конфигурация.
2. 203.0.113.50
```

ВАРИАНТ 19

ЗАДАЧА 4.

Как называется атака на отказ в обслуживании?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, атака типа DoS, DoS-атака, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: «Кибератака, при которой злоумышленник пытается сделать ресурс (например, веб-сайт, сервер или сеть) недоступным для законных пользователей. Это достигается за счёт отправки большого количества запросов, что перегружает ресурс и делает его неспособным обслуживать нормальных пользователей»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «когда сервер не обслуживает пользователя» или «атака на сервер» без указания на методы атаки	**0**

Ответ:
атака типа DoS, DoS-атака.

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами на AstraLinux стал работатьнестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): 3**200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	3200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+

```
   13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   14 root      20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
   15 root      20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
netstat -lnptux | head
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599        0.0.0.0:*         LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Загруженный процессор (32 ядра из 32 имеющихся) наводит на мысль, что это – майнер. Также процесс слушает сетевые соединения (получает команды извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и

запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим мандатный контроль доступа (т. к. дистрибутив AstraLinux).

ЗАДАЧА 6.

Петя стал разбираться в системе доменных имён и получил список DNS записей нескольких серверов.

1)
```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME server2.example.net.
server2.example.net. IN CNAME app3.corp.example.org.
app3.corp.example.org. IN CNAME web4.example.io.
web4.example.io. IN CNAME api5.example.dev.

api5.example.dev. IN A 103.0.113.70

api5.example.dev. IN AAAA 2001:db8::70
foo.example.com. IN TXT "goida"
bar.example.com. IN MX 10 mail.example.com.
x.example.com. IN SRV 0 0 443 svc.example.com.
```

2)
```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME alpha2.example.net.
alpha2.example.net. IN CNAME beta3.corp.example.org.
beta3.corp.example.org. IN CNAME gamma4.example.io.
gamma4.example.io. IN CNAME delta5.example.dev.
delta5.example.dev. IN CNAME beta3.corp.example.org.

delta5.example.dev. IN A 198.51.100.55
dead.example.com. IN A 192.0.2.9
```

3)
```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME node2.example.net.
node2.example.net. IN CNAME host3.lab.example.org.
host3.lab.example.org. IN CNAME service4.example.io.
service4.example.io. IN CNAME final5.example.dev.

final5.example.dev. IN TXT "goida"
final5.example.dev. IN MX 10 mail.example.com.

host3.lab.example.org. IN A 198.51.100.33
service4.example.io. IN A 198.51.100.44
```

Задание:

Какая из конфигураций работает, то есть вернёт IPv4 адрес? Какой IPv4 адрес вернётся при запросе к `1.example.ru`?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Выбрана верная конфигурация	**5**
Выбран верный IP	**5**
ИТОГО	**10**

Ответ:

1. Первая конфигурация.
2. 103.0.113.70

ВАРИАНТ 20

ЗАДАЧА 4.

Как называется вредоносный код, проникающий на компьютер под видом полезной программы? Допускается ответ на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, троян/ trojan, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: «разновидность вредоносной программы, которая проникает в компьютер под видом легитимного программного обеспечения. Например, под видом игр, офисных программ, утилит»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «червь» или «вирус» без указания на методы работы трояна	**0**

Ответ:
троян/ trojan.

ЗАДАЧА 5.

В организации виртуальный сервер на процессоре Эльбрус с 32 ядрами стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): 3**200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	3200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+

```
   13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   14 root      20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
   15 root      20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
netstat -lnptux | head
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599         0.0.0.0:*               LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
ИТОГО		**15**

Ответ:
Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Загруженный процессор (32 ядра из 32 имеющихся) наводит на мысль, что это – майнер. Также процесс слушает сетевые соединения (получает команды извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс

(kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим и режим безопасных вычислений (т. к. процессор Эльбрус).

ЗАДАЧА 6.

Петя настроил на домашнем компьютере почтовый сервер, но публичные почтовые сервисы почему-то отправляли его письма в папку «Спам». При проверке с помощью сервиса отладки SMTP он увидел предупреждение: "record broadband-192-0-4-10.ele-ele.com does not match petya.itclass.org"

Задание:

Назовите основную причину попадания писем в папку со спамом. Что необходимо предпринять, чтобы письма доходили до адресатов?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определена основная причина	**5**
Предложена верная рекомендация по устранению неполадок	**5**
ИТОГО	**10**

Ответ:

1. PTR запись для ipv4 не совпадает с доменом отправителя.
2. Завести в реверс зоне запись на домен Васи.

ВАРИАНТ 21

ЗАДАЧА 4.

Как называется метод разведки, использующий открытые источники? Ответ дайте в виде аббревиатуры.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, OSINT, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: процесс сбора, анализа и распространения разведывательной информации, полученной исключительно из публично доступных источников	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «разведка» или «гугл» без указания на методы сбора данных из открытых источников	**0**

Ответ:
OSINT.

ЗАДАЧА 5.

В организации виртуальный сервер с 100-гигабайтным жёстким диском на процессоре Эльбрус стал работать с перебоями.

Команда df вывела:root@server#df -h

```
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        4.0M     0  4.0M   0% /dev
tmpfs           3.9G  4.0K  3.9G   1% /dev/shm
tmpfs           1.6G  9.7M  1.6G   1% /run
tmpfs           5.0M     0  5.0M   0% /run/lock
/dev/nvme0n1p7   95G   95G   0G  100% /
tmpfs           795M     0  795M   0% /run/user/0
```

Команда mount вывела:root@server# mount| grep sd

```
/dev/nvme0n1p7 on / type ext3 (rw,relatime)
```

Команда du -h -s /home/*/*| grep G вывела:root@server# du -h -s /*home*/*/* | grep G80G /*home/vasya/proof_of_storage*

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определил, что кончилось дисковое пространство	1	
Учащийся определил, что из разделов жёстких дисков смонтирован только nvme0n1p7	1	
Учащийся определил, что proof_of_storage, полностью использующий дисковое пространство, может быть майнером криптовалюты по принципу Proof-of-Storage	1	
Меры по ликвидации проблемы		**8**
Использован резерв суперпользователя tune2fs -m 0 /*dev*/nvme0n1p7. Команда tune2fs выполнена корректно и без синтаксических или орфографических ошибок	1	
Смонтирован накопитель для резервного копирования	1	
Каталог proof_of_storage перемещён на резервный накопитель	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Видим, что закончилось место на 100-гигабайтном жёстком диске, но видим только 95 Гб на файловой системе ext3. Значит, есть стандартные 5 Гб, зарезервированные для суперпользователя. По занятому месту видим, что дисковое пространство потребляет пользователь vasya, причём в каталоге proof_of_storage. Это сразу наводит на подозрения, что это – майнер на базе предоставления жёсткого диска как места хранения.Чтобы система была управляемой, разблокируем зарезервированные 5%.tune2fs -m 0 /dev/nvme0n1p7Смонтируем резервный накопитель, перенесём на него proof_of_storage, поинтересуемся у Васи, с какой целью он майнит криптовалюту на рабочем сервере и предупредим об ответственности.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p /home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys), просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим режим безопасных вычислений (так как у нас процессор Эльбрус).

ЗАДАЧА 6.

Студент первого курса Петя заметил, что на студенческом форуме в постах всех его однокурсников адреса отображаются в виде routervendorname1234.campus.pet-gu.su.
Он решил использовать это для размещения сайта в сети Интернет.
Однако, вернувшись домой на каникулы, он не смог подключиться к своему сайту.Петя стал исследовать:dig routervendorname1234.campus.pet-gu.su<<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> routervendorname1234.campus.pet-gu.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38556
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; routervendorname1234.campus.pet-gu.su. IN A

;; ANSWER SECTION:
routervendorname1234.campus.pet-gu.su 2928 IN A 10.55.242.2

;; Query time: 19 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Oct 13 11:58:32 MSK 2025
;; MSG SIZE rcvd: 52

Задание:

Назовите протокол, выдающий сетевые адреса и его опцию, позволяющую обратиться к компьютеру по доменному имени. Назовите причину невозможности подключения к сайту.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определён источник адресов	**5**
Верно определена причина	**5**
ИТОГО	**10**

Ответ:
1. Адреса выдаются на основе DHCP-запросов (опция hostname).
2. Адреса выдаются только в локальной сети.

ВАРИАНТ 22

ЗАДАЧА 4.

Как называется раздел OSINT, занимающийся поиском географических объектов и мест на карте?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, GeoINT (Geospatial Intelligence), без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: «геопространственная разведка. Это комплексный подход к сбору, обработке и интерпретации данных, связанных с геолокацией объектов. GEOINT сочетает спутниковую разведку, географическую информацию и аналитические методы, позволяя получать подробные сведения о перемещениях объектов и территориальных изменениях»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «карты в поисковике» или «поиск места по фотографии» без указания на методы сбора геоданных из открытых источников	**0**

Ответ:
GeoINT (Geospatial Intelligence).

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами на AstraLinux стал работать нестабильно.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): 3**200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
12345	vasya	20	0	169652	14136	9084	S	3200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns

```
    8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker+
   10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_perc+
   11 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   12 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   13 root      20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
   14 root      20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
   15 root      20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
netstat -lnptux | head
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599        0.0.0.0:*         LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а

свободной памяти хватает. Загруженный процессор (32 ядра из 32 имеющихся) наводит на мысль, что это – майнер. Также процесс слушает сетевые соединения (получает команды извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим мандатный контроль доступа (т. к. дистрибутив AstraLinux).

ЗАДАЧА 6.

Вася стал разбираться в системе доменных имён и получил список DNS записей нескольких серверов.
1)
```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME alpha2.example.net.
alpha2.example.net. IN CNAME beta3.corp.example.org.
beta3.corp.example.org. IN CNAME gamma4.example.io.
gamma4.example.io. IN CNAME delta5.example.dev.
delta5.example.dev. IN CNAME beta3.corp.example.org.

delta5.example.dev. IN A 198.51.100.55
dead.example.com. IN A 192.0.2.9
```

2)
```$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME node2.example.net.
node2.example.net. IN CNAME host3.lab.example.org.
host3.lab.example.org. IN CNAME service4.example.io.
service4.example.io. IN CNAME final5.example.dev.

final5.example.dev. IN TXT "goida"
final5.example.dev. IN MX 10 mail.example.com.

host3.lab.example.org. IN A 198.51.100.33
```

service4.example.io. IN A 198.51.100.44

```

3)
```
$ORIGIN example.ru.
$TTL 300

1.example.ru. IN CNAME server2.example.net.
server2.example.net. IN CNAME app3.corp.example.org.
app3.corp.example.org. IN CNAME web4.example.io.
web4.example.io. IN CNAME api5.example.dev.

api5.example.dev. IN A 203.0.124.50
api5.example.dev. IN AAAA 2001:db8::50
foo.example.com. IN TXT "goida"
bar.example.com. IN MX 10 mail.example.com.
x.example.com. IN SRV 0 0 443 svc.example.com.
```

**Задание:**

Какая из конфигураций вернёт IPv4 адрес? Какой IPv4 адрес вернётся при запросе к `1.example.ru`?

**Критерии оценивания:**

Максимальное количество баллов за задание – 10.

| | |
|---|---|
| Выбрана верная конфигурация | **5** |
| Выбран верный IP | **5** |
| **ИТОГО** | **10** |

Ответ:
1. Третья конфигурация.
2. 203.0.124.50
```

ВАРИАНТ 23

ЗАДАЧА 4.

Сколько цифр содержится в пароле от Wi-Fi, если используется защита WPS?

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, 8, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: в пароле от Wi-Fi с защитой WPS (Wi-Fi Protected Setup) обычно 8 цифр	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «6» или «сколько пользователь задаст» без указания деталей	**0**

Ответ:
8.

ЗАДАЧА 5.

В организации виртуальный сервер с 2 ядрами на процессоре Эльбрус стал работать с перебоями.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): **200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1234	vasya	20	0	169652	14136	9084	S	200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+
10	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	mm_perc+
11	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
12	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
13	root	20	0	0	0	0	I	0.0	0.0	0:00.00	rcu_tas+
14	root	20	0	0	0	0	S	0.0	0.0	0:23.83	ksoftir+

15 root 20 0 0 0 0 I 0.0 0.0 11:22.93 rcu_pre+

Задание:

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (2 ядра из 2 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/1234/executable),* убьём процесс (kill -9 1234), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod. Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для

предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим режим безопасных вычислений, который поддерживается процессором Эльбрус.

ЗАДАЧА 6.

Студент первого курса Петя заметил, что на студенческом форуме в постах всех его однокурсников адреса отображаются в виде routervendorname1234.campus.pet-gu.su.
Он решил использовать это для размещения сайта в сети Интернет.
Однако, вернувшись домой на каникулы, он не смог подключиться к своему сайту.Он стал исследовать:dig routervendorname1234.campus.pet-gu.su<<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>> routervendorname1234.campus.pet-gu.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38556
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; routervendorname1234.campus.pet-gu.su. IN A

;; ANSWER SECTION:
routervendorname1234.campus.pet-gu.su 2928 IN A 127.0.0.1

;; Query time: 19 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Oct 13 11:58:32 MSK 2025
;; MSG SIZE rcvd: 52

Задание:

Определите протокол, выдающий сетевые адреса. Назовите причину невозможности подключения к сайту.

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определён сетевой протокол, выдающий адреса	**5**
Верно определена причина недоступности форума	**5**
ИТОГО	**10**

Ответ:
1. Адреса выдаются на основе DHCP-запросов (опция hostname).
2. Выдаётся явно ошибочный адрес. Возможно, форум расположен на том же сервере, который и реализует NAT. А, значит, он не будет доступен в сети. Признаком этого

является ответ, который содержит сетевой адрес 127.0.0.1, что указывает всегда на локальный хост. Значит, форум не доступен из сети.

ВАРИАНТ 24

ЗАДАЧА 4.

Какая уязвимость позволяет загрузить на сайт исполняемый код через не предназначенное для этого поле? Ответ можно дать на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть уязвимости типа инъекции, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: инъекция – это класс уязвимостей, при котором злоумышленник передаёт в приложение неочищённые внешние данные, которые интерпретируются системой как команды или инструкции, что позволяет нарушить нормальную работу системы, получить несанкционированный доступ к данным или выполнить нежелательные действия	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «взлом через ввод» или «вредоносный ввод» без детализации атаки	**0**

Ответ:
injection/инъекция.

ЗАДАЧА 5.

В организации виртуальный сервер с 2 ядрами на процессоре Эльбрус с операционной системой AstraLinux стал работать с перебоями.

Команда top вывела:top - 08:51:34 up 25 days, 15:04, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **191** total, **1** running, **190** sleeping, **0** stopped, **0** zombie
top - 08:52:21 up 25 days, 15:05, 2 users, load average: 0.00, 0.00, 0.00
Tasks: **192** total, **1** running, **191** sleeping, **0** stopped, **0** zombie
%Cpu(s): **200.0** us, **0.0** sy, **0.0** ni, **0.0** id, **0.0** wa, **0.0** hi, **0.0** si, **0.0** st
MiB Mem : **7941.2** total, **813.6** free, **2455.0** used, **4993.9** buff/cache
MiB Swap: **500.0** total, **500.0** free, **0.0** used. **5486.2** avail Mem

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1234	vasya	20	0	169652	14136	9084	S	200.0	20.0	1:44.60	kswapd
2	root	20	0	0	0	0	S	0.0	0.0	0:00.43	kthreadd
3	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_gp
4	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	rcu_par+
5	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	slub_fl+
6	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	netns
8	root	0	-20	0	0	0	I	0.0	0.0	0:00.00	kworker+

```
 10 root      0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_perc+
 11 root     20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
 12 root     20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
 13 root     20   0       0      0      0 I   0.0   0.0   0:00.00 rcu_tas+
 14 root     20   0       0      0      0 S   0.0   0.0   0:23.83 ksoftir+
 15 root     20   0       0      0      0 I   0.0   0.0  11:22.93 rcu_pre+
```

Задание:

1. Определите, что произошло с сервером.
2. Укажите, что вызвало Ваши подозрения.
3. Какие меры нужно предпринять для ликвидации проблемы?4. Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определяет, что kswapd должен быть запущен от root'а, запуск от пользователя vasya указывает на подделку	1	
Учащийся определяет, что процесс kswapd не должен быть активен при наличии свободной памяти и полностью свободного swap	1	
Учащийся определяет, что процесс, полностью использующий CPU, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	1	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	1	
У вредоносного исполняемого файла удалены права на исполнение	1	
Заблокирован вход пользователю vasya по паролю	1	
Удалены авторизованные ключи пользователя vasya	1	
Удалены задачи пользователя vasya в crontab	1	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:

Процесс kswapd должен быть запущен от пользователя root, а не vasya. Это сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. К тому же, настоящему kswapd не нужно ничего делать, так как swap в данный момент пуст, а свободной памяти хватает. Полностью загруженный процессор (2 ядра из 2 имеющихся) наводит на мысль, что это – майнер.Найдём, что это за исполняемый файл (ls -al */proc/1234/executable),* убьём процесс (kill -9 1234), переименуем и переместим

вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod. Заблокируем скомпрометированному пользователю vasya вход по паролю (passwd -L vasya), переименуем его авторизованные ключи (cp -p */home/vasya/.ssh/authorized_keys /tmp/vasya_kswapd_keys, rm /home/vasya/.ssh/authorized_keys),* просмотрим, а затем удалим его таблицу автоматически запускаемых задач (crontab -l -u vasya, crontab -r -u vasya).Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим мандатный контроль доступа (возможность AstraLinux) и режим безопасных вычислений (возможность Эльбрус).

ЗАДАЧА 6.

Петя проводит открытую олимпиаду по программированию bricscode. Открыв доступ к IP сервера, он заметил, что страничка открывается только у трети пользователей.

Петя стал исследовать:dig contest.bricscode.su

```
; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>>  contest.bricscode.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19089
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; contest.bricscode.su.                IN      A

;; ANSWER SECTION:
contest.bricscode.su.        201     IN      A       6.255.255.242
contest.bricscode.su.        201     IN      A       75.88.55.242
contest.bricscode.su.        201     IN      A       39.88.44.242
```

Задание:

Определите причину произошедшего. Что необходимо предпринять для того, чтобы страничка Пети стала доступна всем участникам конкурса?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определена причина произошедшего	**5**
Предложена верная рекомендация	**5**
ИТОГО	**10**

Ответ:

1. У сервера заданы 3 сетевых адреса. Логично предположить, что, если страница открывается в 1/3 случаев, то это означает, что только по одному из сетевых адресов возможно обращение к сайту.
2. Необходимо диагностировать причину блокировки двух недоступных из сети интерфейсов и дать доступ к ним.

ВАРИАНТ 25

ЗАДАЧА 4.

Какая уязвимость позволяет атакующему выдать себя за другого пользователя? Ответ можно дать на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть уязвимости аутентификации, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: уязвимость аутентификации / Authentication Failures или ответ, указывающий на уязвимость, связанную с компрометацией сессии (например, «перехват сессии», «угон сессии», «session fixation», «отсутствие шифрования сессии»	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «подбор пароля» или «маскарад» без указания на детализацию атаки	**0**

Ответ:
уязвимость аутентификации / Authentication Failures или ответ, указывающий на уязвимость, связанную с компрометацией сессии (например, «перехват сессии», «угон сессии», «session fixation», «отсутствие шифрования сессии»).

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами стал работать нестабильно.

Команда netstat вывела: netstat -lnptux | head

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599       0.0.0.0:*           LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определяет, что kswapd не должен слушать сеть, это указывает на подделку	1	

Учащийся определяет, что процесс kswapd запускается одним из первых и не может иметь такой большой PID	1	
Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	2	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	2	
У вредоносного исполняемого файла удалены права на исполнение	2	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:
Процесс kswapd должен быть одним из первых. Большой PID 12345 сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. Также процесс слушает сетевые соединения (получает команды извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим SELinux.

ЗАДАЧА 6.
Андрей проводит открытую олимпиаду по программированию sngcode. Открыв доступ к IP сервера, он заметил, что страничка открывается только у четверти пользователей.
Андрей стал исследовать:dig contest.sngcode.su

```
; <<>> DiG 9.11.3-1ubuntu1.18-Ubuntu <<>>  contest.sngcode.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19089
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
; contest.sngcode.su.                IN      A

;; ANSWER SECTION:
```

contest.sngcode.su.	201	IN	A	6.255.255.242
contest.sngcode.su.	201	IN	A	75.88.55.242
contest.sngcode.su.	201	IN	A	39.88.44.242
contest.sngcode.su.	201	IN	A	12.88.44.242

Задание:

Определите причину произошедшего. Что необходимо предпринять?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определена причина произошедшего	**5**
Предложена верная рекомендация	**5**
ИТОГО	**10**

Ответ:

1. У сервера заданы 4 сетевых адреса. Логично предположить, что, если страница открывается в ¼ случаев, то это означает, что только по одному из сетевых адресов возможно обращение к сайту.
2. Необходимо диагностировать причину блокировки трёх недоступных из сети интерфейсов и дать доступ к ним.

ВАРИАНТ 26

ЗАДАЧА 4.

Какая уязвимость позволяет атакующему получить более высокий уровень доступа в системе или совершать операции, для которых у него не хватает прав? Ответ можно дать на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть уязвимости повышение уровня доступа, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: это процесс, при котором злоумышленник получает неавторизованный доступ к повышенным правам (привилегиям) сверх тех, которые изначально были присвоены пользователю, учётной записи или машине	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «взлом доступа» или «угон учетки» без указания на детализацию атаки	**0**

Ответ:
повышение уровня доступа/ Broken Access Control / Privilege Escalalation.

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами на OpenSuSE стал работать нестабильно.
Команда netstat вывела:netstat -lnptux | head

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599        0.0.0.0:*         LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определяет, что kswapd не должен слушать сеть, это указывает на подделку	1	
Учащийся определяет, что процесс kswapd запускается одним из первых и не может иметь такой большой PID	1	

Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	2	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	2	
У вредоносного исполняемого файла удалены права на исполнение	2	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:
Процесс kswapd должен быть одним из первых. Большой PID 12345 сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. Также процесс слушает сетевые соединения (получает команды извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим AppArmour (так как дистрибутив OpenSuSE).

ЗАДАЧА 6.

Борис проводит открытую олимпиаду по программированию sngcode. Открыв доступ к IP сервера, он заметил, что страничка открывается только по http, но не https, хотя год назад открывалась.

Борис стал исследовать:dig TXT sngcode.su

```
; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> TXT sngcode.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52614
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;sngcode.su.                    IN      TXT

;; ANSWER SECTION:
sngcode.su              3600    IN      TXT     "MS=E8A668AA93DA3566440B5D30932F42417C65D045"
```

sngcode.su 3600 IN TXT "v=spf1 ip4:181.5.91.6 ip4:82.5.91.10 ip4:81.6.91.71 ip4:81.5.92.85 mx -all"
sngcode.su 3600 IN TXT "_globalsign-domain-verification=OlhVWRFDWokpD52Bn5EqccWsOm86dTkOfXb33hWlAQ"

Задание:

Определите причину произошедшего. Что необходимо предпринять?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определена причина произошедшего	**5**
Предложена верная рекомендация	**5**
ИТОГО	**10**

Ответ:

1. Истёк срок действия сертификата. 2. Нужно обратиться к поставщику сертификата — globalsign — для пролонгации срока действия сертификата.

ВАРИАНТ 27

ЗАДАЧА 4.

Какой тип уязвимости чаще всего приводит к раскрытию зашифрованных данных из-за ошибок в реализации шифрования? Ответ можно дать на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть уязвимостей шифрования, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: уязвимость шифрования / Cryptographic Failures / использование устаревших алгоритмов (DES, RC4), хранение ключей в открытом виде, отсутствие шифрования при передаче данных, утечка ключей и т.п.	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «реализация хеширования» или «кодирование» без указания на недостатки того или иного метода	**0**

Ответ:
уязвимость шифрования / Cryptographic Failures / использование устаревших алгоритмов (DES, RC4), хранение ключей в открытом виде, отсутствие шифрования при передаче данных, утечка ключей и т.п.

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами на AstraLinux стал работать нестабильно.
Команда netstat вывела:netstat -lnptux | head

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address  Foreign Address   State       PID/Program name
tcp   0    0 0.0.0.1:41599        0.0.0.0:*         LISTEN      12345/kswapd
```

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся определяет, что kswapd не должен слушать сеть, это указывает на подделку	1	

Учащийся определяет, что процесс kswapd запускается одним из первых и не может иметь такой большой PID	1	
Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убит процесс	2	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	2	
У вредоносного исполняемого файла удалены права на исполнение	2	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:
Процесс kswapd должен быть одним из первых. Большой PID 12345 сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. Также процесс слушает сетевые соединения (получает команды извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим мандатный контроль доступа.

ЗАДАЧА 6.
Владимир проводит открытую олимпиаду по программированию bricscode. Он заметил, что письма регистрации не доходят до ящиков на mail.ru.

Владимир стал исследовать:dig TXT bricscode.su

```
; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> TXT bricscode.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52614
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;bricscode.su.                  IN      TXT

;; ANSWER SECTION:
```

bricscode.su 3600 IN TXT
"MS=E8A668AA93DA3566440B5D30932F42417C65D045"
bricscode.su 3600 IN TXT "maelru-verification: 3636e40fa09e95c6"
bricscode.su 3600 IN TXT "e-maelru-verification: 3636e40fa09e95c6"

Задание:

Какая из настроек сервера указана неправильно? Как исправить ошибку? Определите причину произошедшего. Что необходимо предпринять?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Верно определена причина произошедшего	**5**
Предложена верная рекомендация	**5**
ИТОГО	**10**

Ответ:

1. Опечатка в mailru-verification. Добавлена лишняя строка, надо убрать bricscode.su 3600 IN TXT "e-maelru-verification: 3636e40fa09e95c6"2. Исправить опечатку в TXT секции.

ВАРИАНТ 28

ЗАДАЧА 4.

Как называется уязвимость во взаимодействии разных компонентов одного сайта/ приложения? Допускается ответ на русском или английском языках.

Критерии оценивания:

Максимальное количество баллов за задание – 5.

Учащийся дал точный и корректный ответ, отражающий суть ошибки интеграции, без орфографических ошибок. Допустимы верхний и нижний регистр, а также разные формулировки при условии, что смысл соответствует следующему: software and Data Integrity Failures/ ошибка интеграции софта/данных	**5**
Ответ близкий по смыслу, но частично некорректный; допущена незначительная ошибка	**3**
Ответ неправильный, либо отсутствует.Общие фразы вроде «сбой» или «ошибка» без указания на механизм появления недостатка	**0**

Ответ:
Software and Data Integrity Failures/ ошибка интеграции софта/данных / Нарушение целостности программного обеспечения и данных.

ЗАДАЧА 5.

В организации виртуальный сервер с 32 ядрами на процессоре Эльбрус стал работать нестабильно.

Команда netstat вывела:netstat -lnptux | head

Active Internet connections (only servers)

Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name

tcp 0 0 0.0.0.1:41599 0.0.0.0:* LISTEN 12345/kswapd

Задание:

Определите, что произошло с сервером. Укажите, что вызвало Ваши подозрения. Какие меры нужно предпринять для ликвидации проблемы? Какие меры нужно предпринять для предупреждения её возникновения в дальнейшем?

Критерии оценивания:

Максимальное количество баллов за задание – 15.

Расследование		**3**
Учащийся правильно определяет, что kswapd не должен слушать сеть, это указывает на подделку	1	
Учащийся определяет, что процесс kswapd запускается одним из первых и не может иметь такой большой PID	1	

Учащийся определяет, что процесс, активно использующий CPU и слушающий команды из сети, может быть майнером	1	
Меры по ликвидации проблемы		**8**
Убить процесс	2	
Вредоносный исполняемый файл найден и переименован для дальнейшего анализа	2	
У вредоносного исполняемого файла удалены права на исполнение	2	
Проверены задачи других пользователей	1	
Скомпрометированная система восстановлена из резервной копии	1	
Меры по предотвращению проблемы		**4**
Разрешён вход по ssh только по ключам	1	
Вход по ssh разрешён только из рабочей сети (или VPN в неё)	1	
Сервисы помещены в контейнеры с ограничением ресурсов	1	
У пользователей ограничены ресурсы	1	
	ИТОГО	**15**

Ответ:
Процесс kswapd должен быть одним из первых. Большой PID 12345 сразу наводит на подозрения, что это – вредоносный код, а не настоящий kswapd. Также процесс слушает сетевые соединения (получает команды извне).Найдём, что это за исполняемый файл (ls -al */proc/12345/executable),* убьём процесс (kill -9 12345), переименуем и переместим вредоносный файл для дальнейшего анализа и запретим его исполнение командой chmod.Для предотвращения инцидентов разрешим вход только по ключам и только из рабочей сети (или из VPN в неё). По возможности восстановим систему из бэкапа, дата которого раньше времени модификации вредоносного файла и authorzed_keys. Задачи отправим в контейнеры с ограничением ресурсов, также настроим с помощью ulimit ограничения отдельным пользователям. Обновим систему, включим режим безопасных вычислений (так как у нас процессор Эльбрус).

ЗАДАЧА 6.
Даниил проводит открытую олимпиаду по программированию bricscode. Он заметил, что письма регистрации не доходят до пользователей.

Даниил стал исследовать:dig TXT bricscode.su

```
; <<>> DiG 9.11.3-1ubuntu1.9-Ubuntu <<>> TXT bricscode.su
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 52614
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;bricscode.su.                  IN      TXT

;; ANSWER SECTION:
bricscode.su            3600    IN      TXT     "v=spf1 ip4:1815.91.6 ip4:825.91.10 ip4:81.6.91.71
```

ip4:81.5.92.85 mx -all"

Задание:

Определите причину произошедшего. Что необходимо предпринять?

Критерии оценивания:

Максимальное количество баллов за задание – 10.

Участник обратил внимание на SPF-секцию	**5**
Участник обратил внимание на IP-адреса с пропущенной точкой	**5**
ИТОГО	**10**

Ответ:

1. С какого адреса приходит легальная почта, указано в SPF секции "v=spf1 ip4:1815.91.6 ip4:825.91.10 ip4:81.6.91.71 ip4:81.5.92.85 mx -all".
2. IP адреса 1815.91.6 и 825.91.10 не может содержать октеты 1815 или 825. В этих адресах пропущена точка между первым и вторым октетом.