**Легенда**

Злоумышленник с помощью цепочки атак получил доступ к инфраструктуре предприятия, связанного с электроснабжением города. В результате большинство компьютеров было захвачено, доступ к ним потерян, а кое-где даже зашифрованы данные. Захватив промышленный сегмент, злоумышленник распространил бот-зловред, в результате которого на подстанции происходят аварийные события и блокируется работа операторов.

**Задача**

**Вам необходимо:**

- Провести инвентаризацию хостов в 4 сетевых сегментах**1**: сегмент DMZ (10.x.2.0/24), сегмент SERVERS (10.x.3.0/24), сегмент OFFICE (10.x.4.0/24) и сегмент АСУ ТП (10.x.239.0/24, 10.x.240.0/24)**2**.

- Расследовать цепочку атак злоумышленника, используя журналы безопасности и логи средств защиты.

- Вернуть контроль над захваченными компьютерами, восстановив легитимный доступ.

- Найти и расшифровать ценные файлы.

- Остановить распространение бота-зловреда во всей инфраструктуре, а также понять, что он делает.

1. В каждом сегменте сети машины с адресами .1 .2. .3 .4 в четвертом октете не участвуют в задаче.
2. В вашей инфраструктуре в IP адрес вместо «X» необходимо подставить второй октет ip адреса машины kali linux.