Задание

Фабула. В сети обнаружено неизвестное устройство:

- В системе контроля доступа появилось неизвестное устройство с MAC-адресом 00:1A:3F:4B:66:6D

Устройство подключилось к Wi-Fi и пытается сканировать сетевые папки.

Гипотезы

Ключевые детали:
1. В сети появилось неизвестное устройство, которое подключилось к сети через Wi-Fi.
2. На данном устройстве запущено некоторое ПО (не обязательно вредоносное - это может быть, например, тот же nmap), которое сканирует сетевые папки.
3. Мы не знаем, через конкретно какую точку доступа подключилось данное неизвестное устройство и к какой именно сети подключилось (к гостевой или нет)?
4. Мы также не знаем, была ли зафиксирована какая-либо еще активность с данного устройства.

Попробуем выдвинуть несколько гипотез:
1. Данное устройство было использовано отделом ИБ для тестирования существующей инфраструктуры на возможность проникновения.
2. Данное устройство было подключено кем то из системных администраторов для выполнения своих обязанностей, но информацию о нем не успели/забыли внести в систему контроля доступом. Сканирование сетевых папок - это одна из рабочих активностей (например, в целях проведения инвентаризации) сотрудника, которому принадлежит устройство.
3. Данное устройство является личным устройством одного из сотрудников, которое он принес и подключил к корпоративной сети для совершения некоторых противоправных действий (внутренний нарушитель). Попытка сканирования сетевых папок - это как раз начало таких противоправных действий (разведка).
4. Данное устройство принадлежит лицу, не являющемуся сотрудником (внешний нарушитель), которое подключилось либо к гостевой Wi-Fi сети (если у ней нет пароля или есть известный пароль), либо к основной Wi-Fi сети (с помощью подбора/взлома пароля) для совершения некоторых противоправных действий. Попытка сканирования сетевых папок - это как раз начало таких противоправных действий (разведка).

Способы проверки гипотез:
1. Обратиться в отдел ИБ по поводу проведения ими тестирования существующей инфраструктуры на возможность проникновения. Это даст нам понимание, что данная активность в сети является законной и по этому поводу не следует беспокоиться.
2. Обратиться в отдел ИТ (к системным администраторам) с вопросом о подключении ими нового устройства. Это даст нам понимание, что появление нового устройства в Wi-Fi сети и его активность являются законными.
3. Локализовать точку подключения неизвестного устройства и попытаться найти его физически. В случае удачи - снять с него снять образы памяти и диска. В случае неудачи - заблокировать его, а также запретить возможность подключения к не гостевой сети Wi-Fi неизвестных устройств. Это даст нам возможность в лучшем

случае информацию о намерениях и используемых средствах, а в худшем случае - устройство, с которого начинается потенциальная атака будет заблокировано.
4. Локализовать точку подключения неизвестного устройства и попытаться найти его физически. В случае удачи будет известна личность атакующего (внешнего нарушителя) - эту информацию можно будет передать правоохранительным органам. В случае неудачи - заблокировать его. Также, если злоумышленник подключался к основной Wi-Fi сети (с помощью подбора/взлома пароля), то необходимо запретить возможность подключения к не гостевой сети Wi-Fi неизвестных устройств, а также поменять пароль на подключение на более стойкий (т.к. существующий пароль уже не надежен). Это даст нам в лучшем случае информацию о злоумышленнике (например, его фотографию), а в худшем случае - устройство, с которого начинается потенциальная атака будет заблокировано.