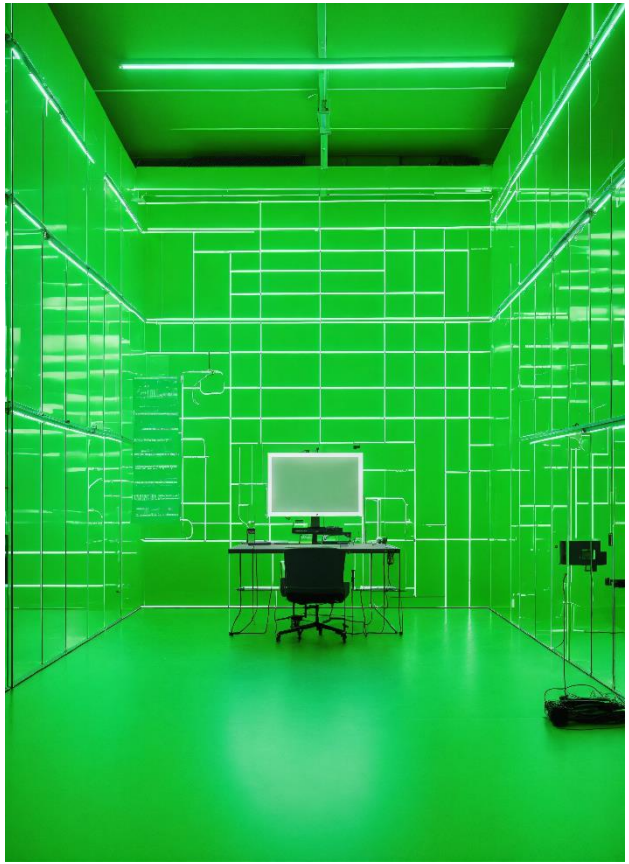
АВТОМАТИЗИРОВАННОЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ: КОМУ? КОГДА? ЗАЧЕМ?

Владимир Соловьев
Руководитель группы, Группа внедрения систем защиты от атак
АО «ДиалогНаука»

ДиалогНаука

О компании

- Создана в 1992 году СП «Диалог» и Вычислительным центром РАН
- Первые продукты – ревизор ADinf, антивирусы Aidstest и Dr. WEB
- На сегодняшний день «ДиалогНаука» является одной из ведущих российских компаний, специализирующихся в области информационной безопасности



Агенда

- История появления автоматизированного пентеста
- Рутина как проблема
- Пентестер vs. ПО
- Архитектура, принцип работы
- Результаты запуска, опыт
- Текущие векторы проникновения и как их закрыть
- Текущие игроки на мировом рынке и в РФ

История появления автоматизированного пентеста

- Скрипты/руки
- VS (Vulnerability Scanner)
- BAS (Breach and Attack Simulation)
- CEMP (Cyber Exposure Management Platform)

История появления автоматизированного пентеста

- Скрипты/руки
- VS (Vulnerability Scanner)
- BAS (Breach and Attack Simulation)
- CEMP (Cyber Exposure Management Platform)

- APT (Automated Penetration Testing)

История появления автоматизированного пентеста

- Скрипты/руки
- VS (Vulnerability Scanner)
- BAS (Breach and Attack Simulation)
- CEMP (Cyber Exposure Management Platform)

- APT (Automated Penetration Testing)
- APT + BAS

*Минутка сравнения APT и BAS

Критерий	Automated Penetration Testing	Breach and Attack Simulation
Цель	Автоматизация процесса тестирования на проникновение	Моделирование атак для оценки защиты и реагирования
Методы	Использование сканеров уязвимостей и эксплойтов	Симуляция реальных атак с использованием сценариев
Частота использования	Регулярные тесты для постоянной оценки безопасности	Регулярные тесты для постоянной оценки безопасности
Подход	Ориентирован на нахождение уязвимостей и узких мест в сети	Ориентирован на оценку готовности к атакам
Интерактивность	Обычно требуется ручное вмешательство	Может быть полностью автоматизирована

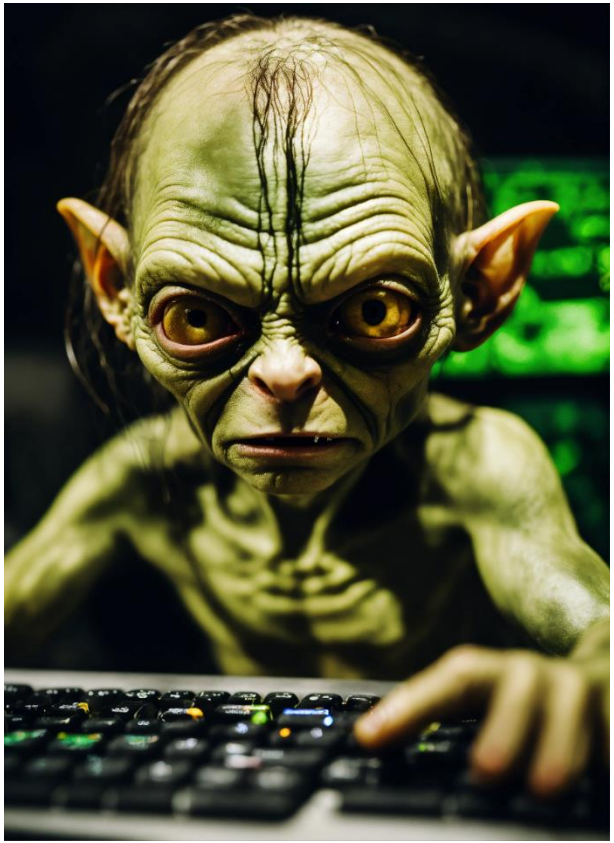
*Минутка сравнения APT и BAS

Критерий	Automated Penetration Testing	Breach and Attack Simulation
Выводы и отчеты	Подробные отчеты о найденных уязвимостях	Отчеты о том, как СЗИ справились с атаками
Аудит безопасности	Фокус на выявлении уязвимостей и узких мест сети	Фокус на оценке процессов реагирования на инциденты
Требования к знаниям	Знания о методах тестирования и эксплуатации	Знания о методах атак и защиты
Применение в реальном времени	Может использоваться для тестирования в реальном времени	Может использоваться для тестирования в реальном времени
Целевая аудитория	Тестировщики, специалисты по безопасности	Команды безопасности, ответственные за инциденты

Рутина как проблема

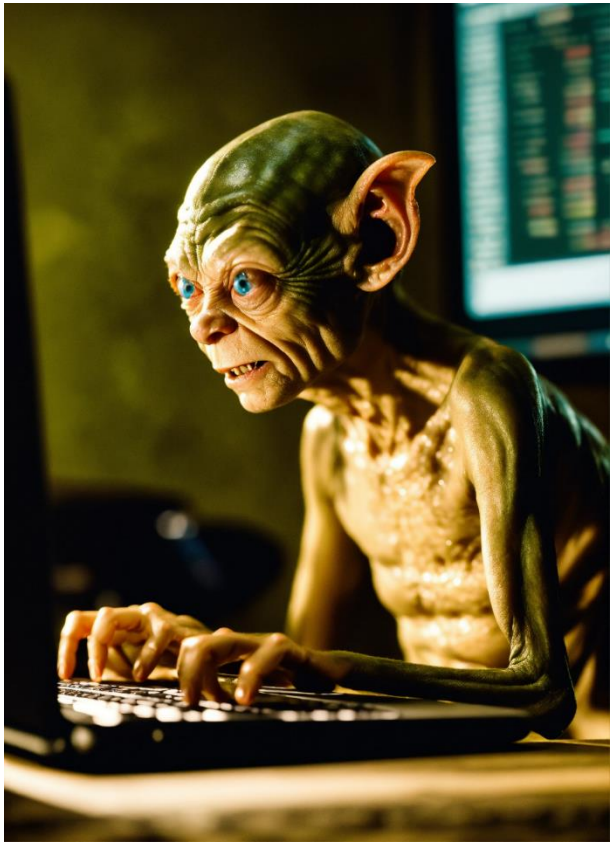
- **Сбор информации**

Рутина как проблема



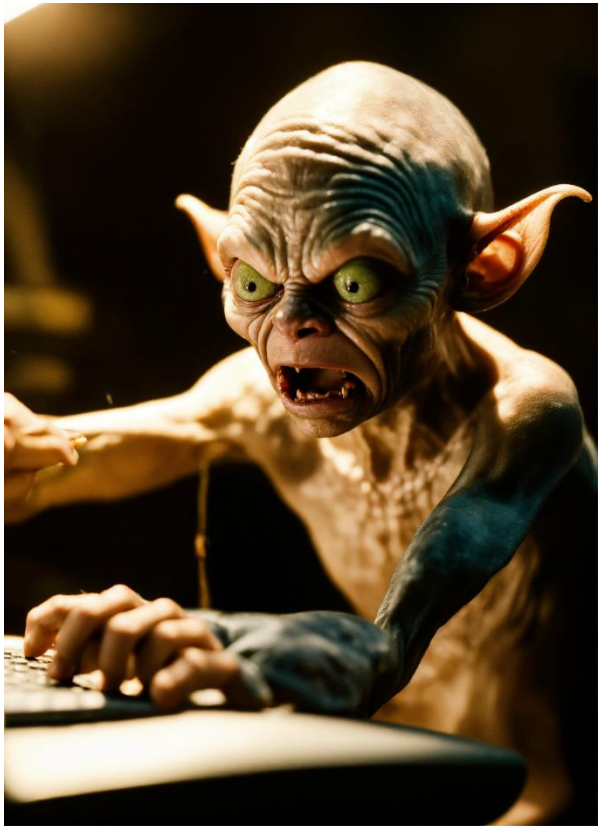
- Сбор информации

Рутина как проблема



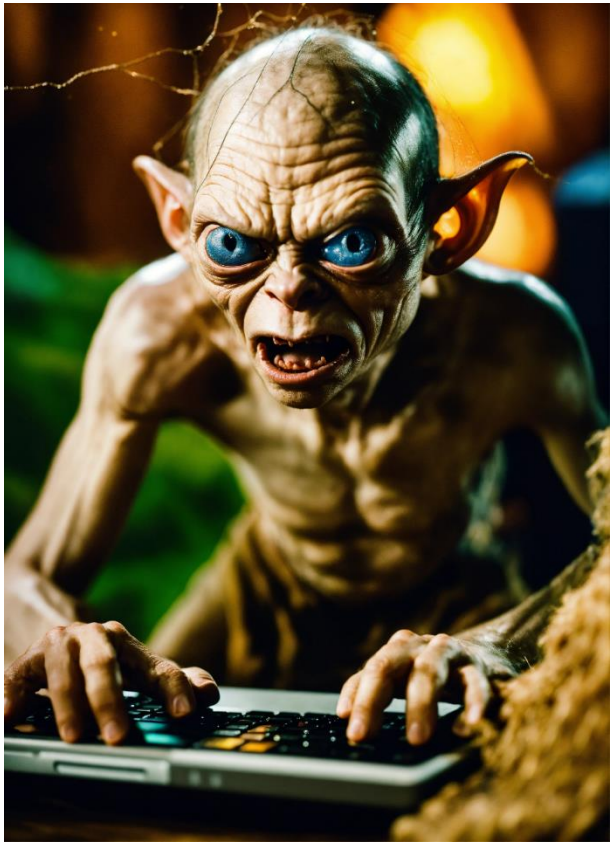
- Сбор информации
- **Анализ уязвимостей**

Рутина как проблема



- Сбор информации
- Анализ уязвимостей
- **Проверка на наличие уязвимостей**

Рутина как проблема

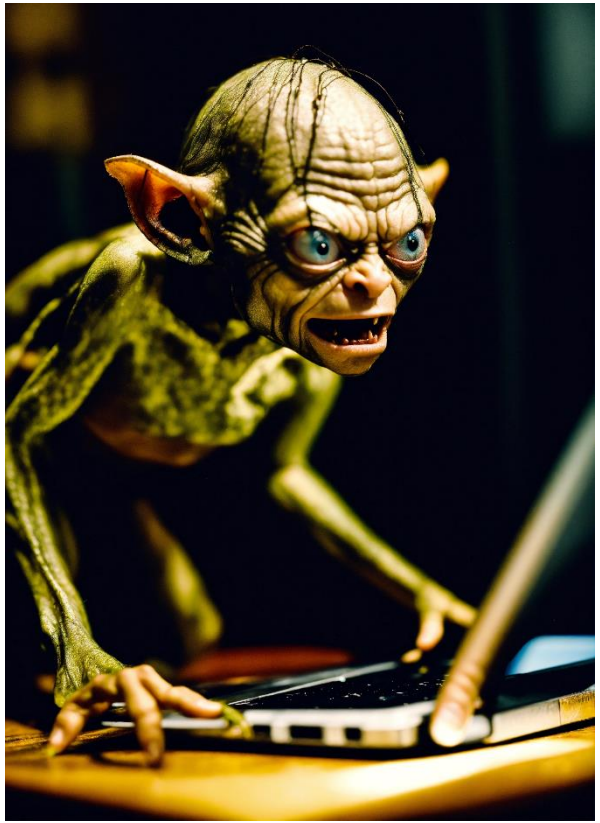


- Сбор информации
- Анализ уязвимостей
- Проверка на наличие уязвимостей
- **Эксплуатация уязвимостей**

Рутина, как проблема

- Сбор информации, разведка
- Анализ уязвимостей
- Проверка на наличие уязвимостей
- Эксплуатация уязвимостей
- **Документирование результатов**

Рутина, как проблема



- Сбор информации
- Анализ уязвимостей
- Проверка на наличие уязвимостей
- Эксплуатация уязвимостей
- Документирование результатов
- **И всё по новой…**

Пентестер vs. ПО

Заказчик: 800 АС ~ 30000 IP

Типовой проект: (разовый пентест в масштабе 3 АС ~ 100 IP) выполняется 1 человеком за месяц (20 рабочих дней):

- продолжительность - 4 недели
- трудоемкость - 20 чел./дней
- средняя скорость обхода сети - 3 АС/мес. (36 АС/год) – или с учетом отпусков 32 АС/год
- полный обход всего масштаба сети - 1 раз в 22 года
- совокупные трудозатраты за год - 1 FTE

Пентестер vs. ПО

Затраты на пентестера:

При ставке пентестера 200 т.р./мес. (*полная стоимость специалиста - 300т.р./мес., 3600т.р./год*):

- стоимость человеческого ресурса для ручного выполнения одного типового проекта на 3 АС – 300 т.р.
- трудозатраты для проверки всей сети (~800 АС) вручную за 1 год - 22 FTE (или с учетом отпусков 25,4 FTE)
- стоимость человеческого ресурса для ручной проверки всей сети за 1 год - 81 млн.р. (или с учетом отпусков 91,4 млн.р.)

Но это только 1 проход всех АС, а изменения в инфраструктуре наступают намного чаще. Если проходить 4 раза, то получается 360 млн.р. (или с учетом отпусков 403 млн.руб.)

Пентестер vs. ПО

Затраты на ПО:

- без перерывов на выходные дни
- средняя скорость обхода сети - 90 АС/мес. (~1000 АС/год)

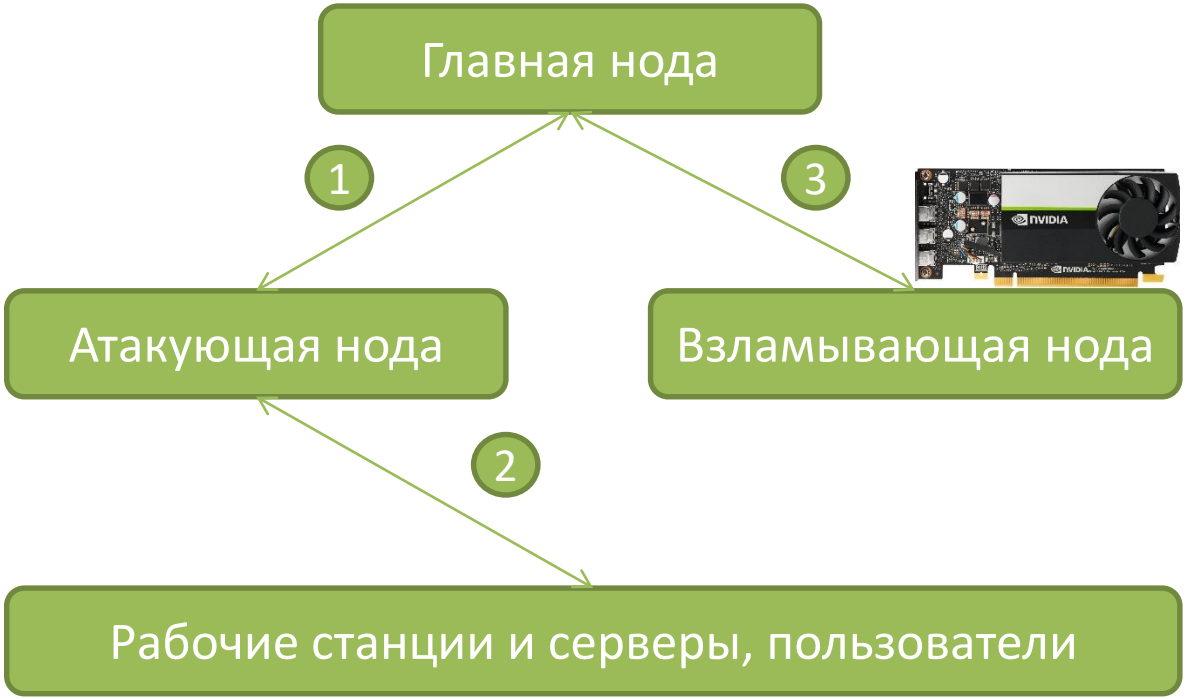
  // в 30 раз выше, чем пентестер
- стоимость человеческого ресурса для автоматического выполнения одного типового проекта на 3 АС - 3.6 т.р.
- стоимость человеческого ресурса для автоматической проверки всей сети (~800 АС) за 1 год - 750 т.р.
- стоимость подписки на *n* лет

*Минутка сравнения APT и Ручного пентеста

Критерий	Automated Penetration Testing	Ручной пентест
Частота использования	Непрерывно/По запросу	Ежегодно/Ежеквартально
Скорость	Минуты, Часы	Дни, Недели
Плотность тестирования	Максимальная	Частичная
Охват сети	Полное покрытие	Зависит от сроков работы и количества пентестеров
Подготовка к работам	Минимальная	Необходимо найти сильную команду, привлечение Заказчика
Конфиденциальность	Всё в периметре	Могут быть подрядные организации (небезопасно)
Актуальность	Постоянное обновление атакующих техник	Типовые сценарии устаревают

Пентестер vs. ПО

Архитектура, принцип работы



Результаты запуска, опыт

Входные параметры:

1 подсеть/24, контроллеры домена, шлюз, рабочие станции пользователей

Результаты запуска (длительность: ~4 дней):

- Уязвимостей: 733
  - Критических: 308
  - Высоких: 313
  - Средних: 32
  - Низких: 80
- Достижений: 9200
- Всего «живых» хостов в указанном диапазоне адресов: 68

Результаты запуска, опыт

- **Было захвачено:** 209 учетных записей (9 из которых привилегированные): 208 доменных пользователей, 1 локальный администратор
- **Подслушано в трафике:** 4 учетных записи, 2 из которых были использованы для relay-атаки
- **Взломано:** 72 пароля из 408, 22 стойких, 1 средний, 49 легких
- Горизонтальное передвижение на 30 АРМ и 5 серверов
- Полный доступ к 35 АРМ

Результаты запуска, опыт

- **Рекомендации к устранению:**
  1. Отключена подпись SMB-пакетов – требуется включить
  2. Службы LLMNR, NetBIOS-NS и mDNS включены – требуется выключить
  3. Антивирус позволил записать «зловредный» код в файловую систему АРМ – требуется обновление антивируса

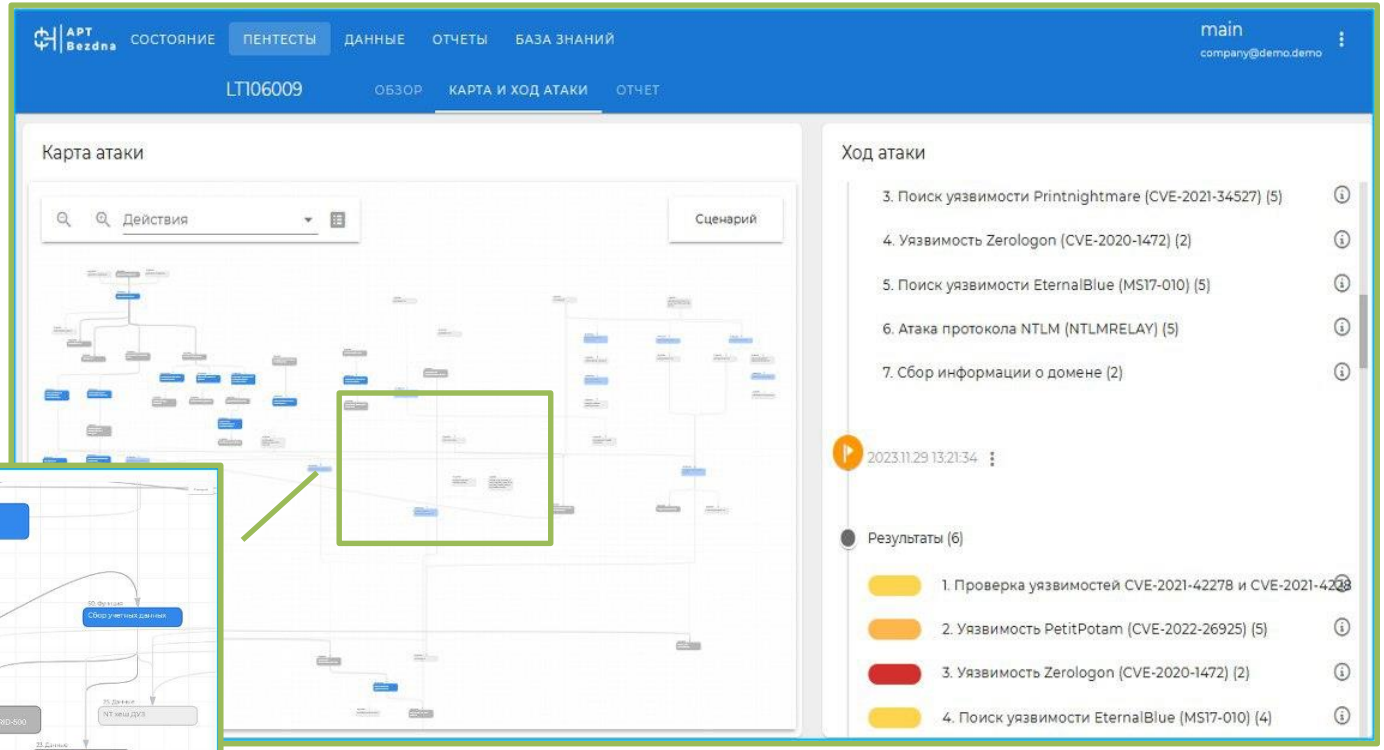
Результаты запуска, опыт

- **Полученные достижения:**
  - Завершена цепочка атак с использованием программ-вымогателей на хосте. Блокировки не было
  - Провалидированный хешированный пароль учетной записи администратора домена
  - Злоумышленник может извлечь хешированные пароли из памяти и использовать их для подключения к контроллеру домена или другим хостам, используя атакуемый метод pass-the-hash
  - Злоумышленник может найти на хосте конфиденциальную информацию и учетные данные, которые могут помочь в дальнейших атаках

Результаты запуска, опыт

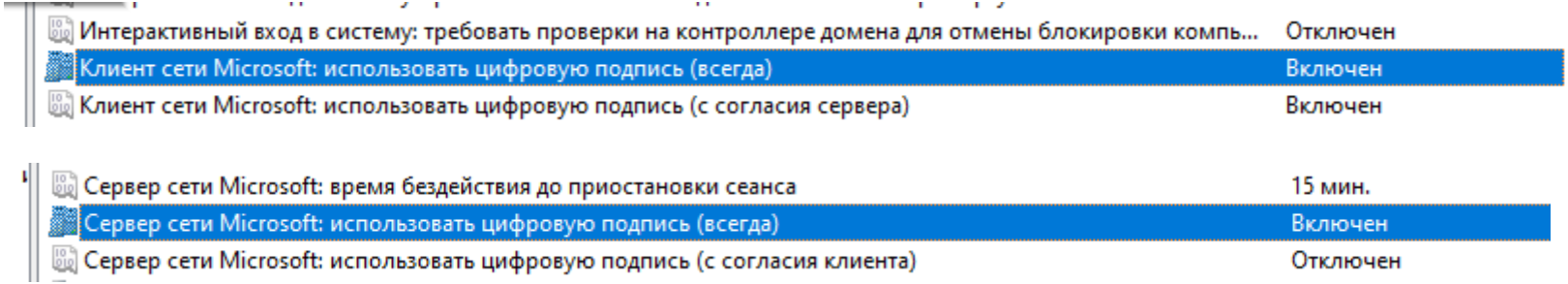
- **Полученные достижения:**
  - Открыт сеанс удаленного доступа
  - Получен пароль пользователя в открытом виде
  - Эмулированное удаление журнала событий Windows
  - Эмулированное отключение функций восстановления Windows
  - Эмулированное удаление AV/EDR
  - Эмулированное удаление теневых копий (shadow copy)

Результаты запуска, опыт



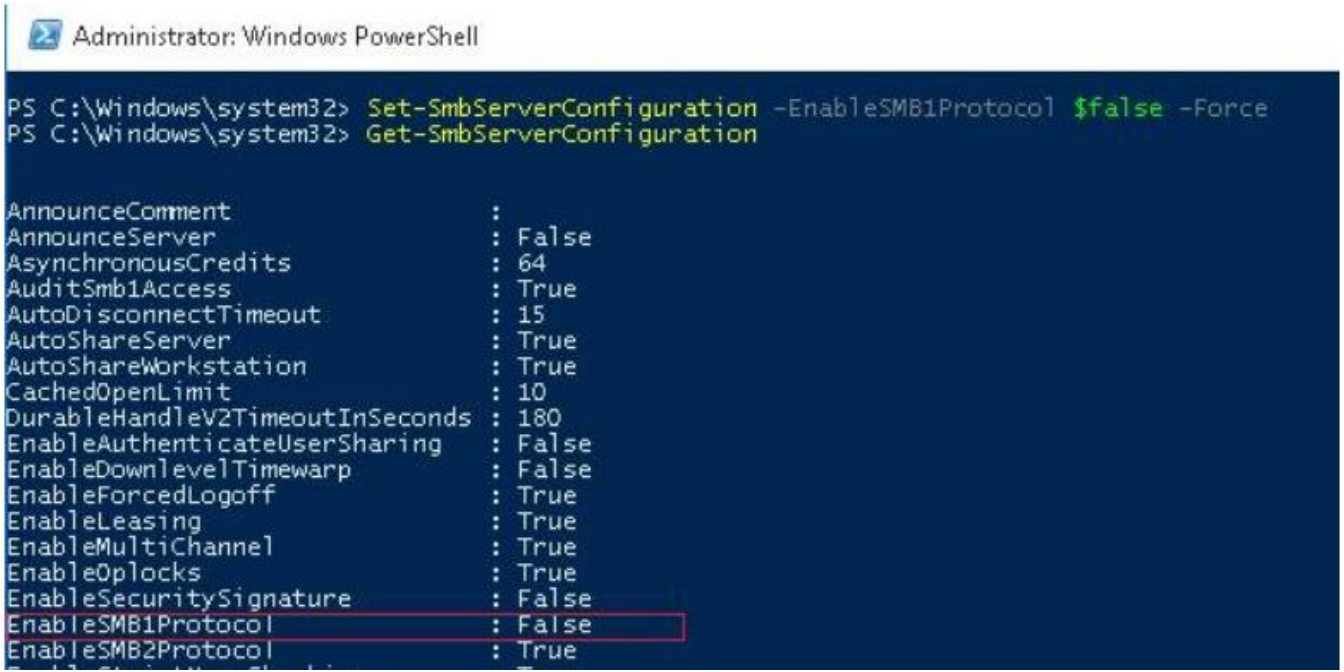
Текущие векторы проникновения и как их закрыть

- Подписывание протокола SMB (SMB Signing)



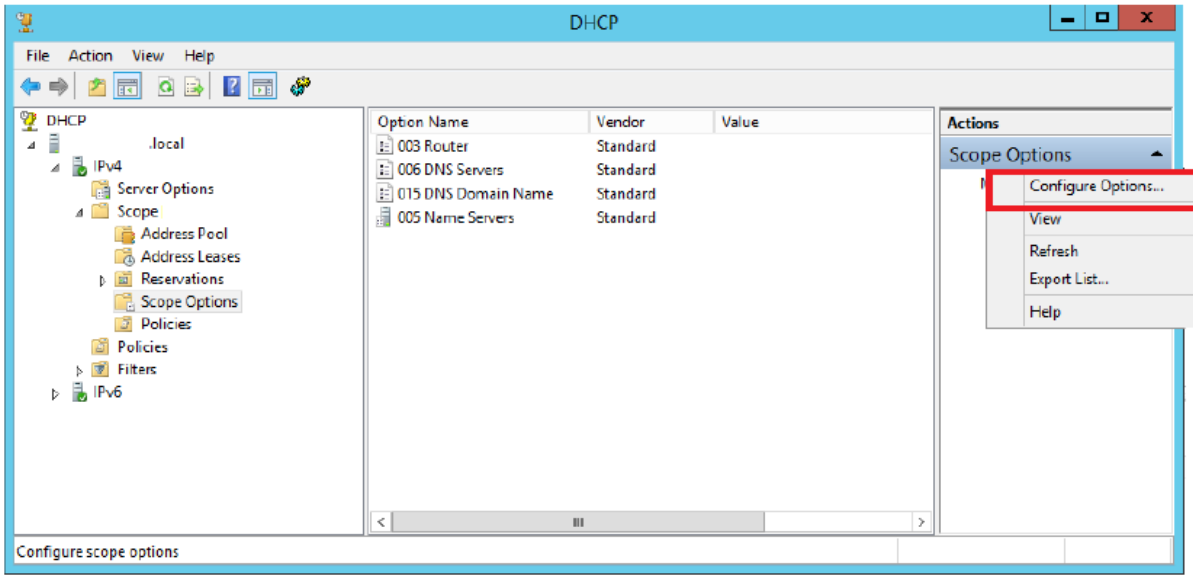
Текущие векторы проникновения и как их закрыть

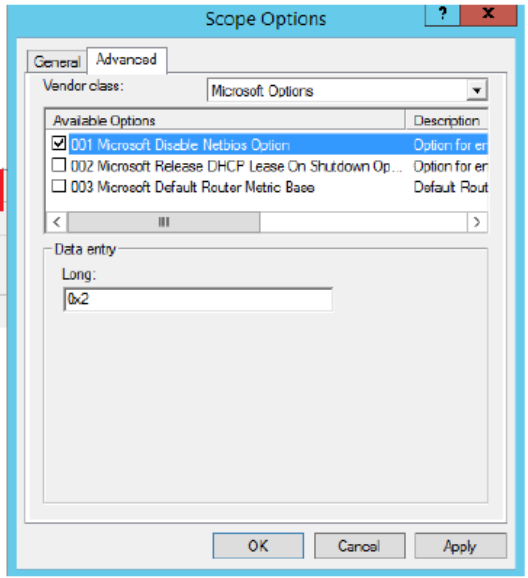
- Отключение старых версий протокола SMB (хотя бы v1, а так и v2)



Текущие векторы проникновения и как их закрыть

- Отключение протокола LLMNR и NBNS (WINS)





Текущие векторы проникновения и как их закрыть

- Списки доступа на уровне коммутатора или виртуального коммутатора, запрещающие сетевое взаимодействие между АРМ в одной подсети (например, пользовательской) - arp inspection + ACL на vlan. По желанию 802.1x

Текущие векторы проникновения и как их закрыть

- Слабые пароли/мисконфигурации (человеческий фактор)

Текущие игроки на мировом рынке и в РФ

В мире: 

- Pentera
- Схожие, но не APT:
  - CyBot
  - Core Security
  - Rapid7 Metasploit Pro
  - Prancer
  - Acunetix
  - CybSafe

В РФ: 

- CTRLHACK APT Bezdna
- KTSG Armug
- PT Dephaze

Вопросы

Спасибо за внимание