

# АВТОМАТИЗИРОВАННОЕ ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ: КОМУ? КОГДА? ЗАЧЕМ?

Владимир Соловьев

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

- ❖ 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



- ❖ История появления автоматизированного пентеста
- ❖ Рутинная работа 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

Изменение уровня риска в случае ежегодного пентеста



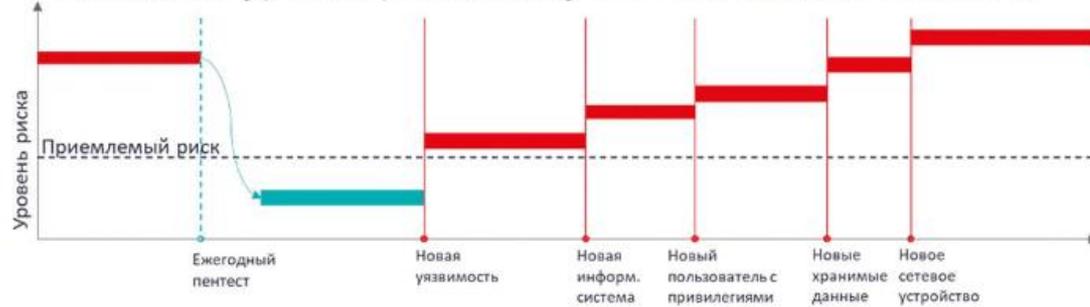
- ❖ Скрипты/руки
- ❖ VS (Vulnerability Scanner)
- ❖ BAS (Breach and Attack Simulation)
- ❖ CEMP (Cyber Exposure Management Platform)

Изменение уровня риска в случае ежегодного пентеста

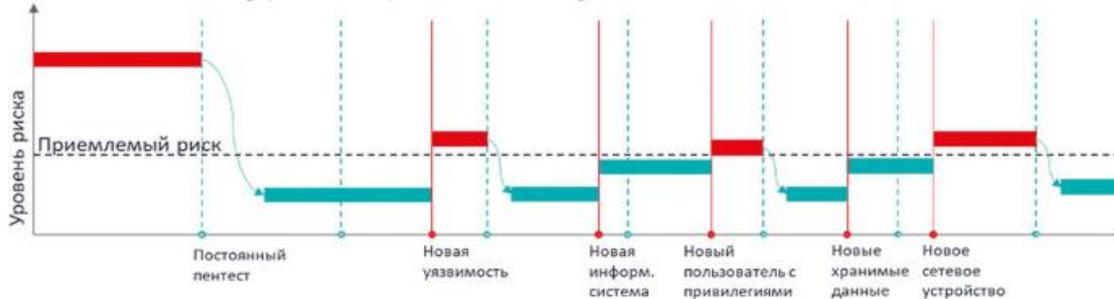


# История появления автоматизированного пентеста

Изменение уровня риска в случае ежегодного пентеста



Изменение уровня риска в случае постоянного пентеста



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

# История появления автоматизированного пентеста

Изменение уровня риска в случае ежегодного пентеста



Изменение уровня риска в случае постоянного пентеста



- Скрипты/руки
- VS (Vulnerability Scanner)
- BAS (Breach and Attack Simulation)
- CEMP (Cyber Exposure Management Platform)
- APT (Automated Penetration Testing)
- APT + BAS

## \*Минутка сравнения АРТ и ВАС

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

## \*Минутка сравнения АРТ и ВАС

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



**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

## 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.**)

## 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

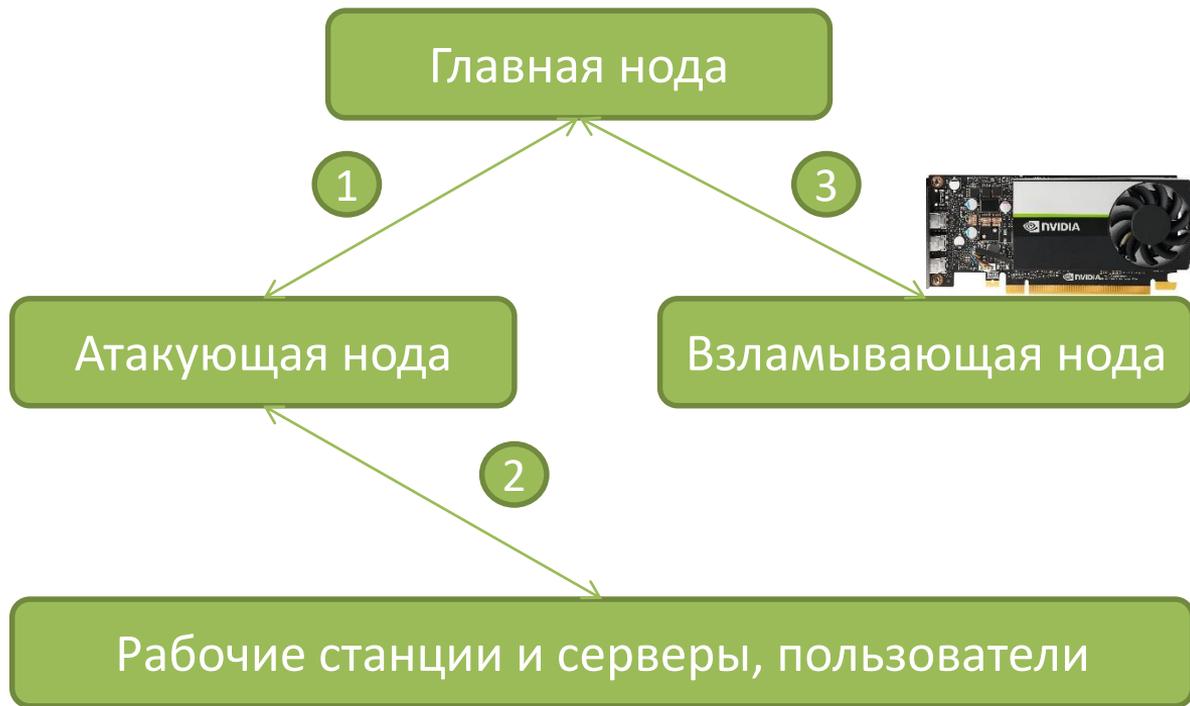
## \*Минутка сравнения АРТ и Ручного пентеста

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



## 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

- ❖ **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

## ❖ 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 APM – требуется обновление антивируса

## ❖ 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

## ❖ 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)

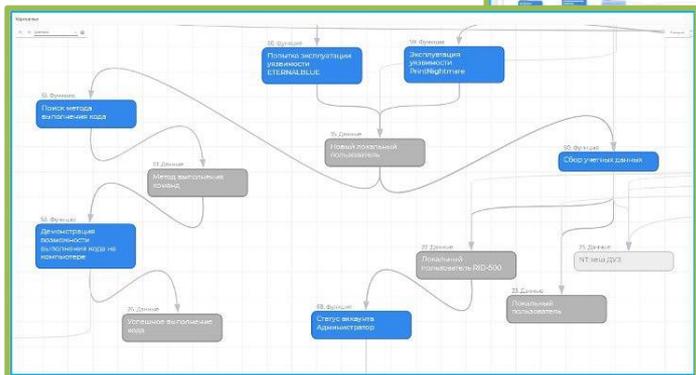
# Результаты запуска, опыт

The screenshot displays the APT Bezdna web interface. At the top, there is a navigation bar with tabs for 'СОСТОЯНИЕ', 'ПЕНТЕСТЫ', 'ДАННЫЕ', 'ОТЧЕТЫ', and 'БАЗА ЗНАНИЙ'. The current scenario is identified as 'LT06009'. Below the navigation, the 'Карта атаки' (Attack Map) section shows a complex flowchart of the attack process. A search bar labeled 'Действия' and a 'Сценарий' button are present. A green box highlights a specific part of the attack map. To the right, the 'Ход атаки' (Attack Progress) section lists the following steps:

3. Поиск уязвимости Printnightmare (CVE-2021-34527) (5)
4. Уязвимость Zerologon (CVE-2020-1472) (2)
5. Поиск уязвимости EternalBlue (MS17-010) (5)
6. Атака протокола NTLM (NTLMRELAY) (5)
7. Сбор информации о домене (2)

Below the list, there is a timestamp '2023.11.29 13:21:34' and a section for 'Результаты (6)' (Results (6)). The results are listed as follows:

1. Проверка уязвимостей CVE-2021-42278 и CVE-2021-42388
2. Уязвимость PetitPotam (CVE-2022-26925) (5)
3. Уязвимость Zerologon (CVE-2020-1472) (2)
4. Поиск уязвимости EternalBlue (MS17-010) (4)



# Текущие векторы проникновения и как их закрыть

## ❖ Подписывание протокола SMB (SMB Signing)

 Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компь...	Отключен
 Клиент сети Microsoft: использовать цифровую подпись (всегда)	Включен
 Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера)	Включен
 Сервер сети Microsoft: время бездействия до приостановки сеанса	15 мин.
 Сервер сети Microsoft: использовать цифровую подпись (всегда)	Включен
 Сервер сети Microsoft: использовать цифровую подпись (с согласия клиента)	Отключен

# Текущие векторы проникновения и как их закрыть

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

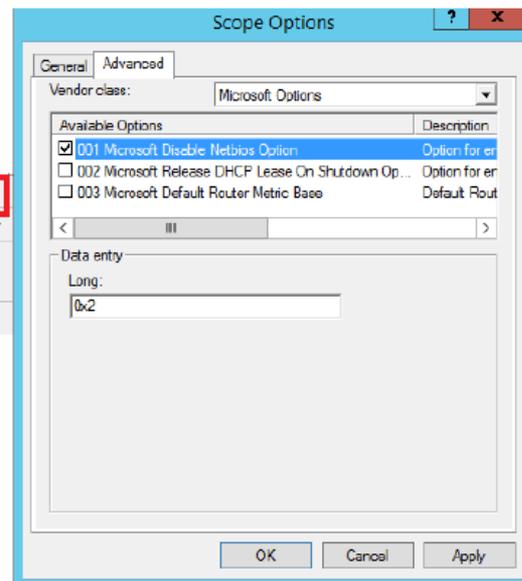
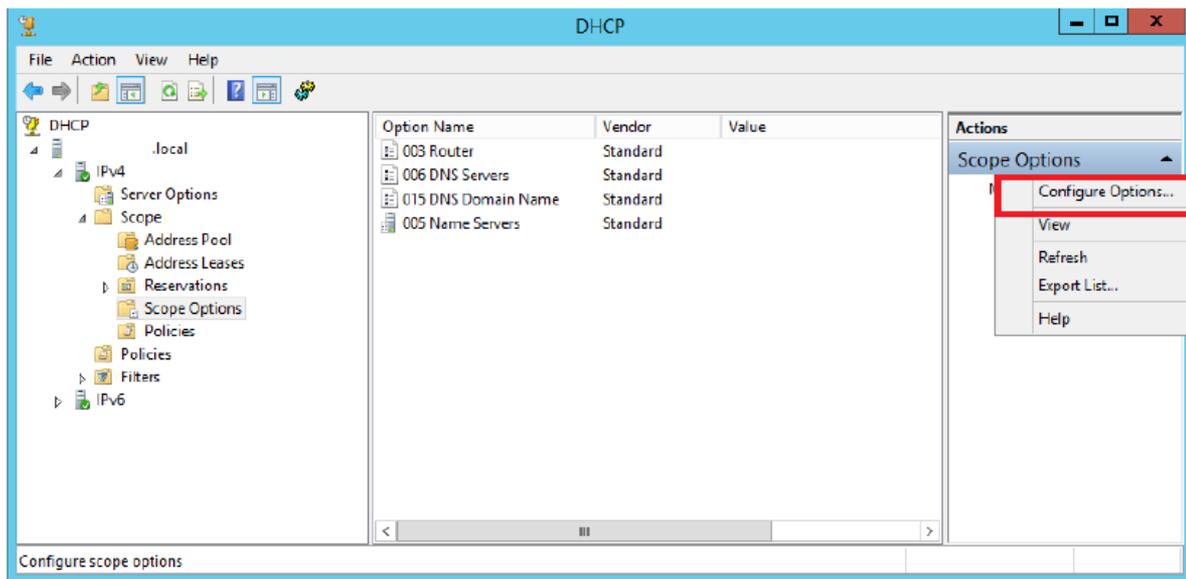
```
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-SmbServerConfiguration -EnableSMB1Protocol $false -Force
PS C:\Windows\system32> Get-SmbServerConfiguration

AnnounceComment           :
AnnounceServer             : False
AsynchronousCredits       : 64
AuditSmb1Access            : True
AutoDisconnectTimeout     : 15
AutoShareServer           : True
AutoShareWorkstation      : True
CachedOpenLimit           : 10
DurableHandleV2TimeoutInSeconds : 180
EnableAuthenticateUserSharing : False
EnableDownlevelTimewarp   : False
EnableForcedLogoff        : True
EnableLeasing              : True
EnableMultiChannel        : True
EnableOplocks              : True
EnableSecuritySignature    : False
EnableSMB1Protocol        : False
EnableSMB2Protocol        : True
```

# Текущие векторы проникновения и как их закрыть

## ❖ Отключение протокола LLMNR и NBNS (WINS)

Регрессирование основного DNS-суффикса	Не задана	Нет
Отключить многоадресное разрешение имен	Включена	Нет



# 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

Спасибо за внимание