CyberED

ПРАКТИЧЕСКИЕ ПРИЕМЫ КОМПРОМЕТАЦИИ ВНУТРЕННЕЙ ИНФРАСТРУКТУРЫ С МИНИМАЛЬНЫМИ ПРИВИЛЕГИЯМИ

[ЕВГЕНИЙ СТРОЕВ]

[СПИКЕР]

CyberED

EVGENY STROEV

- **Pentest**
  БОЛЬШИЕ И НЕ ОЧЕНЬ КОМПАНИИ, БАНКИ, ЗАВОДЫ.
- **Business Information Security**
  ИЗМЕНЕНИЕ ПРОЦЕССОВ, АНАЛИЗ РИСКОВ, ПРАКТИЧЕСКАЯ ИБ
- **Professional Consultation**
  КАРЬЕРНЫЕ КОНСУЛЬТАЦИИ, VIRTUAL-CISO, АНАЛИЗ ЗАЩИЩЕННОСТИ
- **Career**
  POSITIVE TECHNOLOGIES – RESEARCH & DEVELOPMENT
  ALFABANK – SECURITY OPERATION CENTER & RED TEAM
  TINKOFF – BUSINESS INFORMATION SECURITY OFFICER
  EXNESS – SECURITY BUSINESS ANALYST

pt

Tinkoff

Альфа-Банк

exness



CyberED

ЧТО МЫ БУДЕМ ДЕЛАТЬ?



А)

МЫ РАССМОТРИМ ПРОСТЫЕ, НО ЭФФЕКТИВНЫЕ МЕТОДЫ ПОЛУЧЕНИЯ ДОСТУПА К ВНУТРЕННЕЙ ИНФРАСТРУКТУРЕ В СРЕДЕ WINDOWS ACTIVE DIRECTORY

Б)

ЭТИ ПРИЕМЫ ОСОБЕННО ЭФФЕКТИВНЫ НА НАЧАЛЬНОМ ЭТАПЕ АНАЛИЗА ЗАЩИЩЕННОСТИ, КОГДА У АТАКУЮЩЕГО НЕТ ДОМЕННОЙ УЧЁТНОЙ ЗАПИСИ

CyberED

У САМУРАЯ НЕТ ЦЕЛИ, ЕСТЬ ТОЛЬКО ПУТЬ

01 Бесплатный курс приоткрывает “карту мира” - осознание возможностей и путей развития.

02 Вебинар показывает рабочие техники - понимание, как это выглядит на практике.

03 Программа нарабатывает навык - получение опыта, комплексных и системных знаний.

CyberED

ЧТО МЫ БУДЕМ ИСПОЛЬЗОВАТЬ ?

- **Поиск приоритетных целей для атак**
  - КОНТРОЛЛЕРЫ ДОМЕНА
  - NETWORK MAPPING
  - УСТАРЕВШИЕ ВЕРСИИ ОС
- **Эксплуатацию небезопасных настроек**
  - СЛАБАЯ ПАРОЛЬНАЯ ПОЛИТИКА
  - ПАРОЛИ ПО УМОЛЧАНИЮ
  - ОТСУТСТВИЕ КОНТРОЛЯ ДОСТУПА
- **Получение доступа к учетным записям**
  - ЛОКАЛЬНЫЕ УЗ
  - ПРИВИЛЕГИРОВАННЫЕ УЗ
  - ДОМЕННЫЕ УЗ
- **Сбор и анализ данных**
  - ОПРЕДЕЛЕНИЕ ВЕКТОРОВ АТАКИ
  - ПОИСК СЕКРЕТОВ

CyberED

ПЛАН ДЕЙСТВИЙ

01

Discovery

Domain Controllers
Network Mapping

02

Scanning

SNMP
SMB

03

Enumeration

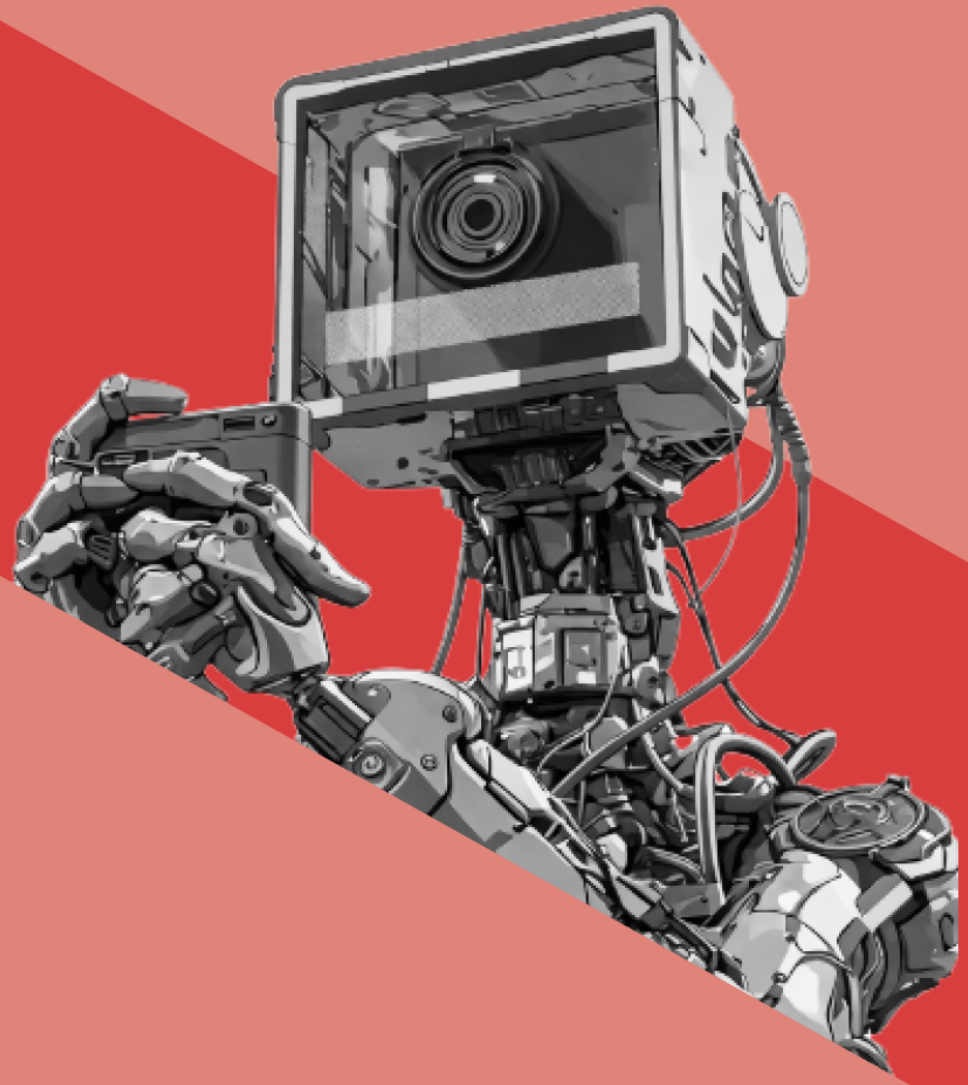
Shared folders
Accounts

04

Exploitation

Credential dumping
Password Spraying

DISCOVERY



CyberED

DISCOVERY

ОПРЕДЕЛЕНИЕ АДРЕСА КОНТРОЛЛЕРА ДОМЕНА (DC)

Это первый шаг для понимания структуры сети.
Контроллер домена управляет аутентификацией и является главной целью для сбора данных и дальнейших атак.

ИНСТРУМЕНТЫ

01  **NSLOOKUP**

02  **NMAP**

CyberED

NSLOOKUP

УТИЛИТА, ПРЕДОСТАВЛЯЮЩАЯ ПОЛЬЗОВАТЕЛЮ ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ ДЛЯ ОБРАЩЕНИЯ К СИСТЕМЕ DNS

Пример использования:

ЗАПРАШИВАЕТ У DNS-СЕРВЕРА ЗАПИСЬ ТИПА SRV (SERVICE RECORD), КОТОРАЯ ПОЗВОЛЯЕТ НАЙТИ IP-АДРЕСА ХОСТОВ, ПРЕДОСТАВЛЯЮЩИХ КОНКРЕТНУЮ СЛУЖБУ (НАПРИМЕР, LDAP ИЛИ KERBEROS) В ДОМЕНЕ

```
nslookup -type=srv _ldap._tcp.dc._msdcs.$FQDN_DOMAIN
nslookup -type=srv _kerberos._tcp.$FQDN_DOMAIN
```

CyberED

NMAP (NETWORK MAPPER)

УТИЛИТА С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ, ПРЕДНАЗНАЧЕННАЯ ДЛЯ БЫСТРОГО СКАНИРОВАНИЯ, ИССЛЕДОВАНИЯ СЕТЕЙ И АУДИТА БЕЗОПАСНОСТИ

Пример использования:

ОБНАРУЖЕНИЕ СЕРВЕРОВ DHCP В ЛОКАЛЬНОЙ СЕТИ И ИЗВЛЕЧЕНИЯ ИЗ НИХ СЕТЕВЫХ НАСТРОЕК

```
nmap --script broadcast-dhcp-discover
```

ПЕРЕЧИСЛЕНИЕ СЕРВИСНЫХ ЗАПИСЕЙ DNS (SRV) ДЛЯ ДОМЕНА.

Скрипт dns-srv-enum опрашивает DNS-сервер на наличие стандартных имен сервисных записей, которые Windows использует для работы домена. Вместо того чтобы вручную перебирать типы записей через nslookup, этот скрипт проверяет целый список известных префиксов за один раз.

```
nmap --script dns-srv-enum --script-argsdns-srv-enum.domain=$FQDN_DOMAIN
```

DISCOVERY

ПОСТРОЕНИЕ КАРТЫ СЕТИ

Позволяет атакующему обнаружить максимальное количество потенциальных машин для компрометации.

ИНСТРУМЕНТЫ

01 

IOXIDRESOLVER

CyberED

IOXIDRESOLVER

ИНСТРУМЕНТ ПОЗВОЛЯЕТ ПРОВЕСТИ МАССОВУЮ РАЗВЕДКУ ИНТЕРФЕЙСОВ (NETWORK MAPPING) БЕЗ АУТЕНТИФИКАЦИИ:

РАСКРЫТИЕ ВНУТРЕННИХ IP:

Даже если вы сканируете внешний адрес сервера (например, в DMZ), метод ServerAlive2 может вернуть список всех IPv4 и IPv6 адресов, привязанных к сетевым адаптерам хоста

ОБНАРУЖЕНИЕ СКРЫТЫХ ПОДСЕТЕЙ:

Вы можете узнать о существовании внутренних сетей (например, управления или бэкапа), которые невидны из вашей текущей позиции в сети

ПОСТРОЕНИЕ КАРТЫ СЕТИ:

Помогает обнаружить максимальное количество потенциальных машин для дальнейшей компрометации

IOXIDRESOLVER

ИНСТРУМЕНТ ПОЗВОЛЯЕТ ПРОВЕСТИ МАССОВУЮ РАЗВЕДКУ ИНТЕРФЕЙСОВ (NETWORK MAPPING) БЕЗ АУТЕНТИФИКАЦИИ:

Пример использования:

КОНВЕЙЕР ДЛЯ АВТОМАТИЗАЦИИ ПОИСКА СЕТЕВЫХ ИНТЕРФЕЙСОВ НА БОЛЬШОМ КОЛИЧЕСТВЕ ХОСТОВ.

Он объединяет чтение списка целей, передачу их в аргументы и выполнение специализированного Python-скрипта для эксплуатации протокола DCE-RPC.

```
cat ip-ips.txt | xargs -I IP python IOXIDResolver.py -t IP
```

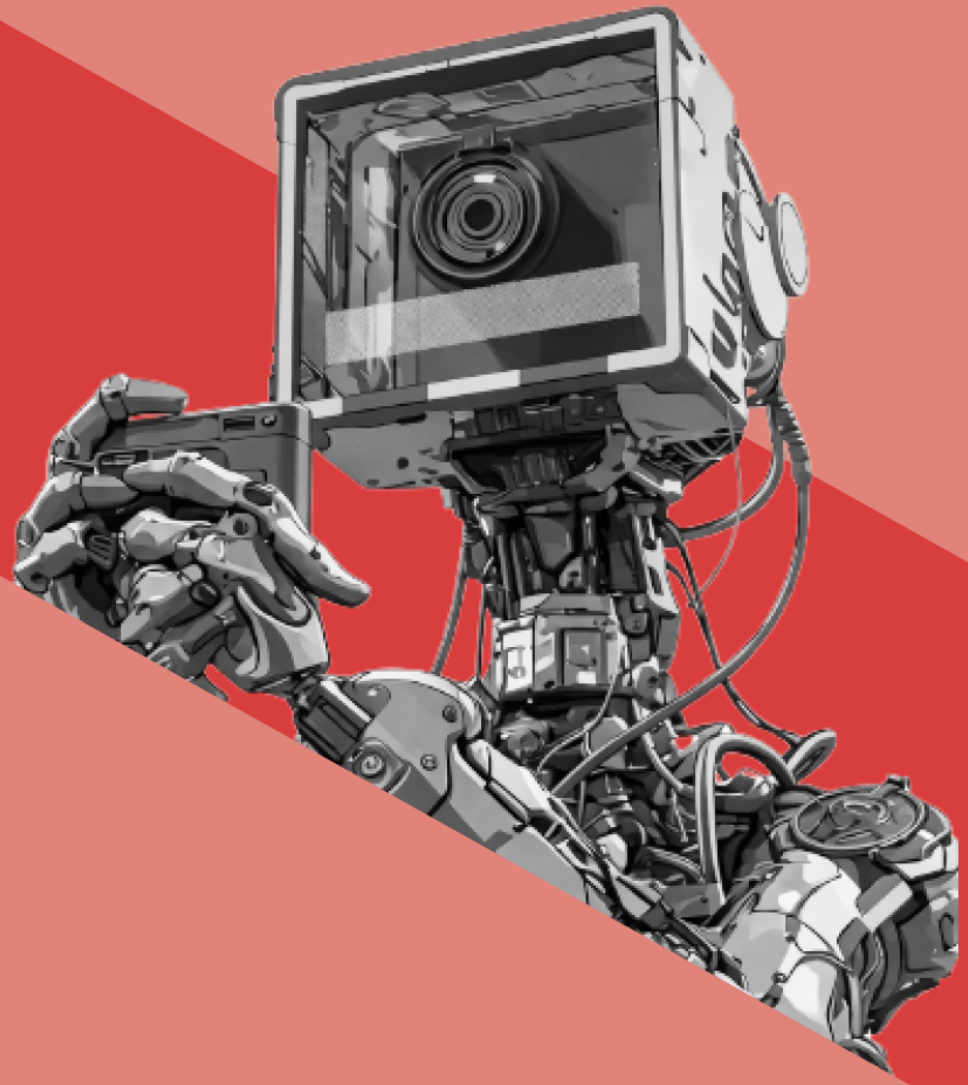
CyberED

КАК БЫВАЕТ В РЕАЛЬНОЙ ЖИЗНИ

Лабораторная среда как песочница, на практике атака складывается в цепочку из нескольких этапов

- Как получить доступ к обнаруженным сетям
- Как запустить инструмент без прав администратора
- Что делать, если на хосте нет Python

SCANNING



CyberED

SCANNING

ПОИСК ХОСТОВ С НЕБЕЗОПАСНЫМИ НАСТРОЙКАМИ ПРОТОКОЛОВ SNMP И SMB ПОЛУЧЕНИЕ ИНФОРМАЦИИ О ХОСТАХ:

- [smb] Версия операционной системы Windows
- [smb] Имя компьютера и домена
- [smb] Версия используемого протокола SMB (SMBv1 или SMBv2)
- [smb] Статус SMB Signing (цифровой подписи SMB)
- [smb] Наличие роли контроллера домена
- [snmp] Список пользователей (Users: 1.3.6.1.4.1.77.1.2.25)
- [snmp] Установленное ПО (Installed Software: 1.3.6.1.2.1.25.6.3.1.)
- [snmp] Список открытых портов (TCP Ports: 1.3.6.1.2.1.6.13.1.3)
- [snmp] Список запущенных процессов (Process: 1.3.6.1.2.1.25.4.2.1.2)

ИНСТРУМЕНТЫ

01  **ONESIXTYONE**

02  **NMAP**

ONESIXTYONE

ВЫСОКОПРОИЗВОДИТЕЛЬНЫЙ СКАНЕР ПРОТОКОЛА SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL), ПРЕДНАЗНАЧЕННЫЙ ДЛЯ БЫСТРОГО ПЕРЕБОРА ИМЕН СООБЩЕСТВ (COMMUNITY STRINGS). В ОТЛИЧИЕ ОТ МНОГИХ АНАЛОГОВ, ОН ИСПОЛЬЗУЕТ ЭФФЕКТИВНЫЙ МЕХАНИЗМ ОТПРАВКИ ПАКЕТОВ, ЧТО ПОЗВОЛЯЕТ СКАНИРОВАТЬ ЦЕЛЫЕ ПОДСЕТИ ЗА ОЧЕНЬ КОРОТКОЕ ВРЕМЯ.

Пример использования:

КОМАНДА ЗАПУСКАЕТ МАССОВЫЙ ПЕРЕБОР ПАРОЛЕЙ SNMP В УКАЗАННОМ ДИАПАЗОНЕ АДРЕСОВ

```
onesixtyone -c snmp_pass.txt ip/prefix -o output.txt
```

ИНСТРУМЕНТЫ

[SCANNING. SMB]

01 

NMAP

02 

CRACKMAPEXEC

03 

RUNFINGER

CyberED

CRACKMAPEXEC

(ТАКЖЕ ИЗВЕСТНЫЙ КАК CME, А В АКТУАЛЬНЫХ ВЕРСИЯХ КАК NETEXEC) - ЭТО МНОГОФУНКЦИОНАЛЬНЫЙ ИНСТРУМЕНТ ДЛЯ ПРОВЕДЕНИЯ АУДИТА БЕЗОПАСНОСТИ И ПОСТ-ЭКСПЛУАТАЦИИ В СЕТЯХ WINDOWS ACTIVE DIRECTORY.

АВТОМАТИЗИРУЕТ ВЗАИМОДЕЙСТВИЕ С РАЗЛИЧНЫМИ СЕТЕВЫМИ ПРОТОКОЛАМИ И ПОЗВОЛЯЕТ ПРОВОДИТЬ РАЗВЕДКУ, ПЕРЕБОР ПАРОЛЕЙ И ИЗВЛЕЧЕНИЕ СЕКРЕТОВ В ПРОМЫШЛЕННЫХ МАСШТАБАХ

Пример использования:

СКАНИРУЕТ УКАЗАННЫЙ ДИАПАЗОН АДРЕСОВ И ПЫТАЕТСЯ СОБРАТЬ БАЗОВУЮ ИНФОРМАЦИЮ О КАЖДОМ ХОСТЕ, НЕ ТРЕБУЯ ПРИ ЭТОМ АУТЕНТИФИКАЦИИ

```
crackmapexec smb ip/prefix
```

CyberED

RUNFINGER

СПЕЦИАЛИЗИРОВАННАЯ УТИЛИТА ДЛЯ РАЗВЕДКИ В СЕТЯХ WINDOWS, ВХОДЯЩАЯ В СОСТАВ ПОПУЛЯРНОГО ФРЕЙМВОРКА RESPONDER.

ОСНОВНОЕ НАЗНАЧЕНИЕ - БЫСТРОЕ СКАНИРОВАНИЕ ПОДСЕТЕЙ ПО ПРОТОКОЛУ SMB ДЛЯ ОПРЕДЕЛЕНИЯ КОНФИГУРАЦИИ БЕЗОПАСНОСТИ УДАЛЕННЫХ ХОСТОВ

Пример использования:

СКРИПТ ОПРАШИВАЕТ УКАЗАННЫЙ ДИАПАЗОН IP-АДРЕСОВ ПО ПРОТОКОЛУ SMB И СОБИРАЕТ ИНФОРМАЦИЮ О КОНФИГУРАЦИИ БЕЗОПАСНОСТИ КАЖДОЙ МАШИНЫ.

Его главная задача - определить статус SMB Signing (цифровой подписи SMB).
Помимо статуса подписи, RunFinger предоставляет полезные данные для разведки:

- Версияоперационнойсистемы Windows
- Имякомпьютера и домена
- Версияиспользуемогопротокола SMB (например, SMBv1 или SMBv2)
- Наличиероликонтроллерадомена

```
python3 RunFinger.py -iip/prefix
```

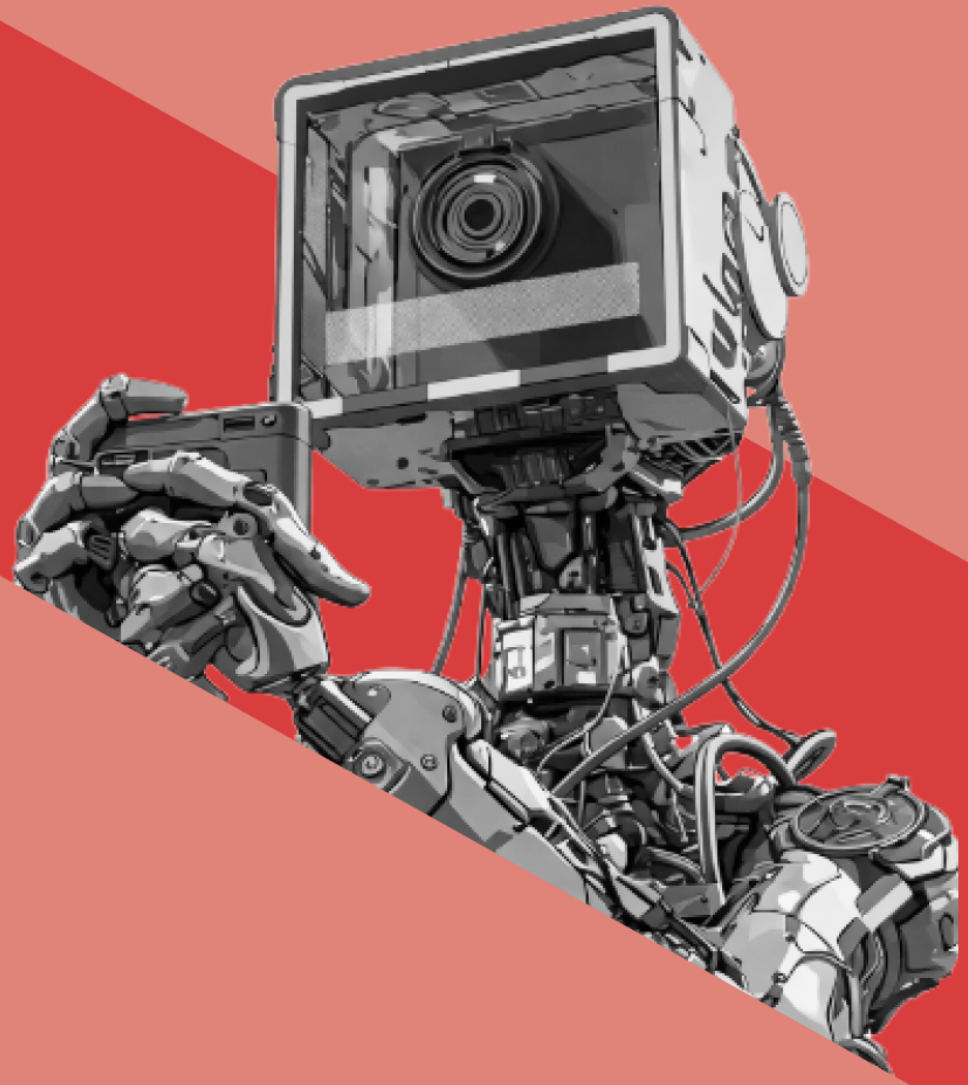
CyberED

КАК БЫВАЕТ В РЕАЛЬНОЙ ЖИЗНИ

Лабораторная среда дает поверхностное понимание, на практике важен навык

- Что делать с хостами без SMB signing
- Как определить куда двигаться дальше
- Что делать с хостами с устаревшей ОС
- Какие уязвимости надо проверить в первую очередь

ENUMERATION



CyberED

ENUMERATION



ИСПОЛЬЗУЯ НЕБЕЗОПАСНУЮ НАСТРОЙКУ ПРОТОКОЛА SMB (NULL-СЕССИЯ), ОТКРЫТЫЙ ДОСТУП ПОЛЬЗОВАТЕЛЮ GUEST ИЛИ ДОМЕННУЮ УЧЕТНУЮ ЗАПИСЬ ПОЛУЧАЕМ СЛЕДУЮЩИЕ ДАННЫЕ:

- Список доменных пользователей
- Доменные группы
- Опции парольной политики
- Содержимое общих папок

ENUMERATION [NULL-СЕССИЯ]



Анонимное подключение к сетевымсервисам Windows. Если сервер уязвим, атакующий без логина и пароля может выгрузить список всех доменных пользователей, групп, парольную политику и общие папки.

CRACKMAPEXEC

Пример использования:

ИЗВЛЕЧЕНИЕ ПОЛИТИКИ ПАРОЛЕЙ

```
crackmapexec smb 10.129.203.121 -u "" -p "" --pass-pol
```

ПРОВЕРКА ДОСТУПНЫХ СЕТЕВЫХ ШАР БЕЗ ПАРОЛЯ ИЛИ ЧЕРЕЗ ПОЛЬЗОВАТЕЛЯ GUEST

```
crackmapexec smb 10.129.203.121 -u guest -p "" --shares
```

ENUMERATION [ACCOUNTS]



Получив начальный доступ с правами обычного пользователя, можно изучить структуру домена: связи, права, GPO и активные сессии пользователей на серверах.

CyberED

CRACKMAPEXEC

Пример использования:

ВЫПОЛНЯЕТ УДАЛЕННЫЙ ЗАПРОС К ЦЕЛЕВОЙ СИСТЕМЕ, ЧТОБЫ УЗНАТЬ, КАКИЕ ПОЛЬЗОВАТЕЛИ В ДАННЫЙ МОМЕНТ НА НЕЙ АВТОРИЗОВАНЫ

```
crackmapexec smb ip -u user -p pass --loggedon-users
```

CyberED

КАК БЫВАЕТ В РЕАЛЬНОЙ ЖИЗНИ

Лабораторная среда показывает первый шаг, но что делать дальше

- Как найти пользователей с правами админа
- Точно ли нужна УЗ доменного администратора
- Какие группы или УЗ могут помочь достигнуть цели

ENUMERATION [SHARED FOLDERS]

Корпоративные общие папки часто содержат конфигурационные файлы, скрипты с зашитыми паролями и конфиденциальные документы.

ИНСТРУМЕНТЫ

01  CRACKMAPEXEC

02  SMBMAP

CyberED

SMBMAP

СПЕЦИАЛИЗИРОВАННАЯ УТИЛИТА ДЛЯ ПЕРЕЧИСЛЕНИЯ СЕТЕВЫХ РЕСУРСОВ (ШАР) В СЕТЯХ WINDOWS, ПРЕДНАЗНАЧЕННАЯ ДЛЯ БЫСТРОЙ ОЦЕНКИ ПРАВ ДОСТУПА И ПОИСКА ФАЙЛОВ

Пример использования:

КОМАНДА ИСПОЛЬЗУЕТСЯ ДЛЯ ДЕТАЛЬНОГО ИЗУЧЕНИЯ СОДЕРЖИМОГО ВСЕХ ДОСТУПНЫХ СЕТЕВЫХ РЕСУРСОВ НА КОНКРЕТНОМ СЕРВЕРЕ

```
smbmap -u user -p pass -H target -R
```

CyberED

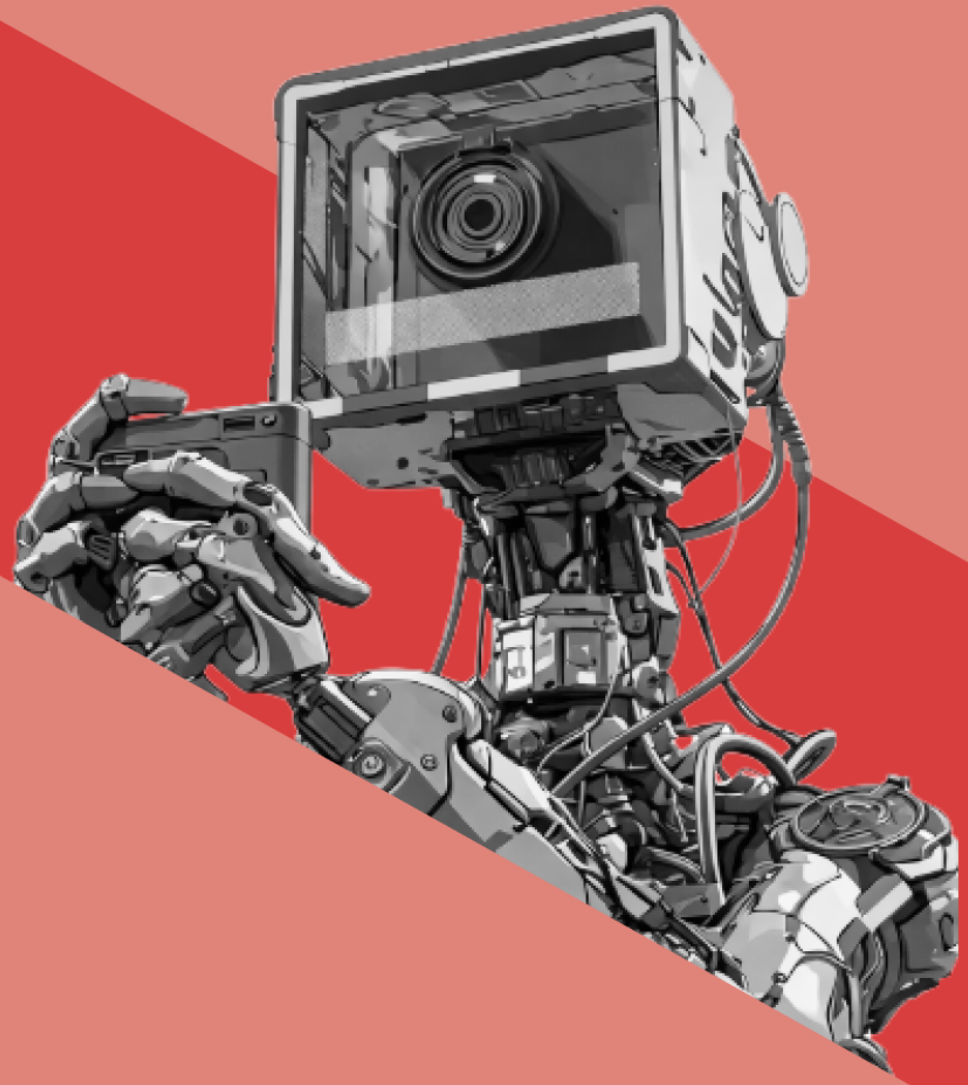
КАК БЫВАЕТ В РЕАЛЬНОЙ ЖИЗНИ

Лабораторная среда демонстрирует отдельный прием, на практике важно смотреть комплексно и системно

- Количество доступных папок огромно
- Как найти нужные файлы
- Как проверить найденный секрет

Как автоматизировать ручной анализ

EXPLOITATION



CyberED

EXPLOITATION [AS-REPROASTING]

Одна из немногих атак на Kerberos, не требующая изначального доступа к домену. Если у учетной записи пользователя включена настройка «Не требовать предварительную проверку подлинности Kerberos», атакующий может запросить зашифрованный TGT-билет от имени этого пользователя и взломать его оффлайн.

ИНСТРУМЕНТЫ

01  IOXIDRESOLVER

GETNPUSERS.PY

УТИЛИТА ИЗ ПАКЕТА IMPACKET. ОНА ИЩЕТ ПОЛЬЗОВАТЕЛЕЙ, У КОТОРЫХ В НАСТРОЙКАХ ACTIVE DIRECTORY УСТАНОВЛЕНА ОПЦИЯ «DO NOT REQUIRE KERBEROS PREAUTHENTICATION» (НЕ ТРЕБОВАТЬ ПРЕДВАРИТЕЛЬНУЮ ПРОВЕРКУ ПОДЛИННОСТИ KERBEROS).
ДЛЯ ТАКИХ УЧЕТНЫХ ЗАПИСЕЙ КОНТРОЛЛЕР ДОМЕНА ВЫДАЕТ ОТВЕТ AS-REP, ЗАШИФРОВАННЫЙ КЛЮЧОМ НА ОСНОВЕ ПАРОЛЯ ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ МОЖНО ВЗЛОМАТЬ ОФФЛАЙН.

Пример использования:

ЗАПРОС ХЭШЕЙ ДЛЯ СПИСКА ПОЛЬЗОВАТЕЛЕЙ С ПОМОЩЬЮ УТИЛИТЫ GETNPUSERS ИЗ СОСТАВА ПАКЕТА IMPACKET

```
GetNPUsers.py domain.local/ -no-pass -usersfile users.txt -request
```

EXPLOITATION [KERBEROASTING]



Атака основана на механизме аутентификации сервисов в протоколе Kerberos. В домене AD сервисы представлены учетными записями, для которых настроен Service Principal Name (SPN). SPN - это атрибут учетной записи, связывающий сервис с учетными данными, под которыми он работает. Kerberos использует SPN, чтобы определить, для какого сервиса должен быть выдан билет. Любой аутентифицированный пользователь домена может запросить сервисный билет (Ticket-Granting Service, TGS) для такого SPN. При его выдаче часть данных билета шифруется ключом соответствующей сервисной учетной записи.

Получив TGS, злоумышленник извлекает зашифрованную часть и подбирает пароль в оффлайн-режиме без последующего взаимодействия с контроллером домена.

CyberED

GETUSERSPNS.PY

УТИЛИТА ИЗ ПАКЕТА IMPACKET. ОНА ПРЕДНАЗНАЧЕНА ДЛЯ ПОИСКА В ACTIVE DIRECTORY УЧЕТНЫХ ЗАПИСЕЙ ПОЛЬЗОВАТЕЛЕЙ, У КОТОРЫХ НАСТРОЕН SERVICE PRINCIPAL NAME (SPN). ОБЫЧНО ЭТО СЕРВИСНЫЕ АККАУНТЫ (НАПРИМЕР, ДЛЯ SQL SERVER, IIS ИЛИ ДРУГИХ СЛУЖБ), ПАРОЛИ КОТОРЫХ ЧАСТО ДЛИННЕЕ И СЛОЖНЕЕ ОБЫЧНЫХ, НО ИХ МОЖНО ПОПЫТАТЬСЯ ВЗЛОМАТЬ ОФФЛАЙН.

Пример использования:

КОМАНДА ЗАПРАШИВАЕТ СЕРВИСНЫЕ БИЛЕТЫ ДЛЯ ВСЕХ ОБНАРУЖЕННЫХ АККАУНТОВ С SPN И ВЫВОДИТ ИХ ЗАШИФРОВАННУЮ ЧАСТЬ В ТЕРМИНАЛ

```
GetUserSPNs.py domain.local/user -request
```

EXPLOITATION [PASSWORD SPRAYING]



Имея на руках политику паролей и список пользователей, мы генерируем один вероятный пароль (например, ИмяКомпании2023!) и проверяем его сразу по всему списку пользователей. Это позволяет избежать блокировки учетных записей (Account Lockout).

CyberED

PASSWORD SPRAYING

Пример использования:

СПРЕИНГ ОДНОГО ПАРОЛЯ ПО СПИСКУ ПОЛЬЗОВАТЕЛЕЙ (DOMAIN AUTH)

```
crackmapexec smb target -u users.txt -p pass
```

ПРОВЕРКА ПЕРЕИСПОЛЬЗОВАНИЯ ПАРОЛЯ ЛОКАЛЬНОГО АДМИНИСТРАТОРА (LOCAL AUTH)

```
crackmapexec smb target -u users.txt -p pass --local-auth
```

EXPLOITATION [CREDENTIAL DUMPING]



Имея права локального администратора на скомпрометированной машине, можно извлечь локальные пароли (база SAM), кэшированные учетки домена (LSA Secrets) и пароли в открытом виде из памяти системного процесса (LSASS).

CyberED

CREDENTIAL DUMPING

Пример использования:

ДАМП БАЗЫ SAM (ЛОКАЛЬНЫЕ ХЭШИ)

```
crackmapexec smb target -u user -p pass --sam
```

ДАМП СЕКРЕТОВ LSA И КЭШИРОВАННЫХ УЧЕТОК ДОМЕНА

```
crackmapexec smb target -u user -p pass --lsa
```

ДАМП ПАМЯТИ ПРОЦЕССА LSASS (CLEARTEXT ПАРОЛИ И ХЭШИ)

```
crackmapexec smb target -u user -p pass -M lsassy
```

CyberED

КАК БЫВАЕТ В РЕАЛЬНОЙ ЖИЗНИ

Лабораторная среда показывает “чистый сценарий”, на практике все сложнее

- Средства защиты не позволяютвыполнить запрос
- Нет сетевого доступа до нужных хостов
- Дамп получили, но подобрать пароли не получается
  Инструмент не работает как ожидалось

CyberED

ДАВАЙТЕ РАЗБЕРЕМ ВАШИ ВОПРОСЫ



CyberED



КАК УСТРОЕНА ПРОГРАММА

[И КАК МЫ ПРИВОДИМ К РЕЗУЛЬТАТУ]

CyberED

Этап 1. Разведка

- Модуль 1. Исследование целей тестирования (Reconnaissance) +
- Модуль 2. Получение первичного доступа через атаки на аутентификацию (Authentication) +
- Модуль 3. Получение первичного доступа через атаки на веб-приложения +
- Модуль 4. Получение первичного доступа через атаки социальной инженерии +

Этап 2. Получение первоначального доступа

- Модуль 5. Эксплуатации известных уязвимостей +

Этап 3. Повышение привилегий/закрепление

- Модуль 6. Повышение привилегий в Linux +
- Модуль 7. Повышение привилегий в контейнерных средах +
- Модуль 8. Повышение привилегий в Windows +

Этап 4. Боковое перемещение в сети

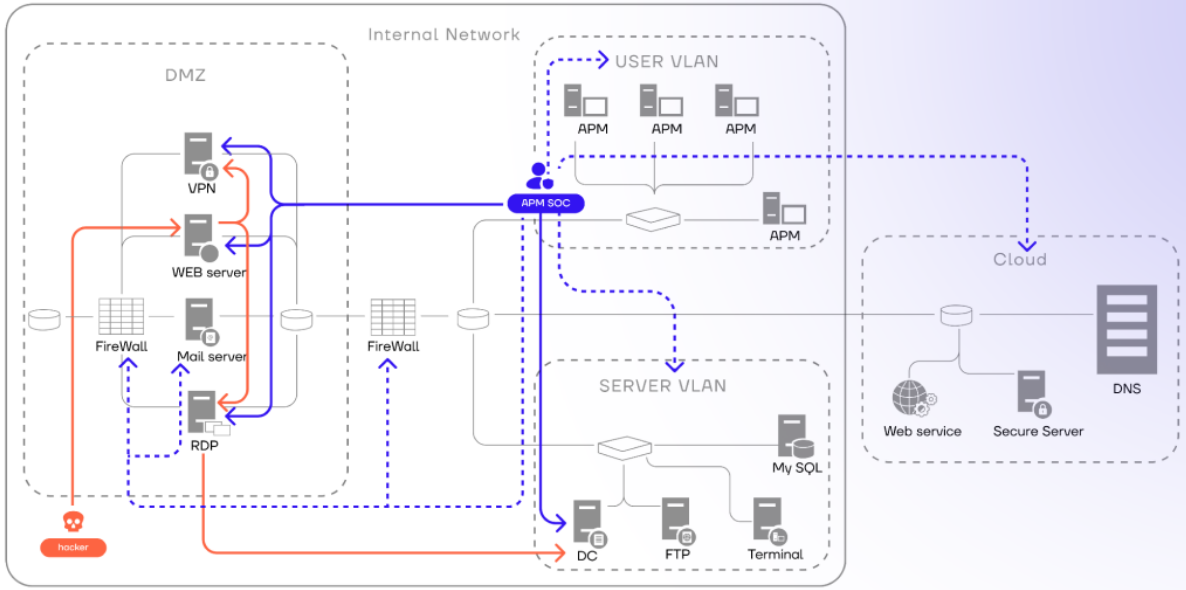
- Модуль 9. Проброс сетевого трафика (Pivoting) +
- Модуль 10. Проведение атак на локальные сети +
- Модуль 11. Проведение атак на Active Directory +

Этап 5. Получение импакта

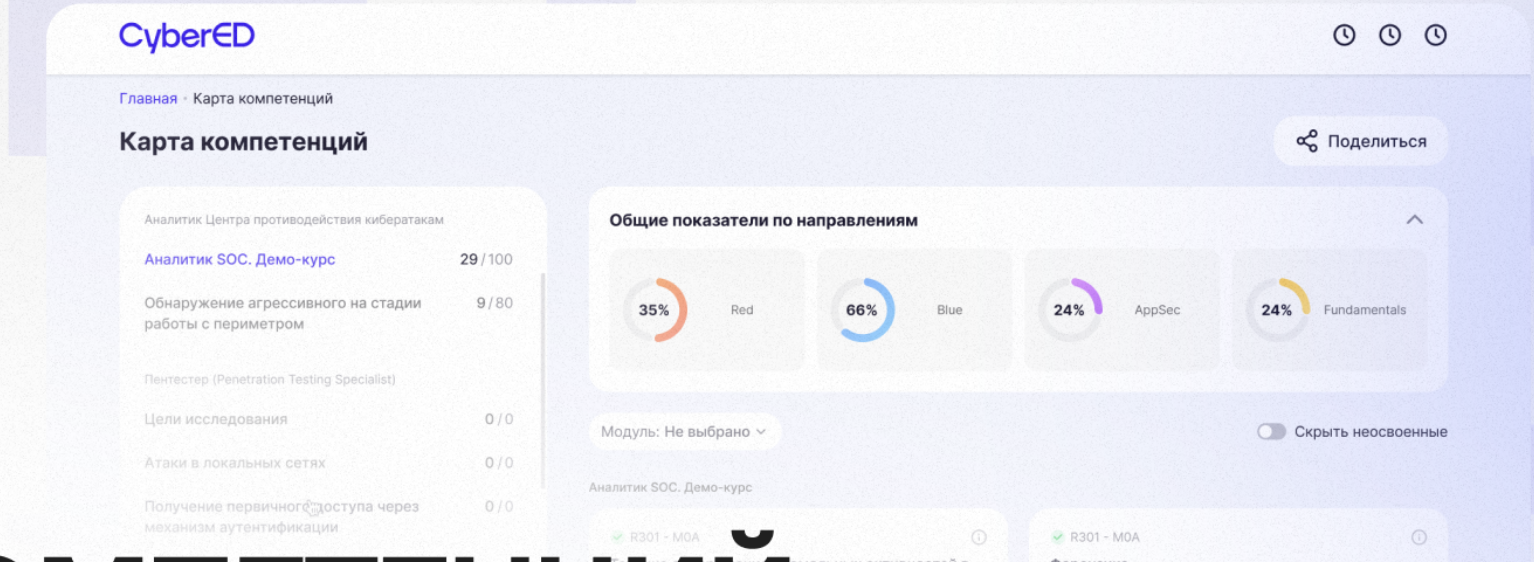
- Модуль 12. Написание отчета +
- Дополнительный модуль. Оценка устойчивости средств защиты +
- Встречи с экспертами по развитию своего профессионального трека: 5 встреч, 20 ак.ч.

ТЕМЫ МОДУЛЕЙ

ЭТО ГОТОВЫЙ ПЛАН ВЫПОЛНЕНИЯ ВСЕЙ ЦЕПОЧКИ АТАКИ В КОМПАНИЯХ



CyberED



КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

КАЖДАЯ ЗАДАЧА → ЗАКРЫВАЕТ НАВЫК

УРОВЕНЬ: БАЗОВЫЙ / СРЕДНИЙ / СЛОЖНЫЙ

- Видно, что ты реально умеешь
- Не «написал в CV» а подтвердил

CyberED

ИНДИВИДУАЛЬНЫЙ СТЕНД ПОД КАЖДОГО

КАЖДОМУ СТУДЕНТУ ПОДНИМАЕТСЯ СВОЯ ИНФРАСТРУКТУРА

01
Ты не зависишь от других

02
Никто не «сломал всё за тебя»

03
Можно спокойно копать и ошибаться

04
Доступ 24/7 к машинам

CyberED

ПРАКТИКА, БЛИЗКАЯ К BUG BOUNTY / РЕАЛЬНОЙ РАБОТЕ

ПРАКТИКА = РАЗВЁРНУТЫЙ СТЕНД + ФЛАГ

Ты **не** «решаешь тест»

Ты работаешь в инфраструктуре и получаешь **результат** (флаг)

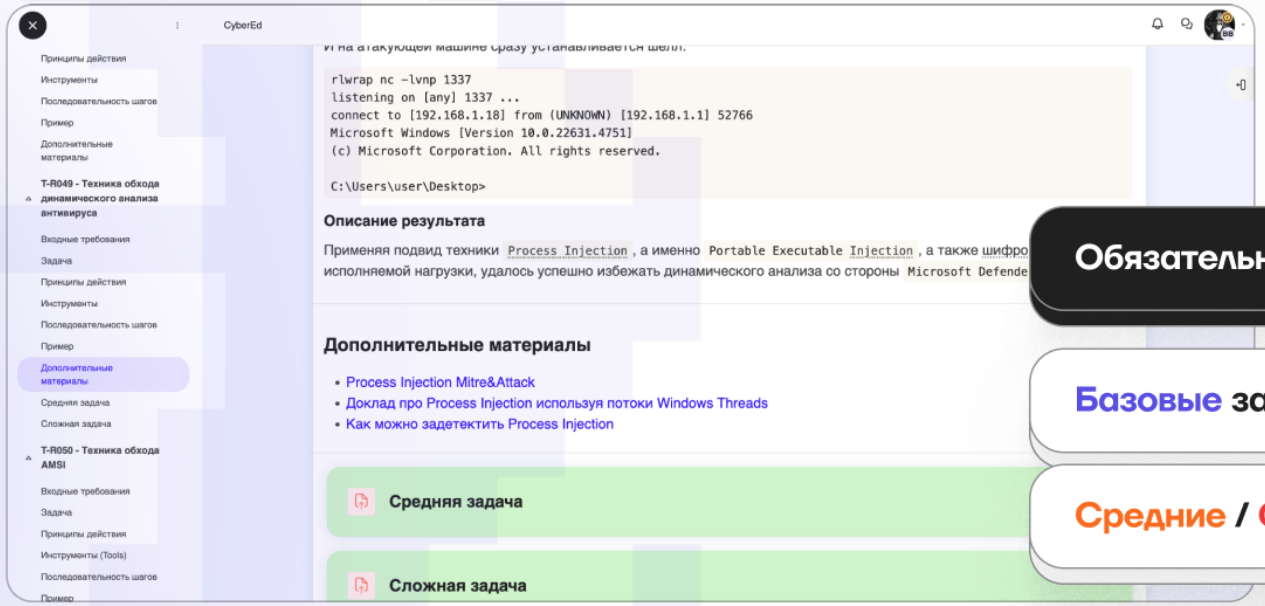


CyberED

КАК МЫ ДОВОДИМ ТЕМУ

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

ПРОГРАММУ МОЖНО ОСВАИВАТЬ ДО УРОВНЯ СЛОЖНОСТИ, КОТОРЫЙ ПОТЯНЕШЬ



- Встроенная система давления на результат ⟶ Нельзя «проскочить»

Обязательная база → Добровольный рост

Базовые задачи — обязательны (иначе нет сертификата)

Средние / Сложные — для прокачки уровня

CyberED

КАК МЫ ДОВОДИМ ТЕМУ

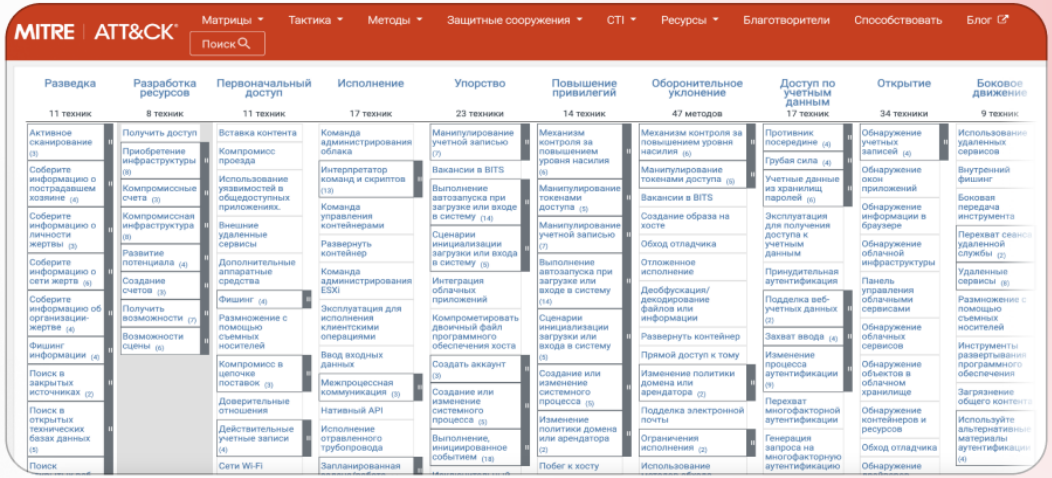
ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

КАЖДАЯ ТЕХНИКА
= ОТДЕЛЬНЫЙ СКИЛЛ
= ОТДЕЛЬНАЯ ПРАКТИКА

- 1–2 задачи на ⚠ каждую технику
- от 1 до 3 уровня сложности
- 3й уровень - на 🔑 киберполигоне

Не «один раз попробовал»
→ а **закрепление** через повторение

- **120+** техник (скиллов) для пентеста из MITRE ATT&CK и от архитекторов программы



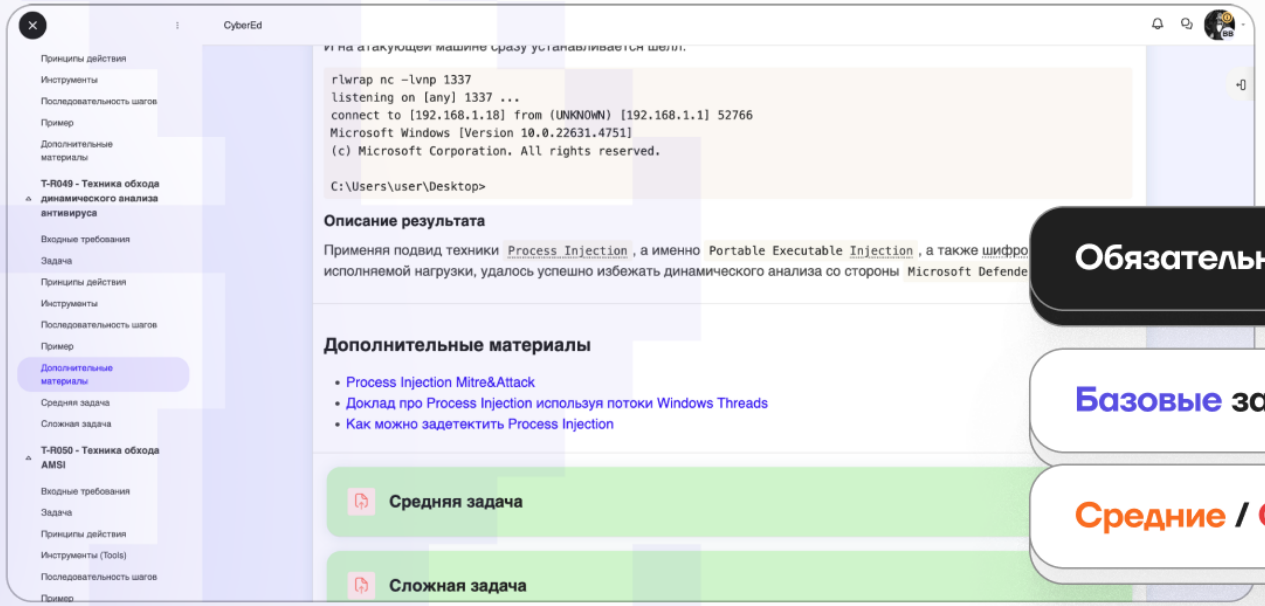
Матрица ATT&CK - всемирно признанная карта действий хакеров, основанная на реальных атаках.

CyberED

КАК МЫ ДОВОДИМ ТЕМУ

ДО ПРАКТИЧЕСКОГО ПОНИМАНИЯ

ПРОГРАММУ МОЖНО ОСВАИВАТЬ ДО УРОВНЯ СЛОЖНОСТИ, КОТОРЫЙ ПОТЯНЕШЬ



- Встроенная система давления на результат ⟶ Нельзя «проскочить»

Обязательная база → Добровольный рост

Базовые задачи — обязательны (иначе нет сертификата)

Средние / Сложные — для прокачки уровня

CyberED

ПЕРЕХОД ОТ ТЕХНИКИ К ХАОСУ



СНАЧАЛА

Ты знаешь, какую технику применять

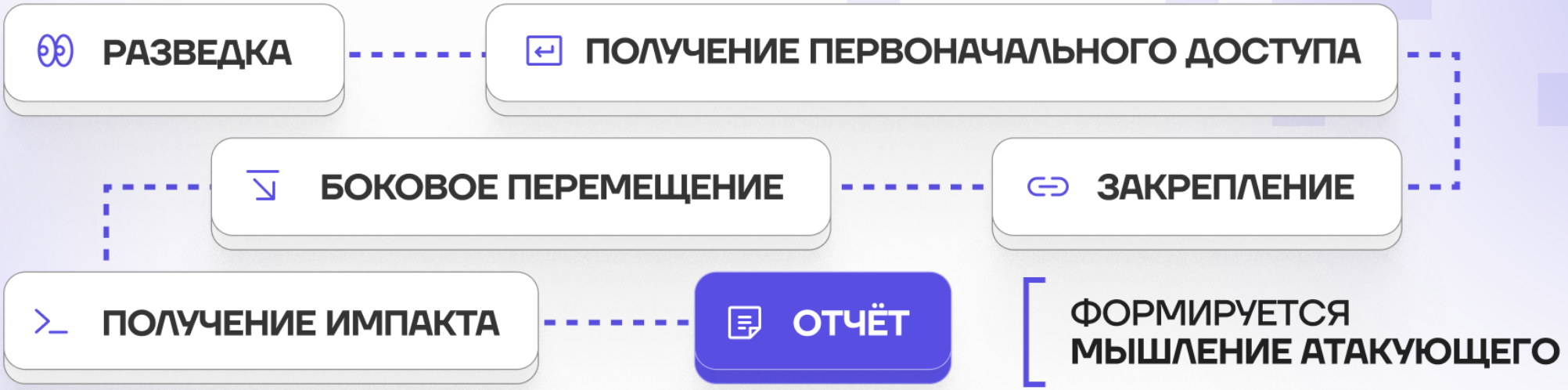
ПОТОМ

Тебе дают инфраструктуру
→ Сам разбирайся

Не изолированные упражнения, а **связанный процесс**

CyberED

ЦЕПОЧКИ АТАК ВМЕСТО ОТДЕЛЬНЫХ ЗАДАЧ



ФОРМИРУЕТСЯ
МЫШЛЕНИЕ АТАКУЮЩЕГО

CyberED

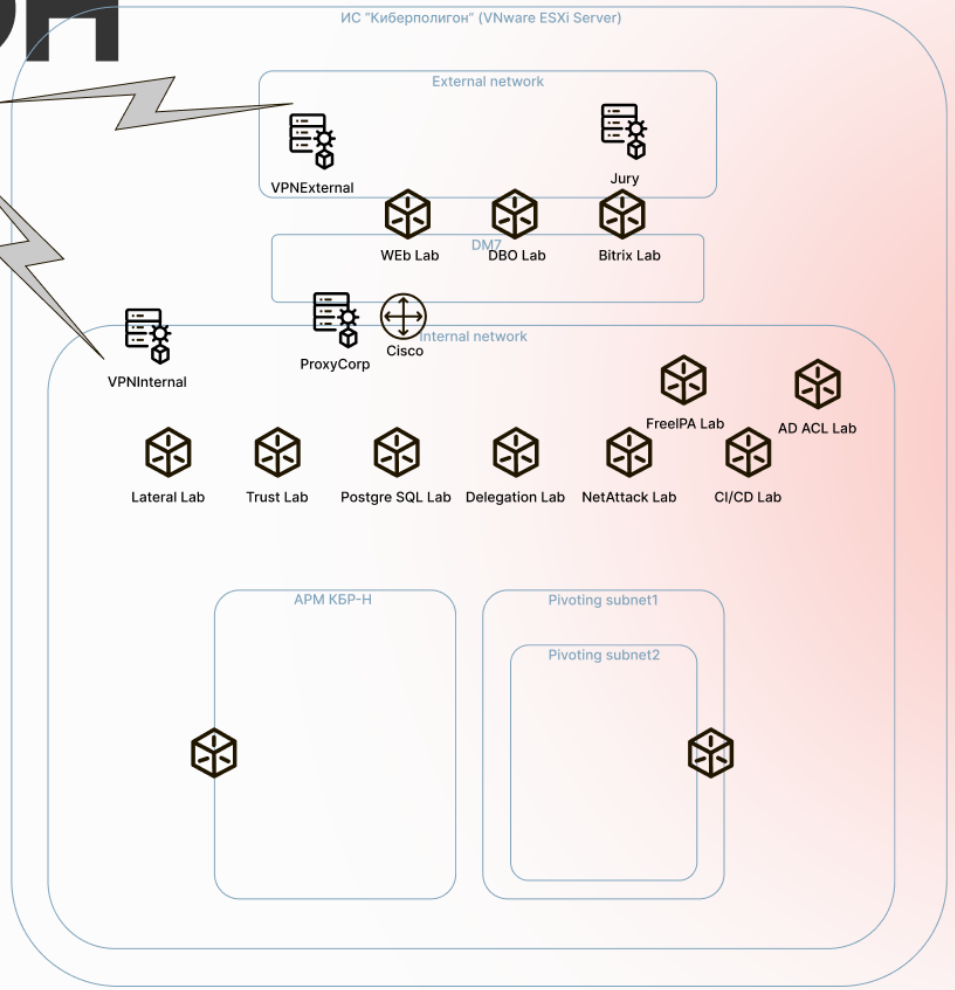
КИБЕРПОЛИГОН

|** CyberED

- Имитация инфраструктуры компании
- Цепочки атак
- Нет подсказок, нет «правильного пути»

Максимально близко к работе:

« ВОТ ТЕБЕ КОМПАНИЯ - ЛОМАЙ »



CyberED

КИБЕРПОЛИГОН

CyberED

30
Сценариев

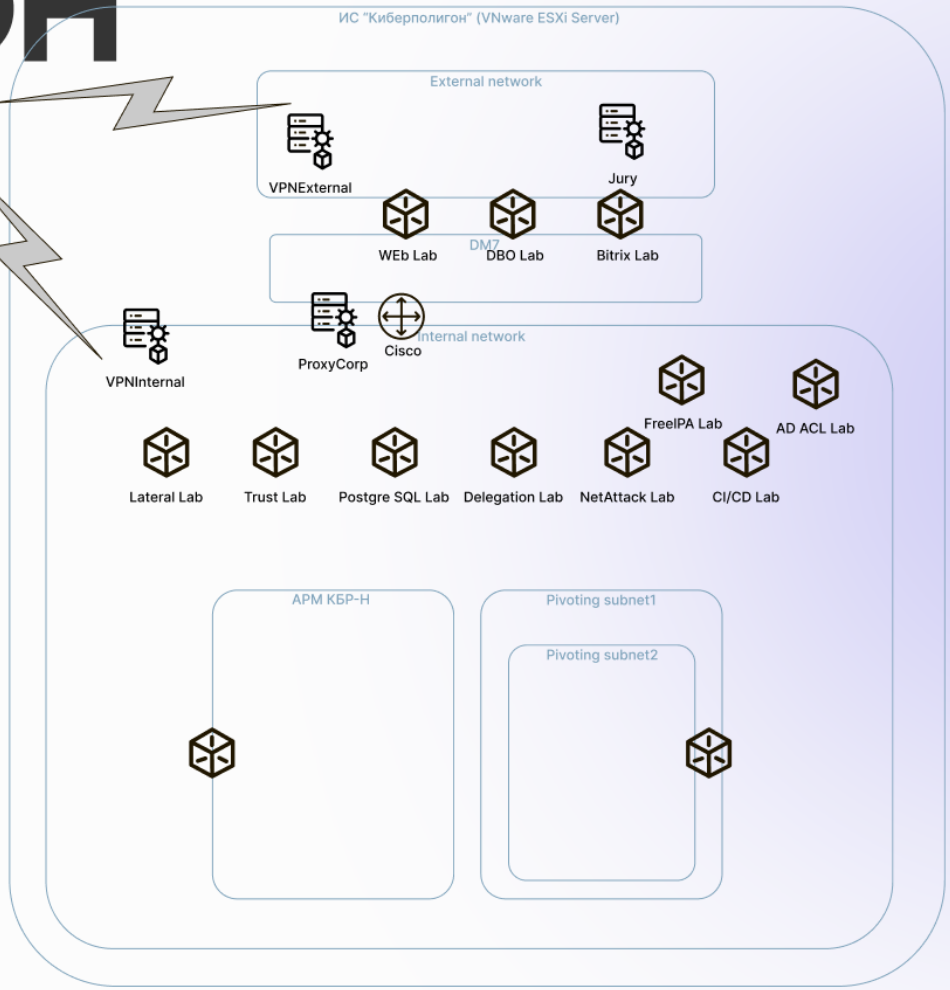
30
Виртуальных машин

60+
Тасок,
в каждой из которых может быть несколько уязвимостей.

ЗАДАЧИ

- атаки на операционные системы (Windows, Linux),
- веб
- сетевые атаки.

+ Нарабатываете насмотренность по сценариям атак
+ Сталкиваетесь с вариативностью уязвимостей



CyberED

УКАЖЕТЕ В РЕЗЮМЕ КОНКРЕТНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ

Не так: умею применять BurpSuite - X

А так: нашел уязвимость path traversal в таком-то сервисе, используя инструмент BurpSuite, эксплуатировал данную уязвимость и получил учетные данные для последующей компрометации инфраструктуры Заказчика - Y.

Не так: умение работать в среде Active Directory - X

А так: реализовал цепочку атаки до компрометации AD и захвата инфраструры с помощью обнаруженной уязвимости в центре сертификации - Y.

ПРИМЕР 1

Не так: умею сканировать порты и подбирать пароли.

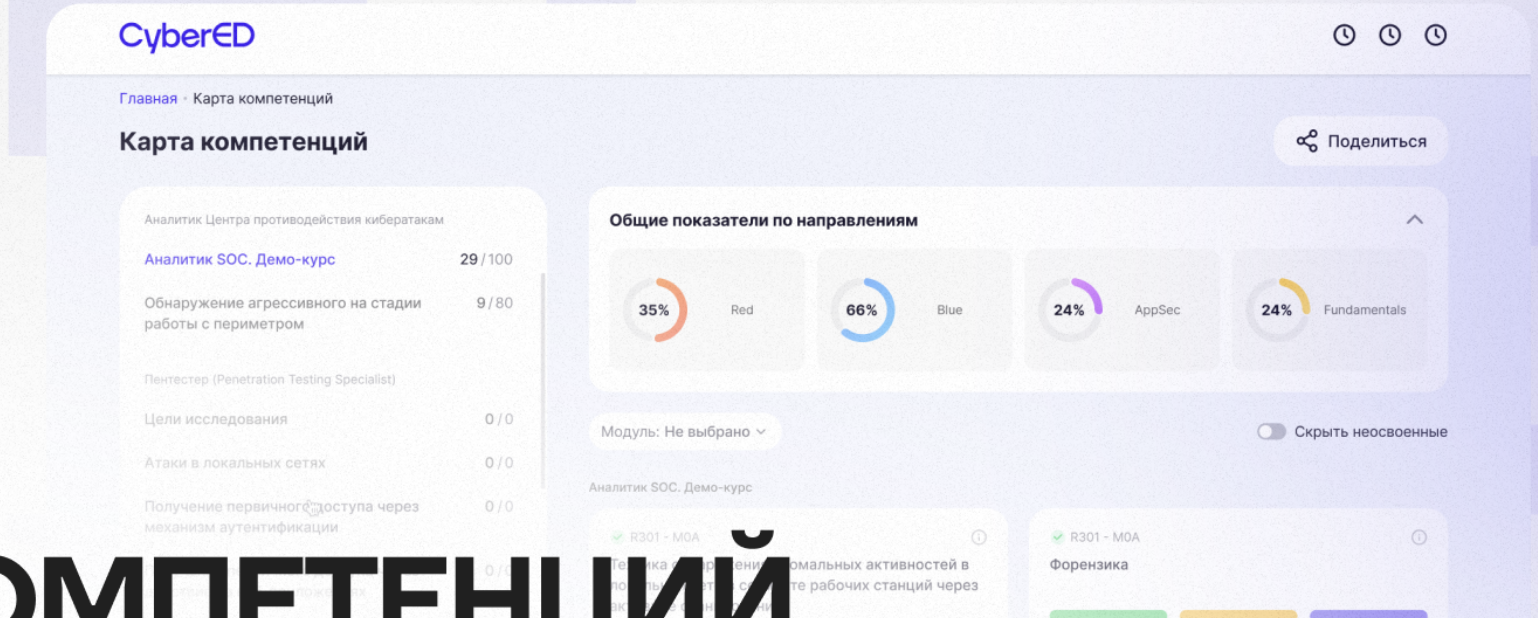
Так: обнаружил открытый порт 3389 на непубличном хосте, осуществил подбор пароля для учётной записи локального администратора через RDP, получил shell и развернул прокси для дальнейшего движения по внутренней сети Заказчика.

ПРИМЕР 2

Не так: знаю Docker и Kubernetes.

Так: через уязвимость в конфигурации GitLab CI (незащищённые переменные окружения) получил токен доступа к приватному registry, внедрил вредоносный образ, извлёк секреты production-окружения и достиг компрометации оркестратора кластера.

CyberED



КАРТА КОМПЕТЕНЦИЙ = ЦИФРОВОЕ РЕЗЮМЕ

ПУБЛИЧНЫЙ ПРОФИЛЬ

МОЖНО ОТКРЫТЬ ССЫЛКУ / ПОКАЗАТЬ НАВЫКИ РАБОТОДАТЕЛЮ

Это уже не обучение, это **переход к найму**

CyberED

[ИНТЕНСИВ] AI-УСИЛЕННЫЙ ПЕНТЕСТ: СБОРКА AI-ПАЙПЛАЙНА ДЛЯ OFFENSIVE SECURITY



АВТОР КУРСА:

СЕРГЕЙ ЗЫБНЕВ

- Тимлид пентестеров в «Бастион» с 5+ лет опыта в ИБ
- Автор Telegram-канала «Похек» (16к+ подписчиков)
- Опыт в AI/LLM:
- $5 000+ инвестировано в эксперименты с AI-агентами
- 1,5 года R&D в AI для пентеста

В ОСНОВЕ ИНТЕНСИВА – РЕАЛЬНЫЙ ПРАКТИЧЕСКИЙ ОПЫТ ЭКСПЕРТА:

01 **Разбор** рабочих кейсов

02 **Тестирование** AI-инструментов в задачах offensive security

03 **Эксперименты** с различными подходами к автоматизации пентеста

Основная аудитория:

+ Пентестеры
+ Специалисты offensive security
+ Bug bounty-исследователи
+ Red team инженеры

Также будет полезен:

+ Blue Team специалистам - для понимания логики атакующего
+ AppSec-инженерам
+ DevSecOps-специалистам
+ Security engineers, участвующим в security-тестировании инфраструктуры

CyberED

ОСТАВЛЯЙ ЗАЯВКУ!

- \+ ИИ в пентесте от Похек
- \+ DETA / Авторский курс Егора Зайцева «Обход антивирусов»
- \+ 1 любой мини-курс из платных программ на выбор
- \+ программа «Bug Bounty Hunter» совместно со Standoff 365
- \+ Карьерный модуль по трудоустройству

CyberED

ДАВАЙТЕ РАЗБЕРЕМ ВАШИ ВОПРОСЫ

