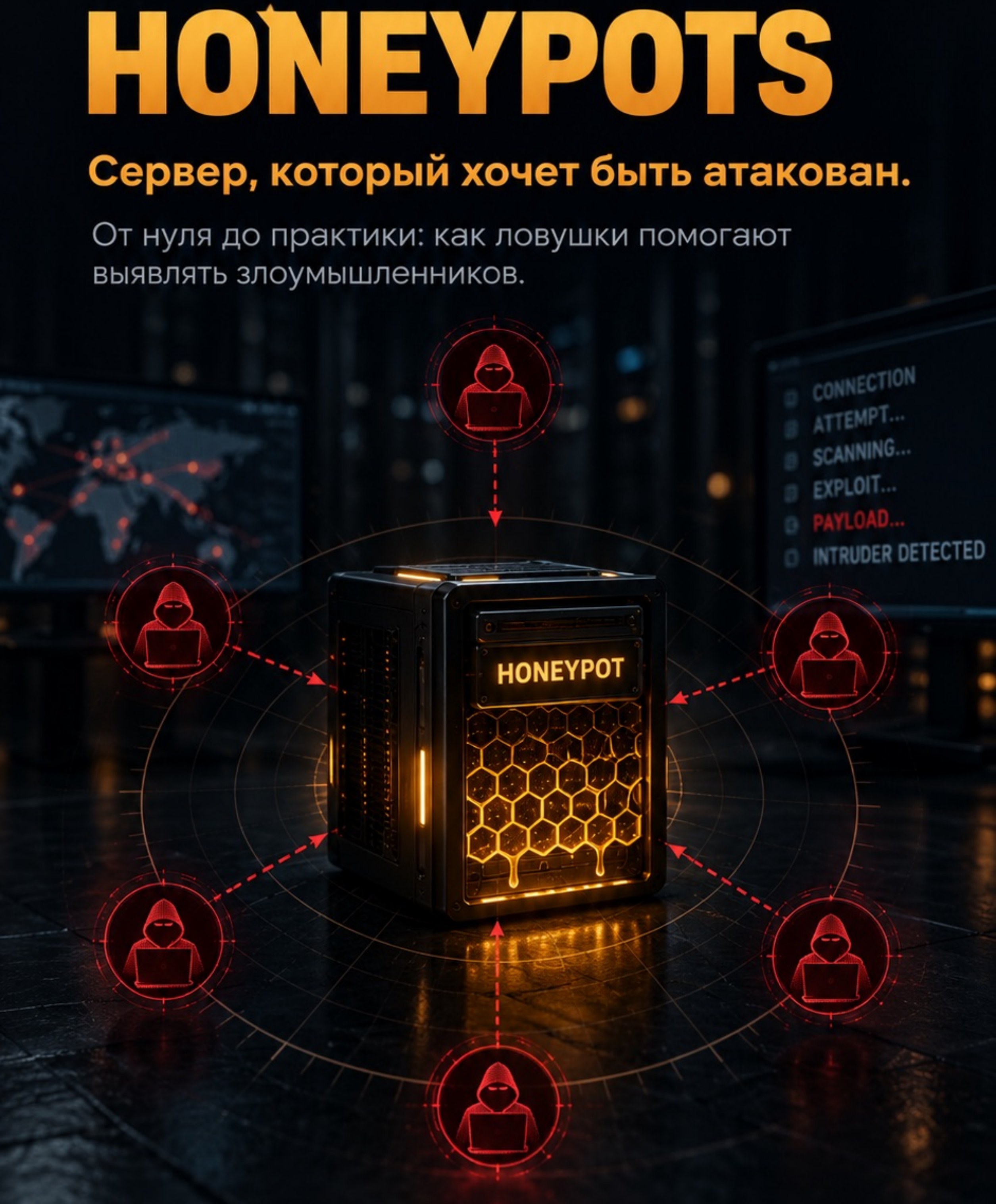
КАК РАБОТАЮТ HONEYPOTS

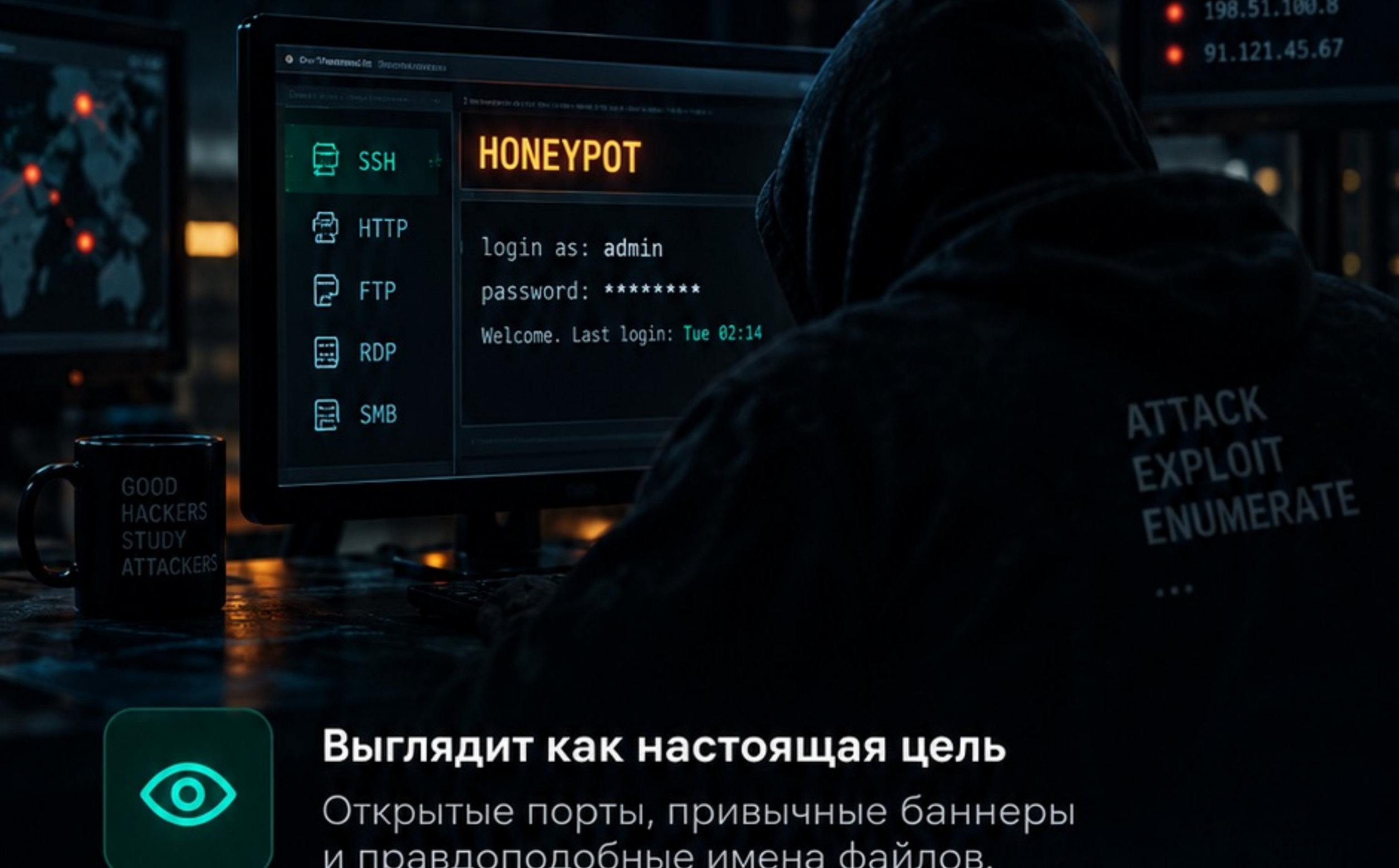
Сервер, который хочет быть атакован.

От нуля до практики: как ловушки помогают выявлять злоумышленников.



ЧТО ТАКОЕ HONEYPOT?

Honeypot — это приманка, специально созданная для того, чтобы её находили, исследовали и атаковали. Она выглядит как настоящая цель, но внутри ничего реального.



Выглядит как настоящая цель

Открытые порты, привычные баннеры и правдоподобные имена файлов.

Не содержит реальных данных

Все файлы, пользователи и записи — искусственные.

Нет легитимных пользователей

Ни один сотрудник, скрипт или клиент не должен иметь к нему доступ.

По определению, любое взаимодействие с honeypot — это подозрительная активность.

ПОЧЕМУ HONEYPOTS ВАЖНЫ

Больше, чем просто приманка.
Вот почему honeypots — мощный инструмент в кибербезопасности.



01

Почти нет ложных срабатываний

Обычные пользователи не заходят в систему, которой не должно быть. Любое взаимодействие — это реальный сигнал о злоумышленнике.

02

Раннее обнаружение

Фиксирует атакующего ещё до того, как он доберётся до реальных систем, позволяя быстрее реагировать.

03

Реальное поведение, а не теория

Вы видите реальные инструменты, команды и техники, которые используют атакующие именно против вас.

04

Отнимает время у атакующего

Каждая минута, потраченная на исследование ложной цели, — это минута, которую он не тратит на настоящую инфраструктуру.

**Honeypots не просто обнаруживают атаки.
Они меняют правила игры.**

HONEYPOT VS РЕАЛЬНАЯ СИСТЕМА

Внешне может выглядеть похоже.
Но цель, данные и последствия — совсем разные.



	Обслуживает реальных пользователей	**Не обслуживает никого** Создан, чтобы привлекать злоумышленников
Назначение		
Данные	Настоящие бизнес-данные	**Только поддельные данные** (fake data)
Трафик	Постоянная рабочая нагрузка	По сути **нулевой трафик** до момента атаки
Алерты	Требуют приоритизации и анализа	**Имеют высокий приоритет и требуют немедленной реакции**
Доступ	Жёстко защищён и ограничен	**Намеренно выглядит уязвимым**, чтобы привлечь атаки

Honeypots не заменяют защиту.
Они усиливают вашу видимость.

КАК УСТРОЕН HONEYPOT

Внутри выглядит как настоящая цель,
но на самом деле всё под контролем.



01 Приманка
(Decoy surface)

Фальшивые сервисы, баннеры и файлы, которые видит злоумышленник. Всё выглядит как реальная цель.



02 Изоляция
(Isolation cage)

Жёсткие ограничения не позволяют приманке взаимодействовать с реальной инфраструктурой.



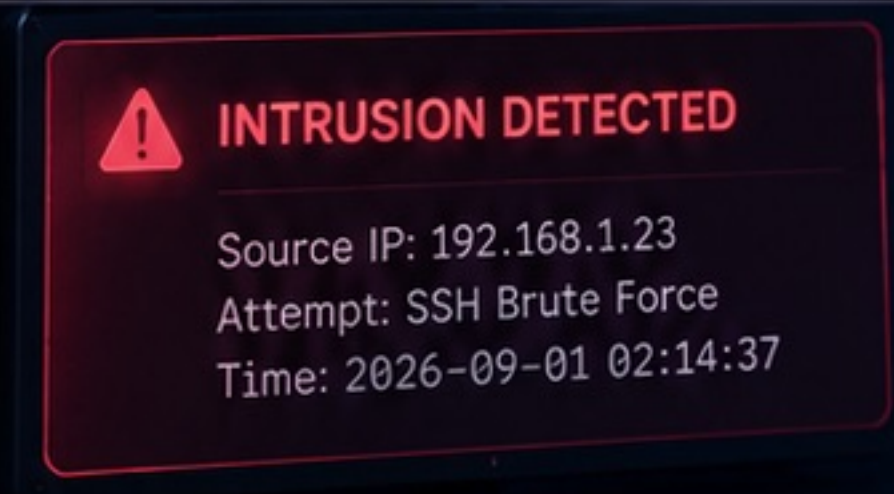
03 Сбор данных
(Capture engine)

Фиксирует каждый пакет, команду, введённый пароль и загруженный файл.



04 Оповещения
(Alert pipeline)

Мгновенно отправляет события в вашу систему мониторинга (SIEM, Slack, Email и др.).



05 Анализ
(Analysis)

Преобразует сырые данные в инсайты: правила детекта, blacklists и отчёты.



**Honeypots не просто ловят атаки.
Они дают знания, которые помогают лучше защищаться.**

КАК ПРОХОДИТ АТАКА НА HONEYPOT

Пошаговый взгляд на то, как злоумышленник взаимодействует с приманкой.



01

Разведка

Злоумышленник сканирует диапазоны IP-адресов в поиске открытых портов.

```
nmap -sS 10.0.0.0/24

PORT     STATE   SERVICE
22/tcp   open    ssh
23/tcp   open    telnet
80/tcp   open    http
445/tcp  open    smb
```

02

Обнаружение

Приманка откликается на обращение к интересному порту, заманивая атакующего дальше.

```
Connecting to 10.0.0.5:22 ...
SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0
root@10.0.0.5
```

03

Исследование

Злоумышленник изучает систему: читает баннер, проверяет версии ПО, пытается понять, что перед ним.

```
root@honeypot:~# uname -a
Linux honeypot 5.15.0-101-generic ...
root@honeypot:~# cat /etc/os-release
PRETTY_NAME="Ubuntu 20.04.6 LTS"
root@honeypot:~#
```

04

Атака

Злоумышленник использует украденные учетные данные или известный эксплойт, чтобы получить доступ.

```
hydra -l admin -P passwords.txt ssh://10.0.0.5

[22][ssh] host: 10.0.0.5   login: admin
password: 123456

[SUCCESS] Valid password found!
```

05

Фиксация активности

Приманка имитирует успех и записывает каждое действие атакующего — команды, загруженные файлы, нажатия клавиш.

```
2025-03-14 10:24:11   COMMAND   whoami
2025-03-14 10:24:13   COMMAND   wget http://mal
2025-03-14 10:24:17   FILE      /tmp/malware.sh
2025-03-14 10:24:20   COMMAND   chmod +x malwar
2025-03-14 10:24:22   COMMAND   ./malware.sh
...
```

06

Оповещение

Ваша команда получает уведомление в реальном времени, пока злоумышленник продолжает активность.

```
Honeypot Alert
New attacker activity detected
Source IP: 185.199.110.23
Service: SSH
Time: 2025-03-14 10:24:11
```

Каждая атака на honeypot — это ценные данные для вашей защиты.

УРОВНИ ВЗАИМОДЕЙСТВИЯ С HONEYPOT

Насколько реалистичной выглядит приманка для атакующего. Чем выше реализм — тем больше информации и выше риск.

НИЗКИЙ УРОВЕНЬ

Простая приманка



Имитирует один порт и статичный баннер. Просто, но эффективно.

ИМИТИРУЕТ

- PORT
- SERVICE
- SYSTEM

ВЫ УВИДИТЕ

Сканирование и попытки подключения.

```
nmap 10.0.0.10
PORT     STATE
22/tcp   open
```

ИНФОРМАЦИИ 28%

РИСК 12%

СРЕДНИЙ УРОВЕНЬ

Интерактивная приманка



Имитирует сервис и отвечает на действия злоумышленника.

ИМИТИРУЕТ

- PORT
- SERVICE
- SYSTEM

ВЫ УВИДИТЕ

Команды, полезные нагрузки и попытки эксплуатации.

```
ssh user@10.0.0.20
Password: ********
Last login: Wed Mar 12 10:24:3
```

ИНФОРМАЦИИ 62%

РИСК 45%

ВЫСОКИЙ УРОВЕНЬ

Почти как реальная система



Имитирует полноценную систему в изолированной среде (cage).

ИМИТИРУЕТ

- PORT
- SERVICE
- SYSTEM

ВЫ УВИДИТЕ

Всю сессию: от разведки до попыток закрепиться в системе.

```
root@honeypot:~# whoami
root
root@honeypot:~#
```

ИНФОРМАЦИИ 100%

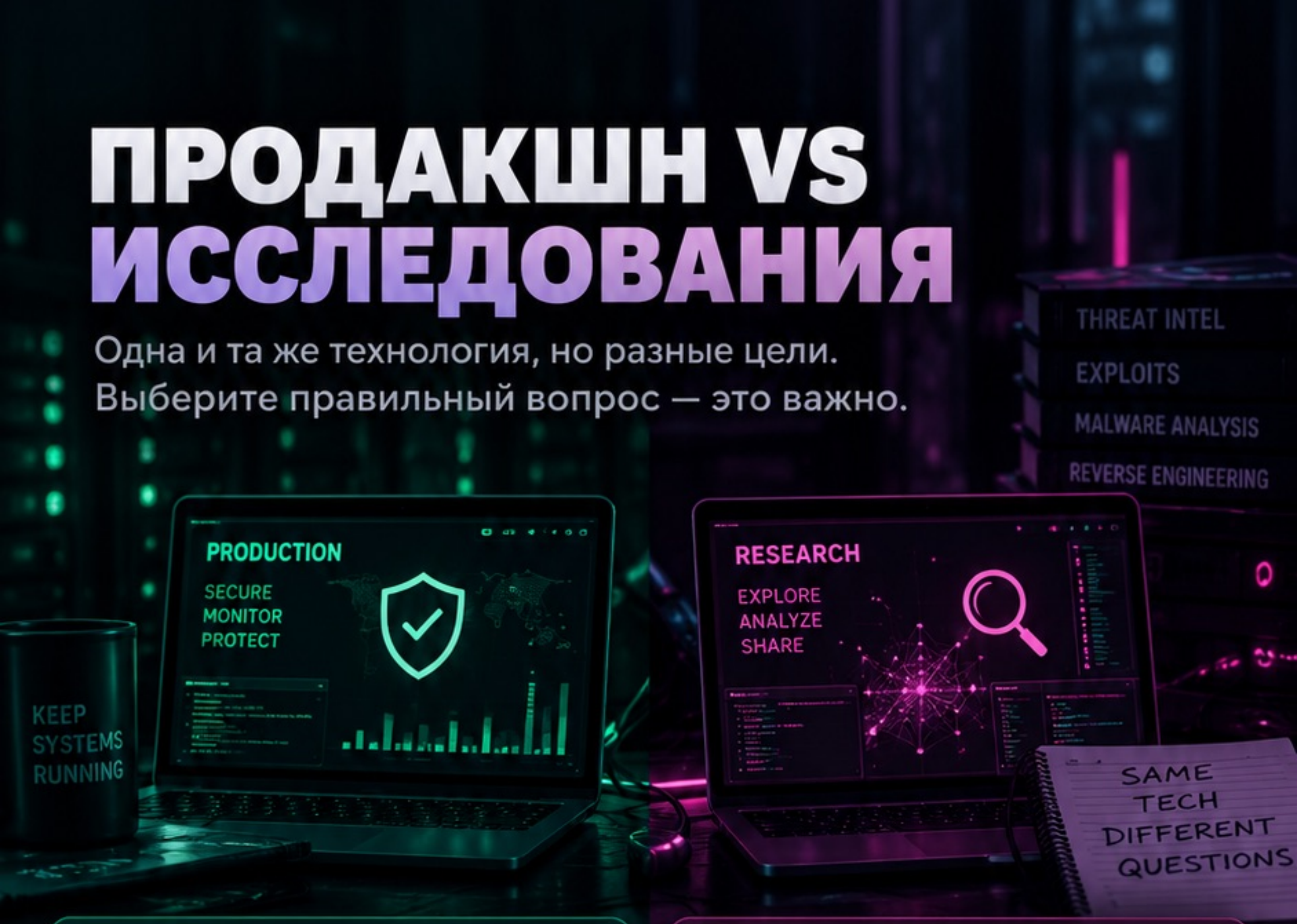
РИСК 92%

Не запускайте honeypot с высоким уровнем взаимодействия без изоляции (cage).

Больше реализма — больше данных, но и выше риск.

ПРОДАКШН VS ИССЛЕДОВАНИЯ

Одна и та же технология, но разные цели.
Выберите правильный вопрос — это важно.



ПРОДАКШН

Создан для обнаружения

Живёт внутри корпоративной сети

Работает в реальной инфраструктуре компании.

Мелкое взаимодействие, минимум шума

Иммитирует обычную активность, чтобы не привлекать внимание.

Принадлежит команде безопасности

Разворачивается и поддерживается SOC.

Задаёт простой вопрос:

«Уже кто-то внутри?»

ИССЛЕДОВАНИЯ

Создан для получения знаний

Живёт в открытом интернете

Нацелен на весь мир, не ограничен инфраструктурой.

Глубокое взаимодействие, максимум данных

Собирает максимум информации об атакующих.

Принадлежит аналитикам и исследователям

Используется командами TI, malware-анализа и R&D.

Задаёт другой вопрос:

«Что сейчас делают злоумышленники?»

Одна технология. Разные задачи.
Главное — задать правильный вопрос.

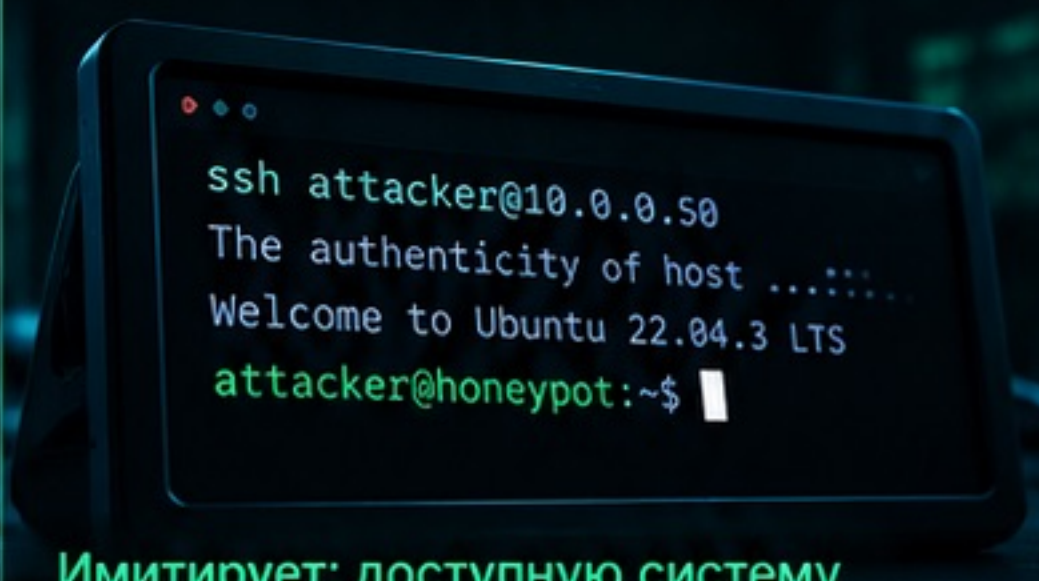
DETECT
DECEIVE
LEARN
STAY AHEAD

ТИПЫ ПРИМАНОК И ПО ЧЕМУ ОНИ ИМИТИРУЮТ

Разные приманки имитируют разные цели, чтобы привлечь определённый тип атакующих.

Удалённый доступ

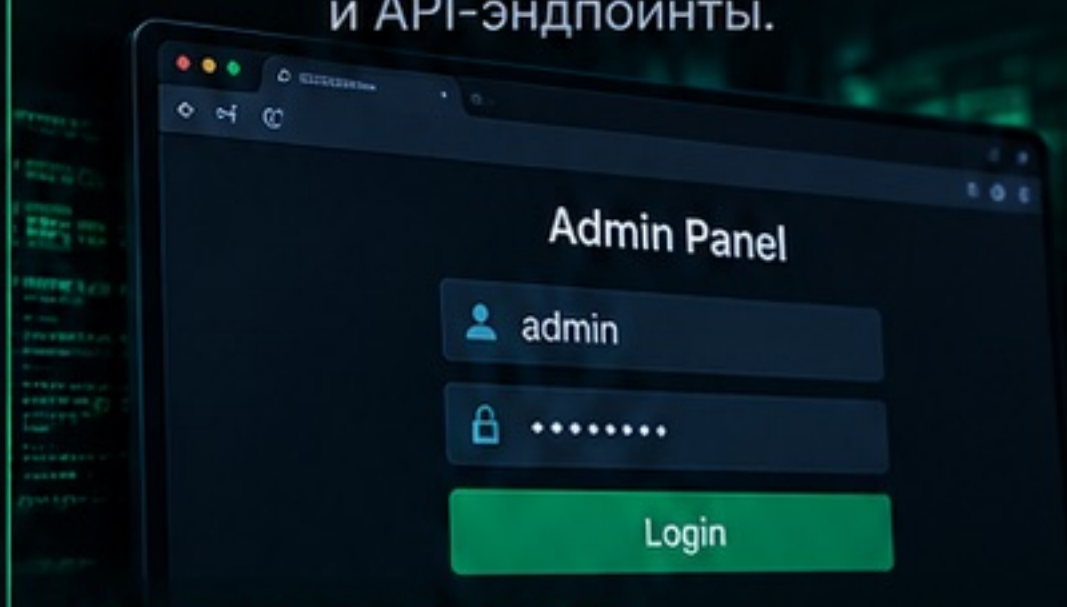
Фальшивый сервис для входа через SSH/RDP на открытом порту.



Имитирует: доступную систему

Веб-приложение

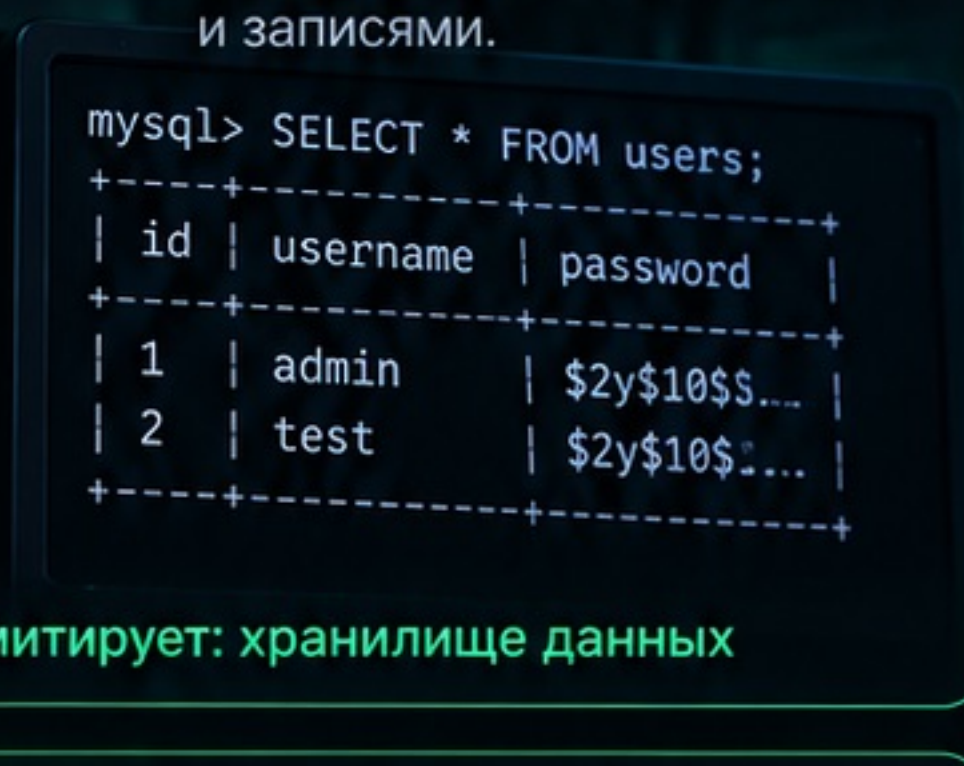
Поддельная панель администратора, формы и API-эндпоинты.



Имитирует: веб-сервис

База данных

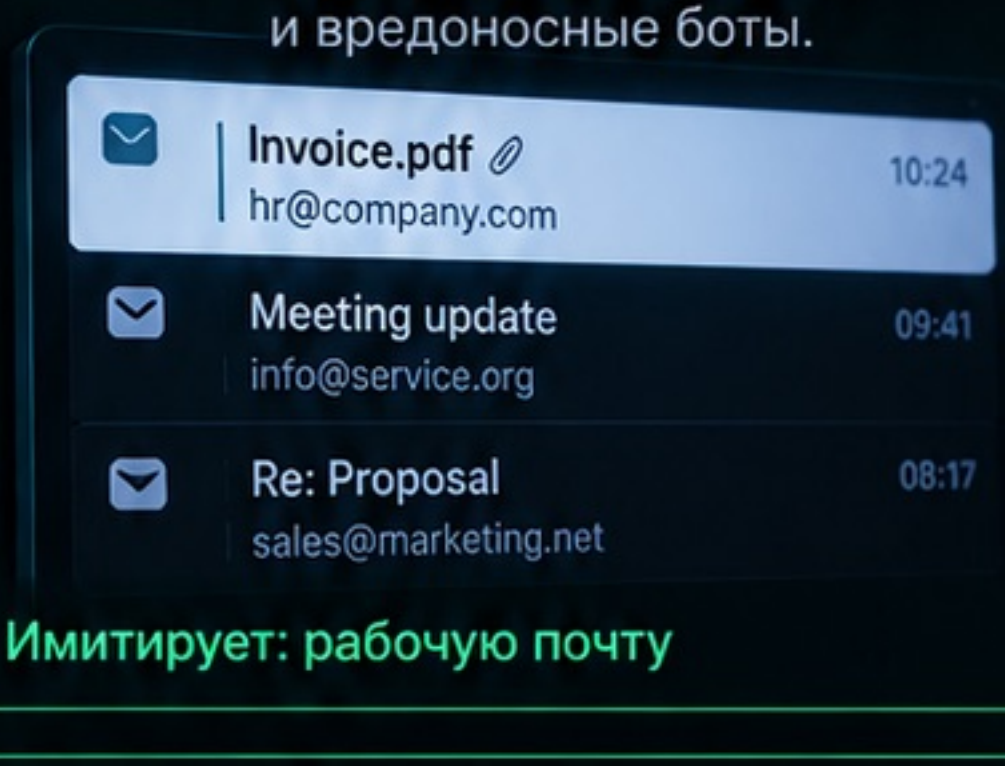
Фальшивые таблицы с вымышленными данными и записями.



Имитирует: хранилище данных

Почтовая ловушка

Почтовый адрес, который находят только спамеры и вредоносные боты.



Имитирует: рабочую почту

Промышленное устройство

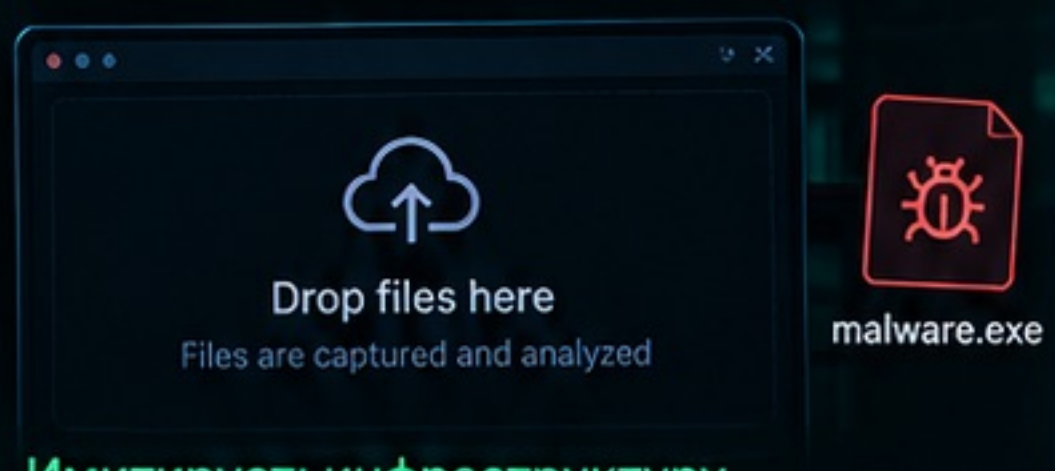
Фальшивый датчик или контроллер в OT/ICS-сети (например, Modbus, S7).



Имитирует: устройства OT/ICS

Сборщик вредоносов

Приманка, которая принимает и сохраняет отправленные вредоносные файлы.



Имитирует: инфраструктуру для загрузки файлов

Зная, что имитирует приманка, вы получаете больше контекста об атакующем.

Правильный тип — больше данных, лучше защита.

HONEYTOKENS

DETECT DECEIVE RESPOND

SECURITY THROUGH DECEPTION

HONEYTOKENS

HONEYTOKEN — это не система и не инструмент.
Это специально размещённые данные,
которые никогда не должны использоваться.
Достаточно одного касания — и срабатывает
тревога.



01

Фальшивый логин

Учётная запись, которая нигде не работает, но выглядит как настоящая.

fake_admin
••••••••••
Authentication failed
Alert triggered

02

Приманочный файл

Документ, который никто не должен открывать, но он выглядит интересным.

Q3_Financial_Report.pdf
2.4 MB

03

Ключ без прав

Доступ (API key, токен и т.п.), который не имеет реальных разрешений, но кажется рабочим.

```
export API_KEY=
sk_live_51H0ney...FAKE123"
# no real permissions
```

04

Фальшивые данные

Записи в базе данных, которые выглядят как реальные, но специально добавлены.

users

id	username	role
1001	john.doe	user
1002	backup_admin	admin
1003	test	user

05

Скрытая ссылка

Ссылка, которую должен найти только атакующий (не индексируется, скрыта в коде или документах).

https://internal.local/backup

Crawler: no index

Как только приманки используют — вы точно знаете, откуда утечка.

Honeypokens превращают любопытство атакующих в вашу осведомлённость.

DETECT DECEIVE UNDERSTAND

HONEYPOTS
STRONGER
DEFENSE

ОТ HONEYPOT К HONEYNET

Одна приманка ловит первый удар.
Фальшивая сеть ловит весь путь атакующего.



Шлюз
пропускает атаки,
но не выпускает их наружу.

Атакующий заходит внутрь,
но остаётся в изоляции.

Фальшивые хосты
выглядят как обычная
подсеть.

Имитируют реальную
инфраструктуру: серверы,
сервисы, рабочие станции.

Реалистичный трафик
специально сгенерированные
данные.

Создаёт видимость живой сети,
чтобы атакующий действовал
как обычно.

**Теперь вы отслеживаете
боковое перемещение, а не только
первый контакт.**

Honeynets помогают увидеть полную картину атаки.

MORE VISIBILITY.
A SAFER TOMORROW.

CYBERSECURITY
IN PRACTICE

THINK
LIKE AN
DEFENDER

OBSERVE
QUESTION
STAY AHEAD

КУДА РАЗМЕСТИТЬ HONEYPOT

Место размещения определяет, на какой вопрос вы получите ответ.

На периметре

Кто сканирует интернет
и какими инструментами?



В DMZ

Кто охотится за моими
публичными сервисами?



Внутри LAN

Кто уже находится
в моей сети?



В облачной среде

Пытаются ли использовать
скомпрометированные
ключи против меня?



Ставьте honeypot там, где хотите получить ответ.

Разное расположение — разная видимость
атак и разные инсайты.

MORE SIGNALS
LESS NOISE

CYBERSECURITY
IN ACTION

THREAT INTELLIGENCE
TURNS CHAOS INTO CONTEXT

COLLECT
ANALYZE
DETECT
STAY AHEAD

КАКУЮ ИНФОРМАЦИЮ СОБИРАЕТ HONEYPOT

Даже один тихий honeypot может дать ценную информацию об атакующих.

ORIGIN

Источник атаки

IP-адрес, владелец сети и страна, откуда пришла попытка.



CREDENTIALS

Учётные данные

Точные username и пароли, которые пытаются использовать.



COMMANDS

Команды

Все команды, которые вводит атакующий после успешного входа.



PAYLOADS

Полезная нагрузка

Скрипты, бинарные файлы и инструменты, которые загружают на систему.



TIMING

Время активности

Когда приходят, сколько времени остаются и как часто возвращаются.

2024-03-18	10:14:23	CONNECT
2024-03-18	10:15:01	LOGIN
2024-03-18	10:16:37	COMMAND
2024-03-18	10:20:11	DOWNLOAD
2024-03-18	10:45:03	DISCONNECT

Один тихий honeypot — и ты уже меняешь свои detection rules и blocklist.

Реальные атаки. Реальные поведенческие паттерны.
Больше контекста — лучше защита.

LESS NOISE
MORE INTEL

CYBERSECURITY
IN PRACTICE

REAL THREATS
REAL CONTEXT

OBSERVE
ANALYZE
ADAPT
STAY SECURE

РИСКИ И ПОДВОДНЫЕ КАМНИ

Honeypot — мощный инструмент, но у него есть свои особенности. Важно понимать риски.

ATTACK
LEARN
IMPROVE_

01

Становится опорной точкой

Плохо изолированный honeypot может быть использован как плацдарм для дальнейших атак в вашей сети.



02

Оставляет следы

Если приманка выглядит неестественно, опытные злоумышленники быстро её распознают и изменят тактику.



03

Оповещения никто не читает

Honeypot без ответственных и без процессов — это просто ещё один лог-файл, который никто не анализирует.



04

Правовые и policy ограничения

Запись сессий, перехват трафика и приманивание атакующих могут быть ограничены законодательством и внутренними политиками.



05

Уходит в забытьё

Заброшенный honeypot со старым баннером и уязвимостями может годами вводить в заблуждение и не приносить никакой пользы.



Понимание этих рисков помогает использовать honeypot эффективно.

Больше контекста — лучше детекция и защита.

DEPLOY SMART
CATCH MORE

PLAN
DEPLOY
LEARN
IMPROVE

ЧЕКЛИСТ РАЗВЁРТЫВАНИЯ HONEYPOT

Простые, но важные шаги, чтобы ваш honeypot давал максимум пользы и оставался незаметным.



01

Выделите отдельный сегмент

Размещайте honeypot в изолированном сетевом сегменте и по умолчанию блокируйте исходящий трафик (egress).



02

Сделайте правдоподобным

Используйте реалистичные баннеры, правдоподобные имена и некоторые фальшивые файлы, чтобы привлечь внимание атакующих.

```
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.6

login: admin
Password:
```

03

Не храните настоящие данные

Никогда не размещайте реальные клиентские или бизнес-данные в honeypot.



04

Отправляйте события на мониторинг

Интегрируйте honeypot с вашей SIEM/лог-платформой и настройте собственные alert rules.

```
2024-03-18 10:14:23 [HONEYPOT] SSH login attempt
2024-03-18 10:15:02 [HONEYPOT] File download
2024-03-18 10:16:37 [HONEYPOT] Command executed
2024-03-18 10:20:11 [HONEYPOT] New connection
```

05

Регулярно обновляйте

Обновляйте баннеры, файлы и версии, чтобы honeypot не выглядел заброшенным. Начните с небольшого, простого honeypot, прежде чем строить полноценную фальшивую сеть.

```
Updating...
Downloading banners...
Refreshing files...
Deployment complete.
```

Правильная настройка — больше данных и более качественные инсайты.

Хорошо настроенный honeypot превращает атаки в полезную информацию.

MORE VISIBILITY
STRONGER DEFENSE

CYBERSECURITY
IN PRACTICE

TURN ATTACKS
INTO INSIGHTS

DEPLOY
DETECT
LEARN
STAY AHEAD

КЛЮЧЕВЫЕ ВЫВОДЫ

Honeypot — простой инструмент
с большой ценностью, если использовать его правильно.

01

Узкая цель

Honeypot существует
только для того, чтобы
быть атакованным.



02

Нет легитимных пользователей

В honeypot не должно быть
настоящих пользователей,
поэтому любое взаимодействие
— это признак активности.

```
Login: root
Password: ***********
ACCESS DENIED
```

03

Больше контекста для анализа

Чем глубже уровень
взаимодействия, тем больше
разведданных (intel) вы получаете.
Планируйте это осознанно.

```
$ whoami
$ uname -a
$ cat /etc/passwd
$ wget http://...
$ ./exploit.sh
```

04

Те же срабатывания, но без шума

Honeypot генерирует те же
алерты, что и реальная система,
но без необходимости её
запускать и поддерживать.

Intrusion detected
203.0.113.45

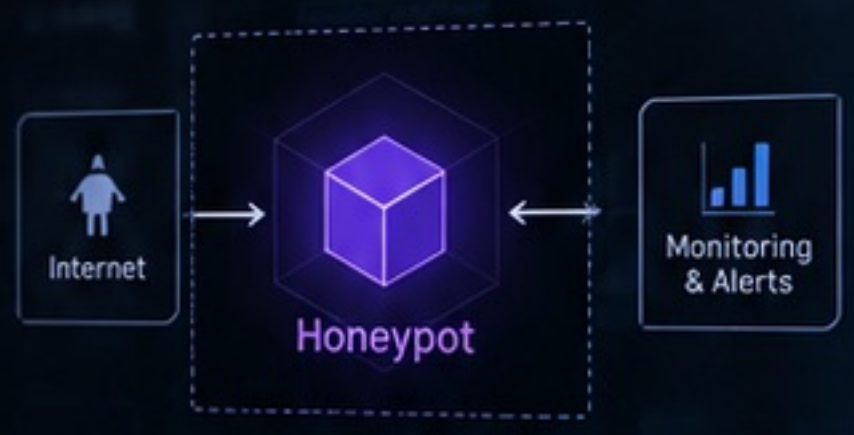
Intrusion detected
185.199.110.23

Intrusion detected
198.51.100.7

05

Изоляция, правдоподобие и наблюдение

Чтобы honeypot был эффективным,
ему нужны isolation, правдоподобная
среда и постоянный мониторинг.
Без одного из этих элементов
ценность резко падает.



Осознанный honeypot превращает атаки в полезные знания.

Больше инсайтов — сильнее защита.