positive technologies

pt

PT DEPHAZE

Система для безопасного внутреннего автопентеста

Проверит, как далеко сможет продвинуться хакер в вашей инфраструктуре

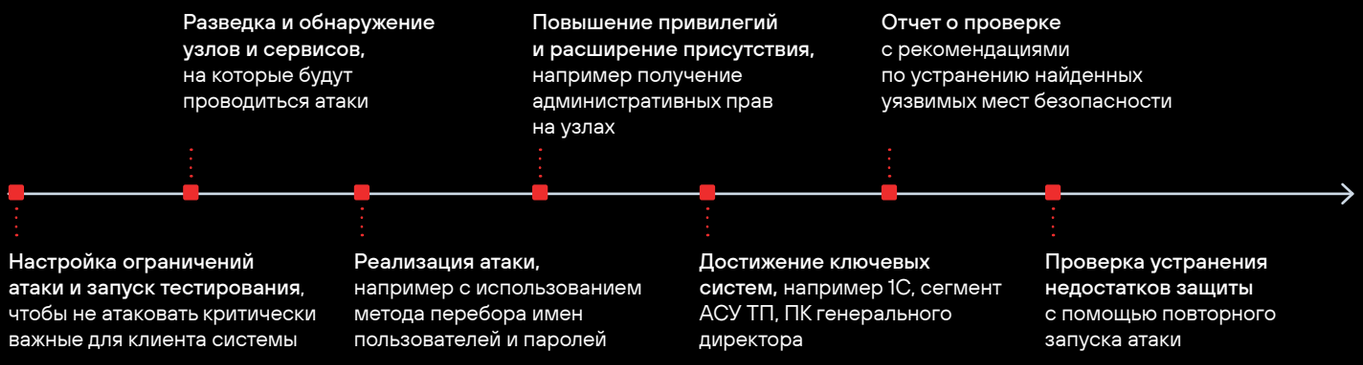
Автоматизация для регулярной оценки защищенности

Positive Technologies разработала решение **PT Dephaze**, позволяющее запускать пентест в автоматическом режиме и проверять устойчивость различных сегментов внутренней инфраструктуры к реальным угрозам в контексте возможных векторов атак. С его помощью можно управлять воздействием на критически важные активы и оценивать значимые риски безопасности.

Как работает PT Dephaze

Принцип работы PT Dephaze схож с ручным тестированием: продукт последовательно проверяет системы и их элементы на возможность добраться до критически важных данных, бухгалтерских приложений или систем управления промышленным оборудованием. Продукт использует те же техники и инструменты, что и хакеры, но делает это в автоматическом режиме, предоставляя в интерфейсе всю информацию о ходе тестирования.

Для запуска проверки пользователю нужно установить ПО на сервер, указать цели, выбрать режим согласования атаки и определить область тестирования. Целями могут быть информационные системы, приложения, устройства или недопустимые события. На основе полученных данных специалисты по кибербезопасности определяют приоритетные направления работы и оптимизируют стратегию защиты ИТ-систем.



Процесс тестирования инфраструктуры с помощью PT Dephaze

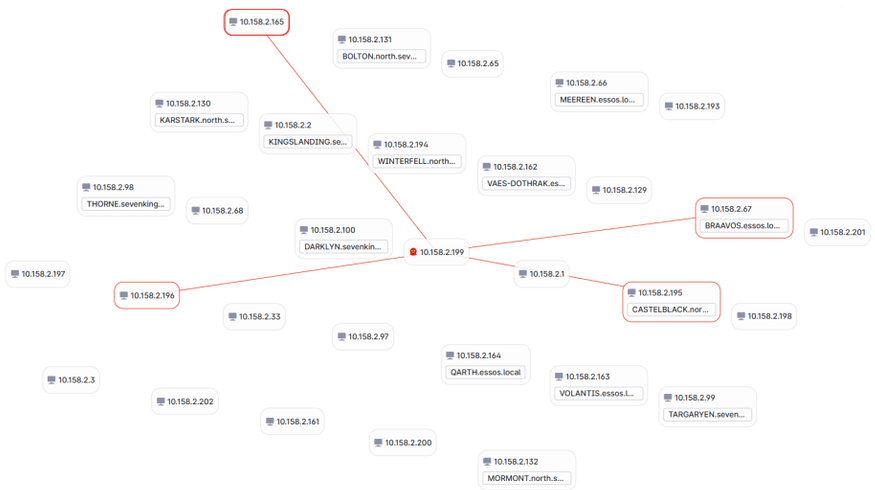
PT Dephaze поможет

- Определить векторы атак, которыми могут воспользоваться злоумышленники
- Выявить критически значимые риски безопасности
- Оптимизировать рутинные операции тестирования на проникновение
- Проверить корректность настройки средств защиты информации
- Подготовить инфраструктуру к ручному пентесту
- Приоритизировать недостатки безопасности для их своевременного устранения

Объективная проверка безопасности с экспертизой Positive Technologies

PT Dephaze тестирует инфраструктуру с использованием тех практик, которые используют реальные хакеры и пентестеры, демонстрируя службе ИБ потенциальный ущерб от действий злоумышленников. Продукт помогает превентивно проверить безопасность с помощью широкого спектра реальных методов взлома, фреймворка атак по матрице MITRE ATT&CK и набора этических эксплойтов. Автопентест позволяет посмотреть на инфраструктуру глазами злоумышленника, выявить и устранить уязвимые места защиты, которыми тот воспользуется в первую очередь.

PT Dephaze использует многолетний опыт Positive Technologies в тестировании на проникновение, проведении киберучений, программ багбаунти и разработке защитных продуктов. Это позволяет ему всегда достигать цель — находить уязвимые места в инфраструктуре компаний и помогать исправлять бреши в защите.



Как процесс тестирования выглядит в интерфейсе PT Dephaze

Экспертиза PT Dephaze основана на лучших практиках Positive Technologies

Pentest & red teaming
Более 20 лет в тестировании защищенности

Incident response & threat intelligence & antimalware lab
Тысячи расследованных инцидентов и проведенных анализов

Detection engineering
Более 25 продуктов для защиты

Standoff 365
Самое большое сообщество хакеров, платформа багбаунти и международная кибербитва

Сотни выявленных уязвимостей нулевого дня ежегодно
В ИТ-системах различных классов и типов, в том числе в продуктах Cisco, Citrix, IBM, Intel, Microsoft и VMware

Преимущества

- Безопасен для инфраструктуры, может работать в полностью контролируемом режиме и ограничивать атаки на критически важные системы
- Наглядно показывает результаты тестирования, позволяя ускорить процесс исправления недостатков защиты за счет понятных рекомендаций
- Основан на многолетнем опыте Positive Technologies в белом хакинге и проверке защищенности компаний
- Прост в эксплуатации, не требует длительного обучения и специальной квалификации сотрудников при использовании. Не требует установки на устройства

Автопентест без последствий

При проведении тестирования на проникновение в автоматическом режиме очень важно обеспечить безопасность, так как неконтролируемый взлом может привести к печальным последствиям. Вот почему PT Dephaze — в первую очередь управляемый автопентест, который минимизирует риски при проведении тестирования. Все действия, потенциально способные причинить реальный вред, требуют подтверждения пользователя для дальнейшего продвижения PT Dephaze внутри инфраструктуры. Можно выбрать, какие узлы точно не надо тестировать, какие атаки нужно согласовывать, а также задать важные узлы в качестве целей для продукта. PT Dephaze описывает, какие последствия могут наступить в случае успешной атаки. Так пользователь сможет оценить риски и остановить проверку. Безопасность реализована и с помощью возможности настраивать расширенный набор параметров атакующих действий. Кроме того, PT Dephaze позволяет настраивать интенсивность атаки, чтобы не нарушать работу основных бизнес-процессов.

Если продукт создает новую учетную запись с повышенными привилегиями, для нее автоматически генерируется уникальный и устойчивый к перебору пароль, что не дает злоумышленникам возможности использовать учетную запись в случае компрометации узла. PT Dephaze покажет изменения для последующего удаления созданных учетных записей.

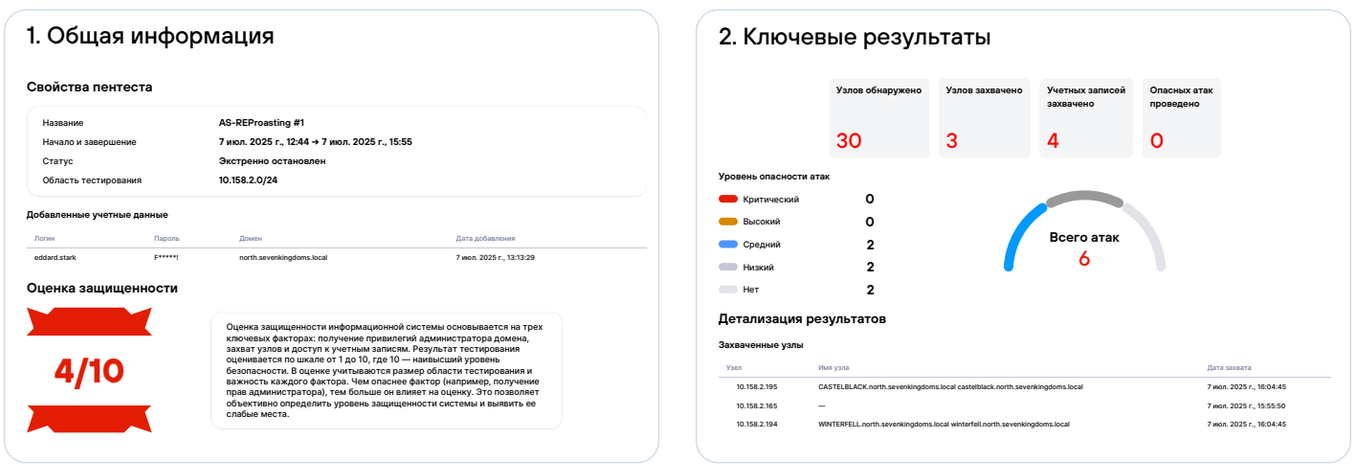
Безопасное тестирование с PT Dephaze

- Ограничение области тестирования
- Исключение критически важных бизнес-активов
- Выбор атакующих действий
- Журналирование всех действий продукта
- Настройка интенсивности атак
- Согласование опасных действий
- Экстренная остановка тестирования

Исправление уязвимых мест безопасности

PT Dephaze дает понимание, как реально могут атаковать инфраструктуру и какими векторами атак злоумышленники воспользуются в первую очередь. Он может попытаться получить высокие привилегии в ключевых системах, например в домене Active Directory, захватить домен и получить доступ к целевым системам, а также завладеть доступными учетными записями и узлами. Такой результат позволяет определить, какие узлы уязвимы и требуют немедленной защиты. Но недостаточно просто получить векторы компрометации от продукта, важно понимать, как исправить недостатки безопасности.

В ходе тестирования PT Dephaze не только показывает весь процесс атаки, но и формирует отчет с подробным описанием последствий, к которым может привести найденная уязвимость безопасности или ошибка конфигурации, а также предоставляет базовые рекомендации по их устранению и внедрению компенсирующих мер. Кроме того, система автопентеста указывает на возможные варианты мониторинга подобной нелегитимной активности в средствах защиты информации.



1. Общая информация

Свойства пентеста

Название	AS-REProasting #1
Начало и завершение	7 июл. 2025 г., 12:44 → 7 июл. 2025 г., 15:55
Статус	Экстренно остановлен
Область тестирования	10.158.2.0/24

Добавленные учетные данные

Логин	Пароль	Домен	Дата добавления
eddard.stark	F*****!	north.sevenkingdoms.local	7 июл. 2025 г., 13:13:29

Оценка защищенности

4/10

Оценка защищенности информационной системы основывается на трех ключевых факторах: получение привилегий администратора домена, захват узлов и доступ к учетным записям. Результат тестирования оценивается по шкале от 1 до 10, где 10 — наивысший уровень безопасности. В оценке учитываются размер области тестирования и важность каждого фактора. Чем опаснее фактор (например, получение прав администратора), тем больше он влияет на оценку. Это позволяет объективно определить уровень защищенности системы и выявить ее слабые места.

2. Ключевые результаты

Узлов обнаружено	Узлов захвачено	Учетных записей захвачено	Опасных атак проведено
30	3	4	0

Уровень опасности атак

Критический	0
Высокий	0
Средний	2
Низкий	2
Нет	2

Всего атак 6

Детализация результатов

Захваченные узлы

Узел	Имя узла	Дата захвата
10.158.2.195	CASTELBLACK.north.sevenkingdoms.local castelblack.north.sevenkingdoms.local	7 июл. 2025 г., 16:04:45
10.158.2.165	—	7 июл. 2025 г., 15:55:50
10.158.2.194	WINTERFELL.north.sevenkingdoms.local winterfell.north.sevenkingdoms.local	7 июл. 2025 г., 16:04:45

Отчет с результатами тестирования

Техническая спецификация

Аппаратные требования к серверу PT Dephaze

Параметр	Минимальные требования	Рекомендуемые требования
Виртуальный процессор	8 ядер	8 ядер (и больше)
Физический процессор	Intel Xeon серии E3 (или аналогичные)	Intel Xeon Gold (или более поздние)
Память (ОЗУ)	16 ГБ	32 ГБ
Твердый накопитель (SSD)	100 ГБ (или HDD со скоростью вращения 10 000 об./мин или выше)	200 ГБ

Аппаратные требования к атакующему узлу

Параметр	Минимальное значение	Рекомендуемое значение
Виртуальный процессор	4 ядра	8 ядер
Память (ОЗУ)	8 ГБ	16 ГБ
Жесткий диск (HDD)	40 ГБ	—
Твердый накопитель (SSD)	—	100 ГБ

Атакующие действия

Поддержка систем	Windows XP, 7, 10, 11; Windows Server 2003, 2008, 2012, 2016, 2019, 2022, 2025; клиентские и серверные Linux: Debian 6–12, Ubuntu 12–23
Типы атакующих действий	**Сетевые атаки** Проведение атак, связанных с эксплуатацией уязвимостей протоколов LLMNR, NBT-NS, mDNS, и атак типа NTLM Relay для перехвата аутентификационных данных. Выполнение MITM-атак на SMB. Получение доступа к SMB, RDP, SSH, WinRM (протоколам удаленного управления) с использованием различных типов учетных данных и протоколов аутентификации. **Атаки на Active Directory и Windows** Анализ доменных структур, распыление паролей, извлечение данных через LDAP, Kerberoasting, LAPS и эксплуатацию уязвимостей (MS17-010, NoPAC, ZeroLogon, PrintNightmare и PetitPotam). **Извлечение учетных данных** Получение логинов и паролей из памяти LSASS, реестра Windows, в том числе через NTLM-сессии. **Повышение привилегий** Использование уязвимостей (CVE-2021-1675, ESC15 и других) или политик (AlwaysInstallElevated) для расширения прав до уровня привилегий системы или администратора. **Атаки на приложения** Обнаружение веб-сервисов (GitLab), баз данных (PostgreSQL, Microsoft SQL Server) и FTP-серверов и их тестирование

PT Dephaze: думает как хакер, действует как пентестер

Уровень защищенности компаний напрямую связан с их способностью думать и действовать как злоумышленник — и делать это до того, как будет совершена атака. Понимание, каким будет следующий шаг хакера, необходимо для выстраивания комплексной информационной защиты.

PT Dephaze позволяет увидеть, как хакер будет перемещаться внутри инфраструктуры, определить уязвимости безопасности, которыми он воспользуется в первую очередь, и посмотреть, как отреагируют на его действия средства защиты. Зная это, специалисты по ИБ могут контролировать киберустойчивость компании и постоянно оптимизировать эффективность защиты, сокращая время на устранение недостатков безопасности.

Протестировать PT Dephaze