# ОПРЕДЕЛЕНИЕ РИСКОВ И УЯЗВИМОСТЕЙ ДЛЯ ЛОКАЛЬНЫХ ПРИВИЛЕГИРОВАННЫХ УЧЁТНЫХ ЗАПИСЕЙ С ПОМОЩЬЮ РЕШЕНИЯ CYBERARK ZBANG


## ВВЕДЕНИЕ

Сегодня многие организации работают в гибридной облачной среде, в которой многие критически важные данные и приложения уровня Tier0 всё ещё находятся в традиционных локальных средах. Помимо традиционных неуправляемых привилегированных учётных записей и учётных данных, например, учётных записей локальных администраторов, учётных записей администраторов домена, учётных записей приложений и баз данных, существует множество других (нетрадиционных) привилегированных рисков и уязвимостей, которые необходимо устранить, чтобы снизить вероятность успешной кибератаки. CyberArk zBang - это инструмент с открытым исходным кодом, предназначенный для создания углублённой оценки рисков. Он автоматизирует и унифицирует ручное сканирование, выявляющее риски безопасности привилегированного доступа в локальных средах. Разработанный командой CyberArk Threat Research Labs,

Данный инструмент помогает специалистам по безопасности во время сканирования сети обнаруживать и визуализировать критические риски, связанные с привилегированными учётными записями и учётными данными.

## ОСНОВНЫЕ МОМЕНТЫ

- Выявление потенциальных векторов атак и повышение безопасности сети
- Для выполнения сканирования инструменту требуется только доменная учётная запись пользователя с разрешением на чтение.
- Стандартное время сканирования в сети с 1 000 машин составляет около 7 минут.
- Инструмент представляет собой бесплатное решение с открытым исходным кодом: https://github.com/cyberark/zBang

## ФУНКЦИОНАЛ СКАНИРОВАНИЯ

zBang состоит из 5 разных модулей сканирования:

1. **Сканирование ACLight:** просматривает привилегированные учётные записи, которые могут не входить в известные привилегированные группы организации, но все же имеющие очень важные права доступа.
2. **Сканирование Sceleton Key:** Sceleton Key - это разновидность вредоносного ПО, которое заражает доменные контроллеры и позволяет проникнуть в сеть. Зараженный контроллер позволяет злоумышленнику получать доступ к каждой учётной записи домена с предварительно установленным паролем с резервным копированием и установленным вредоносной программой.
3. **Сканирование истории SID:** атрибут истории SID - это атрибут, который может быть назначен каждой учётной записи домена и может использоваться в случае миграции учётной записи между двумя доверенными доменами. Атрибут может использоваться злоумышленниками для повышения привилегий.
4. **Сканирование RiskySPNs:** инструмент сканирует доменный контроллер на наличие развёрнутых служб, работающих с учётными записями людей с высокими привилегиями. Эти службы могут стать целью проникновения злоумышленника для извлечения учётных данных и использования привилегированной учётной записи в злонамеренных целях..
5. **Mystique-сканирование:** обнаруживает в сети опасные конфигурации делегирования. Рискованные конфигурации делегирования могут быть использованы злоумышленниками.

| | | |
|---|---|---|
| 1 | Сканирование | ACLight |
| | Основная ценность | **Обнаружение самых важных привилегированных учётных записей, которые необходимо защитить** |
| | Результат сканирования | Визуализация обнаруженных привилегированных учётных записей, включая теневых администраторов, с прямыми назначениями разрешений конфиденциального ACL. Каждая учётная запись будет представлена в виде графика с её разрешениями. |
| | Рекомендации CyberArk | Три вопроса по каждой обнаруженной учетной записи:<br>1. Аккаунт распознан? Злоумышленник может создать новые скрытые учётные записи администратора.<br>2. Нужны ли для учётной записи нужны наивысшие привилегии во всем домене? Управление сетью должно осуществляться по методологии «наименьших привилегий».<br>3. Правильно ли защищена учётная запись? Привилегированные учётные записи нуждаются в сквозной защите: надёжные пароли с частой ротацией, мониторинг сеансов, контрольный журнал действий и т. д. |
| 2 | Сканирование | Skeleton Key |
| | **Основная ценность** | **Обнаружение зараженных доменных контроллеров** |
| | Результат | Визуализация списка контроллеров домена, зараженных вредоносной программой Skeleton Key . |
| | Рекомендации CyberArk | Если сканирование обнаруживает зараженный контроллер домена, необходимо инициировать процесс реагирования на инцидент. |
| 3 | Сканирование | SID History |
| | **Основная ценность** | **Обнаружение скрытых привилегий во вторичном SID учётных записей домена** |
| | Результат | Визуализированный список учётных записей с историей SID (вторичный SID) |
| | Рекомендации CyberArk | При обнаружении вторичной привилегированной SID, необходимо проверить её легитимность. Если она существует, тогда эту учётную запись следует приоритезировать и передать для управления в CyberArk. Это обязательно надо сделать, если вторичный SID учётной записи является привилегированным, а основной - нет. Это хорошо известный метод, который часто используется для обеспечения устойчивости целевой сети и скрытого выполнения вредоносных действий. |
| 4 | Сканирование | RiskySPNs |
| | **Основная ценность** | **Обнаружение слабых конфигураций SPN, способных привести к краже учётных данных администраторов домена** |
| | Результат | Визуализированный список подверженных риску сервисов и счетов. |
| | Рекомендации CyberArk | Все обнаруженные учётные записи пользователей с SPN (учётная запись зарегистрированного пользователя) должны быть защищены. Если учётная запись скомпрометирована, то же самое происходит и с зарегистрированной службой. Необходимо преобразовать SPN для регистрации под учётной записью компьютера, а не под учётной записью пользователя. Более того, если у привилегированной учётной записи есть SPN (например, учетная запись администратора домена), регистрация SPN (услуги) должна быть преобразована в непривилегированную учётную запись. Иначе злоумышленник может легко запросить TGS (билет Kerberos) для этого SPN, а затем выполнить полное шифрование билета. Извлечённый ключ является паролем привилегированной учётной записи администратора домена этого SPN. Это мощный метод для злоумышленников с целью повышения привилегий в целевой сети. |
| 5 | Сканирование | Mystique |
| | **Основная ценность** | **Обнаружение рискованных конфигураций делегирования в сети** |
| | Результат | Визуализированный список вариантов делегирования доменов и их риски. |
| | Рекомендации CyberArk | Необходимо пересмотреть разрешения на делегирование в сети. Действительно ли необходимы разрешения на делегирование? Отключите старые и неиспользуемые учетные записи делегирования.<br>В частности, отметьте рискованные типы делегирования «Без ограничений» и «Ограничено переходом по протоколу». Преобразуйте «неограниченное» делегирование в «ограниченное» делегирование, чтобы оно было разрешено только для определенных необходимых служб. Если возможно, тип делегирования «Protocol Transition» должен быть повторно подтвержден и отключён. |

## ТРЕБОВАНИЯ К ПРОЦЕДУРЕ ВЫПОЛНЕНИЯ

1. Запустите zBang с машины, подключённой к домену (любой версии ОС Windows).
2. Запустите zBang под любым доменным именем. Сканирование не требует каких-либо дополнительных привилегий, так как инструмент выполняет только запросы для чтения к контроллеру домена.
3. PowerShell версии 3 или выше и .NET 4.5 (примечание: по умолчанию в Windows 8/2012 и выше).

## СЛЕДУЮЩИЙ ШАГ

CyberArk zBang - одно из дополнительных решений для сканирования, помогающих выявить уровень привилегированного риска организации. Этот инструмент можно использовать для того, чтобы специалисты безопасности и проверяющие могли выявлять дополнительные векторы атак в сети, а также помогать поддерживать бизнес-модель для реализации программы безопасности привилегированного доступа. Начните сегодня, обратившись к представителю CyberArk по работе с клиентами или к Краткому руководству по началу работы на GitHub: https://github.com/cyberark/zBang