



Превращаем ВН в швейцарскую собаку

BloodHound

OpenGraph

Cypher

Attack paths

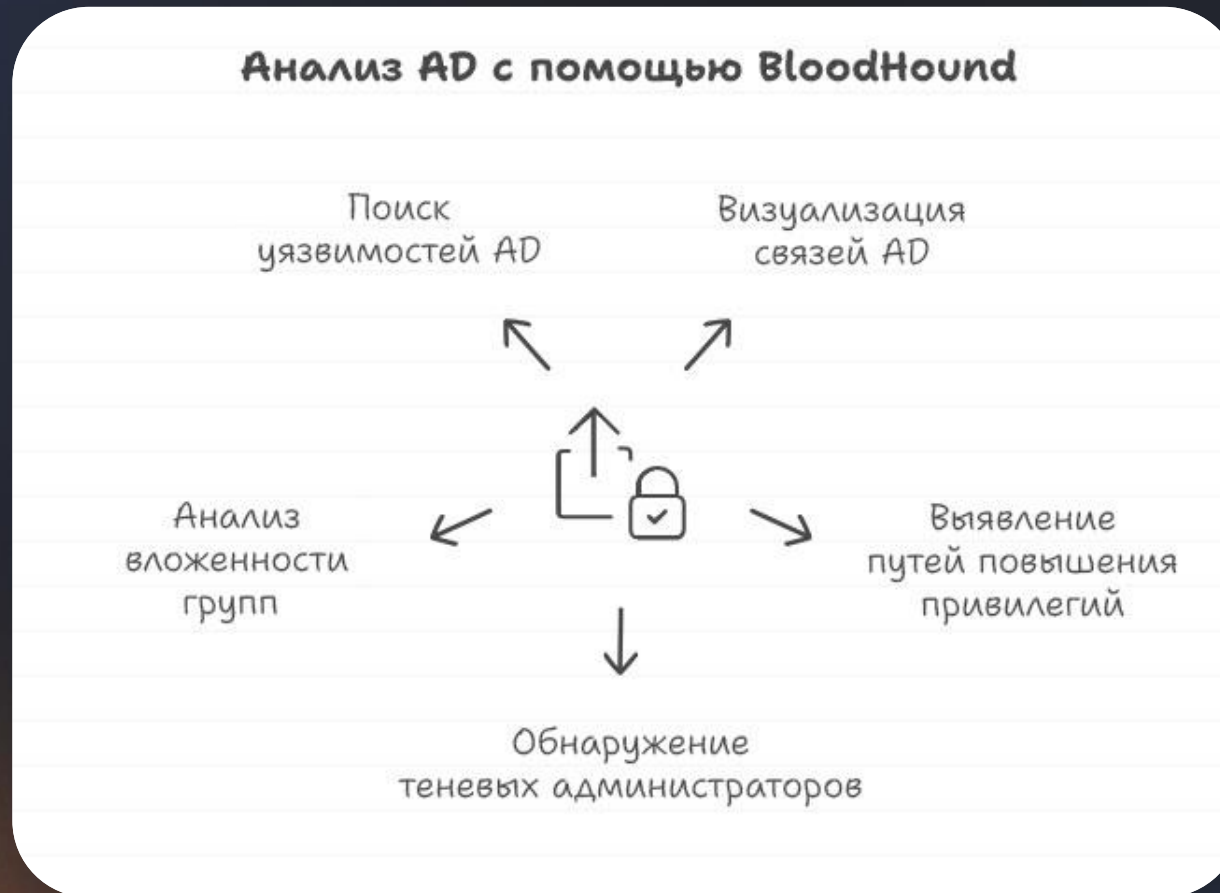
Коллекторы

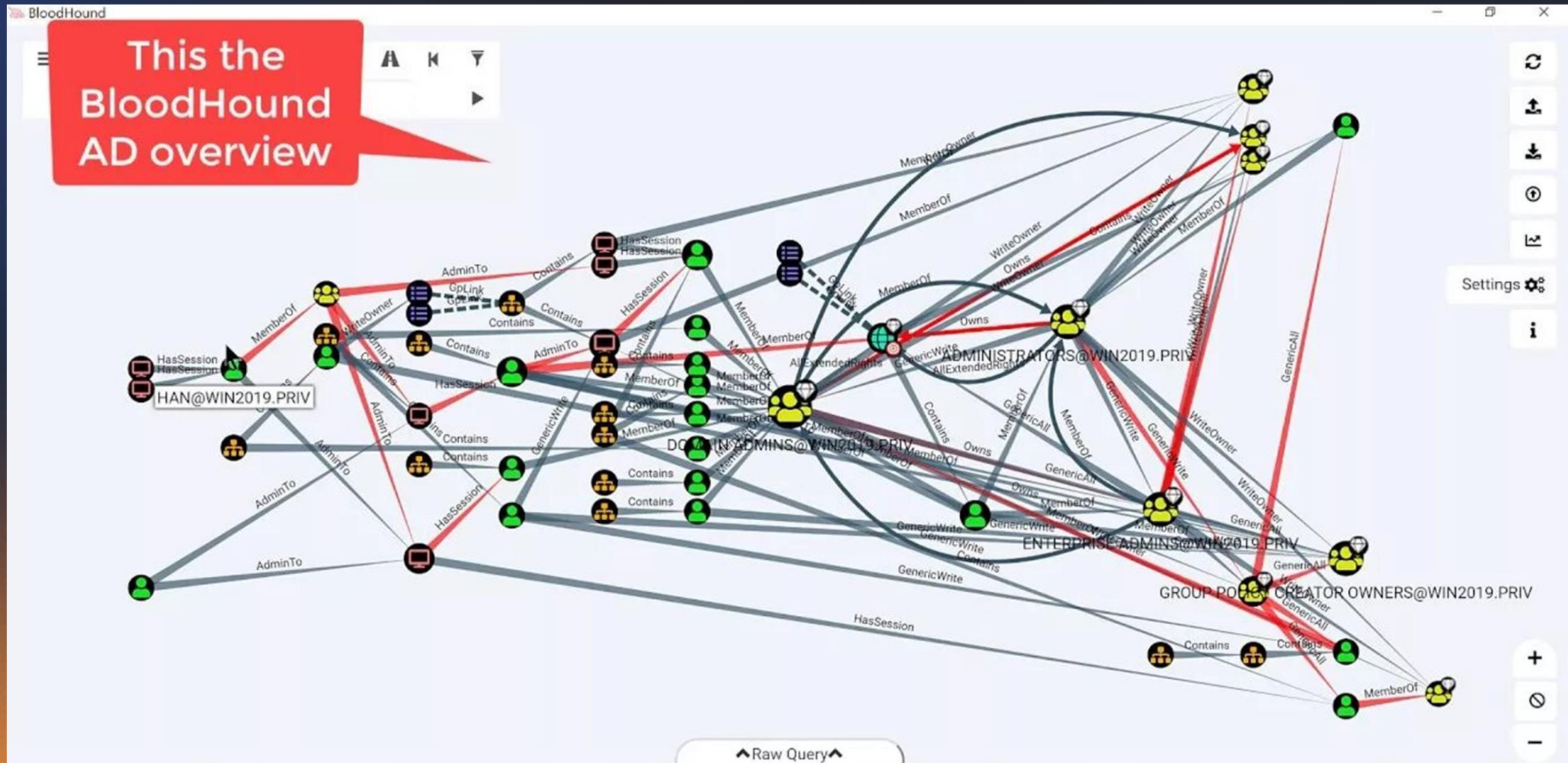
Константин Захаров

Младший исследователь
АО «Перспективный мониторинг»



Принцип работы и преимущества





С чего такой интерес к ВН?

BloodHound стал удобной точкой сборки разных источников данных об инфраструктуре

- ✓ За последнее время появилось много инструментов и коллекторов вокруг BloodHound
- ✓ Появилась потребность анализировать не только классическую Active Directory
- ✓ OpenGraph позволяет добавлять новые типы объектов и связей без переписывания BloodHound
- ✓ Для российских инфраструктур отдельно важны FreeIPA/IdM и смешанные среды

01 Ручные методы добавления информации

Исследователь сам формулирует гипотезы, пишет Surfer-запросы и добавляет недостающие сущности

Ручные методы добавления информации

Исследователь сам формулирует гипотезы,
пишет Surfer-запросы и добавляет недостающие сущности



Примеры Cypher

На слайде — демонстрация принципа: добавляем свойства, связи и проверяем влияние на пути атаки

```
// Password Spray: пометить пользователя как
owned
MATCH (u:User)
WHERE u.objectid IN ["ObjectID"]
SET u.owned = true,
    u.ClearTextPassword = "Spring2026!"
RETURN u.objectid, u.owned;
```

```
// Повторное использование пароля
MATCH (u1:User), (u2:User)
WHERE u1.ClearTextPassword =
    u2.ClearTextPassword
    AND id(u1) < id(u2)
MERGE (u1)-[:SharePasswordWith]->(u2)
RETURN u1.objectid, u2.objectid;
```

☒ Auto-run selected query

```
1 MATCH p=(u1:User)-[:WriteUserAccountControl]-
  →(u2:User)
2 RETURN p
3 LIMIT 10;
```

Tag ▾

Save ▾

i

Run ▶



S-1-5-21-3100864409-...
Active Directory | User

WriteUserAccountControl



S-1-5-21-3100864409-...
Active Directory | User



S-1-5-21-3100864409-1979241233-3334073533-34650
Active Directory | User

Node Type: User

Object ID:
S-1-5-21-3100864409-1979241233-3334073533-34650

Clear Text Password: Spring2026!

Last Seen by BloodHound: 2026-05-12 04:11 EDT (GMT-0400)

Owned: TRUE

Testname: TEST_USER_2



S-1-5-21-3100864409-...
Active Directory | User

SharePasswordWith

SharePasswordWith



S-1-5-21-3100864409-...
Active Directory | User

SharePasswordWith



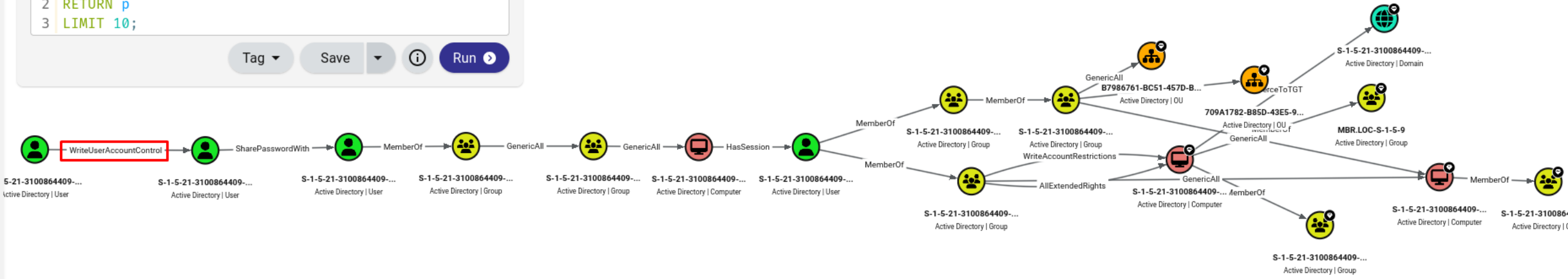
S-1-5-21-3100864409-...
Active Directory | User

☒ Auto-run selected query

```
1 MATCH p=(u1:User)-[:WriteUserAccountControl]-
  →(u2:User)-[*1..8]→(t:Tag_Tier_Zero)
2 RETURN p
3 LIMIT 10;
```

Tag ▼

Save

Run 

Книга Неверова



Статья Ardent101

Автоматизаторы и утилиты вокруг BloodHound



AD Miner

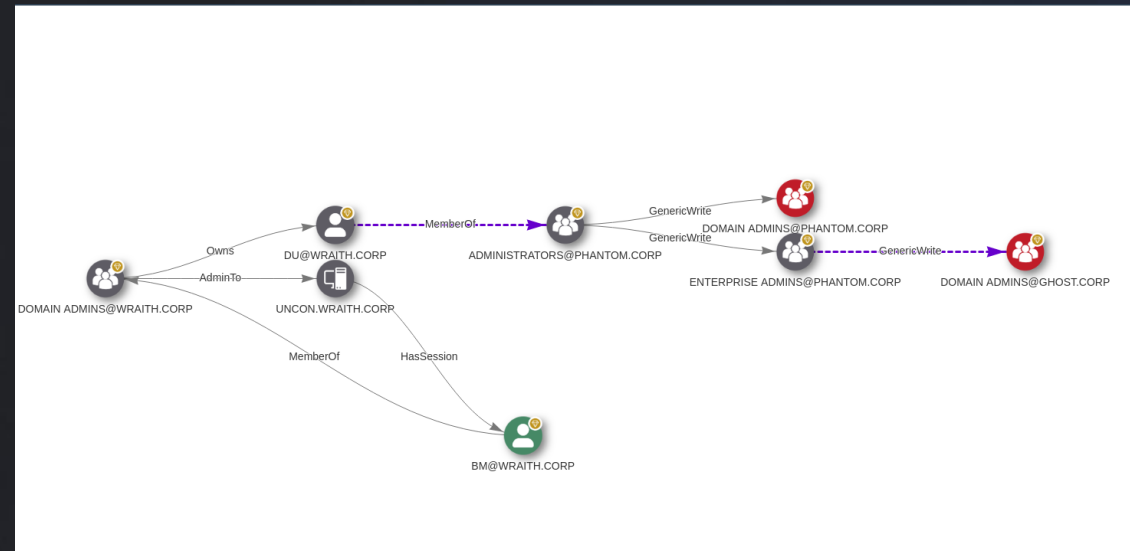
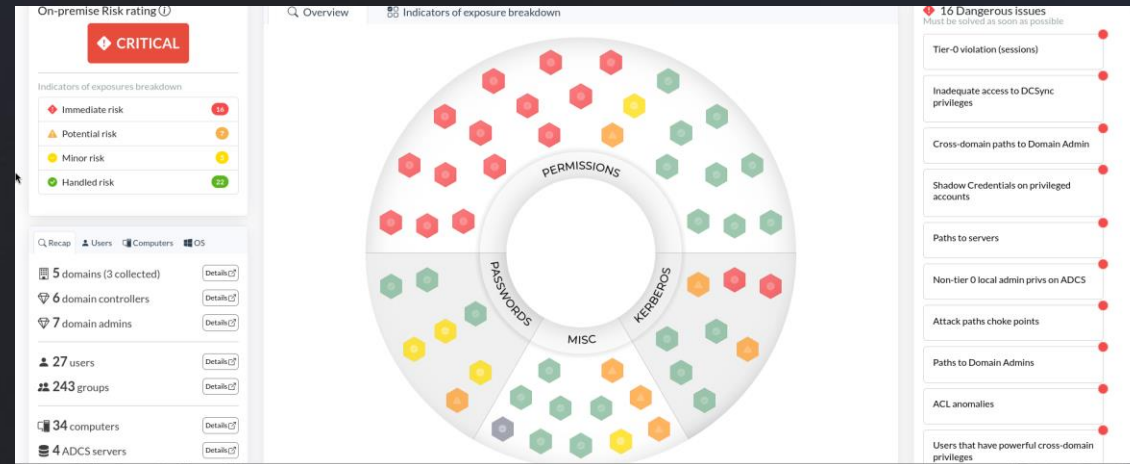
Генерация отчёта по данным BloodHound

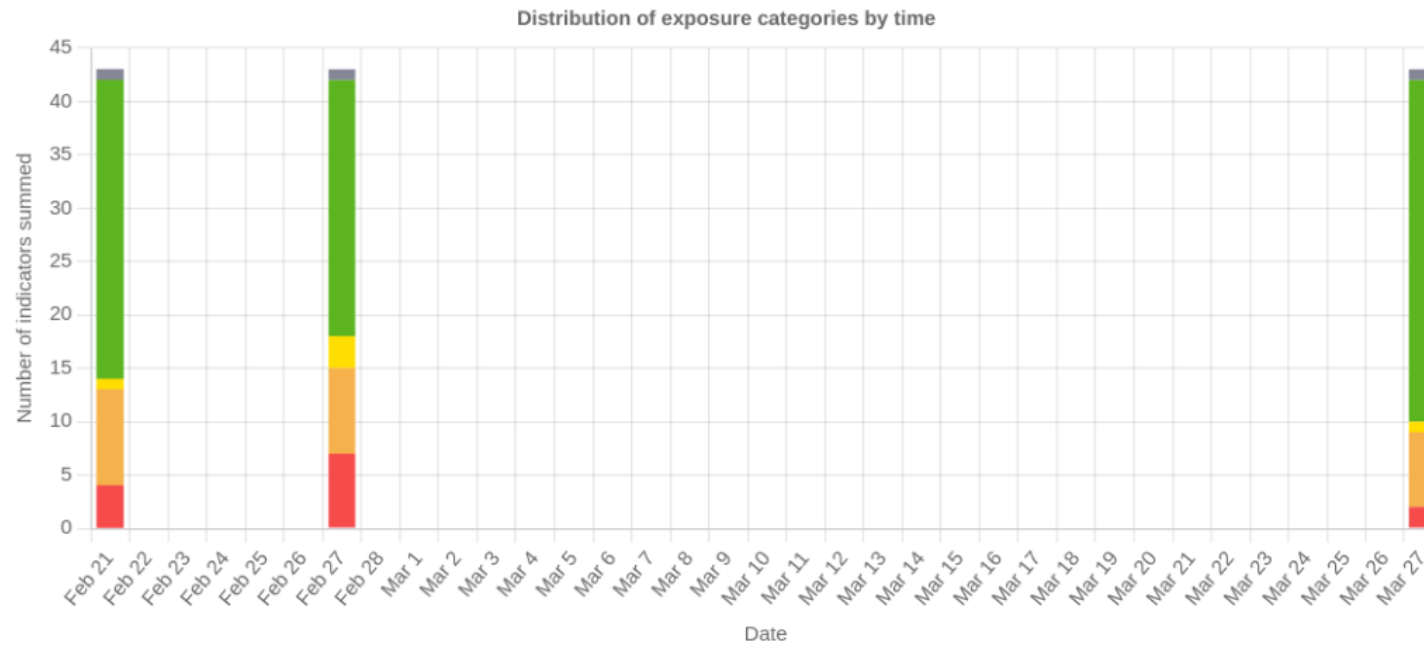
Как работает

Подключается к Neo4j и автоматически выполняет набор Cypher-проверок по AD/Entra ID

Практическая польза

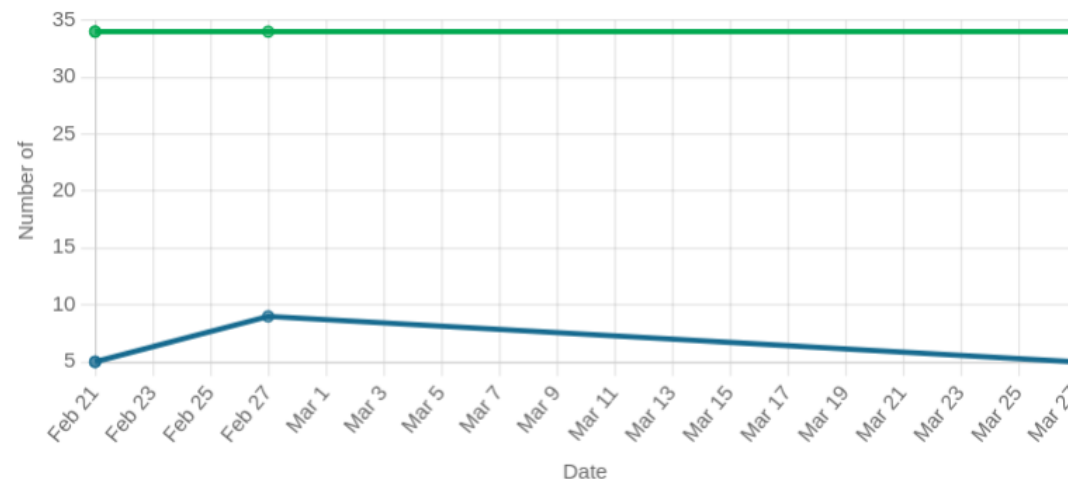
Формирует статический web-отчёт с категориями риска, графиками, списками объектов и режимом evolution для сравнения нескольких запусков





General statistics

- ☐ Domains
- ☐ Domain controllers
- ☐ Domain admins
- ☒ Users
- ☐ Groups
- ☒ Computers



Users Computers

ImproHound

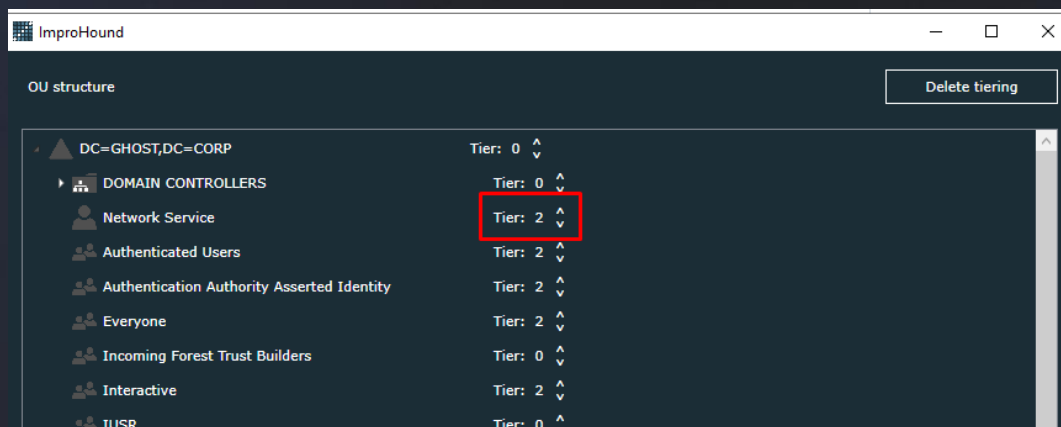
аудит Tier-модели

Как работает

Проверяет, соблюдается ли модель административных уровней Tier 0/1/2

Практическая польза

Полезен для поиска нарушений изоляции: когда объект низкого уровня может влиять на более привилегированный сегмент



tiering-violations-202605151242219812 - Excel

Поиск

Файл Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид Справка

Вставить Вырезать Копировать Буфер обмена Шрифт Выравнивание Число Ячейки

Условное форматирование Форматировать как таблицу Стили

Вставить Удалить Формат

ВОЗМОЖНА ПОТЕРЯ ДАННЫХ При сохранении книги в формате с разделителями-запятыми (CSV-файл) некоторые возможности могут быть потеряны. Если вы не хотите терять эти возможности, сохраните ее в формате файла Excel. Больше не показывать

	A	B	C	D	E	F	G	H	I
	SourceTier	SourceType	SourceName	SourceDistinguishedname	Relation	IsInherited	TargetTier	TargetType	TargetName
1	Tier2	Group	ORGANIZATION MANAGEMENT@W.CN=ORGANIZATION MANAGEMENT,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=CORP	GenericAll	False	True	Tier1	OU	MICROSOFT EXCHANG
2	Tier2	Group	ORGANIZATION MANAGEMENT@W.CN=ORGANIZATION MANAGEMENT,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=CORP	GenericAll	True	True	Tier1	Group	EXCHANGE SERVERS@
3	Tier2	Group	EXCHANGE TRUSTED SUBSYSTEM.CN=EXCHANGE TRUSTED SUBSYSTEM,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=CORP	AddMember	True	True	Tier1	Group	EXCHANGE SERVERS@
4	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	EXCHANGE SERVERS@
5	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	ADLocalGroup	WINDOWS AUTHORIZA
6	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	RAS AND IAS SERVERS
7	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	PERFORMANCE LOG U
8	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	TERMINAL SERVER LO
9	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	DENIED RODC PASSW
10	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	RDS ENDPOINT SERVE
11	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	PERFORMANCE MONIT
12	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	RDS REMOTE ACCESS
13	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	EVENT LOG READERS@
14	Tier2	Group	ORGANIZATION MANAGEMENT@W.CN=ORGANIZATION MANAGEMENT,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=CORP	GenericAll	False	True	Tier1	Group	\$141000-LDV9MS90T
15	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	\$141000-LDV9MS90T
16	Tier2	Group	EXCHANGE WINDOWS PERMISSIC CN=EXCHANGE WINDOWS PERMISSIONS,OU=MICROSOFT EXCHANGE SECURITY GROUPS,DC=WRAITH,DC=COI	AddMember	True	True	Tier1	Group	EXCHANGE-ADMIN@
17	Tier2	Group	TIER2SUPPORT@PHANTOM.CORP.CN=TIER2SUPPORT,OU=TIER1,DC=PHANTOM,DC=CORP	MemberOfLocalGroup	True	True	Tier0	ADLocalGroup	ADMINISTRATORS@PH
18	Tier2	Group	TIER2SUPPORT@PHANTOM.CORP.CN=TIER2SUPPORT,OU=TIER1,DC=PHANTOM,DC=CORP	AdminTo	True	True	Tier0	Computer	DC01.PHANTOM.CORP
19	Tier2	ADLocalGroup	USERS@PHANTOM.CORP.CN=USERS,CN=BUILTIN,DC=PHANTOM,DC=CORP	LocalToComputer	True	True	Tier0	Computer	DC01.PHANTOM.CORP
20	Tier2	ADLocalGroup	PRE-WINDOWS 2000 COMPATIBL CN=PRE-WINDOWS 2000 COMPATIBLE ACCESS,CN=BUILTIN,DC=PHANTOM,DC=CORP	LocalToComputer	True	True	Tier0	Computer	DC01.PHANTOM.CORP
21	Tier2	ADLocalGroup	GUESTS@PHANTOM.CORP.CN=GUESTS,CN=BUILTIN,DC=PHANTOM,DC=CORP	LocalToComputer	True	True	Tier0	Computer	DC01.PHANTOM.CORP
22	Tier2	Group	HR@PHANTOM.CORP.CN=HR,OU=GROUPS,OU=TIER1,DC=PHANTOM,DC=CORP	AddMember	True	True	Tier0	Group	ENTERPRISE READ ON

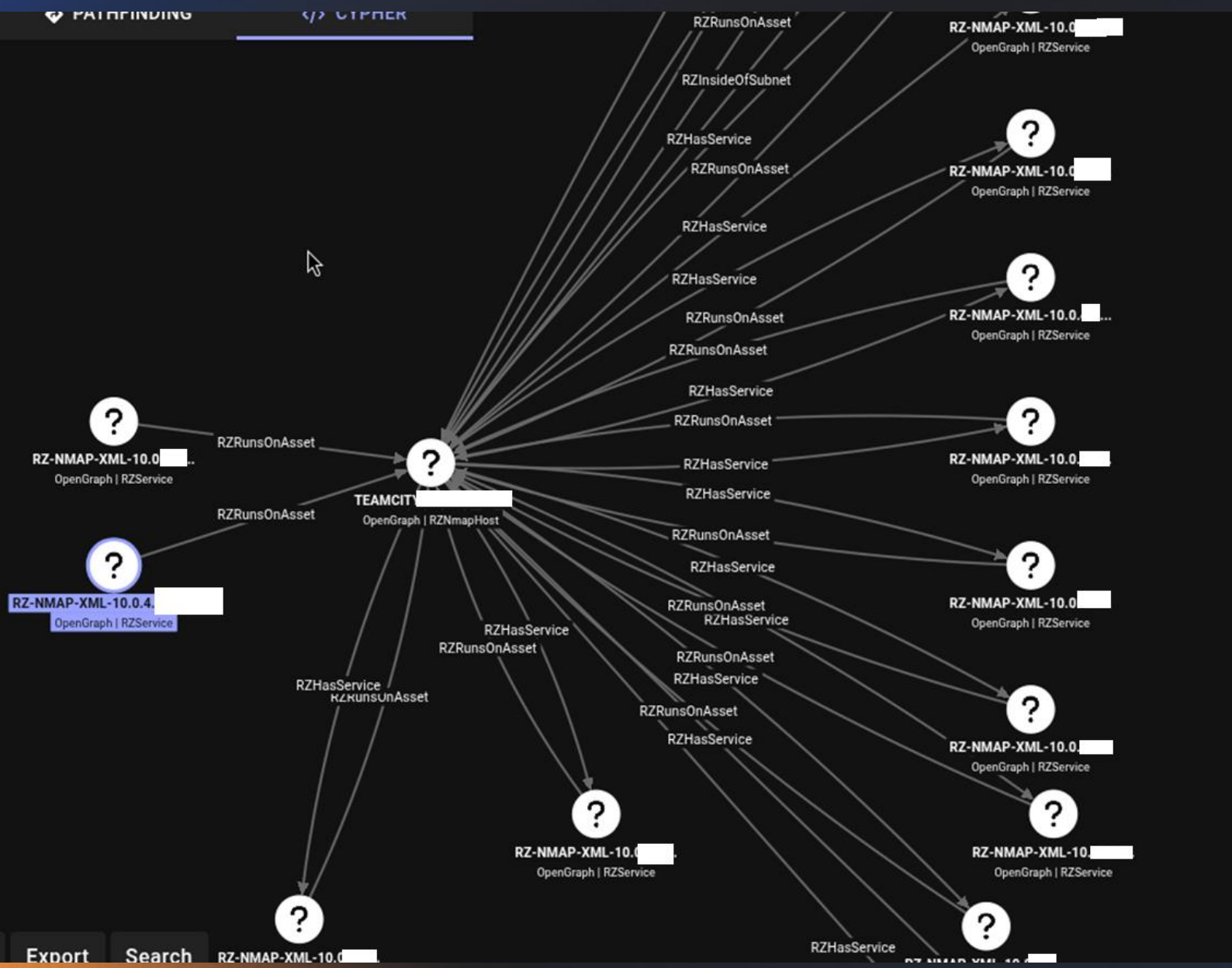
runZeroHound

Это один из самых полезных инструментов подборки: он добавляет в **BloodHound** данные из популярных сканеров и связывает её с векторами атаки.

Благодаря этому видно не только кто к чему имеет доступ, но и какие активы, сервисы и уязвимости действительно могут участвовать в цепочке атаки.

Источник данных	Что извлекается
runZero	Полная модель активов: атрибуты, сервисы, IP, MAC, домены, VLAN
Nmap	IP, MAC, hostnames, OS, сервисы, SSH-ключи, TLS-сертификаты, SMB GUID, SNMP Engine ID, traceroute hops
Nessus	IP, MAC, hostnames, OS, сервисы, SSH-ключи, TLS-сертификаты, SMB GUID, SNMP Engine ID, traceroute hops
OpenVAS / GVM	IP, MAC, hostnames, OS, сервисы, SSH-ключи, TLS-сертификаты, SMB GUID, SNMP Engine ID
Qualys VM scan	IP, MAC, hostnames, OS, сервисы, SSH-ключи, TLS-сертификаты, SMB GUID, SNMP Engine ID
Masscan	IP, открытые порты, service banners
Shodan	IP, hostnames, OS, сервисы, TLS-сертификаты, SSH-ключи, уязвимости
NetBox	IP, hostnames, device types, roles, platforms, sites, racks
snmpwalk	IP, MAC, hostnames, OS, SNMP Engine ID, ARP cache, MAC table





RZ-NMAP-XML-10.0.4.13-SVC-4

Object Information

Node Type:	RZService
Display Name:	443/tcp
Object ID:	RZ-NMAP-XML-10.0.4.13-SVC-4
Address:	10.0.4.13
Attr Service Name:	http
Last Seen by BloodHound:	2026-08-10 09:40 EDT (GMT-0400)
Port:	443
Primary Kind:	RZService
Product:	nginx
Protocol:	tcp

BLOODHOUND
COMMUNITY EDITION

+

Q SEARCH

PATHFINDING

</> CYPHER

Explore

Privilege Zones

Quick Upload

Profile

Administration

API Explorer

Docs and Support

Try BH Enterprise

Dark Mode

Log Out

?

RZ-OPENVAS-212.40.19...

OpenGraph | RZOpenVASHost

?

RZ-NETWORK-212.40.19...

OpenGraph | RZNetwork

?

RZ-VULN-OPENVAS-1.3....

OpenGraph | RZVuln

?

RZ-OPENVAS-212.40.19...

OpenGraph | RZService

RZSubnetContains

RZInsideOfSubnet

RZVulnAsset

RZHasVuln

RZRunsOnAsset

RZHasService

Hide Labels

Layout

Export

Search

GPOHound



Как работает

Инструмент для анализа групповых политик Active Directory из SYSVOL

Практическая польза

По сути, это автоматизация ручного анализа GPO: вместо того чтобы самому читать XML-файлы политик и вручную добавлять связи в Neo4j, можно получить уже структурированный результат



Rakound

интерактивная консоль для Neo4j-базы ВН

Как работает

Работает с готовой базой BloodHound и запускает встроенные команды статистики и поиска

Практическая польза

Позволяет быстро смотреть Domain/Enterprise Admins, локальных админов, LAPS-права, password never expires и другие проверки.

Его основная цель — упростить визуализацию данных Bloodhound.

Он позволяет получать доступ к незначительным данным, таким как пароли, хранящиеся в Active Directory

Ключевые элементы

console

queries

Neo4j

post-processing



```

(rakound_env)kali@kali: ~/Rakound
Session Actions Edit View Help
(rakound_env)kali@kali: ~/Rakound x kali@kali: ~/runZeroHound x

+-----+-----+
Found 0 occurrence(s)

> admin administrators
+-----+-----+
| account | status |
+-----+-----+
| ADMINISTRATOR@GHOST.CORP | True |
+-----+-----+

Found 1 occurrence(s)

> admin
+-----+-----+
| account | status |
+-----+-----+
| ADMINISTRATOR@GHOST.CORP | True |
+-----+-----+

Found 1 occurrence(s)

> password userpassword
+-----+-----+-----+-----+
| account | userpassword | status | type |
+-----+-----+-----+-----+
| BH@GHOST.CORP | Password123! | True | Tag_Tier_Zero |
+-----+-----+-----+-----+

Found 1 occurrence(s)

> admin domain
+-----+-----+
| account | status |
+-----+-----+
| BH@GHOST.CORP | True |
+-----+-----+
| TOM@GHOST.CORP | False |
+-----+-----+
| WALTER@GHOST.CORP | False |
+-----+-----+
| ADMINISTRATOR@GHOST.CORP | True |
+-----+-----+

Found 4 occurrence(s)

> computer obsolete

```



lj with live data

ample graph that demon
y patterns.

es in cross-referenced by

BloodHoundOperator

PowerShell- клиент API BloodHound

Как работает

Это консольная утилита, подключается к БД Neo4j. По сути работает как органайзер cypher запросов.

Вы вводите команду в терминале и получаете ответ от БД, не прописывая длинный cypher-запрос.

Ключевые элементы

PowerShell

REST API

BHcypher

CE/Enterprise

Практическая польза

Автоматизирует вывод сессии, API-ключи, Cypher-запросы, группы узлов, импорт и повторяемые операционные действия.



BloodHound Penetrator 2000

чек-листы и Obsidian-отчёты

Как работает

Подключается к Neo4j,
выполняет запросы из
queries.json и ownedqueries.json

Практическая польза

Преобразует находки
в Markdown-отчёт, чек-лист и трекер
прогресса для Obsidian; проверки
легко расширять

Ключевые элементы

queries.json

Owned

Obsidian

checklist

```
{ "name": "Kerberoasting",
  "type": "Nodes",
  "query": "MATCH (u:User {hasspn:true}) RETURN u.name" }
```

Запросы можно расширять: добавляется новый
объект проверки с описанием и Surfer-командой.

BloodHound чек-лист (2026-05-28_0506)

#checklist

Общие проверки

☐ Проверка LDAP подписи state:: провал comments:: -

- Отсутствие LDAP signing на контроллерах домена позволяют проводить некоторые типы Relay атак

☒ Проверка MachineAccountQuota state:: ycnex comments:: -

- Параметр machineaccountquota определяет сколько объектов компьютер может создавать пользователь, параметр также зависит от прав SeMachineAccountQuotaPrivilege

☐ Атака Kerberoasting state:: na comments:: -

- Пользователи с SPN, для которых может быть проведена атака kerberoasting

☐ Атака AsRepRoasting state:: na comments:: -

- Пользователи с включенным флагом не требовать пре-аутентификацию

☒ Контроллеры домена, позволяющие NTLMv1 или LM аутентификацию state:: провал comments:: -

Проверка MachineAccountQuota

Описание: Параметр machineaccountquota определяет сколько объектов компьютер может создавать пользователь, параметр также зависит от прав SeMachineAccountQuotaPrivilege

Cypher запрос:

```
MATCH (m:Domain) RETURN m.machineaccountquota
```

Всего записей: 4

Результат

- None
- None
- None
- None

Атака Kerberoasting

Описание: Пользователи с SPN, для которых может быть проведена атака kerberoasting

Cypher запрос:

```
MATCH (u:User {hasspn:true}) WHERE NOT u.name STARTS WITH 'KRBTGT' RETURN u.name
```

Всего записей: 2

Результат

- [ADMINISTRATOR@PHANTOM.CORP](#)
- [SVC_KERB_DEL@PHANTOM.CORP](#)

Все задачи

Статус (56)	Задача	Комментарий
☐	Проверка LDAP подписи	-
☒	Проверка MachineAccountQuota	-
☐	Атака Kerberoasting	-
☐	Атака AsRepRoasting	-
☒	Контроллеры домена, позволяющие NTLMv1 или LM аутентификацию	-
☒	Компьютеры, позволяющие NTLMv1 или LM аутентификацию	-
☒	Пароли в атрибутах *password пользователей	-
☐	Пользователи с флагом PASSWD_NOTREQD	-
☒	Компьютеры с флагом PASSWD_NOTREQD	-
☒	Компьютеры с неограниченным делегированием Kerberos	-
☒	ACL от Domain Computers до любого объекта	-
☐	ACL от Domain Users до любого объекта	-
☒	ACL от Authenticated Users до любого объекта	-
☐	ACL от Everyone до любого объекта	-
☒	ACL от Users до любого объекта	-
☐	ACL от Domain Computers до любого объекта через членство в группах	-
☐	ACL от Domain Users до любого объекта через членство в группах	-
☐	ACL от Authenticated Users до любого объекта через членство в группах	-
☒	ACL от Everyone до любого объекта через членство в группах	-
☒	ACL от Users до любого объекта через членство в группах	-
☐	Короткий путь от общих групп до группы DOMAIN ADMINS	-
☐	Короткий путь от общих групп до группы DOMAIN ADMINS (все связи)	-



DCSyncHound

постобработка DCSync-результатов

Как работает

Берёт вывод
Mimikatz/secretsdump/SharpKatz
и результаты Hashcat

Практическая польза

Собирает Excel-отчёт,
сопоставляет пользователей,
хэши и cracked-пароли, может
загрузить данные обратно
в BloodHound.

Ключевые элементы

DCSync

Hashcat

xlsx

passwords

BRANDON.BUTLER@MORLAB.COM

Database Info Node Info Analysis

BRANDON.BUTLER@MORLAB.COM

OVERVIEW +

NODE PROPERTIES +

EXTRA PROPERTIES -

distinguish edname	CN=BRANDON BUTLER,CN=USERS,DC=MORLAB,DC=COM
domain	MORLAB.COM
domainsid	S-1-5-21-3164229210-3968512189-1251865757
isaciprotected	False
ntlm	5694
password	sc
passwordnotreqd	False
samaccountname	Brandon.Butler
trustedtoauth	False

BRANDON.BUTLER@MORLAB.COM

	A	B	C	D	E	
1	Domain	User	Plaintext	NTLM	Enabled	
2	morlab.com	Administrator	Aa		Enabled	
3	morlab.com	domain.admin_history0	Aa			
4	morlab.com	domain.admin_history1	Aa			
5	morlab.com	mor.david	Aa		Enabled	
6	morlab.com	domain.admin.protect	Aa		Enabled	
7	morlab.com	addhost	Aa		Enabled	
8	morlab.com	Brian.Perez	abi		Enabled	
9	morlab.com	Kevin.Mitchell	ant		Enabled	
10	morlab.com	Maria.Price	ass		Enabled	
11	morlab.com	Aaron.Morgan	bal		Enabled	
12	morlab.com	Sean.Price	bli		Enabled	
13	morlab.com	Monica.Cox	car		Enabled	
14	morlab.com	Elizabeth.Morris	che		Enabled	
15	morlab.com	Jacqueline.Brooks	chr		Enabled	
16	morlab.com	Monica.Foster	cla		Enabled	
17	morlab.com	Kenneth.Cooper	con		Enabled	
18	morlab.com	April.Richardson	cou		Enabled	
19	morlab.com	Peter.Bryant	cris		Enabled	
20	morlab.com	Richard.Hernandez	cut		Enabled	



Дополнительные коллекторы BloodHound

Коллекторы собирают данные из систем, которые стандартный SharpHound не покрывает или покрывает не полностью.



PrivHound

Windows: локальное повышение привилегий

Что собирает

PowerShell-скрипт запускается на хосте и анализирует службы, права на файлы, креды, историю PowerShell, токены и autorun

Зачем нужен

Нужен для отображения локальных privesc-находок в общем графе BloodHound

Новые узлы

Service, File, UserProfile, Credential, TokenPrivilege, Autorun

Новые связи

PHCanWriteServiceBinary, PHContainsCredential, PHHasDangerousPrivilege

PowerShell

local privesc

custom nodes





^ Saved Queries

☐ Auto-run selected query

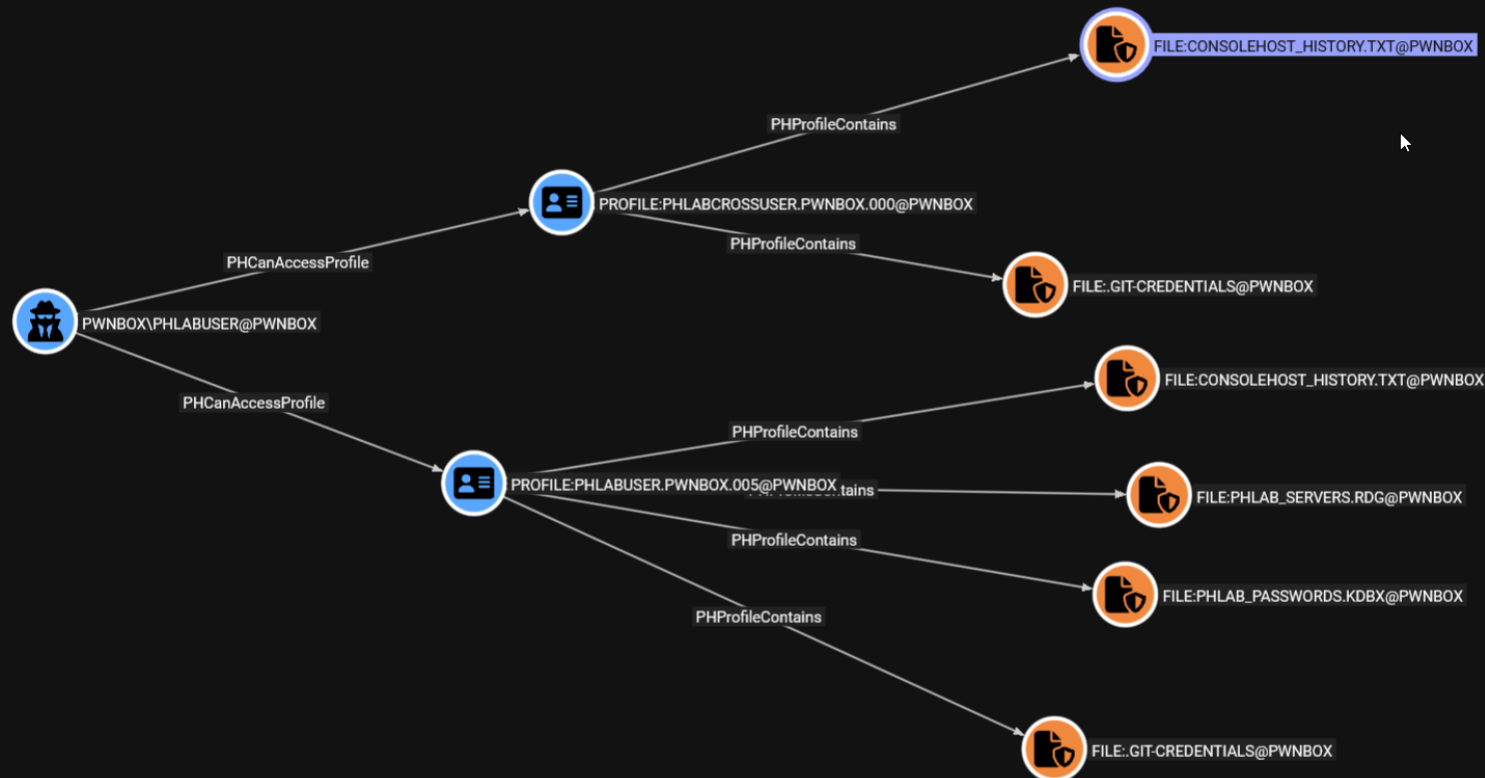
```
1 MATCH p=(u:PHUser)-[:PHCanAccessProfile]->(prof:PHUserProfile)-[:PHProfileContains]->(f:PHSensitiveFile)
2 RETURN p
```

Save Run

FILE:CONSOLEHOST_HISTORY.TXT@PWN...

Object Information

Node Type:	PHSensitiveFile
Object ID:	8EAD8935660DF417E0F73D635DDF61D9
Description:	PS history (in PHLabCrossUser.PwnBox.000's profile)
File Path:	C: \Users\PHLabCrossUser.PwnBox.000\AppData\Roaming\Micr...
Hostname:	PWNBOX
Last Seen by BloodHound:	2026-03-06 17:17 GMT+5:30 (GMT+0530)
Primary Kind:	PHSensitiveFile



—

Q SEARCH

◆ PATHFINDING

</> CYPHER

^ Saved Queries

☐ Auto-run selected query

1 MATCH p=(u:PHUser)-[:PHCanWriteProgDir]->(d:PHWritableProgramDir)-[:PHHostsBinaryFor]->(s:PHService)-[:PHRunsAs]->(t:PHPrivTarget)

2 RETURN p

Save

▼

ⓘ

Run ▶

× PHRunsAs ⌵

— Relationship Information

Source Node:

SVC:PHLABPROGSVC@PWNBOX

Target Node:

NT AUTHORITY\SYSTEM@PWNBOX

Abuse Info:

Exploit the parent finding (modifiable service, writable binary, unquoted path, etc.) to inject a payload into this service's execution context.

Description:

This service or task runs under a privileged account (typically SYSTEM). Compromising it yields execution as that account.

Last Seen by BloodHound:

2026-03-06 17:17 GMT+5:30 (GMT+0530)

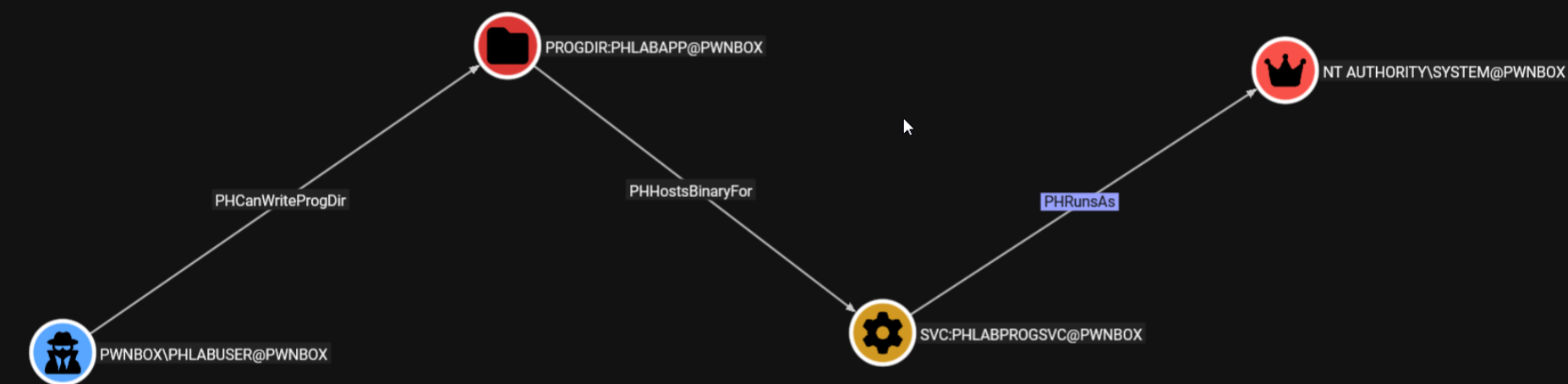
Opsec:

Service restarts may be logged and noticed. Check if the service is set to auto-start.

Run Account:

LocalSystem

The edge PHRunsAs does not have any additional contextual information at this time.



TaskHound

Windows: запланированные задачи

Что собирает

Консольный инструмент на Python, подключается к хостам по SMB, забирает XML-задачи и смотрит, от каких учётных записей они запускаются.

Зачем нужен

Помогает найти задачи с сохранёнными кредитами, показать путь: компьютер → задача → учётка.

Новые узлы

ScheduledTask, компьютер с задачей, RunAs-учётка

Новые связи

HasTask, HasTaskWithStoredCreds, RunsAs



SMB

ScheduledTask

RunsAs

OpenGraph



ConfigManBearPig

SCCM / Microsoft Configuration Manager

Что собирает

PowerShell-коллектор находит SCCM-сайты, клиентов, коллекции, роли, SQL и варианты relay

Новые узлы

SCCM_AdminUser, SCCM_ClientDevice, SCCM_Collection, SiteServer, MSSQL

SCCM

AdminService

MSSQL

OpenGraph

SCCM, или Microsoft Configuration Manager, — это инструмент Microsoft для централизованного управления устройствами в организации.

Он помогает администраторам устанавливать приложения, обновлять Windows, собирать инвентаризацию компьютеров и управлять настройками рабочих станций из одной консоли.



Ampire 360°



SCCMHound

SCCM-данные, сессии и локальные админы

Что собирает

C#-коллектор для SCCM: собирает пользователей, компьютеры, текущие сессии и локальных администраторов управляемых хостов

Зачем нужен

Пересекается с ConfigManBearPig, но больше ориентирован на сбор SCCM-информации и legacy-сценарии

Новые узлы

SCCMUser, SCCMComputer, SCCMManagedComputer, Session, LocalAdmin

Новые связи

HasSession, AdminTo, SCCMManaged



C#

SCCM

sessions

local admins

SCCM, или Microsoft Configuration Manager — это инструмент Microsoft для централизованного управления устройствами в организации

Он помогает администраторам устанавливать приложения, обновлять Windows, собирать инвентаризацию компьютеров и управлять настройками рабочих станций из одной консоли

ShareHound-CE

сетевые шары и права доступа

Что собирает

Собирает информацию о SMB-шарах, файлах, директориях и реальных правах доступа

Новые узлы

Share, Directory, File, FileShare, Computer

SMB

File

CanWrite

secrets

Зачем нужен

Позволяет искать конфиги, бэкапы, VMDK, скрипты и другие чувствительные файлы не как список, а как граф

Новые связи

CanRead, CanWrite, CanModify, CanDelete, Contains, HostedOn



USERINFO.EXE.ZIP
OpenGraph | File



USERINFO.EXE.ZIP



Object Information

Node Type: File

Object ID: FILE:\\DC\\SUPPORT-TOOLS\\USERINFO.EXE.ZIP

Created At: 133028100667915870

Extension: .zip

File Size: 277499

Last Seen by BloodHound: 2026-05-20 16:48 EDT (GMT-0400)

Modified At: 133028100671509420

Path: UserInfo.exe.zip

Primary Kind: File

UNC Path: \\DC\\support-tools\\UserInfo.exe.zip

ExchangeHound

Exchange-разрешения и делегирования

Что собирает

ExchangeHound собирает данные из Microsoft Exchange и добавляет в BloodHound почтовый слой инфраструктуры: почтовые ящики, папки, публичные папки, базы почтовых ящиков, транспортные правила, Exchange RBAC-роли и делегированные права

Новые узлы

Mailbox, MailboxFolder, PublicFolder, TransportRule, ExchangeRbacRole

Exchange

Mailbox

RBAC

SendAs

Зачем нужен

Нужен он для того, чтобы увидеть Exchange не как отдельную почтовую систему, а как часть общей модели attack paths

Новые связи

HasFullAccess, HasSendAs, HasFolderAccess, HasExchangeRole



ProfileHound

профили доменных пользователей на Windows

Что собирает

Подключается к C\$ на хостах, смотрит C:\Users и определяет, какие доменные профили там существуют

Новые узлы

UserProfile, Computer, User

C\$

UserProfile

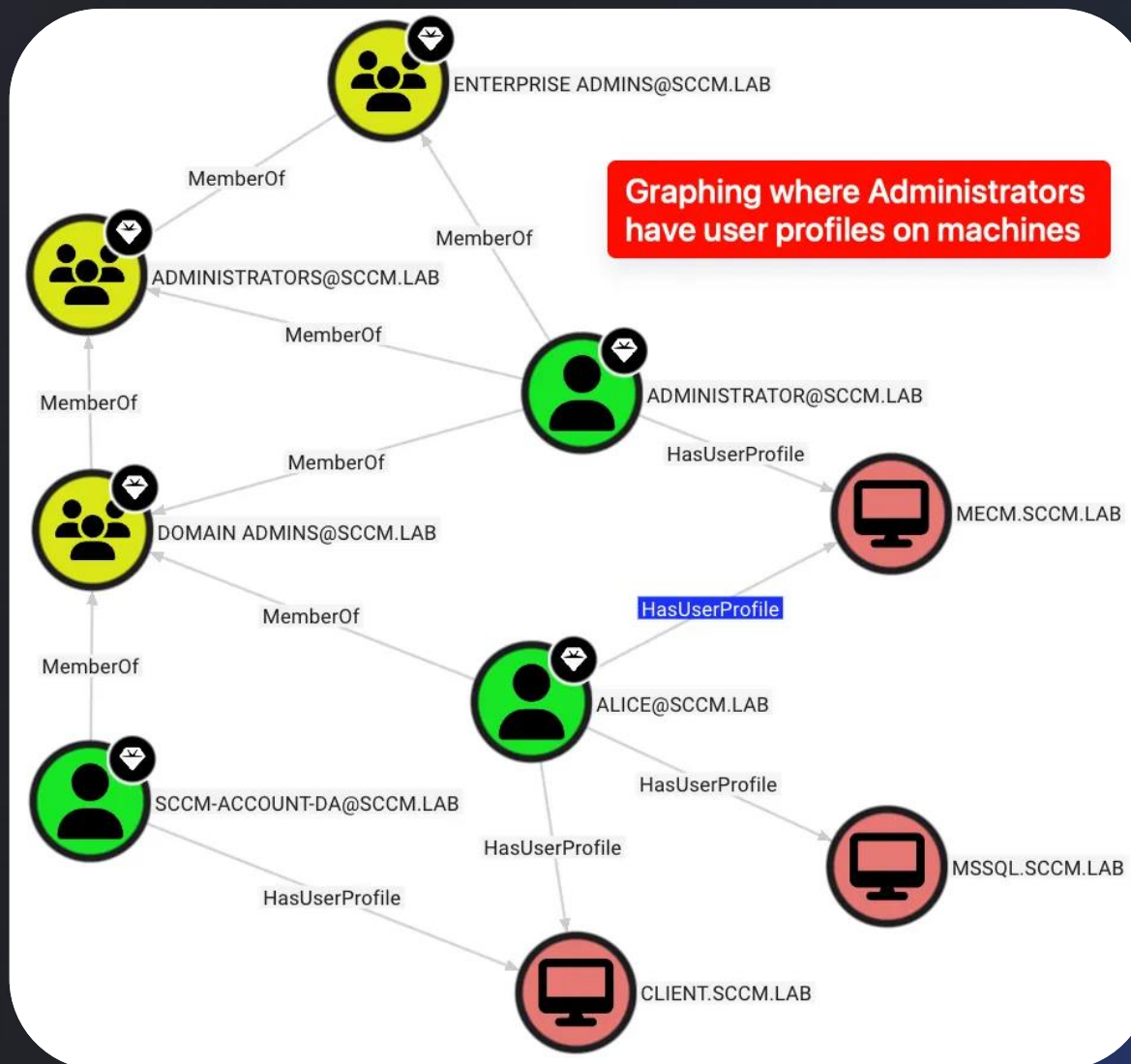
post-exploitation

Зачем нужен

Помогает приоритезировать машины, где могли остаться токены, ключи, браузерные артефакты или конфиги привилегированных пользователей

Новые связи

HasUserProfile



NetworkHound

сетевой слой поверх AD-графа

Что собирает

- Active Directory Objects
- Network Infrastructure
- Port Scanning: открытые порты на всех обнаруженных устройствах с идентификацией служб
- Web Services
- SSL-сертификатов и обнаружением веб-сайтов
- SMB Services
- Shadow-IT Discovery
- Network Topology



NetworkHound



Новые узлы

Domain, Site, Subnet, Computer, Device, Website, FileShare, IP, Port, Service

Новые связи

PartOfDomain, LocatedIn, HostToIP, IPToPort, PortToService

SCOMHound

System Center Operations Manager

Что собирает

PoC-OpenGraph-коллектор: ищет SCOM-инфраструктуру в AD и добавляет SCOM-объекты в граф

Зачем нужен

SCOM интересен как система мониторинга: агенты, RunAs-аккаунты и management server могут давать новые пути атаки

Новые узлы

SCOM-сервер, management-сервер, SCOM-агент, RunAs-учётка

Новые связи

SCOM_Contains, SCOM_Manages, SCOM_HasRole, SCOM_RunsAs

SCOM

PoC

RunAs

monitoring

SCOM, или System Center Operations Manager, — это инструмент Microsoft для мониторинга IT-инфраструктуры

Он позволяет из одной консоли контролировать состояние серверов, приложений, сервисов и сетевых устройств, получать alerts и быстро находить проблемы в работе системы



CertiHound

Active Directory Certificate Services

Что собирает

Собирает AD CS: Enterprise CA, шаблоны сертификатов, NTAUTH, права enrollment и ACL.

Зачем нужен

Нужен для отображения certificate-based attack paths и потенциальных ESC-сценариев в BloodHound.

Новые связи

PublishedTo, Enroll, GenericAll, WriteDacl, WriteOwner

Новые узлы

CertTemplate, EnterpriseCA, RootCA, NTAUTHStore, AIACA



Также можно пользоваться
Certipy 😊

ESC1 – изменение SAN

Saved Queries

Search

Import
Export

Platforms
Categories
Source
Personal

Saved Queries

Enrollment rights on published ESC4 certificate templates

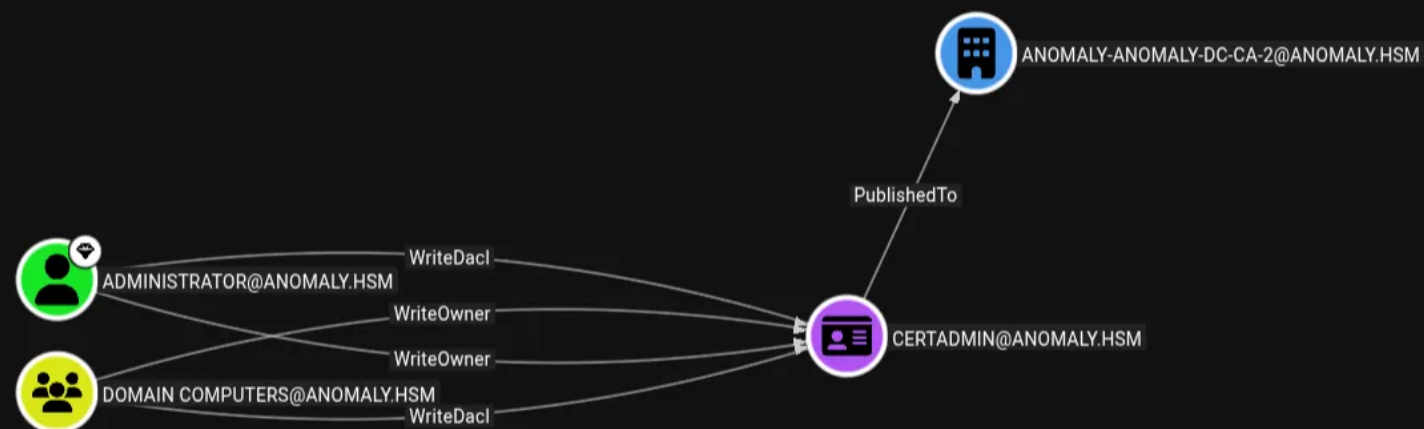
Auto-run selected query

```

1 MATCH p = (principal)-
  [:WriteDacl|WriteOwner|GenericWrite|GenericAll|Write
  AllProperties]->(ct:CertTemplate)-[:PublishedTo]->
  (ca:EnterpriseCA)
2 WHERE NOT principal.objectid ENDS WITH '-512'
3 AND NOT principal.objectid ENDS WITH '-519'
4 AND NOT principal.objectid ENDS WITH '-544'
5 RETURN p

```

Save
Run



The diagram illustrates the relationship between various roles and the ANOMALY-ANOMALY-DC-CA-2@ANOMALY.HSM role. On the left, three roles are listed: DOMAIN COMPUTERS@ANOMALY.HSM (AllExtendedRights), ENTERPRISE ADMINS@ANOMALY.HSM (Enroll), and DOMAIN ADMINS@ANOMALY.HSM (roll). These roles are connected to two intermediate roles: CERTADMIN@ANOMALY.HSM and SUBCA@ANOMALY.HSM. Both CERTADMIN@ANOMALY.HSM and SUBCA@ANOMALY.HSM are connected to the final role, ANOMALY-ANOMALY-DC-CA-2@ANOMALY.HSM, via the relationship PublishedTo.

GoLinHound

Что собирает

Собирает Linux-хосты, локальных пользователей, SSH-ключи, sudo-права и SSH-доверия

Новые узлы

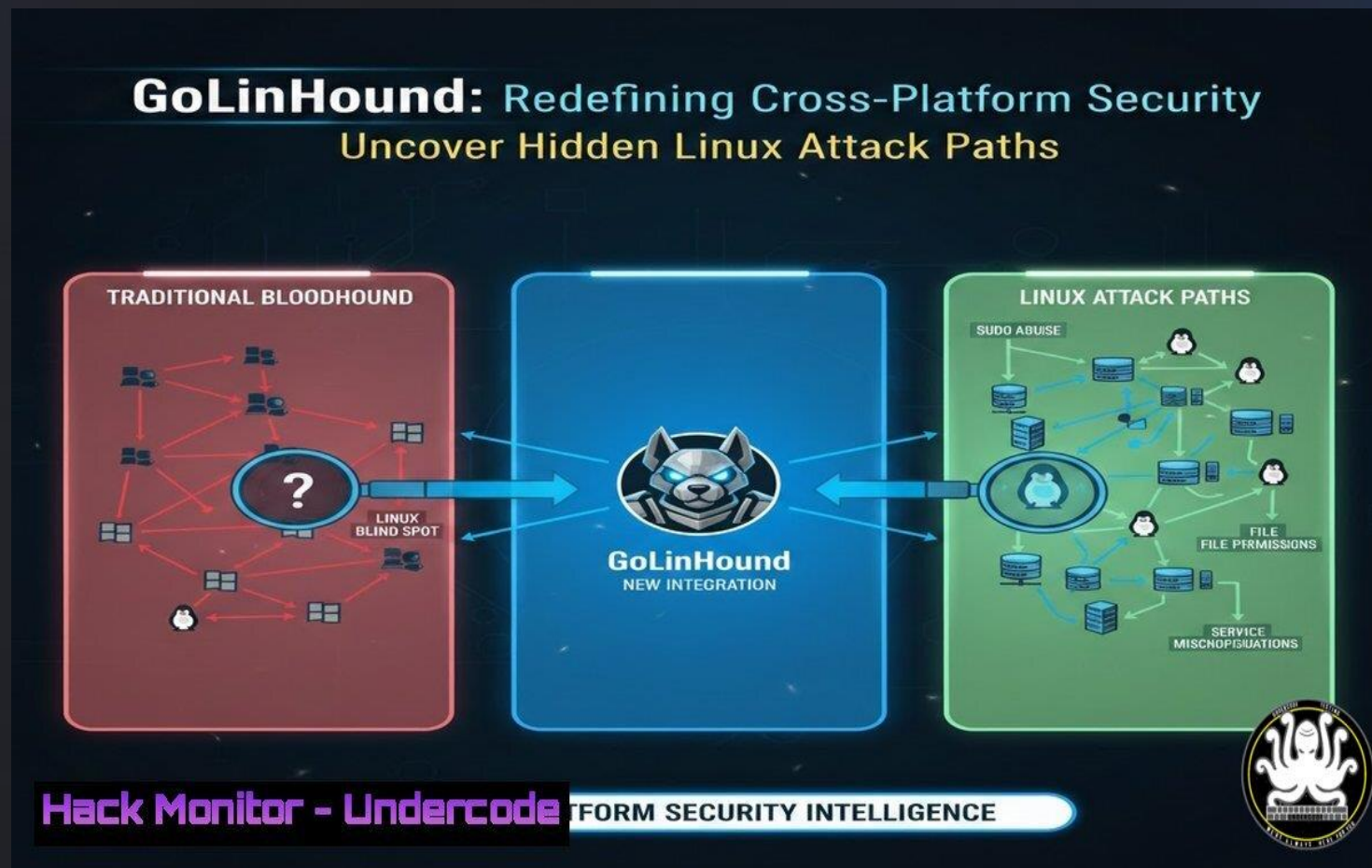
Linux-хост, локальный пользователь, SSH-ключ, sudo-права

Зачем нужен

Показывает, как путь атаки может проходить через Linux jump-host, reused SSH-ключи или sudo-цепочки

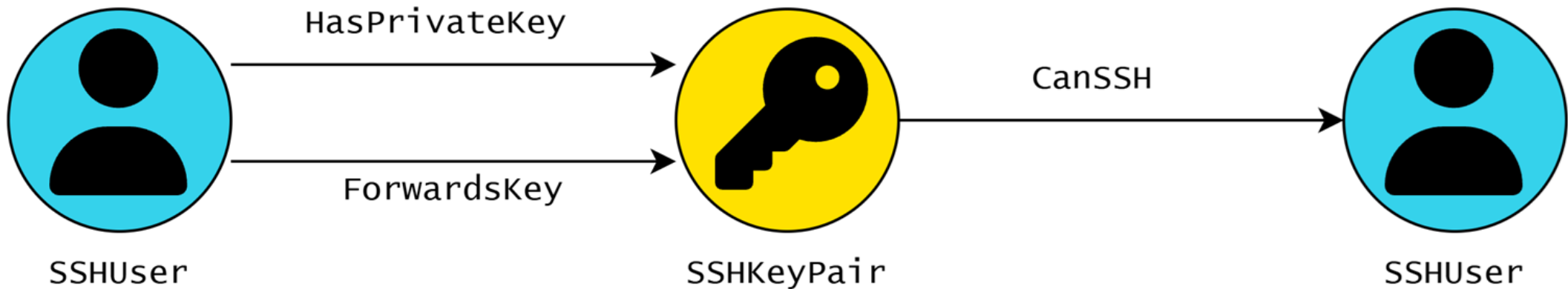
Новые связи

CanSSH, HasSSHKey, KeyCanAccessHost, HasKeytab, CanSudo



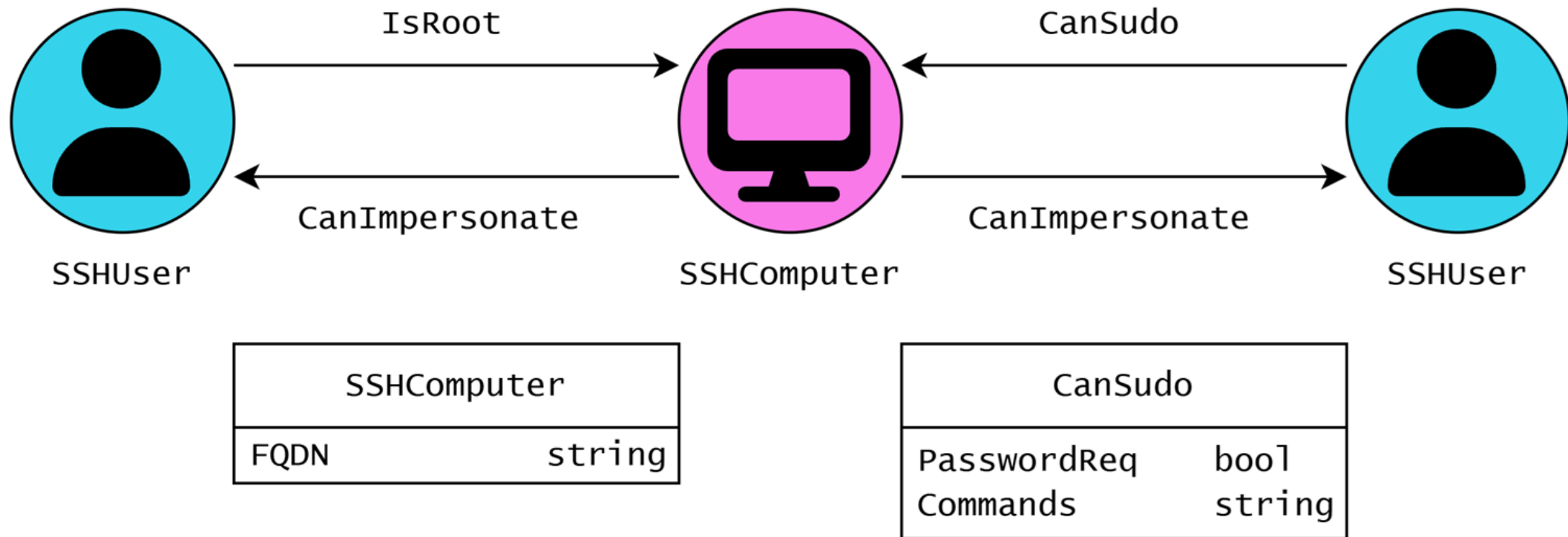
HasPrivateKey	
FilePath	string
KeyFormat	string
Encrypted	bool
KDF	string
Cipher	string

SSHKeyPair	
Algorithm	string
Base64	string
FingerprintSHA256	string
FingerprintMD5	string
FIDO2	bool

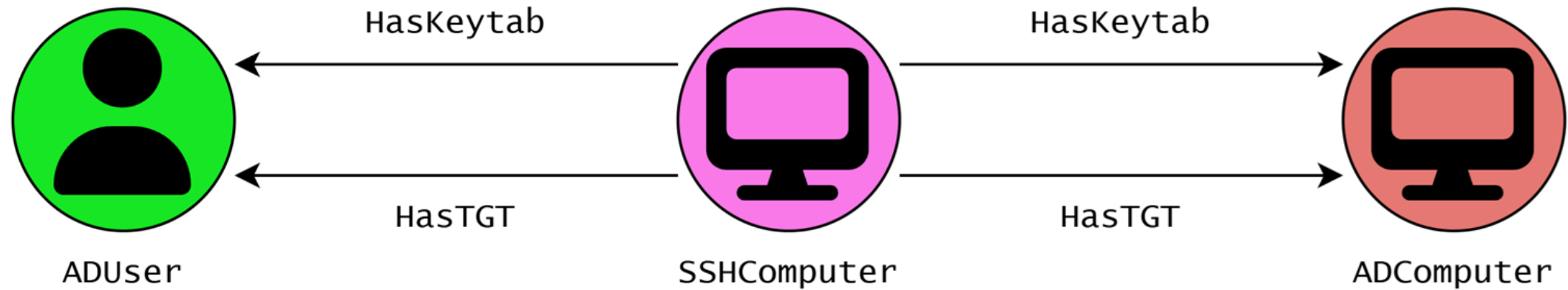


ForwardsKey	
LastLoginTime	string
LastLoginIP	string
LastLoginSocket	string
Comment	string

CanSSH	
FilePath	string
Comment	string



Active Directory



HasKeytab	
FilePath	string

HasTGT	
FilePath	string
StartTime	string
RenewTime	string
EndTime	string

Форки и аналоги по мотивам BloodHound

IPAHound переносит графовый подход на
FreeIPA/IdM-инфраструктуру.



IPAHound / BloodHoundFreeIPA

Что это

Коллектор подключается к LDAP FreeIPA, собирает пользователей, группы, хосты, сервисы, роли, permissions, sudo/НВАС, СА и сертификатные сущности

Почему не обычный коллектор BH

IPAHound-GUI — форк BloodHound с поддержкой FreeIPA-узлов и связей. Это скорее перенос BloodHound-подхода, а не расширение стандартной AD-модели.

Узлы

IPADomain, IPAUser, IPAGroup, IPAComputer, IPAService, IPAPermission, IPARole, IPACA, IPACertificateTemplate, IPASLinux

Связи

TrustedBy, MemberOf, AddMember, ForceChangePassword, ReadKerberosKey, Owns, CanSSH,



FreeIPA Data Collector

Благодарю за внимание!

Константин Захаров

Младший исследователь



Ampire 360°