



# FreeIPA Pentesting

Olga Karelova

Independent Researcher

Moscow, August 26, 2022



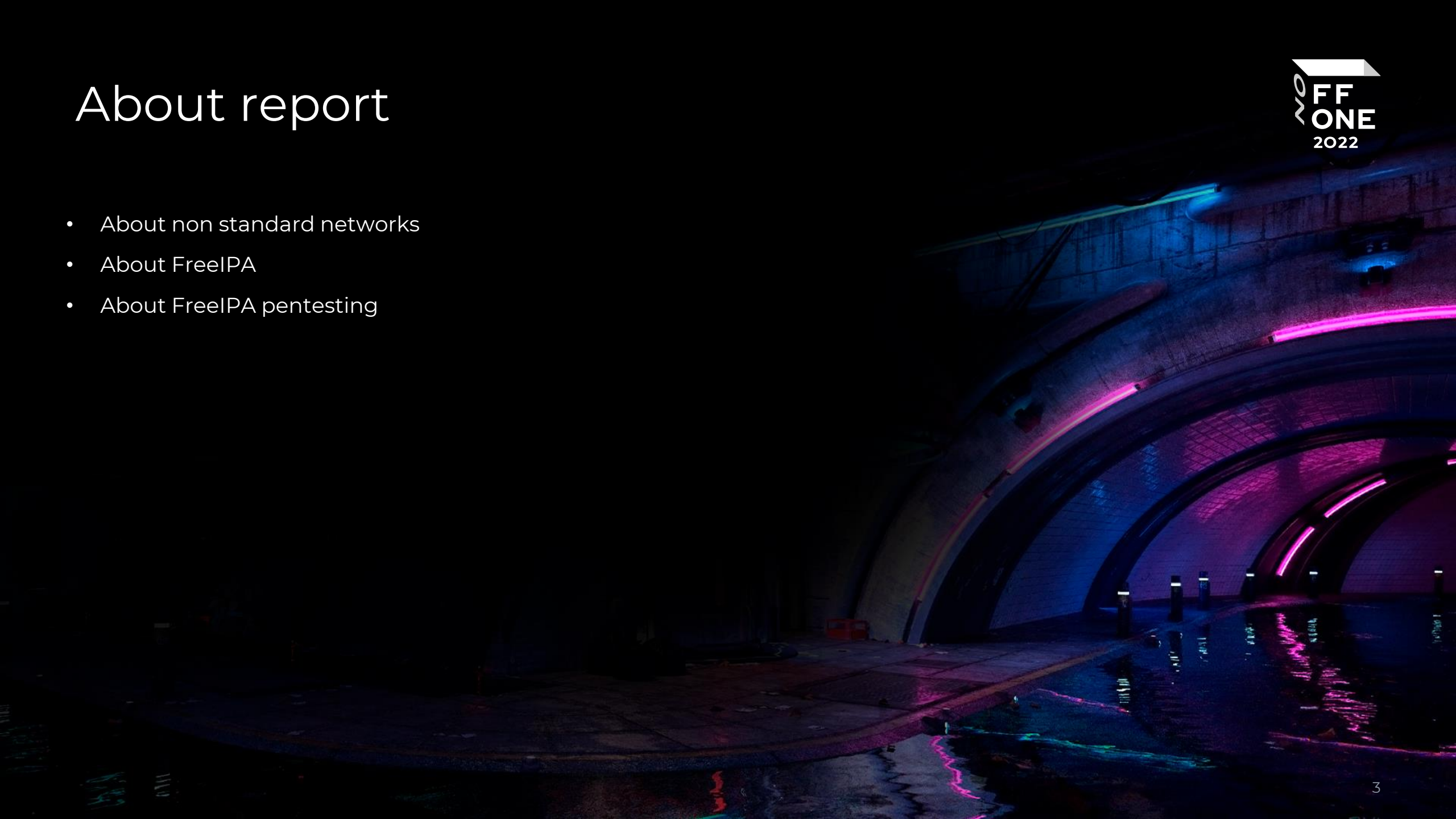
# Who am I



- CTF team's "rm -rf" captain (VolgaCTF winner in 2012 & 2013)
- M\*CTF technical director in 2014-2016
- OSCP
- Offzone and DefconNN speaker
- Tg channel @mis\_tam author
- RedTeamer/independent reasecher
- Associate Professor of the Department of Cryptology and Cyber Security, Mephi

# About report

- About non standard networks
- About FreeIPA
- About FreeIPA pentesting



# Networking

Every organization needs a domain for easy resources management

- Identification
  - ✓ Users
  - ✓ Computers
  - ✓ VMs
  - ✓ Groups
- Policy
  - ✓ Access Control
- SSO

Solutions:

- Active Directory
- Novell Identity Manager
- FreeIPA

# Active Directory vs FreeIPA



## Active Directory

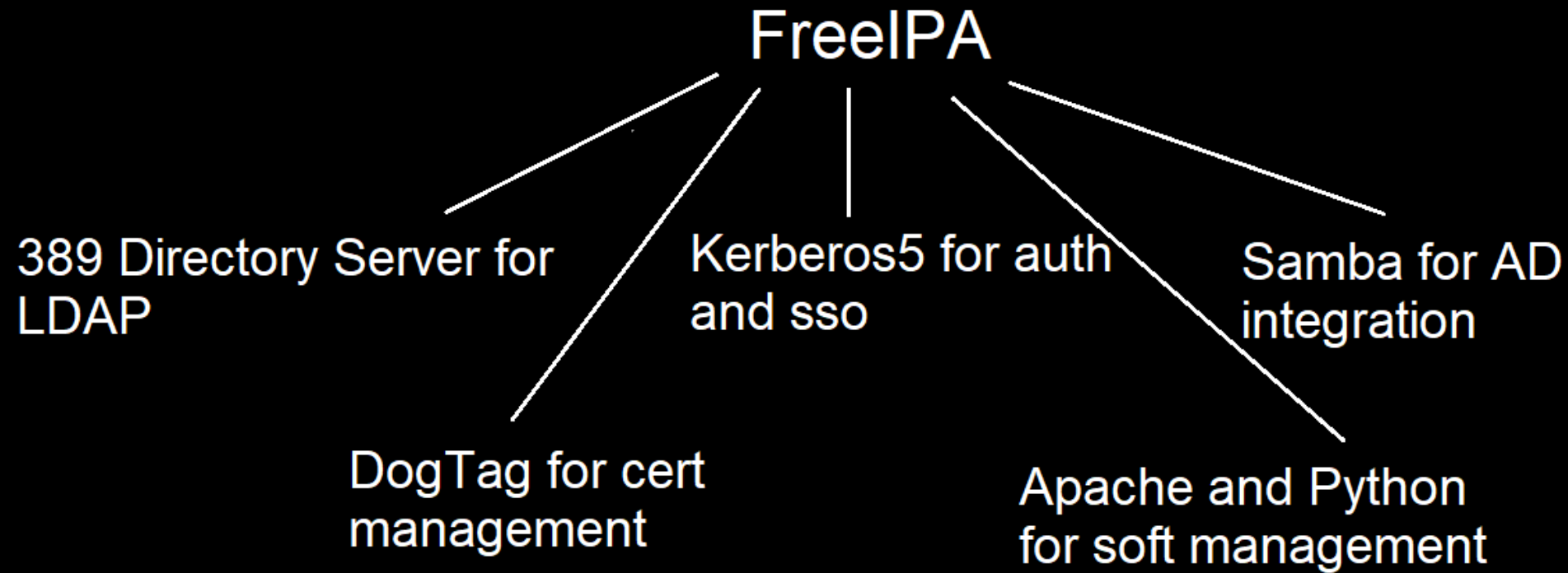
- Windows computer management
- Microsoft Corporation
- Comfortable installation
- Can use 2FA

## FreeIPA

- Unix computer management
- Opensource
- May be some problems with installation (FedOS + FreeIPA = easy install)
- Can use 2FA

FreeIPA is the Linux version or implementation of Active Director

# FreeIPA



- Local server
- Demo Server for interface testing from Red Hat (<https://www.freeipa.org/page/Demo>)

# LDAP

- Password hashes are stored in the LDAP database
- User “Directory Manager” have permission to access to password hashes
- User root in IPA server have permission to access to password hashes
- “Directory Manager” password is used by FreeIPA installation tools when bootstrapping the PKI installation and for the admin user in the PKI
- Admin is user for administrative tasks (freeipa admin = ad domain admin)

```
Certain directory server operations require an administrative user.  
This user is referred to as the Directory Manager and has full access  
to the Directory for system management tasks and will be added to the  
instance of directory server created for IPA.  
The password must be at least 8 characters long.
```

```
Directory Manager password:  
Password (confirm):
```

```
The IPA server requires an administrative user, named 'admin'.  
This user is a regular system account used for IPA server administration.
```

# Passwords



- The password hash store as base64 in the “userPassword” attribute.
- Nthash of the password store as base64 in “ipaNTHash”. If system has integration with AD
- “userPassword” can be SSHA512 (if company user old version of FreeIPA) or PBKDF2\_SHA256 (if company user newer version of FreeIPA)

```
homeDirectory: /home/vasechkinvv
mail: vasechkinvv@ipa.test.local
krbCanonicalName: vasechkinvv@IPA.TEST.LOCAL
userPassword:: e1BCS0RGM19TSEEyNTZ9QUFBSUFQQ2R0U3NRQU1INXV6T1NUbG1NZ0dJa05TeHN
6TmI4LzM5a250NEtRYjBDMXJPajV0aH11Yjk5LzFjeEtReHVxbzN4aUpSMU5ZbWhDZ2xTdnNYVE91
NHYrcE5HMzEzYmtuWVZHwke4aU1vUX1mQXV1US8v0TF5VnAxcjFyTHg2bXYyenJsaStudUdId0V0d
3dKN1BBYmdRU2NJWk5tdTNIa0NVT1p1ek1NdTdsY11Ib21QSj14MDd2bW5pWW4yd1owV2czZ2o5ZE
J1aS9NNDBMNUkvQTV1eE9NRmVpNXEvNksWQ2xYc115dy9iVGN2NEdTbzNLRWJnbTZ5VGJSMFhWbGU
3Ty8vZn13NTZPR3F3azJ4Z1RQq1FXNWfwb3crN3JWN09UM0tTM3hEM1R3SXo4bWI0NW9UajVkanVM
d3FUaERnQV1kcDFIV01BejVMNHNRbDVXZjRXNDF5VFhqN11EN1VDMEY0amV1amhpVF1JNVU0Z0Vac
jNxTTM4VmtGZDvaQ2E3MXJCdH1hQitIOUgrTnQ5V25zTEI5RDAvdE14Qjhya21CK11JZnBn
creatorsName: uid=admin,cn=users,cn=accounts,dc=ipa,dc=test,dc=local
modifiersName: cn=Directory Manager
createTimestamp: 20220810090913Z
modifyTimestamp: 20220811110508Z
```

```
ipaNTHash:: WKR4E1qTrDvwWKXqDo/bcQ==
```



# Passwords crack



- ipaNTHash is easy to crack. You should decode base64 -> re-encoded it as ASCII hex -> John The Ripper can help you to crack it fast
- SSHA512. You should decode base64 -> find SSHA512 hash -> John The Ripper can help you to crack it
- PBKDF2\_SHA256. You should decode base64 -> find PBKDF2\_SHA256 -> it's length is 256 byte. John can work with 256 bits (32 byte) -> SHA-265 used as the pseudo-random function, block size is 32 byte -> you can use only first 256 bit of our PBKDF2\_SHA256 hash -> John The Ripper can help you to crack it

```
{PBKDF2_SHA256}AAAIAPCdtSsQAIH5uzNSTImMgGikNSxsZNb8/39knN4KQb0C1rOj5thyub99/1cxKQxuqd3xiJR1N  
YmhCglSvsXTOu4v+pNG313bknYVGZA8iloQyfAuuQ//91yVp1r1rLx6mv2zrli+nuGHwENwwJ7PAbgQScIzNmu3HkCU  
NZuzIMu7IbYHoiPJ9x07vmniYn2vZ0Wg3gj9dBbi/M40L5I/A5uxOMFei5q/6K0CIXsYyw/bTcv4GSo3KEbgm6yTbR0XVle  
7O//fyw56OGqwk2xgTPBQW5apow+7rV7OT3KS3xD3Twlz8mb45oTj5djuLwqThDgAYdp1HWIAz5L4sQl5Wf4W41yTXj  
7YD6UC0F4jeujhiTYI5U4gEZr3qM38VkfD5ZCa71rBtyaB+H9H+Nt9WnsLB9D0/tMxB8rkmB+Ylfpq
```

# Pentest

- You want to know usernames
- You want to know user's roles
- You want to know some user's or admin's passwords
- You want to know main or interesting resources
- You want to release some risk
  
- CVE-2022-2414 RCE via XXE via pki-core

<https://portswigger.net/daily-swig/vulnerability-in-open-source-identity-management-system-free-ipa-could-lead-to-xxe-attacks>

# How identify FreeIPA

- Special open ports

389+443+22 -> freeipa server

```
(kali㉿kali)-[~]
└─$ nmap 192.168.56.134
Starting Nmap 7.92 ( https://nmap.org ) at 2022-08-10 03:48 EDT
Nmap scan report for server.ipa.test.local (192.168.56.134)
Host is up (0.0016s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
111/tcp   open  rpcbind
389/tcp   open  ldap
443/tcp   open  https
464/tcp   open  kpasswd5
636/tcp   open  ldapssl
749/tcp   open  kerberos-adm
8080/tcp  open  http-proxy
8443/tcp  open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

# IPA Users

- Check LDAP anonymous bind

`ldapsearch -H ldap://server -x`

Works with default settings

- ldapsearch with passwords

`ldapsearch -x -H ldap://server -D 'domain\user' -w 'password'`

- Login to IdM



The image shows the FreeIPA login interface. At the top left is the FreeIPA logo, which consists of a stylized 'F' and 'I' in green and blue, followed by the text 'FreeIPA' and 'Open Source Identity Management Solution' below it. Below the logo are two input fields: 'Username' with a placeholder 'Username' and 'Password' with a placeholder 'Password or Password+One-Time Password'. At the bottom right, there are three links: 'Log In Using Certificate', 'Sync OTP Token', and a blue 'Log in' button.

# IdM FreeIPA



- Policy information
- Users and groups information
- Computers information (if admin user)

## Password Policy

Group: global\_policy

Max lifetime (days)	<input type="text" value="90"/>
Min lifetime (hours)	<input type="text" value="1"/>
History size (number of passwords)	<input type="text" value="0"/>
Character classes	<input type="text" value="0"/>
Min length	<input type="text" value="8"/>
Max failures	<input type="text" value="6"/>
Failure reset interval (seconds)	<input type="text" value="60"/>
Lockout duration (seconds)	<input type="text" value="600"/>
Priority	

FreeIPA Ivan Ivanovich Ivanov

Users | OTP Tokens

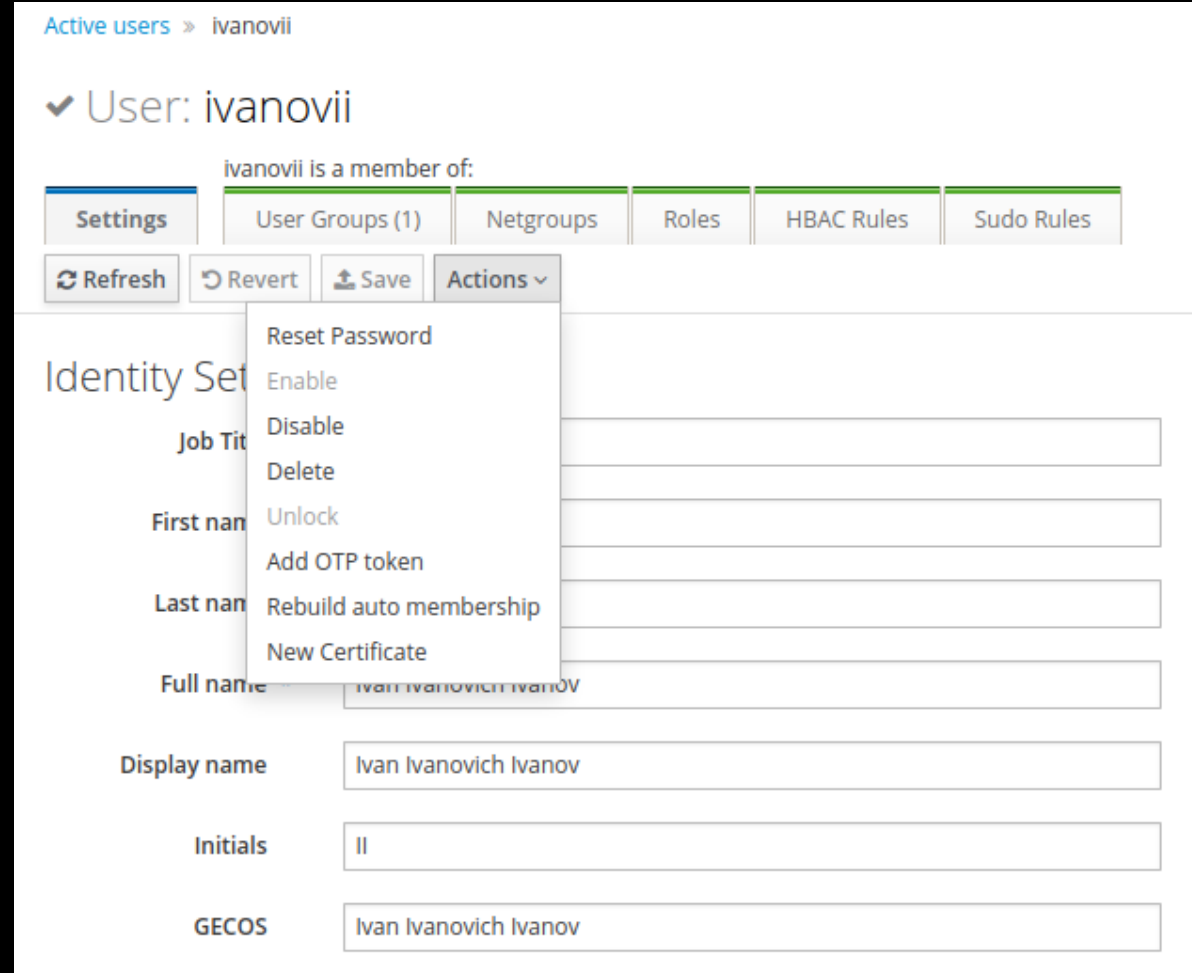
### Active users

<input type="checkbox"/>	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
<input type="checkbox"/>	admin		Administrator	✓ Enabled	1493600000			
<input type="checkbox"/>	ivanovii	Ivan Ivanovich	Ivanov	✓ Enabled	1493600001	ivanovii@ipa.test.local		
<input type="checkbox"/>	petrovpp	Petr Petrovich	Petrov	✓ Enabled	1493600003	petrovpp@ipa.test.local		
<input type="checkbox"/>	vasechkinv	Vasili Vasilievich	Vasechkin	✓ Enabled	1493600005	vasechkinv@ipa.test.local		

Showing 1 to 4 of 4 entries.

# IdM FreeIPA

- Add user's ssh certificate
- Admin can add ssh cert to all users



The screenshot shows the user management interface for 'ivanovii'. At the top, it says 'Active users > ivanovii'. Below that, there's a checkmark and 'User: ivanovii'. A navigation bar shows 'Settings' (selected), 'User Groups (1)', 'Netgroups', 'Roles', 'HBAC Rules', and 'Sudo Rules'. Below the navigation bar are buttons for 'Refresh', 'Revert', 'Save', and 'Actions'. The 'Actions' dropdown menu is open, showing options: 'Reset Password', 'Enable', 'Disable', 'Delete', 'Unlock', 'Add OTP token', 'Rebuild auto membership', and 'New Certificate'. The main content area shows 'Identity Set' and several input fields: 'Job Title', 'First name', 'Last name', 'Full name' (with value 'ivan ivanovich ivanov'), 'Display name' (with value 'Ivan Ivanovich Ivanov'), 'Initials' (with value 'II'), and 'GECOS' (with value 'Ivan Ivanovich Ivanov').

# Password brute

- Default policy – 6 logon failures
- Every ipa domain's user can login to ipa server via ssh
- Brute via ssh with hydra
- Brute via IdM with burp

```
(kali@kali)-[~]
└─$ ssh ivanovii@192.168.56.134
(ivanovii@192.168.56.134) Password:
[ivanovii@server ~]$ ls
[ivanovii@server ~]$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.134 netmask 255.255.255.0 broadcast 192.168.56.255
    inet6 fe80::20c:29ff:fea5:9e9d prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:a5:9e:9d txqueuelen 1000 (Ethernet)
    RX packets 154805 bytes 163541360 (155.9 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 52174 bytes 10960280 (10.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 26859 bytes 16669902 (15.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 26859 bytes 16669902 (15.8 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

# Extract hash

- You should know IPA Server root password -> you can find hashes
- Dbscan can help you to extract hashes from ldap db

```
[root@server user]# dbscan -f /var/lib/dirsrv/slapd-IPA-TEST-LOCAL/db/userRoot/id2entry.db
```

```
cn: Ivan Ivanovich Ivanov
displayName: Ivan Ivanovich Ivanov
initials: II
gecos: Ivan Ivanovich Ivanov
krbPrincipalName: ivanovii@IPA.TEST.LOCAL
objectClass: top
objectClass: person
objectClass: organizationalperson
objectClass: inetorgperson
objectClass: inetuser
objectClass: posixaccount
objectClass: krbprincipalaux
objectClass: krbticketpolicyaux
objectClass: ipaobject
objectClass: ipasshuser
objectClass: ipaSshGroupOfPubKeys
objectClass: mepOriginEntry
loginShell: /bin/sh
homeDirectory: /home/ivanovii
mail: ivanovii@ipa.test.local
krbCanonicalName: ivanovii@IPA.TEST.LOCAL
userPassword: e1BCS0RGM19TSEyNTZ9QUFBsUFOMEd4ME9yNGVJS01oR1Q4RVNGcGE0N0RqM31
SUGgyODdnS3Byd253S0tqUFBjJThA0aG42RnhJanpKOT10YSs0clhUcVUrcjVWTW12NWh5aGhKRnkx
aUZHwklDMW1HenUxcMjJDRlSkhoK0xKcDFhaTVXOWtaKzNZR1VLcFlKmk1JKzNNMnc40Fc4T0p2Y
2cvNkh2N0htNDdtbXE1a1hxZmZNSzJ1b1VxV0N1dzRnNTNIS0gyYnBMRW5ndVNDS0FjOVhzNGQrc0
1kSUXSNStJUjc5c1EySmtMbnBREddyVkxISDQ0NWNvV0VhXsXppcFpxSFFpdKrtZVIRr3RTMDJhVhd
GbEtqUXdWazQ5MEF3MHNDc1VTaThxTXh3amc0NEwyZ1JybXJqR3FGaHVRUxjamImakdDa1Iz0W1Y
MEFRbk1pR0tuMDdiU01FWFgzSkRtYlprNmVXTG5US1VLRDV0cnBqZUhiOGlGMittQVBma3BtaitmD
XZCb0ZRY011VkrIS1JFVzdUL3RpR1BMSkU1a2t0NGpnVTRna1ZURGIxa1pFWGdUelhnR0Zz
creatorsName: uid=admin,cn=users,cn=accounts,dc=ipa,dc=test,dc=local
modifiersName: cn=Directory Manager
createTimestamp: 20220808094435Z
```



# Kerberos

- FreeIPA Kerberos tickets = AD Kerberos tickets
- But FreeIPA Kerberos tickets stored and utilize otherwise

Tickets stored:

- Unix keyring (first TGT when user login to domain)
- CCACHE Ticket Files (Kerberos tickets in /tmp/)
- Keytab Files (auth without password)

```
[ivanovii@server ~]$ klist
Ticket cache: KEYRING:persistent:1493600001:krb_ccache_s8xC3g1
Default principal: ivanovii@IPA.TEST.LOCAL
Valid starting Expires Service principal
08/25/2022 00:54:37 08/26/2022 00:54:37 krbtgt/IPA.TEST.LOCAL@IPA.TEST.LOCAL
```

# Kerberos



- Extract ticket from keyring (server root account) via tickey  
<https://github.com/TarlogicSecurity/tickey>
- Use keytab for TGT
  - Parse keytab file (<https://github.com/its-a-feature/KeytabParser>)
  - Kinit -kt keytab server - generate tgt to some server
- Extract CCACHE ticket from /tmp/  
export KRB5CCNAME=/tmp/krb5cc\_0

# Conclusion

- You can pentesting any non standart system
- You should understand system components
- You should research-research and research



NO  
FF  
ONE  
2022

tg: @karelovao





**NO  
OFF  
ONE  
2022**