

The Unavoidable Pain Of Backups

—
Security Deep-Dive Into
The Internals Of NetBackup



1

INTRODUCTION

2

LET'S MEET NETBACKUP

Target Overview: Key Technical Aspects

3

HOW WE DUG INTO NETBACKUP

The Approach, The Challenges And How We Tackled Them

4

FINDINGS

Overview Of Vulnerabilities And Attack Paths

5

TAKEAWAYS

WHO ARE WE?

Airbus Security Lab

SPEAKERS



Nicolas Devillers ([@nikaiw](#))

10+ years in offensive security
Focus on vulnerability research and red teaming
Member of Airbus security lab



Jean-Romain Garnier ([@JRomainG](#))

Security evaluator for 2 years
Focus on reverse engineering and low-level security
Member of Airbus security lab

CO-AUTHORS



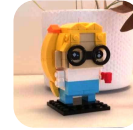
Mouad Abouhali ([@_m00dy_](#))

Security evaluator



Benoît Camredon ([@ben64_](#))

Security evaluator



Anaïs Gantet

Security evaluator

AIRBUS

Missions include:

- As an internal offensive team, evaluating products that Airbus uses (or intends to) or sells to **increase the company's overall security**
- Performing red teaming, vulnerability research, tooling development...

Checkout <https://airbus-seclab.github.io> and [@AirbusSecLab](#)

MOTIVATIONS

Why Backup Software?



BUSINESS PERSPECTIVE

- Proper backup deployment paramount for resilience
- Specialized software required for large-scale infrastructure
- Often considered as “last line of defense”



RED TEAM PERSPECTIVE

- Widely deployed across infrastructure with high privileges
- Potential access to sensitive/critical data
- Ability to move large amounts of data

MOTIVATIONS

Why NetBackup?

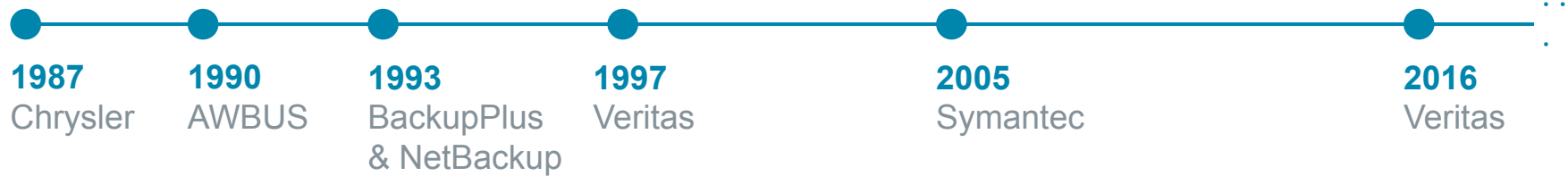


NetBackup

The #1 enterprise backup and recovery solution.

87% of the Fortune Global 500 choose NetBackup.

Source: [veritas.com/protection/netbackup](https://www.veritas.com/protection/netbackup)



BeeRumP Paris 2016, *APT Cyber-Numérique Sur Sauvegardiciel Connecté* – Émilien Girault



Full Disclosure 2017 – Sven Blumenstein, Xiaoran Wang and Andrew Griffiths from Google Security



1

INTRODUCTION

2

LET'S MEET NETBACKUP

Target Overview: Key Technical Aspects

3

HOW WE DUG INTO NETBACKUP

The Approach, The Challenges And How We Tackled Them

4

FINDINGS

Overview Of Vulnerabilities And Attack Paths

5

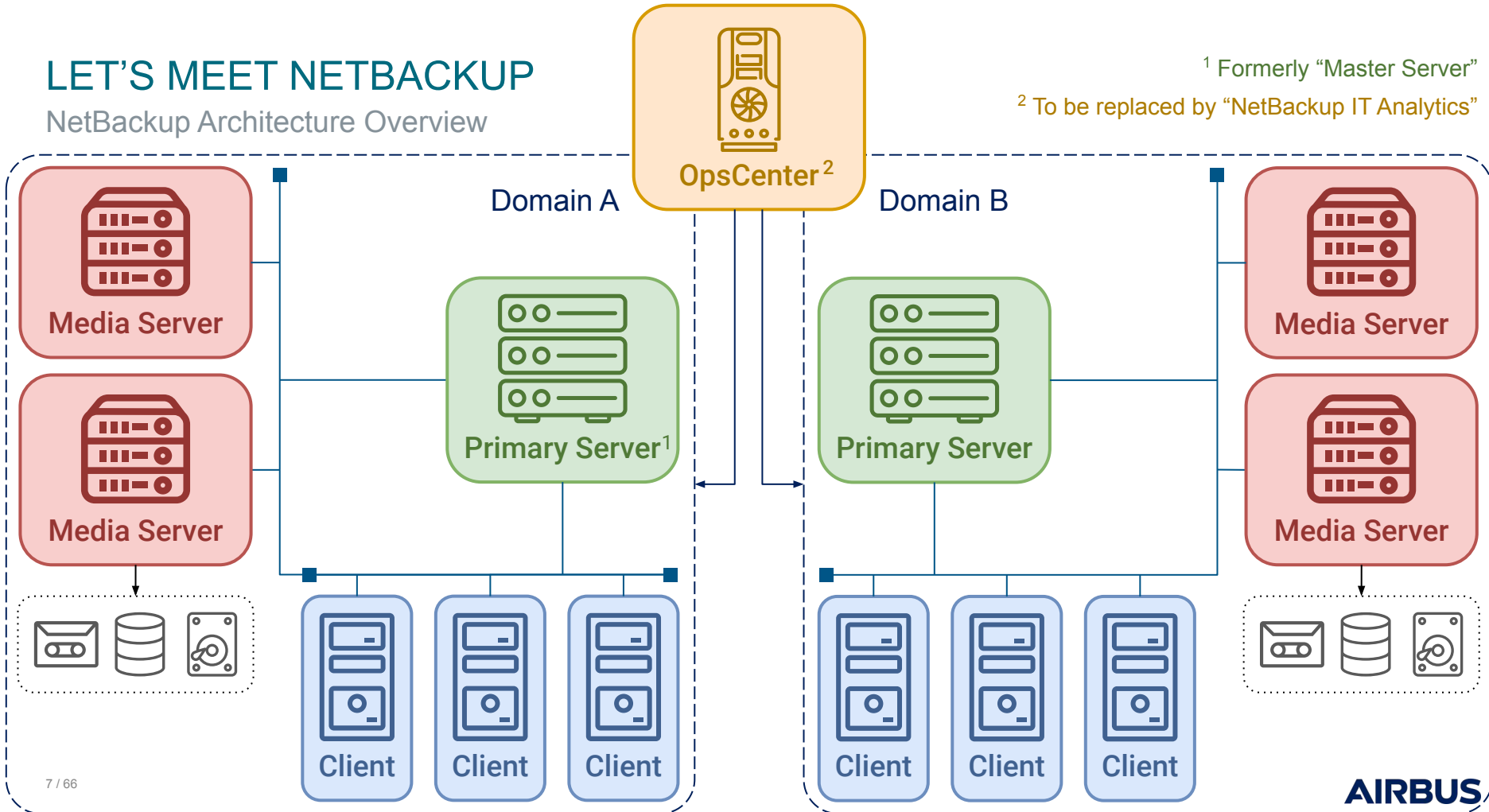
TAKEAWAYS

LET'S MEET NETBACKUP

NetBackup Architecture Overview

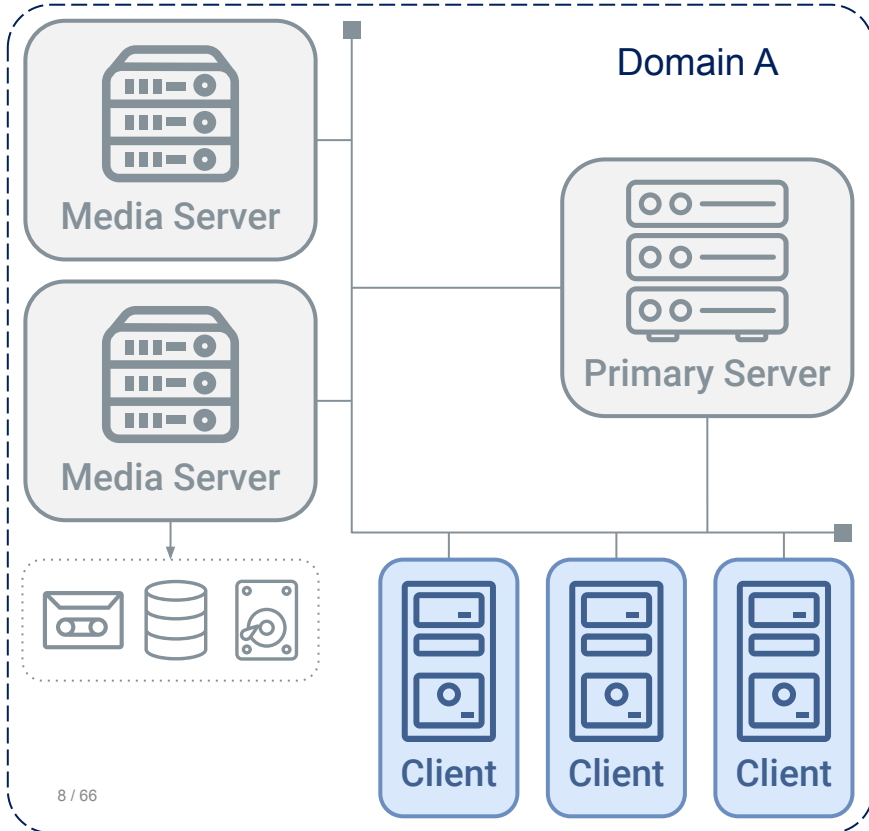
¹ Formerly "Master Server"

² To be replaced by "NetBackup IT Analytics"

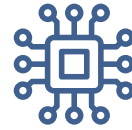


LET'S MEET NETBACKUP

More About NetBackup Clients



CLIENT DEPLOYMENT OPTIONS



Bare-metal



Cloud



Virtualized



Database

OPERATING SYSTEM



Windows



Red Hat



IBM AIX



HP-UX

...

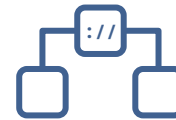
CONFIGURATION



Client-side
Encryption



Secure
communication

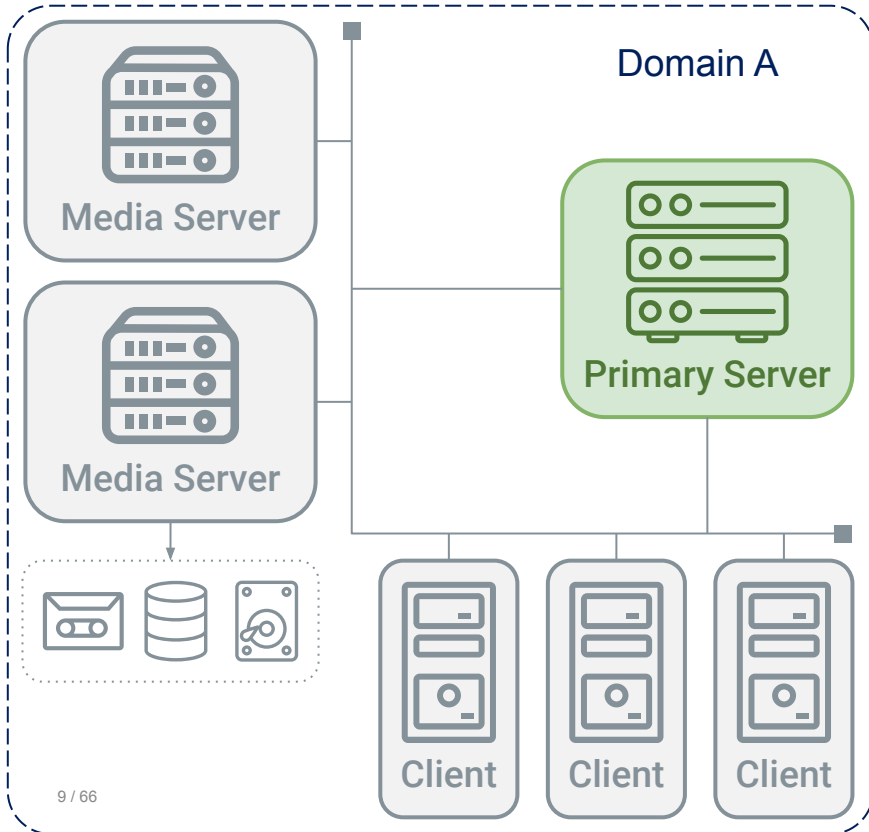


HTTP
Tunneling

...

LET'S MEET NETBACKUP

More About NetBackup Primary Servers



9 / 66

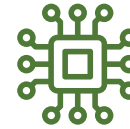
PRIMARY SERVER DEPLOYMENT OPTIONS



Cluster



Media



Appliance

...

BACKUP COMPONENTS



Policies



Catalog



API



Web UI

...

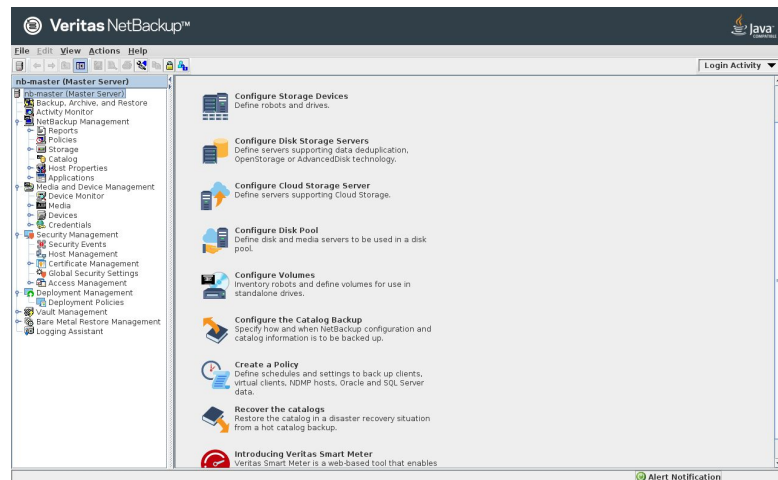
SECURITY CONFIGURATION



Secure
communication

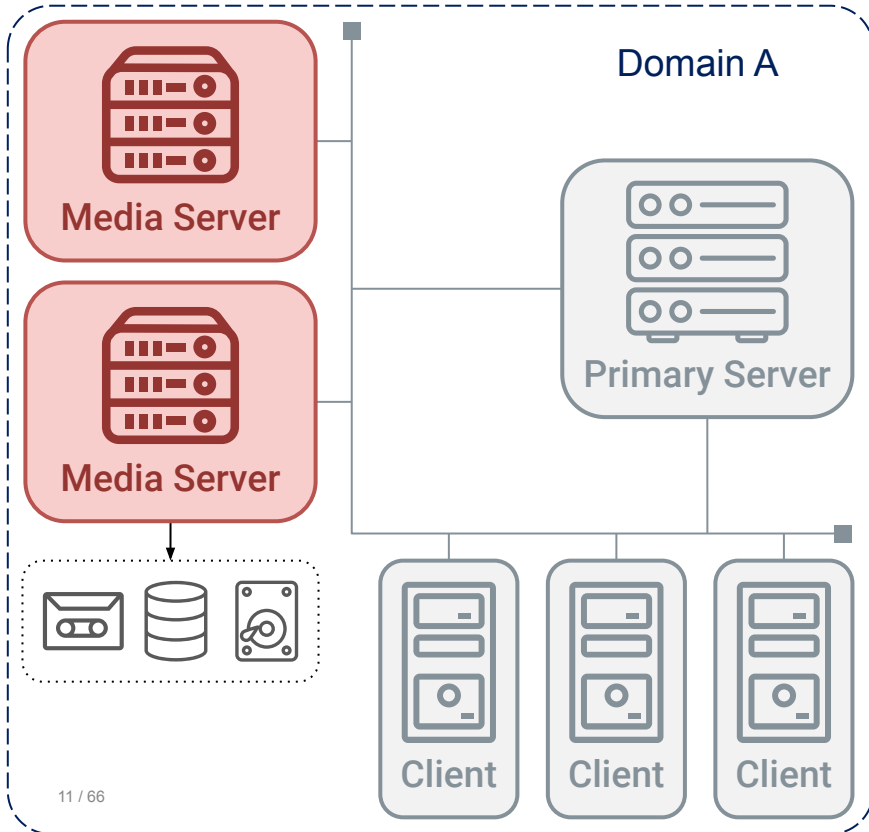
...

More About NetBackup Primary Servers



LET'S MEET NETBACKUP

More About NetBackup Media Servers



11 / 66

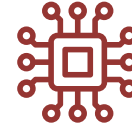
MEDIA SERVER DEPLOYMENT OPTIONS



Disk pool



Tape library



Appliance

STORAGE CONFIGURATION



Deduplication



Catalog

...

STORAGE SECURITY



Data encryption



Offline storage

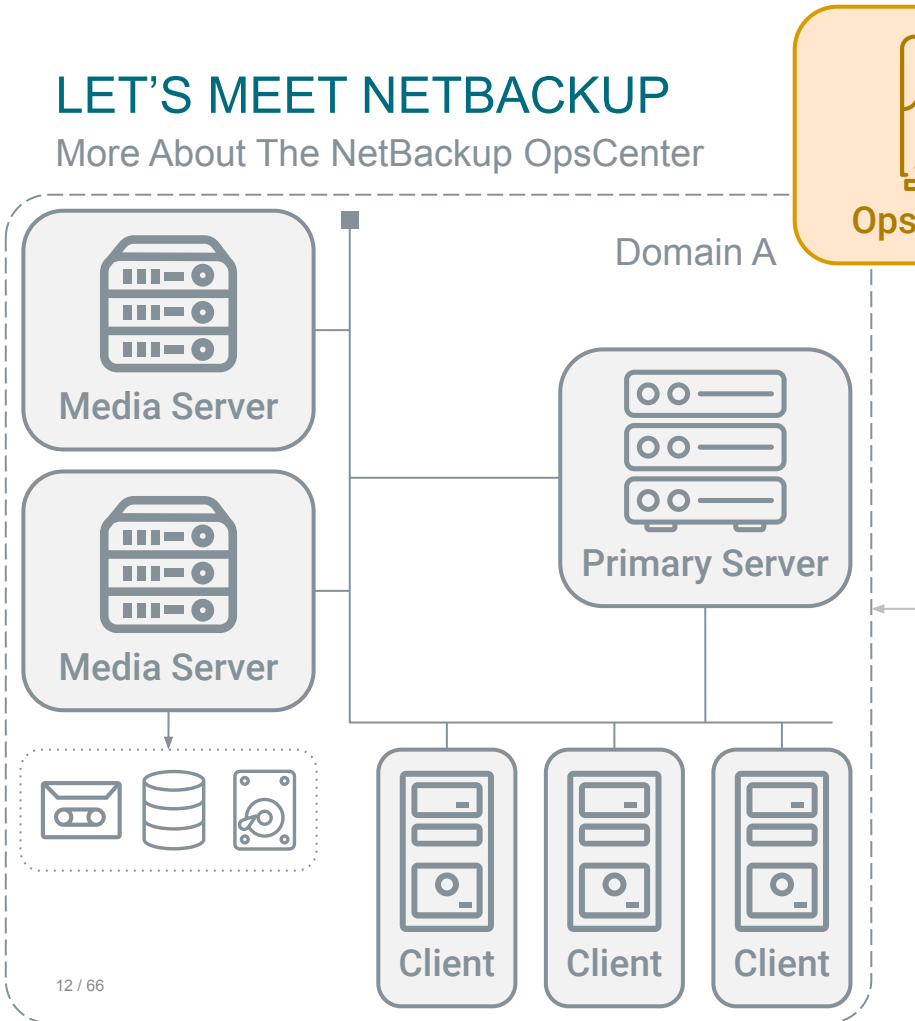


WORM

...

LET'S MEET NETBACKUP

More About The NetBackup OpsCenter



OPSCENTER ROLES



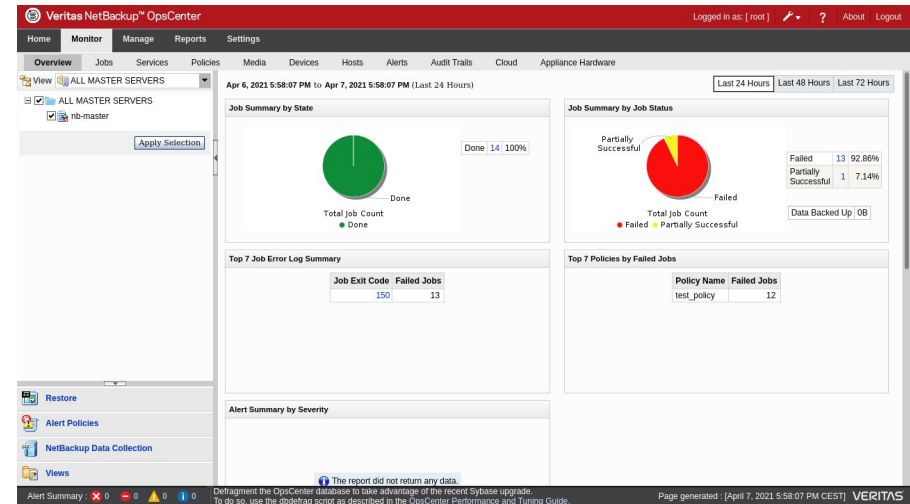
Monitor



Manage

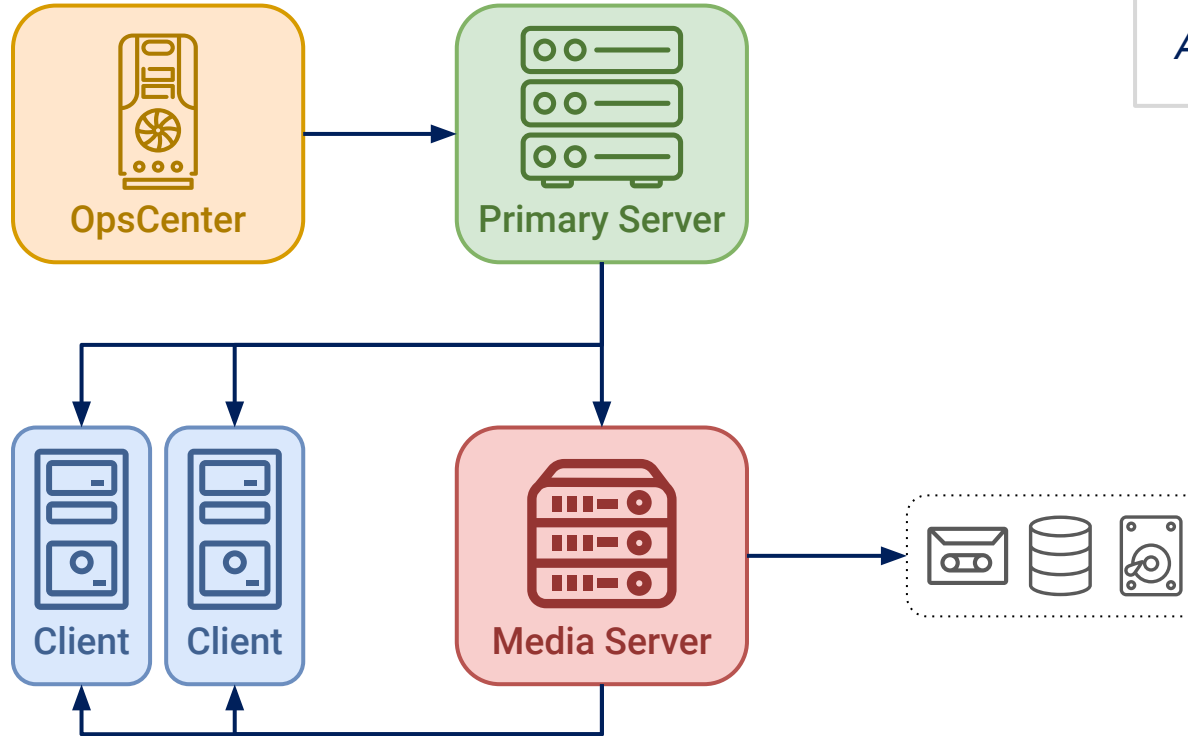


Report



LET'S MEET NETBACKUP

NetBackup Trust Model



Caption

A \longrightarrow B

A is trusted by B



1

INTRODUCTION

2

LET'S MEET NETBACKUP

Target Overview: Key Technical Aspects

3

HOW WE DUG INTO NETBACKUP

The Approach, The Challenges And How We Tackled Them

4

FINDINGS

Overview Of Vulnerabilities And Attack Paths

5

TAKEAWAYS

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

HOW WE DUG INTO NETBACKUP

Our Approach To Discover What's Under The Hood



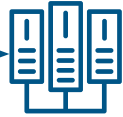
Find a team of motivated people

⇒ 5 evaluators over the course of several months



Read some documentation

⇒ Learn about main components & concepts



Setup some labs

⇒ Use customer installers (8.2–9.1), apply & check understanding, find questions



Talk with architects

⇒ Get practical knowledge, understand risks & ask questions



Read more documentation

⇒ Don't forget about security & administrator guides



Play with our labs

⇒ Don't forget to go back to previous steps

HOW WE DUG INTO NETBACKUP

Our Approach To Discover What's Under The Hood



Play with our labs?

⇒ What does it even mean?

First naive questions

- What processes are running on each component?
- How do components communicate with each other?
- What services are exposed remotely? Locally?

HOW WE DUG INTO NETBACKUP

Too Many Binaries, Too Little Time: `$ ps` To The Rescue

Java Web Server
ops_atd
OpsCenterDBd
OpsCenterServerd
pbx_exchange

bpcd
nbdisco
nbrmms
nbsl
nbsvcmon
pbx_exchange
vmd
vnetd

bpcd
bpcompatd
bpdbm
bpjobd
bprd

Java Web Server
ltid
nbars
nbatd
nbaudit

nbazd
nbdisco
nbemm
nbevtmgr
nbim

nbjm
nbkms
nbpem
nbproxy
nbrb

avrd
bmrbd
bmr
bmrpxeserver
bpinetd
nbostpxy
PXEMTFTP
spoold
spad

nbrmms
nbsl
nbstserv
nbsvcmon
nbvault

NB_dbsrv
pbx_exchange
vmd
vnetd

avrd

bpinetd
nbcssc

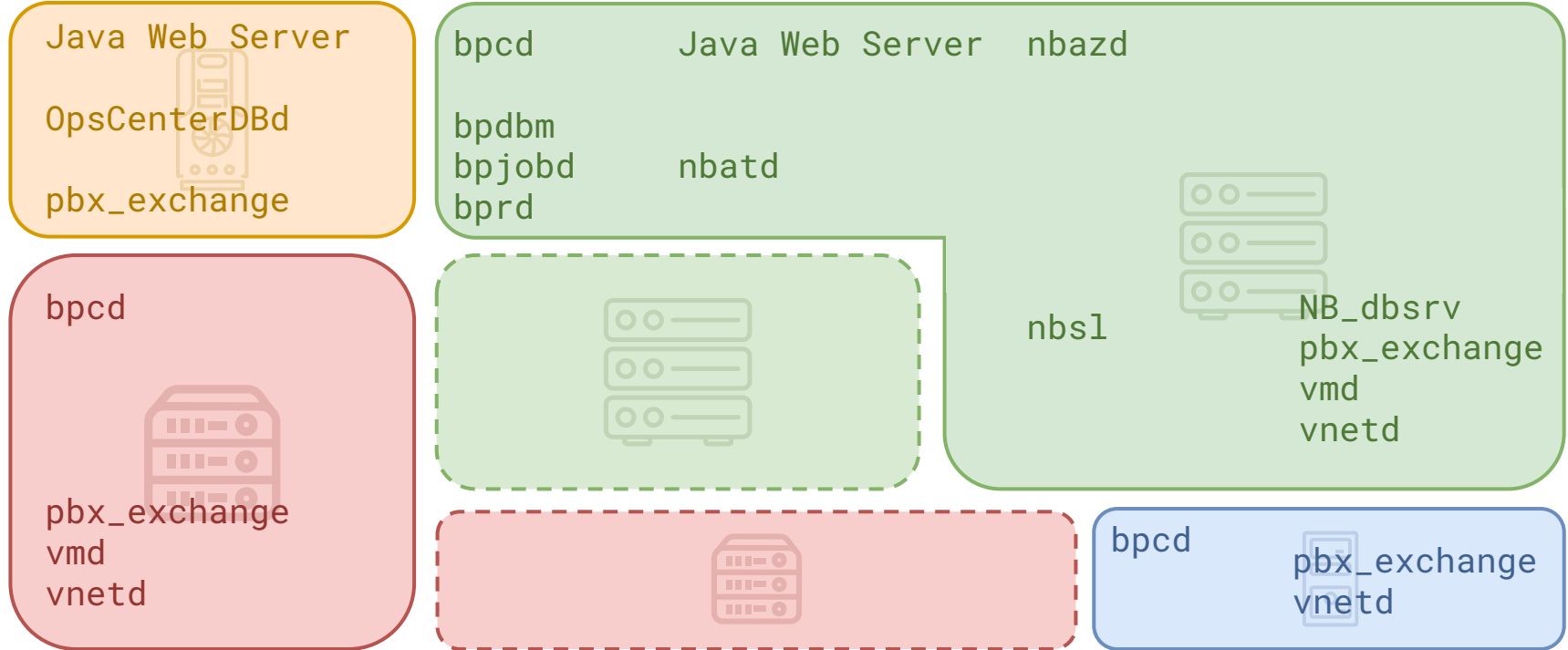
nbostpxy
nbrntd

bpcd
bpbkar
nbdisco

pbx_exchange
vnetd























HOW WE DUG INTO NETBACKUP

Too Many Daemons, Too Little Time: `$ ss` To The Rescue



HOW WE DUG INTO NETBACKUP























Too Many Daemons, Too Little Time: \$ ss To The Rescue

Binary name	Address:Port	Client	Media	Primary	OpsCenter
OpsCenterDBd	127.0.0.1:13786				
Java Web Server	0.0.0.0:8443				
pbx_exchange	0.0.0.0:1556				
vnetd	0.0.0.0:13724				
bpcd	0.0.0.0:13782				
vmd	0.0.0.0:13701				
bprd	0.0.0.0:13720				
bpdbm	0.0.0.0:13721				
nbazd	0.0.0.0:13722				
bpjobd	0.0.0.0:13723				
nbatd	0.0.0.0:13783				
NB_dbsrv	0.0.0.0:13785				
nbsl	127.0.0.1:9284				

HOW WE DUG INTO NETBACKUP

Too Many Daemons, Too Little Time: \$ ss To The Rescue

legacy ports

Binary name	Address:Port	Client	Media	Primary	OpsCenter
OpsCenterDBd	127.0.0.1:13786				
Java Web Server	0.0.0.0:8443				
pbx_exchange	0.0.0.0:1556				
vnetd	0.0.0.0:13724				
bpcd	0.0.0.0:13782				
vmd	0.0.0.0:13701				
bprd	0.0.0.0:13720				
bpdbm	0.0.0.0:13721				
nbazd	0.0.0.0:13722				
bpjobd	0.0.0.0:13723				
nbatd	0.0.0.0:13783				
NB_dbsrv	0.0.0.0:13785				
nbsl	127.0.0.1:9284				

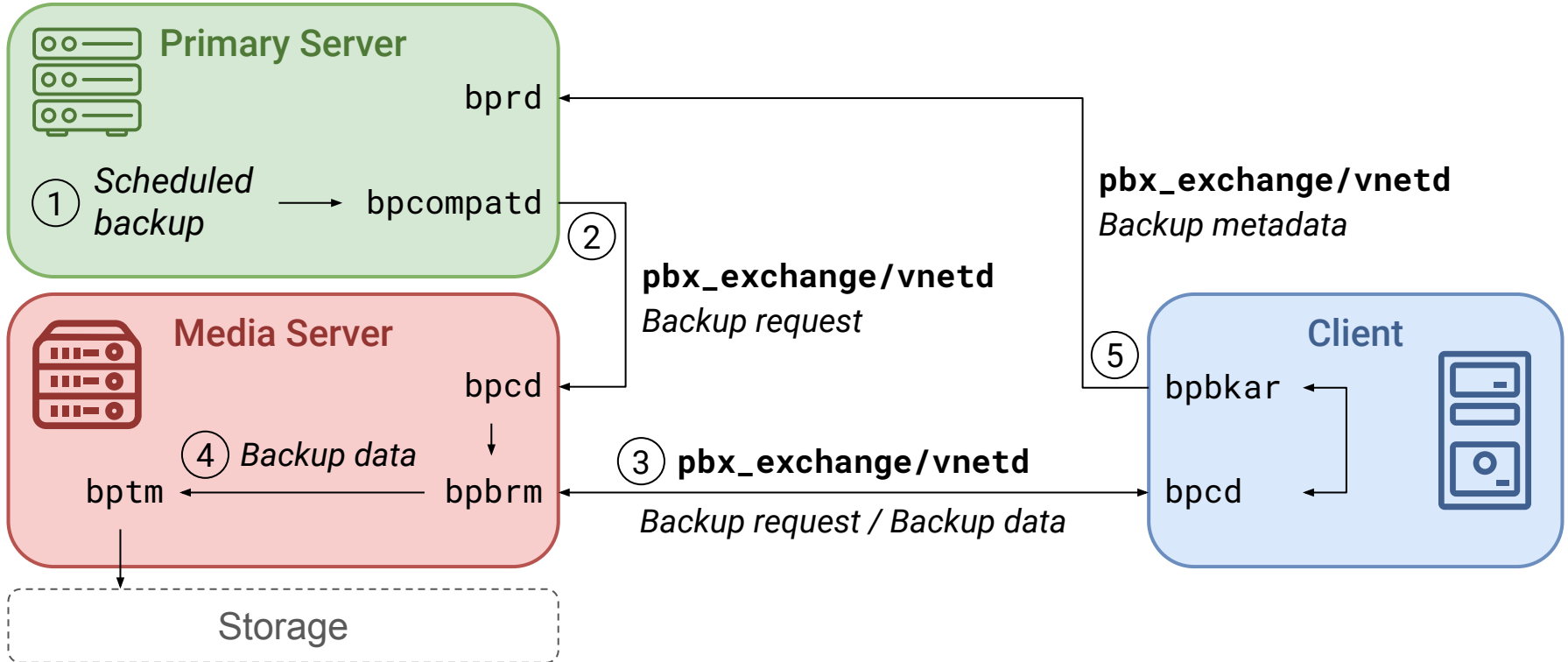
HOW WE DUG INTO NETBACKUP

java bpcompatd
bprdbm ops_atd bpcd nbemm
nbsvcmon nbatd
OpsCenterDBd
nbdisco nbvault
nbrmms nbars
vnetd
nbaudit
nbazd nbsl ltid
nbx_exchange bpbkar nbsvcmon nbstserv
nbevtmgr bpjobd nbim
nbkms nbpem nbrb nbproxy
nbjm vmd NB_dbsrv

How to keep going on

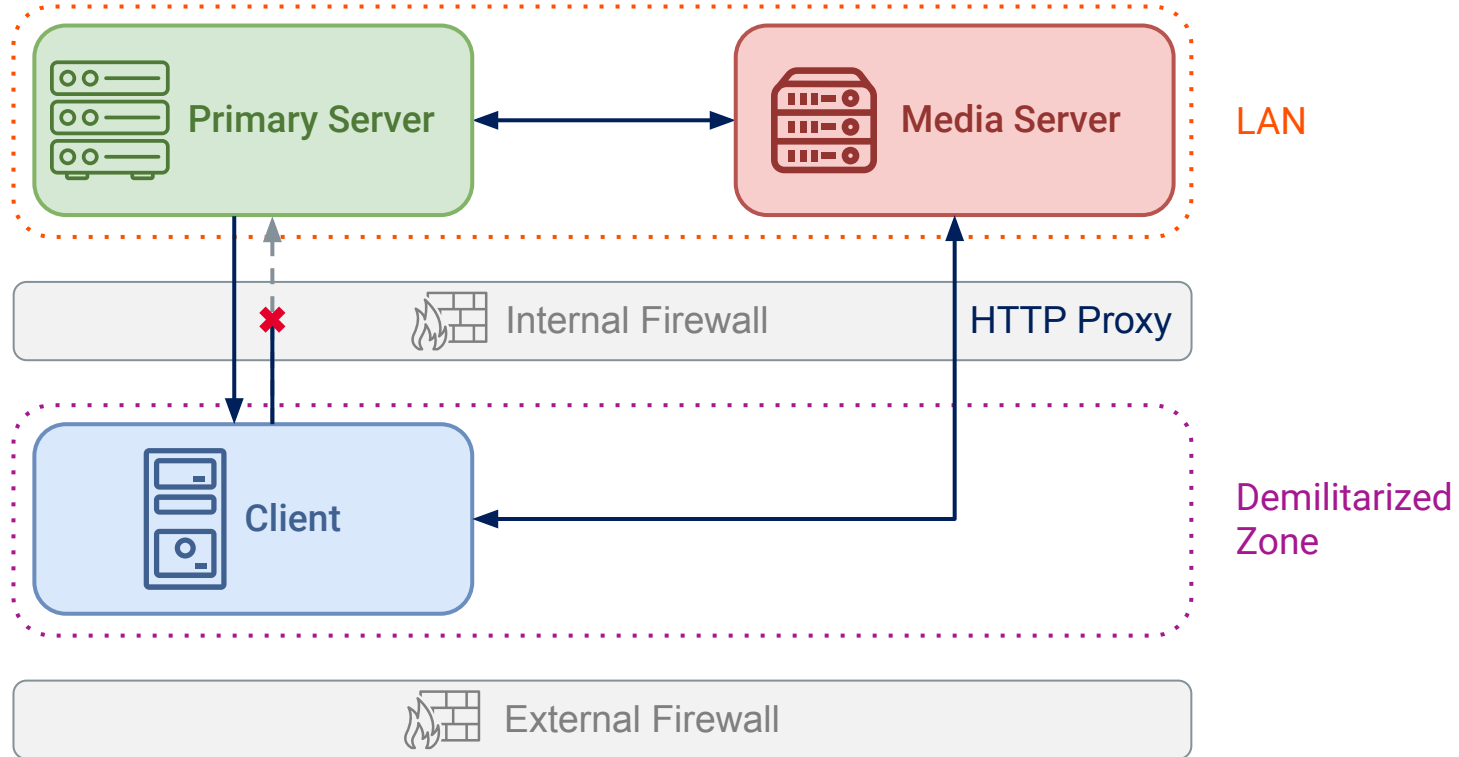
HOW WE DUG INTO NETBACKUP

Understanding A (Simplified) Workflow: The Use Case Of A Client Backup




















HOW WE DUG INTO NETBACKUP

Understanding The Workflow Of Some Edge Cases: The Use Case Of Dmz Clients



HOW WE DUG INTO NETBACKUP

Our Covered Attack Surface

Binary name	Acronym meaning	Client	Media	Primary	OpsCenter
ops_atd	OpsCenter Authentication Daemon				
OpsCenterServerd	OpsCenter Server Daemon				
pbx_exchange	Private Branch Exchange Service				
vnetd	NetBackup Network Communications Service Daemon				
bpcd	NetBackup Client Service Daemon				
nbsl	NetBackup Service Layer				
bprd	NetBackup Request Daemon				
nbatd	NetBackup Authentication Daemon				
NB_dbdrv	NetBackup Relational Database Manager				

HOW WE DUG INTO NETBACKUP

Going Back To A More Standard Approach



Component-specific documentation

⇒ Veritas knowledge base



Static analysis

⇒ Linux & Windows



Process debugging

⇒ perf-tools (ebpf), GDB / x64dbg, function hooking



Network traffic analysis

⇒ Wireshark, MITM (pynet), TLS decryption



Custom tooling

⇒ Scripts, plugins, etc.



Follow logs

⇒ Debug level contains *a lot of very useful* information

⇒ inotify, Git to track modified files

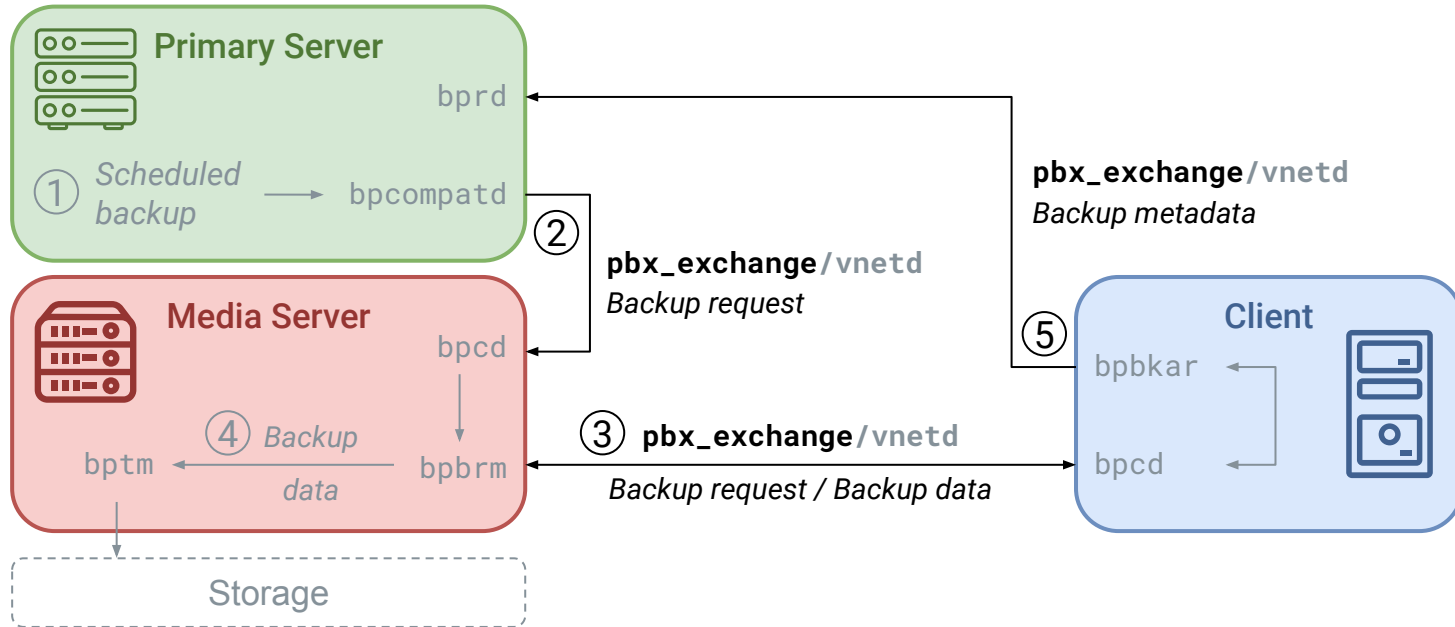
HOW WE DUG INTO NETBACKUP

The Role Of pbx_exchange



> **pbx_exchange**

- > The Private Branch Exchange (PBX) service provides single-port access to clients outside
- > the firewall that connect to Veritas product services



HOW WE DUG INTO NETBACKUP

The Role Of pbx_exchange



> **pbx_exchange**

- > The Private Branch Exchange (PBX) service provides single-port access to clients outside
- > the firewall that connect to Veritas product services

```
# ss | grep pbx_exchange
127.0.0.1:42437 pbx_exchange
127.0.0.1:33075 pbx_exchange
127.0.0.1:1557 pbx_exchange
0.0.0.0:1556 pbx_exchange
```

```
# ss | grep pbx_exchange
127.0.0.1:36493 pbx_exchange
127.0.0.1:35003 pbx_exchange
127.0.0.1:1557 pbx_exchange
0.0.0.0:1556 pbx_exchange
```

```
# ss | grep pbx_exchange
127.0.0.1:41011 pbx_exchange
127.0.0.1:32841 pbx_exchange
127.0.0.1:1557 pbx_exchange
0.0.0.0:1556 pbx_exchange
```

```
# ss | grep pbx_exchange
127.0.0.1:36227 pbx_exchange
127.0.0.1:33765 pbx_exchange
127.0.0.1:1557 pbx_exchange
0.0.0.0:1556 pbx_exchange
```

HOW WE DUG INTO NETBACKUP

The Role Of pbx_exchange

pbx init

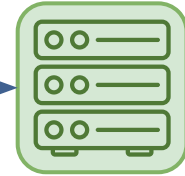
```
ack=25
extension=bprd
```

secure comm init



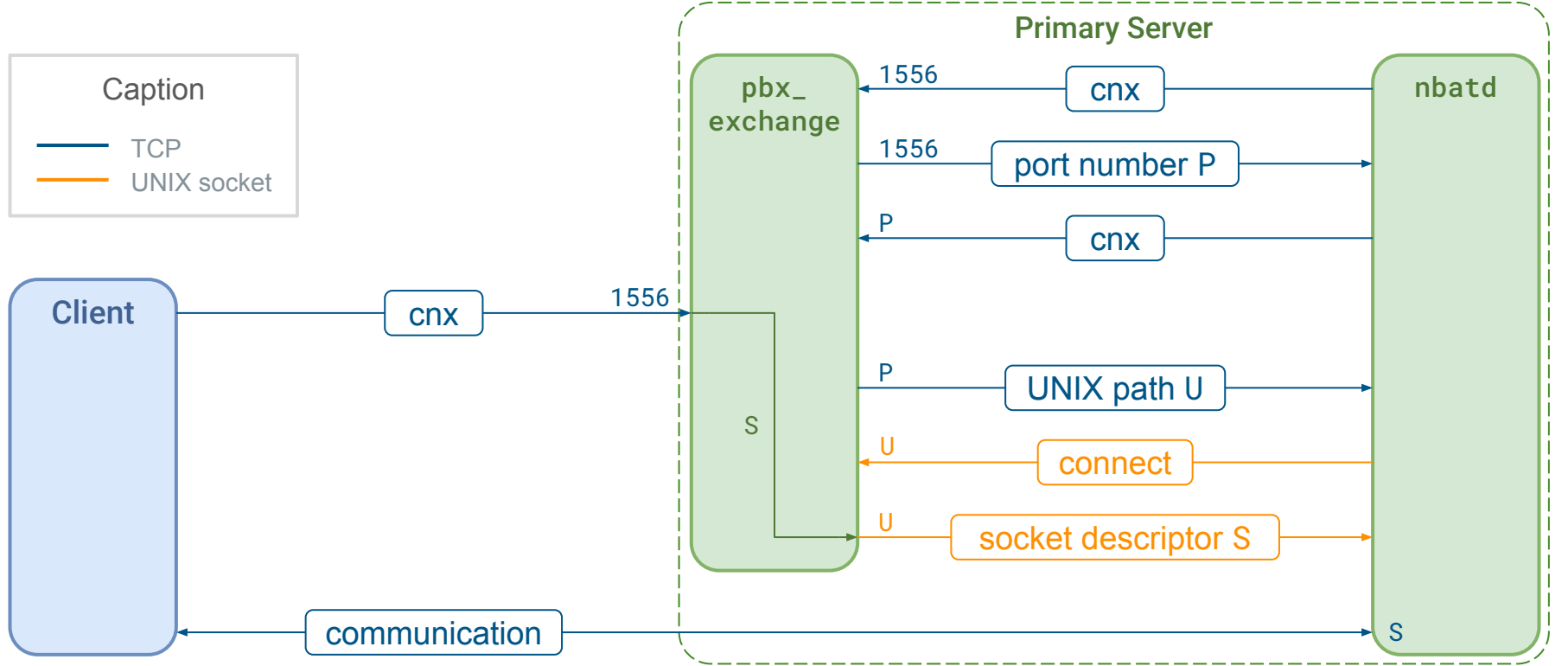
TLS handshake

```
.....{"remote_proxy_info": {"ca_roots": ["126ff840-839e-4701-bb7b-dc3d55697991"], "ca_roots_excluded":
["UNCONSTRAINED"], "issuers_included": [{"domain_id": "126ff840-839e-4701-bb7b-dc3d55697991", "ca_usage":
"NBCA"}], "issuers_excluded": [], "is_eca_compatible": false, "connection_id": "{8D0252DE-6538-11EB-
B868-6C23D53C462D}:INBOUND", "pid": 1187, "proxy_version": 1}, "remote_endpoint_info": {"bpcd_info": null,
"i_am_daemon": true, "domain_constraints": {"svc_type": 1}, "service": "bprd", "auth_only": false,
"auth_flipped": false, "pid": 6032, "exe_name": "bprd", "ssa": false, "local_user": "root", "NB_ORG_USER":
null, "local_group": "root", "host": "192.168.122.148", "peer_host": "192.168.122.148", "peer_client":
null, "local_client": "localhost.localdomain", "local_dhcp_interval": 0, "peer_dhcp_info": null,
"local_hostname": "nb-master", "light_proxy": false, "secure_peer": true, "resilient": false,
"nbrntd_peer_addr": null, "nbrntd_sock_addr": null, "hand_back": false, "request_timeout": 300,
"reverse_connect": false, "accept_reverse": false}}.....{"remote_proxy_info": {"ca_roots":
["126ff840-839e-4701-bb7b-dc3d55697991"], "ca_roots_excluded": ["UNCONSTRAINED"], "issuers_included":
[{"domain_id": "126ff840-839e-4701-bb7b-dc3d55697991", "ca_usage": "NBCA"}], "issuers_excluded": [],
"is_eca_compatible": false, "connection_id": "{8D02B42C-6538-11EB-A0F4-186A926F8830}:OUTBOUND", "pid":
5633, "proxy_version": 1}, "remote_endpoint_info": {"bpcd_info": null, "i_am_daemon": false,
"domain_constraints": {}, "service": "bprd", "auth_only": false, "auth_flipped": false, "pid": 5713,
"exe_name": "bpcIntcmd", "ssa": false, "local_user": "root", "NB_ORG_USER": null, "local_group": "root",
"host": "nb-master", "peer_host": "nb-master", "peer_client": null, "local_client": "nb-client2",
"local_dhcp_interval": 0, "peer_dhcp_info": null, "local_hostname": "nb-client2", "user_info_uid": 0,
"user_info_gid": 0, "light_proxy": false, "secure_peer": true, "resilient": false, "nbrntd_peer_addr":
null, "nbrntd_sock_addr": null, "hand_back": false, "request_timeout": 310, "reverse_connect": false,
"accept_reverse": false}}.....[PR.....r.L.X.....Ab.Y.n.0..(.$.
.....k.j.i.h.9.8.7.6.2...*.&.....=.5./+.'.#... ..g.@.?.>.3.2.1.0.1.-.).
%......<./.....I.....
.....#...
.....B...>...Z....k. ....'.....>Mx...f_.2.i..
0.....#.....0...0..P.....V.'.....0
.....*H..
..
..071.0
..U...broker1.0...U...root@nb-master1.0 ..U.
..vx0..
210201085844Z.
220201101344Z0P1.0+...U...$126ff840-839e-4701-bb7b-dc3d556979911.0...U... NBU_HOSTS1.0 ..U.
..vx0..0
.....*H..
.....0.....!.....j[.../H.b2.T.Xa.Py2.Y...i.s....C.
..U.[4xJ,V.5h]..u`...8.^...;:yW\...9..R...t 2[...~...~..W....8.....Z.....Z]~.H..C.....
0...0...U.....0.0...*...
```



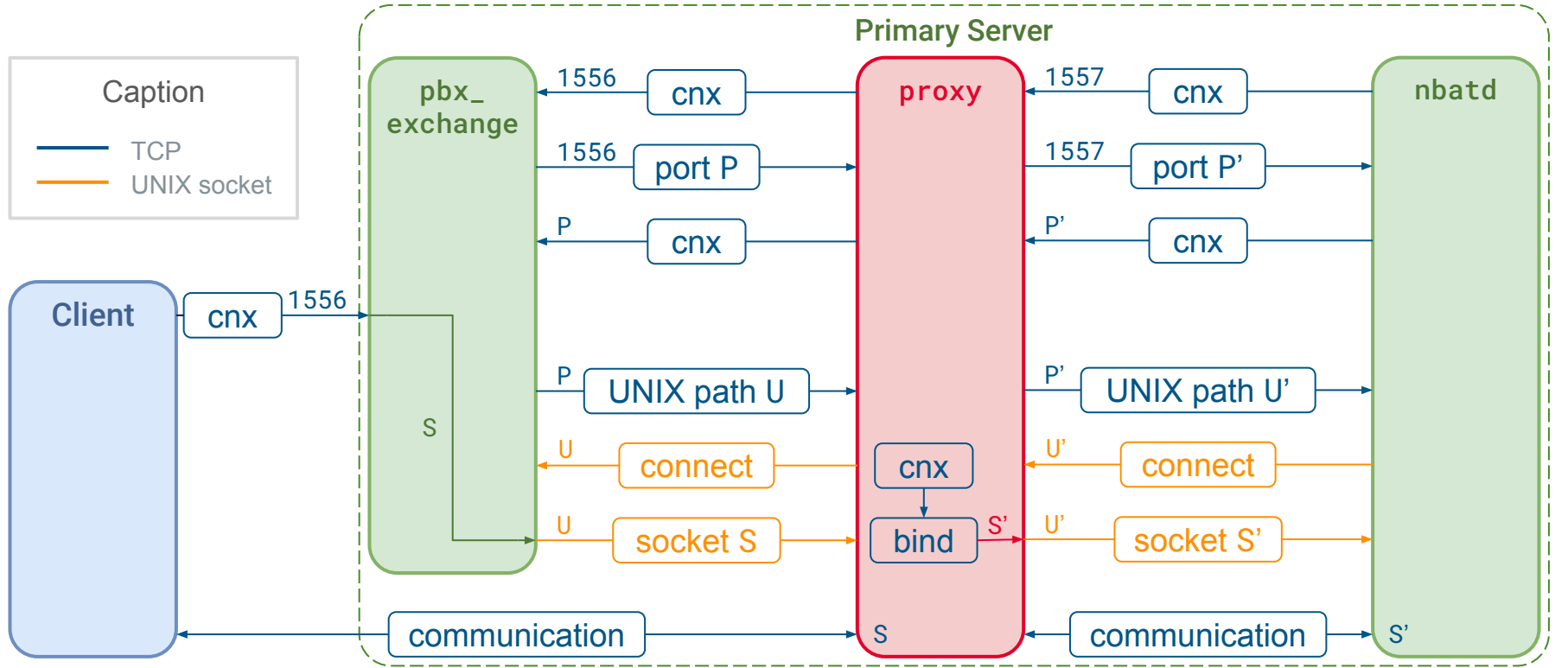
HOW WE DUG INTO NETBACKUP

Component Communication With pbx_exchange: Example Of nbatd



HOW WE DUG INTO NETBACKUP

Component Communication With pbx_exchange: MITM-ing nbatd



HOW WE DUG INTO NETBACKUP

Remote Procedure Call: Example Of CORBA



BeeRumP Paris 2016: *APT Cyber-Numerique Sur Sauvegardiciel Connecté* – Émilien Girault

Time	Source	Destination	Protocol	Length	Info
2 1989.2637314...	192.168.122.238	192.168.122.26	GIOP	200	GIOP 1.2 Request, s=120 id=0: op=_non_existent
6 1989.3415779...	192.168.122.26	192.168.122.238	GIOP	368	GIOP 1.2 Reply, s=288 id=0: Location Forward

▶ Frame 7086: 368 bytes on wire (2944 bits), 368 bytes captured (2944 bits) on interface 0	
▶ Linux cooked capture	
▶ Internet Protocol Version 4, Src: 192.168.122.26, Dst: 192.168.122.238	
▶ Transmission Control Protocol, Src Port: 1556, Dst Port: 41985, Seq: 2, Ack: 155, Len: 300	
▶ General Inter-ORB Protocol	
▶ General Inter-ORB Protocol Reply	

0000	00 00 00 01 00 06 52 54	00 59 5f d4 00 00 08 00RT_Y.....
0010	45 00 01 60 6d a0 40 00	40 06 55 9e c0 a8 7a 1a	E...m@...@U...z...
0020	c0 a8 7a ee 06 14 a4 01	f3 ad 5f 79 13 fa b1 f1	...z..._...y...
0030	80 18 00 eb 77 ac 00 00	01 01 08 0a 01 f3 a0 2f	...w.../...
0040	9f 68 b4 d5 47 49 4f 50	01 02 01 01 20 01 00 00	..h..GIOP.....
0050	00 00 00 00 03 00 00 00	00 00 00 00 2d 00 00 00
0060	49 44 4c 3a 56 65 72 69	74 61 73 2f 4e 65 74 42	IDL:Veri tas/NetB
0070	61 63 6b 75 70 2f 48 6f	73 74 53 65 73 73 69 6f	ackup/Ho stSessio
0080	6e 46 61 63 74 6f 72 79	3a 31 2e 30 00 00 00 00	nFactory :1.0....
0090	01 00 00 00 01 49 43 4f	d4 00 00 00 01 01 02 00ICO
00a0	0a 00 00 00 6e 62 2d 6d	61 73 74 65 72 00 14 06nb-m aster...
00b0	05 00 00 00 6e 62 73 6c	00 00 20 00 1b 00 00 00nbsl
00c0	14 01 0f 00 52 53 54 d2	59 3d 63 ec de 04 00 00RST_Y=c.....
00d0	00 00 00 01 00 00 00 01	00 00 00 00 04 00 00 00
00e0	00 00 00 00 08 00 00 00	01 28 52 03 00 4f 41 54(R...OAT
00f0	01 00 00 00 14 00 00 00	01 28 52 03 01 00 01 05(R...OAT
0100	00 00 00 00 09 01 01 00	00 00 00 00 00 49 43 4fICO
0110	18 00 00 00 01 28 a7 00	86 00 00 00 0c 00 00 00(.....
0120	6e 62 73 6c 5f 73 65 63	73 76 63 00 03 00 00 00	nbsl_sec svc.....
0130	3c 00 00 00 01 28 52 03	0f 00 00 00 31 39 32 2e	<.....(R...192.
0140	31 36 38 2e 31 32 32 2e	32 36 00 00 14 06 00 00	168.122. 26.....
0150	05 00 00 00 6e 62 73 6c	00 00 a7 00 86 00 00 00nbsl
0160	0c 00 00 00 6e 62 73 6c	5f 73 65 63 73 76 63 00nbsl_secsvc...

⇒ CORBA with proprietary layer (PBXIOP) in C++ binaries

HOW WE DUG INTO NETBACKUP

Remote Procedure Call: find To The Rescue

```
[root@nb-opscenter ~]# find / -iname "*orb*.jar" -o -iname "*iop*.jar" 2>/dev/null
/opt/SYMCopsCenterServer/lib/pbxiorp2.jar
/opt/SYMCopsCenterServer/lib/corbaservice.jar
/opt/SYMCopsCenterServer/lib/nbu_corba.jar
/opt/SYMCopsCenterServer/lib/corbaservice_idl.jar
/opt/SYMCopsCenterServer/lib/jacorb-omgapi.jar
/opt/SYMCopsCenterServer/lib/jacorb-services.jar
/opt/SYMCopsCenterServer/lib/jacorb.jar
/opt/SYMCopsCenterServer/lib/vxssiorp2.jar
/opt/SYMCopsCenterGUI/webserver/webapps/opscenter/WEB-INF/lib/corbaservice_idl.jar
/opt/SYMCopsCenterGUI/webserver/webapps/opscenter/WEB-INF/lib/jacorb-omgapi.jar
/opt/SYMCopsCenterGUI/webserver/webapps/opscenter/WEB-INF/lib/jacorb-services.jar
/opt/SYMCopsCenterGUI/webserver/webapps/opscenter/WEB-INF/lib/jacorb.jar
/opt/SYMCopsCenterGUI/webserver/webapps/opscenter/WEB-INF/lib/nbu_corba.jar
/opt/SYMCopsCenterGUI/webserver/webapps/opscenter/WEB-INF/lib/pbxiorp2.jar
/opt/SYMCopsCenterGUI/webserver/webapps/opscenter/WEB-INF/lib/vxssiorp2.jar
```

HOW WE DUG INTO NETBACKUP

Remote Procedure Call: (Not) Learning CORBA

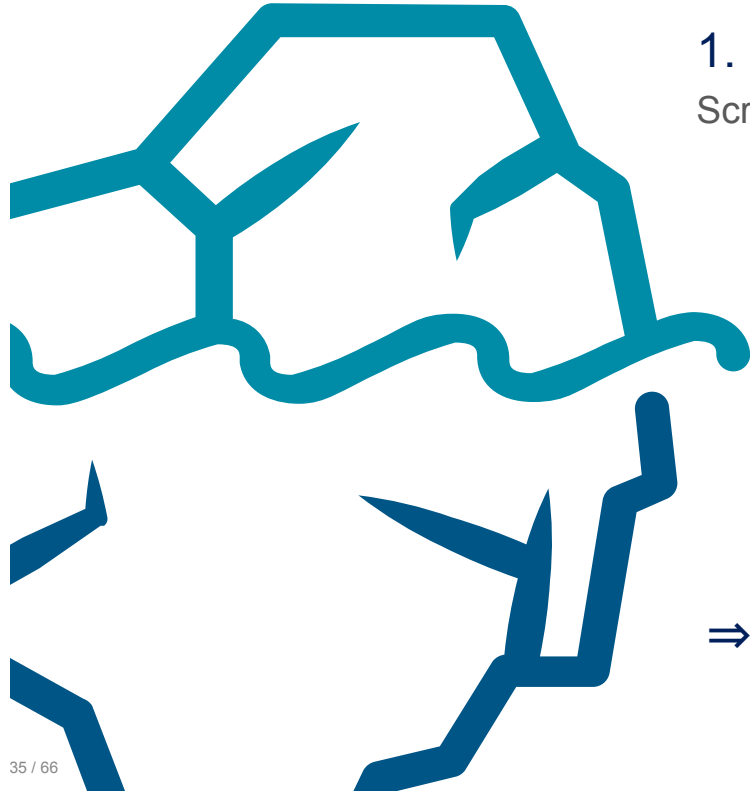
```
public static synchronized DiscoveryService getDiscoveryService(String serverHostname) {
    String servantName = "DiscoveryService";
    String pbxServiceName = "DiscoveryService";
    org.omg.CORBA.ORB localOrb = makeLocalOrb(servantName, pbxServiceName);
    String corbaloc = OrbUtil.createPBXCorbaLoc(serverHostname, 1556, pbxServiceName, servantName, false);
    org.omg.CORBA.Object remoteObject = localOrb.string_to_object(corbaloc);
    return DiscoveryServiceHelper.narrow(remoteObject);
}

public static synchronized void testDiscoSvc(String serverHostname) {
    DiscoveryService service = getDiscoveryService(serverHostname);
    service.registerExplorer("A", "B", "C", "D", AuthorityType.AT_ANYANDALL, (short)10);
}

public static void main(String[] args) {
    String serverHostname = "192.168.1.100";
    testDiscoSvc(serverHostname);
}
```

HOW WE DUG INTO NETBACKUP

Summary



1. Learned about the target

Scratched the surface to avoid falling too deep

2. Tried to keep head out of the water

Took step back when lost: relied on documentation & architects

3. Dove deeper into ~8 binaries

Focused on (our understanding of) critical components

⇒ ~30 CVEs published

⇒ Only the top of the iceberg has been studied!



1

INTRODUCTION

2

LET'S MEET NETBACKUP

Target Overview: Key Technical Aspects

3

HOW WE DUG INTO NETBACKUP

The Approach, The Challenges And How We Tackled Them

4

FINDINGS

Overview Of Vulnerabilities And Attack Paths

5

TAKEAWAYS

FINDINGS

Disclaimer



- Coordinated disclosure with Veritas
 - Disclosed vulnerabilities
 - Patches are available to customers
 - Veritas published CVEs & security advisories
- Present *our* understanding
 - We are in no way NetBackup experts
 - Did not study every configuration option
 - Focused on version 8.2

FINDINGS

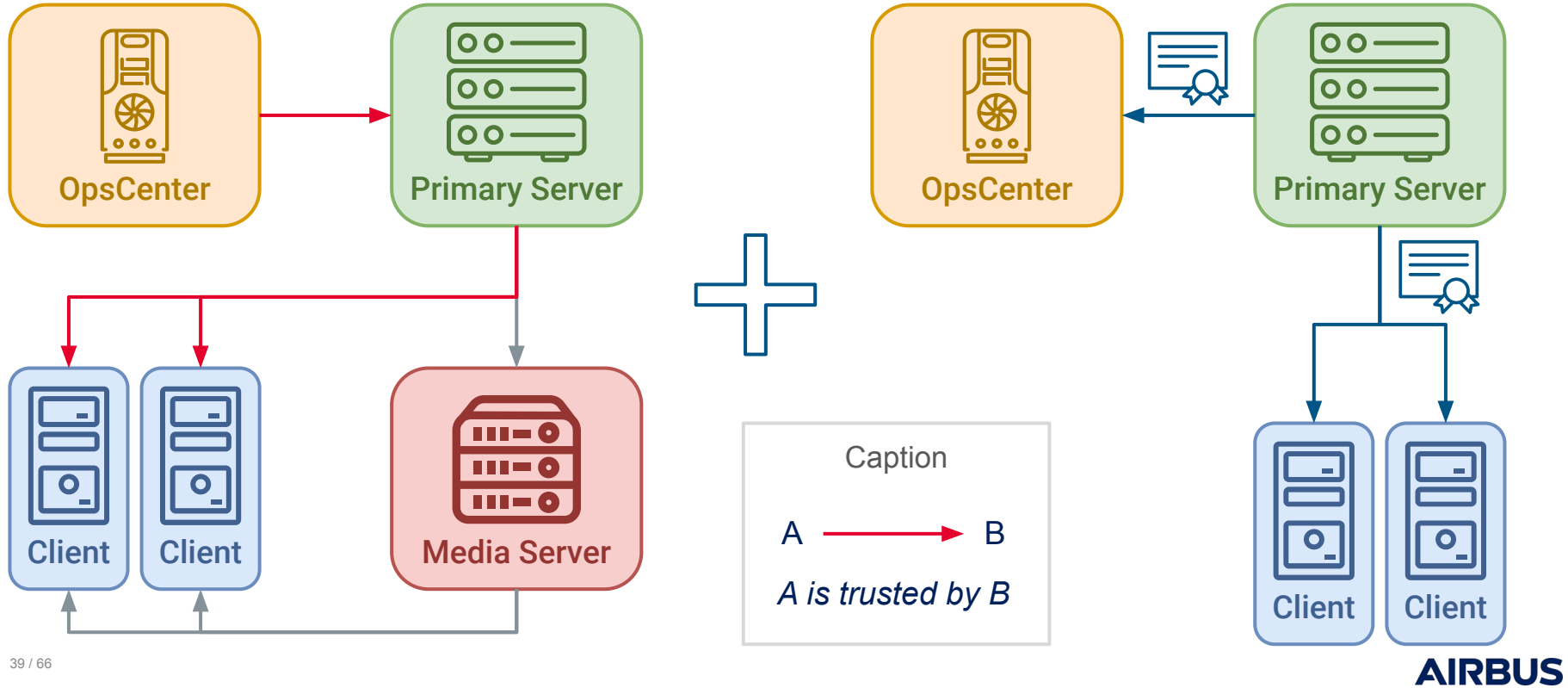
Quick Overview Of Discovered Vulnerabilities

Binary name	Vulnerabilities
bpcd	LPE
bprd	Authenticated RCE, arbitrary file read/write, arbitrary traversal file write, DoS, info leak, arbitrary directory creation
nbatd	Pre-auth DoS
nbsl	Authenticated RCE
ops_atd	Pre-auth DoS
pbx_exchange	Arbitrary file deletion, XXE, DoS
OpsCenterServerd	Unauthenticated RCE, unauthorized account creation, LPE, info leak
Ops Java Web Server	Unauthenticated RCE, web UI authentication bypass
bpdgclone	Local command injection
nbars	XXE, DoS
DiscoveryService	SQLi, DoS, XML injection, path traversal, DOM XSS

Severity: Critical, High, Medium, Low

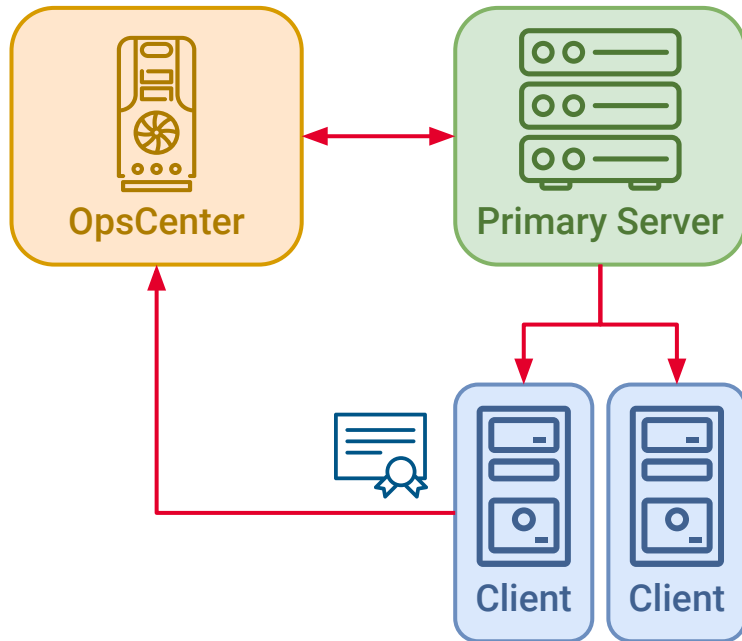
FINDINGS

Example: Exploiting The Trust Chain With Secure Communication And NBAC



FINDINGS

Example: Understanding The *Practical* Trust Chain With NBAC



⇒ Access to authenticated endpoints (CORBA)

```
UserImpl user = new UserImpl();
user.uniqueIdentifier = "backdoor";
// ...
SecurityMemberImpl member = new SecurityMemberImpl();
member.uniqueId = "backdoor";
member.password = "password";
// ...
manager.createUser(user, member, true, viewList);
```


FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers - Attacking From The LAN


Approach:

- Attempted to open CORBA connection to all known pbx_exchange services
 - Checked for NO_PERMISSION / OBJECT_NOT_EXIST / COMM_FAILURE errors
- Discovered services with unauthenticated CORBA endpoints:
 - DiscoveryService (DiscoveryService)
 - nbevtmgr (Event.EventMgr)
 - NBFSMCLIENT (FSM.ClientClusterMgr)
- Found a variety of vulnerabilities, some more interesting than others
⇒ Let's talk about a couple of them!

FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers – SQL injection (CVE-2022-42302)

```
ClientClusterMgr manager = getClientClusterMgr(serverHostname);  
manager.updateActiveAppClusters("injection'");--", new String[0], false);
```



```
SELECT A.MachineKey, A.MachineID, A.FQMachineName, [...]  
FROM EMM_Machine A  
left outer join EMM_Machine X ON A.ParentKey = X.MachineKey  
[...]  
WHERE UPPER(EMM_MachineAlias.MachineAliasName)  
= UPPER('injection');-- ) AND EMM_MachineAlias.MachineNbuType [...]
```

FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers – Dead End?

Permissions:

- SQLAnywhere runs as root / SYSTEM
- EMM_MAIN database user has access to list of hosts, disks, jobs, some credentials...

Limitations:

- Requests are not stackable
- Blind injection
- Many functions are undefined (e.g. xp_cmdshell)
- EMM_MAIN user doesn't have permission to read / write files
- Valid NetBackup hosts require a database entry + a file
- No interesting data found in our lab in these tables

FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers – Digging Around

Where to go from there?

- Requests are stackable in newer versions
- SQLAnywhere allows INSERT in SELECT statement!
- Second order SQLi can be triggered in JOBD_MAIN database (CVE-2022-42303)
- Still no RCE in sight...


⇒ What if we abuse NetBackup features and logic?

FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers – Path Traversal (CVE-2022-42305)



```
service.registerExplorer(  
    "A", "B", "C", "../D", AuthorityType.AT_ANYANDALL, (short)10  
);
```



Unable to open /usr/opencv/netbackup/db/discovery/4 ../d c.xml
Failed to persist discovery record.

FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers – URL encoding / decoding

```
service.registerExplorer(  
    "A", "B", "/C1\\\\" + "\0\0blahblah", "\\plopiplop\0\01234",  
    AuthorityType.AT_ANYANDALL, (short)10  
);
```

→

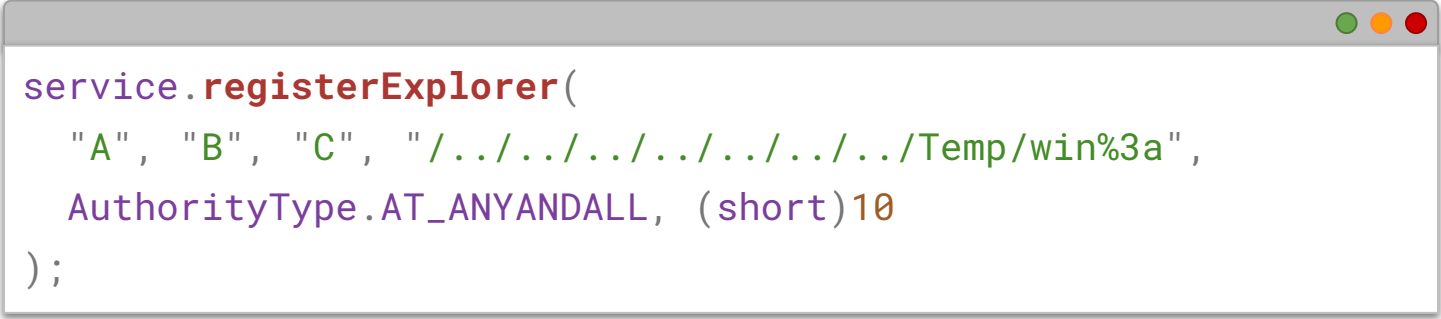
```
-rw-r--r-- 1 root root 181 '4 \plopiplop %252fc1%255c.dat'  
-rw-r--r-- 1 root root 325 '4 \plopiplop %252fc1%255c.xml'
```

decoded

encoded

FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers – Path Traversal + Alternate Data Stream



```
service.registerExplorer(  
    "A", "B", "C", "../../../../../../../../Temp/win%3a",  
    AuthorityType.AT_ANYANDALL, (short)10  
);
```

(Ab)use special NetBackup files to bypass authentication:

- /usr/opensv/var/bprd/remote_ops/<hostname>
- /usr/opensv/var/vxss/credentials/dhcp_cred
- /usr/opensv/var/vxss/credentials/match_required.txt
- /usr/opensv/var/vxss/credentials/no_match_required.txt

FINDINGS

Example: A Tale Of CORBA On Windows Primary Servers – Full Chain

1. Path traversal (CVE-2022-42305)

⇒ Create `../../../../var/bprd/remote_ops/<hostname>`

2. SQL injection (CVE-2022-42302)

⇒ Add host as “known” NetBackup client in EMM_MAIN database

Authentication bypass

3. Authenticated RCE (e.g. CVE-2022-36989)

⇒ Execute arbitrary code from NetBackup client to Primary Server

4. Let's see a demo!

⇒ Exploit full chain of vulnerabilities

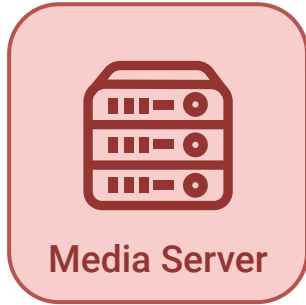


DEMO

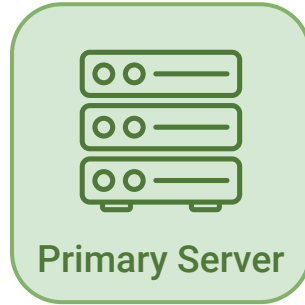
CVE-2022-36989, CVE-2022-42302, CVE-2022-42305

FINDINGS

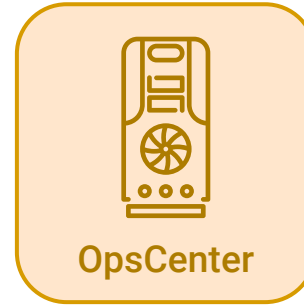
Playing Out Attack Scenarios



?



?



?

?

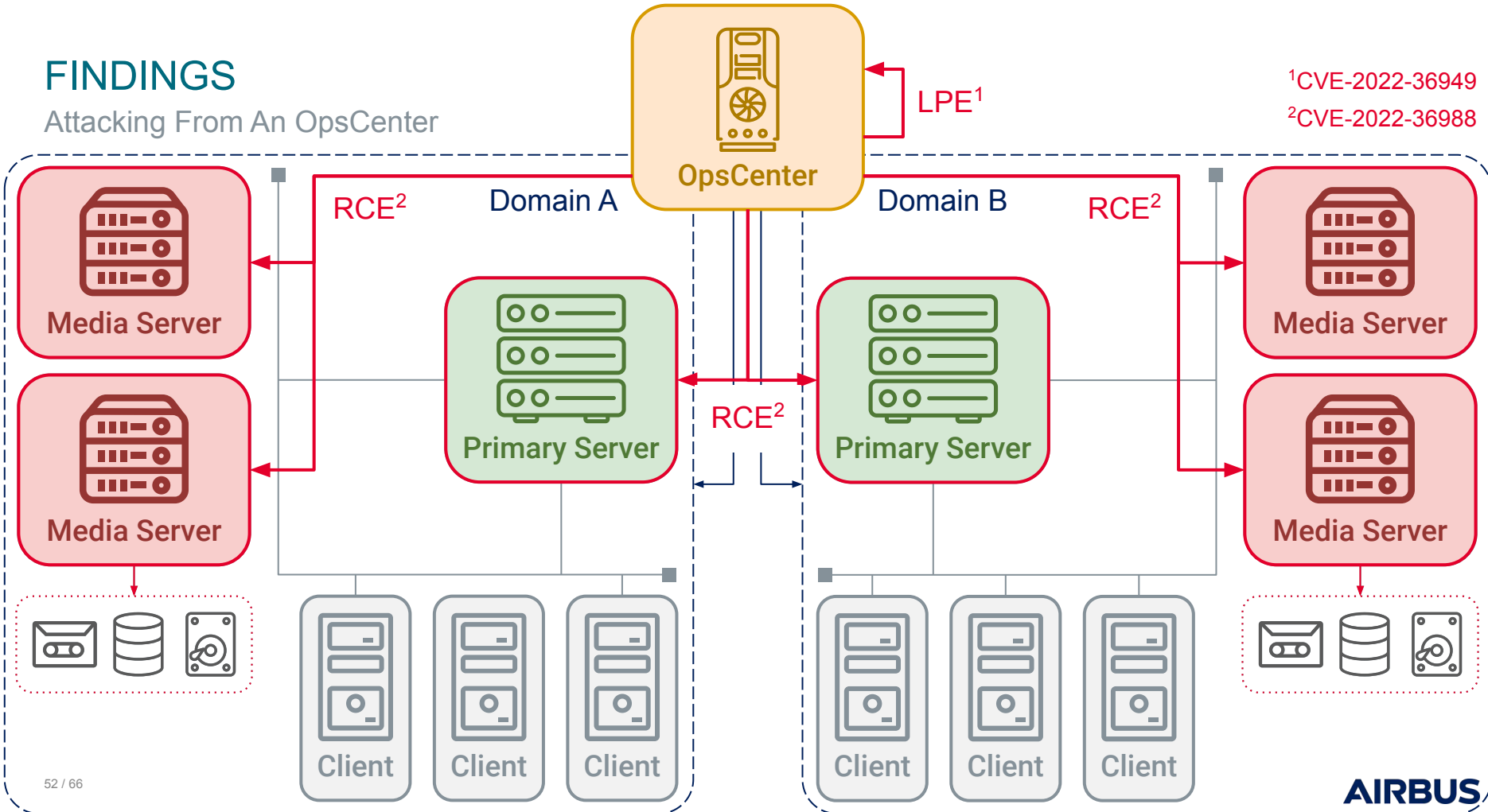


?



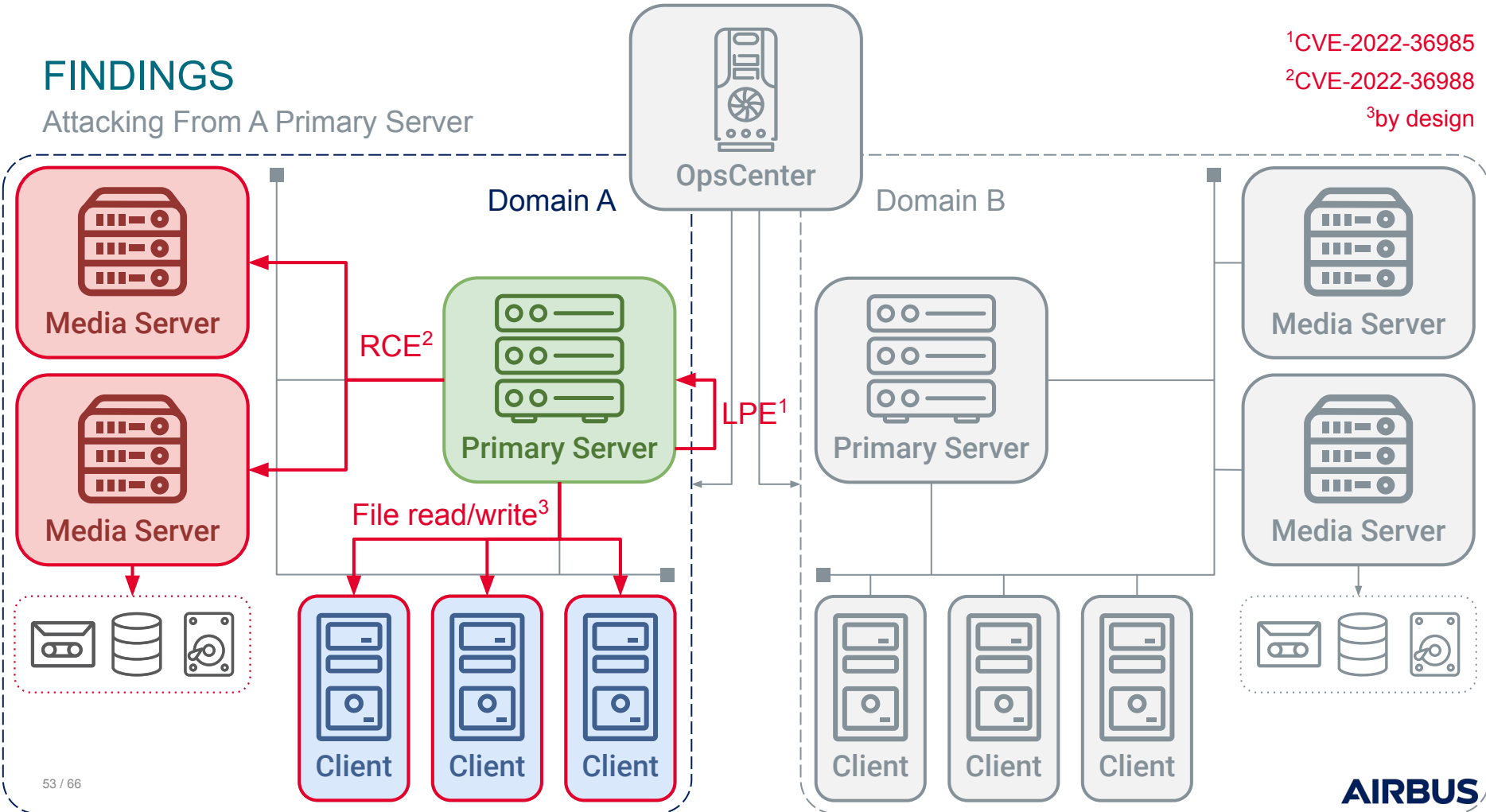
FINDINGS

Attacking From An OpsCenter



FINDINGS

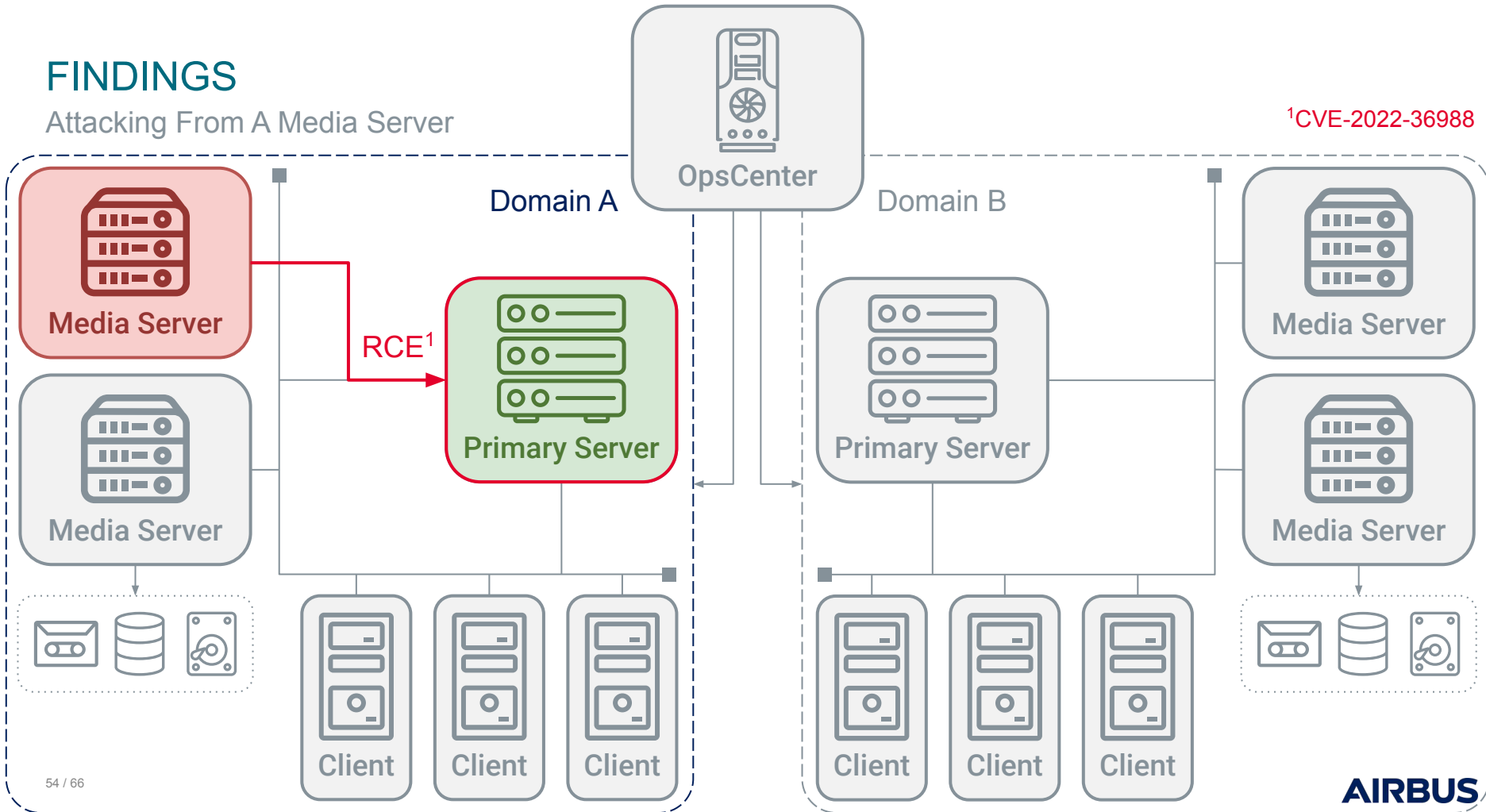
Attacking From A Primary Server



FINDINGS

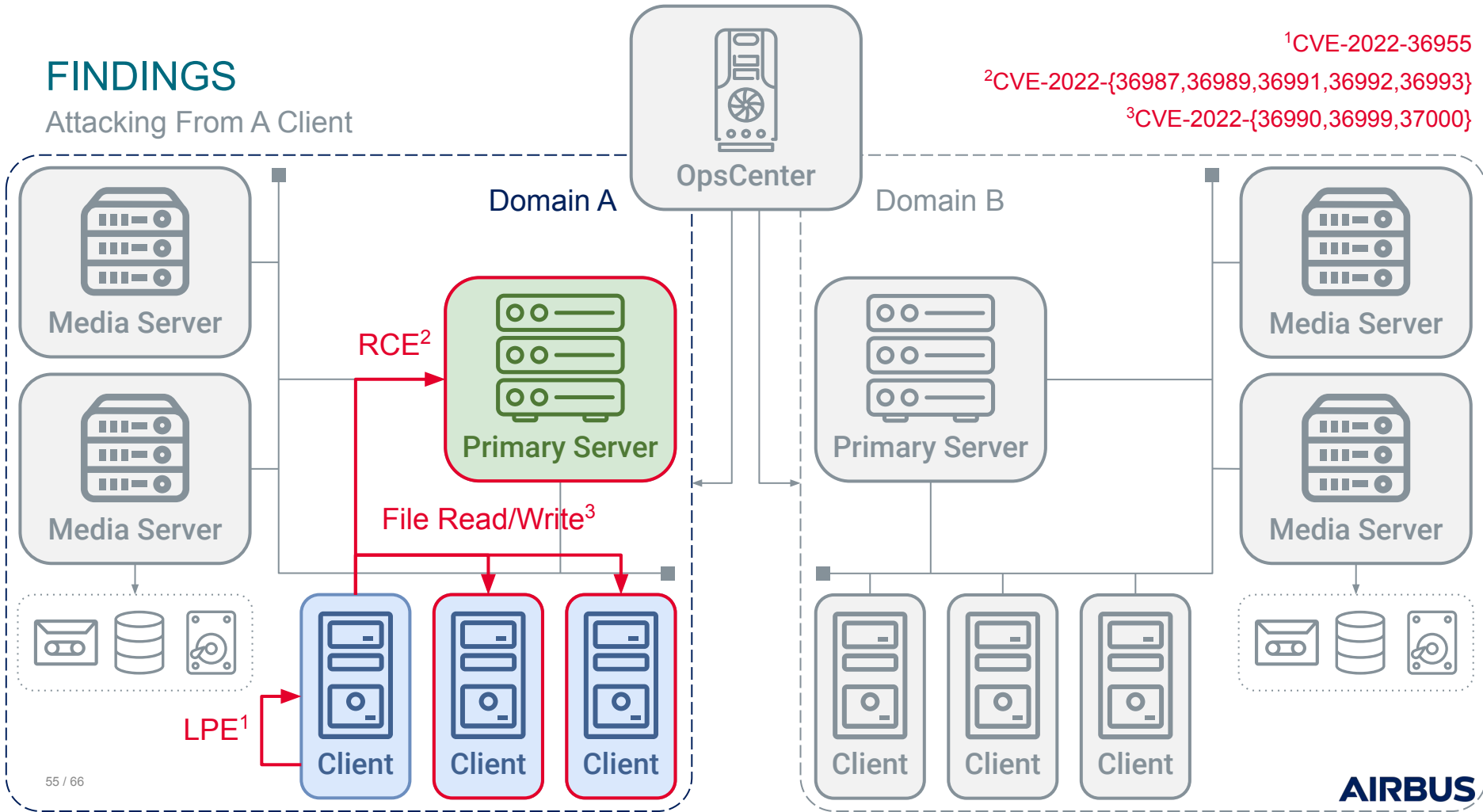
Attacking From A Media Server

¹CVE-2022-36988



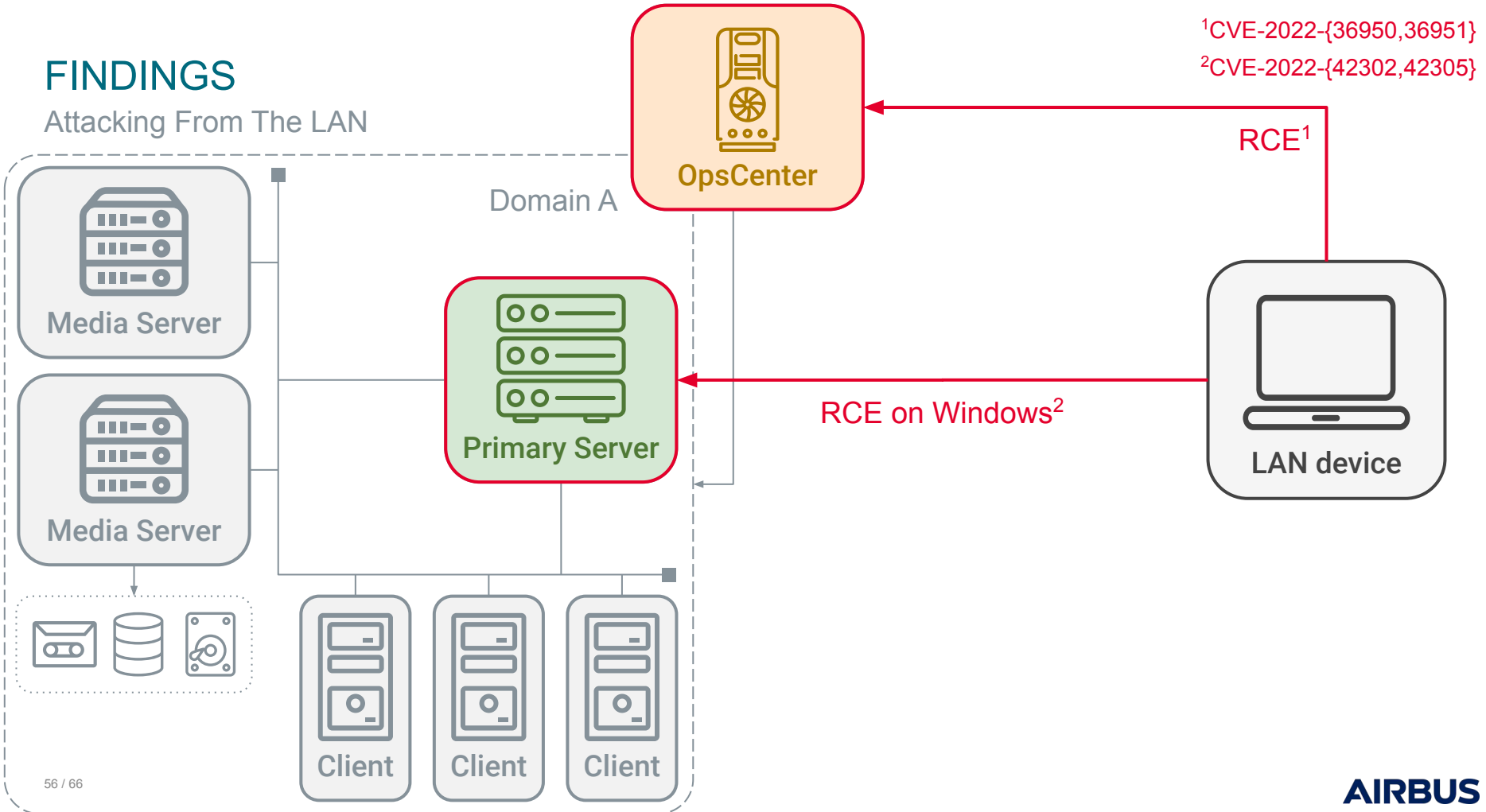
FINDINGS

Attacking From A Client



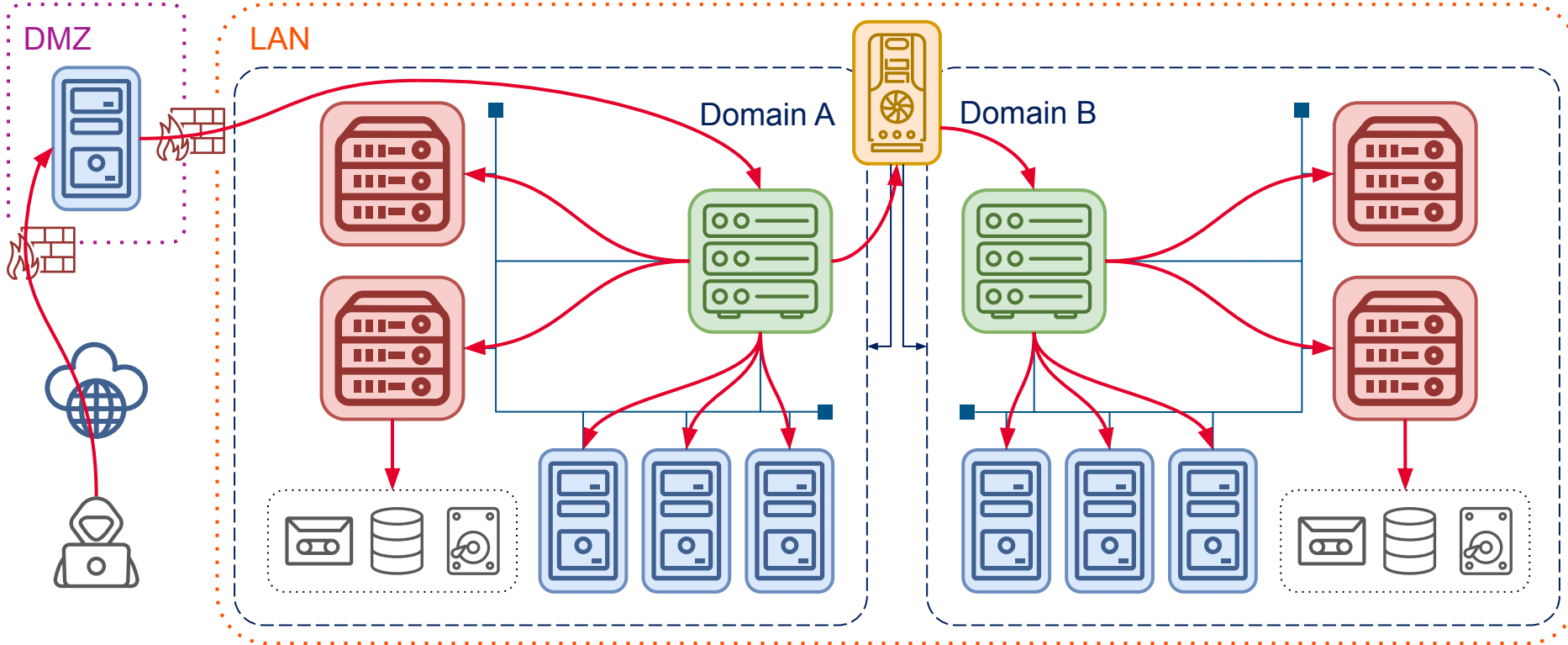
FINDINGS

Attacking From The LAN



FINDINGS

Example Real World Scenario





DEMO

CVE-2022-36951, CVE-2022-36988, CVE-2022-36989

FINDINGS

Reviewing Security Questions



1. What would it take for an attacker to exploit NetBackup?
⇒ **Specific tooling & workflow knowledge**, not out of reach of motivated attackers
⇒ pbx_exchange, backup policies, trust model, NetBackup commands, etc.



2. Can a Primary Server be compromised from a NetBackup client?
⇒ **Yes**, and much more



3. Could the NetBackup system be used as a pivot to attack other interconnected systems?
⇒ **Yes**, as shown in our demo



4. Which data could an attacker target to prevent NetBackup recovery?
⇒ **Let's take a step back**

FINDINGS

Minimal Requirements To Restore A NetBackup Infrastructure



Backup data (obviously)
⇒ To restore clients' files



Primary server catalog
⇒ To know where to find clients' data



Media server deduplication catalog (if enabled)
⇒ To rebuild full backups



Encryption secret(s) (if enabled)
⇒ To decrypt stored data



Disaster recovery file (optional)
⇒ To automate some recovery steps

FINDINGS

Reviewing Security Questions



1. What would it take for an attacker to exploit NetBackup?
⇒ **Specific tooling & workflow knowledge**, not out of reach of motivated attackers
⇒ pbx_exchange, backup policies, trust model, NetBackup commands, etc.



2. Can a Primary Server be compromised from a NetBackup client?
⇒ **Yes**, and much more



3. Could the NetBackup system be used as a pivot to attack other interconnected systems?
⇒ **Yes**, as shown in our demo



4. Which data could an attacker target to prevent NetBackup recovery?
⇒ **Backup data, catalogs, encryption secrets, disaster recover file**

FINDINGS

Disclosure Timeline

FIRST VULNERABILITY REPORT

- **2021-10-13:** SecLab sent first report to Veritas.
- **2021-11-22:** Veritas acknowledged the report and ask some more details.
- **2021-12-13:** SecLab provided answer to Veritas and a reminder about the 90 days policy.
- **2022-01-26:** Veritas answered with the expected timeline of patch for the different component.
- **2022-02-28:** Veritas provided patches of NetBackup OpsCenter to SecLab for review.
- **2022-05-10:** First patch for NetBackup Primary Server, Media Servers released.
- **2022-07-13:** Veritas released patches and a security advisory for NetBackup OpsCenter: [VTS22-009](#).
- **2022-07-18:** Veritas released a security advisory for NetBackup Clients, Primary Server, Media Server: [VTS22-004](#) , [VTS22-008](#).
- **2022-09-21:** Veritas released hotfix patches for Clients related to [VTS22-008](#).

SECOND VULNERABILITY REPORT

- **2022-04-11:** SecLab sent a 2nd report to Veritas with more findings.
- **2022-04-11:** Veritas acknowledged the 2nd report.
- **2022-08-01:** Veritas released patch for NetBackup Clients (VTS22-010).
- **2022-08-29:** Veritas released patch for NetBackup Primary Server, Media Server. (VTS22-011)
- **2022-09-23:** Veritas released hotfix patches for NetBackup Primary Server, Media Server. (VTS22-010, VTS22-011)
- **2022-09-26:** New advisories released [VTS22-010](#); [VTS22-011](#); [VTS22-012](#); [VTS22-013](#).



1

INTRODUCTION

2

LET'S MEET NETBACKUP

Target Overview: Key Technical Aspects

3

HOW WE DUG INTO NETBACKUP

The Approach, The Challenges And How We Tackled Them

4

FINDINGS

Overview Of Vulnerabilities And Attack Paths

5

TAKEAWAYS

TAKEAWAYS

1. Discovered vulnerabilities illustrate wide attack surface & security impact

~30 CVEs attributed to Airbus Security Lab, official patches available

Presented attack paths showcase possible impact & complexity

2. Work presented only scratches the surface

Plenty of attack surface not yet studied: there's a lot of room for more work!

Your work is needed and there are plenty of uncharted waters for you to have fun


3. Your favorite enterprise backup software can be broken / better protected

Consider this a gift to convince your employers to let you have an offensive / defensive deep dive!

Skilling-up on such software can help red teaming, pentesting, detecting, etc.

4. The unavoidable pain of backups

Backups are a pain, but French people eat pain for breakfast! 🥖



Thank you for your attention!
Any questions?

<https://airbus-seclab.github.io>



[@AirbusSecLab](https://twitter.com/AirbusSecLab)



[airbus-seclab](https://github.com/airbus-seclab)