# DPS Challenge

Tuesday, June 15, 2021 9:58 PM

| Protocol | Percent Packets | Packets | Percent Bytes |
|---|---|---|---|
| Frame | 100.0 | 59334 | 100.0 |
| Ethernet | 100.0 | 59334 | 1.6 |
| Internet Protocol Version 4 | 99.9 | 59302 | 2.3 |
| User Datagram Protocol | 1.1 | 626 | 0.0 |
| Transmission Control Protocol | 98.9 | 58662 | 96.0 |
| Transport Layer Security | 30.2 | 17931 | 88.2 |
| NetBIOS Session Service | 0.5 | 302 | 1.2 |
| Malformed Packet | 0.0 | 16 | 0.0 |
| Hypertext Transfer Protocol | 0.8 | 452 | 2.1 |
| Data | 0.3 | 149 | 1.5 |
| Internet Group Management Protocol | 0.0 | 8 | 0.0 |
| Internet Control Message Protocol | 0.0 | 6 | 0.0 |
| Address Resolution Protocol | 0.1 | 32 | 0.0 |

Not much in terms of UDP. If we briefly scroll through the packets, we'll see most of the TLS packets are actually HTTPS. No way to decrypt (if you observe the handshakes, they're Diffie-Hellman and RSA, uncrackable. You're going to have to find a key to decrypt if that's the intended solution).

Expand the NetBIOS Session and you'll see that SMB2 is also pretty common. Other things to look at usually are DNS packets, but there is nothing of interest there.

| | | |
|---|---|---|
| NetBIOS Session Service | 0.5 | 302 |
| SMB2 (Server Message Block Protocol version 2) | 0.5 | 290 |
| Distributed Computing Environment / Remote Procedure Call (DCE/RPC) | 0.0 | 4 |
| Server Service | 0.0 | 2 |
| SMB (Server Message Block Protocol) | 0.0 | 4 |

Filter for NBSS (or SMB2 if you want to be more specific) and scrolling through, you can see that files are accessed (Create/Find/GetInfo/Close)

```
49273 129.444039   192.168.200.5   192.168.200.7   SMB2   150 GetInfo Response
49275 129.444142   192.168.200.7   192.168.200.5   SMB2   146 Close Request File:
49276 129.444172   192.168.200.5   192.168.200.7   SMB2   182 Close Response
49278 129.444306   192.168.200.7   192.168.200.5   SMB2   179 Create Request File:
49279 129.444364   192.168.200.5   192.168.200.7   SMB2   210 Create Response File:
49281 129.444465   192.168.200.7   192.168.200.5   SMB2   163 GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
49282 129.444501   192.168.200.5   192.168.200.7   SMB2   234 GetInfo Response
49284 129.444603   192.168.200.7   192.168.200.5   SMB2   146 Close Request File:
49285 129.444636   192.168.200.5   192.168.200.7   SMB2   182 Close Response
49287 129.478616   192.168.200.7   192.168.200.5   SMB2   126 KeepAlive Request
49288 129.478719   192.168.200.5   192.168.200.7   SMB2   126 KeepAlive Response
49290 129.478863   192.168.200.7   192.168.200.5   SMB2   179 Create Request File:
49291 129.478973   192.168.200.5   192.168.200.7   SMB2   210 Create Response File:
49293 129.479079   192.168.200.7   192.168.200.5   SMB2   163 GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
49294 129.479128   192.168.200.5   192.168.200.7   SMB2   234 GetInfo Response
49296 129.479221   192.168.200.7   192.168.200.5   SMB2   146 Close Request File:
49297 129.479264   192.168.200.5   192.168.200.7   SMB2   182 Close Response
49299 129.481118   192.168.200.7   192.168.200.5   SMB2   179 Create Request File:
49300 129.481328   192.168.200.5   192.168.200.7   SMB2   210 Create Response File:
49302 129.481468   192.168.200.7   192.168.200.5   SMB2   163 GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
49303 129.481522   192.168.200.5   192.168.200.7   SMB2   234 GetInfo Response
49305 129.481635   192.168.200.7   192.168.200.5   SMB2   146 Close Request File:
49306 129.481690   192.168.200.5   192.168.200.7   SMB2   182 Close Response
49308 129.495867   192.168.200.7   192.168.200.5   SMB2   179 Create Request File:
49309 129.496053   192.168.200.5   192.168.200.7   SMB2   210 Create Response File:
49311 129.496216   192.168.200.7   192.168.200.5   SMB2   163 GetInfo Request FILE_INFO/SMB2_FILE_ALL_INFO File:
49312 129.497011   192.168.200.5   192.168.200.7   SMB2   234 GetInfo Response
49314 129.497462   192.168.200.7   192.168.200.5   SMB2   146 Close Request File:
49315 129.497515   192.168.200.5   192.168.200.7   SMB2   182 Close Response
49317 129.497673   192.168.200.7   192.168.200.5   SMB2   179 Create Request File:
49318 129.497748   192.168.200.5   192.168.200.7   SMB2   210 Create Response File:
49320 129.497972   192.168.200.7   192.168.200.5   SMB2   156 Find Request File:  SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
49321 129.504733   192.168.200.5   192.168.200.7   SMB2   828 Find Response
49322 129.504966   192.168.200.7   192.168.200.5   SMB2   156 Find Request File:  SMB2_FIND_ID_BOTH_DIRECTORY_INFO Pattern: *
49323 129.505518   192.168.200.5   192.168.200.7   SMB2   130 Find Response, Error: STATUS_NO_MORE_FILES
```

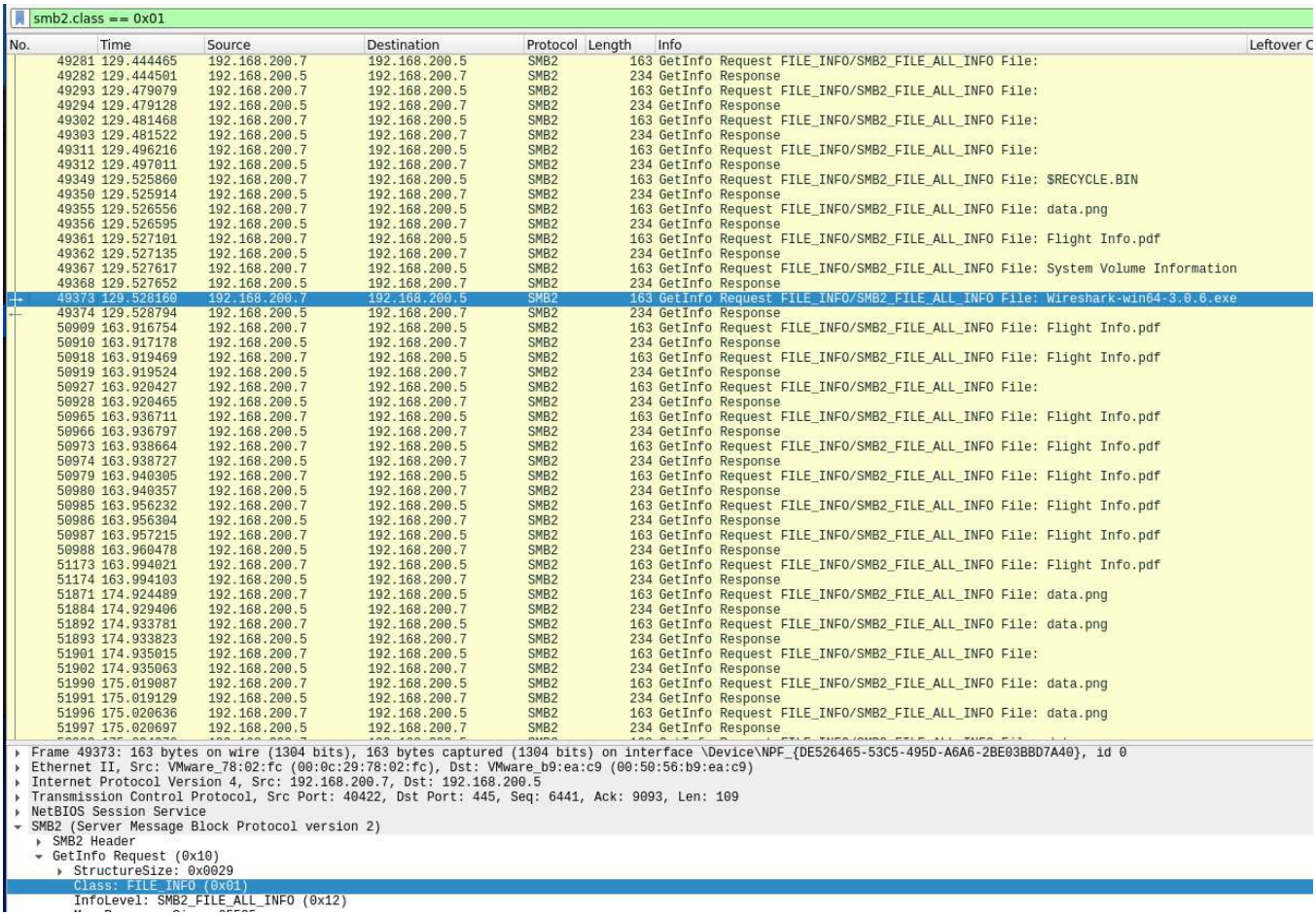
If we look at the start, we can see that it looks like a SMB server set up by a Kali box (which miiight be dubious), especially since that is initiating the request to our host in question.

```
43438 76.012750   192.168.200.7   192.168.200.5   SMB2   258 Session Setup Request, NTLMSSP_AUTH, User: \
43461 76.023817   192.168.200.5   192.168.200.7   SMB2   130 Session Setup Response, Error: STATUS_ACCESS_DENIED
49148 120.582481  192.168.200.7   192.168.200.5   NBSS   126 Session request, to 192.168.200.5<20> from KALI<00>
49149 120.582505  192.168.200.5   192.168.200.7   NBSS    59 Negative session response, Called name not present
49155 120.582744  192.168.200.7   192.168.200.5   NBSS   126 Session request, to *SMBSERVER<20> from KALI<00>
49156 120.582781  192.168.200.5   192.168.200.7   NBSS    59 Negative session response, Called name not present
49162 120.583135  192.168.200.7   192.168.200.5   SMB    270 Negotiate Protocol Request
```

If we try and go to File -> Export -> SMB, we can find files that were transferred through SMB in the capture. Download them and we can see the flight details and some things on tom's computer.

| Packet | Hostname | Content Type | Size | Filename |
|---|---|---|---|---|
| 51155 | \\192.168.200.5\e | FILE (223214/223214) R [100.00%] | 223 kB | \Flight Info.pdf |
| 52231 | \\192.168.200.5\e | FILE (350555/350555) R [100.00%] | 350 kB | \data.png |

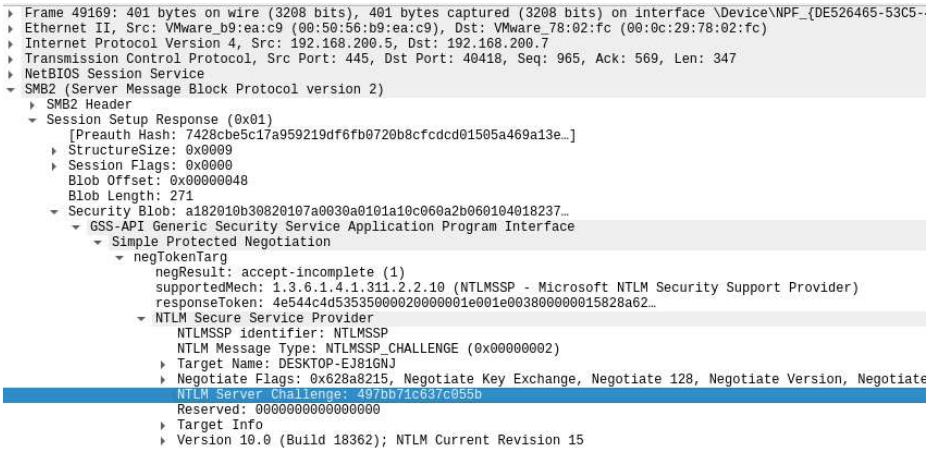
We can take a packet for GetInfo and apply it as a filter to see all of the enumerated files. (Open the SMB2 payload part of a GetInfo packet, right click the Class where it says FILE_INFO and select "Apply as Filter")

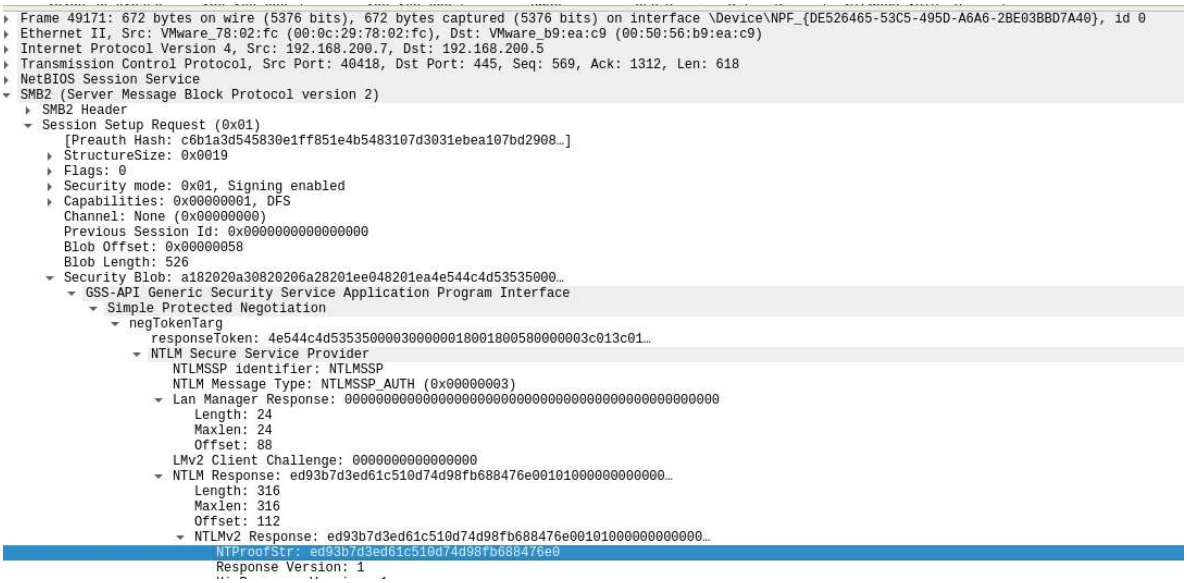



We see other things, but Wireshark seems to be the kicker. So, now, how do we get a password? Well, we saw that at the beginning, the SMB connection was set up using NTLMSSP. Lets look to try and crack that? There are actually several session setups, and lets use the ones that were successful (aka not the ERROR: STATUS ACCESS DENIED). (There are actually 2 successful connections, and both crack to the same password).

```
43227 75.934917    192.168.200.5   192.168.200.7   SMB2      566 Negotiate Protocol Response
43388 75.988470    192.168.200.7   192.168.200.5   SMB2      220 Session Setup Request, NTLMSSP_NEGOTIATE
43436 76.012390    192.168.200.5   192.168.200.7   SMB2      401 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHA…
43438 76.012750    192.168.200.7   192.168.200.5   SMB2      258 Session Setup Request, NTLMSSP_AUTH, User: \
43461 76.023817    192.168.200.5   192.168.200.7   SMB2      130 Session Setup Response, Error: STATUS_ACCESS_DENIED
49163 120.583481   192.168.200.5   192.168.200.7   SMB2      506 Negotiate Protocol Response
49165 120.584636   192.168.200.7   192.168.200.5   SMB2      240 Negotiate Protocol Request
49166 120.584943   192.168.200.5   192.168.200.7   SMB2      566 Negotiate Protocol Response
49168 120.585377   192.168.200.7   192.168.200.5   SMB2      220 Session Setup Request, NTLMSSP_NEGOTIATE
49169 120.585566   192.168.200.5   192.168.200.7   SMB2      401 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHA…
49171 120.585842   192.168.200.7   192.168.200.5   SMB2      672 Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\tom_fedder
49172 120.586816   192.168.200.5   192.168.200.7   SMB2      159 Session Setup Response
49174 120.587064   192.168.200.7   192.168.200.5   SMB2      170 Tree Connect Request Tree: \\192.168.200.5\IPC$
49175 120.587215   192.168.200.5   192.168.200.7   SMB2      138 Tree Connect Response
49177 120.602435   192.168.200.7   192.168.200.5   SMB2      190 Create Request File: srvsvc
49178 120.602793   192.168.200.5   192.168.200.7   SMB2      210 Create Response File: srvsvc
49180 120.603251   192.168.200.7   192.168.200.5   DCERPC    250 Bind: call_id: 1, Fragment: Single, 1 context items: SRVSVC V3.0 (32bit NDR)
49181 120.603428   192.168.200.5   192.168.200.7   DCERPC    238 Bind_ack: call_id: 1, Fragment: Single, max_xmit: 4280 max_recv: 4280, 1 re…
49183 120.612392   192.168.200.7   192.168.200.5   SRVSVC    278 NetShareEnumAll request
49184 120.612736   192.168.200.5   192.168.200.7   SRVSVC    658 NetShareEnumAll response
49186 120.616407   192.168.200.7   192.168.200.5   SMB2      146 Close Request File: srvsvc
49187 120.616457   192.168.200.5   192.168.200.7   SMB2      182 Close Response
49231 129.419885   192.168.200.5   192.168.200.7   SMB2      506 Negotiate Protocol Response
49233 129.419983   192.168.200.7   192.168.200.5   SMB2      240 Negotiate Protocol Request
49234 129.420149   192.168.200.5   192.168.200.7   SMB2      566 Negotiate Protocol Response
49246 129.440327   192.168.200.5   192.168.200.7   SMB2      506 Negotiate Protocol Response
49248 129.440449   192.168.200.7   192.168.200.5   SMB2      240 Negotiate Protocol Request
49249 129.440619   192.168.200.5   192.168.200.7   SMB2      566 Negotiate Protocol Response
49251 129.442073   192.168.200.7   192.168.200.5   SMB2      220 Session Setup Request, NTLMSSP_NEGOTIATE
49252 129.442212   192.168.200.5   192.168.200.7   SMB2      401 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHA…
49254 129.442391   192.168.200.7   192.168.200.5   SMB2      672 Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\tom_fedder
49255 129.443062   192.168.200.5   192.168.200.7   SMB2      159 Session Setup Response
49257 129.443216   192.168.200.7   192.168.200.5   SMB2      170 Tree Connect Request Tree: \\192.168.200.5\IPC$
```

Both the highlighted exchanges work. Go ahead and pull challenges, and response (ProofStr and Full Response)




Put that into a notepad file and crack it using hashcat.
The format for a NTLM hash should be
user:domain::challenge:proofstr:response without proofstr

With that, we can just crack it with hashcat.

```
┌──(lite㉿kali)-[~/Downloads]
└─$ hashcat -m 5600 stolen.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.5, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-9600K CPU @ 3.70GHz, 5824/5888 MB (2048 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 2 digests; 2 unique digests, 2 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Applicable optimizers applied:
* Zero-Byte
* Not-Iterated

ATTENTION! Pure (unoptimized) backend kernels selected.
Using pure kernels enables cracking longer passwords but for the price of drastically reduced performance.
If you want to switch to optimized backend kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

INFO: Removed 1 hash found in potfile.

Host memory required for this attack: 65 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344384
* Bytes.....: 139921497
* Keyspace..: 14344384

TOM_FEDDER::WORKGROUP:497bb71c637c055b:ed93b7d3ed61c510d74d98fb688476e0:0101000000000000006201533f649bd501e17dd2637b53d5b8000000
4a00380031004700 4e004a0001001e00440045005300 4b0054004f0050002d0045004a00380031004700 4e004a0004001e00440045005300 4b0054004f0050
450053004b0054004f0050002d0045004a00380031004700 4e004a0007000800 6201533f649bd501060004000200000008003000300000000000000000000000
aca797b867c2c20a8ff0a559ebfb0a0010000000000000000000000000000000000000000090024006300690066007300 2f00310039003200 2e00310036003800 2e

Session..........: hashcat
Status...........: Cracked
Hash.Name........: NetNTLMv2
Hash.Target......: stolen.txt
Time.Started.....: Tue Jun 15 22:15:22 2021 (5 secs)
Time.Estimated...: Tue Jun 15 22:15:27 2021 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1714.1 kH/s (1.49ms) @ Accel:1024 Loops:1 Thr:1 Vec:8
Recovered........: 2/2 (100.00%) Digests, 2/2 (100.00%) Salts
Progress.........: 18526208/28688768 (64.58%)
Rejected.........: 0/18526208 (0.00%)
Restore.Point....: 9261056/14344384 (64.56%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: catalinateamo -> cassroo

Started: Tue Jun 15 22:15:19 2021
Stopped: Tue Jun 15 22:15:29 2021
```

As we can see, both are cracked and actually lead to the same result (I added the 2nd and recracked it, and they both yield the same, which is why we only see one in the screenshot).