

New SMB3 features in Wireshark

POSIX extensions, decryption and wireshark-based tools

Aurélien Aptel <aaptel@suse.com> SUSE

Who am I

- Aurélien Aptel
- Employed by SUSE Linux from Nuremberg, Germany
- Samba team member
- Work on open source SMB-related things
 - cifs.ko: the Linux SMB kernel client to mount remote shares
 - Samba: userspace client and server implementation for Linux
 - Wireshark: this talk :)
 - ...

Wireshark: what is it?

- Network sniffer and analyzer
- Open Source (GNU GPLv2)
- Available on most platforms (Windows, Mac, Linux and other unixes)
- http://wireshark.org

WIRESHARK

Network sniffer?

- Traditional solution (unix): tcpdump
 - Simple command line tool for simple environment (embedded?)

tcpdump -s 0 -w trace.pcap port 445

- Captures network traffic to trace.pcap file
- No size limit for the packets
- Load trace in wireshark
- Wireshark can also capture
 - Same capture filters (!= display filters)
 - tcpdump, WinDump, Analyzer, ... programs using libpcap/WinPcap library
 - But many display filters!
 - Personal choice capture everything, filter later.
 - Display filter: smb||smb2||dns||krb4

Network sniffer?

• Windows 7/2008 and above

netsh trace start persistent=yes capture=yes tracefile=c:\temp\
mytrace.etl

netsh trace stop

- Open in netmon (https://www.microsoft.com/en-us/download/4865)
- Save as pcap

...

• "persistent=yes" makes it work across reboot

• Sample trace

	🚄 🖈 smbtest.pcapng v 🔨 😒										$\sim \otimes$			
Fil	e Edit	View	Go	Capture A	Analyze	Statistics	Telephon	y Wirel	ess To	ols Help				
		6			(۹ <	> >·	K >) (
	Apply a	display filte	r <(Ctrl-/>								→	Expression.	+
No).	Time		Source		Destinati	on	Protoc	Lengtl	Info				
×.	1 0	9.000000	00	192.168.2	.105	192.168	2.107	TCP	74	56664 → 445	[SYN] Se	q=0 Win=292	200 Len=0 MS	
Т		0.0018042	33	192.168.2	.107	192.168	2.105	тср	74	445 → 56664	[SYN, AC	K] Seq=0 Ad	ck=1 Win=819	
	3 (0.0018305	17	192.168.2	.105	192.168	2.107	тср	66	56664 → 445	[ACK] Se	q=1 Ack=1 W	Vin=29312 Le	
	4 0	0.0019306	26	192.168.2	.105	192.168	2.107	SMB	282	Negotiate P	rotocol R	equest		
	5 0	0.0026826	83	192.168.2	.107	192.168	2.105	SMB2	240	Negotiate P	rotocol R	esponse		
	6 0	0.0026984	22	192.168.2	.105	192.168	2.107	TCP	66	56664 → 445	[ACK] Se	q=217 Ack=1	175 Win=3033	
	70	9.0027517	33	192.168.2	.105	192.168	2.107	SMB2	174	Negotiate P	rotocol R	equest		
	8 0	0.0032500	73	192.168.2	.107	192.168	2.105	SMB2	240	Negotiate P	rotocol R	esponse		
	9 (0.0044510	75	192.168.2	.105	192.168	2.107	SMB2	232	Session Set	up Reques	t, NTLMSSP_	NEGOTIATE	
	10 0	0.0053869	85	192.168.2	.107	192.168	2.105	SMB2	413	Session Set	up Respon	se, Error:	STATUS_MORE	
	11 (0.0055759	20	192.168.2	.105	192.168	2.107	SMB2	702	Session Set	un Reques	t. NTLMSSP	AUTH. User:	
5-	Frame 2	2: 74 byt	es o	n wire (59	2 bits),	. 74 bytes	captur	ed (592	bits)	on interfac	e 0			
>-	Etherne	, et II, Sr	c: R	ealtekU_fe	:30:b5 ((52:54:00:	fe:30:b	5), Dst:	LcfcH	lefe_f3:c3:9	5 (68:f7:2	28:f3:c3:95	5)	
>-	Interne	et Protoc	ol V	ersion 4,	Src: 192	2.168.2.10	7, Dst:	192.168	8.2.105	_				
>-	Transm:	ission Co	ntro	l Protocol	, Src Po	ort: 445,	Dst Por	t: 56664	, Seq:	0, Ack: 1,	Len: 0			
	0.0 68	f7 28 f3	1 63	95 52 54	00 fe 30	9 b5 68 66	45 00	h · (· · ·	RT A)F.				
00	10 00	3c 15 4e	40	00 80 06	5f 49 c0	9 a8 02 6b	c0 a8	< N@	I	··k··				
00	20 02	69 01 bd	dd 00	58 a7 4e 00 02 04	18 d5 20 05 b4 01	9 57 5d 7d 1 03 03 08	a0 12 04 02	·i···)	(·N ··	W]}··				

0040 08 0a 03 4b ec b9 7d d9 4b 50 ····K··}· KP

Filter expression

• Sample trace

smb||smb2||dns||krb4

No.	Time	Source	Destination	Protoc	Lengtl Info	
4	0.001930626	192.168.2.105	192.168.2.107	SMB	282 Negotiate Protocol Request	
5	0.002682683	192.168.2.107	192.168.2.105	SMB2	240 Negotiate Protocol Response	
7	0.002751733	192.168.2.105	192.168.2.107	SMB2	174 Negotiate Protocol Request	
8	0.003250073	192.168.2.107	192.168.2.105	SMB2	240 Negotiate Protocol Response	
9	0.004451075	192.168.2.105	192.168.2.107	SMB2	232 Session Setup Request, NTLMSSP_NEGOTIATE	
10	0.005386985	192.168.2.107	192.168.2.105	SMB2	413 Session Setup Response, Error: STATUS_MORE_PROCESSING_RE	
11	0.005575920	192.168.2.105	192.168.2.107	SMB2	702 Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\adm	
12	0.006856115	192.168.2.107	192.168.2.105	SMB2	171 Session Setup Response	
13	0.006983478	192.168.2.105	192.168.2.107	SMB2	182 Tree Connect Request Tree: \\192.168.2.107\IPC\$	
14	0.007593926	192.168.2.107	192.168.2.105	SMB2	150 Tree Connect Response	
15	0.007650402	192.168.2.105	192.168.2.107	SMB2	218 Toctl Request ESCTL VALIDATE NEGOTIATE INFO	

>-Frame 4: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface 0

>-Ethernet II, Src: LcfcHefe_f3:c3:95 (68:f7:28:f3:c3:95), Dst: RealtekU_fe:30:b5 (52:54:00:fe:30:b5)

>-Internet Protocol Version 4, Src: 192.168.2.105, Dst: 192.168.2.107

>-Transmission Control Protocol, Src Port: 56664, Dst Port: 445, Seq: 1, Ack: 1, Len: 216

>-NetBIOS Session Service

>-SMB (Server Message Block Protocol)

RT··O·h· (····E· 0000 52 54 00 fe 30 b5 68 f7 28 f3 c3 95 08 00 45 00 0010 01 0c 32 ed 40 00 40 06 80 da c0 a8 02 69 c0 a8 · · 2 · @ · @ · · · · · · i · · ·k·X·· W]}·N···· 0020 02 6b dd 58 01 bd 20 57 5d 7d a7 4e 18 d6 80 18 0030 00 e5 87 23 00 00 01 01 08 0a 7d d9 4b 52 03 4b ···#··· ··}·KR·K 0040 ec b9 00 00 00 d4 ff 53 4d 42 72 00 00 00 18 · · · · · · · S MBr · · · · 0060 fe ff 00 00 00 00 00 b1 00 02 50 43 20 4e 45 54 ···· PC NET 0070 57 4f 52 4b 20 50 52 4f 47 52 41 4d 20 31 2e 30 WORK PRO GRAM 1.0 $\times \rightarrow$

Expression...

• Sample trace

smb smb2 dns krb4 Expression +									
No.	Time	Source	Destination	Protoc	Lengtl	Info			
4	0.001930626	192.168.2.105	192.168.2.107	SMB	282	Negotiate Protocol Request			
5	0.002682683	192.168.2.107	192.168.2.105	SMB2	240	Negotiate Protocol Response			
7	0.002751733	192.168.2.105	192.168.2.107	SMB2	174	Negotiate Protocol Request			
8	0.003250073	192.1 2 3 7 K C	192.168.2.105	SMB2	240	Negotiate Protocol Response			
9	0.004451075	192.168.2.105	192.168.2.107	SMB2	232	Session Setup Request, NTLMSSP_NEGOTIATE			
10	0.005386985	192.1 S.2:07 M	apr. 105 . 105	SMB2		Session Setup Response, Error: STATUS_MORE_PROCESSING_RE			
11	0.005575920	192.168.2.105	192.168.2.107	SMB2	702	Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\adm			
12	0.006856115	192.168.2.107	192.168.2.105	SMB2	171	Session Setup Response			
13	0.006983478	192.168.2.105	192.168.2.107	SMB2	182	Tree Connect Request Tree: \\192.168.2.107\IPC\$			
14	0.007593926	192.168.2.107	192.168.2.105	SMB2	150	Tree Connect Response			
15	0.007650402	192.168.2.105	192.168.2.107	SMB2	218	Toctl Request ESCTL VALIDATE NEGOTIATE INFO			

>-Frame 4: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface 0

>-Ethernet II, Src: LcfcHefe_f3:c3:95 (68:f7:28:f3:c3:95), Dst: RealtekU_fe:30:b5 (52:54:00:fe:30:b5)

>-Internet Protocol Version 4, Src: 192.168.2.105, Dst: 192.168.2.107

>-Transmission Control Protocol, Src Port: 56664, Dst Port: 445, Seq: 1, Ack: 1, Len: 216

>-NetBIOS Session Service

>-SMB (Server Message Block Protocol)

• Sample trace

	smb	smb2 dns krb4				Expression	+
	No.	Time	Source	Destination	Protoc Le	engtl Info	1
	4	0.001930626	192.168.2.105	192.168.2.107	SMB	282 Negotiate Protocol Request	
	5	5 0.002682683	192.168.2.107	192.168.2.105	SMB2	240 Negotiate Protocol Response	
	7	7 0.002751733	192.168.2.105	192.168.2.107	SMB2	174 Negotiate Protocol Request	
	8	3 0.003250073	192.168.2.107	192.168.2.105	SMB2	240 Negotiate Protocol Response	
	g	0.004451075	192.168.2.105	192.168.2.107	SMB2	232 Session Setup Request, NTLMSSP_NEGOTIATE	
	10	0.005386985	192.168.2.107	192.168.2.105	SMB2	413 Session Setup Response, Error: STATUS_MORE_PROCESSING_RE	
	11	L 0.005575920	192.168.2.105	192.168.2.107	SMB2	702 Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\adm	
	12	2 0.006856115	192.168.2.107	192.168.2.105	SMB2	171 Session Setup Response	
	13	3 0.006983478	192.168.2.105	192.168.2.107	SMB2	182 Tree Connect Request Tree: \\192.168.2.107\IPC\$	
	14	4 0.007593926	192.168.2.107	192.168.2.105	SMB2	150 Tree Connect Response	
	15	5 0.007650402	192.168.2.105	192.168.2.107	SMB2	218 Toctl Request FSCTL VALIDATE NEGOTIATE INFO	1
F		4. 202 huton	on wine (2256 bits)) 202 hutee cent	uned (225	C hita) an intenface O	
L	- Frame	9 4: 282 Dyles	of wire (2250 bits)), 282 bytes capt so:f7:20:f2:c2:05) Det: P	o bits) on interface o	
L	Inter	net Protocol V	ersion A Src: 102	160 2 105 Det.), DSL. N 102 169 2		
	Trans	mission Contro	l Protocol Src Po	.108.2.105, DSt.	192.100.2		
	-NetRT	IOS Session Ser	vice	, 03010	10. 443,	Jeq. 1, Ack. 1, Len. 210	
	S-SMB (Server Message	Block Protocol)				
	, 0112 (oor oor noosage	510010 110000017				
F	0000 5	52 54 00 fe 30	b5 68 f7 28 f3 c3	95 08 00 45 00	RT · · O · h ·	(E.	_
	0010 6	01 Oc 32 ed 40	00 40 06 80 da c0	a8 02 69 c0 a8	· · 2 · @ · @ ·	····i··	
	0020 0	02 6b dd 58 01	bd 20 57 5d 7d a7	4e 18 d6 80 18	·k·X·· w		1
	0030 e	ec b9 00 00 00	d4 ff 53 4d 42 72	00 00 00 00 18	· · · · · · · · · S	Br	1
	0050 4	13 c8 00 00 00	00 00 00 00 00 00	00 00 00 00 00	C · · · · · ·		
	0060 1	re tt 00 00 00 57 4f 52 4b 20	00 00 b1 00 02 50 50 52 4f 47 52 41	43 20 4e 45 54 4d 20 31 2e 30	WORK PRO	ORAM 1.0	

• Sample trace

smb smb2 dns krb4 Expression +										
	Time	Source	Destination	Protoc	Lengtl	Info				
4	0.001930626	192.168.2.105	192.168.2.107	SMB	282	Negotiate Protocol Request				
5	0.002682683	192.168.2.107	192.168.2.105	SMB2	240	Negotiate Protocol Response				
7	0.002751733	192.168.2.105	192.168.2.107	SMB2	174	Negotiate Protocol Request				
8	0.003250073	192.168.2.107	192.168.2.105	SMB2	240	Negotiate Protocol Response				
9	0.004451075	192.168.2.105	192.168.2.107	SMB2	232	Session Setup Request, NTLMSSP_NEGOTIATE				
10	0.005386985	192.168.2.107	192.168.2.105	SMB2	413	Session Setup Response, Error: STATUS_MORE_PROCESSING_RE				
11	0.005575920	192.168.2.105	192.168.2.107	SMB2	702	Session Setup Request, NTLMSSP_AUTH, User: WORKGROUP\adm				
12	0.006856115	192.168.2.107	192.168.2.105	SMB2	171	Session Setup Response				
13	0.006983478	192.168.2.105	192.168.2.107	SMB2	182	Tree Connect Request Tree: \\192.168.2.107\IPC\$				
14	0.007593926	192.168.2.107	192.168.2.105	SMB2	150	Tree Connect Response				
15	0.007650402	192.168.2.105	192.168.2.107	SMB2	218	Toctl Request ESCTL VALIDATE NEGOTIATE INFO				

>-Frame 4: 282 bytes on wire (2256 bits), 282 bytes captured (2256 bits) on interface 0

>-Ethernet II, Src: LcfcHefe_f3:c3:95 (68:f7:28:f3:c3:95), Dst: RealtekU_fe:30:b5 (52:54:00:fe:30:b5)

>-Internet Protocol Version 4, Src: 192.168.2.105, Dst: 192.168.2.107

>-Transmission Control Protocol, Src Port: 56664, Dst Port: 445, Seq: 1, Ack: 1, Len: 216

>-NetBIOS Session Service

>-SMB (Server Message Block Protocol)

0000 52 54 00 fe 30 b5 68 f7 28 f3 c3 95 08 00 45 00 RT··O·h· (····E 0010 01 0c 32 ed 40 00 40 06 80 da c0 a8 02 69 c0 a8 · · 2 · @ · @ · · · · · · i · · 0020 02 6b dd 58 01 bd 20 57 5d 7d a7 4e 18 d6 80 18 · k · X · · W]} · N · · · · 0030 00 e5 87 23 00 00 01 01 08 0a 7d d9 4b 52 03 4b Hex dump 0040 ec b9 00 00 00 d4 ff 53 4d 2 00 00 00 18 •••••S MBr•••• 0050 43 c8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0060 fe ff 00 00 00 00 00 b1 00 02 50 43 20 4e 45 54 · · · · · · · · · PC NET 0070 57 4f 52 4b 20 50 52 4f 47 52 41 4d 20 31 2e 30 WORK PRO GRAM 1.0

- Wireshark handles reassembling (large packet split, retransmission)
- Only see the good stuff
- Each filter can do more than filtering
 - Dissectors
- 2 different dissectors for SMB1 and SMB2+
 - SMB3 shows up as SMB2
- Mostly written by Ronnie Sahlberg

• Generated fields in [brackets]

• Tracks context

21 2.427531679	127.0.0.1	127.0.0.1	SMB2	150 Tree Connect Response
22 2.427625118	127.0.0.1	127.0.0.1	SMB2	238 Create Request File:
23 2.429988625	127.0.0.1	127.0.0.1	SMB2	298 Create Response File:
24 2.430044805	127.0.0.1	127.0.0.1	SMB2	175 GetInfo Request FS_INFO/F:
25 2.430211777	127.0.0.1	127.0.0.1	SMB2	162 GetInfo Response
26 2.430258531	127.0.0.1	127.0.0.1	SMB2	175 GetInfo Request FS_INFO/F:
27 2.430421688	127.0.0.1	127.0.0.1	SMB2	150 GetInfo Response

```
— Message ID: Unknown (5)
— Process Id: 0x00001e5e
~ Tree Id: 0x784d580a \\localhost\test
- [Tree: \\localhost\test]
- [Tree: \\localhost\test]
- [Share Type: Physical disk (0x01)]
- [Connected in Frame: 21]
```

- Generated fields in [brackets]
- Tracks context
- Clickable link to Request/Response
- When files are opened or closed
- When session is opened
- ...

- Generated fields in [brackets]
- Tracks context
- Clickable link to Request/Response
- When files are opened or closed
- When session is opened
- ...
- Discoverable, filterable

smb2.tree == "\\\\localhost\\test"

13 2.383373352	127.0.0.1	
14 2.383522449	127.0.0.1	
15 2.390041064	127.0.0.1	
16 2.390272514	127.0.0.1	
17 2.422983948	127.0.0.1	
18 2.423105311	127.0.0.1	
19 2.426093046	127.0.0.1	
20 2.426184568	127.0.0.1	
21 2.427531679	127.0.0.1	
22 2.427625118	127.0.0.1	
23 2.429988625	127.0.0.1	
24 2.430044805	127.0.0.1	
25 2.430211777	127.0.0.1	
26 2.430258531	127.0.0.1	
27 2.430421688	127.0.0.1	
— Message ID: Ur	nknown (5)	

13 2.38337335	52 127.0.0.1		Apply as Column	Ctrl+Shift+I		F5 [ACK] S	eq=189	Ack=
14 2.38352244	9 127.0.0.1		Apply as Filter		->	Selected		SP
15 2.39004106	4 127.0.0.1	- 4	Prepare a Filter		>	Not Selecte	d	r:
17 2.42298394	14 127.0.0.1		Conversation Filter		>	and Selec	ted	ər
18 2.42310531	1 127.0.0.1		Colorize with Filter		>	or Selecte	ed	1
19 2.42609304	16 127.0.0.1		Follow		>	and not S	elected	
20 2.42618456 21 2.42753167	38 127.0.0.1 79 127.0.0.1		Сору		>	or not Sel	ected	
22 2.42762511	127.0.0.1		Show Packet Bytes	Ctrl+Shift+O		quest File	:	
23 2.42998862	25 127.0.0.1		Export Packet Bytes	Ctrl+Shift+X		sponse Fil	e:	
24 2.43004480 25 2.43021177	05 127.0.0.1 77 127.0.0.1		Wiki Protocol Page		≥quest FS_ ≥sponse	INF0/F1	lleFs	
26 2.43025853	31 127.0.0.1		Filter Field Reference			quest FS_	INF0/Fi	ileFs
27 2.43042168	88 127.0.0.1		Protocol Preferences		>	sponse		
— Message ID:	: Unknown (5)		Decode As			_		
-Process Id	0x00001e5e		Go to Linked Packet					
∽-Tree Id: 0>	<784d580a \\loca	lhos	Show Linked Packet in New Window					
Tree: \	\localhost\test]		0.01)]					
Charo T	VDOI DEVOZOOI dz	5 Iz /						

-[Share Type: Physical disk (0x01)

- Wireshark can decrypt SMB3 traffic
 - SMB3.0 since version 2.5.0 (released february 2018)
 - SMB3.1.1 in next version (not yet released :)
 - AES-128-CCM only
 - NTLMSSP and kerberos authentification
- Requirements
 - User must provide Session Key
 - Trace must have initial connection steps
 - negotiate protocol & session setup
 - If you do not want to capture the whole session
 - Capture session setup, Stop, Capture rest later
 - Merge traces

mergecap -w output.pcap input1.pcap input2.pcap inputN.pcap

SMB3 decryption: Getting Session Key

• Linux:

- Compile with CIFS_DEBUG_DUMP_KEYS enabled
- Keys printed in kernel log:

CIFS VFS: generate_smb3signingkey: dumping generated AES session keys CIFS VFS: Session Id 61 00 00 28 64 1c 00 00 CIFS VFS: Session Key 7b 7c 77 53 cf 29 7b ca 69 26 ce 58 bb 1b 12 df CIFS VFS: Signing Key 29 a3 f0 e6 72 45 01 b9 aa e3 cd 75 15 88 4a 85 CIFS VFS: ServerIn Key ec de b2 7c 49 13 78 89 d7 5b d2 6c 42 20 b3 c3 CIFS VFS: ServerOut Key 35 a4 dc 80 2c d3 4c 87 cb bd 78 82 f7 ea 66 15

• Windows: ?

• Edit > Preference > Protocols > SMB2



- Alternatively can be passed via CLI
 - wireshark -ouat:smb2_seskey_list:<ses_id>,<ses_key> smb311.pcap

E.g.:

wireshark -ouat:smb2_seskey_list:2900009c003c0000,f1fa528d3cd182cca67bd4596dabd885 smb311.pcap

254 Negotiate Protocol Request 378 Negotiate Protocol Response 190 Session Setup Request, NTLMSSP_NEGOTIATE 328 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE 434 Session Setup Request, NTLMSSP AUTH, User: \administrator 142 Session Setup Response 244 Decrypted SMB3;Tree Connect Request Tree: \\dfsroot1.foo.test\IPC\$ 202 Decrypted SMB3;Tree Connect Response 244 Decrypted SMB3;Tree Connect Request Tree: \\dfsroot1.foo.test\data 202 Decrypted SMB3; Tree Connect Response 330 Decrypted SMB3;Create Request File: 354 Decrypted SMB3;Create Response File: 243 Decrypted SMB3; Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO 690 Decrypted SMB3; Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO 227 Decrypted SMB3;GetInfo Request FS_INFO/FileFsAttributeInformation File:

01 101002002	102110011001100	1011001001101	SHEE	to roooton oocab hoquooc, me
38 18.088585	10.160.65.192	192.168.100.168	SMB2	142 Session Setup Response
39 18.120176	192.168.100.168	10.160.65.192	SMB2	244 Decrypted SMB3;Tree Connect
40 18.145154	10.160.65.192	192.168.100.168	SMB2	202 Decrypted SMB3;Tree Connect

Frame 38: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) Ethernet II, Src: RealtekU_07:03:2d (52:54:00:07:03:2d), Dst: 52:55:00:d1:44:45 (52:55:00:d1:4 Internet Protocol Version 4, Src: 10.160.65.192, Dst: 192.168.100.168 Transmission Control Protocol, Src Port: 445, Dst Port: 39264, Seq: 575, Ack: 681, Len: 76 NetBIOS Session Service

NetBIOS Session Service

SMB2 (Server Message Block Protocol version 2)

>-SMB2 Header

Session Setup Response (0x01)

— [Preauth Hash: de24cb14f91c1d6739f0d7019bd90051f75a90b01b17a292…] ◄

StructureSize∙ AxAAAA

SMB2 POSIX extensions

- Not merged yet (extension isn't final yet :)
- https://github.com/aaptel/wireshark/commits/smb3unix
- git clone https://github.com/aaptel/wireshark.git && git checkout smb3unix

Negotiate protocol capability

- Negoliale Concest. SMD2_FREADIN_INTEGRITY_CAPADILITES

- >-Negotiate Context: SMB2_ENCRYPTION_CAPABILITIES
- -Negotiate Context: SMB2_POSIX_EXTENSIONS_CAPABILITIES
 - Type: SMB2_POSIX_EXTENSIONS_CAPABILITIES (0x0100)
 - DataLength: 8
 - -Reserved: 00000000
 - POSIX Reserved: 0x00000000

SMB2 POSIX extensions

Create context request/response

└-ExtraInfo SMB2_CREATE_REQUEST_LEASE SMB2_POSIX_CREATE_CONTEXT

>-Chain Element: SMB2_CREATE_REQUEST_LEASE "RqLs"

-Chain Element: SMB2_POSIX_CREATE_CONTEXT "5025ad93-b49c-e711-b423-83de968bcd7c"

— Chain Offset: 0x00000000

>-Tag: 5025ad93-b49c-e711-b423-83de968bcd7c

-Blob Offset: 0x00000020

— Blob Length: 4

└──Data: POSIX Create Context request

- POSIX perms: 0131

SMB2 POSIX extensions

• New INFO level

55 5.020975	127.0.0.1	127.0.0.1	SMB2	170 Find Request File:	SMB2_FIND_POSIX_INFO Pat
56 5.021150	127.0.0.1	127.0.0.1	SMB2	576 Find Response	
57 5.021995	127.0.0.1	127.0.0.1	SMB2	160 Close Request File:	testfile.txt

```
-Blob Offset: 0x00000048
```

— Blob Length: 432

```
>-FilePosixInfo: .
```

```
>-FilePosixInfo: ..
```

└-FilePosixInfo: testfile.txt

— Next Offset: 0

— Create: Jun 6, 2018 17:22:18.435431300 CEST

—Last Access: Jun 6, 2018 17:22:18.435431300 CEST

—Last Write: Jun 6, 2018 17:22:18.435431300 CEST

—Last Change: Jun 6, 2018 17:22:18.435431300 CEST

See https://wiki.samba.org/index.php/SMB3-Linux for more

Other new things

- Better parsing of Filesystem attributes
- Better parsing for all level info of FIND responses
- Bug fixes: opening share root (empty file name) context properly saved

New wireshark-based tool: smbcmp

- Wireshark has a CLI version
 - Tshark
- Mostly same CLI options and flags
 - Can get summary view or detailed view

Summary:

• tshark -r <cap>

Detailed:

• tshark -r <cap> -V

New wireshark-based tool: smbcmp

Diff traces to debug problems

https://github.com/aaptel/smbcmp

	INEROLIALE FLOTOCOL REQUEST
ate Protocol Response	Negotiate Protocol Response
n Setup AndX Request, NTLMSSP_NEGOTIATE	Session Setup AndX Request, NTLMSSP_NEGOTIATE
n Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSI
n Setup AndX Request, NTLMSSP_AUTH, User: \administrator	Session Setup AndX Request, NTLMSSP_AUTH, User: \administrator
n Setup AndX Response	Session Setup AndX Response
onnect AndX Request, Path: \\foo.com\dfs	Tree Connect AndX Request, Path: \\foo.com\dfs
onnect AndX Response, Error: STATUS_BAD_NETWORK_NAME	Tree Connect AndX Response, Error: STATUS_BAD_NETWORK_NAME
onnect AndX Request, Path: \\10.160.65.124\IPC\$	Tree Connect AndX Request, Path: \\10.160.65.124\IPC\$
onnect AndX Response	Tree Connect AndX Response
Request, GET_DFS_REFERRAL, File: \foo.com\dfs	Trans2 Request, GET_DFS_REFERRAL, File: \foo.com\dfs
Response, GET_DFS_REFERRAL	Trans2 Response, GET_DFS_REFERRAL
isconnect Request	Logoff AndX Request
isconnect Response	Logoff AndX Response
AndX Request	Negotiate Protocol Request
AndX Response	Negotiate Protocol Response
ate Protocol Request	Session Setup AndX Request, NTLMSSP_NEGOTIATE
ate Protocol Response	Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESS
n Setup AndX Request, NTLMSSP_NEGOTIATE	Session Setup AndX Request, NTLMSSP_AUTH, User: \administrator
n Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED	Session Setup AndX Response
n Setup AndX Request, NTLMSSP_AUTH, User: \administrator	Tree Connect AndX Request, Path: \\FOO-NS1.foo.com\dfs
n Setup AndX Response	Tree Connect AndX Response

s-logic-error-fail.pcap

8 +1,8 @@
Server Message Block Protocol)
MB Header
Server Component: SMB
[Response to: 21]
[Time from request: 0.047731000 seconds]
[Response to: 19]
[Time from request: 0.024939000 seconds]
SMB Command: Session Setup AndX (0x73)
NT Status: STATUS_MORE_PROCESSING_REQUIRED (0xc0000016)
Flags: 0x80, Request/Response

DEMO

28

Wireshark development

- Git / gerrit based
- https://www.wireshark.org/docs/wsdg_html_chunked/ChSrcContribute.html
- Make gerrit account on https://code.wireshark.org/review
- git clone <account>@code.wireshark.org:29418/wireshark
- cp tools/pre-commit tools/commit-msg .git/hooks
- git checkout -b frobnify
- *hack, hack, hack...*
 - Almost always limited to epan/dissectors/packet-smb2.c
- git commit -a -m "smb3: frobnify XYZ"
- git push -f origin HEAD:refs/for/master/smb3-frob
- Web/email based reviewing process
- Iterate on your changes depending on the feedback and push -f again
- Web UI is automatically updated

Wireshark development

https://code.wireshark.org/review/q/topic:"<branch name>"

PolyGerrit Changes Your Admin	Docun	Documentation v topic:"smb311-decryption"				Search		
Subject	Status	Owner	Project	Branch	Updated	Size	CR	
test/suite_decryption.py: add smb2 decryption t	Merged	🔅 Aurélien Aptel	wireshark	master	Jan 25	+52, - 0	~	
🔺 smb2: cleanup	Merged	Aurélien Aptel	wireshark	master	Jan 24	+4, -4	~	
索 smb2: add NULL checks	Merged	Aurélien Aptel	wireshark	master	Jan 24	+8, -8	~	
索 smb2: factor out session lookup&create	Merged	Aurélien Aptel	wireshark	master	Jan 23	+44, -68	~	
* smb2: implement generation of SMB3.1.1 decry	Merged	Aurélien Aptel	wireshark	master	Jan 22	+157, -11	~	
索 smb2: stash dialect in conversation stuct	Merged	Aurélien Aptel	wireshark	master	Jan 22	+3, -3	~	
索 smb2: factor out generated session info	Merged	Aurélien Aptel	wireshark	master	Jan 22	+33, -32	~	
索 smb2: replace magic value by macro	Merged	Aurélien Aptel	wireshark	master	Jan 22	+1, -1	~	

Thanks!

Questions?