## Using Zeek to track communication state

Corelight.com/blog/using-zeek-to-track-communication-state

Time 1991 51.068872 1994 51.070407	Source	Destination	Protocol  Len	ngtr   Info	
1994 51.070407	192.168.0.15	192.168.0.85		94   HHO 142 Bind: call_id: 1, Fragment: Single, :	l context items: E…
	192.168.0.85	192.168.0.15		06 Bind_ack: call_id: 1, Fragment: Sing	le, max_xmit: 4280…
1995 51.073268 2042 52.096420	192.168.0.15 192.168.0.85	192.168.0.85 192.168.0.15		278 EfsRpcOpenFileRaw request 186 EfsRpcOpenFileRaw response, Error: W	ERR_BAD_NETPATH
<pre>rame 1991: 242 b thernet II, Src: nternet Protocol ramsmission Cont etBIOS Session S MB2 (Server Mess </pre> <pre>SMB2 Header ProtocolId: Header Lengt Credit Chanel Sequ Reserved: 00 Command: Wri Credits requ &gt; Flags: 0x000 Chain Offset Message ID: Process Id: &gt; Tree Id: 0x0 &gt; Session Id: Signature: a</pre>	ytes on wire (1936 b VMware_39:e1:09 (00 Version 4, Src: 192 rol Protocol, Src Po ervice age Block Protocol v 0xfe534d42 h: 64 e: 1 ence: 0 00 0t (9) ested: 127 00008, Signing : 0x00000000 6 0x00000000 0x00000000 0x00000000 0x00001 \\192.168.0 0x00000001 \\192.168.0 0x00000001 \\192.168.0 0x00000000 1922] 0x001 0x0070 : 72 0 File: lsarpc e (0x00000000 1920] 0x0000 1920] 5 0 0 0 0 0 0 0 0 0 0 0 0 0	its), 242 bytes captu :0c:29:39:e1:09), Dst .168.0.15, Dst: 192.1 rt: 33524, Dst Port: - ersion 2) .85\IPC\$ cct: Domain: Host:	red (1936 bits) c : VMware_f9:91:35 68.0.85		
Blob Length: Channel Info istributed Compu Version: 5 Version (minor) Packet type: Bi Packet Flags: 0 Data Representa Frag Length: 77 Auth Length: 0 Call ID: 1 Max Xmit Frag: Max Recv Frag: Num Ctx Items:	0 Blob: NO DATA ting Environment / Ru : 0 und (11) bx83 ttion: 10000000 (Orde 2 4280 4280 4280	er: Little-endian, Cha		Fragment: Single, FragLen: 72, Call: 1 IEEE)	
Context ID:					
Num Trans It	ems: 1				
Abstract Syn	tax: EFS V1.0 EFS UUID: c681d488-	-d850-11d0-8c52-00c041	fd90f7e		
Interface:					
Interface Interface Interface	tax[1]: 32bit NDR V2				

<u>Home</u> >>> Using Zeek to track communication state September 21, 2021 by <u>Paul Dokas</u> One of <u>Zeek's</u> greatest strengths is its ability to deeply inspect packet streams that are fed into it. It is adept not only at identifying network protocols but also parsing them to extract large amounts of useful information. There is another strength that is often overlooked: Zeek not only extracts information from individual packets of network sessions, it also provides a very flexible and useful way to track state across the lifetime of network sessions. This is particularly useful when examining network protocols such as Server Message Block (SMB) that rely on the endpoint devices to track the state of their conversation.

To illustrate this point, <u>here</u> is a Zeek script for detecting attempts to exercise the PetitPotam exploits. We will walk through how this works in this blog post.

The <u>PetitPotam</u> exploit offers an opportunity to illustrate the power of Zeek for tracking the state of network conversations over their lifetime. PetitPotam abuses <u>EFS</u> DCERPC functions to trigger an <u>NTLM relay attack</u> that can be used to gain elevated privileges in a Windows AD domain. The exploit takes place inside of an SMB session that involves several phases that must be tracked: the negotiation of the session's parameters, an authentication, one or more RPC function calls, and their matching responses. As a result, detecting this exploit requires tracking the state of several network protocols over the lifetime of their sessions. There is no single packet or portion of the ongoing conversation that contains everything necessary for detection.

First, let's examine the different parts of a successful PetitPotam exploitation, and then we'll see how Zeek tracks the state of the network protocols for us to enable the detection process.

PetitPotam exploitation works by abusing the lack of sufficient permission checking when calling EFS DCERPC functions on remote Windows systems. In most cases, calling a remote DCERPC function occurs over an SMB session, so each exploitation starts by negotiating the SMB session's parameters. Zeek takes care of tracking the state of each SMB session and its associated TCP session for us out of the box by storing much of what it knows for later use. This information is stored inside of the record that Zeek keeps for each network connection that it sees. By tradition, the connection record is referred to by the variable **c**, and additional information about each connection is stored in sub-variables delimited by the \$ operator. For example, additional information about the current state of each SMB session is stored in **c**\$smb\_state . Figure 1 shows a small portion of the information that Zeek has recorded about an SMB read operation from

\\192.168.0.85\IPC\$ (Note: this snippet is paired down for readability; <u>there is a lot more</u> information available in c\$smb\_state). What you need to know is that Zeek is tracking this type of information for us across the lifetime of each SMB session. As each SMB session progresses, Zeek will add or update values to this subrecord so that it represents a summary of the SMB session's current state.

```
c$smb state=[
     current cmd=[
     ts=1630594390.078445,
     uid=CPQgUe4i19bDTvuTld,
     command=READ,
     status=SUCCESS,
     rtt=1.0 sec 20.0 msecs 879.983902 usecs,
     version=SMB2
     ],
     current file=[
     ts=1630594390.069815,
     uid=CPQqUe4i19bDTvuTld,
     action=SMB::PIPE READ,
     path=\\192.168.0.85\IPC$,
     name=lsarpc,
     size=0,
     fid=34359743200,
     1
]
```

## Figure 1

The next step in detecting a PetitPotam exploit is to dissect the DCERPC function calls that ride on top of the SMB session, and look for signs of someone attempting to trigger an NTLM relay by making an EFS function call. Again, Zeek takes care of most of these details for us by treating DCERPC as just another network layer above SMB. Also like the SMB sessions, Zeek stores state information about the current DCERPC call or response in several places within the c variable. In the case of DCERPC, this state information is stored in c\$dce\_rpc, c\$dce\_rpc\_state, and c\$dce\_rpc\_backing.

Unfortunately, the DCERPC protocol's multiplexed nature makes it more difficult to analyze than other protocols. Function calls and responses do not need to be sequential; they can be interleaved and sometimes even out of order. That is, inside of a single SMB session, there can be more than one DCERPC function call active at the same time awaiting a response. To add to the complexity, DCERPC requires a separate bind action within the SMB session that selects the family of functions that will be called. This means that a single remote function call will require a bind action, a function call, and a response, all of which will appear in separate portions of the TCP session.

Thankfully, Zeek tracks all of these details for us. Consider Figures 2, 3, and 4 below which show the bind, call, and response sequence of packets that exist during an attempt to trigger the PetitPotam exploit. Prior to this, the attacker (192.16.0.15) has negotiated an SMB2 session with the victim (192.168.0.85). In Figure 2, the attacker binds to the DCERPC

endpoint c681d488-d850-11d0-8c52-00c04fd90f7e, which is associated with the <u>Windows Encrypted File System</u> DCERPC functions (see the line near the bottom of Figure 2 that is highlighted in blue).

			<b>u</b> 🔽 🗖	📕 @, @, @, 🔛	
cerpc   Time	Source	Destination	Protocol	Length Info	•
1991 51.068872 1994 51.070407 1995 51.073268	192.168.0.15 192.168.0.85 192.168.0.15	192.168.0.85 192.168.0.15 192.168.0.85	DCERPC DCERPC EFS	242 Bind: call_id: 1, Fragment: Sin 206 Bind_ack: call_id: 1, Fragment: 278 EfsRpcOpenFileRaw request	
2042 52.096420	192.168.0.85	192.168.0.15	EFS	186 EfsRpcOpenFileRaw response, Err	or: WERR_BAD_NETPATH
<pre>thernet II, Src: nternet Protocol ransmission Contr tetBIOS Session Se MB2 (Server Messa &gt; SMB2 Header ProtocolId: @ Header Length Credit Charge Channel Seque &gt; Flags: 0x0000 Command: Writ Credits reque &gt; Flags: 0x0000 Chain Offset: Message ID: @ Process Id: @ &gt; Tree Id: 0x000 &gt; Session Id: @ Signature: ac (Response in: * Write Request (0 &gt; StructureSize Data Offset: Write Length: File Offset: &gt; GUID handle F Channel: None Remaining Byt &gt; Write Flags: Blob Offset: Blob Deffset: Blob Deffset: Blob Deffset: Blob Deffset: Blob Deffset: Blob Deffset: Blob Deffset: Blob Deffset: Blob Deffset: Blob Data Representai Frag Length: 72 Auth Length: 0 Call ID: 1 Max Xnit Frag: A Assoc Group: 0x1 Num Ctx Items: Ctx Item[1]: Con Context ID: @ Num Trans Ite Abstract Synt Interface Interface</pre>	<pre>VMware_39:e1:09 (00 Version 4, Src: 192 ol Protocol, Src Po rvice ge Block Protocol v krfe534d42 :: 64 :: 1 mince: 0 00 00 00000000 is ked0: 127 00008, Signing 0x00000000 0000001 \\192.168.0 kr000000000 0000001 \\192.168.0 kr00001000e0000022 A d5fa5ccd7460cb75fc9 19921 0x000 :: 0x0001000e000000 0 0 0 iie: 1sarpc : (0x00000000 0 800000000 0 800000000 0 8000000</pre>	:0c:29:39:e1:09), Dst 160.0.15, Dst: 192.1 rt: 33524, Dst Port: / ersion 2) .85\IPC\$ cct: Domain: Host: fle381b71c5 emote Procedure Call r: Little-endian, Cha	: VMware_f9:91 68.0.85 145, Seq: 773, (DCE/RPC) Bind nr: ASCII, Floo	, Fragment: Single, FragLen: 72, Call	
0 00 e4 11 2f 40 0 00 55 82 f4 01 0 01 f5 ae 0b 00	35 00 0c 29 39 e1 00 40 06 a7 30 c0 bd bd b0 30 e5 d3 00 00 00 00 b8 fe	a8 00 0f c0 a8, 8f 2c 3f 50 18 .U. 53 4d 42 40 00	5 )9 E /@ @ 0 		
00 00 06 00 00 0 00 00 2d 00 00 0 60 cb 75 fc 9f	1e 38 1b 71 c5 31	00 00 00 01 00 d5 fa 5c cd 74 00 70 00 48 00 `.u			
00 00 01 00 00 00 00 00 00 00 00 0 00 00 48 00 00	00 00 00 00 00 00 df 00 04 00 00 00 00 00 00 00 00 00 00 00 05 00 01 00 00 00 00 08	00 00 00 00 00 00 00 0b 03 10 00 10 b8 10 00 00	·····		
0 d0 11 8c 52 00	00 00 00 01 00 88 c0 4f d9 0f 7e 01 11 9f e8 08 00 2b	d4 81 c6 50 d8 00 00 00 04 5d 10 48 60 02 00	ι		
0.0 0.0					

Next, the attacker tells the victim that it wants to call the <u>EfsRpcOpenFileRaw</u> function, which has the operation number 0. This is visible as the <u>Opnum</u> value on the line near the bottom of Figure 3, again highlighted in blue.

erpc			₽⊻	📕 સ્વ્વ્		80.
Time	Source	Destination		Lengt/ Info		
1991 51.068872 1994 51.070407 1995 51.073268	192.168.0.15 192.168.0.85 192.168.0.15	192.168.0.85 192.168.0.15 192.168.0.85	DCERPC DCERPC EFS		<pre>ragment: Single, 1 context 1, Fragment: Single, max_x request</pre>	
2042 52.096420	192.168.0.85	192.168.0.15	EFS		esponse, Error: WERR_BAD_N	IETPATH
thernet II, Src: thernet II, Src: thernet Protocol ansmission Contr etBIOS Session Se HB2 (Server Messa SHB2 Header ProtocolId: ( Header Length Credit Charge Channel Seque Reserved: 004 Command: Writ Credits reque > Flags: 0x0040 Chain Offset: Mrite Reguest ( > StructureSize Data Offset: StructureSize Data Offset: Blob Offset: Blob Length: Channel Info istributed Compat: 0 Auth Length: 9 Version (minor) Packet Type: Re Data Representa Frag Length: 10 Auth Length: 8 Call D: 1 Alloc hint: 84 Context ID: 0 Opnum: 0	<pre>VMware_39:e1:09 (d Version 4, Src: 15 rool Protocol, Src: 16 rool Protocol, Src: 16 ervice age Block Protocol axfe534d42 h: 64 e: 1 ence: 0 00 te (9) ested: 127 00008, Signing : 0x00000000 0000001 \\192.168 bx000000000 0000001 \\192.168 bx0000000000 1 \\192.168 bx000000000 fileshof000000 e: 0x0001 0x0070 : 108 0 File: lsarpc e (0x00000000) tes: 0 0x00000000 0 Blob: NO DATA ting Environment / : 0 quest (0) x83 tion: 10000000 (or 8</pre>	00:00:29:39:e1:09), Dst 22.168.0.15, Dst: 192.1 Port: 33524, Dst Port: version 2) .0.85\IPC\$ Acct: Domain: Host: c27ecee578f8c	t: VMware_f9:9 168.0.85 445, Seq: 107 (DCE/RPC) Req	1:35 (00:0c:29:f9:91:35) 8, Ack: 1409, Len: 224 uest, Fragment: Single, Fr	F_{55866BDCD-AF33-438A-BED1 agLen: 108, Call: 1, Ctx:	
[Response in fr Complete stub d						
FS (pidl), EfsRpc Operation: EfsR [Response in fr Max Count: 33 Offset: 0 Actual Count: 3	COpenFileRaw: \\193 pcOpenFileRaw (0) ame: 2042]	2.168.0.15\test\Setting tings.ini	js.ini			
01       15       19       99       00         01       00       00       00       00       00         00       00       00       2d       00       00         00       00       02       2d       00       00         00       00       2d       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       00       00       00         00       00       00       21       00       00	bd         bd         b0         32         16           00         00         00         00         00         00           00         00         00         00         00         00         00           00         00         00         00         00         00         00         00           00         00         00         00         00         00         00         00           00         04         00         00         00         00         00         00           00         04         00         00         00         00         00         00           00         04         00         00         00         00         00         00           00         04         00         00         00         00         00         00           00         04         00         00         00         00         00         00         00           00         04         00         00         00         00         00         00         00         00         00         00         00         00         00         00         00	1         3         4         4         4         6         6           18         0         0         0         0         0         0         0           18         0         0         0         0         0         0         0         0           18         0         0         0         0         0         0         0         0           16         18         1         0         0         0         0         0         0           11         10         70         0         0         0         0         0         0         11	2			
2e 00 30 00 2e 73 00 74 00 5c	00 31 00 35 00 5 00 53 00 65 00 7 00 2e 00 69 00 6	c 00 74 00 65 00 .0	).1 5∖te ∖S etti  s. ini			

Finally, when the victim host has finished executing the EfsRpcOpenFileRaw function, it sends back a response with a return value, which in this case is 0x00000035, per Figure 4.

991         51.068872         192.168.0.15         192.168.0.85         DCERPC         242         Bind:         call_id:         1, Fragment:         Single,         1 context         items:         E_           994         51.078407         192.168.0.85         192.168.0.15         DCERPC         206         Bind_ack:         call_id:         1, Fragment:         Single,         max_xmit:         4280_           995         51.073268         192.168.0.15         192.168.0.85         EFS         278         EfsRpcOpenFileRaw         request	erpc   Time	Source	Destination	Protocol Le	ngth Info			•
999 51:09260 102:460.615 102:160.015 102:160.015 102 102 105 175 00 1150 1760.00141ker request 402 52:06027 105 Dytes on vire (1488 bits). 145 Dytes captured (1488 bits) on interface DeviceMPTL (5586800-A733-38A-803-4986875500 Hermer 11, for (vertise A, Src 102:160.0458, Datt 102:160.0458) termer Frotecol, For Portecol, Port 140, Dyte Port 13024, 566.0453 maintains interface Portecol, Port 140, Dyte Port 13024, 566.0453 maintains interface Portecol, Port 140, Dyte Port 13024, 566.0453 maintains interface Port 140, Dyte Port 13024, 566.0453 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.015 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 200 Portor Protecol Lis Vertaion 2, Port 140, Dyte Port 13024, 566.01 201 Portor Protecol Lis Vertaion 2, Portor Protecol Lis Vertaion 1, Portor Protecol Lis Vertaion 1, Portor Protecol Lis Vertaion 2, Portor Protecol Lis Vertaion 1, Port 140, Dyte Port 13024, 566.01 Protecol Lis Vertaion 1, Portor Protecol Lis Vertaion 1, Port 140, Dyte Port 1, Float: 1EED Protecol Lis Vertaion 1, Port 140, Dyte Port 1, Float: 1EED Protecol Lis Vertaion 1, Port 140, Dyte Port 1, Float: 1EED Protecol Lis Vertaion 1, Port 140, Dyte Port 1, Float 1, Port 14, Dyte Port 140, Dyte Po	1991 51.068872	192.168.0.15	192.168.0.85	DCERPC	242 Bind: call			
<pre>mb</pre>	1994 51.070407 1995 51.073268						: Single, max_xm	1t: 4280
herner 11, 5rci Wware_0193135 (0010c23):931235), Dirt Wware_392c1200 (0010c23039cc120) TerrerFrometry Version 4, 5rc 120, 120, 120, 120, 120, 120, 120, 120,	2042 52.096420	192.168.0.85	192.168.0.15	EFS	186 EfsRpcOpen	FileRaw response, En	ror: WERR_BAD_NE	TPATH
ternet Protocol Version 4, 5rc: 192:188.85, Dot: 192:188.05 mathissis Charles Protocol Version 2) Closure massign lock Protocol version 2) Der Stocol Theoder Lenging Block Protocol Version 2) Der Stocol Command: Read (8) Command: Stocol Version 4, Stocol Version 2) Session (8) In Meddel Meddel Meddel Version 4, Stopping Command: Stocol Version 4, Stopping Command, Signing Command: Stocol Version 4, Stopping Command: A Read Lenging Command: Stopping Command: A Read Lenging							-AF33-438A-BED1-4	4996867D5CB0
amanistical Control Protocol, Src Port: 445, Dit Port: 33524, Seq: 1569, Ack: 1419, Len: 132 (MESG Session Service RESSNER Elock Protocol, version 2) SP2 Reader Protocoling, Ack Protocol, version 2) (Freq: Control Protocoling, Control Proto					9 (00:0c:29:39	:e1:09)		
HBIOS Session Service JSP2 Reader Protect[10: shr53442 Header Length: 64 Command: Read (0) Command: Read (0) The Read Response (0) Resson: Subset Read Response (0) Response (0)					Ack: 1419, Len	: 132		
9402 Header Protecolize KorS14422 Header Length: 64 Credit Charge: 16 NT Status: STATUS_SUCCESS (#0.00000000) Command: January Clair & Montecolize Clair & Montec	etBIOS Session Se	ervice						
Protocolf: br(53442) Medder Lengt: 64 Credit parates: 8 Fr Status: STADE_SUCCESS (ex00000000) Communit: Read (0) Credits parates: 8 From request: 1.0200000000 Session if: br000000000000 Session if: br00000000000000 Session if: br000000000000000000000000000000000000		age Block Protocol v	version 2)					
Credit Charge: 16 Mr Status: STADS_SUCCESS (0x0000000) Command: Read (8) Credits granted: 0 / Flag: Exd0000000022 Actr: Demain: Host: Signing Credits granted: 0 / Session if is to0000000000022 Actr: Demain: Host: Signing Credits (status) / Session if is to000000000002 Actr: Demain: Host: Signing Credits (status) Time from request: 1.02000000 seconds] Read Response (sto00000 / Status of response (sto000000) / Status of response (sto00000) / Status of response (sto000000) / Status of response (sto0000000) / Status of response (sto00000000) / Status of response (sto0000000000) / Status of response (sto000000000000000000000000000000000000		ðxfe534d42						
NT Status: STATUS_SUCCESS (#A00000000)           Command: Based (0)           Credits granted: 0           P Hags: B000000000, B0000000000000000000000000								
Command: Read (8) Credits gravit de Command, Signing Chain diffet: beebeebeeb Message 10: 24 Ayn: Cid beebeebeebeebeebe Message 10: 24 Ayn: Cid beebeebeebeebeebee Jobschrift de Command, Signing Time for any Cid beebeebeebee Message 10: 24 Message 10: 24 Messa			000000)					
<pre>&gt; Plag: booleeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee</pre>	Command: Read	d (8)						
Chain Offset: 8x800000 Message ID: 24 Async Id: 8x800000000000000000000000000000000000			upc command Signing					
Messape ID: 24 Ayrc 5: developmentedevelopmented Signature: Stoc2re64Ded24Stolde22deGP781d [Response to: 1980] [Time from request: 1.62086800 seconds] Read Engning Fourier average StructorsExt extended Aread Length: 48 Read Amemining: 8 Read Engning Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 48, Call: 1, Ctx: 0, [Req: #199 Version: 5 Read English: 6 Read Response (0x00) Packet Tupp: 0: 0 Packet Tupp: 0: 0 Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE) Present: 6 Arth Length: 6 Concet Count: 0 (Gpnm: 6] [Request: In frame: 1995] [Request: In frame: 1995] Prime from request: 1.423152000 seconds] Computer stub data (24 Systes) S (pidU), EffactopentileMar Operation: EffactopentileMar (Mar Mar Mar Mar Mar Mar Mar Mar Mar Mar			ne command, signing					
<pre>&gt; Series 15: 0 e00001000000000000000000000000000000</pre>	Message ID: 2	24						
Signature: 385:27:0640bd/2df/350/6d-29:06781d [Response: 00:00] [Time from request: 1.02888000 seconds] Read Response: 1.02888000 seconds] Read Response: 1.02888000 seconds] Read Response: 1.0288000 Read Response: 1.0288000 Read Response: 1.0288000 Read Response: 1.0288000 Read Response: 1.0288000 Version (minor): 0 Packet Hugs: 0.03 Data Offset: 0.04 Packet Hugs: 0.03 Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE) FragLength: 0 Auch Length: 0 Context Dp: 1.00 Auch Length: 0 Context Dp: 1.00 Auch Length: 0 Context Dp: 1.02880000 seconds] (Fine from request: 1.023152000 seconds] (Fine from request:			Acct: Domain: Most:					
<pre>[ficepose_toi_1990] [Time from request: 1-20880000 seconds] Read Response (0x80) &gt; StructureScie :0x001 Data Offset: 0x0000 stributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 48, Call: 1, Ctx: 0, [Req: #199 Version: 5 Version: 5 Version: 5 Version: 6 Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE) Frag Length: 48 Auth Length: 6 Call Dp: 1 Alloc hint: 24 Context Dp: 6 Cantel court: 0 (Bpount 6) [Request in frame: 1995] [Time from request: 1.023152000 seconds] Complete stub data (24 bytes) \$ (pidd), EfsqCopenFileBaw Operation: EfsqCopenFileBaw Operation: EfsqCopenFileBaw Operation: EfsqCopenFileBaw Operator: EfsqCopenFileBaw Oper</pre>								
Read Response (bids)           > StructureScie: 0.0011           Data Offset: 0.00504           Read Length: 46           Read Memaining: 0           Reserved: 0.0000000           StructureScience           StructureScience           Version: 5           Version: 6           Packet type: Response (2)           Packet tin frame: 1995)           T	[Response to:	1998]						
<pre>&gt; Structure5ize: 0x0011 Data Offse: 0x0001 Reserved: 0x00000 Reserved: 0x000000 Reserved: 0x000000 (Order: Little-endian, Char: ASCII, Float: Single, FragLen: 48, Call: 1, Ctx: 0, [Req: #199 Version (sinor): 0 Packet Type: Response (2) Packet Type</pre>			seconds]					
Read Length: 48         Control (1)           Read Ressining: 0         Rescrete: 0000000           Stributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 48, Call: 1, Ctx: 0, [Req: #199           Version: 3         Packet type: Response (2)           Packet type: Response (2)         Packet type: Response (2)           Frag Length: 48         Response (2)           Packet type: Response (2)         Packet type: Response (2)           Frag Length: 48         Response (2)           Call to: 1         Alloc hint: 24           Context to: 0         (Context 10: 0           (Bequest in frame: 1995)         (Fidd), EfspeQuenitaken (6)           [Request in frame: 1995]         Packet type: Sin frame: 1995]           Pointer to Pointex: Fudd_EMO (METPATH (6x00000035))         Packet type: Sin frame: 1995]           Pointer to Pointext Fudd_EMO (METPATH (6x00000035))         Packet ty								
Read Rem_Ining: 0         Reserved: 0000000         stributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 48, Call: 1, Ctx: 0, [Req: #199         Version (sinor): 0         Packet type: Response (2)         Context type: Response (2)         Compete stub data (24 bytes)         S (pid10), FrageOpenTileRaw         Operation: EfforcePartitype         Pointer to Pointer to Pointer type								
Reserved: 00000000           Stributed Computing Environment / Remote Procedure Call (DCE/RPC) Response, Fragment: Single, FragLen: 48, Call: 1, Ctx: 0, [Req: #199           Version (sinor): 0           Packet type: Response (2)           Context ID: 0           Cancet court: 0           (Bopun: 0)           (Request in frame: 1995)           Time frame coupst in frame: 1995)           Pointer to Pointers (Policy_handle)           Windows Error: WERM_BOD_NETPATH (ex00000035)								
Version: 5         Version: 6:007: 0         Packet type: Response (2)         Packet Plags: 0x03         Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE)         Frag Length: 48         Auth Length: 0         Call ID: 1         Alloc hint: 24         Context ID: 0         Canect count: 0         (Dpum: 0)         Request: 1.02152000 seconds]         Compute stub data (24 bytes)         S (jdi), fisspcopenFileRaw (0)         (Request in frame: 1995)         Pointer to PvContext (policy_handle)         Windows Error: MERR_BAD_METPATH (0x0000005)         Windows Error: MERR_BAD_METPATH (0x0000005)								
Version (minor): 0           Packet type: Response (2)           Packet type: Ne83           Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE)           Frag Length: 48           Auth Length: 0           Call ID: 1           Alloc hint: 24           Context ID: 0           Cancel count: 0           [Dgnum: 0]           Request in frame: 1995]           Time fram request: 1.023152000 seconds]           Complet study data (24 bytes)           \$ (pidl), fragecopentileRaw           Operation: EffonçOpentileRaw (0)           [Request in frame: 1995]           Pointer to PxContext (policy_handle)           Windows Error: WERM_BAD_METPATM (0x00000035)		ting Environment / F	Remote Procedure Call	(DCE/RPC) Respon	ise, Fragment:	Single, FragLen: 48,	Call: 1, Ctx: 0	, [Req: #199
Packet Fügs: 0x03         Data Representation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE)         Frag Length: 48         Auth Length: 0         Call ID: 1         Alloc hint: 24         Context ID: 0         Cancel count: 0         (Opnum: 0)         Request in frame: 1995]         Trime from request: 1.023152000 seconds]         Complete studied at (24 bytes)         5 (pidl), EfsRpcOpenFileRaw (0)         Deparation: EfsRpcOpenFileRaw (0)         Request in frame: 1995]         Pointer to PuContext (policy_handle)         Windows Error: WEM_BAD_HETPATH (ex0000035)		: 0						
Data Reprisentation: 10000000 (Order: Little-endian, Char: ASCII, Float: IEEE)         Frag Length: 48         Auth Length: 0         Call ID: 1         Alloc hint: 24         Context ID: 0         Cancet count: 0         [Opnum: 0]         Request in frame: 1995]         [Time fram request: 1.023152000 seconds]         Complete stub data (24 bytes)         5 (fuid), Frame: 1995]         [Request in fr								
Frag Length: 48         Auth Length: 0         Call ID: 1         Alloc hint: 24         Context ID: 0         Cancet count: 0         [0pnue: 0]         [Request in fram: 1995]         [Time fram request: 1.023152000 seconds]         Complete stub data (24 bytes)         S (pidl), EfsRpCopenFileRaw (0)         [Request in frame: 1995]         Pointer to PvContext (point)         Pointer to PvContext (point)         Vindows Error: WERA_BAD_NETPATH (0x0000035)			er: Little-endian. Ch	ar: ASCII. Float	: TFFF)			
Call ID 1 Alloc hint: 24 Context ID: 0 Cancel count: 0 [Gonue: 0] [Request in frame: 1995] [Time from request: 1.023152000 seconds] Complete stub data (24 bytes) 5 (pid1), EfsRpcOpenFileRaw (0) [Request in frame: 1995] Pointer to PvContext (policy_handle) Windows Error: WERK_BAD_NETPATH (0x00000035) Windows Error: WERK_BAD_NETPATH (0x00000035) 00 0 c 29 39 cl 00 00 0 c 29 f9 91 35 08 00 45 00)9).5.E. 00 ac 81 27 40 00 20 66 00 00 a 05 5 c 28 a 			err carere enotony en					
Alloc hint: 24 Context ID: 0 Cancel count: 0 [Opuma: 0] [Request in frame: 1995] [Time from request: 1.023152000 seconds] Complete stub data (24 bytes) 5 (jail), EfsRpcOpenFileRaw (0) [Request in frame: 1995] Pointer to PvContext (Dplicy_handle) Windows Error: WERM_BAD_NETPATH (0x00000035) Windows Error: WERM_BAD_NETPATH (0x00000035) 0 0 0 c 29 39 c1 09 00 0c 29 f9 91 35 08 00 45 00)9								
Context ID: 0 Cancel count: 0 [Conue: 0] [Request in frame: 1995] [Time from request: 1.023152000 seconds] Complete stub data (24 bytes) S (pidl), EfsRpcOpenFileRaw Operation: EfsRpcOpenFileRaw Operation: EfsRpcOpenFileRaw (0) [Request in frame: 1995] Pointer to PvContext (policy_handle) Windows Error: WERR_BAD_NETPATH (0x0000035) Windows Error: WERR_BAD_NETPATH (0x0000035) 00 0c 29 39 cl 09 00 0c 29 f9 91 35 08 00 45 00 0 0f 0c 10 42 f4 d3 f2 dc bd b0 33 65 51 81 								
[Opnum: 0] [Request in frame: 1995] [Time from request: 1.023152000 seconds] Complete stub data (24 bytes) S (pidl), EfsRpcOpenFileRaw Operation: EfsRpcOpenFileRaw (0) [Request in frame: 1995] Pointer to PvContext (policy_handle) Windows Error: WERE_BAD_NETPATH (0x00000035) Windows Error: WERE_BAD_NETPATH (0x00000035) 0 0 0 0 0 2 39 el 09 00 cc 29 f9 91 35 08 00 45 00 								
[Request in frame: 1995]         [Time from request: 1.023152000 seconds]         Complete stub data (24 bytes)         S (pidl), EfsRpcOpenFileRaw         Operation: EfsRpcOpenFileRaw (0)         [Request in frame: 1995]         Pointer to PvContext (policy_handle)         Windows Error: WERR_BAD_NETPATH (0x00000035)								
Complete stub data (24 bytes) S (pidl), EfsRpCOpenFileRaw Operation: EfsRpCOpenFileRaw (0) [Request in frame: 1995] Pointer to PvContext (policy_handle) Windows Error: WERR_BAD_NETPATH (0x00000035) 00 0c 29 39 e1 09 00 ec 29 f9 91 35 08 00 45 00)9 >-5E- 00 ac 81 27 40 00 80 06 00 00 c as 00 55 c0 as		me: 1995]						
S (pidl), EfsRpcOpenFileRaw Operation: EfsRpcOpenFileRaw (0) [Request_10 frame: 1995] Pointer to PvContext (policy_handle) Windows Error: WERR_BAD_NETPATH (0x00000035) 00 0 c 29 39 cl 09 00 cc 29 f9 91 35 08 00 45 00)9)-5E. 00 a c 81 27 40 00 88 06 00 00 cd a8 00 55 cd a8'eU. 00 0f 01 bd 82 f4 d3 8f 2d cb bd bd 33 6b 50 18			conds]					
Operation: EfsRpCOpenFileRaw (0)         [Request_in_frame: 1995]         Pointer to PvContext (policy_handle)         Windows Error: WERR_BAD_NETPATH (0x0000035)         Windows Error: MERR_BAD_NETPATH (0x0000035)         00 0c 29 39 cl 09 00 oc 29 f9 91 35 08 00 45 00	[Time from requ							
Pointer to PvContext (policy_handle) Windows Error: WERR_BAD_WETPATH (0x00000035) 00 0c 29 39 el 09 00 ec 29 f9 91 35 08 00 45 00)9)-5E- 00 ac 81 27 40 00 80 06 00 c0 as 00 55 c0 as'eU 00 0f 01 bd 82 f4 d3 8f 2d cb bd b0 33 6b 50 18	[Time from requ Complete stub d							
Windows Error: MERR_BAD_NETPATH (0x00000035)	[Time from requ Complete stub d FS (pidl), EfsRpc	OpenFileRaw						
00       0c       29       f9       91       35       08       00       45       00      )9)          00       ac       81       27       40       00       80       65       c6       as        10 <td>[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra</td> <td>COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u></td> <td>- )</td> <td></td> <td></td> <td></td> <td></td> <td></td>	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u>	- )					
00       ac       61       27       40       00       80       96       ac       61       27       40       00       80       96       ac       10       96       97       10       10       80       26       b0       80       95       50       88	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
00       ac       61       27       40       00       80       96       ac       61       27       40       00       80       96       ac       10       96       97       10       10       80       26       b0       80       95       50       88	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
00       ac       61       27       40       00       80       96       ac       61       27       40       00       80       96       ac       10       96       97       10       10       80       26       b0       80       95       50       88	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
00       ac       61       27       40       00       80       96       ac       61       27       40       00       80       96       ac       10       96       97       10       10       80       26       b0       80       95       50       88	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
00       ac       61       27       40       00       80       96       ac       61       27       40       00       80       96       ac       10       96       97       10       10       80       26       b0       80       95       50       88	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
00       ac       61       27       40       00       80       96       ac       61       27       40       00       80       96       ac       10       96       97       10       10       80       26       b0       80       95       50       88	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
00       ac       b1       27       40       00 <td< td=""><td>[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo</td><td>COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
00       ac       b1       27       40       00 <td< td=""><td>[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo</td><td>COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl</td><td></td><td></td><td></td><td></td><td></td><td></td></td<>	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo	COpenFileRaw pcOpenFileRaw (0) <u>me: 1995]</u> ntext (policy_handl						
28       6f       52       53       60       00       80       66       53       4d       42       40       00       -5       -5       5MBQ         10       60	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo Windows Error: 1	:OpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0	x00000035)	19)SE.				
00       01       18       00 <td< td=""><td>[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo Windows Error: ] 0 00 0c 29 39 e1 0 00 ac 81 27 40</td><td>COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0 00 00 00 0c 29 f9 91 000 80 0c 00 00 c0</td><td>x00000035) . 35 08 00 45 00 ···) a8 00 55 c0 a8 ···</td><td>'aU</td><td></td><td></td><td></td><td></td></td<>	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo Windows Error: ] 0 00 0c 29 39 e1 0 00 ac 81 27 40	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0 00 00 00 0c 29 f9 91 000 80 0c 00 00 c0	x00000035) . 35 08 00 45 00 ···) a8 00 55 c0 a8 ···	'aU				
00       00 <td< td=""><td>[Time from requ ) Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra &gt; Pointer to PvCo Windows Error: Windows Error: 0 00 0c 29 39 e1 0 00 ac 81 27 40 0 00 of 01 bd 82 20 20 01 25 30 00</td><td>COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 100 80 00 29 99 91 100 80 00 80 00 80 70 10</td><td>x00000035) . 35 08 00 45 00) 0 88 00 55 c0 88 b0 33 6b 50 18 53 4d 42 40 00</td><td>'@ U - 3kP S SMB@</td><td></td><td></td><td></td><td></td></td<>	[Time from requ ) Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra > Pointer to PvCo Windows Error: Windows Error: 0 00 0c 29 39 e1 0 00 ac 81 27 40 0 00 of 01 bd 82 20 20 01 25 30 00	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 100 80 00 29 99 91 100 80 00 80 00 80 70 10	x00000035) . 35 08 00 45 00) 0 88 00 55 c0 88 b0 33 6b 50 18 53 4d 42 40 00	'@ U - 3kP S SMB@				
00 00 00 00 00 00 00 00 00 00 00 00 00	[Time from requ Complete stub d Operation: EfsR [Request in fra Pointer to PvCo Windows Error: ] 0 00 0c 29 39 c1 0 00 ac 81 27 40 0 00 f 82 53 00 10 00 00 00 00	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 00 00 00 00 00 00 00 00 14 d3 8f 2d cb bd 00 00 00 00 00 00 00 00	x00000035) 35 08 00 45 00 35 08 55 c0 a8 53 46 22 40 00	'@3kP SSMB@				
00 00 30 00 00 01 00 00 00 18 00 00 00 00 00 00 ··········	[Time from requ Complete stub d FS (pidl), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo Windows Error: 0 00 0c 29 39 e1 00 ac 81 27 40 0 00 of 01 bd 82 2 20 of 82 53 00 10 00 00 00 00 0 00 01 800 00 0 00 00 00 00 00	COpenFileRaw pcOpenFileRaw (0) met: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 00 00 00 00 00 00 00 2 f4 d3 8f 2d cb bd 00 00 00 00 00 86 fe 00 00 00 00 00 86 fe 00 00 00 00 00 00 00 fe	x00000035) . 35 08 00 45 00 a8 00 55 c0 a8 b0 33 6b 50 18 b3 36 b5 0 18 b0 00 00 00 00 b0 00 00 00 b5 c2 7b 60 bb	'e U - 3kP S SMBe				
00 00 00 00 <u>35 00 00 00</u> <u>5</u>	[Time from requ Complete stub d FS (pid), EfsRpc Operation: EfsR [Request in fra > Pointer to PvCo Windows Error: 0 00 0c 29 39 e1 0 00 ac 81 27 40 0 00 f 01 bd 82 2 00 f 82 53 00 10 00 00 00 00 00 00 00 2 53 00 10 00 00 00 00 00 00 00 2 53 00 0 00 00 18 00 00 00 00 0 2 53 00 0 00 0 0 0 00 00 0 00 0 0 0 00 00 0 00 0	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 00 80 06 00 00 00 21 44 38 f 2d cb bd 00 80 00 08 00 00 00 2 44 43 8f 2d cb bd 00 80 00 00 00 00 2 60 01 0 00 08 00	x00000035) 35 08 00 45 00 38 00 55 c0 a8 b0 33 6b 50 18 53 4d 42 40 00 00 00 08 08 00 00 00 08 08 00 00 00 08 08 00 00 00 08 08 00 00 55 c2 7b 66 bb 00 55 08 30 00 00 02 03 10 00	'@ U 3kP S SMB@ 				
	[Time from requ ) Complete stub d Operation: EfsR [Request in fra Pointer to PvCO Windows Error: 0 00 0c 29 39 e1 0 00 ac 81 27 40 0 00 ac 81 27 40 0 00 0 00 00 00 0 00 0	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 00 68 66 00 00 00 14 d3 8f 2d cb bd 00 68 60 00 88 fe 00 68 60 00 88 fe 00 68 60 00 88 fe 10 60 68 00 00 88 fe 10 60 68 00 00 80 60 10 60 61 60 00 00 81 10 60 61 60 00 80 80	x00000035) 35 08 00 45 00	'@3kP 53kP 5				
	[Time from requ ) Complete stub d Operation: EfsR [Request inn fra ) Pointer to PvCo Windows Error: 0 00 0c 29 39 e1 0 00 ac 81 27 40 0 00 0f 01 bd 82 20 0f 82 53 00 10 00 00 00 00 00 0 00 00 20 00 00 0 00 00 00 00 0 00 00 00 00 0 00 0	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 100 80 06 00 00 00 14 d3 86 00 00 00 14 d3 86 20 00 00 16 00 60 00 00 50 10 00 80 00 00 55 10 00 55	x00000035) 35 06 00 45 00) a6 00 55 c0 a8 b0 33 6b 50 18 b0 33 6b 50 18 c0 00 00 00 00 b5 52 4d 42 40 00 c0 00 00 00 00 00 b5 c2 7b 60 bb c0 50 00 30 00 c0 50 00 31 0 00 c0 50 00 80 00 c0 00 00 00 00	'@3kP SSMB@ 				
	[Time from requ Complete stub d Sopiete stub d Operation: EfsR [Request in fra- Pointer to PvCo Windows Error:] 0 00 0c 29 39 e1 0 00 ac 81 27 40 0 00 f 01 bd 82 20 0f 82 53 00 10 00 00 e0 00 0 00 00 20 00 00 0 00 00 00 00 0 00 00 00 00 0 00 0	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 100 80 06 00 00 00 14 d3 86 00 00 00 14 d3 86 20 00 00 16 00 60 00 00 55 10	x00000035) 35 06 00 45 00) a6 00 55 c0 a8 b0 33 6b 50 18 b0 33 6b 50 18 c0 00 00 00 00 b5 52 4d 42 40 00 c0 00 00 00 00 00 b5 c2 7b 60 bb c0 50 00 30 00 c0 50 00 31 0 00 c0 50 00 80 00 c0 00 00 00 00	'@3kP 53kP 5				
Windows Error (efs.werror), 4 bytes Packets: 3286 - Displayed: 26 (0.8%) Profile: Dr	[Time from requ Complete stub d SS (pid)), EfsRpc Operation: EfsR [Request in fra Pointer to PvCo Windows Error:] 0 00 ac 81 27 40 0 00 0f 01 bd 82 20 0f 82 53 00 10 00 00 20 00 00 0 00 00 00 00 00 0 00 00 00 00 0 00 0	COpenFileRaw pcOpenFileRaw (0) me: 1995] ntext (policy_handl WERR_BAD_NETPATH (0) 100 80 06 00 00 00 14 d3 86 00 00 00 14 d3 86 20 00 00 16 00 60 00 00 55 10	x00000035) 35 06 00 45 00) a6 00 55 c0 a8 b0 33 6b 50 18 b0 33 6b 50 18 c0 00 00 00 00 b5 52 4d 42 40 00 c0 00 00 00 00 00 b5 c2 7b 60 bb c0 50 00 30 00 c0 50 00 31 0 00 c0 50 00 80 00 c0 00 00 00 00	'@3kP 53kP 5				

Figure 4

The only guarantees offered by DCERPC are that these three calls will be in that order within a single SMB session. There may be other function calls and responses interspersed between them which could result in the different stages of the PetitPotam exploit being more broadly spread across an SMB session and intermixed with other, legitimate, SMB operations.

Zeek, however, takes care of keeping track of the state of each DCERPC bind, function call, and response for us out of the box. By the time the response to the function call is finally seen on the network, Zeek has bundled up all of this information for us in <a href="https://csale.com">c\$dce\_rpc\_backing</a> . See Figure 5.

```
dce rpc backing={
     [34359743200] = [
      info=[
           ts=1630594390.076173,
           uid=CPQgUe4i19bDTvuTld,
           id=[orig h=192.168.0.15, orig p=33524/tcp,
resp h=192.168.0.85, resp p=445/tcp],
           rtt=1.0 sec 23.0 msecs 151.874542 usecs,
           named pipe=\pipe\lsass,
           endpoint=efsrpc2,
           operation=EfsRpcOpenFileRaw
      ],
      state=[
       uuid=c681d488-d850-11d0-8c52-00c04fd90f7e,
       named pipe=\pipe\lsass,
       ctx to uuid={
       [0] = c681d488 - d850 - 11d0 - 8c52 - 00c04fd90f7e
       }
      ]
     ]
     }
```

## Figure 5

The only part still missing is the index number ( 34359743200 ), which is the reference number for the open DCERPC call associated with this response. Zeek again takes care of the tracking details for us by passing this value to the <u>dce rpc response</u> event as the value of the argument <u>fid</u>.

We now have everything we need to detect attempts to trigger a PetitPotam exploit. Since Zeek has taken care of the task of tracking and collecting information through the lifetime of the DCERPC session, we only need to capture DCERPC response events by writing a

handler for the <u>dce rpc response stub</u> event. Using the <u>fid</u> argument passed into the event handler, we can extract the DCERPC endpoint UUID, and the name of the function called from the saved state. Then, by comparing the DCERPC endpoint against those that are abused by the PetitPotam exploits, and by examining the function's return code we will notify the analysts in near real time that a possible exploit attempt has occurred and whether it appears to have been successful or not.

By Paul Dokas, Director of Corelight Labs