

Workshop - Passwort-Cracking

Windows XP mit Rainbowtable (Ophrack) - VIDEO



Dokumenten URL:

<http://docs.tx7.de/TT-7XP>

Autor:

Tom Gries <TT-7XP@tx7.de>
@tomo@chaos.social

Lizenz:

Creative Commons BY-NC-ND

Version:

7.1.0 vom 20.10.2024



Legal Disclaimer - Hackerparagraf

Die hier vorgestellten Methoden und Tools dienen zum Schutz der eigenen Systeme. Das Knacken fremder Passwörter ebenso wie das Eindringen in Systeme kann eine Straftat darstellen. Die vorgestellten Tools können unter den Hackerparagrafen 202c StGB fallen. Entsprechend dürfen Sie nur auf eigene Kennwörter oder Testsysteme losgehen, beziehungsweise sich schriftlich die Erlaubnis des Systembesitzers einholen.

Zudem können Cracking-Tools die getesteten Systeme stark beeinträchtigen oder außer Funktion setzen. Entsprechend vorsichtig sollten Sie bei Produktivsystemen sein.

Windows XP Passwörter aufdecken



Ergebnis - das waren die Passwörter

Nr.	Username	Passwort	Crackbar?
1	-- BlackHat	smurfs	[]
2	-- TOMO	my20\$	[]
3	Alpha	BananenDrachen	[]
4	Bravo	smurfs	[]
5	Charlie	moppel77	[]
6	Delta	1u2p3t4o5y6o7u8	[]
7	Echo	DrachenBananen	[]
8	Foxtrott	u1p2t3o4y5o6u7	[]
9	Golf	Sommerschlussverkauf	[]
10	Hotel	MVemjSunP	[]
11	India	MV19emjSu88nP	[]

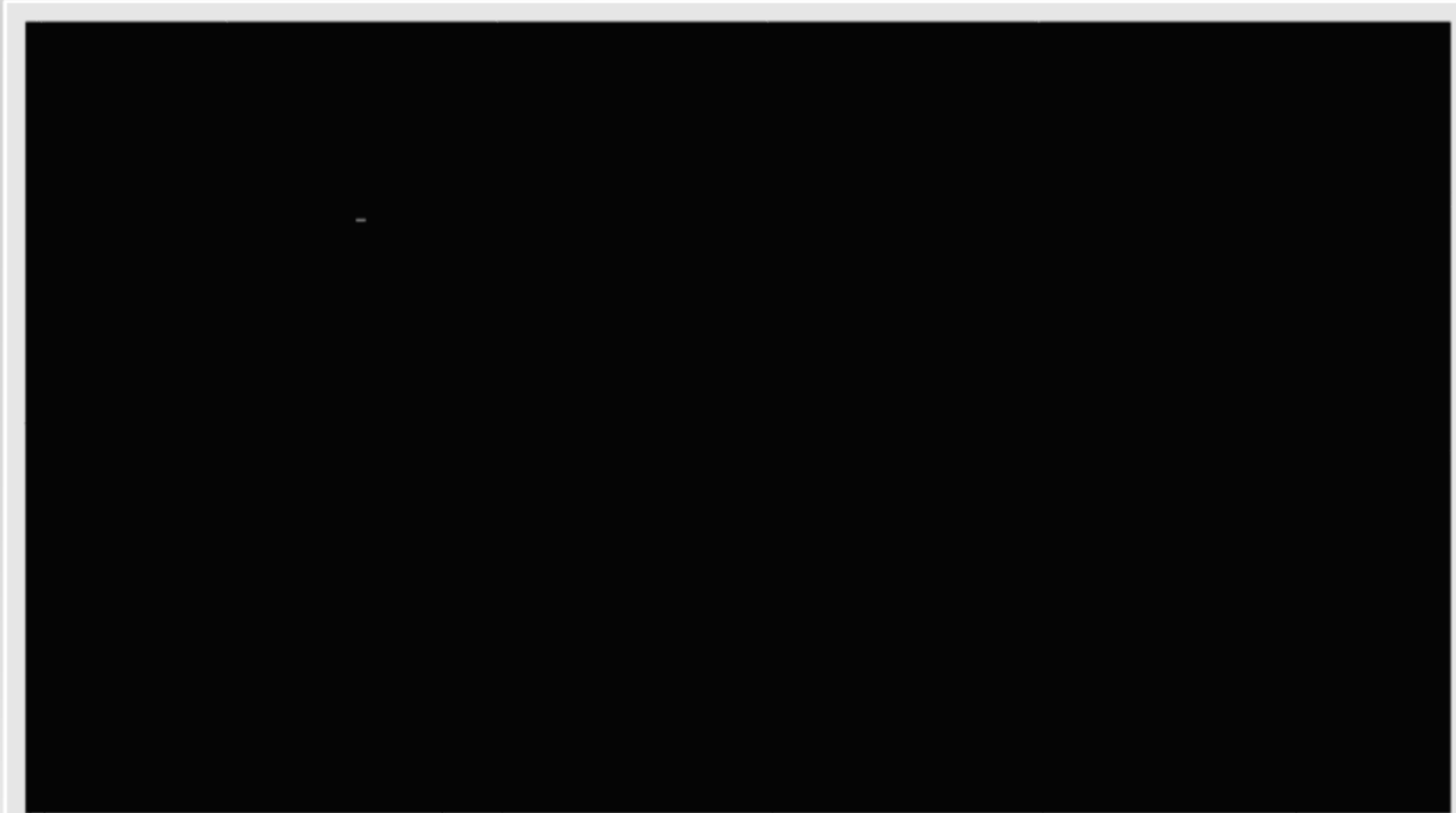
Normaler Boot von Windows XP ...

Windows Passwörter mit Ophcrack ermitteln



Booten mit Ophcrack ...

Windows Passwörter mit Ophcrack ermitteln



Lokale Windows Passwörter

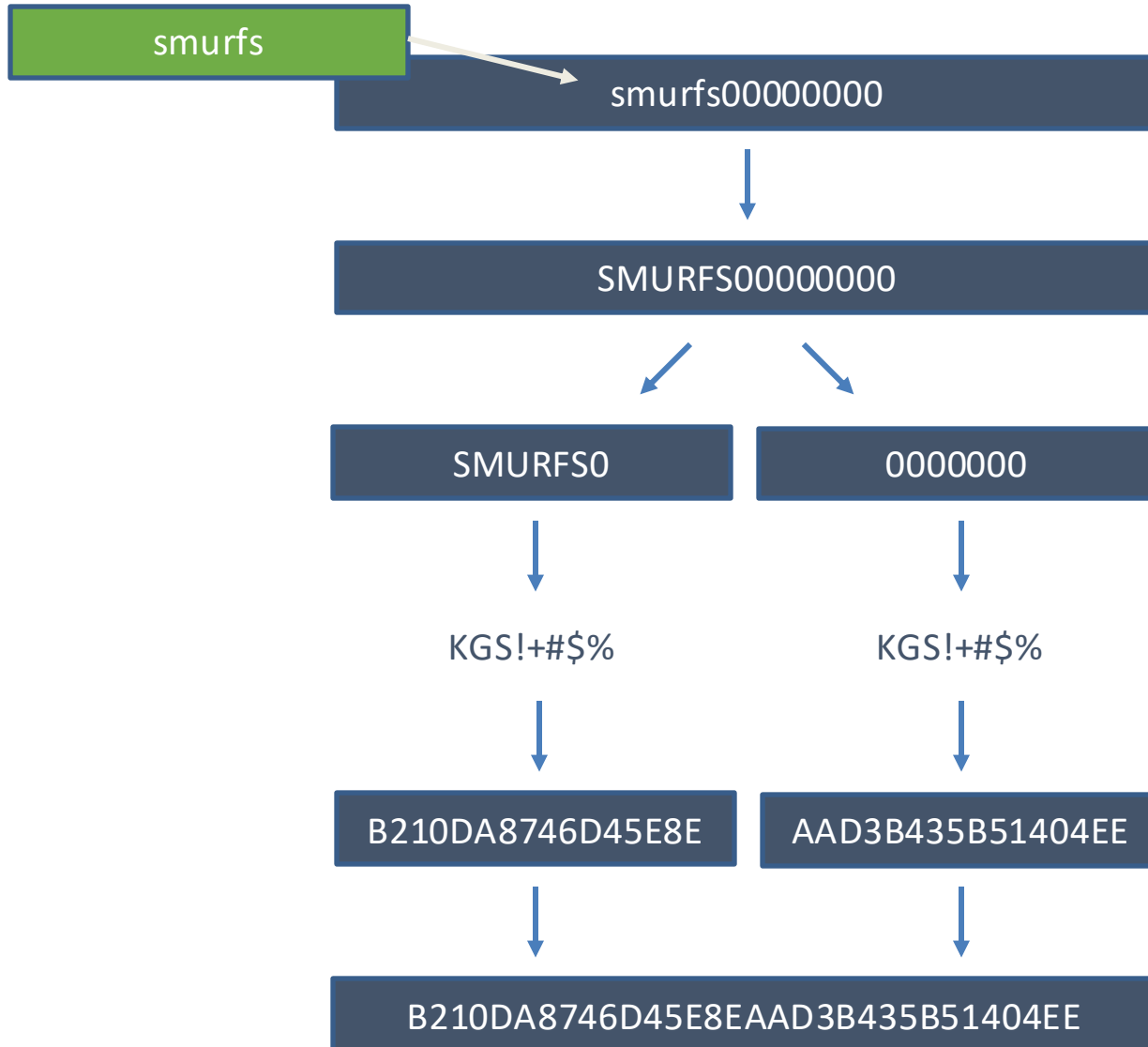
The screenshot shows the L0phtCrack application interface. At the top is a menu bar with icons for Load, Delete, Save, Tables, Crack, Help, Exit, and an OS logo with an 'About' button. Below the menu bar are three tabs: Progress, Statistics, and Preferences. The main window displays a table of local Windows users and their hashes. The table has columns for User, LM Hash, NT Hash, LM Pwd 1, LM Pwd 2, and NT Pwd. The users listed are Alpha, Bravo, Charly, Delta, Echo, Foxtrott, Golf, Hotel, India, -- TOMO, and -- BlackHat. The LM Pwd 1 and LM Pwd 2 columns show the passwords found for each user, with some entries marked as 'empty'. Below the table is a progress bar and a status section. The status section shows the current table being processed (XP fre...), the directory being scanned (///media/hdb...), and the progress (100% in RAM). At the bottom, there are status fields for Preload, Brute force, Pwd found, and Time elapsed.

User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Alpha	89a0c5eea69b2726c751b00e46c404c7	e6f69e1a3e9bf...	BANANEN	DRACHEN	BananenDrachen
Bravo	b210da8746d45e8eaad3b435b51404ee	6302b0bb032e...	SMURFS	empty	smurfs
Charly	9b0df2319e688cc87c3113b4a1a5e3a0	ff71d1eeb1542...	MOPPEL7	7	moppel77
Delta		b4190891f770a...			
Echo	c751b00e46c404c789a0c5eea69b2726	9d15905fee3cf...	DRACHEN	BANANEN	DrachenBananen
Foxtrott	389f986faf0aee6a9dc2eec4a362a4af	533d9864db42...	U1P2T3O	4Y5O6U7	ulp2t3o4y5o6u7
Golf		a5e4ae5873f07...			
Hotel	fdea7f704330de9515a8b184c8fdf2ce	312597bcd054...	MVEMJSU	NP	MVemjSunP
India	564e78fa3238c9e6d3c0535ea8d23e26	05274d8a0a4c...	MV19EMJ	SU88NP	MV19emjSu88nP
-- TOMO	b210da8746d45e8eaad3b435b51404ee	6302b0bb032e...	SMURFS	empty	smurfs
-- BlackHat	d78561d3d0dca0c6aad3b435b51404ee	faf8c1cb5754a...		empty	

Table	Directory	Status	Progress
XP fre...	///media/hdb...	100% in RAM	<div></div>

Preload: done Brute force: done Pwd found: 8/11 Time elapsed: 0h 0m 46s

Wie funktioniert LM?



Der Rest des eingegebenen Passworts wird bis zur Stelle 14 mit NULL (ASCII 0) aufgefüllt (hier mit 0 dargestellt).

Umwandlung in Großbuchstaben (ASCII Stelle 6).

Key	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111	1200	1201	1210	1211	1220	1221	1230	1231	1240	1241	1250	1251	1260	1261	1270	1271
000	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F
001	10	11	12	13	14	15	16	17	18	19	1A	1B	1C	1D	1E	1F	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F
010	20	21	22	23	24	25	26	27	28	29	2A	2B	2C	2D	2E	2F	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F
011	30	31	32	33	34	35	36	37	38	39	3A	3B	3C	3D	3E	3F	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F
100	40	41	42	43	44	45	46	47	48	49	4A	4B	4C	4D	4E	4F	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F
101	50	51	52	53	54	55	56	57	58	59	5A	5B	5C	5D	5E	5F	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F
110	60	61	62	63	64	65	66	67	68	69	6A	6B	6C	6D	6E	6F	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F
111	70	71	72	73	74	75	76	77	78	79	7A	7B	7C	7D	7E	7F	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F
120	80	81	82	83	84	85	86	87	88	89	8A	8B	8C	8D	8E	8F	90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	9F
121	90	91	92	93	94	95	96	97	98	99	9A	9B	9C	9D	9E	9F	A0	A1	A2	A3	A4	A5	A6	A7	A8	A9	AA	AB	AC	AD	AE	AF
122	A0	A1	A2	A3	A4	A5	A6	A7	A8	A9	AA	AB	AC	AD	AE	AF	B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	BA	BB	BC	BD	BE	BF
123	B0	B1	B2	B3	B4	B5	B6	B7	B8	B9	BA	BB	BC	BD	BE	BF	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	CE	CF
124	C0	C1	C2	C3	C4	C5	C6	C7	C8	C9	CA	CB	CC	CD	CE	CF	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	DC	DD	DE	DF
125	D0	D1	D2	D3	D4	D5	D6	D7	D8	D9	DA	DB	DC	DD	DE	DF	E0	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	EB	EC	ED	EE	EF
126	E0	E1	E2	E3	E4	E5	E6	E7	E8	E9	EA	EB	EC	ED	EE	EF	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	FB	FC	FD	FE	FF
127	F0	F1	F2	F3	F4	F5	F6	F7	F8	F9	FA	FB	FC	FD	FE	FF																

Lokale Windows Passwörter

Nr.	Username	Windows LM Hashe		#	Passwort
1	-- BlackHat	D78561D3D0DCA0C6	AAD3B435B51404EE	<8	
2	-- TOMO	B210DA8746D45E8E	AAD3B435B51404EE	<8	
3	Alpha	89A0C5EEA69B2726	C751B00E46C404C7	<15	
4	Bravo	B210DA8746D45E8E	AAD3B435B51404EE	<8	
5	Charlie	9B0DF2319E688CC8	7C3113B4A1A5E3A0	<15	
6	Delta	----- <Nur NTLM> -----		>14	
7	Echo	C751B00E46C404C7	89A0C5EEA69B2726	<15	
8	Foxtrott	389F986FAF0AEE6A	9DC2EEC4A362A4AF	<15	
9	Golf	----- <Nur NTLM> -----		>14	
10	Hotel	FDEA7F704330DE9	515A8B184C8FDF2CE	<15	
11	India	564E78FA3238C9E6	D3C0535EA8D23E26	<15	

Lokale Windows Passwörter

Nr.	Username	Windows LM Hashe				#	Passwort
1	-- BlackHat	D78561D3D0DCA0C6	=	AAD3B435B51404EE	= <leer>	5	My20\$
2	-- TOMO	B210DA8746D45E8E	= SMURFS	AAD3B435B51404EE	= <leer>	6	smurfs
3	Alpha	89A0C5EEA69B2726	= BANANEN	C751B00E46C404C7	= DRACHEN	14	BananenDrachen
4	Bravo	B210DA8746D45E8E	= SMURFS	AAD3B435B51404EE	= <leer>	6	smurfs
5	Charlie	9B0DF2319E688CC8	= MOPPEL7	7C3113B4A1A5E3A0	= 7	8	moppel77
6	Delta	----- <Nur NTLM> -----				>14	1u2p3t4o5y6o7u8
7	Echo	C751B00E46C404C7	= DRACHEN	89A0C5EEA69B2726	= BANANEN	14	DrachenBananen
8	Foxtrott	389F986FAF0AEE6A	= U1P2T3O	9DC2EEC4A362A4AF	= 4Y5O6U7	14	u1p2t3o4y5o6u7
9	Golf	----- <Nur NTLM> -----				>14	Sommerschlussverkauf
10	Hotel	FDEA7F704330DE9	= MVEMJSU	515A8B184C8FDF2CE	= NP	9	MVemjSunP
11	India	564E78FA3238C9E6	= MV19EMJ	D3C0535EA8D23E26	= SU88NP	13	MV19emjSu88nP

Und die 3 nicht gefundenen Passwörter?

Der User "-- Blackhat" hat LM Hashe, aber der zweite LM Hash ist leer. Das Passwort hat also 7 oder weniger Zeichen. Aber mit Zeichen, die nicht in der Rainbowtable enthalten sind (Sonderzeichen). Eine Brute-Force Attacke mit bis zu 7 Zeichen auf diesen Hash dauert mit John the Ripper nur wenige Sekunden.

Nr.	Username	Hashtype	LM/NTLM Hashe und Klartextpasswörter		#
1	-- BlackHat	NTLM	FAF8C1CB5754A7A29DB3F8C4DB5E2D16		
1	-- BlackHat	LM	D78561D3D0DCA0C6	AAD3B435B51404EE	<8
1	-- BlackHat	Klartext	my20\$	<leer>	5

Und die 3 nicht gefundenen Passwörter?

Die User "Delta" und "Golf" haben keine LM Hashe. Daraus folgt, dass die Passwörter mehr als 14 Zeichen haben müssen. Mit der Crackstation (<https://crackstation.net/>) findet man das Passwort **Sommerschlussverkauf** von Golf in unter 1 Sekunde. Lediglich das **1u2p3t4o5y6o7u8** hält länger stand.

Nr.	Username	Hashtype	LM/NTLM Hashe und Klartextpasswörter	#
6	Delta	NTLM	B4190891F770A964AD6753FC0823E98E	
6	Delta	LM	<leer>	>14
6	Delta	Klartext	1u2p3t4o5y6o7u8	15
9	Golf	NTLM	A5E4AE5873F070F3DCD87E9E5CEA51BD	
9	Golf	LM	<leer>	>14
9	Golf	Klartext	Sommerschlussverkauf	20

Das waren die Passwörter

Nr.	Username	Passwort	#	Crackbar?
1	-- BlackHat	smurfs	6	[x]
2	-- TOMO	my20\$	5	[x]
3	Alpha	BananenDrachen	14	[x]
4	Bravo	smurfs	6	[x]
5	Charlie	moppel77	8	[x]
6	Delta	1u2p3t4o5y6o7u8	15	[-]
7	Echo	DrachenBananen	14	[x]
8	Foxtrott	u1p2t3o4y5o6u7	14	[x]
9	Golf	Sommerschlussverkauf	20	[x]
10	Hotel	MVemjSunP	9	[x]
11	India	MV19emjSu88nP	13	[x]

Warum war das so einfach?

Welche Schutzmaßnahmen eignen sich gegen solche Angriffe?

Anmerkungen oder Fragen?

Anhang

BIN		x0000	x0001	x0010	x0011	x0100	x0101	x0110	x0111	x1000	x1001	x1010	x1011	x1100	x1101	x1110	x1111
	HEX	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
000x	0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
001x	1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
010x	2x	SP	!	"	#	\$	%	&	'	()	*	+	,	-	.	/
011x	3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
100x	4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
101x	5x	P	Q	R	S	T	U	V	W	X	Y	Z	[\]	^	_
110x	6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
111x	7x	p	q	r	s	t	u	v	w	x	y	z	{		}	~	DEL