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

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	[ ]

Windows Passwörter mit Ophcrack ermitteln

Normaler Boot von Windows XP …

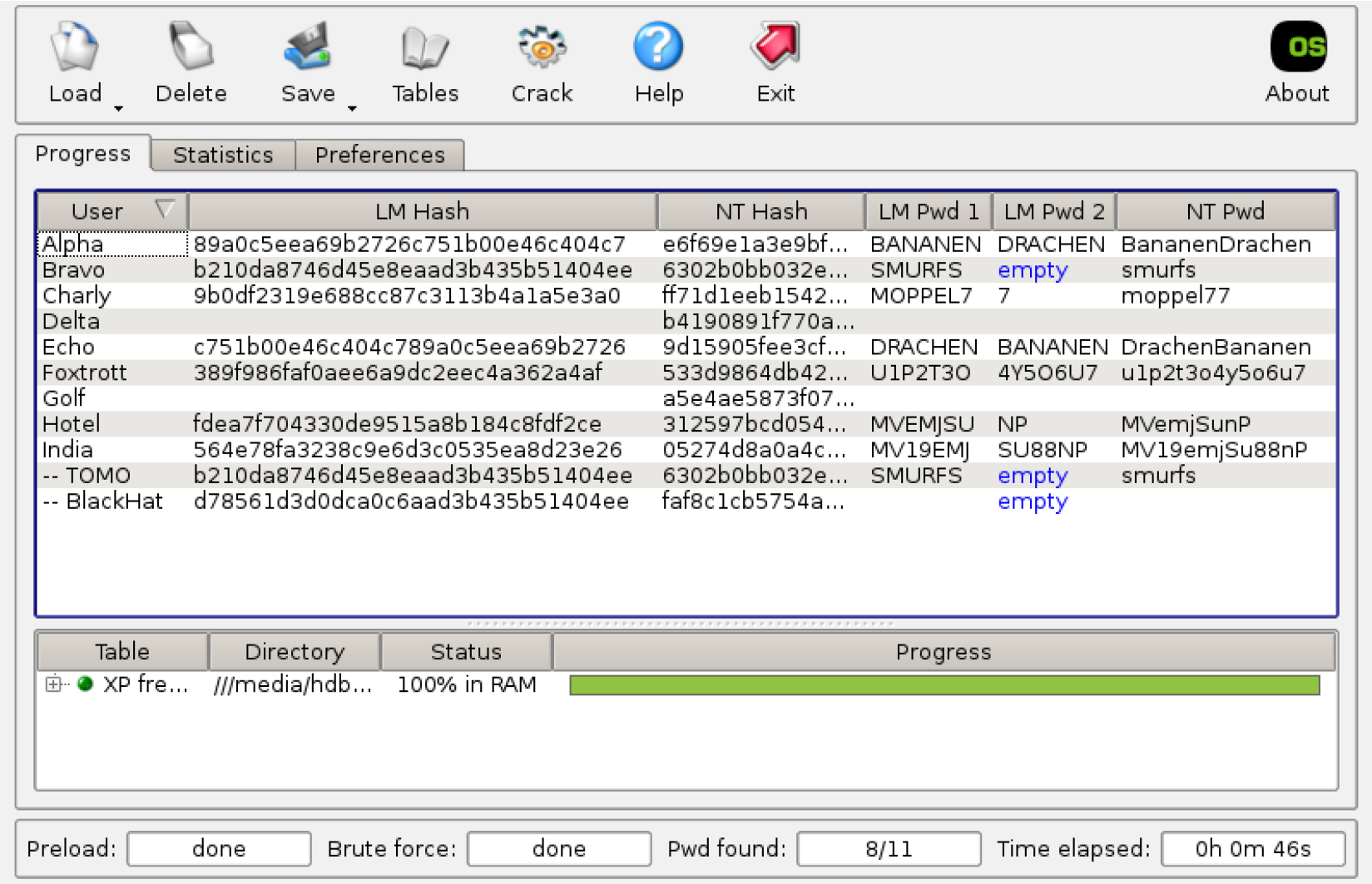
Windows Passwörter mit Ophcrack ermitteln

Windows Passwörter mit Ophcrack ermitteln

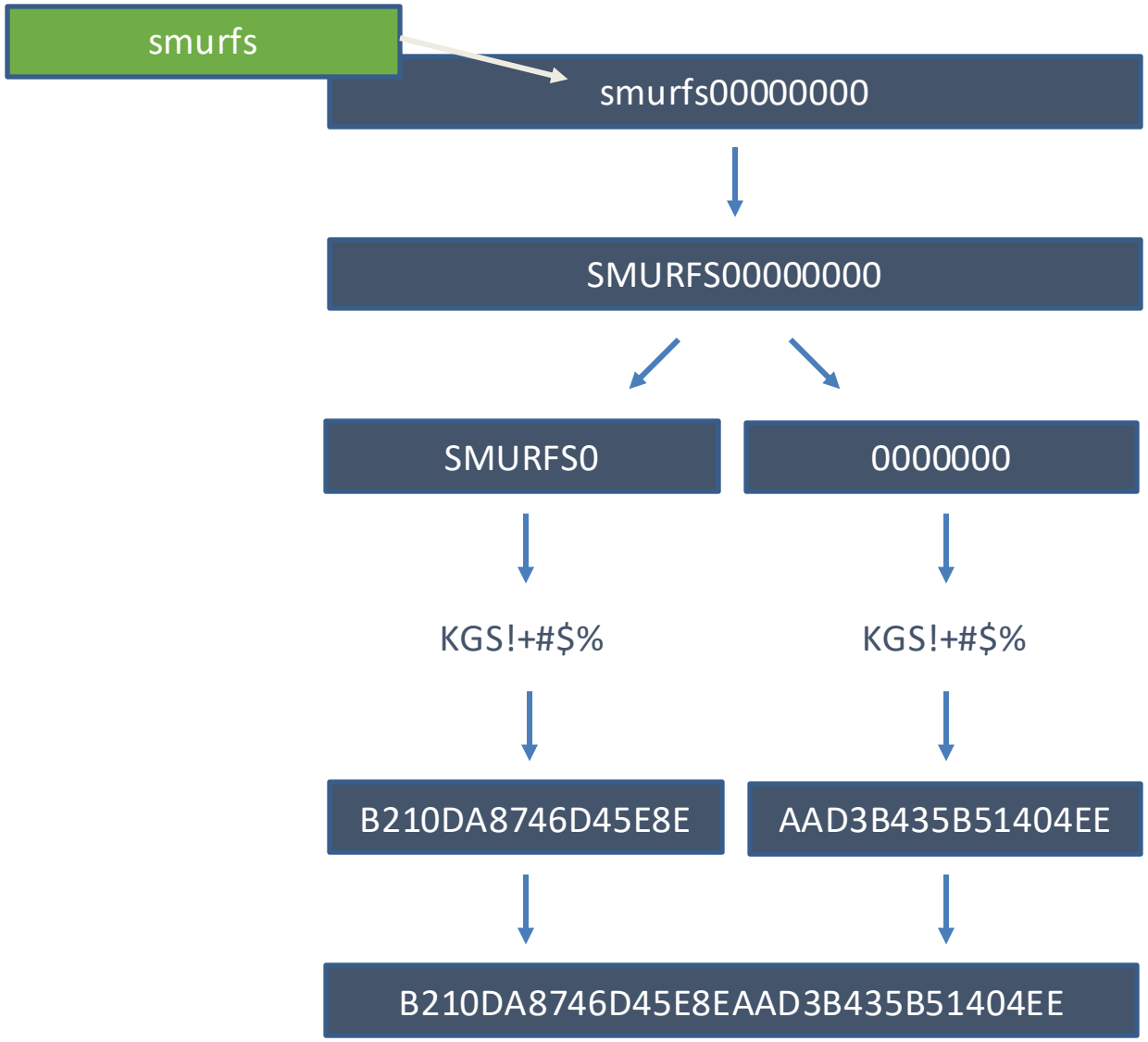
Booten mit Ophcrack …

Windows Passwörter mit Ophcrack ermitteln

Lokale Windows Passwörter

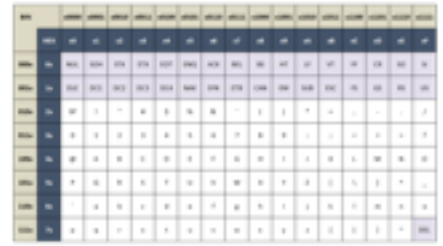


Wie funktioniert LM?



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).



Aufteilung in 2 x 7 Zeichen/Stellen.

Verschlüsselung des Strings KGS!+#$% mit DES und dem zuvor erstelltem 7-stelligem Passwort als Schlüssel.

Zusammenführen der beiden Hashe.

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