	Types (-m)	<b>1731</b> 200	MSSQL (2012, 2014) MySQL323	Attack Modes
**RAW 900	HASH** MD4	300	MySQL4.1/MySQL5	-a 0 Straight -a 1 Combinati
0	MD5	3100 112	Oracle H: Type (Oracle 7+) Oracle S: Type (Oracle 11+)	-a 3 Brute-Ford
5100 100	Half MD5 SHA1	12300	Oracle T: Type (Oracle 12+)	-a 6 Hybrid Wo
1300	SHA-224	8000 *** uTT	Sybase ASE P, SMTP, LDAP, FTP ***	-a 7 Hybrid Ma
1400	SHA-256	141	Episerver 6.x < .NET 4	Chamatar Sate (Da
10800 1700	SHA-384 SHA-512	1441 1 <b>600</b>	Episerver 6.x >= .NET 4	Character Sets (De ?l Abcdefghi
5000	SHA-3 (Keccak)	12600	Apache \$apr1\$ MD5, md5apr1, MD5 ( ColdFusion 10+	?u ABCDEFGH
600 10100	BLAKE2b-512 SipHash	1421	hMailServer	?d 01234567
6000	RIPEMD-160	101 111	nsldap, SHA-1(Base64), Netscape LDAP SHA nsldaps, SSHA-1(Base64), Netscape LDAP SSHA	?h 01234567
6100 6900	Whirlpool GOST R 34.11-94	1411	SSHA-256(Base64), LDAP {SSHA256}	?H 012345678 ?s !"#\$%&'()*
11700	GOST R 34.11-2012 (Streebog) 256-bit	1711	SSHA-512(Base64), LDAP {SSHA512} CRAM-MD5 Dovecot	?a     #3/08 ()
11800	GOST R 34.11-2012 (Streebog) 512-bit V HASH + SALT / ITERATION *****	15000	FileZilla Server >= 0.9.55	?b 0x00 - 0xff
10	md5(\$pass.\$salt)	*** CHE	CRSUM ***	
20	md5(\$salt.\$pass)		RATING SYSTEMS ***	Device Types (-D)
30 40	md5(utf16le(\$pass).\$salt) md5(\$salt.utf16le(\$pass))	3000 1000	LM NTLM	-D 1 CPU -D1 GPU
3800	md5(\$salt.\$pass.\$salt)	1100	Domain Cached Credentials (DCC), MS Cache	-D3 FPGA, DSP
3710 4010	md5(\$salt.md5(\$pass)) md5(\$salt.md5(\$salt.\$pass))	2100	Domain Cached Credentials 2 (DCC2), MS Cache 2	
4110	md5(\$salt.md5(\$pass.\$salt))	15300 15900	DPAPI masterkey file v1 DPAPI masterkey file v2	Options
2600 3910	md5(md5(\$pass)) md5(md5(\$pass).md5(\$salt))	12800	MS-AzureSync PBKDF2-HMAC-SHA256	-m
4300	md5(strtoupper(md5(\$pass)))	1500 12400	descrypt, DES (Unix), Traditional DES BSDi Crypt, Extended DES	-a
4400	md5(sha1(\$pass))	500	md5crypt, MD5 (Unix), Cisco-IOS \$1\$ (MD5)	-r [f
110 120	sha1(\$pass.\$salt) sha1(\$salt.\$pass)	3200	bcrypt \$2*\$, Blowfish (Unix)	sta
130	sha1(utf16le(\$pass).\$salt)	7400 1800	sha256crypt \$5\$, SHA256 (Unix) ha512crypt \$6\$, SHA512 (Unix)	
140 4500	sha1(\$salt.utf16le(\$pass)) sha1(sha1(\$pass))	122	macOS v10.4, MacOS v10.5, MacOS v10.6	runtime
4520	sha1(\$salt.sha1(\$pass))	1722 <b>7100</b>	macOS v10.7 macOS v10.8+ (PBKDF2-SHA512)	-session [te
4700 4900	sha1(md5(\$pass))	6300	AIX {smd5}	resto -o [filenan
14400	sha1(\$salt.\$pass.\$salt) sha1(CX)	6700	AIX {ssha1} AIX {ssha256}	usernar
1410	sha256(\$pass.\$salt)	6400 6500	AIX {ssha256} AIX {ssha512}	potfile-disal
1420 1430	sha256(\$salt.\$pass) sha256(utf16le(\$pass).\$salt)	2400	Cisco-PIX MD5	-d
1440	sha256(\$salt.utf16le(\$pass))	2410 500	Cisco-ASA MD5 Cisco-IOS \$1\$ (MD5)	-D
1710 1720	sha512(\$pass.\$salt) sha512(\$salt.\$pass)	5700	Cisco-IOS type 4 (SHA256)	
1730	sha512(utf16le(\$pass).\$salt)	9200 <b>9300</b>	Cisco-IOS \$8\$ (PBKDF2-SHA256) Cisco-IOS \$9\$ (scrypt)	
1740	sha512(\$salt.utf16le(\$pass)) N HASH, AUTHENTICATED ***	22	Juniper NetScreen/SSG (ScreenOS)	increment-min
50	HMAC-MD5 (key = \$pass)	501 15100	Juniper IVE Juniper/NetBSD sha1crypt	increment-max
60	HMAC-MD5 (key = \$salt)	7000	FortiGate (FortiOS)	
150 160	HMAC-SHA1 (key = \$pass) HMAC-SHA1 (key = \$salt)	5800	Samsung Android Password/PIN	hashcat-utils
1450	HMAC-SHA256 (key = \$pass)	13800 8100	Windows Phone 8+ PIN/password Citrix NetScaler	Cap2hccapx (.pcap
1460 1750	HMAC-SHA256 (key = \$salt) HMAC-SHA512 (key = \$pass)	8500	RACF	./cap2hccapx.bi
1760	HMAC-SHA512 (key = \$salt)	7200 9900	GRUB 2 Radmin2	./ct3_to_ntlm.b
*** RAV	W CIPHER, KNOWN ATTACK ***  DES (PT = \$salt, key = \$pass)	125	ArubaOS	deskey_2_ntlm (D
14100	3DES (PT = \$salt, key = \$pass)	7700	ERPRISE APPLICATION SOFTWARE *** SAP CODVN B (BCODE)	./deskey_to_ntl
14900 15400	Skip32 (PT = \$salt, key = \$pass) ChaCha20	7800	SAP CODVN F/G (PASSCODE)	keyspace (calculat
*** GEI	NERIC KDF***	10300 8600	SAP CODVN H (PWDSALTEDHASH) iSSHA-1 Lotus Notes/Domino 5	./keyspace.bin [
400 8900	phpass scrypt	8700	Lotus Notes/Domino 6	Variance Substituti
	PBKDF2-HMAC-MD5	9100 133	Lotus Notes/Domino 8 PeopleSoft	Keyspace Exhausti 20 x ?a 2.2 T Sol
	PBKDF2-HMAC-SHA1 PBKDF2-HMAC-SHA256	13500	PeopleSoft PS_TOKEN	10 x ?a 8,290 ye
	PBKDF2-HMAC-SHA512	*** ARC 11600	CHIVES ***	7 x ?a 3.4 days
	TWORK PROTOCOLS ***	12500	RAR3-hp	5 x ?a 38 secor
23 <b>2500</b>	Skype WPA/WPA2	13000	*	10 x ?l 7 days
2501	WPA/WPA2 PMK		AxCrypt AxCrypt in-memory SHA1	- 0:
4800 5300	iSCSI CHAP authentication, MD5(CHAP		14/1m71m	/ x ?l 35 secor
	IKE-PSK MDS			
5400	IKE-PSK MD5 IKE-PSK SHA1		KUP ***	5 x ?l 51 millis
5500	IKE-PSK MIDS IKE-PSK SHA1 NetNTLMv1	14700 14800	:KUP *** iTunes backup < 10.0 iTunes backup >= 10.0	5 x ?l 51 millise *A solar orbit or "Cos
5500 5500 5600	IKE-PSK SHA1	14700 14800 *** FUL	<u>:KUP ***</u> iTunes backup < 10.0 iTunes backup >= 10.0 L DISK ENCRYPTION ***	5 x ?l 51 millison  *A solar orbit or "Cosone time and takes appropriate the character password with the state of the character password with
5500 5500 5600	IRE-PSK WIDS IKE-PSK SHA1 NetNTLMv1 NetNTLMv1+ESS NetNTLMv2 IRM12 RAKD HMAC-SHA1	14700 14800 *** FUL 62XY	KUP *** iTunes backup < 10.0 iTunes backup>= 10.0 L DISK ENCRYPTION *** TrueCrypt	*A solar orbit or "Cos one time and takes a character password v second will take appr
5500 5500 5600	IKE-PSK SHA1 NetNTLMv1 NetNTLMv1+ESS NetNTLMv2	14700 14800 *** FUL 62XY 8800 12900	KUP ***  Titunes backup < 10.0  iTunes backup >= 10.0  L DISK ENCRYPTION ***  TrueCrypt  Android FDE <= 4.3  Android FDE (Samsung DEK)	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/22900000000
5500 5500 5600 7300 7500 8300 10200	IRE-PSK MUSI IRE-PSK SHA1 NetNTLMv1-ESS NetNTLMv2-ESS NetNTLMv2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5	14700 14800 *** FUL 62XY	KUP ***  Titunes backup < 10.0  iTunes backup >= 10.0  L DISK ENCRYPTION ***  TrueCrypt  Android FDE <= 4.3  Android FDE (Samsung DEK)	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/22900000000
5500 5500 5600 7300 7500 8300 10200 11100	IRE-PSK MUDS IRE-PSK SHAT NetNTLMv1- NetNTLMv1-ESS NetNTLMv2- IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5)	14700 14800 *** FUL 62XY 8800 12900 12200 137XY 14600	KUP ***  'ITunes backup < 10.0  'ITunes backup >= 10.0  LDISK ENCRYPTION **  TrueCrybt  Android FDE (< 4.3  Android FDE (Samsung DEK)  eCryptfs  VeraCrypt  LUKS	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/22900000000
5500 5500 5600 7300 7500 8300 10200 11100 11200 11400	IRE-PS MUDS IRE-PSK SHA1 NetNTLMV1 NETNTLMV1 NETNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (MD5) SIP digest authentication (MD5)	14700 14800 *** FUL 62XY 8800 12900 12200 137XY 14600	IXUP ***  ITunes backup < 10.0  ITunes backup >= 10.0  LDISK ENCRYPTION ***  TrueCrypt  Android FDE <= 4.3  Android FDE (Samsung DEK)  €Cryptfs  VeraCrypt  LUKS  LUMENTS ***	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/22900000000
5500 5500 5600 7300 7500 8300 10200 11100 11200 11400 13100	IRE-PSK MUDS IRE-PSK SHA1 NetNTLMv1 NetNTLMv1+ESS NetNTLMv2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23	14700 14800 *** FUL 62XY 8800 12900 12200 137XY 14600 *** DOI 9700 9710	XUP ***   Titunes backup < 10.0   iTunes backup >= 10.0   LDISK ENCRYPTION ***   TrueCrypt   Android FDE <= 4.3   Android FDE (Samsung DEK)   eCryptfs   VeraCrypt   Usik   CUMENTS ***   MS Office <= 2003 \$0/\$1, MD5 + RC4   MS Office <= 2003 \$0/\$1, MD5 + RC4   MS Office <= 2003 \$0/\$1, MD5 + RC4, collider #1	5 x ?I 51 millisr  *A solar orbit or "Cos one time and takes ap character password w second will take app 95^20/22900000000 USE WORDLISTS/C
5500 5500 5600 7300 7500 8300 10200 11100 11400 13100 16100	IRE-PSK MUDS IRE-PSK SHAT NENTILMV1 NENTILMV1-ESS NEUTILMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSDN Web Token)	14700 14800 *** FUL 62XY 8800 12900 12200 137XY 14600 *** DOI 9700 9710 9720	XUP ***   Titunes backup < 10.0   Titunes backup >= 10.0   LDISK ENCRYPTION ***   TrueCrybt	5 x ?l 51 millis:  *A solar orbit or "Cos one time and takes aj character password v second will take app 95^20/2290000000 USE WORDLISTS/L
5500 5500 5600 7300 7500 8300 10200 11100 11200 13100 16100 16500 *** FOI	IRE-PSK MUDS IRE-PSK SHAT NetNTLMv1- NetNTLMv1-ESS NetNTLMv2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS****	14700 14800 *** FUL 62XY 8800 12900 12200 137XY *** DOI 9700 9710 9720 9800 9810	XUP ***    Tiunes backup < 10.0    Tiunes backup > = 10.0    LDISK ENCRYPTION ***    TrueCrypt    Android FDE <= 4.3   Android FDE (Samsung DEK)   Ccryptfs   VeraCrypt    UKS    UMENTS ***   MS Offlice <= 2003 \$0/\$1, MD5 + RC4   MS Offlice <= 2003 \$0/\$1, MD5 + RC4, collider #1   MS Offlice <= 2003 \$0/\$1, MD5 + RC4, collider #2   MS Offlice <= 2003 \$3/\$4, SHA1 + RC4   MS Offlice <= 2003 \$3/\$4, SHA1 + RC4, collider #1	*A solar orbit or "Cos one time and takes at character password w second will take appr 95^20/22900000000 USE WORDLISTS/E
5500 5500 5600 7300 7500 8300 10200 11100 11400 13100 16100	IRE-PSK MUDS IRE-PSK SHAT NetNTLMv1- NetNTLMv1-ESS NetNTLMv2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS****	14700 14800 *** FUL 62XY 8800 12900 12200 137XY 14600 *** DOI 9700 9710 9810 9820	XUP ***	*A solar orbit or "Cos one time and takes ay character password w second will take appr 95*20/22900000000 USE WORDLISTS/E
5500 5500 7300 7300 7500 8300 10200 11100 11400 13100 16500 *** FOI 121 400 2611	IRE-PSK MUDS IRE-PSK SHA1  NetNTLMv1  NetNTLMv1+ESS  NetNTLMv2  IPMI2 RAKP HMAC-SHA1  Kerberos 5 AS-REQ Pre-Auth etype 23  DNSSEC (NSEC3)  CRAM-MD5  PostgreSQL CRAM (MD5)  MySQL CRAM (SHA1)  SIP digest authentication (MD5)  Kerberos 5 TGS-REP etype 23  TACACS+  JWT (ISON Web Token)  RUMS ***  SMF (Simple Machines Forum) > v1.1  phpBB3 (MD5)  vBulletin < v3.8.5  vBulletin < v3.8.5	14700 14800 *** FUL 62XY 8800 12900 12900 137XY 14600 *** DOI 9700 9710 9720 9800 9810 9820 9400 9500	XUP ***    Times backup < 10.0   Times backup >= 10.0   LDISK ENCRYPTION ***    TrueCrybt	*A solar orbit or "Cos one time and takes ay character password w second will take appr 95*20/22900000000 USE WORDLISTS/E
5500 5500 5600 7300 7500 8300 10200 11100 11400 13100 16100 16500 *** FOI 121 400	IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTLMV1 NetNTLMV1-ESS NetNTLMV2 IPM12 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (ISON Web Token) RUMS SMF (Simple Machines Forum) > v1.1 phpB83 (MD5) WBulletin < v3.8.5 WBulletin < v3.8.5 VBulletin < v3.8.5	14700 14800 *** FUL 62XY 8800 12900 12200 137XY 14600 *** DOI 9700 9710 9720 9800 9810 9820 9400 9500 9600	XUP ***	*A solar orbit or "Cos one time and takes at character password w second will take appr 95^20/2290000000 USE WORDLISTS/C
5500 5500 5600 7300 7500 8300 10200 11100 11400 13100 16500 *** FOI 121 400 2611 2711 2811	IRE-PSN MUSI IRE-PSK SHA1 NetNTLMV1 NetNTLMV1 NETNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (ISON Web Token) RUMS*** SWH (Simple Machines Forum) > v1.1 phpB83 (MD5) Willetin < v3.8.5 WyB8 1.2+ IPB24 (Invision Power Board)	14700 14800 *** FUL 62XY 8800 12900 137XY 14600 *** DOI 9700 9710 9720 9800 9810 9820 9400 9500 9600 10400	XUP ***    Times backup < 10.0   Times backup >= 10.0   LDISK ENCRYPTION ***    TrueCrybt	*A solar orbit or "Cos one time and takes at character password w second will take appr 95^20/2290000000 USE WORDLISTS/C
5500 5500 7300 7300 7500 8300 11200 11400 13100 16100 *** FO! 121 400 2611 2711 2811 2811 8400	IRE-PSN MUSI IRE-PSK SHAT  NetNTIMV1  NetNTIMV1  NENTIMV1-ESS  NetNTIMV2  IPMI2 RAKP HMAC-SHA1  Kerberos 5 AS-REQ Pre-Auth etype 23  DNSSEC (NSEC3)  CRAM-MD5  PostgreSQL CRAM (SHAT)  SP digest authentication (MD5)  Kerberos 5 TGS-REP etype 23  TACACS+  JWT (JSON Web Token)  RUMS***  JWT (JSON Web Token)  RUMS***  SWF (Simple Machines Forum) > v1.1  phpBB3 (MD5)  vBulletin > v3.8.5  WyBB 1.2+  IPB24 (Invision Power Board)  WBB3 (Woltlab Burning Board)  WBB3 (Woltlab Burning Board)	14700 14800 *** FUL 62XY 8800 12900 12900 137XY 14600 *** DOI 9710 9710 9810 9820 9810 9820 9400 9500 10400 10410 10420	XUP ***	*A solar orbit or "Cosone time and takes ap character password v second will take app 95*20/2290000000  USE WORDLISTS/E  hashcat [O]  hashcat -b -m 96  Benchmark MD4  hashcat -m 1310  Create a hashcat
5500 5500 7500 7300 7500 8300 10200 11100 11200 13100 16100 16500 *** FOI 121 400 2611 2711 2811 8400 *** COI	IRE-PSK MUDS IRE-PSK SHAT NetNTLMV1 NetNTLMV1 NENTLMV1-ESS NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** SWF (Simple Machines Forum) > v1.1 phpB83 (MD5) vBulletin < v3.8.5 WyB81.2+ IPB2+ (Invision Power Board) WBB3 (Woltlab Burning Board) WBB3 (Woltlab Burning Board) NTENT MANAGEMENT SYSTEMS *** Joomla < 2.5.18	14700 14800 **** FUL 62XY 8800 12900 12200 137XY 14600 **** DOI 9710 9710 9810 9820 9820 98400 9500 9600 10410 10420 10420 10500	XUP ***     Titunes backup < 10.0     Titunes backup > 10.0     LDISK ENCRYPTION ***     TrueCrypt	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/2290000000 USE WORDLISTS/II  hashcat -b -m 99 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 0 -a
5500 5500 7500 7300 7500 8300 11100 11200 11400 16100 16500 2611 2711 2811 2811 8400 *** CO 11	IRE-PSK MUDS IRE-PSK SHAT NetNTLMV1 NetNTLMV1-ESS NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** SWF (Simple Machines Forum) > v1.1 phpB83 (MD5) vBulletin < v3.8.5 WJB8 1.2+ IPB2+ (Invision Power Board) WB83 (Woltlab Burning Board) WTENT MANAGEMENT SYSTEMS *** Joomla < 2.5.18 Joomla > 2.5.18 JOOMLE SEC. SHED SHED SHED SHED SHED SHED SHED SHED	14700 14800 14800 14800 14800 12900 12900 137XY 14600 9710 9720 9820 9810 9820 9400 10410 10420 10500 10600 10700	XUP ***     Titunes backup < 10.0     Titunes backup > 10.0     LDISK ENCRYPTION ***     TrueCrypt	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/2290000000 USE WORDLISTS/II  hashcat -b -m 99 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 0 -a
5500 5500 7300 7300 7300 7500 8300 10200 111000 11200 11400 16100 16500 *** FOI 211 2011 2711 2811 2811 8400 *** COI 11 400 400 400 400	IRE-PSK MUDS IRE-PSK MUDS IRE-PSK SHAT NetNTLMV1 NetNTLMV1-ESS NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSDN Web Token) RUMS*** SWH (Simple Machines Forum) > v1.1 phpB83 (MD5) vBulletin < v3.8.5 WJB8 1.2+ IPB24 (Invision Power Board) WBB3 (Woltlab Burning Board) WTENT MANAGEMENT SYSTEMS*** Joomla < 2.5.18 Joomla > 2.5.18 Joomla SWOrders (MD5) PHPS	14700 14800 14800 12900 12900 12900 137XY 14600 9710 9720 9810 9820 9840 99500 9600 10400 10410 10420 10500 10600 10500 16200	XUP ***   Times backup < 10.0   iTunes backup < 10.0   iTunes backup < 10.0   LDISK ENCRYPTION **   TrueCrybt   Android FDE (< 4.3   Android FDE (< 5.4)   Android FDE (Samsung DEK)   Cryptfs   VeraCrypt   LUKS   ZUMENTS ***   MS Office < 2003 \$0/\$1, MD5 + RC4   MS Office < 2003 \$0/\$1, MD5 + RC4, collider #1   MS Office < 2003 \$0/\$1, MD5 + RC4, collider #1   MS Office < 2003 \$3/\$4, SHA1 + RC4   MS Office < 2003 \$3/\$4, SHA1 + RC4   MS Office < 2003 \$3/\$4, SHA1 + RC4, collider #2   MS Office 2003 \$3, SHA1 + RC4, collider #2   MS Office 2003 \$3, SHA1 + RC4, collider #2   MS Office 2003 \$3, SHA1 + RC4, collider #2   MS Office 2010   MS Office 2010	*A solar orbit or "Cos one time and takes ay character password v second will take appr 95*20/2290000000 USE WORDLISTS/E  hashcat [O] hashcat -b -m 90 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 0 -a: Crack MD5 hash
5500 5500 7500 7300 7300 7300 10200 11100 11100 11100 16100 16500 *** FOI 121 400 2611 2811 2811 2811 2811 2811 400 *** COI 11 400 400 400 2612 7900	IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTIMV1 NetNTIMV1-ESS NetNTIMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** SMF (Simple Machines Forum) > v1.1 phpB83 (MD5) v8Bulletin < v3.8.5 v8Bulletin > v3.8.5 v8Bulletin     v3.8.5 v8Bulletin     v3.8.5 v8Bul	14700 14800 14800 14800 14800 12900 12200 12200 137XY 9700 9710 9720 9800 10400 10410 10420 10500 10700 16200 16200 16200 9000	XUP ***	*A solar orbit or "Cosone time and takes ap character password v second will take app 95*20/2290000000  USE WORDLISTS/E  hashcat -b -m 99  Benchmark MD4  hashcat -m 1310  Create a hashcat  hashcat -m 0 -a Crack MD5 hash
5500 5500 7500 7300 7300 7300 10200 11100 11100 11100 16100 16500 *** FOI 121 400 2611 2811 2811 2811 2811 2811 400 *** COI 11 400 400 400 2612 7900	IRE-PS MUDS IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTLMV1 NetNTLMV1-ESS NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (ISON Web Token) RUMS*** SMF (Simple Machines Forum) > v1.1 phpB83 (MD5) WBB3 (MD5) WBB3 (WD15) FB2+ (Invision Power Board) WBB3 (Woltlab Burning Board) PSEC (MD5) PMPS Joomla < 2.5.18 Joomla > 2.5.18 (MD5) WordPress (MD5) PHPS MMERCE, FRAMEWORKS ***	14700 14800 14800 14800 12900 12200 12200 137xy 9700 9700 9720 9800 10400 10410 10420 10500 10600 10600 10600 10600 10600 10600 10600 10500 5200	XUP ***	*A solar orbit or "Cos one time and takes ay character password w second will take appr 95°20/22900000000 USE WORDLISTS/C  hashcat [O] hashcat -b -m 90 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 0 -a is Crack MD5 hash hashcat -m 100 -Crack SHA1 by us
5500 5500 5500 7500 8300 10200 11100 11400 13100 16100 16500 *** FOI 121 400 2611 2811 2811 2811 400 *** COI 11 400 2612 7900 *** COI 21 21	IRE-PSK MUDS IRE-PSK MUDS IRE-PSK SHA1 NetNTIMV1 NetNTIMV1-ESS NetNTIMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS-4 JWT (ISON Web Token) RUMS *** SMF (Simple Machines Forum) > v1.1 phpB83 (MD5) WBB3 (WD15) WBB3 (WOItlab Burning Board) WBB3 (Woltlab Burning Board) WBB3 (Woltlab Burning Board) WBB3 (Woltlab Burning Board) MYBB 1.2- Joomla > 2.5.18 (MD5) WordPress (MD5) PHPS Drupal7 MMERCE, FRAMEWORKS *** acsCommerce xt:Commerce	14700 14800 14800 12900 12900 12900 12900 12900 9700 9700 9810 9800 9800 10400 10400 10500 10600 10600 10700 16200 5200 5600 6600	XUP ***	*A solar orbit or "Cos one time and takes ay character password v second will take appr 95°20/22900000000  USE WORDLISTS/E  hashcat -b -m 90 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 0 -a: Crack MD5 hash hashcat -m 100 Crack SHA1 by u hashcat -m 1360
5500 5500 5500 7500 8300 10200 11100 11400 13100 16100 16500 *** FOI 121 400 2611 2811 2811 2811 400 *** COI 11 400 2612 7900 *** COI 21 21	IRE-PSK MUDS IRE-PSK MUDS IRE-PSK SHA1 NetNTLMV1 NetNTLMV1-ESS NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** SWF (Simple Machines Forum) > v1.1 phpB83 (MD5) vBulletin < v3.8.5 VBulletin > v3.8.5 WyB8 1.2+ IPB2+ (Invision Power Board) WBB3 (Woltlab Burning Board) NTENT MANAGEMENT SYSTEMS *** Joomla < 2.5.18 Joomla > 2.5.18 Joomla > 2.5.18 Joomla > 2.5.18 MOPS Drupal7 Drupal7 Drupal7 SCOmmerce VECTOR STANNEY STANNEY STANNEY OSCOmmerce VECTOR STANNEY STANNEY PROSERVER STANNEY PROSERVER STANNEY SCOMMERCE, FRAMEWORKS *** OSCOMMERCE, FRAMEWORKS *** OSCOMMERCE, FRAMEWORKS *** OSCOMMERCE, FRAMEWORKS *** OSCOMMERCE, FRAMEWORKS *** OSCOMMERCE PrestaShop	14700 14800 14800 14800 14800 14800 14800 14900 12900 12900 9710 137XY 14600 9700 9700 9810 9820 9810 9820 10420 10420 10420 10420 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 10700 10500 1	XUP ***	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/2290000000 USE WORDLISTS/U hashcat -b -m 99 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 100 Crack SHA1 by u hashcat -m 1360 Crack WinZip hash
5500 5500 5500 5500 5600 7300 3800 10200 11200 11100 13100 16100 2611 2711 2811 400 2612 7900 2612 111000 124	IRE-PS MUDS IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTLMV1 NetNTLMV1-ESS NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos S AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos S TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** JWT (JSON Web Token) RUMS*** JWHOSP MUDS INFORMATION OF MUDS INFO	14700 14800 14800 14800 12900 12200 12200 12200 9700 9710 9710 97800 9810 9400 9500 10410 10420 10500 10700 16200 10700 16200 10700 5200 6600 6600 6600 11300	XUP ***	*A solar orbit or "Cos one time and takes a character password v second will take appr 95^20/2290000000 USE WORDLISTS/U hashcat -b -m 99 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 100 Crack SHA1 by u hashcat -m 1360 Crack WinZip hash
5500 5500 5500 5500 5500 5600 7300 7300 11200 11200 11400 15100 1500 1500 16100 16500 10200 11201 201 11000 121 11000 124 10000	IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTIMV1 NetNTIMV1-ESS NetNTIMV2 IPM12 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (ISON Web Token) RUMS SWE (Simple Machines Forum) > v1.1 phpBB3 (MD5) SWB (12-SWB) SWB (12-WB) SWB (12	14700 14800 14800 14800 14800 12900 12200 12200 9710 9700 9710 9800 9810 9800 9600 10400 10410 10420 10500 10700 10600 10700 6600 6600 6600 6600	XUP ***	*A solar orbit or "Cos one time and takes ay character password v second will take appr 95°20/22900000000  USE WORDLISTS/L  hashcat [O] hashcat -b -m 90 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 100 Crack SHA1 by u hashcat -m 1360 Crack WinZip ha: Crack WINZip ha: Crack WINZip ha: Crack PHPASs us
5500 5500 5500 5500 5600 7300 3300 10200 11200 13100 13100 16100 16100 16100 16500 16500 10201 10201 10201 10201 10201 10201 10201 10201 10201 103900 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000 15000	IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTIMV1 NetNTIMV1-ESS NetNTIMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** SMF (Simple Machines Forum) > v1.1 php883 (MD5) v8Bulletin >= v3.8.5 v8Bulletin     v3.8.5 v8Bulletin     v3.8.5 v8Bull	14700 14800 14800 14800 14800 14800 14800 14800 14800 12900 12000 13700 9700 9710 9700 9800 10410 10420 10500 16200 16200 16200 8200 12700 8200 12700 15200 15200 15200 15200 15200 15200 15200 15200 15200 15200 15200 15200	XUP ***	*A solar orbit or "Cosone time and takes ap character password v second will take appr 95°20/22900000000  USE WORDLISTS/E  hashcat -b -m 90 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 100 Crack SHA1 by u hashcat -m 1360 Crack WinZip has Crack PHPAss us hashcat -a 0 -m
5500 5500 5500 5500 5500 5500 5600 73000 11100 11100 11100 16000 1711 1711	IRE-PSK MUDS IRE-PSK SHA1 NetNTLMV1 NetNTLMV1 NetNTLMV1 NETNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (ISON Web Token) RUMS *** SMF (Simple Machines Forum) > v1.1 phpB83 (MD5) WBB3 (WOS) WBB1 2+ IPB2+ (Invision Power Board) WBB3 (Woldtab Burning Board) NYEBN (MOS) INTENT MANAGEMENT SYSTEMS *** Joomla > 2.5.18 (MD5) WordPress (MD5) PHPS Drupal7 MMERCE, FRAMEWORKS *** OSCOMMERCE xt:Commerce restashop Django (PBKDF2-SHA256) Tripcode MediaWiki B type OpenCart Redmine	14700 14800 ****FUL 14800 ****FUL 14800 ****FUL 14800 ****FUL 12900 12900 9700 9710 9720 9800 9500 9600 10410 10420 ****POL 16900 16200 ****POL 16900 16200 8200 12700 6600 12700 16200 16	XUP ***	*A solar orbit or "Cos one time and takes ay character password w second will take appr 95^20/22900000000 USE WORDLISTS/C  hashcat   D   hashcat - b - m 90 Benchmark MD4 hashcat - m 1310 Create a hashcat hashcat - m 100 - crack SHA1 by ushashcat - m 1360 Crack WinZip hashcat - a 0 - m 10 Crack MD5 hashcat - a 0
5500 5500 5500 5500 5600 7300 1300 10200 11200 11100 13100 16100 2611 2711 2811 400 2612 7900 2612 11000 121 11000 121 11000 15000 1	IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTIMV1 NetNTIMV1-ESS NetNTIMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** SMF (Simple Machines Forum) > v1.1 php883 (MD5) v8Bulletin >= v3.8.5 v8Bulletin     v3.8.5 v8Bulletin     v3.8.5 v8Bull	14700 14800 17900	XUP ***	7 x ?l 35 secon 5 x ?l 51 millis *A solar orbit or "Cos one time and takes aj character password w second will take appr 95^20/22900000000 USE WORDLISTS/C  hashcat -b -m 90 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 100 Crack SHA1 by u: hashcat -m 136 Crack WinZip has Crack WinZip has Crack MD5 hash crack PHPAss us hashcat -a 0 -m 1 Crack MD5 hash
5500 5500 5500 5500 5600 7300 7300 10200 11200 11200 11200 11400 16100 16500 ***F01 2811 2811 2811 2811 400 2612 271 11000 16000 124 10000 16000 16000 16000 164521 45221 2001	IRE-PS MUDS IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTLMV1 NetNTLMV1 NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (ISON Web Token) RUMS*** SWF (Simple Machines Forum) > v1.1 phpB83 (MD5) WBB3 (MD5) WBB3 (WOST) WBB3 (WOST) WBB3 (WOST) WBB3 (WOST) SWF (SIMPLE STEEMS*** JOOMIA 2 2.5.18 MMERCE, FRAMEWORKS*** oSCOmmerce vs.t.Commerce PrestaShop Django (PBKDF2-SHA256) Tripcode MediaWiki B type OpenCart Redmine PunB8 Atlassian (PBKDF2-HMAC-SHA1) TABASES SERVERS****	14700 14800 17900	XUP ***	*A solar orbit or "Cos one time and takes ay character password w second will take appr 95^20/22900000000 USE WORDLISTS/C  hashcat   D   hashcat - b - m 90 Benchmark MD4 hashcat - m 1310 Create a hashcat hashcat - m 100 - crack SHA1 by ushashcat - m 1360 Crack WinZip hashcat - a 0 - m 10 Crack MD5 hashcat - a 0
5500 5500 5500 5500 5500 5500 5600 7300 1300 11200 11100 16500 16500 121 400 2612 2711 12811 2811 2811 2811 2811 2811 2	IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTIMV1 NetNTIMV1-ESS NetNTIMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (JSON Web Token) RUMS*** SMF (Simple Machines Forum) > v1.1 php8B3 (MD5) v8B1 (Wolfath Swell Barber Systems JWB 1.2* IPB2+ (Invision Power Board) WBB3 (WOlfab Burning Board) NTENT MANAGEMENT SYSTEMS *** Joomla < 2.5.18 Joomla > 2.5.18 (MD5) WordPress (MD5) PHPS Drupal7 MMERCE, FRAMEWORKS *** OSCOmmerce xt.Commerce xt.Commerce ycrestaShop Django (SHA-1) Django (PBKDF2-SHA256) Tripcode MediaWiki B type OpenCart Redmine PunBB Atlassian (PBKDF2-HMAC-SHA1) TABASE SERVERS *** PostgreSQL	14700 14800 1780 1780 1780 1780 1780 1780 1780 1	XUP ***	*A solar orbit or "Cos one time and takes ay character password will take appr 95°20/22900000000 USE WORDLISTS/C  hashcat [O] hashcat -b -m 90 Benchmark MD4 hashcat -m 1310 Create a hashcat hashcat -m 100 Crack SHA1 by u: hashcat -m 1360 Crack WinZip ha: Crack PHPAss us hashcat -a 0 -m 1 Crack MD5 hash
5500 5500 5500 5500 5500 5500 5500 7300 73	IRE-PS MUDS IRE-PS MUDS IRE-PS MUDS IRE-PSK SHA1 NetNTLMV1 NetNTLMV1 NetNTLMV2 IPMI2 RAKP HMAC-SHA1 Kerberos 5 AS-REQ Pre-Auth etype 23 DNSSEC (NSEC3) CRAM-MD5 PostgreSQL CRAM (MD5) MySQL CRAM (SHA1) SIP digest authentication (MD5) Kerberos 5 TGS-REP etype 23 TACACS+ JWT (ISON Web Token) RUMS*** SWF (Simple Machines Forum) > v1.1 phpB83 (MD5) WBB3 (MD5) WBB3 (WOST) WBB3 (WOST) WBB3 (WOST) WBB3 (WOST) SWF (SIMPLE STEEMS*** JOOMIA 2 2.5.18 MMERCE, FRAMEWORKS*** oSCOmmerce vs.t.Commerce PrestaShop Django (PBKDF2-SHA256) Tripcode MediaWiki B type OpenCart Redmine PunB8 Atlassian (PBKDF2-HMAC-SHA1) TABASES SERVERS****	14700 14800 12900 13701 14900 14900 14900 14900 14900 14900 15900 15900 16900 15900 16900	XUP ***   Times backup < 10.0     ITunes backup > 10.0     LDISK PICKERYPTION ***   TrueCrybt	*A solar orbit or "Cosone time and takes a character password viscond will take appr 95^20/2290000000  USE WORDLISTS/II  hashcat -b -m 90 Benchmark MD2 hashcat -m 1310 Create a hashcat hashcat -m 0 -a Crack MD5 hash hashcat -m 136 Crack SHA1 by u hashcat -m 136 Crack WinZip ha Crack PHPAss us hashcat -a 0 -m Crack MD5 hash hashcat -a 3 -m Crack MD5 using

k Modes		
Straight	[hash] [dictionary]	
Combination	[hash] [dictionary] [dictionary]	
Brute-Force	[hash] [mask]	
Hybrid Wordlist + Mask	[hash] [dictionary] [mask]	
Hybrid Mask + Wordlist	[hash] [dictionary] [mask]	
cter Sets (Default) [?]		BLACK HILLS
Abcdefghijklmnopqrstuv	wxyz [26]	Information Security
ABCDEFGHIJKLMNOPQR:	STUVWXYZ [26]	CELEBRATING 10 YEARS
0123456789	[10]	•2008-2018•
0123456789abcdef	[16]	

[16]

[33]

[95]

## Hashcat 4.10 Cheat Sheet v.2018.1

@BHInfoSecurity @Krelkci

https://www.blackhillsinfosec.com

https://hashcat.net/hashcat/ https://github.com/hashcat/hashcat

### Common Dictionary Repos

CrackStation: https://crackstation. Lots of others: https://wiki.sk Custom: cewl -d3 -w wordlist.txt -v http://domain.tld

#### **Hash Sources to Hash Type**

Inveigh NetNTLMv1 Inveigh NetNTLMv2 Mimikatz/LSAdump 1000 esedbexport/secretsdump.py ntds.dit (LM) esdbexport/secretsdump.py ntds.dit (NTLM) 3000 airmon-ng (WPA/WPA2) 2500 2501

#### Common Hash Types MD4 90 MD5

NTLM 1000 NetNTI Mv1 5500 NetNTLMv2 mscache1 (xp, w2k3) 5600 1100 mscache2 (v, w7, w8, w10, w2k8+) 2100 LanManager SHA512 3000 Kerberos REQ 7500 13100 400 2500 Kerberos TGS-REP Wordpress WPA WPA PMK

## Lookup Hash Modes (Type) from Command Line

hashcat --help| grep -l [keyword] hashcat --help| grep -i salt hashcat --help| grep -i Network hashcat --help| grep -i raw hashcat --help| grep -i Office hashcat --help| grep -i Cisco hashcat --help| grep -i Forum hashcat --help| grep -i Domain hashcat --help| grep -i SHA256 hashcat --help| grep -i MD5

# Empty Hashes LanManager aad3b435b51404eeaad3b435b51404ee

NTLM 31d6cfe0d16ae931b73c59d7e0c089c0

Lookup Hash Examples from Command Line
hashcat –example-hashes -m [hash-mode#]
NTLM – hashcat –example-hashes -m 1000

#### -username Ignore username field in hashfile --potfile-disable

Ignore potfile and do not write -d [#] Specify an OpenCL Device -D [#] Specify an OpenCL Device type List OpenCL Devices & Types -0 Optimized Kernel, Passwords <32 char

Hash Type (mode) Attack Mode

Keep screen updated Benchmark

Abort after x seconds

Define output/potfile

Restore/Resume session

Set session name (resumeable)

Rules file

Version

Increment (brute force) -increment-min [#] Start increment at [#] of chars

Stop increment at [#[ of chars increment-max [#]

0123456789ABCDEE !"#\$%&'()\*+,-./:;<=>?@[\]^\_`{|}~

FPGA, DSP, Co-Proc

-m [#]

-a [#]

-r [file]

--status

--runtime [#]

-session [text]

-o [filename]

restore

Cap2hccapx (.pcap to WPA/WPA2)

/cap2hccapx.bin input.pcap output.hccapx [essid]

t3 to ntlm (mschap to ntlm)

./ct3\_to\_ntlm.bin 8-byte-ct3-in-hex 8-byte-salt-in-hex [24bESS]

eskey\_2\_ntlm (DES KPA to NTLM)

./deskey\_to\_ntlm.pl 8-byte-key-in-hex

eyspace (calculate keyspace with hashcat masks)

./keyspace.bin [options] mask

## Eyspace Exhaustion At 229 GH/s

0 x ?a 2.2 T Solar orbits around the center of the Milky way\*

10 x ?a 8,290 years 7 x ?a 3.4 days

5 x ?a 38 seconds 10 x ?l 7 days

7 x ?l 35 seconds

5 x ?l 51 milliseconds

A solar orbit or "Cosmic Year" is the Sun orbiting the center of the Milkyway ne time and takes approximately 225 million Earth years. Brute forcing a 20haracter password with a 95 character mask at 229,000,000,000 hashes per cond will take approximately 2.2 Trillion Cosmic Years.

5^20/22900000000/3600/24/365/255000000000~3.202.000.000.000 Years

JSE WORDLISTS/DICTIONARIES

## hashcat [options]... hash|hashfile|hccapxfile [dictionary|mask|directory]

hashcat -b -m 900

Benchmark MD4 hashes

## hashcat -m 13100 -a 0 --session crackin1 hashes.txt wordlist.txt -o output.pot

Create a hashcat session to hash Kerberos 5 tickets using wordlist.txt

## hashcat -m 0 -a 3 -i hashes.txt ?a?a?a?a?a?a?a -o output.txt

Crack MD5 hashes using all characters in 7 character passwords

## hashcat -m 100 -a 6 hashes.txt wordlist.txt ?a?a -o output.txt

Crack SHA1 by using wordlist with two ?a characters after

## hashcat -m 13600 -a 3 hashes.txt ?u?!?!?!?!?d?d?d?d! -o output.txt

Crack WinZip hash, mask for Eighth2018!, Summer2018!, Etcetc5050hashcat -a 0 -m 400 example400.hash example.dict Crack PHPAss using dictionary file example.dict

## hashcat -a 0 -m 0 example0.hash example.dict -r rules/best64.rule

Crack MD5 hashes using dictionary example.dict and modify with rules in best64.rule

## hashcat -a 3 -m 0 example0.hash ?a?a?a?a?a?a

Crack MD5 using brute force with 6 characters that match the ?a characterset (upper, lower, numbers, symbols)

## hashcat -a 1 -m 0 example0.hash example.dict example.dict

Crack MD5 using combinator function combining two dictionaries.