



Angriffe auf Authentifizierungs- Protokolle

mit Lösungen von:



14.10.2009

Vorstellung

8com GmbH & Co. KG

René Mathes



- *IT-Security-Consultant*
- *Penetrationstester*

Aufgaben



- *IT-Sicherheitsanalysen*
- *IT-Sicherheitsforschung*
- *IT-Forensik*
- *Malware Analysis*

14.10.2009

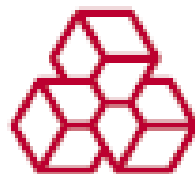
Inhalte



**Angriffe auf
Hashwerte**



- Windowsanmeldung
- Was ist Bruteforce
- Parallelisierung durch CUDA
- Vergleich Gestern / Heute



ELCOMSOFT
P R O A C T I V E S O F T W A R E

14.10.2009

Windows- Anmeldung

LM-Hashes

- Verwendet von LAN Manager und Windows bis Version ME
- Auch in neueren Windows-Versionen wird ein LM Hash gespeichert
- verwendet DES
- wegen Schwächen in der Implementierung leicht angreifbar
 - Maximale Passwortlänge: 14 Zeichen
 - Halbierung des Passworts in zwei Blöcke
 - Verwendet keinen „Salt“-Wert

NTLM-Hashes

- Verwendet ab Windows NT 4.0
- Bestehend aus NT-Hash und LM-Hash
- NT-Hash verwendet MD4
- Härter als LM-Hash alleine
- Keine Längenbeschränkung des Passworts

14.10.2009

Angriffe

Was ist Bruteforce?

- „Raten“ aller möglichen Passwörter
- Findet theoretisch immer das richtige Passwort
- Benötigte abhängig vom Passwort und dem verwendeten Algorithmus beliebig viel Zeit

Parallelisierung durch CUDA

- Zerlegung des Problems in kleine Teilprobleme, die parallel abgearbeitet werden können
- CUDA wurde entwickelt von Nvidia
 - Mittlerweile ähnliche Technologie von ATI
- Auslagerung von Rechenschritten auf den Grafikprozessor
- Massive Parallelisierung

14.10.2009

LIVE-Vorführung Hash-Dekodierung mit Elcomsoft

... LIVE

- Kennwort mit 4 Zeichen
- Kennwort mit 5 Zeichen
- Kennwort mit 6 Zeichen
- Kennwort mit 7 Zeichen

***Dauer eines Angriffs auf einen NTLM-Hash, vor ca 3 Jahren
circa 5,000,000 Versuche in der Sekunde***

Länge	alpha 26	Alpha 52	AlphaNum 62	AlphaNum+ 96	
5	Sek	Min	Min	Std	
6	Min	Std	Std	Tage	
7	Std	Woche	Wochen	Jahre	
8	Tage	Jahr	Jahre	JH	
9	Wochen	JH	JH	TJT	
10	Jahre	JT	TJT	Millionen	

Dauer eines Angriffs auf einen NTLM-Hash, Heute circa 5,000,000,000 Versuche in der Sekunde

Länge	alpha 26	Alpha 52	AlphaNum 62	AlphaNum+ 96	
5	ms	ms	Sek	Sek	
6	ms	Sek	Min	Min	
7	Sek	Min	Std	Tag	
8	Min	Std	Tag	Wochen	
9	Std	Wochen	Wochen	Jahre	
10	Tag	Jahre	Jahre	JT	

. . . weitere Informationen über:

- Kennwortwiederherstellung
 - PDF
 - Winzip
 - u.v.m.
 - Kennwortsicherheitsprüfungen
-

Halle 6

Stand 542



14.10.2009

8com GmbH & Co. KG

Im Ringel 29

67435 Neustadt an der Weinstraße

Telefon 06327 976428-0

Fax 06327 976428-99

info@8com.de

www.8com.de