

Hacking für Manager Handout



Sichere IT

WWW.SICHERE.IT

WWW.SICHERE.IT

Tobias Schrödel

Wichtiger Hinweis :

Einige der hier erläuterten Techniken sind geeignet, um Schutzmechanismen zu überwinden, die eigentlich eine unberechtigte Nutzung von Dienstleistungen oder Funktionen verhindern soll(t)en.

Der Autor weist ausdrücklich darauf hin, dass eine Umgehung dieser Mechanismen im echten Leben illegal sein kann.

Daher sind die vorgestellten Mechanismen oft nur angerissen und werden nicht im Detail erklärt.

Hacking für Manager Handout

Passwort geschützte Excel Sheets können mit entsprechenden Tools in O Sekunden geöffnet werden.

Reiseangaben		PKW-Kilometergeld		Sonstige Kosten													
Datum	Abfahrtsort	Ankunftszeit	km	EUR/km	Sa. EUR	Ein- EUR	Wen- EUR	Flug- EUR	Taxi- EUR	Hot- EUR	sonst. EUR	ggf. Abzug EUR	Neben- EUR	Kosten in EUR	sonstige Kosten in EUR	Summe	
22. Sep. 04	München	10:15	81	0,30	24,30			269,46	17,00							6,00	316,76 €
Rückfahrt: 22. Sep. 04 München 16:40 Uhr, 19:30 Uhr																	
Bemerkungen:																	
Mitarbeiter: Ich bestätige die Richtigkeit der Angaben: 27 Sep 2004																	
Führungskraft: Abrechnung geprüft und betriebliche Notwendigkeit der Reise bestätigt. Datum: 27 Sep 2004																	
Name in Druckschrift: Tobias Schrödel																	
Name in Druckschrift: Michaela Hötzl																	
Unterschrift: _____ oder <input type="checkbox"/> elektronisch anerkannt																	
Auszahlung: 316,76 €																	

Excel speichert einen Hash-Wert des Passworts ab.

Dieser ist nicht eindeutig, so dass ein anderes Passwort errechnet werden kann, welches den gleichen Hash-Wert ergibt und das Arbeitsblatt dann ebenfalls öffnet.

Erst ab Excel 2003 sind starke Verschlüsselungsmethoden vorhanden.

Diese sind aber aus Gründen der Abwärts-Kompatibilität meist nicht aktiviert.



Hacking für Manager Handout

Hersteller von Farblaser-Druckern bringen auf den
Ausdrucken hellgelbe, winzige Punkte an, die vom Nutzer
mit bloßem Auge kaum zu erkennen sind.

Diese Punkte sind in einer speziellen Anordnung platziert,
so dass sich durch Anlegen einer Matrix die Ausdruckszeit,
das Modell und die Seriennummer des Druckers ablesen lassen.
Registrierte Anwender (z.B. nach Reparatur) sind damit
rückverfolgbar.

Hersteller die Tracking Dots einsetzen sind unter anderem :

- Hewlett Packard
- Brother
- Canon
- Dell
- Epson
- Konica / Minolta
- OKI

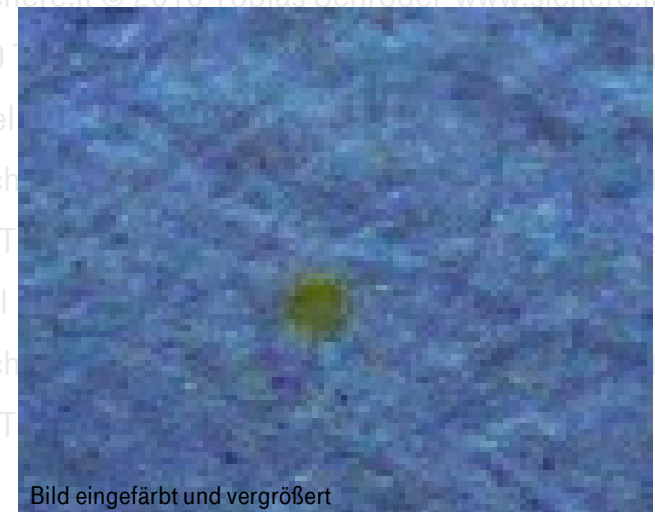


Bild eingefärbt und vergrößert

Hacking für Manager Handout

Mit Pringles Dosen kann man sehr gute WLAN Richtfunk-Antennen bauen.



Benötigte Bauteile:

- M5 Gewindestange
- Aluminiumrohr, Innendurchmesser so wählen, dass die Gewindestange noch gerade hindurch passt (8 mm Außendurchmesser passte bei uns)
- 5 Unterlegscheiben 30 mm, Innendurchmesser M5, Dicke 1 mm
- 2 M5 Muttern
- Pappscheibe, Durchmesser gleich Innendurchmesser der Pringles-Dose
- N-Flanschbuchse
- Kupferdraht, 5cm lang, 4mm²

Bauanleitung und Quelle:

http://www.ping.de/aktiv/wavelan/wavelan_antennenbau_yagi.html

Hacking für Manager Handout

Fehlerhafte Implementierungen erlauben fremden Personen den Zugriff auf Mobiltelefone oder Headsets per Bluetooth:

Beispiel : Nokia 6310i, SE T610

Bei einigen der o.g. Geräte kann ein Angreifer das Gerät bedienen und dabei u.a.:

- Anruferliste ausgeben
- Telefonbuch anzeigen
- Telefonbuch löschen
- Einen Anruf tätigen

Eingesetzte Tools sind *hcitool*, *carwhisperer* und *bluesnarfer* unter Linux.



Hacking für Manager Handout

Word Dokumente enthalten viele Hinweise (z.B. gelöschter Text, frühere Dateinamen), die mit einem beliebigen Freeware HEX Editor gelesen werden können.

Diese Metadaten sind notwendig für bestimmte Funktionen in Word, somit teilweise unvermeidbar.

Daher Angebote, Bewerbungen etc nur als PDF Dokument versenden.

In neuen Word-Versionen sind Funktionen zum Entfernen von Metadaten vorhanden.

Alte Versionen lassen sich mittels Plugin „nachrüsten“.

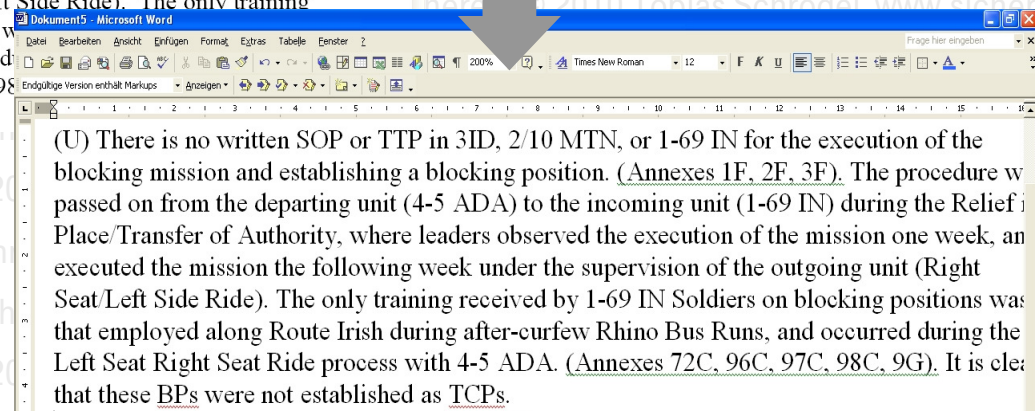
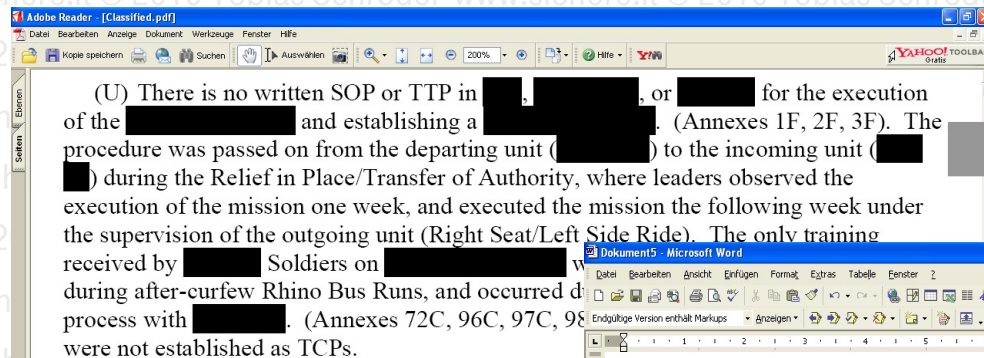
```
oem5C:\
Eigene D
ateien\B
ewerbung
\010728j
bh\Ansch
reiben.d
oc oem6
C:\Eigene
Dateie
n\Bewerb
ung\0107
28j\Ansch
reibe
n1.doc
oem6C:\E
igene Da
teien\Be
werbung\
010728j\
h\Anschre
iben1.d
oc oem6
C:\Eigene
Dateie
n\Bewerb
ung\0107
28j\Ansch
reibe
n1.doc
oem+C:\E
igene Da
teien\Be
werbung\
Anschrei
ben.doc
oem+C:\
Eigene D
ateien\B
ewerbung
\Anschre
```

```
iben.doc
oem=C:\
\Eigene
Dateien\
Bewerbun
g\010728
KnorrBre
mse\Ansch
reiben.
doc oem
=C:\Eige
ne Datei
en\Bewer
bung\010
728Knorr
Bremse\A
nschreib
en.doc
oem:C:\E
igene Da
teien\Be
werbung\
010728TS
ystems\A
nschreib
en.doc
oem:C:\E
igene Da
teien\Be
werbung\
010728TS
ystems\A
nschreib
en.doc y@e
```

Hacking für Manager Handout

Geschwärzte Textstellen in PDF Dokumenten können wiederhergestellt werden.

Voraussetzung dafür ist, dass das Dokument nicht als Grafik gedruckt wurde und dass die Berechtigung für das Kopieren von Textstellen in PDF vorhanden ist.



Hacking für Manager Handout

Passwort- länge	Benötigte Zeit für eine Brute-Force-Attacke (Ausprobieren aller möglichen Passwörter)	
	OHNE Sonderzeichen (O..9 und A..Z)	MIT Sonderzeichen (wie z.B. %\$?!-)
1	8.5 Mikrosekunden	11.75 Mikrosekunden
2	0.58 Millisekunden	1.10 Millisekunden
3	0.39 Sekunden	0.10 Sekunden
4	2.67 Sekunden	9.76 Sekunden
5	3.03 Minuten	15.29 Minuten
6	3.43 Stunden	23.95 Stunden
7	9.73 Tage	93.82 Tage
8	1.81 Jahre	24.14 Jahre
9	123.14 Jahre	2260 Jahre
10	8370 Jahre	213350 Jahre
11	569380 Jahre	10.05 Millionen Jahre
12	38.72 Millionen Jahre	1.89 Milliarden Jahre

Sichere IT

WWW.SICHERE.IT

WWW.SICHERE.IT

Hacking für Manager Handout

Gute Passwörter bestehen aus mindestens acht Zeichen und setzen sich aus Groß- und Kleinschreibung sowie Sonderzeichen und Ziffern zusammen.

Besser merken kann man sich das durch Sätze und die Ersetzung von Zeichen, die sich ähnlich sehen, wie z.B. 4 und A oder S und 5 bzw. ! und I.

FdhdGgg5wh!

Fuchs du hast die Gans
gestohlen gib sie wieder her!

TOb!a55chrO3)3l

TobiasSchroedel

Pf3!3rw3hr

Pfeierwehr

G3h3!m35Pa55wOrt

GeheimesPasswort

Sichere IT

WWW.SICHERE.IT

WWW.SICHERE.IT

Hacking für Manager Handout

Unauffällig unter dem Tisch und hinter dem Rechner platziert zeichnen
KeyKatcher zwischen 32.000 und 1.000.000 Tastendrucke auf.

Diese Aufzeichnungen enthalten also eMails, Briefe und andere Texte aber
natürlich auch Benutzerkennungen und Passwörter.

Ausgelesen werden die Geräte i.d.R. ohne zusätzliche Software an jedem
anderen beliebigen PC oder Laptop.

Sie sind für PS/2
und USB Tastaturen
erhältlich.

Kosten : ab 55 Euro



Hacking für Manager Handout

Gelöschte Daten sind mit z.T. kostenlosen Tools in Sekunden wiederherstellbar. Bei einem Test wurden bei eBay Ioo gebrauchte Festplatten gekauft.

Ergebnis: Nur 10% waren sicher gelöscht.

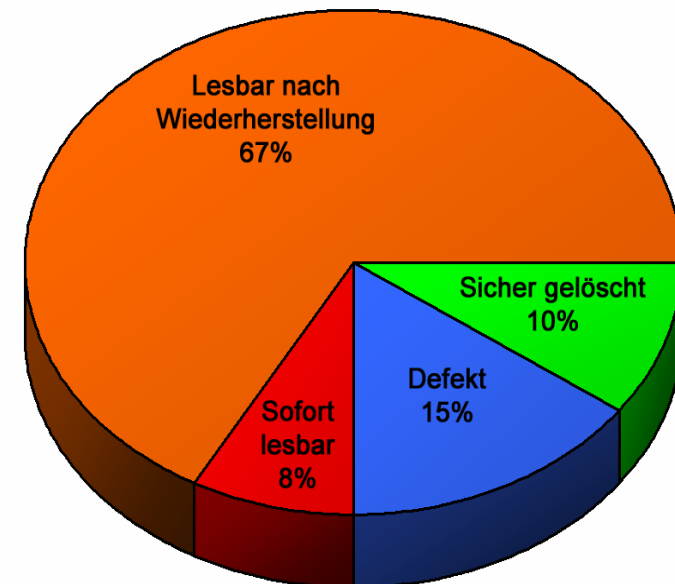
Alle anderen enthielten z.T. persönliche Daten.

Sicheres Löschen durch mehrfaches Überschreiben ist mit einfachen Tools machbar.
(z.B. Freewaretool Eraser).

Magnete machen modernen Platten übrigens nichts mehr aus.

Alternative: Bohrmaschine

75% der Festplatten waren lesbar



Hacking für Manager Handout

Kontakt:

Tobias Schrödel
IT Security & Awareness

Connollystraße 20/EG, 80809 München

schroedel@sichere.it

<http://www.sichere.it>

Fax: 089 / 35 70 97 80

Sichere IT

WWW.SICHERE.IT

WWW.SICHERE.IT

