Cracken lernen

In diesem Tutorial wird Ihnen Schritt für Schritt erklärt, wie Sie, ohne einen aus dem Internet gezogen Crack, Patch oder Serial, ein Programm zur Vollversion cracken können. Ihnen wird also das Cracken von Software beigebracht. Alle Informationen die hier zur Verfügung gestellt werden dienen der reinen Information. TutorialKing.de distanziert sich ausdrücklich vor illegalem gebrauch dieser Informationen und weißt darauf hin, dass man durch die nicht sachgemäße Anwendung Urheberrechte verletzt.

Benötigte Programme:

- ✓ Ein Programm, dass man cracken möchte (hier: bCad 3.7 Deutsch)
- ✓ Einen Win32 Disassembler (Hier: W32Dasm: http://www.softpedia.com/progDownload/WDASM-Download-1821.html)
- ✓ Einen HexEditor (Hier: HexWizard: http://www.wintotal.de/softw/index.php?rb=41&id=478)

Bevor es losgeht noch ein bisschen BLABLA.... Warum gerade bCAD, na ja das ist ein Super CAD Proggie und es ist einfach zu cracken. Zum anderen gibt es keinen Crack im WWW zu diesem Programm.

Schritt 1:

Zuerst installieren wir bCAD und starten nach der Installation den Rechner neu. Danach bCad.exe starten und schauen was passiert. Egal wo man hinklickt, man hat immer nur die Demo zur Verfügung. → Shit. Jetzt versuchen wir mal eine Serial einzugeben z.B. 1111111111 → Geht nicht wird du merken, da diese Serial nicht richtig ist. OK

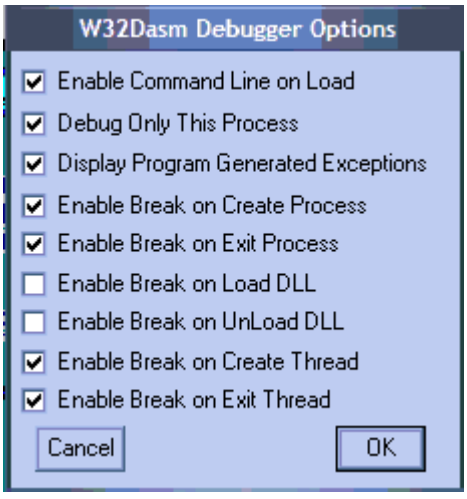
Schritt 2:

Raus aus bCad und ab ins bCad Verzeichnis, wo wir 2 Kopien von der bCad.exe herstellen. Eine Kopie brauchen wir zum debuggen, die andere werden wir patchen. Falls etwas schief läuft haben wir immer noch die original EXE.

Schritt 3:

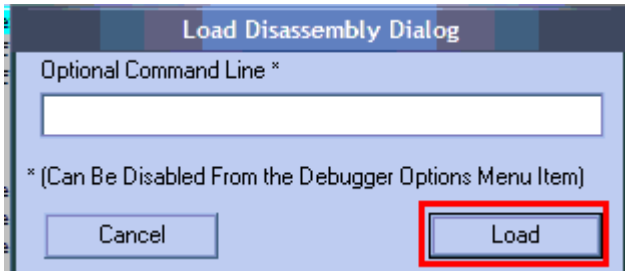
Wir starten Win32Dasm und starten die erste Kopie von bCad zum Disassemblerieren:

Danach rufen wir unter Debugger Options die Optionen auf und machen überall ein Häkchen außer bei Enable Break on Load DLL + Enable Break on Unload DLL:



Jetzt auf Debug → Load Process

Und jetzt auf Load klicken:



Schritt 4:

Hui .... da gehen wieder jede Menge Fenster auf .... Ist alles halb so wild, für uns ist nur das Fenster wichtig in dem sich die Buutons mit dem F6...F9 befinden.

Klicke also so oft F9 (Run Programm) bis wieder die Meldung zum Registrieren kommt.
Also wieder die selbe Prozedur → Serial mit 1111111111 eingeben und was kommt?? → Wieder nichts, aber dieses Mal geht noch eine Dialogbox auf mit folgender Meldung: „Incorrect Serial Number". Diesen String (Satz) müssen wir uns merken.

Schritt 5:

Klicke jetzt auf Step Into und dann auf Terminate. Alles mit JA bestätigen, bis du wieder den AssemblerCode vor dir siehst. Schaue dann in der Menüzeile nach Refs → String Data References und suche nach unserem String.

Hast du Ihn gefunden → Doppelklick auf den String Win32Dasm springt automatisch zu dieser Stelle im Quellcode. Diese Methode, über die vom Programm angegebene Fehlermeldung an die Stelle zu kommen, an der man die Sicherheitsabfrage korrigiert (also cracked), wird oft verwendet → So kann man z.B. auch Programme oder Spiele cracken, wenn Sie eine CD verlangen. Einfach den vom Spiel angegebenen String (Fehlermeldung) z.B. „Biete CD einlegen!" kopieren in Win32Dasm danach suchen und weiter wie im folgenden Text....

Schritt 6:

Etwas weiter nach unten Blättern, bis wir folgenden Code sehen:

```
:00403DF9 E8C24C1900              Call 00598AC0
:00403DFE 8B16                    mov edx, dword ptr [esi]
:00403E00 52                      push edx
:00403E01 E84A010000              call 00403F50
:00403E06 83C404                  add esp, 00000004
:00403E09 85C0                    test eax, eax
:00403E0B 752C                    jne 00403E39
:00403E0D 6A02                    push 00000002
:00403E0F 8BCF                    mov ecx, edi

* Reference To: MFC42.Ordinal:0A55, Ord:0A55h
                                  |
:00403E11 E8F84C1900              Call 00598B0E

* Possible StringData Ref from Data Obj ->"Incorrect serial number!"
                                  |
```

Schau dir diesen Codeabschnitt genauer an. Mit dem Call Befehl wird etwas aufgerufen (Die Dialogbox). Dann wird noch was in den Speicher geschoben. Dann kommt noch ein Call → Wahrscheinlich die Serial. Aber das interessiert uns nicht, wir wollen ja unsere eigene Serial, also weiter gucken. Aha, jetzt wird's interessant. Die Zeile **00403E0B ..... jne00403E39** ist unser Favorit. Mit anderen Worten steht hier → Vergleiche eingegebene Serial mit Serialvorgabe und springe zu Demoversion, wenn diese nicht gleich sind. Dort wird nämlich unsere Serial mit der korrekten verglichen. Wir müssen dem Proggie nur noch mitteilen, dass es zur Demoversion springen soll, wenn unsere Serial einen falschen Wert zurückt gibt, also wenn die eingegebene Serial = korrekter Serial ➔ (springe) zur Demo und wenn eingegebene Serial ≠ korrekter Serial ➔ nicht zur Demo springen = Vollversion. Dazu machen wir einfach aus unserem **jne** ein **je**.

Schritt 7:

So wir wollen also den Sprungbefehl ändern von jne (jump if not equal) in je (jump if equal). Dazu müssen wir uns von diesem Sprung die Offsetadresse merken, welche wir, nachdem wir den Befehl „**jne**...." bei Adresse **00403E0B** im Programm markiert hast (doppelt anklicken) ganz unten in der Statusleiste siehst. Diese lautet: **@Offset 0000320Bh.** Das h am Ende sagt lediglich aus, dass es sich um einen Hexadezimalwert handelt.

Jetzt haben wir alle Infos, die wir brauchen, um das Proggie zu patchen.

Schritt 8:

Starte deinen HexEditor und öffne die 2 Kopie der bCad.exe und gehe in der Menüleiste unter Edit → Goto. In der nächsten Dialogbox geben wir unseren ermittelten Offset ein (0x**0000320B**) ändere die **75 (jne)** in eine **74(je)** und speichere das ganze ab. HexWizard schließen.

Solche HexBefehle Gibt es einige. Meisten muss man einfach den Wert (Hier: 75) in einen Gegenwert (Hier: 74) umtauschen...

Eine kleine Liste von Hexbefehlen und Ihre Bedeutung:

75 oder 0F85 jne jump if not equal (Springe wenn nicht gleich) --- die beiden kommen am häufigsten vor 74 oder 0F84 je jump if equal (Springe wenn gleich)--------------/ 77 or 0F87 ja jump if above 0F86 jna jump if not above 0F83 jae jump if above or equal 0F82 jnae jump if not above or equal 0F82 jb jump if below 0F83 jnb jump if not below 0F86 jbe jump if below or equal 0F87 jnbe jump if not below or equal 0F8F jg jump if greater 0F8E jng jump if not greater	0F8D jge jump if greater or equal 0F8C jnge jump if not greater or equal 0F8C jl jump if less 0F8D jnl jump if not less 0F8E jle jump if less or equal 0F8F jnle jump if not less or equal EB jmp oder jmps jump directly to 84 test test 90 nop no operation

Achtung: Beim ersetzen von diesen Hexadezimalzahlen immer bedenken, dass Ihr, wenn Ihr eine Zahl oder Zeichen löscht auch nur eins und auch nicht mehr dazufügen könnt!

Schritt 9:

Starte die gepatchte bCad.exe und gebe irgendeine Serial ein, die garantiert falsch ist z.B. unsere → 1111111111

Huiiiii, was den nun los, keine Meldung wegen der Demo und alle Funktionen funktionieren.

Gratulation, Sie haben Ihr erstes Proggie selbst gecracked