FTP-HACKEN

Huhu ! Habt ihr nicht schon immer einmal daran gedacht wie es wäre einen FTP Server zu hacken, sich als root uneingeschränkten Zugriff verschaffen und eventuell auch noch die Web Seiten auszutauschen um euch zu präsentieren ??? Also, ich kenne keinen Hacker (oder solche, die es werden wollen), die sich dieser Vorstellung bisher entzogen haben. Zuerst brauchen wir noch ein paar Dinge, bevor wir richtig loslegen: * einen FTP Client (ich bevorzuge den von Windows) * einen Password Cracker (John The Ripper) * eine möglichst grosse Wordlist oder einen Dictionary Maker (dieser Punkt fällt weg, wenn wir einen BruteForce Password Cracker haben) * viel Zeit Ich bevorzuge noch das hinzuziehen von irgendwelchen Getränken wie Cola, Kaffee oder auch Tee. Wenn wir all diese Dinge geklärt haben, können wir endlich loslegen ;-) Probieren wir es zuerst mit der einfachsten Methode, indem wir unseren FTP Client starten und eine Verbindung zum "Opfer - FTP" herstellen. Dort versuchen wir uns nun als "anonymous" einzuloggen und senden als Passwort eine falsche E-Mail Adresse. Hierzu gehen wir in die DOS-Eingabeaufforderung und tippen ein (nach jeder Zeile Return drücken): ftp open target.comanonymous(hier teilen wir dem Server unseren Benutzernamen mit) Bill@Microsuck.com(hier teilen wir dem Server "unsere" E-Mail Adresse mit) get /etc/passwd(wir downloaden das file mit dem Namen passwd) get /etc/shadow(falls die passwd nicht existiert, downloaden wir die shadow) disconnect(trennt die Verbindung zum Server) quit(schliesst den FTP Client) Sollten wir hier schon Glück gehabt haben, ist der Rest ein Kinderspiel. Wir besitzen schonmal das passwd file und müssen dieses nur noch cracken. Dazu nehmen wir unseren Cracker und lassen ihn entweder nach der Dictionary oder Brute Force Methode das Passwort entschlüsseln. Das Ergebnis was wir bekommen, ist das Passwort des "root" Account (unter Novell: Supervisor; unter NT: Administrator), mit dem wir nun wieder eine neue FTP Verbindung zu unserem Server herstellen und uns als root und dem frisch gecrackten Passwort anmelden. Sollten wir allerdings an der ersten Methode gescheitert sein, können wir uns einen kleinen Bug in einigen UNIX Versionen zu Nutze machen. Hierzu benötigst du nur noch einen Webbrowser, in den du folgende Adresse eingibst (anstelle des www.target.com einfach den Domainnamen eintragen): http://www.target.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd bzw. http://www.target.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/shadow Wiederum kann es hier klappen,

dass wir den Inhalt der passwd oder shadow file sehen. Sollte dies der Fall sein, so speichern wir diese und cracken sie nur noch mit Hilfe unserer Proggies, loggen uns als root ein und treiben nun nach belieben dort unser Spielchen auf dem FTP Server. Es kann trotzdem geschehen, dass wir noch durch keine der beiden Methoden Erfolg gehabt haben ;-(An dieser Stelle sollten wir es mit dem Brute Force Hacking probieren. Brute Force bedeutet ganz einfach, ALLE möglichen Kombinationen zu probieren, was sehr zeitaufwendig sein kann und wird. TIP: UNIX Passwörter sind maximal 8 Zeichen lang !!!So, hiermit hätten wir dann auch das Thema mit dem FTP / Website hacken abgeschlossen. Eigentlich ist das ganze ziemlich simpel. Solltet ihr es dennoch nicht beim ersten Mal lesen verstanden haben, so lest es immer und immer wieder und sollten dann noch Fragen auftauchen, mailt mir und fragt mich. c u all Cyberdemon_98 Es gilt für jede Transaktion: Solltet ihr erfolgreich in ein System mit einem Administrator Account eingebrochen sein, killt zuerst die LOG Files, denn diese enthalten, was wirklich geschehen ist. Und wir wollen doch wirklich nicht, dass wir unseren Gegnern eine Spur hinterlassen. Alle Web-Server speichern irgendwo LOG-Files, indenen steht, wer sich wann, mit welchem Namen, mit welcher IP von wo aus eingeloggt hat.