```
----------------------------
-=[ FTP-Hacking Tutorial ]=-
----------------------------

(c) by Fre@ky D


1NHALT5V3R231CHN15
-----------------------------------------------------
```


---

1. Warum dieses Tutor

Dieses Tutor soll einen kurzen Einblick über die Funktionsweise, Sicherheiten und Spielereien :o) von FTP- Servern/FTP geben.

2. Was man wissen sollte und benötigt für dieses Tutor

Was man natürlich haben sollte, das wäre ein Zugang zum Internet und einen FTP-Client. Bei Windows9x ist solch einer dabei. Zu finden ist er unter c:\windows FTP.exe Dieser müsste euch so ziemlich bekannt vorkommen, weil er aussieht wie die MS-DOS Eingabeaufforderung, nur das sich der FTP-Prompt mit FTP> zu erkennen gibt.
Was sehr hilfreich wäre, das wären Kenntnisse auf FTP-/Unix-Ebene, und/oder ein Buch zu diesem Thema. Ich selber habe ein etwas älteres Buch,
(Unix - Ein Umfassendes Kompendium für Anwender und Syst4emspezialisten) das von dem Autor Horst Drees geschrieben wurde.
Es tut's eigentlich fast jedes...

3. Eine kurze Erläuterung und Funktionsweise zu FTP

FTP heißt File-Transfer-Protocol das überhalb des TCP/IP läuft und zwangsläufig den Port 21 benutzt. FTP ist die Standardmethode zur Datenübertragung zwischen zwei entfernten Systemen.
Ausgeführt wird das ganze in der Client-/Server-Umgebung und funktioniert so:
Der anfragende Rechner startet einen FTP-Client (wie oben beschrieben) und stellt Anfrage die an den Host eines anderen Netzwerkes (man kann den auch Ziel-Server nennen) übertragen wird. Damit eine Verbindung zu diesem Host auch funkt, muss auf diesem auch ein FTP-Server bzw. ein FTP-Daemon laufen.
FTPD ist ein Standard-FTP-Server-Daemon der normalerweise in den meisten integriert ist. Dieser Daemon hat die einfache Aufgabe auf Verbindungsanfragen zu reagieren. (Dies ist jetzt wichtig, weil wir das später brauchen.)Wenn diese Verbindung steht, verlangt der FTP-Server den Benutzernamen, und ein passendes Passwort dazu.
Damit wäre der Login dann abgeschlossen.

4. Zum eigentlich Thema

Nun möchte ich mal zum Thema meines Tutors zurückkommen, welches ja das Hacken eines FTP-Server ist! Dies ist auch der Erste Schritt in Richtung Sitehacking. Und am Besten lernt man wohl immer noch in der Praxis, also wollen wir gleich mal anfangen. Wie im Kapitel 3 beschrieben, brauchen wir erst einmal eine Verbindung zu einem FTP-Server (natürlich auch eine Internetverbindung *g*). Dazu benötigt man nur dessen URL oder IP-Adresse.

Nehmen wir mal irgendeine IP-Adresse, z.B. 123.123.123.123 Achso, bei einem Firewall oder Proxy könnte es vielleicht ein paar Problemchen geben. Aber nicht unbedingt.

Also, dann lasst uns mal connecten, in dem ihr den FTP-Client öffnet, und den Connect-Befehl 'open' mit der dazugehörigen ServerURL/IP-Adresse eingebt. Das wäre in diesem Beispiel: open 123.123.123.123 Dann müsste nach kurzer Zeit eine Antwort kommen, das ihr mit dem FTP-Server verbunden seid. Da ist auch gleich die Version des Betriebssystems des Connecteten Servers zu erkennen. Dann müssten wir eigentlich gleich nach unserem Benutzernamen abgefragt werden. Da wir natürlich keinen haben, müssen wir uns anonym einloggen, sofern der Server anonyme Arbeitssitzungen zulässt. Das machen wir in dem wir als Benutzername einfach 'anonymous' eingeben.(Es kommt drauf an mit welchem System man es zu tun hat, ansonsten mal 'guest' probieren) Dann folgt auch schon in der nächsten Zeile die Aufforderung zur Passworteingabe (manchmal auch als E-Mail Adresse, Leutz, dann bitte nicht die Echte eingeben... :o))
Am besten ist es aber wenn man einfach nochmals 'anonymous' eingibt (man fällt durch die Eingabe des Benutzernamens nicht so sehr auf). Es geht natürlich auch jede weitere Zeichenfolge. Nun müsstet ihr eigentlich eine Meldung bekommen das der Loggin ein Erfolg war (succesful), worauf dann wieder der nackte FTP-Prompt folgt. Nun seit ihr drin...ging doch fast so einfach wie bei Boris oder? :o)
Aber ihr werdet es euch doch sicherlich schon gedacht haben, das da irgendwo ein Haken ist. Damit habt ihr Vollkommen recht. Zum Glück, na gut man kann es sehen wie man's will, sind wir heute auf einem etwas besserem Sicherheitsniveau, weil natürlich der anonyme Benutzer, wie wir es in diesem Fall sind, fast keine Rechte hat. (Eigentlich nur Leserechte in einem bestimmten Gebiet *g*). Erweiterte Rechte haben nur die zugelassenen Benutzer, deren Benutzername und Passwort, was wir für den Login benötigen würden, nicht haben. Dann ist das ganz einfach. Wir holen uns diese Informationen. Diese Infos sind nämlich in der Passwd-Datei auf dem Server vorhanden (Jetzt kommen allmählich die Unixkenntnisse *g*).
Nun sollte man nur noch wissen wo genau. Damit man aber erstmals weiß wo man sich befindet sollte man den Befehl pwd eingeben, worauf dann die Antwort folgen müsste, das wir uns im Root-Verzeichnis befinden. Das wir dann auch noch wissen was es sonst noch für Verzeichnisse gibt, gibt man einfach den DOS-Befehl dir (steht für directory, das war mal wieder was für die extra lamerz *g*) Dann landet man meistens unter den folgenden Verzeichnissen einen Volltreffer: /etc/passwd , /etc/security/passwd wie aber auch unter /etc/shadow und /etc/security/shadow. (In ein Verzeichnis wechselt man natürlich mit 'cd', für change directory)
Dort müsste dann die Passwd-Datei vorhanden sein, in welcher alle Benutzer mit Passwort, Benutzernummer....usw. vorhanden sind. Also wechseln wir in dieses Verzeichnis und kopieren uns diese Datei am besten auf die Festplatte, was man aber eigentlich nicht machen dürfte (man dürfte sie eigentlich nur lesen), wie so manches im Leben :o) Diese Datei kann man sich mit dem Befehl 'get passwd' kopieren. Dann ist diese Datei sicher in eurem Windows-Verzeichnis aufbewahrt (Natürlich nur bei Windowsanwendern). Naja, ob sie wirklich sicher ist bei diesem Verzeichnisname *g* :o)...
Dann wechseln wir wieder in unser Stammverzeichnis mit dem Befehl 'cd ..' wo wir dann unsere Verbindung zum angewählten Server schließen können. Das geht mit dem Befehl 'disconnect' aber auch etwas kürzer mit 'close'. Und um uns von unserem hilfreichen FTP-Client zu verabschieden, geben wir einfach den Befehl 'bye' ein, und schon verschwindet unser FTP-Window!
Somit ist der fast einfachste Teil erledigt. (Ich weiß, das klingt jetzt deprimierend, aber wir haben noch was vor uns, und zwar die Passwd-Datei *g*)

5. Die Passwd-Datei

Nachdem wir in unserem Windows-Verzeichnis nun die Passwd-Datei geöffnet haben, (das geht mit jedem einfachen ASCII Editor, also auch mit dem Notepad von Microsoft) sehen wir die für manche unbekannte Datei. (Wie gesagt, UNIX zahlt sich nun mal aus *g*)

Hier mal ein Beispiel wie so eine Datei aussehen könnte:

```
Root:avUzz7bfF:0:0::/usr/manfred::
Manfred:xZaBD5ersN7:10:100::/usr/manfred::
monika:yxZZrdtPLN7:11:100::/usr/monika::
peter:00pmutD&u(7:12:100::/usr/peter::
klaus:UPFHHimoTEl:13:100::/usr/klaus::
harry:77tMNUlssky:14:110::/usr/harry:/bin/csh:
neu::15:100::/usr/neu::
```

Das mag für manche auf den ersten Blick verwirrend wirken,aber nur keine Angst, wir werden uns diese Datei mal genauer anschauen, dann lernen wir auch ihre Unterteilung kennen:

Was ganz allgemein mal gesagt werden kann, ist, das in dieser Datei für jeden Benutzer eine Zeile vorgesehen ist. Diese Zeile ist wiederum in bestimmte Felder eingeteilt, welche sich durch Doppelpunkte voneinander trennen. Diese Felder haben folgende Eigenschaften bzw. Inhalt:

Feld1: Benutzername
Feld2: (verschlüsseltes) Passwort
Feld3: Benutzernummer
Feld4: Gruppennummer
Feld5: Kommentar oder Eintrag für systeminterne Verwendung
Feld6: der volle Pfadname des Arbeitsdirectorys des Benutzers
Feld7: Name des Kommandointerpreters oder eines Programmes, mit dem der
Benutzer ausschließlich arbeiten soll.

Aus diesem Beispiel ist klar zu erkennen, das nur der sogenannte Super-User root die Benutzernummer 0 hat. Diese Benutzernummer verschafft ihm die besonderen Privilegien. Die anderen Benutzer, haben beliebige, fortlaufende Nummern, die größer sein müssen als 0!!! Was auch zu erkennen ist, ist das bis auf den letzen Benutzer 'neu' schon alle anderen ein Passwort haben, auf welches wir gleich zu sprechen kommen. Das Passwort des neuen Benutzers muss er selbst vergeben, wenn er sich so zu sagen zum ersten Mal in das System eingeschaltet hat. Dann benutzt der neue Benutzer das Kommando 'passwd'. Wenn das dann erfolgreich geschehen ist, wird auch sein Passwort in seiner eigenen Zeile im Feld2 VERSCHLÜSSELT abgelegt. Und genau das ist hier das Problem. (ihr seid doch bestimmt schon draufgekommen oder *g*) Hier sind nämlich alle Passwörter der Benutzer verschlüsselt und man muss nun versuchen sie zu entschlüsseln bzw. cracken. Das kann manchmal einfach sein mit Hilfe von Tools wie Passwortcracker, die nach bestimmten Schemen vorgehen, aber auch etwas schwieriger. Wenn ihr das dann hinbekommen habt, habt ihr Zugang auf das System und könnt alles machen, was der Benutzer auch darf. Wenn euch aber sogar das Super-Userpasswort in die Hände gelangt, dann seit ihr der King. Wenn ihr dann nämlich als Super-User einloggt, werdet ihr alle Zugriffsrechte haben und herrscht somit über dieses System!
Leider kann diese Vorstellung aber auch sehr sehr leicht verdorben werden.
Oft steht nämlich anstatt 'nur' *g* ein verschlüsseltes Passwort ein einfaches 'X' oder '*' (es betrifft eigentlich allgemein die Sonderzeichen, z.B. auch '!' und '#'). Dann sind die Passwörter nämlich 'shadowed', das heißt soviel, wie wenn man ein Passwort schattiert oder unsichtbar macht. Das ist ein Sicherheitssystem, das die ENTSCHLÜSSELTE Passwortdatei, welche meist an einem für User unzugänglichen Ort aufbewahrt wird, durch ein Sonderzeichen ersetzt.
Jetzt möchte ich aber noch eine Kleinigkeit zu Feld 7 sagen. In diesem Feld werden normalerweise keine Einträge gemacht, weil es meistens so ist, das alle Benutzer nach dem Login auf der gleichen Kommandoebene arbeiten können.
(Diese nennt man übrigens Shell *ggg*). Möchte aber ein Benutzer z.B. auf einer andere als die Standart-Shell benutzen, und ist diese im System verfügbar, dann kann hier (im Feld7) der Pfadname dieser Shell eingetragen werden.

6. Passwortcracking mit Brute Force Programmen

Wer von euch natürlich sehr viel Zeit hat, und seine online kosten erhöhen will, der kann das ganz einfach machen, in dem er seine Verbindung aufmacht und schlafen geht, oder mit der Brute Force Methode versuchen ein Passwort zu knacken. :o)
Dazu braucht man erstmals ein Brute Force Programm, ich empfehle Unsecure, das müsste eigentlich bekannt sein. Das Prinzip dieses Programmes ist ganz einfach:
Man gibt die gewünschte URL oder IP-Adresse an, und schon verbindet sich Unsecure mit dem Server und probiert auf gewünschtem Benutzernamen, alle Zeichenfolgen so wie Zahlenfolgen nacheinander aus, bis das Passwort geknackt ist. Es hat auch eine Funktion, wie die meisten, das es nach allen 100 Versuchen das Ergebnis speichert, so das man nicht nochmals von vorne beginnen muss. Es stellt die Verbindung zum Server auch automatisch wieder her, wenn dieser sie beendet hat, z.B. wegen einer falschen Passworteingabe. Trotzdem ist diese Methode etwas langwierig. Außerdem sieht es etwas merkwürdig für einen Admin aus, wenn ein User 1000 mal versucht sich einzuloggen und sein Passwort nicht richtig ist. :o) Aber zum ausprobieren ist es nicht schlecht, man kann auch mit Wordlists arbeiten, falls es ein

'Sinnvolles' oder einfaches Passwort sein sollte, das geknackt werden will.

So Leutz, jetzt bin ich eigentlich fertig mit meinem Tutor. Aber ihr ahnt schon was? Ja, dazu muss ich meinen Senf auch noch geben :o)

Ihr wisst ja, das Gesetz ist mit diesem Vorgehen nicht ganz einverstanden, und somit möchte ich darauf hinweisen, das ihr selbstverantwortlich seid für das wir ihr mit meinen Informationen macht, und das ich keinerlei Haftung für jeglichen Schaden übernehme, der durch illegales Anwenden dieser Informationen zustande kommt. Der mißbrauch dieser Informationen wird strafrechtlichverfolgt, und mit Geld- und Haftstrafen bestraft.

Sorry, aber das musste sein! :o)

Trotzdem hoffe ich das euch mein Tutor gefallen hat und das ihr auch was lernen konntet :o)

Everyone of us is a little bit freaky

Fre@ky D

Bei weiteren Fragen wendet euch an mich!
Freaky_D@gmx.net