4.8 Absender können gefälscht werden

Kein Entführungskrimi kommt ohne einen anonymen Drohbrief aus. Mit der normalen Post auch kein Problem, denn wer zwingt Sie schon, Ihren Absender auf den Umschlag zu schreiben. Bei E-Mails sieht es im Prinzip nicht anders aus: Es gibt zwar immer einen Absender, aber der lässt sich einfach fälschen.

Fachjargon für Fälschungen

Eine Fälschung wird umgangssprachlich als Fake bezeichnet.

Vor allem Hacker, die anonym Trojaner-Viren verschicken wollen, und Spammer nutzen diesen Umstand rege aus. Sehr zum Leidwesen der Betroffenen, denn so ist eine Strafverfolgung sehr erschwert, und man kann sich auch kaum zur Wehr setzen, denn eine Antwort an den Absender wird meistens mit einer Fehlermeldung eines Mailservers quittiert, der einem mitteilt, dass es den angeblichen Absender gar nicht gibt.

Wie funktioniert das E-Mail-Fälschen?

Nicht nur das anonyme Versenden von E-Mails ist denkbar einfach, auch das Fälschen des Absenders. Damit ein Hacker seine Opfer möglichst optimal täuscht, muss die angebliche Sicherheitswarnung, die zum Installieren der schädlichen Software auffordert, scheinbar auch von einem allgemein vertrauenswürdigen Absender kommen. Dabei wird eine Schwäche des **S**imple **M**ail **T**ransfer **P**rotocol (SMTP) ausgenutzt: Dieses Protokoll ist für den Transport von Nachrichten zuständig – von der Annahme bis zur Auslieferung. Bei der Entgegennahme von E-Mails ist es leider sehr treugläubig und überprüft nicht den angegebenen Absender auf Korrektheit, Existenz oder Missbrauch.

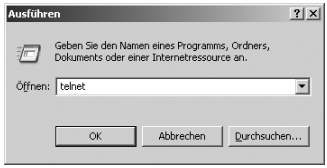
Illegalität zum Greifen nah

Die im Folgenden gezeigten Schritte sind nur zum Eigenstudium auf einem System, bei dem Sie auch tatsächlich einen E-Mail-Account besitzen. Da die meisten SMTP-Server mittlerweile gegen Missbrauch abgedichtet wurden, ist es zum Glück nicht mehr so leicht, eine Fake-E-Mail abzuschicken. Allerdings gibt es immer noch zahlreiche so genannte Open Relay-Listen mit frei zugänglichen Servern im WWW.

Quicksteps: Gefälschte E-Mail absenden

- Starten Sie das Programm Telnet.
- Geben Sie die einzelnen Befehlsschritte ein.
- Schreiben Sie Ihre Nachricht.

1. Starten Sie das Programm Telnet über *Start/Ausführen*.

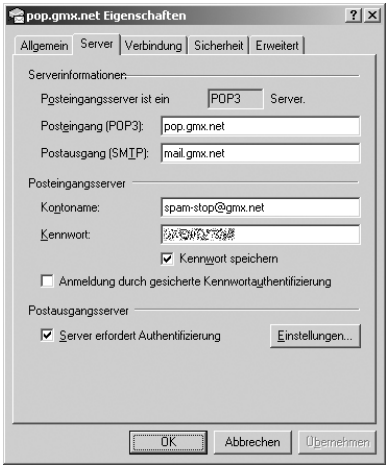


INFO

Telnet

Telnet ist eine Terminalemulation, mit der Sie auf einen entfernten Rechner zugreifen können. Sie haben die Möglichkeit, auf Ihre dort gespeicherten Dateien zuzugreifen oder auf dem entfernten Rechner einen Befehl auszuführen.

2. Sie benötigen einen SMTP-Server, auf den Sie zugreifen können. Die Adresse des Mailservers erfahren Sie von Ihrem Anbieter und haben sie in den Einstellungen Ihres E-Mail-Programms angegeben (*Extras/Konten/E-Mail*, *Eigenschaften*, *Server* bei Outlook Express).



INFO

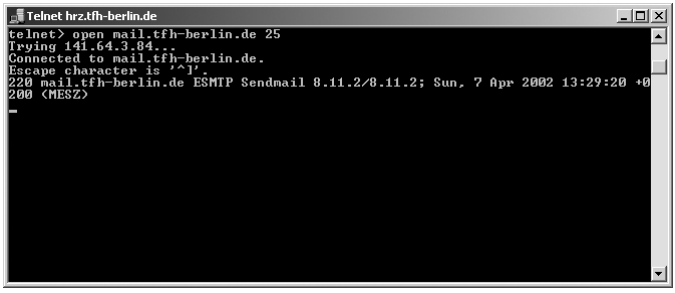
Schotten dicht gemacht

Wie gesagt: Sie können zwar jeden Mailserver ansprechen, aber nur die wenigsten (schlecht konfigurierten) werden es zulassen, dass Sie tatsächlich eine E-Mail abschicken können. In der Regel werden Sie bei einem der

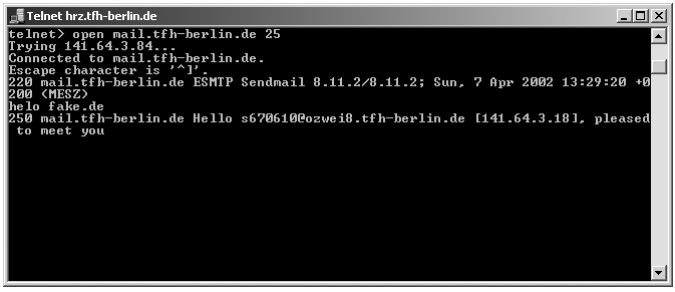
folgenden Schritte eine Fehlermeldung bekommen, da Sie sich authentifizieren müssen. Aus diesem Grund stammen die folgenden Screenshots aus einer etwas anderen Arbeitsumgebung.

3. Geben Sie in der Eingabeaufforderung den Telnet-Befehl „open <SMTP-Server> 25“ ein. Dadurch öffnen Sie eine Verbindung zu dem Server über den SMTP-Port Nummer 25 (der Standardport für SMTP). Was ein Port genau ist, erfahren Sie auf Seite 19.

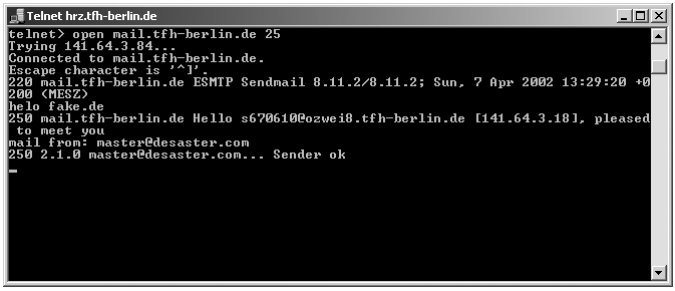
4. Der SMTP-Server meldet sich und gibt eine mehr oder weniger detaillierte Info über das verwendete System aus. Hier ist es Sendmail mit dem Extended SMTP, Version 8.11.2.



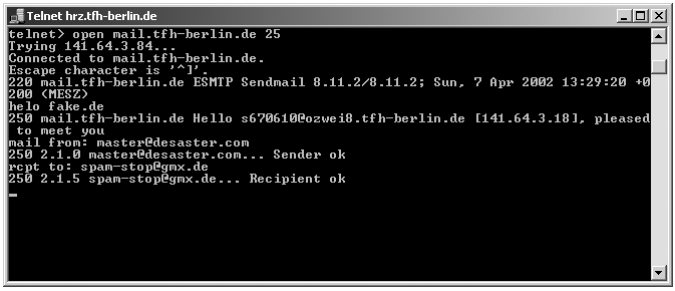
5. Jetzt müssen Sie sich gegenüber dem Server vorstellen. Geben Sie dazu ein: „helo <wunschdomain.wunsch-tld>“ (z. B. *fake.de*). Woraufhin der Server Sie vermutlich begrüßen wird. Die Angabe wird meistens gar nicht überprüft und muss oft nur einen Punkt enthalten.



6. Geben Sie an, wer als Absender der E-Mail eingetragen werden soll: „mail from: <E-Mail-Adresse>“ (z. B. *mail from: master@desaster.com*), wobei die Angabe nicht geprüft wird und Sie sich jede beliebige E-Mail-Adresse ausdenken können. Das System gibt i. d. R. eine Bestätigung der Eingabe aus.



7. Geben Sie den gewünschten Empfänger der Nachricht ein: „rcpt to: <E-Mail-Adresse“. Wieder gibt es eine Rückmeldung.

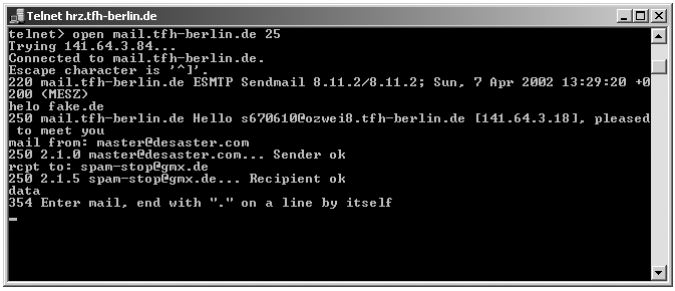


best friend **INFO**

Bis hierhin und nicht weiter

Spätestens hier wird Sendmail stutzig und will Ihren Versuch abblocken. Die Rückmeldung *Relaying denied* bedeutet, dass Sie nicht berechtigt sind, eine Mail ohne Anmeldung am Server oder unter der aktuellen IP-Adresse etc. abzuschicken. Sie können sich die weiteren Mühen auf diesem Server sparen.

8. Wurde der Empfänger akzeptiert, geben Sie den Befehl „data“ ein.

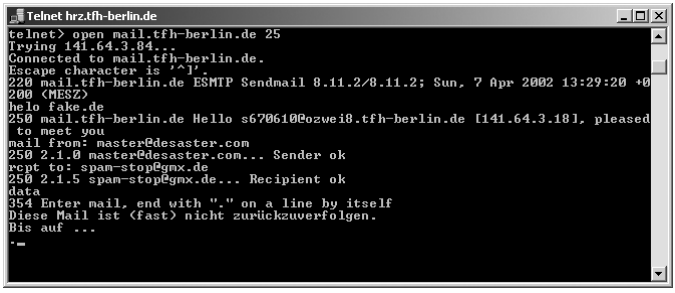


9. Schreiben Sie nun Ihre Nachricht. Um die Mail abzuschließen, geben Sie in einer neuen Zeile einen Punkt ein und drücken Enter.

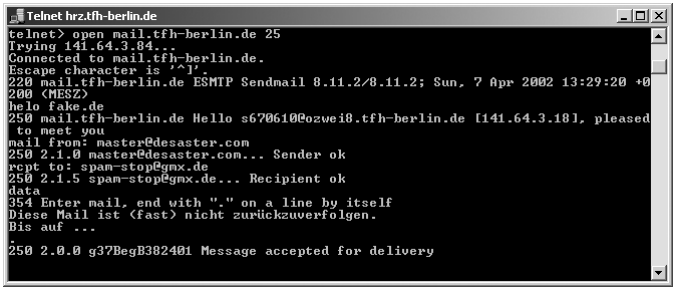
best friend
TIPP

Vorsicht, Sonderzeichen

Die meisten (UNIX-basierten) Systeme kommen nicht mit den Windows-Sonderzeichen zurecht, sodass Sie eventuell keine Zeichen wie gewohnt löschen können oder Umlaute etc. beim Versand verloren gehen.



10. Eine Statusmeldung wird ausgegeben, die Sie über den erfolgreichen Versand informiert. Wenn Sie wollen, können Sie weitere Nachrichten versenden.



11. Wenn Sie fertig sind, beenden Sie die Verbindung zum SMTP-Server mit dem Befehl *quit*.

Am Selbsttest zeigt sich, dass die gefälschte E-Mail wirklich ziemlich echt aussieht und alles geklappt hat. Einzig ein Hinweis stört im Beispiel: Da es wie gesagt kaum noch Mailserver gibt, die Relaying zulassen, musste ich mich für den Versuch an einem Server vorher anmelden. Und genau diese Anmeldung ist in der Mail zu erkennen, denn Sendmail hat meine Anmeldekennung (teilweise unkenntlich gemacht) in der Mail in Klammern zusammen mit einer IP-Adresse notiert, sodass der Absender im Zweifelsfall diesmal doch ermittelt werden kann. Und auch bei Open Relay SMTP-Servern wird Ihre IP-Adresse immer Bestandteil der E-Mail sein. Ausgefuchste Hacker können die IP-Angabe zwar auch fälschen, doch solange Sie das nicht beherrschen, kann zur Strafverfolgung die E-Mail zu Ihnen zurückverfolgt werden (wie, erfahren Sie u. a. ab Seite 86). Deshalb beschäftigen Sie sich besser nur damit, wie Sie eine gefälschte E-Mail erkennen, anstatt eine abzusenden.

Anonyme E-Mails schreiben

Nicht jeder, der eine anonyme E-Mail schreibt, ist gleich ein böser Mensch. Es kann auch durchaus triftige Gründe geben, beispielsweise wenn jemand eine anonyme Anzeige über Kinderpornografie aufgeben will. Allerdings sollten anonyme Mails nicht benutzt werden, um Spams zu verschicken, kriminelle Handlungen zu verschleiern oder um andere Menschen zu verunglimpfen.

Um eine anonyme E-Mail abzuschicken, gibt es so genannte Remailer. Diese nehmen die Nachricht an, entfernen alle Hinweise auf den Absender und schicken sie dann weiter: entweder an den Empfänger oder an einen weiteren Remailer, um die

Rückverfolgung weiter zu erschweren. Es gibt sowohl webbasierte Remailer als auch eigenständige Programme.

best friend TIPP

Remailer

Im Buch „Anti-Hacker Report" von DATA BECKER finden Sie eine ausführliche Beschreibung des Remail-Programms Private Idaho (*http://www.eskimo.com/~joelm/pi.html*). Eine weitere Alternative ist Mixmaster (*http://sourceforge.net/projects/mixmaster*).

best friend INFO

100 % Anonymität gibt es nie

Egal was Sie versuchen: Ganz anonym werden Sie nie sein, denn jeder Remailer protokolliert seine Aktionen mit. Bei Bedarf (z. B. bei kriminellen Delikten) können die Log-Dateien jederzeit darüber Auskunft geben, wer der tatsächliche Absender war. Im Normalfall genießen Remailer aber ein hohes Vertrauen.

best friend

Quicksteps: Anonyme E-Mail per Webseite verschicken

- Tragen Sie auf der Webseite die notwenigen Angaben ein.
- Wählen Sie, über wie viele zufällig ausgewählte Remailer die Nachricht verschickt werden soll.
- Verschicken Sie abschließend die Mail.

1. Um eine anonyme E-Mail per Webseite zu verschicken, begeben Sie sich auf die Webseite *https://riot.eu.org/anon/remailer.html.en*.

2. Tragen Sie einen Empfänger bei *To* ein und eine Betreffzeile bei *Subject*.

3. Wenn Sie wollen, können Sie zusätzliche Header-Informationen angeben, z. B. *Reply-To: <Adresse>*, um eine (temporär eingerichtete) Antwortadresse anzugeben.

4. Tragen Sie die gewünschte Nachricht im Feld *Message* ein.