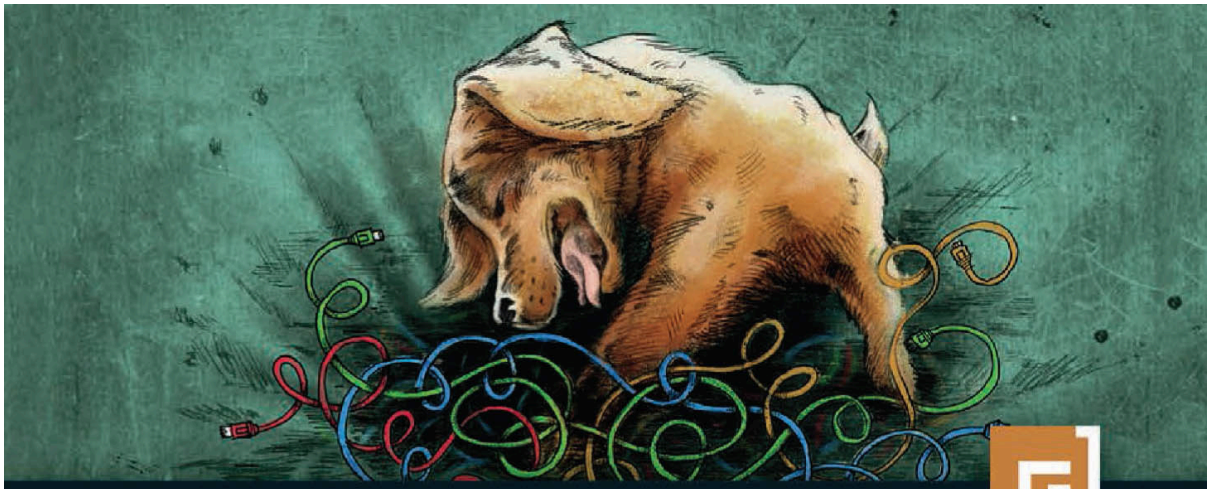

James Forshaw

Netzwerk-protokolle hacken

Sicherheitslücken verstehen, analysieren und schützen

no starch press

dpunkt.verlag

Inhalt

4
Fortgeschrittenes Capturing von Anwendungsverkehr

Üblicherweise reichen die Capturing-Techniken aus, die Sie in Kapitel 2 kennengelernt haben, doch gelegentlich stehen Sie vor schwierigen Situationen, die fortgeschrittene Capturing-Techniken erfordern. Manchmal stellt eine Embedded-Plattform die Herausforderung dar, die nur per DHCP (Dynamic Host Configuration Protocol) konfiguriert werden kann, ein anderes Mal ist es ein Netzwerk, über das Sie keine Kontrolle haben, solange Sie nicht direkt mit ihm verbunden sind.

Ein Großteil der in diesem Kapitel diskutierten fortgeschrittenen Techniken zum Erfassen von Netzwerkverkehr nutzt die existierende Netzwerkinfrastruktur und die vorhandenen Protokolle zur Umleitung des Verkehrs. Keine dieser Techniken verlangt spezielle Hardware. Sie benötigen nur Softwarepakete, die auf unterschiedlichen Betriebssystemen zu finden sind.

4.1 Rerouting von Verkehr

IP ist ein *geroutetes* Protokoll, d. h., keiner der Knoten des Netzwerks muss die genaue Lage eines anderen Knotens im Netzwerk kennen. Sendet ein Knoten Verkehr an ein anderes Netzwerk, mit dem er nicht direkt verbunden ist, dann gibt er den Verkehr an ein *Gateway* weiter, das den Verkehr an das Ziel weiterleitet. Ein Gateway wird üblicherweise auch als *Router* bezeichnet, ein Gerät, das Verkehr von einem Ort an einen anderen routet.

In Abbildung 4–1 versucht zum Beispiel der Client 192.168.56.10 Daten an den Server 10.1.1.10 zu senden, doch der Client hat keine direkte Verbindung mit dem Server. Er sendet den für den Server gedachten Verkehr daher zuerst an Router A. Router A sendet die Daten dann an Router B weiter, der eine direkte

Verbindung zum Zielserver hat. Router B leitet den Verkehr dann an sein eigentliches Ziel weiter.

Wie alle anderen Knoten des Netzwerks kennt auch das Gateway das genaue Ziel der Daten nicht und sucht sich daher ein passendes nächstes Gateway aus, an das es den Verkehr weiterleitet. In unserem Beispiel kennen die Router A und B nur die beiden Netzwerke, mit denen sie direkt verbunden sind. Um vom Client zum Server zu gelangen, muss der Verkehr geroutet werden.

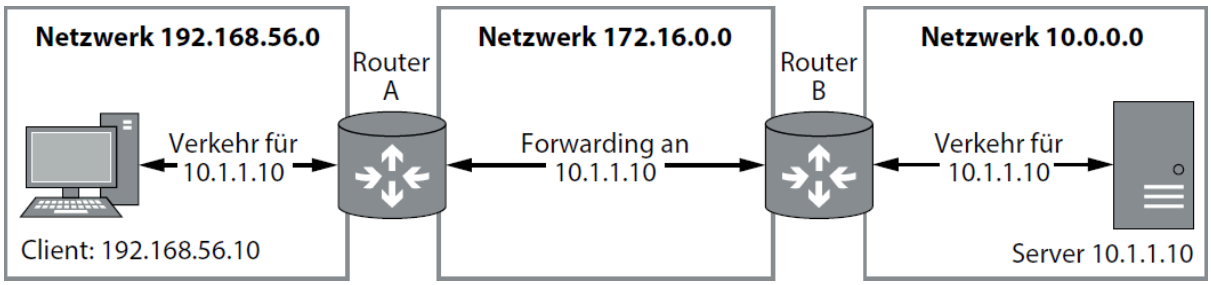

Abb. 4–1 *Beispiel für gerouteten Verkehr*

4.1.1 Traceroute nutzen

Beim »Tracing« einer Route versuchen Sie zu verfolgen, welchen Weg der IP-Verkehr zu einem bestimmten Ziel nimmt. Die meisten Betriebssysteme besitzen fest integrierte Tools, die ein solches Tracing durchführen, z. B. `traceroute` bei den meisten unixoiden Plattformen und `tracert` unter Windows.

Listing 4–1 zeigt das Ergebnis eines Tracings der Route zu *www.google.com* über eine heimische Internetverbindung.

```
C:\Users\user>tracert www.google.com

Tracing route to www.google.com [173.194.34.176]

over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  home.local [192.168.1.254]

  2    15 ms    15 ms    15 ms  217.32.146.64

  3    88 ms    15 ms    15 ms  217.32.146.110
```

```
 4    16 ms    16 ms    15 ms  217.32.147.194

 5    26 ms    15 ms    15 ms  217.41.168.79

 6    16 ms    26 ms    16 ms  217.41.168.107

 7    26 ms    15 ms    15 ms  109.159.249.94

 8    18 ms    16 ms    15 ms  109.159.249.17

 9    17 ms    28 ms    16 ms  62.6.201.173

10    17 ms    16 ms    16 ms  195.99.126.105

11    17 ms    17 ms    16 ms  209.85.252.188

12    17 ms    17 ms    17 ms  209.85.253.175

13    27 ms    17 ms    17 ms  lhr14s22-in-f16.1e100.net
[173.194.34.176]
```

Listing 4–1 *Traceroute für www.google.com mithilfe des tracert-Tools*

Jede nummerierte Ausgabezeile (1, 2 usw.) steht für ein spezifisches Gateway, das den Verkehr an das eigentliche Ziel weiterleitet. Die Ausgabe ist auf eine maximale Anzahl von *Hops* beschränkt. Ein einzelner Hop repräsentiert das Netzwerk zwischen jedem Gateway der Route. Beispielsweise gibt es einen Hop zwischen Ihrem Rechner und dem ersten Router, einen weiteren zwischen dem Router und dem nächsten Router und so weiter bis zum eigentlichen Ziel. Wird die maximale Anzahl von Hops überschritten, bricht traceroute die Suche nach weiteren Routern ab. Die maximale Zahl von Hops kann bei traceroute in der Kommandozeile festgelegt werden. Verwenden Sie `-h ANZAHL` unter Windows und `-m ANZAHL` bei unixoiden Systemen. (Die Ausgabe enthält auch die Umlaufzeit vom Startrechner der Traceroute zum gefundenen Knoten.)

4.1.2 Routing-Tabellen

Das Betriebssystem verwendet *Routing-Tabellen*, um zu bestimmen, an welche Gateways Verkehr geschickt werden muss. Eine Routing-Tabelle enthält eine Liste von Zielnetzwerken und Gateways, an die der Verkehr zu senden ist. Ist ein Netzwerk direkt mit dem Knoten verbunden, der die Daten sendet, dann ist kein Gateway nötig, d. h., der Verkehr kann direkt im lokalen Netzwerk übertragen werden.

Sie können sich die Routing-Tabelle Ihres Computers ansehen, indem Sie `netstat -r` bei den meisten unixoiden Systemen bzw. `route print` unter Windows eingeben. Listing 4–2 zeigt die Ausgabe dieses Befehls unter Windows.

```
> route print

IPv4 Route Table

===========================================================
===================

Active Routes:

Network Destination            Netmask          Gateway
Interface   Metric

(1)              0.0.0.0            0.0.0.0   192.168.1.254
192.168.1.72        10

              127.0.0.0          255.0.0.0         On-link
              127.0.0.1      306

              127.0.0.1   255.255.255.255         On-link
              127.0.0.1      306

        127.255.255.255   255.255.255.255         On-link
        127.0.0.1      306
```

```
          192.168.1.0     255.255.255.0         On-link
          192.168.1.72      266

         192.168.1.72   255.255.255.255         On-link
         192.168.1.72      266

       192.168.1.255   255.255.255.255         On-link
       192.168.1.72      266

          224.0.0.0         240.0.0.0         On-link
          127.0.0.1      306

          224.0.0.0         240.0.0.0         On-link
          192.168.56.1      276

          224.0.0.0         240.0.0.0         On-link
          192.168.1.72      266

    255.255.255.255   255.255.255.255         On-link
    127.0.0.1      306

    255.255.255.255   255.255.255.255         On-link
    192.168.56.1      276

    255.255.255.255   255.255.255.255         On-link
    192.168.1.72      266

===========================================================
====================
```

Listing 4–2 *Beispielhafte Routing-Tabelle*

Wie bereits erwähnt besteht ein Grund für den Einsatz von Routing darin, dass die Knoten den Ort der anderen Knoten im Netzwerk nicht kennen müssen. Doch was passiert mit Verkehr, wenn man das Gateway, das für die Kommunikation mit dem Zielnetzwerk verantwortlich ist, nicht kennt? In diesem Fall ist es üblich, dass die Routing-Tabelle den gesamten unbekannten Verkehr an das sogenannte *Default Gateway* weiterleitet. Sie sehen dieses Standard-

Gateway bei ❶, wo als Zielnetzwerk 0.0.0.0 angegeben ist. Dieses Ziel ist ein Platzhalter für das Standard-Gateway, was die Verwaltung der Routing-Tabelle vereinfacht. Durch den Platzhalter muss die Tabelle nicht geändert werden, wenn sich die Netzwerkkonfiguration ändert, etwa durch eine DHCP-Konfiguration. Verkehr, der an irgendein Ziel gerichtet ist, für das es keine passende Route gibt, wird an das Gateway mit der Platzhalteradresse 0.0.0.0 gesendet.

Wie kann man das Routing nun für seine Zwecke nutzen? Nehmen wir ein Embedded-System an, bei dem Betriebssystem und Hardware in einem einzigen Gerät vereint sind. Möglicherweise haben Sie keinen Einfluss auf die Netzwerkkonfiguration des Embedded-Systems, weil Sie gar nicht auf das zugrunde liegende Betriebssystem zugreifen können, doch wenn Sie Ihre Capturing-Vorrichtung als Gateway zwischen dem System und dem eigentlichen Ziel schalten, können Sie auch den Verkehr dieses Systems erfassen.

Die folgenden Abschnitte zeigen Möglichkeiten auf, wie man ein Betriebssystem konfiguriert, damit der Rechner als Gateway fungieren und den Netzwerkverkehr abgreifen kann.

4.2 Konfiguration eines Routers

Standardmäßig leiten die meisten Betriebssysteme den Verkehr zwischen Netzwerkschnittstellen nicht direkt weiter. Das soll hauptsächlich verhindern, dass jemand auf einer Seite der Route direkt mit den Netzwerkadressen auf der anderen Seite kommunizieren kann. Ist das Routing in der Betriebssystemkonfiguration nicht aktiviert, wird jeder Verkehr, der geroutet werden müsste, verworfen (oder es gibt eine Fehlermeldung an den Sender). Die Standardkonfiguration ist für die Sicherheit sehr wichtig: Stellen Sie sich die Folgen vor, wenn der Router, der Ihre Verbindung zum Internet kontrolliert, Daten aus dem Internet direkt in Ihr privates Netzwerk leitet.

Um also das Routing im Betriebssystem zu aktivieren, müssen Sie mit Administratorrechten einige Änderungen an der Konfiguration vornehmen. Zwar ist die Aktivierung des Routings bei jedem Betriebssystem anders geregelt, doch ein Aspekt bleibt immer gleich: Der Computer muss über mindestens zwei Netzwerkschnittstellen verfügen, um als Router fungieren zu können. Darüber hinaus benötigen Sie Routen auf beiden Seiten des Gateways, damit das Routing korrekt funktioniert. Hat das Ziel keine entsprechende Route zurück zur Quelle, funktioniert die Kommunikation nicht wie gewünscht. Sobald das Routing

aktiviert ist, können Sie Ihre Geräte so konfigurieren, dass der Verkehr über Ihren neuen Router geleitet wird. Läuft ein Tool wie Wireshark auf dem Router, können Sie den gesamten Verkehr festhalten, der durch die beiden von Ihnen konfigurierten Netzwerkschnittstellen läuft.

4.2.1 Routing unter Windows aktivieren

Standardmäßig ist das Routing zwischen Netzwerkschnittstellen unter Windows nicht aktiviert. Um das Routing unter Windows zu aktivieren, müssen Sie die Windows-Registrierung anpassen. Das kann über den grafischen Registrierungseditor erfolgen, doch die einfachste Lösung besteht darin, den folgenden Befehl als Administrator in der Kommandozeile auszuführen:

```
C> reg add
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters ^

    /v IPEnableRouter /t REG_DWORD /d 1
```

Um das Routing zu deaktivieren, nachdem Sie den gewünschten Verkehr erfasst haben, geben Sie den folgenden Befehl ein:

```
C> reg add
HKLM\System\CurrentControlSet\Services\Tcpip\Parameters ^

    /v IPEnableRouter /t REG_DWORD /d 0
```

Bei Änderungen ist außerdem ein Neustart nötig.

Warnung

Sie müssen bei Änderungen an der Windows-Registrierung sehr vorsichtig sein. Fehlerhafte Änderungen können Windows komplett zerstören und das Booten verhindern! Stellen Sie sicher, dass es ein System-Backup gibt (das Sie mit dem in Windows integrierten Backup-Tool erstellen können), bevor Sie gefährliche Änderungen vornehmen.

4.2.2 Routing unter *nix aktivieren

Um das Routing bei unixoiden Betriebssystemen zu aktivieren, ändern Sie einfach die Einstellung des IP-Routing-Systems mit dem Befehl `sysctl`. (Die Anweisungen sind nicht unbedingt für alle Systeme gleich, doch Sie sollten keine Schwierigkeiten haben, die entsprechenden Anweisungen zu finden.)

Um das IPv4-Routing unter Linux zu aktivieren, führen Sie den folgenden Befehl als root aus (ein Neustart ist nicht nötig; die Änderung wird sofort aktiv):

```
# sysctl net.ipv4.conf.all.forwarding=1
```

Das IPv6-Routing unter Linux aktivieren Sie wie folgt:

```
# sysctl net.ipv6.conf.all.forwarding=1
```

Sie können die Routing-Konfiguration wieder rückgängig machen, indem Sie in den obigen Befehlen die `1` durch eine `0` ersetzen.

Das Routing unter macOS aktivieren Sie wie folgt:

```
> sysctl -w net.inet.ip.forwarding=1
```

4.3 Network Address Translation

Beim Capturing von Netzwerkverkehr könnten Sie feststellen, dass Sie zwar ausgehenden Verkehr erfassen können, nicht aber den eingehenden Verkehr. Der Grund dafür liegt darin, dass ein Upstream-Router die Route des ursprünglichen Quellnetzwerks nicht kennt. Daher verwirft er entweder den Verkehr oder er leitet ihn an ein anderes Netzwerk weiter. Sie können dieser Situation per *Network Address Translation (NAT)* entgegenwirken. Diese Technik modifiziert die Informationen der Quell- und Zieladressen von IP und höheren Protokollen wie TCP. NAT wird ausgiebig genutzt, um den beschränkten IPv4-Adressraum zu erweitern, indem man mehrere Geräte hinter einer einzelnen öffentlichen Adresse versteckt.

NAT kann darüber hinaus die Netzwerkkonfiguration vereinfachen und sicherer machen. Bei aktiver NAT können Sie beliebig viele Geräte hinter einer einzelnen NAT-IP-Adresse betreiben und nur diese öffentliche IP-Adresse pflegen.

Heutzutage sind zwei Arten von NAT üblich: *Source NAT (SNAT)* und *Destination NAT (DNAT)*. Der Unterschied zwischen den beiden besteht darin, welche Adresse bei der NAT-Verarbeitung des Netzwerkverkehrs modifiziert wird. SNAT (auch *Masquerading* genannt) verändert die IP-Quelladresse, während DNAT die Zieladresse ändert.

4.3.1 SNAT aktivieren

Soll ein Router mehrere Rechner hinter einer einzigen IP-Adresse verstecken, verwenden Sie SNAT. Ist SNAT aktiv, wird bei Verkehr, der über die externe Netzwerkschnittstelle läuft, die Quell-IP-Adresse des Pakets so umgeschrieben, dass sie der einzelnen durch SNAT bereitgestellten IP-Adresse entspricht.

SNAT zu implementieren kann nützlich sein, wenn Sie Verkehr an ein Netzwerk routen wollen, über das Sie keine Kontrolle haben. Wie Sie wissen, müssen beide Knoten im Netzwerk korrekte Routing-Informationen besitzen, damit der Verkehr zwischen den Knoten übertragen werden kann. Ist die Routing-Information nicht korrekt, läuft der Verkehr im schlimmsten Fall nur in eine Richtung. Doch auch im besten Fall werden Sie den Verkehr nur in einer Richtung erfassen können, weil die andere Richtung über einen alternativen Pfad geroutet wird.

SNAT löst dieses Problem, indem es die Quelladresse des Verkehrs durch eine IP-Adresse ersetzt, an die der Zielknoten die Daten senden kann – üblicherweise diejenige, die der externen Adresse des Routers zugewiesen ist. Auf diese Weise kann der Zielknoten den Verkehr zurück an den Router senden. Abbildung 4–2 zeigt ein einfaches SNAT-Beispiel.

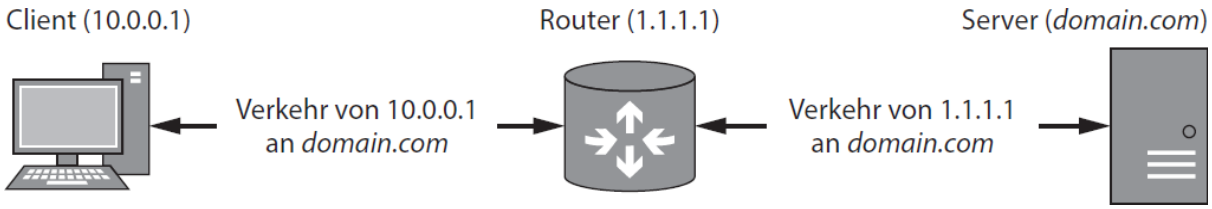

Abb. 4–2 *SNAT von einem Client an einen Server*

Will der Client ein Paket an einen Server in einem anderen Netzwerk übertragen, sendet er es an den mit SNAT konfigurierten Router. Wenn der Router das Paket

vom Client empfängt, entspricht die Quelladresse der des Clients (10.0.0.1) und das Ziel ist der Server (die aus *domain.com* aufgelöste Adresse). An diesem Punkt wird SNAT genutzt: Der Router ändert die Quelladresse des Pakets in seine eigene Adresse (1.1.1.1) ab und leitet das Paket an den Server weiter.

Wenn der Server das Paket empfängt, geht er davon aus, dass es vom Router kommt, d. h., wenn er ein Paket zurückschicken will, sendet er es an 1.1.1.1. Der Router empfängt das Paket, erkennt, dass es von einer NAT-Verbindung stammt (basierend auf Zieladresse und Portnummer) und hebt die Adressänderung wieder auf, d. h., er wandelt 1.1.1.1 wieder in die ursprüngliche Clientadresse 10.0.0.1 um. Zum Schluss kann das Paket an den eigentlichen Client weitergeleitet werden, ohne dass der Server etwas über den Client oder das Routing in diesem Netzwerk weiß.

4.3.2 SNAT unter Linux konfigurieren

Zwar lässt sich SNAT unter Windows und macOS per Internetverbindungsfreigabe (Internet Connection Sharing) konfigurieren, ich beschreibe aber nur, wie man SNAT unter Linux einrichtet, weil es die am einfachsten zu erläuternde Plattform ist und die flexibelste Netzwerkkonfiguration bietet.

Vor der SNAT-Konfiguration müssen Sie Folgendes tun:

- Aktivieren Sie das IP-Routing wie vorhin in diesem Kapitel beschrieben.
- Ermitteln Sie den Namen der ausgehenden Netzwerkschnittstelle, für die Sie SNAT konfigurieren wollen. Sie können dazu den `ifconfig`-Befehl verwenden. Die ausgehende Schnittstelle hat einen Namen wie `eth0`.
- Notieren Sie die IP-Adresse, die an die ausgehende Schnittstelle gebunden ist und von `ifconfig` zurückgegeben wird.

Nun können Sie die NAT-Regeln mit `iptables` definieren. (Der `iptables`-Befehl ist bei Ihrer Linux-Distribution sehr wahrscheinlich bereits installiert.) Zuerst löschen Sie alle vorhandenen NAT-Regeln aus `iptables`, indem Sie den folgenden Befehl mit Root-Rechten ausführen:

```
# iptables -t nat -F
```

Hat die ausgehende Netzwerkschnittstelle eine feste Adresse, führen Sie den folgenden Befehl als root aus, um SNAT zu aktivieren. Ersetzen Sie *INTNAME* durch den Namen der ausgehenden Schnittstelle und *INTIP* mit der dieser Schnittstelle zugewiesenen IP-Adresse.

```
# iptables -t nat -A POSTROUTING -o INTNAME -j SNAT —to
INTIP
```

Wird die IP-Adresse hingegen dynamisch zugewiesen (etwa über DHCP oder über eine Wählverbindung), verwenden Sie den folgenden Befehl, um die ausgehende IP-Adresse automatisch zu ermitteln:

```
# iptables -t nat -A POSTROUTING -o INTNAME -j MASQUERADE
```

4.3.3 DNAT aktivieren

DNAT ist nützlich, wenn Sie den Verkehr an einen Proxy oder einen anderen Dienst umleiten wollen oder bevor Sie den Verkehr an sein eigentliches Ziel weiterleiten. DNAT ändert die IP-Adresse des Ziels und optional auch den Zielport. Sie können DNAT nutzen, um spezifischen Verkehr an ein anderes Ziel umzuleiten. Abbildung 4–3 zeigt, wie man Verkehr sowohl vom Router als auch vom Server auf einen Proxy an 192.168.0.10 umleitet, um eine Man-in-the-Middle-Analyse durchzuführen.

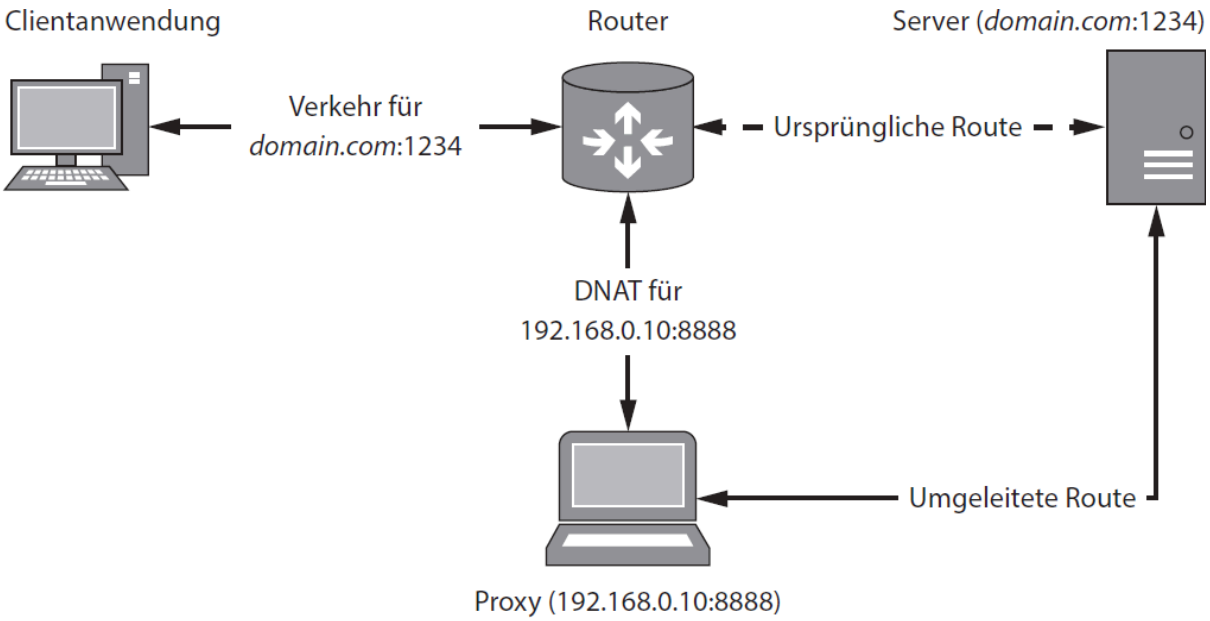

Abb. 4–3 *DNAT für einen Proxy*

Abbildung 4–3 zeigt eine Clientanwendung, die den Verkehr über einen Router an *domain.com*, Port 1234 sendet. Wird ein Paket vom Router empfangen, würde er es normalerweise einfach an das Ziel weiterleiten. Da DNAT aber die Zieladresse und den Port in 192.168.0.10:8888 ändert, wendet der Router seine Weiterleitungsregeln an und sendet das Paket an den Proxy-Rechner, der den Verkehr erfassen kann. Der Proxy baut dann eine neue Verbindung zum Server auf und leitet das vom Client kommende Paket an den Server weiter. Der gesamte Verkehr zwischen dem Client und dem Server kann erfasst und manipuliert werden.

Die DNAT-Konfiguration hängt vom Betriebssystem ab, auf dem der Router läuft. (Unter Windows haben Sie wahrscheinlich kein Glück, weil die für die DNAT-Unterstützung benötigte Funktionalität dem Benutzer nicht zur Verfügung gestellt wird.) Das Setup variiert bei den verschiedenen unixoiden Betriebssystemen und macOS deutlich, weshalb ich nur die DNAT-Konfiguration unter Linux behandle. Zuerst löschen Sie alle existierenden NAT-Regeln durch Eingabe des folgenden Befehls:

```
# iptables -t nat -F
```

Als Nächstes führen Sie den folgenden Befehl als root aus, wobei Sie *ORIGIP* durch die IP-Adresse ersetzen, deren Verkehr Sie umleiten wollen, und *NEWIP* durch die neue Zieladresse, an die der Verkehr geleitet werden soll.

```
# iptables -t nat -A PREROUTING -d ORIGIP -j DNAT –to-
destination NEWIP
```

Die neue NAT-Regel leitet jedes an *ORIGIP* gerichtete Paket an *NEWIP* um. (Da die DNAT unter Linux vor den normalen Routing-Regeln erfolgt, können Sie bedenkenlos eine lokale Netzwerkadresse angeben. Die DNAT-Regel hat keinen Einfluss auf Verkehr, der direkt von Linux gesendet wird.) Um die Regel nur auf TCP oder UDP anzuwenden, ändern Sie den Befehl wie folgt:

```
iptables -t nat -A PREROUTING -p PROTO -d ORIGIP –dport
ORIGPORT -j DNAT \

   –to-destination NEWIP:NEWPORT
```

Der Platzhalter *PROTO* (für Protokoll) muss `tcp` oder `udp` lauten, je nachdem, welches IP-Protokoll Sie mit der DNAT-Regel umleiten wollen. Die Werte für *ORIGIP* und *NEWIP* bleiben gleich.

Sie können auch *ORIGPORT* und *NEWPORT* konfigurieren, wenn Sie den Zielport ändern wollen. Wird *NEWPORT* nicht angegeben, ändert sich nur die IP-Adresse.

4.4 Verkehr an ein Gateway weiterleiten

Sie haben Ihr Gateway so eingerichtet, dass es den Verkehr erfassen und modifizieren kann. Alles scheint zu funktionieren, doch es gibt ein Problem: Sie können nicht einfach so die Netzwerkkonfiguration des Gerätes ändern, dessen Daten Sie abgreifen wollen. Auch sind Ihre Möglichkeiten beschränkt, die Netzwerkkonfiguration der Einheit zu ändern, mit dem dieses Gerät verbunden ist. Sie müssen das sendende Gerät also irgendwie dazu bringen, Verkehr über Ihr Gateway zu leiten. Sie erreichen das durch Paket-Spoofing von DHCP oder ARP (*Address Resolution Protocol)* im lokalen Netzwerk.

4.4.1 DHCP-Spoofing

DHCP wurde entworfen, um die Knoten in einem IP-Netzwerk automatisch mit Konfigurationsinformationen zu versorgen. Wenn Sie also den DHCP-Verkehr fälschen können, können Sie die Netzwerkkonfiguration eines Knotens aus der Ferne ändern. Wird DHCP genutzt, kann die an den Knoten gesendete Netzwerkkonfiguration eine IP-Adresse und ein Standard-Gateway umfassen, aber auch Routing-Tabellen, den Standard-DNS-Server und weitere Parameter. Verwendet das zu testende Gerät DHCP zur Konfiguration der Netzwerkschnittstelle, macht es diese Flexibilität sehr leicht, eine eigene Konfiguration zu senden, die ein einfaches Abgreifen des Verkehrs erlaubt.

DHCP nutzt das UDP-Protokoll, um Requests von und an einen DHCP-Service im lokalen Netzwerk zu übertragen. Vier Arten von DHCP-Paketen werden gesendet, um die Netzwerkkonfiguration auszuhandeln:

- **Discover**

  Wird an alle Knoten des IP-Netzwerks gesendet, um einen DHCP-Server aufzuspüren.

- **Offer**

  Wird vom DHCP-Server an den Knoten geschickt, der das Discovery-Paket gesendet hat, um eine Netzwerkkonfiguration anzubieten.

- **Request**

  Wird vom ursprünglichen Knoten gesendet, um das Angebot (Offer) anzunehmen.

- **Acknowledgment**

  Wird vom Server gesendet, um den Abschluss der Konfiguration zu bestätigen.

Interessant an DHCP ist, dass es ein authentifizierungs- und verbindungsfreies Protokoll für die Konfiguration verwendet. Selbst wenn ein DHCP-Server im Netzwerk existiert, sollten Sie den Konfigurationsprozess fälschen und die Netzwerkkonfiguration des Knotens ändern können, einschließlich der Adresse des Standard-Gateways (das Sie kontrollieren). Diese Technik bezeichnet man als *DHCP-Spoofing*.

Um das DHCP-Spoofing durchzuführen, verwenden wir *Ettercap*, ein freies Tool, das für die meisten Betriebssysteme verfügbar ist (auch wenn Windows

offiziell nicht unterstützt wird).

1. Unter Linux starten Sie Ettercap im grafischen Modus als root:

```
# ettercap -G
```

Es erscheint die Ettercap-GUI wie in Abbildung 4–4.

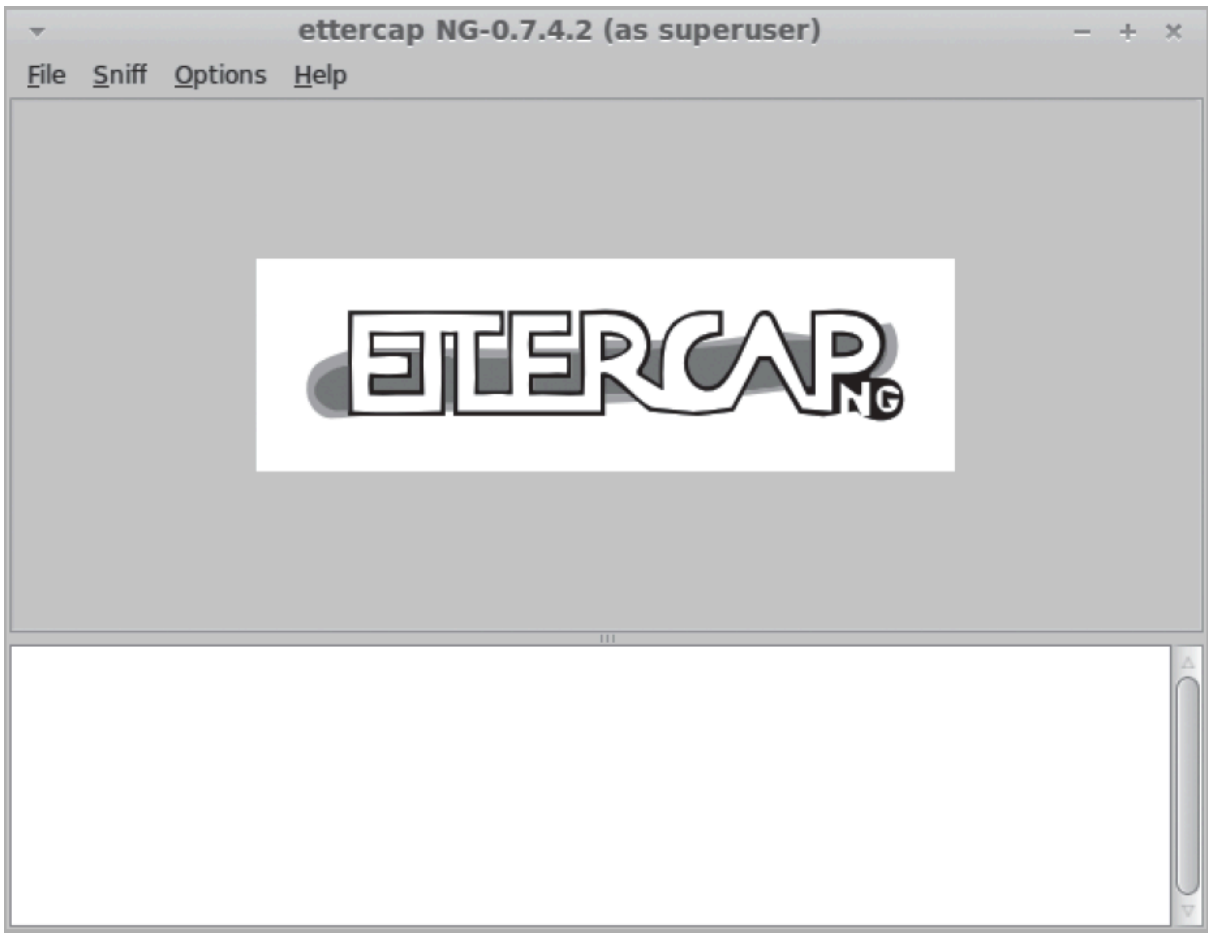

Abb. 4–4 *Die Haupt-GUI von Ettercap*

2. Konfigurieren Sie Ettercaps Sniffing-Modus über **Sniff ▸ Unified Sniffing**.
3. Der Dialog in Abbildung 4–5 fordert Sie auf, die Netzwerkschnittstelle für das Sniffing auszuwählen. Wählen Sie diejenige aus, an der das DHCP-Spoofing erfolgen soll. (Achten Sie auf die korrekte Konfiguration des Netzwerks der Schnittstelle, da Ettercap automatisch die konfigurierte IP-Adresse der Schnittstelle als DHCP-Standard-Gateway sendet.)

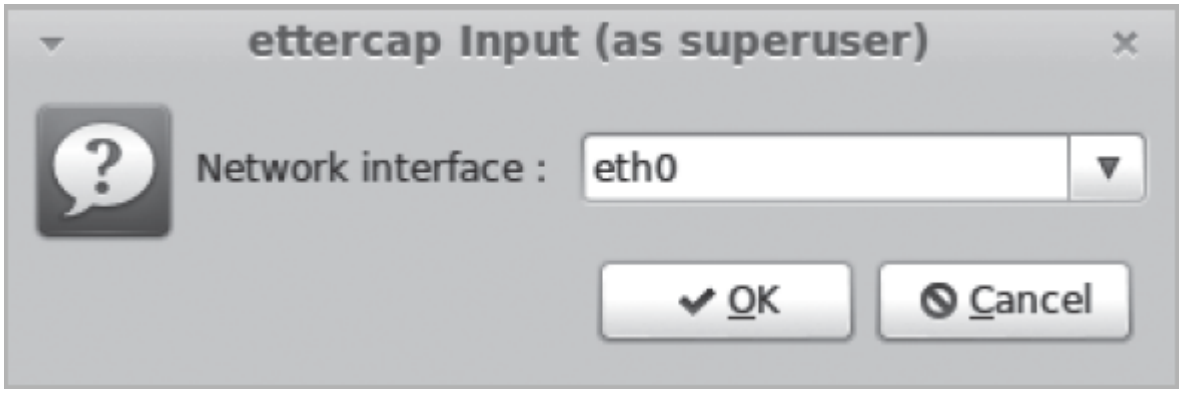

Abb. 4–5 *Sniffing-Interface wählen*

4. Aktivieren Sie das DHCP-Spoofing über **MITM** ▸ **DHCP Spoofing**. Der Dialog aus Abbildung 4–6 erscheint, über den Sie die DHCP-Spoofing-Optionen einstellen können.

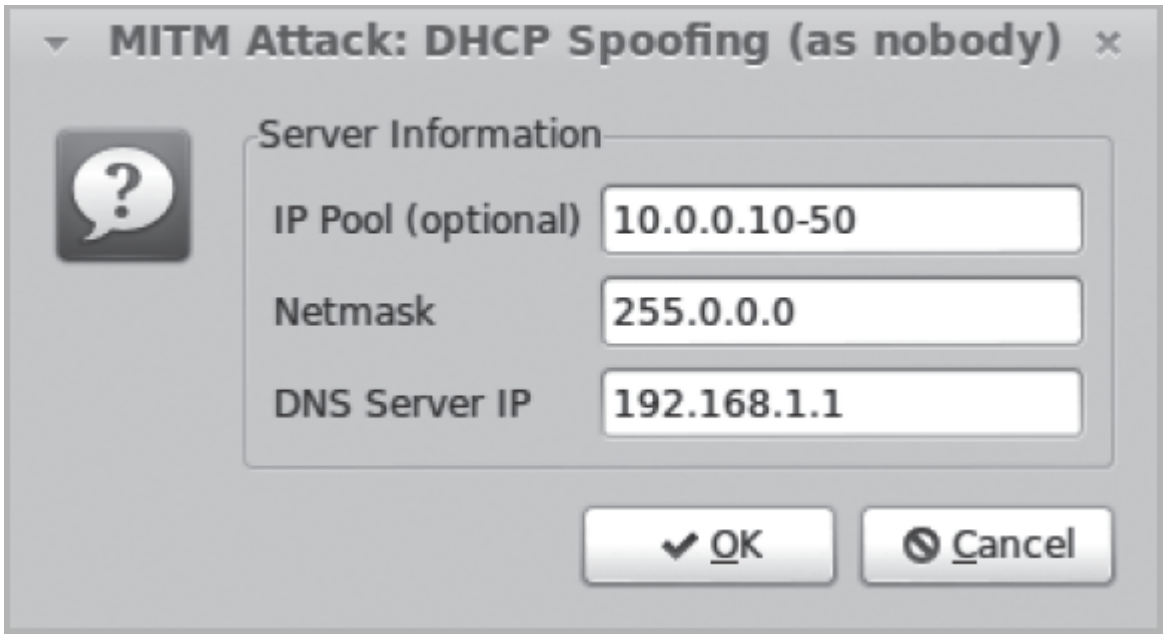

Abb. 4–6 *DHCP-Spoofing konfigurieren*

5. Das Feld IP-Pool legt den Bereich von IP-Adressen fest, die bei DHCP-Requests zurückgegeben werden. Tragen Sie den IP-Adressbereich ein, den Sie für die Netzwerkschnittstelle konfiguriert haben, die den Verkehr erfasst. In Abbildung 4–6 ist der Wert für den IP-Pool z. B. auf 10.0.0.10-50 gesetzt (das Minuszeichen legt alle Adressen innerhalb dieser Werte fest), d. h., wir geben IP-Adressen von 10.0.0.10 bis 10.0.0.50 (einschließlich) zurück. Stellen Sie die Netzmaske entsprechend der Netzmaske Ihres Netzwerks ein, um Konflikte zu vermeiden. Tragen Sie einen DNS-Server Ihrer Wahl ein.

6. Starten Sie das Sniffing über **Start** ▸ **Start sniffing**. Ist das DHCP-Spoofing bei einem Gerät erfolgreich, sollte das Ettercap-Logfenster wie in Abbildung 4–7 aussehen. Die maßgebliche Zeile ist das `fake` ACK, das von Ettercap als Response auf den DHCP-Request gesendet wurde.

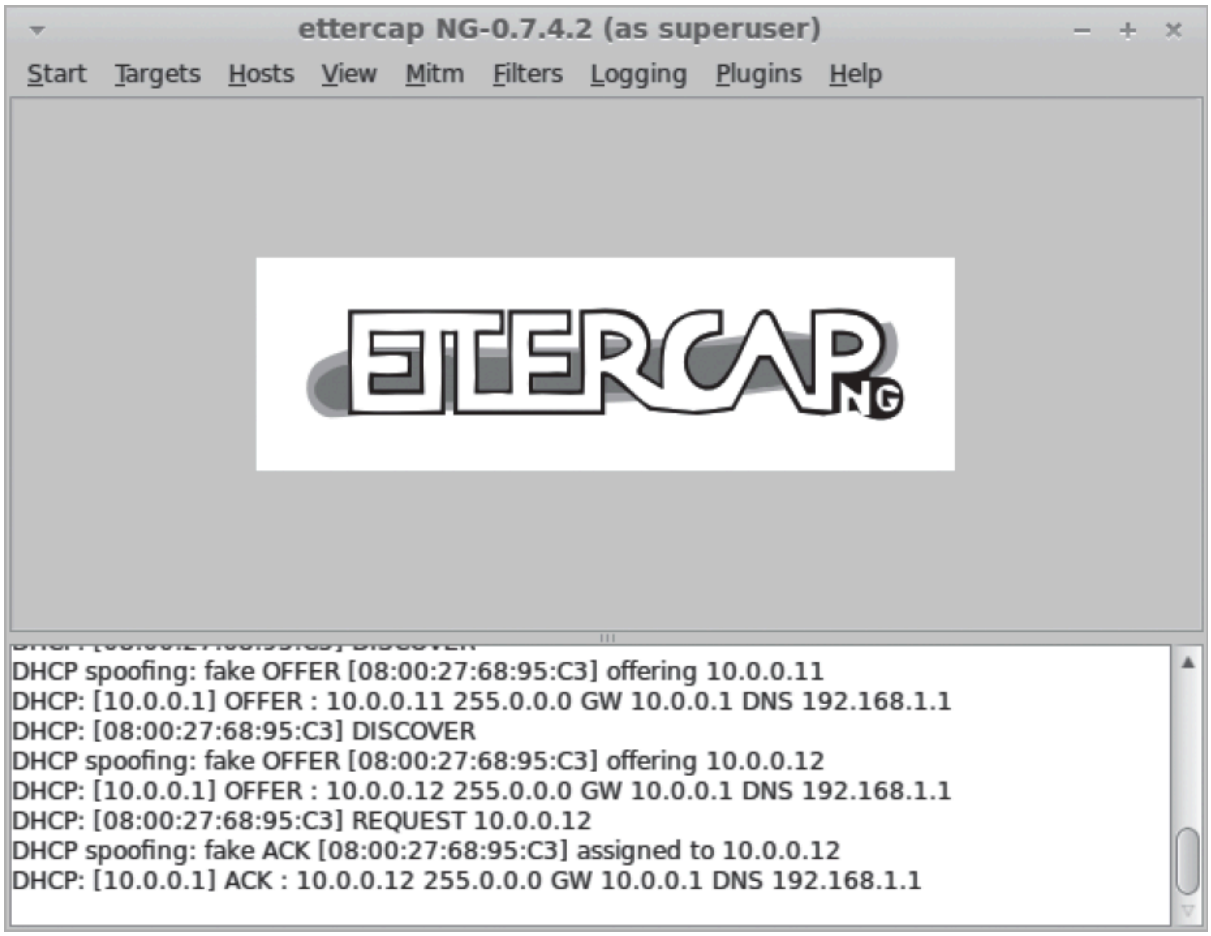

Abb. 4–7 *Erfolgreiches DHCP-Spoofing*

Mehr gibt es beim DHCP-Spoofing mit Ettercap nicht zu tun. Es kann eine sehr leistungsfähige Lösung sein, wenn Sie keine andere Möglichkeit haben und wenn ein DHCP-Server im angegriffenen Netzwerk läuft.

4.4.2 ARP-Poisoning

ARP (Address Resolution Protocol) ist für den Betrieb von über Ethernet laufenden IP-Netzwerken sehr wichtig, weil ARP die Ethernet-Adresse für eine gegebene IP-Adresse ermittelt. Ohne ARP wäre es sehr schwierig, IP-Verkehr effizient über Ethernet zu übertragen. ARP funktioniert wie folgt: Möchte ein Knoten im gleichen Ethernet-Netzwerk mit einem anderen Knoten kommunizieren, muss er die IP-Adresse auf eine Ethernet-MAC-Adresse abbilden können. Erst durch die MAC-Adresse kennt Ethernet den Zielknoten, an den die

Daten gesendet werden sollen. Der Knoten erzeugt ein ARP-Request-Paket (siehe Abb. 4–8), die die 6-Byte-MAC-Adresse des Knotens, seine aktuelle IP-Adresse und die IP-Adresse des Zielknotens enthält. Das Paket wird im Ethernet an die MAC-Zieladresse ff:ff:ff:ff:ff:ff gesendet, was der definierten Broadcast-Adresse entspricht. Normalerweise verarbeitet eine Ethernet-Schnittstelle nur Pakete, deren Zieladresse mit ihrer eigenen Adresse übereinstimmt, doch wenn die Zieladresse der Broadcast-Adresse entspricht, wird das Paket ebenfalls verarbeitet.

Hat einer der Empfänger dieser Broadcast-Nachricht diese Ziel-IP-Adresse, kann er eine entsprechende ARP-Response zurückgeben (siehe Abb. 4–9). Diese Response ist nahezu identisch, nur dass die Felder für Sender und Empfänger vertauscht sind. Weil die IP-Adresse des Senders der ursprünglich angeforderten Ziel-IP-Adresse entsprechen sollte, kann die anfordernde Seite die MAC-Adresse des Senders speichern und für die zukünftige Netzwerkkommunikation nutzen, ohne den ARP-Request erneut senden zu müssen.

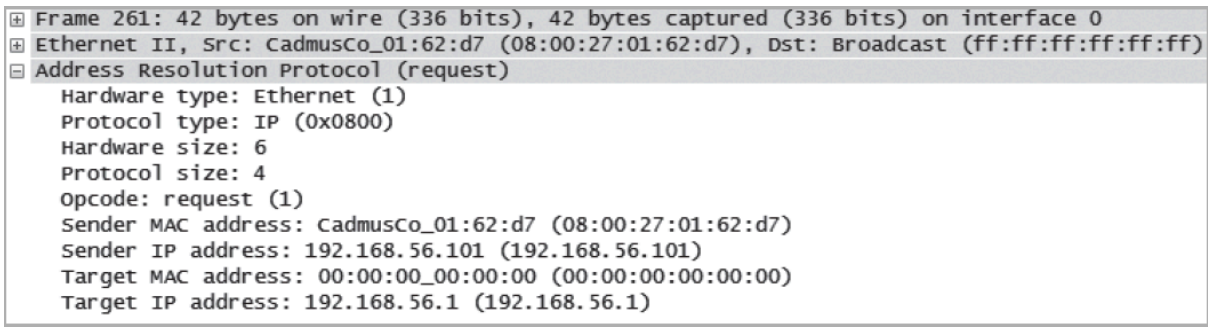

Abb. 4–8 *Beispiel für ein ARP-Request-Paket*

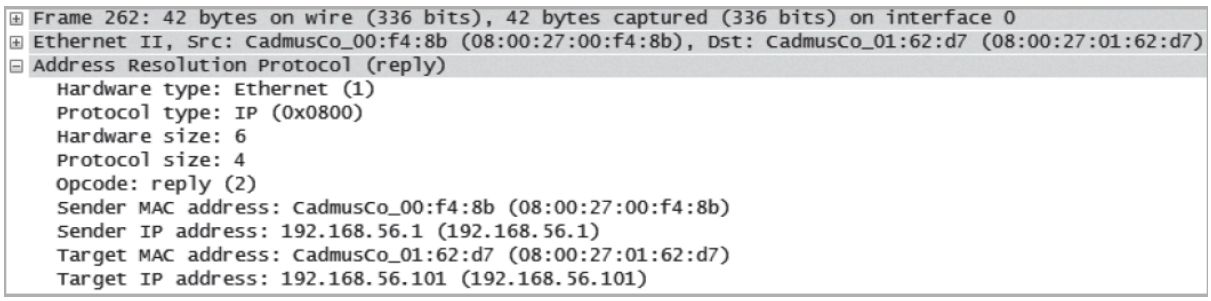

Abb. 4–9 *Beispiel für eine ARP-Response*

Wie kann man ARP-Poisoning nun zum eigenen Vorteil nutzen? Wie bei DHCP gibt es keine Authentifizierung für ARP-Pakete, die bewusst an alle Knoten des Ethernet-Netzwerks gesendet werden. Sie können den Zielknoten also darüber informieren, dass Sie eine bestimmte IP-Adresse haben und sicherstellen, dass der Knoten den Verkehr an Ihr falsches Gateway weiterleitet, indem Sie gefälschte ARP-Pakete senden, um den ARP-Cache des Zielknotens zu

»vergiften« (engl. poisoning). Zum Fälschen der Pakete können Sie Ettercap verwenden, wie in Abbildung 4–10 zu sehen.

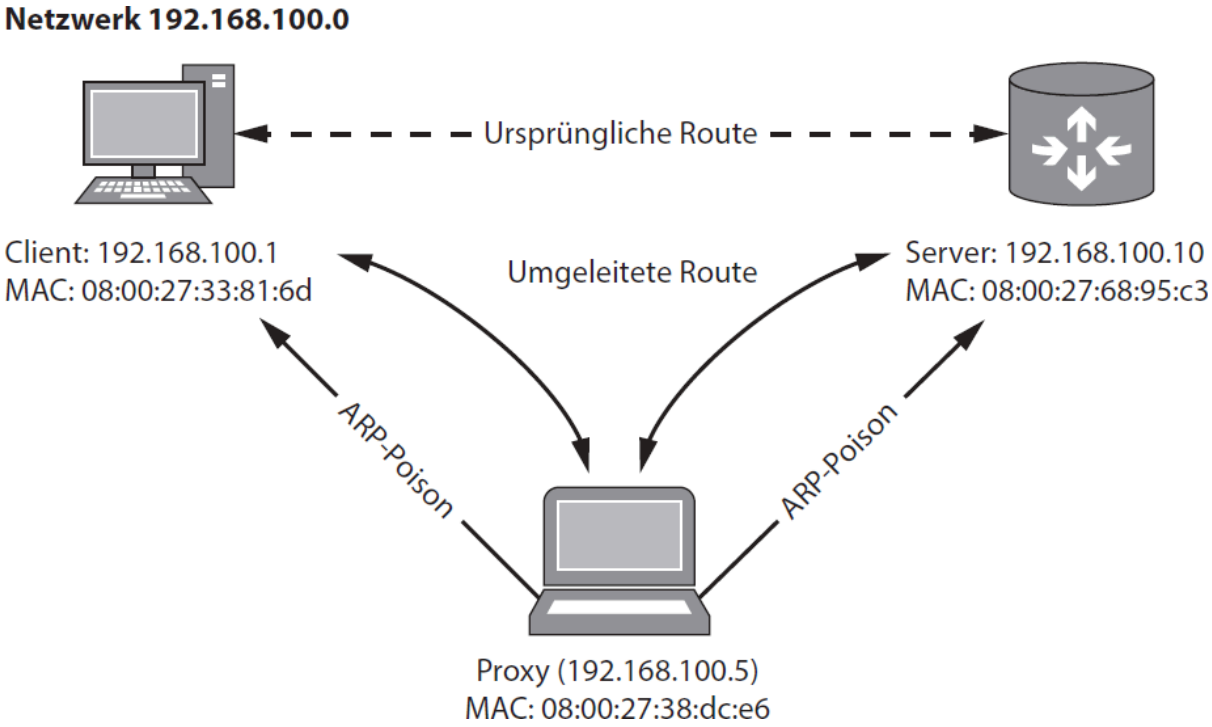

Abb. 4–10 *ARP-Poisoning*

In Abbildung 4–10 sendet Ettercap im lokalen Netzwerk gefälschte ARP-Pakete an den Client und an den Router. Ist das Spoofing erfolgreich, ändern diese ARP-Pakete den ARP-Cache beider Rechner so ab, dass die Einträge auf Ihren Proxy verweisen.

Warnung

Stellen Sie sicher, dass die ARP-Pakete sowohl für den Client als auch für den Router gefälscht werden, damit Sie beide Seiten der Kommunikation erfassen können. Soll nur eine Seite der Kommunikation abgefangen werden, müssen Sie natürlich nur eine der beiden Knoten »vergiften«.

Das ARP-Poisoning starten Sie mit den folgenden Schritten:

1. Starten Sie Ettercap und wechseln Sie wie beim DHCP-Spoofing in den **Unified Sniffing**-Modus.
2. Wählen Sie die Netzwerkschnittstelle aus, die Sie angreifen wollen (diejenige, die mit dem Netzwerk verbunden ist, dessen Knoten Sie angreifen wollen).
3. Konfigurieren Sie eine Liste von Hosts, auf die das ARP-Poisoning angewandt werden soll. Die einfachste Möglichkeit, eine solche Liste zu

erzeugen, besteht darin, sie durch Ettercap über **Hosts ▸ Scan For Hosts** scannen zu lassen. Je nach Größe des Netzwerks kann der Scan ein paar Sekunden oder auch Stunden dauern. Ist der Scan abgeschlossen, wählen Sie **Hosts ▸ Host List**. Ein Dialog wie in Abbildung 4–11 erscheint.

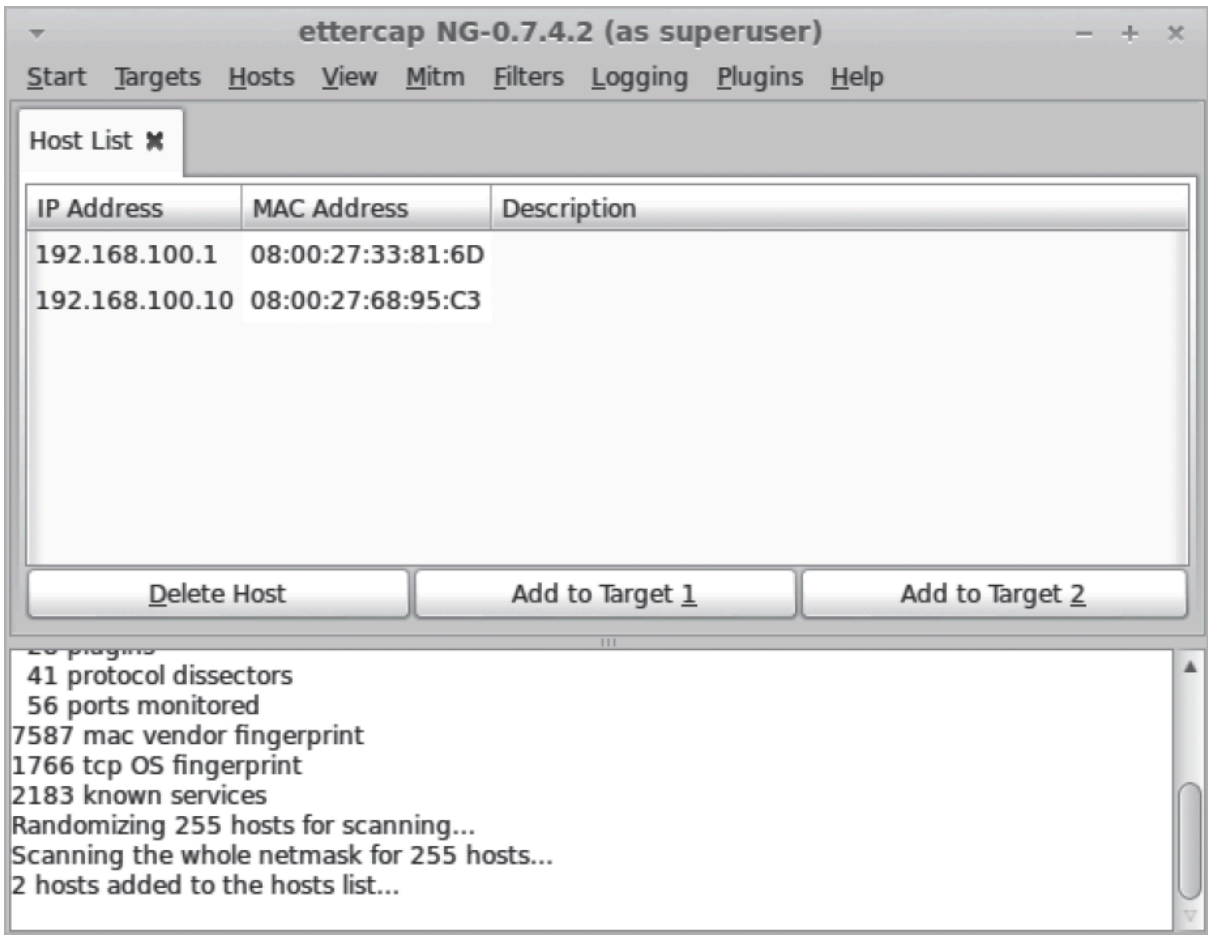

Abb. 4–11 *Liste entdeckter Hosts*

Wie Sie in Abbildung 4–11 sehen, wurden zwei Hosts gefunden. In diesem Beispiel ist einer der Client, dessen Daten Sie abgreifen wollen. Er hat die IP-Adresse 192.168.100.1 und die MAC-Adresse 08:00:27:33:81:6d. Der andere Knoten ist das Gateway zum Internet mit der IP-Adresse 192.168.100.10 und der MAC-Adresse 08:00:27:68:95:c3. Wahrscheinlich kennen Sie die IP-Adressen der Netzwerkgeräte bereits, d. h., Sie können einfach feststellen, welches die lokale und welches die entfernte Maschine ist.

4. Wählen Sie Ihre Ziele. Wählen Sie einen der Hosts aus der Liste und klicken Sie auf **Add to Target 1**. Wählen Sie den anderen anzugreifenden Host und klicken Sie auf **Add to Target 2**. (Target 1 und Target 2 grenzen

Client und Gateway ab.) Das sollte das ARP-Poisoning in einer Richtung aktivieren, bei dem Daten von Target 1 an Target 2 umgeleitet wird.

5. Starten Sie das ARP-Poisoning über **MITM ▸ ARP poisoning.** Ein Dialog erscheint. Akzeptieren Sie die Voreinstellungen und klicken Sie auf **OK**. Ettercap versucht nun, den ARP-Cache des gewählten Ziels zu fälschen. Eventuell wird das ARP-Poisoning nicht sofort funktionieren, weil der ARP-Cache noch aktualisiert werden muss. Ist das Poisoning erfolgreich, sieht der Clientknoten etwa so aus, wie in Abbildung 4–12.

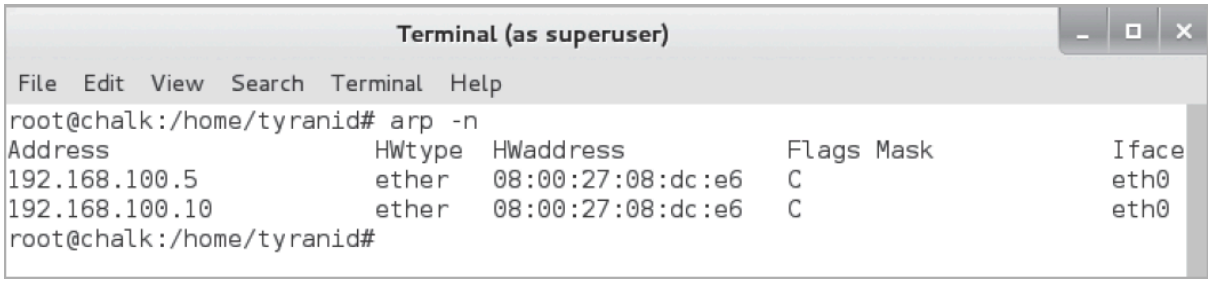

Abb. 4–12 *Erfolgreiches ARP-Poisoning*

Abbildung 4–12 zeigt, dass der Router an IP 192.168.100.10 vergiftet wurde. Seine MAC-Hardwareadresse wurde in die MAC-Adresse des Proxys 08:00:27:08:dc:e6 geändert. (Sehen Sie sich zum Vergleich den entsprechenden Eintrag aus Abb. 4–11 an.) Jeder vom Client an den Router gesendete Verkehr läuft nun über den Proxy (zu erkennen an der MAC-Adresse von 192.168.100.5). Der Proxy kann den Verkehr an das eigentliche Ziel weiterleiten, nachdem er ihn erfasst oder modifiziert hat.

Ein Vorteil von ARP-Poisoning gegenüber DHCP-Spoofing besteht darin, das Sie Knoten im lokalen Netzwerk dazu bringen können, mit Ihrem Gateway zu kommunizieren, selbst wenn das Ziel im lokalen Netzwerk liegt. ARP-Poisoning muss die Verbindung zwischen dem Knoten und dem externen Gateway nicht fälschen, wenn Sie das nicht wünschen.

4.5 Am Ende dieses Kapitels

In diesem Kapitel haben Sie einige zusätzliche Möglichkeiten kennengelernt, den Verkehr zwischen Client und Server zu erfassen und zu modifizieren. Ich habe zuerst erläutert, wie Sie Ihr Betriebssystem als IP-Gateway konfigurieren, denn wenn Sie Verkehr durch ein eigenes Gateway leiten können, stehen Ihnen eine Vielzahl von Techniken zur Verfügung.

Ein Gerät dazu zu bewegen, Verkehr an Ihre Capturing-Vorrichtung zu senden, ist natürlich nicht immer einfach. Der Einsatz von Techniken wie DHCP-Spoofing und ARP-Poisoning ist daher wichtig, um sicherzustellen, dass der Verkehr über Ihre Vorrichtung läuft, und nicht direkt über das Internet. Wie Sie gesehen haben, benötigen wir dazu glücklicherweise keine maßgeschneiderten Tools. Alle erforderlichen Tools sind bereits im Betriebssystem vorhanden (insbesondere unter Linux) oder können einfach heruntergeladen werden.

Index

B

C

E

F

G

H

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Ziffern

Sonderzeichen