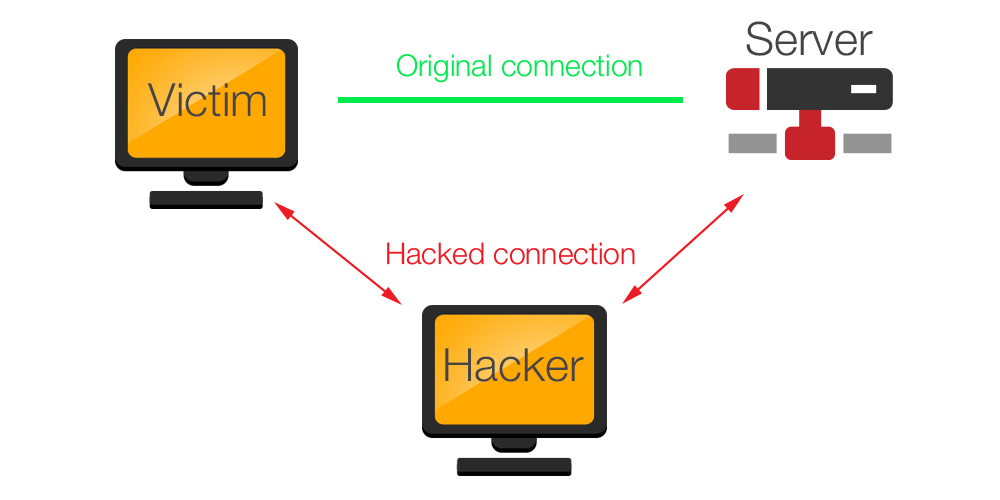
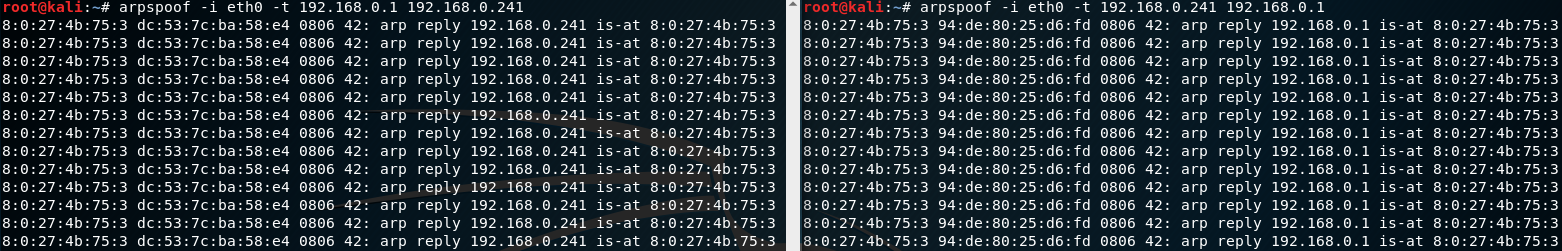
|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** ARP-Spoofing (Man-In-The-Middle Angriff) | **Hauptverantwortlicher**: Daniel Nagel |
| **Ziel des Angriffs**: Datendiebstahl | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure : Opfer, Angreifer **Fallbeschreibung**:  Das Opfer surft in einem öffentlichen WLAN im Internet. Ein neugieriger Angreifer möchte wissen was das Opfer so treibt. Daher startet der Angreifer einen „Man-In-The-Middle“-Angriff mittels ARP-Spoofing. Und gibt sich als Router des öffentlichen Netzwerkes aus. | |
| *1 . Ausgangssituation:* | |

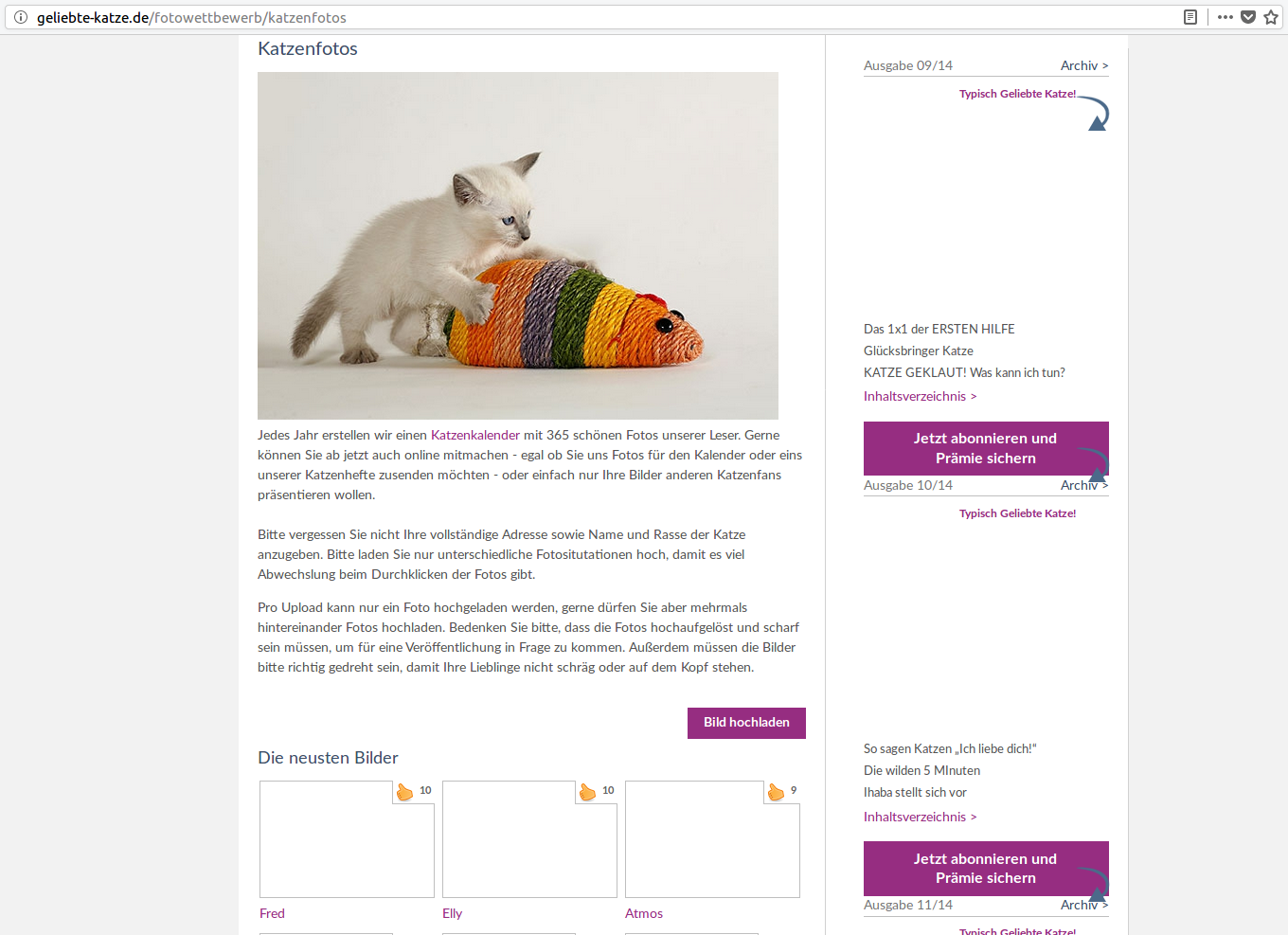


|  |
| --- |
| *2. Vorbereitung des Angriffs* |
| Zunächst werden die ARP-Tabellen „vergiftet“. Der Angreifer gibt sich für das Opfer als der Router des Netzwerkes aus. Für den Router gibt sich der Angreifer als der eigentliche Client aus.  Benötigt werden hierfür die IP-Adressen des Opfers und des Routers.  Jetzt sendet der Angreifer durchgehend seine MAC-Adresse an das Opfer mit der IP-Adresse des Routers. Genauso sendet der Angreifer seine MAC-Adresse an den Router mit der IP-Adresse des Opfers.  Damit der Angreifer als Router arbeiten kann, muss das IP-Forwarding aktiviert werden, dafür wird in der Datei /proc/sys/net/ipv4/ip\_forward der Wert 1 eingetragen. |

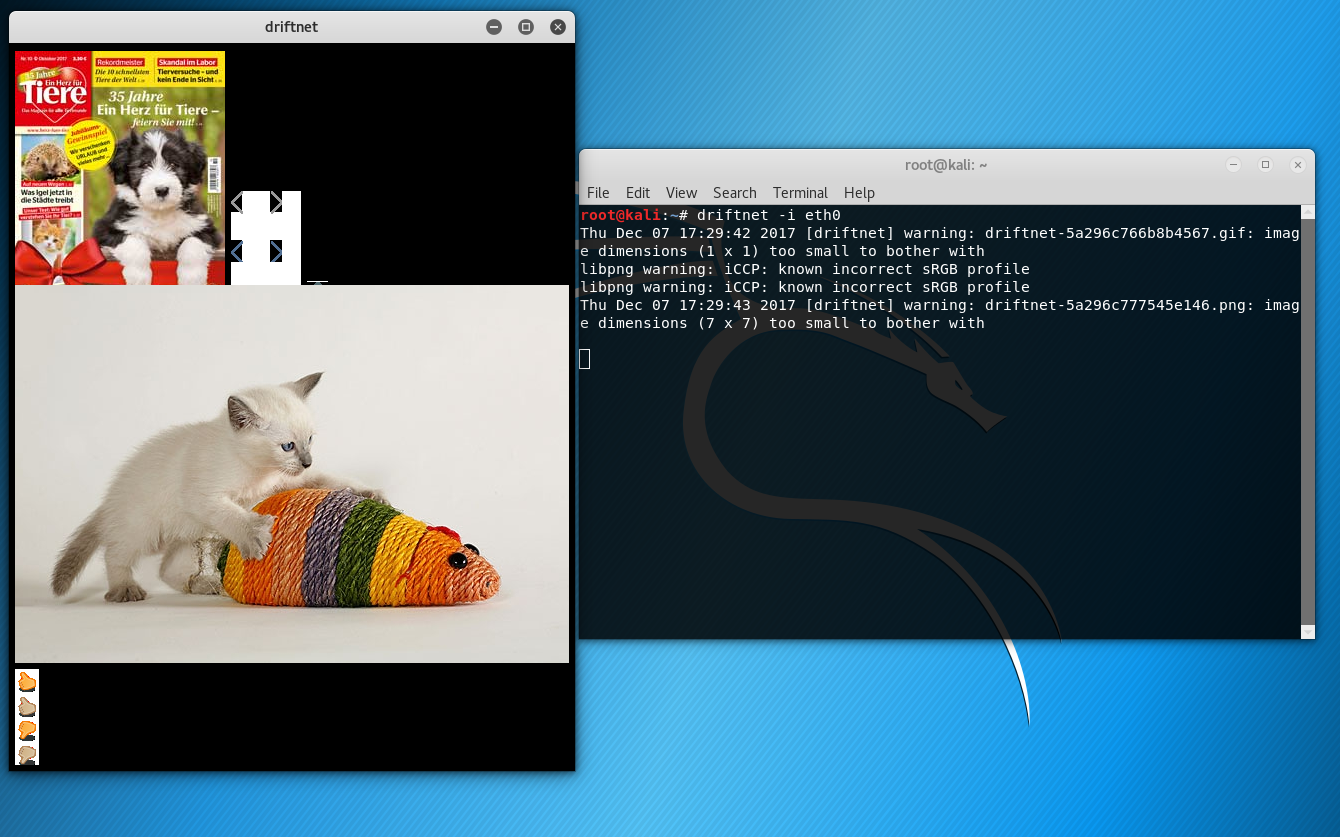
|  |
| --- |
| Das ARP-Spoofing wird mithilfe des Programms „arpspoof“ erreicht.  Die Option -i legt das Interface fest, auf dem gehorcht werden soll.  *Die Option -t <IP-Adresse des Geräts, welches vergiftet werden soll> <vorgetäuschte IP> legt fest als wen sich der Angreifer ausgibt.* |



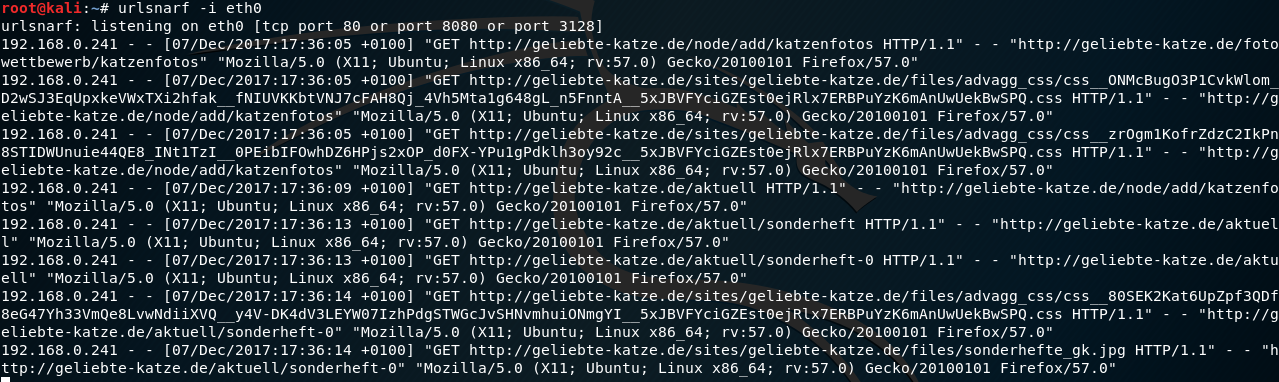
|  |
| --- |
| *3.Durchführen des Angriffs* |
| Das Opfer ist ein Katzenfan und schaut sich daher Bilder von Katzen an. |



|  |
| --- |
| *Der Angreifer kann sich genau die selben Bilder mit dem Programm ‚driftnet‘ anschauen.*  *Die Option -i gibt die Netzwerkschnittstelle an auf der gehorcht werden soll.* |



|  |
| --- |
| Die Webseiten Daten kann sich der Angreifer mit dem Programm „urlsnarf“ anschauen.  *Die Option -i gibt die Netzwerkschnittstelle an auf der gehorcht werden soll.* |



|  |
| --- |
| *4. Limitierungen des Angriffs* |
| Der Angriff funktioniert nur bei unverschlüsselten Verbindungen. Besucht das Opfer etwa eine Seite mittels https-Protokoll können keinerlei Daten eingesehen werden. |