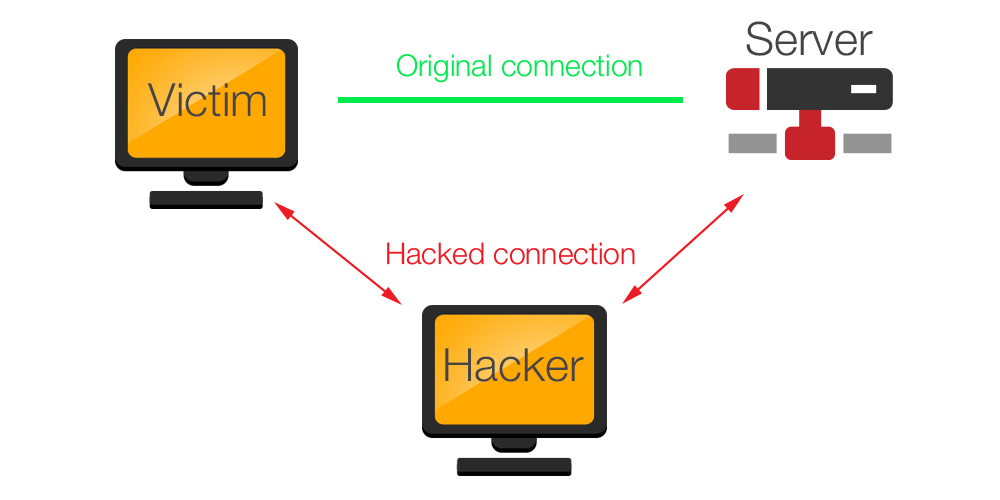
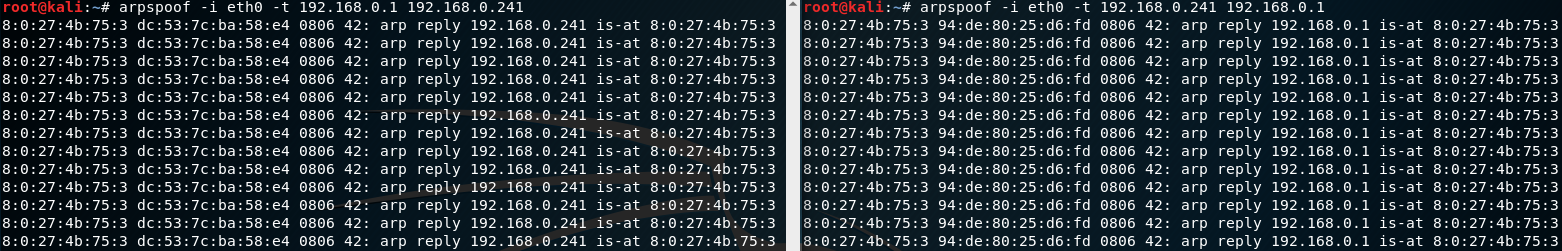
|  |  |
| --- | --- |
| **Angriffsbeschreibung** | |
| **Name:** ARP-Spoofing (Man-In-The-Middle Angriff) | **Hauptverantwortlicher**: Daniel Nagel |
| **Ziel des Angriffs**: Datendiebstahl | **Gefährdete Personengruppen**: Alle |
| **Beispiel eines Angriffsszenarios** | |
| Akteure : Opfer, Angreifer **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:* | |

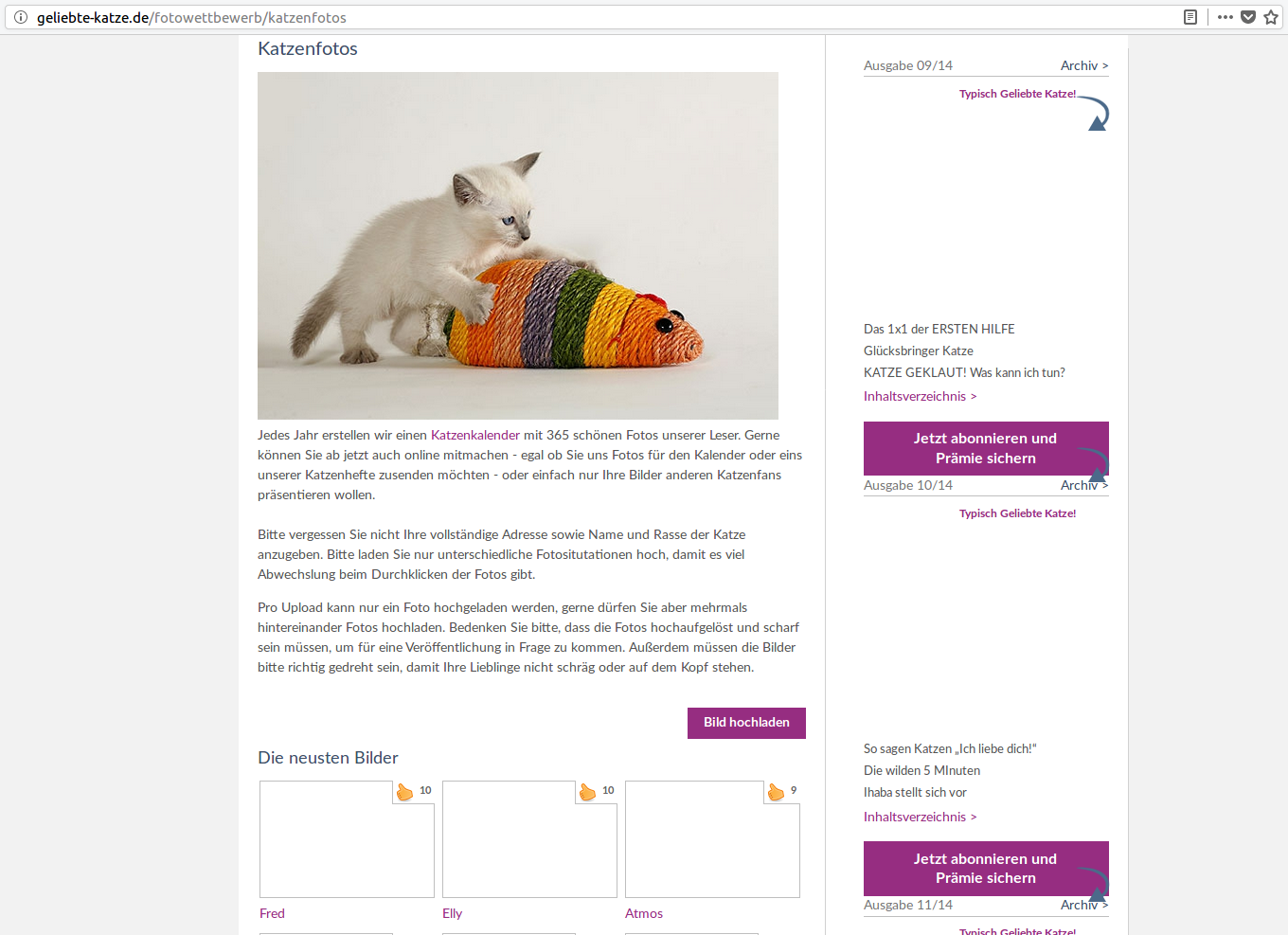


|  |
| --- |
| *2. Vorbereitung des Angriffs* |
| Zunächst werden die ARP-Tabellen „vergiftet“. Der Angreifer gibt sich für das Opfer als der Router des Netzwerkes aus. Für den Router gibt sich der Angreifer als der eigentliche Client aus.  Benötigt werden hierfür die IP-Adressen des Opfers und des Routers.  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. |

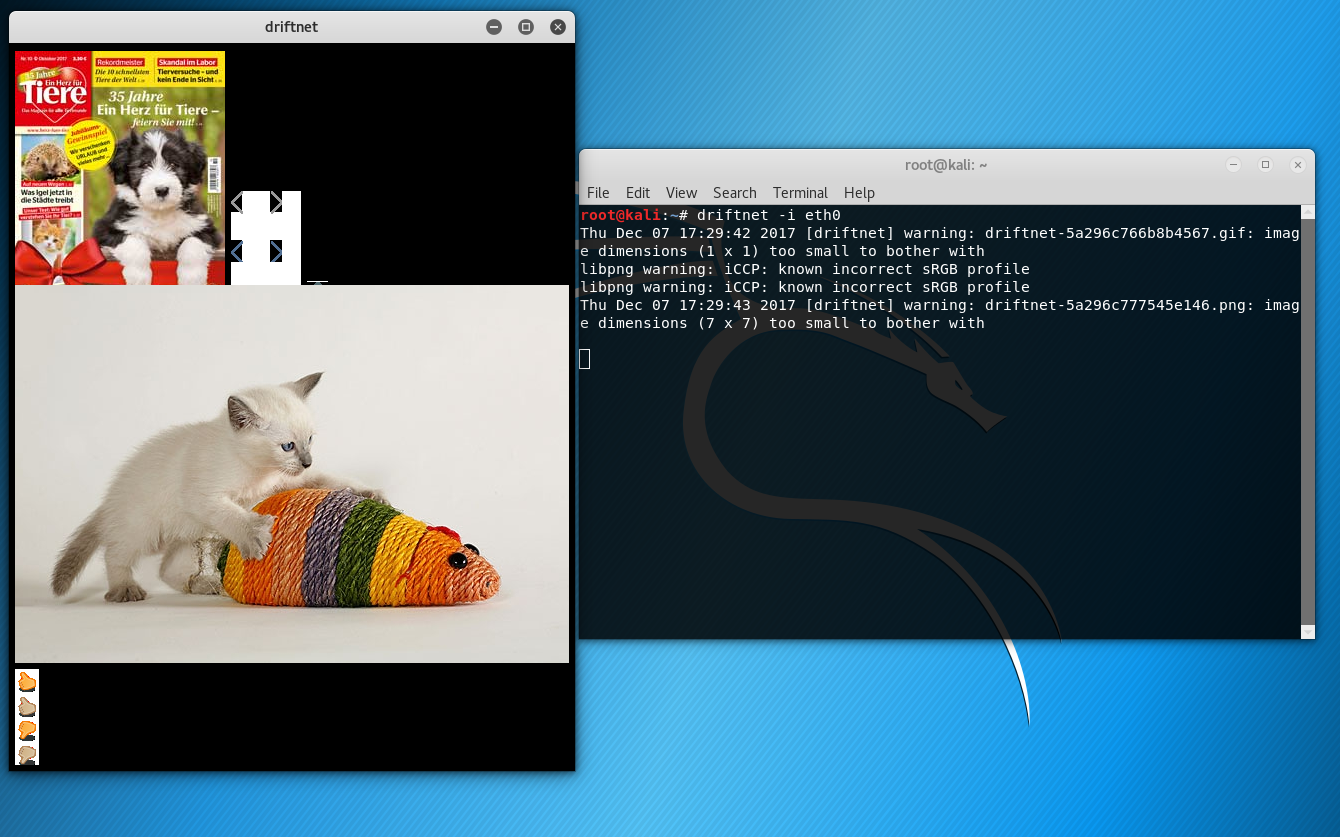
|  |
| --- |
| Das ARP-Spoofing wird mithilfe des Programms „arpspoof“ erreicht.  Die Option -i legt das Interface fest, auf dem gehorcht werden soll.  *Die Option -t <IP-Adresse des Geräts, welches vergiftet werden soll> <vorgetäuschte IP> legt fest als wen sich der Angreifer ausgibt.* |



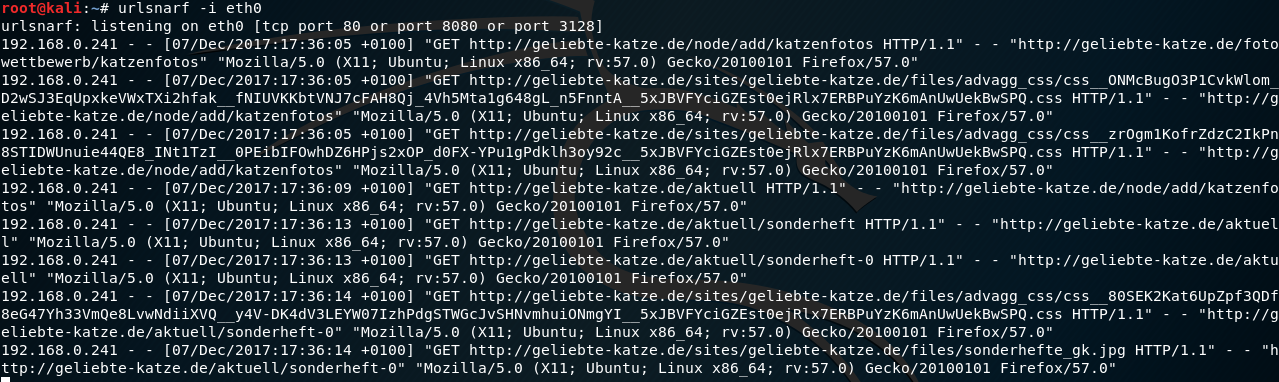
|  |
| --- |
| *3.Durchführen des Angriffs* |
| Das Opfer ist ein Katzenfan und schaut sich daher Bilder von Katzen an. |



|  |
| --- |
| *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.  Diese Möglichkeit bietet zwar Schutz vor einem „Man-in-the-Middle“-Angriff, weißt aber dennoch nicht darauf hin, dass dieser Angriff in einem Netzwerk durchgeführt wurde! |

|  |
| --- |
| *5. Gegenmaßnahme SSL* |
| Sobald die Verbindungen verschlüsselt sind, können keine Pakete mehr ausgelesen werden.  Es gibt mehrere Möglichkeiten SSL zu verwenden.  Zu einem die Standard-Variante https.  Als weitere Möglichkeit gibt es Plugins für gewisse Browser, die den Anwender Warnen, wenn er eine nicht verschlüsselte Seite aufruft.  Außerdem kann der Nutzer über eine SSL-verschlüsselte VPN-Verbindung zu einem anderen Netzwerk/Server surfen. Dies hat zufolge, dass alle Daten die versendet werden verschlüsselt sind. Zumindest bis zum anderen Netzwerk/Server. |

Weitere Gegenmaßnahmen.

|  |
| --- |
| *6. Statische ARP-Einträge* |
| Die Einträge in der ARP-Tabelle können, beispielsweise über Windows mit der Shell und dem Befehl arp -s manuell gesetzt werden. Somit kann man sich vor ARP-Spoofing schützen.  Diese Variante ist dennoch recht mühsam. Da dies für jeden PC/Server im Netzwerk erledigt werden muss. Außerdem müssen neue Geräte immer wieder eingetragen werden. Somit ist diese Variante eher im Business-Bereich bei Servern zu finden. |

|  |
| --- |
| *7. Layer-3-Switche* |
| ARP-Requests in andere Segmente werden vom Switch geprüft. Arbeitet dieser auf der Netzwerkschicht (Layer 3), wird neben der MAC-Adresse auch die IP-Adresse mit vorhergehenden Einträgen abgeglichen. Fallen dabei Unstimmigkeiten oder häufige Neuzuordnungen auf, schlagt der Switch Alarm. |

|  |
| --- |
| *8. Programme* |
| Es gibt einige Programme die das Netzwerk überwachen und auffällige ARP-Vorgänge aufspüren.  Bekannte Tools sind: Arpwatch, ARP-Guard, XAarp |

|  |
| --- |
| *9. Fazit* |
| 1. Das Mitschneiden von Daten in einem öffentlichen Netzwerk ist möglich und einfach. 2. Es sollten keine wichtigen oder persönlichen Daten in öffentlichen Netzwerken eingeben werden. 3. Auf Webstites auf denen relevante Zugansdaten eingegeben werden ist darauf zu achten, dass im Browser https:// und nicht http:// vor der Website steht (Sichere Verbindung). 4. Meldung wie “Die verschlüsselte Seite versucht Daten über eine unsichere Verbindung zu versenden” sollten beachtet werden. |