Artikel von Heise Security über
ARP-Spoofing und ARP-Poisoning-Angriffe

Angriff von innen

[20.01.2005 15:39]

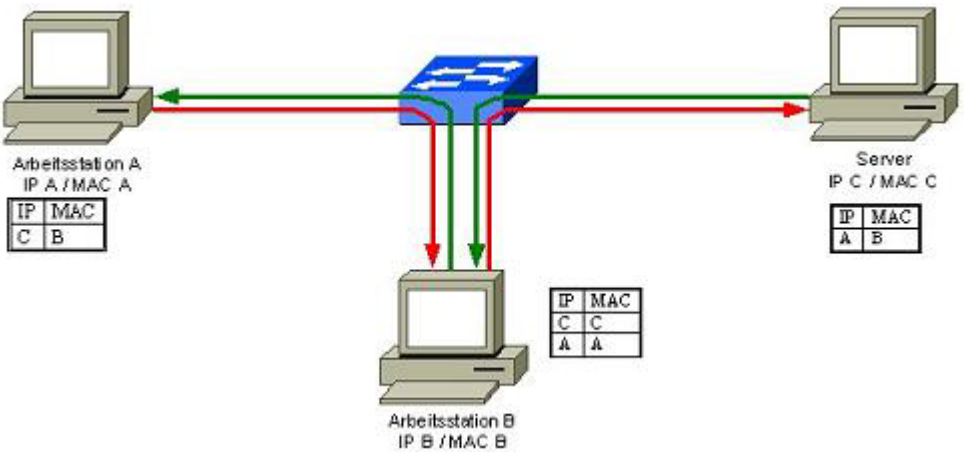
Gereon Ruetten, Oliver Stutzke

Technik und Abwehr von ARP-Spoofing-Angriffen

Nicht nur aus dem Internet werden PCs angegriffen, um Trojaner und Spyware zu installieren. Auch im LAN, beispielsweise in der Firma, versuchen bösartige Zeitgenossen Informationen auszuspähen. Verbindungen zum Homebanking-Server oder zur Online-Auktion lassen sich dort sehr einfach belauschen. Selbst geswitchte Netzwerke bieten keinen Schutz, wenn Angreifer die Verbindung mittels ARP-Spoofing über sich umleiten.

Zur Abwehr von Eindringlingen aus der Außenwelt ist in den letzten Jahren viel Aufwand und Geld in Sicherheitstechniken wie Firewalls, Content-Filter und Intrusion Prevention Systeme gesteckt worden. Der innere Schutz ist hingegen fast überall zu kurz gekommen. Gerade das lokale Netz ist aber meist das schwächste Glied [1]. Hier ist es ein leichtes, zu spionieren und zu manipulieren. Zwar sind auf vielen PCs Virenscanner und Personal Firewalls installiert, die schützen aber nicht gegen alle Angriffe und wiegen selbst erfahrene Anwender in falscher Sicherheit.

Neben Denial-of-Service-Attacken auf den PC des Kollegen oder auf den Firmenserver gehört das Mitlauschen von Datenverkehr zu den häufigsten Angriffsarten. In älteren Netzwerken, deren PCs über einen Hub miteinander verbunden waren, war nur ein Sniffer-Programm wie Ethereal notwendig, um sämtlichen Datenverkehr mitzulesen. Seit der Einführung von Switches ist das etwas schwieriger. Da der Switch nur noch Pakete an den Port mit der richtigen Ziel-MAC-Adresse weiterleitet, sieht man nur noch den eigenen Datenverkehr sowie uninteressante Broadcasts anderer Systeme. Oft halten selbst Netzwerkadministratoren dies für ein Sicherheitsfeature, das so unüberwindlich wie eine Firewall ist. Allerdings lässt sich ein Switch mit einfachen Mitteln austricksen: Mit sogenanntem ARP-Spoofing leiten Angreifer den Verkehr zwischen Geräte an anderen Ports einfach über den eigenen Rechner um und können so alle Daten mitlesen oder fälschen. Das ganze funktioniert sogar in den Rechenzentren vieler Webhoster, die dedizierte Webserver vermieten. Tests von c't belegen immer wieder, dass sich der Verkehr anderer Server auf den eigenen umbiegen lässt [2,3].



Arbeitststation B kann durch Manipulieren der ARP-Caches die Verbindung zwischen Arbeitsstation A und dem Server über sich umleiten.

Täuschung

Das Address Resolution Protocol (ARP) dient in lokalen, auf Ethernet beruhenden Netzen der Zuordnung einer MAC-Adresse zu einer IP-Adresse [4]. Die Kenntnis der IP-Adresse eines Servers allein genügt nicht, um mit ihm eine Verbindung aufzunehmen -- denn alle TCP/IP-Pakete müssen ja in Ethernet-Frames transportiert werden. Deshalb muss ein Client zunächst die Ziel-Ethernetadresse (MAC) erfragen, indem er einfach per Broadcast die Frage stellt: "Welche MAC-Adresse hat der Rechner mit der IP-Adresse B?" (ARP-Who-has). Der Rechner, mit dieser IP-Adresse antwortet darauf mit "IP B ist unter MAC B zu erreichen" an den Fragesteller. Um nicht jedes Mal nachfragen zu müssen, legt der Client die Zuordnung IP-MAC in einem lokalen ARP-Cache ab.

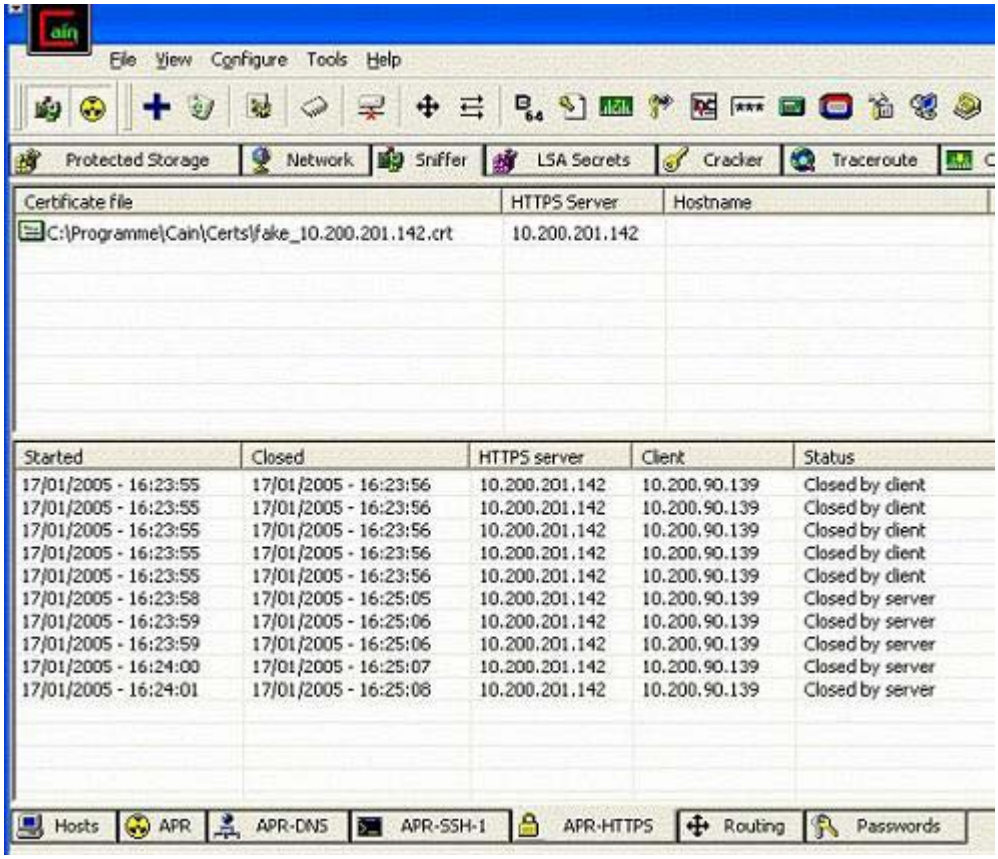
ARP bietet keine Funktionen, um sicherzustellen, dass die Antwort auch wirklich von dem Rechner kommt, mit dem man eine Verbindung aufbauen will. So kann prinzipiell jedes System im LAN vortäuschen, der Besitzer einer IP-Adresse zu sein. Zudem erlaubt das ARP-Protokoll die Verarbeitung von Antwort-Paketen, für die gar keine Anfrage gestellt wurde. Mit sogenannten Gratuitous-ARP-Paketen teilen beispielsweise Windows-PCs nach dem Hochfahren allen anderen Rechnern ihr MAC-IP-Paar mit und testen gleichzeitig, ob es einen IP-Adresskonflikt gibt [5]. Die anderen Systeme speichern solche Paare ohne Murren im Cache.

Missbrauch

Ein Angreifer kann nun die Verbindung zwischen einem Client und Server oder Router über sich umleiten, indem er den Opfern manipulierte ARP-Pakete mit seiner eigenen MAC-Adresse sendet. Dieses Einschleusen von gefälschten Adresspaaren in den Zwischenspeicher nennt man auch Cache-Poisoning. Anschließend schickt der angegriffene Client seine Paket ohne weitere ARP-Anfragen immer zuerst an den Angreifer, der diese nach der Inspektion an den Server weiterleitet. Umgekehrt sendet der Server seine Antwort erst an den Angreifer, bevor dieser sie an den Client schickt. In solch

einer Man-in-the-Middle-Position lässt sich fortan die gesamte IP-basierte Kommunikation zwischen den beiden Systemen mitlesen -- sofern sie nicht verschlüsselt ist.

Mit umgeleiteten Verbindungen kann ein Angreifer nicht nur etwa E-Mails und Zugangskennwörter ausspähen, sondern er kann auch Daten zu manipulieren. Besonders lohnende Ziele dafür sind Name-Server-Anfragen, da sich über sie auch die Kommunikation mit externen Servern umleiten lässt. Durch eine gefälschte DNS-Auskunft landet ein Opfer beispielsweise nicht auf dem eBay-Server, sondern auf einem präparierten System.



Um auch SSL-gesicherte Verbindungen zu belauschen, benutzt Cain & Abel gefälschte Zertifkate

Holzhammer

Neben dem ARP-Spoofing gibt es weitere Methoden, um Verbindungen in geswitchten Netzwerken zu belauschen. Die Zuordnung von MAC-Addressen zu Switchports sowie

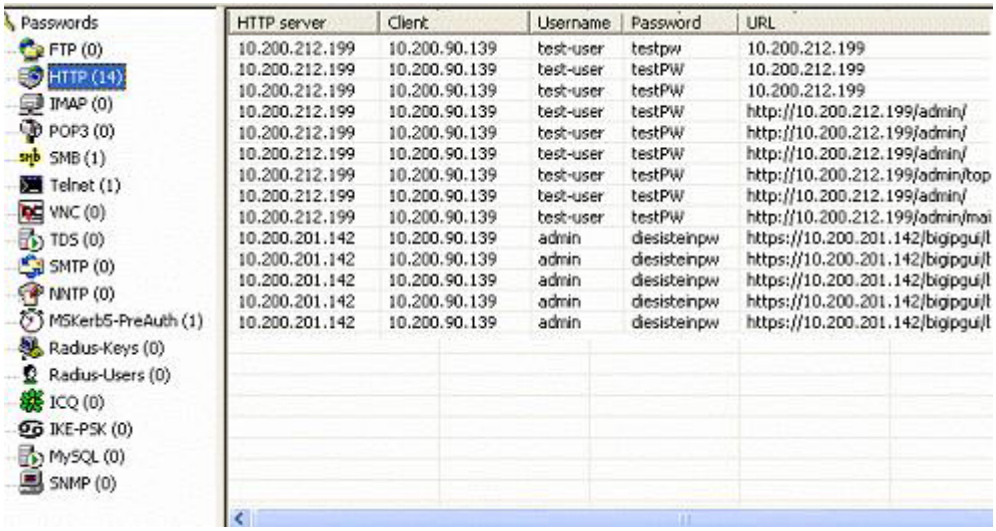
deren VLAN-Zugehörigkeit speichern Switches in einem Content Addressable Memory (CAM). Überflutet ein Angreifer diesen Speicher mit zu vielen MAC-Adressen, fallen viele Switches in den Hub-Modus zurück, in der sie sämtliche Pakete an alle Ports ausgeben. Das Tool macof aus der Netzwerk-Tool-Sammlung Dsniff erledigt solche Angriffe automatisch [6].

Auch durch das Klonen von MAC-Adressen kann sich ein Angreifer als ein anderer Netzteilnehmer ausgeben. Die Adressen von Ethernetadaptern sind zwar weltweit eindeutig, lassen sich aber temporär überschreiben. Die geklonte Adresse ist im LAN uneingeschränkt nutzbar, wenn man das Originalendgerät lahm legt, etwa durch eine DoS-Attacke.

Bastelstunde

Wurde die Fähigkeit zum Spionieren und Manipulieren vor einiger Zeit noch Experten und Hackern zugeschrieben, so existieren mittlerweile Windows-Tools, die einfach zu installieren und zu bedienen sind. Dazu zählen insbesondere Cain&Abel und Ettercap, die nicht nur den eigentlichen ARP-Angriff ausführen und einen Angreifer in die Man-in-the-Middle-Position bringen, sondern durch Filter auch einzelne Protokolle analysieren [7,8]. Die einzige Hürde ist es, die IP-Adresse des anzugreifenden Rechners und dessen Kommunikationspartners herauszufinden -- letzterer ist in den meisten Fällen das Standard-Gateway.

In umgeleiteten Telnet-, FTP-, HTTP- und POP3-Datenströmen entdeckte Passwörter zeigen Cain&Abel und Ettercap sofort an. Verschlüsselte Kennwörter versucht zumindest Cain&Abel mit seinem integrierten Passwort-Cracker per Wörterbuch- oder Brute-Force-Angriff zu entschlüsseln. Für Linux-Plattformen existieren weitaus mehr Programme, wie etwa die Kommandozeilen-Tools Arpoison, Hunt und die Sammlung Dsniff. Diese setzen aber Netzwerkkenntnisse zur Bedienung voraus, bieten dafür aber zahlreiche Angiffsmethoden und Anwendungsfilter. Einzig die Unix-Version von ettercap hat eine rudimentäre Bedienoberfläche. Ab ettercap NG wartet das Tool zwar mit einer komfortableren GUI auf, die ist allerdings weniger intuitiv zu bedienen.



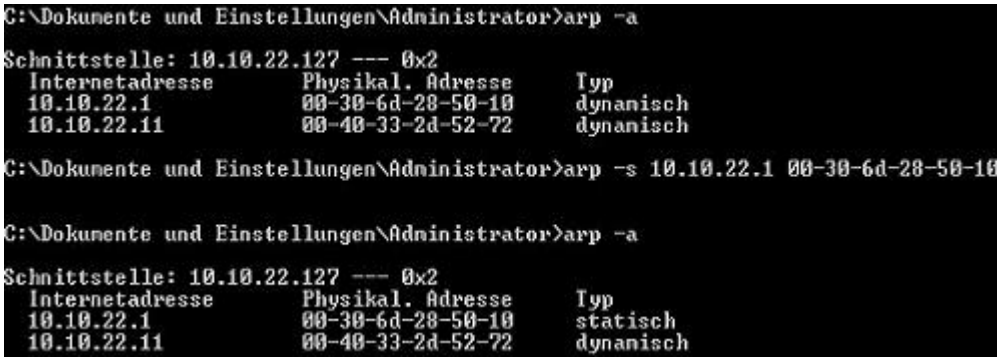
Ist eine Verbindung erst einmal umgeleitet, filtert Cain & Abel automatisch alle Passwörter aus. Sogar per HTTPS übertragene Kennwörter zur Anmeldung an Web-Oberflächen erkennt das Tool.

Mit Cain&Abel ist es unter anderem besonders einfach, eine SSL-gesicherte Verbindung etwa zum Online-Banking kompromittieren. Es bricht diesen Schutz auf, indem es einen SSL-fähigen Web-Server simuliert und dem Opfer selbst erstellte SSL-Zertifikate präsentiert. Diese sind zwar nicht vertrauenswürdig und lassen im Browser eine Warnung erscheinen, aber so mancher Anwender ignoriert die schon gewohnheitsmäßig. Da der Client seine SSL-Verbindung nur zum Rechner des Angreifers aufgebaut hat, kann dieser die Daten im Klartext mitlesen und mit einer neuen SSL-Verbindung an den Bank-Server weitersenden. Außer der Warnung über das seltsame Zertifikat, bemerkt das Opfer solche Manipulationen nicht.

Auf ähnliche Weise lassen sich auch SSH-Verbindungen austricksen. Zwar sollte ein neuer Server-Key stutzig machen, trotzdem ignorieren viele Anwender auch diese Warnung. Bei Putty genügt dazu ein Klick, bei openssh muss der Anwender allerdings schon den alten Eintrag aus seiner know_hosts-Liste löschen. Zudem kann Cain&Abel eine Designschwäche in SSHv1 ausnutzen, um Passwörter on-the-fly mitzulesen.

Schutz im LAN

Wie gut man sich der ARP-Spoofing-Angriffe erwehren kann, hängt davon ab, wie früh Abwehrmaßnahmen ansetzen. Am wirksamsten ist es, bereits die Adress-Manipulation zu unterbinden. Eine einfache Möglichkeit PCs gegen ARP-Spoofing resistent zu machen, ist die Verwendung statischer ARP-Einträge (arp – s). Dies bedeutet aber, dass alle IP-Adressen mit den dazugehörigen MAC-Adressen von Kommunikationspartnern innerhalb einer Broadcast-Domain in den ARP-Cache eingetragen werden müssen. Das ist mit hohem administrativen Aufwand verbunden und in lokalen Netzen mit DHCP kaum möglich. Als Kompromiss kann der Netzadmin zumindest die MAC-Adresse des Standard-Gateways fest eintragen. Unter Windows sind statische ARP-Einträge leider erst ab XP möglich. Bei allen Versionen davor werden die Einträge zwar als statisch angezeigt, sie lassen sich aber trotzdem überschreiben.



Mit statischen ARP-Einträgen für das Gateway lassen sich Verbindungen zu Servern in anderen Subnetzen nicht mehr entführen.

Bei Laptops die häufig an unterschiedlichen LAN-Umgebungen, Home-Office- oder WLAN-Netzen angeschlossen werden, ist ein statischer ARP-Cache ohnehin schwer einzusetzen. Personal Firewalls wie die von Sygate oder spezielle Tools wie SnoopNetCop Pro überwachen den lokalen ARP-Cache und bieten so zusätzlichen Schutz [9,10]. Meist wird der Benutzer aber nur auf einen Angriff hingewiesen -- weitere Maßnahmen muss er dann selbst einleiten.

Quarantäne

Alternativ kann man den Schutz natürlich von den Endgeräten in die Netzwerkkomponenten verlagern. Die Hersteller bieten hier zwei Ansätze, die die Sicherheit im LAN erhöhen. Durch virtuelle LANs (VLANs) lassen sich Endgeräte logischen Netzsegmenten zuordnen und somit voneinander separieren [11]. Nur innerhalb eines Segmentes ist noch eine Kommunikation auf Ethernet-Ebene möglich -- ARP-Informationen verlassen ein VLAN nicht mehr. Die Kommunikation zwischen VLANs erfolgt über einen Router. Dafür muss er Mitglied in jedem VLAN sein.

Je weniger Endgeräte in einem Segment sind, desto weniger kann ein Angreifer stören. Im günstigsten Fall ist jeder PC in einem eigenen VLAN nach 802.1q. Allerdings hat die Sache zwei Haken. Einige Switches unterstützen nur eine kleine Zahl von VLANs, sodass der Idealfall kaum zu schaffen ist. Zudem ist der Router Mitglied in allen VLANs, weshalb ein Angreifer den Verkehr vom Router auf Rechner in anderen Segmenten immer noch auf sich umbiegen kann. Allerdings ist er nicht in der Lage, den Verkehr anschließend an den eigentlichen Empfänger weiterzuleiten. Eine Man-in-the-Middle-Attacke lässt sich so zwar nicht mehr bewerkstelligen, aber als Denial-of-Service-Attacke eignet sich ARP-Spoofing weiterhin.

Auch die von teureren Cisco-Switches unter IOS 12.1(6) EA2 angebotene Option "switchport protected" zur Isolierung der Ports hilft hier nicht weiter. Da der Port des Routers oder Gateways nicht geschützt sein darf, gilt hier das gleiche wie bei VLANs. Immerhin lassen sich die CAM-Tabellen solcher Switches mit der Option "switchport port-security" vor dem Überfluten schützen.

Als alternative Methode verfügen Catalyst-3560/3750-Switches mit Enhanced Multilayer Image (EMI) und Switche der Serie 4500 sowie 6500 über (Dynamic) ARP Inspection (DAI). Damit überwachen die Geräte, ob ARP-Pakete mit ungültiger IP-MAC Zuordnung im Netz unterwegs sind und protokollieren oder verwerfen sie, bevor sie beim Endgerät ankommen. Die dazu notwendige Datenbasis kann eine DHCP-Datenbank oder eine manuell erstellte Liste (ARP Access Control List) sein.

Augenzeuge

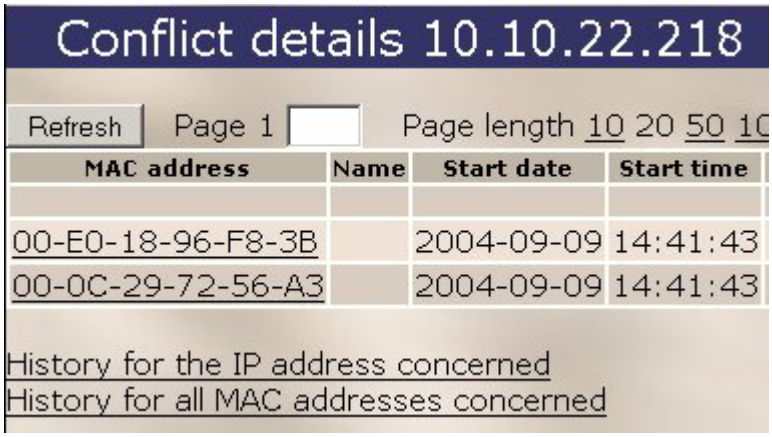
Verhindert die vorhandene Infrastruktur oder ein zu schmales Budget den Einsatz präventiver Maßnahmen, bleibt nur die kontinuierliche Überwachung des Netzverkehrs durch zusätzliche Komponenten. Mit der schnellen Identifizierung von ARP-Spoofing-Versuchen und dem rechtzeitigen Eingriff lassen sich auch so Angriffe erfolgreich abwehren. Dazu ist es notwendig, alle ARP-Meldungen mitzulesen und zu analysieren, beispielsweise indem man Überwachungskomponenten an den Spiegelport eines Switches anschließt. Allerdings besteht hier die Gefahr, dass an diesem Port nicht immer alle Pakete ankommen: Da der Switch versucht, die Pakete aller Ports dorthin zu kopieren, kann der Spiegelport bei hoher Netzlast Pakete verwerfen. Eine andere Möglichkeit bietet die permanente Kontrolle der ARP-Tabelle des Standard-Gateways.

Auch Intrusion Detection Systeme (IDS) sind aufgrund ihres Designs mit Netzsensoren in LAN-Segmenten prinzipiell zur Abwehr von ARP-Spoofing-Angriffen geeignet. Da diese Systeme aber in erster Linie zur Erkennung von Angriffen auf höhere Protokollschichten entwickelt wurden, muss ein IDS auf seine individuelle Eignung geprüft werden. So erkennt die IDS-Software Snort in Netzen mit dynamischer Adressvergabe eine Umleitung per Ettercap erst beim Beenden des Angriffs [12]. Das Tool verschickt beim Beenden eines Spoofing-Angriffes nämlich ungewöhnliche Pakete (SRC MAC conflict). Mit statischer Zuordnung der IP-/MAC-Adressen in der Konfiguration ist aber auch Snort in der Lage, Spoofing-Attacken sofort zu erkennen.

Werkzeug

Arpwatch, ein Open-Source-Tool für UNIX-Plattformen, kann ARP-Pakete in einem lokalen Netz lesen, daraus die MAC-IP-Informationen entnehmen und speichern, sowie mit vorhanden Einträgen vergleichen [13]. Nach einer Lernphase schlägt Arpwatch bei Paketen Alarm, die zu keinem Eintrag passen. Der Einsatz von Arpwatch eignet sich in kleineren Netzen, da sich der Aufwand dort noch in Grenzen hält. Bei Verwendung von DHCP meldet Arpwatch allerdings die für diese Umgebungen erlaubten Änderungen der MAC-IP-Zuordnung. Hier muss ein Administrator selber herausfinden, ob es sich um einen echte Angriff handelt.

Ein speziell zur Erkennung von ARP-Angriffen entwickeltes Produkt ist der ARP-Guard [14]. Ihm liegt eine Sensor-Management-Architektur zugrunde, bei der mehrere Sensoren Adress-Informationen beobachten und an das Management-System weiterleiteten. Das Management analysiert die Meldungen und leitet im Angriffsfall Gegenmaßnahmen ein, etwa indem es automatisch Ports am Switch abschaltet. Die Sensoren können sowohl die Pakete an einen Mirrorport auswerten als auch die ARP-Tabellen aus Routern mittels SNMP auslesen.



Der ARP-Guard bemerkt die Rangelei zweier Rechner um eine IP-Adresse und schlägt gegebenenfalls Alarm

Tunnel

Ein anderer Ansatz ist die Ende-zu-Ende-Sicherung der Kommunikation, sodass ein Angreifer zwar die Verbindung über seinen Rechner umleiten kann, aber dennoch die Daten nicht lesen kann. Üblicherweise setzt man hier IPSec oder SSH in der sicheren Versionen 2 oder SSL mit bidirektionaler Authentifizierung [15]. Allerdings ist dies mit größeren Umkonfigurationen der Endgeräte verbunden und auch alle Server müssen es unterstützen. Daher schützt diese Lösung eigentlich nur firmeninternen Verkehr -- die Verbindung vom Arbeitsplatzrechner zur Online-Auktion im Internet bleibt weiter angreifbar.

Einen hundertprozentigen Schutz vor ARP-Spoofing-Angriffen zu erreichen, ist sehr schwer. Da die Gefahr aber nur im LAN besteht, dämmen zusätzliche organisatorische

und technische Maßnahmen Spionageversuche wirksam ein. Arbeiten die Anwender auf ihren Arbeitsplatz-PCs unter Windows als eingeschränkte Nutzer, so lassen sich etwa Ettercap und Cain&Abel gar nicht erst installieren. Das Booten eines Knoppix, um die Restriktionen unter Windows zu umgehen, verhindert der Administrator durch Einstellungen im passwortgeschützten BIOS auf jedem Rechner. Gegen ein mitgebrachtes Laptop mit gespoofer MAC-Adresse helfen aber auch diese Maßnahmen nicht. **(dab)[1]**

Links & Literatur

[1] **KPMG-Studie: Global survey finds companies underestimate internal threat[2]**

[2] Server-Nachsitzen, Neuer Test von Strato- und Intergenia-Mietservern, c't 02/05, S. 42

[3] Eigenheim zur Miete, Dedizierte Internet-Server der Einstiegsklasse, c't 12/04, S. 142

[4] **RFC 826 - An Ethernet Address Resolution Protocol[3]**

[5] **Windows 2000 TCP/IP Implementation Details[4]**

[6] **dsniff[5]**

[7] **Cain & Abel[6]**

[8] **ettercap NG"[7]**

[9] **Sygate[8]**

[10] **SnoopNetCop Professional[9]**

[11] Logische Netze, Virtuelle Netze schaffen mehr Sicherheit, c't 01/05, S. 90

[12] **Snort[10]**

[13] **arpwatch[11]**

[14] Torwächter, kurz vorgestellt, c't 24/04, S. 82[12]

[15] **Der Pförtner zum Netz - Ein IPSec-Gateway im Eigenbau[13]**

URL dieses Artikels:

http://www.heise.de/security/artikel/55269

Links in diesem Artikel:

[1] mailto:dab@heisec.de

[2] http://www.kpmg.com/about/press.asp?cid=469

[3] http://www.ietf.org/rfc/rfc826.txt

[4] http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/tcpip2k.mspx

[5] http://www.heise.de/security/tools/default.shtml?prg=11&T=dsniff&l_sw=-1&l_aw=-1

[6] http://www.heise.de/security/tools/default.shtml?prg=45&T=cain%2A&os=21&l_sw=-1&l_aw=-1

[7] http://www.heise.de/security/tools/default.shtml?prg=12&T=ettercap&os=21&l_sw=-1&l_aw=-1

[8] http://www.sygate.de/

[9] http://www.snoopanalyzer.com/snoopnetcop/professional_01.asp

[10] http://www.heise.de/security/tools/default.shtml?prg=23&l_sw=-1&l_aw=-1

[11] http://www-nrg.ee.lbl.gov/

[12] http://www.heise.de/security/artikel/38014