Sicherheitstechniken in Kommunikationsnetzen

http://vfhsikdemo2.oncampus.de

Stand 05.11.2015 05:01

Inhalt

Sicherheitstechniken in Kommunikationsnetzen

Die Verwendung des Internets ist für viele Organisationen, seien es private Unternehmen oder öffentliche Einrichtungen, zu einer unbedingten Notwendigkeit geworden, ohne das die eigenen Dienstleistungen nicht mehr erbracht werden können. Die enorme Bedeutung des Internets macht daher auch die Computerkriminalität zu einem Betätigungsfeld, mit dem sehr viel Geld verdient werden kann (siehe z.B. Meldung über Milliardenschäden durch Wirtschaftsspionage oder Meldung über eine Rekordanzahl an Straftaten im Internet). Aus diesem Grunde ist es für Organisationen - egal ob Kleinunternehmen oder große Behörde - notwendig, sich Gedanken zu machen, welche Schutzmaßnahmen notwendig sind. Das Ziel dieses Moduls ist es, hierzu eine Entscheidungshilfe zu bieten, welche Schritte notwendig sind. Aufgrund der Komplexität des Themas ist eine vollständige Behandlung unmöglich. Es sollen aber möglichst viele Hinweise gegeben werden, die eine weitere Vertiefung ermöglichen.

Hinweis

Die nachfolgende Lerneinheit "Angriffe aus dem Internet" gibt Ihnen einen kleinen Einblick in das Modul "Sicherheitstechniken in Kommunikationsnetzen".

Gliederung

1 Angriffe aus dem Internet

Gliederung

Nach einer Erklärung von Grundbegriffen und grundsätzlichen Angriffsszenarien werden in diesem Kapitel Angriffsmöglichkeiten vorgestellt.

Die Darstellung erfolgt jeweils mit einer theoretischen Beschreibung, die aber oftmals durch die Erklärung von echten Vorkommnissen ergänzt wird, um die Praxisrelevanz deutlich zu machen. Anschließend werden Tools vorgestellt, mit denen das Vorhandensein von Schwachstellen überprüft werden kann. Wichtig zu beachten ist, dass aus rechtlichen Gründen einige dieser Werkzeuge nur auf eigene Webseiten angewendet werden dürfen.

Bei der Vorstellung der Angriffsszenarien in diesem Kapitel dient das vom OSI-Modell abgeleitete Hybride Modell als Gliederungshilfe, so dass die Bedrohungen gemäß den Schichten geordnet vorgestellt werden. Das Kapitel setzt dabei die Kenntnis des Modells voraus.

1.1 Einleitung: Angriffe aus dem Internet

Gliederung

Zur Verständnis dieses Kapitels sowie auch der weiteren Kapitel ist die Kenntnis einer Reihe von Grundbegriffen notwendig, die im folgenden erklärt werden. Außerdem ist es notwendig sich zu vergegenwärtigen, dass Angriffe nicht nur aus dem Internet erfolgen können, sondern auch aus dem inneren einer Organisation heraus. Daher werden verschiedene Arten von Angreifern unterschieden. Außerdem gibt es bei der Kommunikation zwischen zwei Personen unterschiedliche Möglichkeiten wie diese von Angreifern beeinflusst werden kann.

1.1.1 Begriffsdefinitionen

Als Voraussetzung für das weitere Modul sollen an dieser Stelle wesentliche Begriffe definiert werden, um Unklarheiten zu vermeiden.

Man unterscheidet fünf Sicherheitsaspekte und die Privatsphäre.

- Die **Vertraulichkeit** (engl. Confidentiality) der Daten stellt sicher, dass die Daten nicht ausgespäht werden können. Wenn die Daten über unsichere Kanäle (wie dem Internet) übertragen werden, kann man jedoch nicht grundsätzlich verhindern, dass die Daten abgehört werden. In diesem Fall müssen die Daten geeignet verschlüsselt sein, so dass Abhörer die Daten nicht entschlüsseln und damit nicht lesbar machen können.
- Durch die **Daten-Integrität** (engl. Integrity) wird sichergestellt, dass die übertragenen Daten nicht geändert wurden, keine Daten eingefügt, gelöscht oder wiederholt übertragen wurden. Ähnlich wie bei der Vertraulichkeit muss man bei unsicheren Kanälen davon ausgehen, dass Manipulationen der Daten vorkommen können. Daher muss sichergestellt werden, dass solche Manipulationsversuche erkannt und die Daten dann erneut übertragen werden. Datenintegrität kann man nicht nur dann betrachten, wenn Daten über Netze übertragen werden. Auch bei lokal gespeicherten Daten möchte man sicherstellen, dass diese nicht unbefugt verändert werden.
- Unter der **Authentizität** (engl. Authenticity) versteht man, dass übertragenene Daten tatsächlich vom angegebenen Absender stammen.
- **Verfügbarkeit** bedeutet, dass Dienste (Netze, Anwendungen) so verwendet werden können, wie man das erwartet. Sie sollen nicht nur grundsätzlich funktionieren, sondern auch in einer guten Qualität. Kriterien für eine hohe Qualität sind in diesem Zusammenhang hohe Bitraten, geringe Latenzzeiten, niedrige Schwankungen der Latenzzeiten sowie geringe Paketverlustraten.

- Bei der **Nicht-Abstreitbarkeit** (engl. Non-repudiation) oder **Verbindlichkeit** (engl. Accountability) wird sichergestellt, dass Handlungen tatsächlich einer Person zugeordnet werden können. Diese Person kann nachher nicht leugnen, die Aktion nicht durchgeführt zu haben.
- Unter der **Privatsphäre** (engl. Privacy) versteht man, dass eine Person die Kontrolle darüber behält, welche Daten über sie gesammelt werden. Diese Daten umfassen persönliche Daten wie Name, Adresse, Telefonnummer, E-Mail-Adresse, aber auch Informationen über das Verhalten wie beispielsweise besuchte Webseiten, Kontakte in sozialen Netzwerken oder Bewegungsprofile bei der Nutzung von Mobiltelefonen.

Außerdem ist es wichtig, zwischen Authentifizierung und Autorisierung zu unterscheiden.

- Bei der **Authentifizierung** (engl. Authentication) wird überprüft, ob der Kommunikationspartner, zu dem eine Verbindung aufgebaut werden soll, der wahre Kommunikationspartner ist (engl. Peer Entity Authentication) und ob die empfangenen Daten tatsächlich vom wahren Sender gesendet wurden (engl. Data Origin Authentication), wobei allerdings nicht die Integrität der Daten überprüft wird. Von besonderer Bedeutung ist im Internet die Authentifizierung eines Servers. Dieser Anwendungsfall wird sehr häufig eingesetzt, z.B. bei Transaktionen mit Banken oder bei der Kommunikation mit File-Servern.
- Der Begriff **Autorisierung** (engl. Authorization) hingegen beschreibt, welche Rechte ein Kommunikationspartner hat. Die Zuweisung dieser Rechte erfolgt nach erfolgreicher Authentifizierung.

Abgekürzt kann man sagen, dass die Authentifizierung besagt, wer jemand ist und die Autorisierung festlegt, was dieser darf.

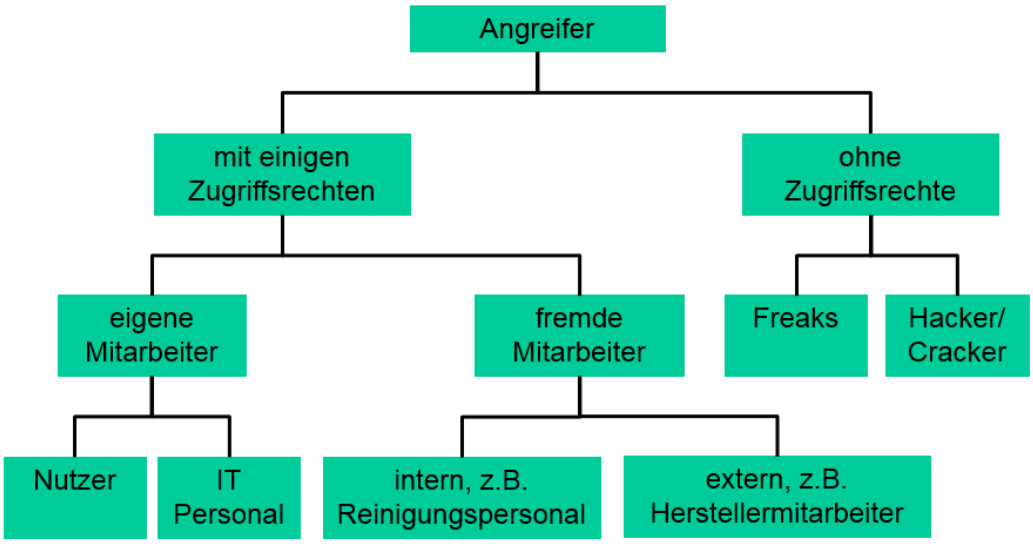
Schließlich können noch die Begriffe Schwachstelle, Bedrohung und Risiko bzgl. eines Systems voneinander abgegrenzt werden.

- Unter einer **Schwachstelle** versteht man eine Eigenschaft eines Systems, die eine mißbräuchliche Verwendung des Systems ermöglicht.
- Als **Bedrohung** wird jegliches mögliche Vorkommen von unerwünschten Effekten auf die Ressourcen des Systems angesehen, wobei dieses Vorkommen absichtlich oder unabsichtlich herbeigeführt sein kann.
- Ein **Risiko** kann aus der Kombination einer Schwachstelle mit einer Bedrohung entstehen. Dieses kann man auch mit der Formel "Risiko gleich Bedrohung * Schwachstelle" ausdrücken.

Schließlich sollte man bei Sicherheit noch zwei Aspekte unterscheiden, die im englischen **Security** und **Safety** heißen. Bei Safety geht es um Bedrohungen, die unvermeidlich sind, auch wenn sich alle Personen bemühen, diese zu verhindern. Ein Beispiel sind beispielsweise Hardwaredefekte, die den Netzbetrieb beeinflussen können. Bei Security geht es dagegen um Bedrohungen, die von Menschen absichtlich herbeigeführt werden, beispielsweise um eine absichtlich erzeugte hohe Netzlast, die zu Ausfällen von Diensten führt. Auch wenn dieser Security-Aspekt in diesem Modul im Vordergrund steht, muss man jedoch auch den Safety-Aspekt berücksichtigen. Beispielsweise kann es bei einer Nichtverfügbarkeit von Diensten nicht klar sein, ob diese Situation unabsichtlich oder absichtlich entstanden ist.

1.1.2 Arten von Angreifern

Die Situation, die in diesem Kapitel meistens angenommen wird, ist eine Organisation, deren Netzwerk mit dem Internet verbunden ist. Aus dem Internet heraus werden Angriffsversuche unternommen, um in das Netzwerk der Organisation einzudringen. Man muss sich jedoch klar machen, dass dieses nur ein Teil der Situation ist und man auch mit Angriffen von innerhalb der Organisation rechnen muss. Deshalb wird in der folgenden Abbildung eine Kategorisierung der Angreifer vorgenommen.



Hierbei wird zunächst unterschieden zwischen Angreifern mit einigen Zugriffsrechten und solchen ohne irgendwelche Zugriffsrechte. Bei den Angreifern ohne Zugriffsrechte kann man differenzieren zwischen *Freaks*, die mehr aus einem Spieltrieb heraus die Sicherheitseinstellungen testen, ohne dabei Schaden anrichten zu wollen, und *Hackern/Crackern*. Im normalen Sprachgebrauch wird zwischen diesen Begriffen kein Unterschied mehr gemacht und bezeichnet Personen, die absichtlich Schaden

herbeiführen wollen. Oftmals beschäftigen sie sich hauptsächlich mit der Durchführung von solchen Angriffen und sind der organisierten Kriminalität zuzurechnen. Der Begriff Hacker hatte ursprünglich übrigens nicht die negative Bedeutung von heute und bezeichnete die kreative Nutzung von Geräten für andere Zwecke als für die sie konzipiert wurden. Außerdem gibt es noch den Begriff *Skriptkiddie*, mit dem jemand gemeint ist, der auch ohne große Fachkenntnisse Schaden anrichten möchte und dabei vorgefertigten Angriffscode verwendet.

Bei den Benutzern mit Zugriffsrechten unterscheidet man zwischen eigenen Mitarbeitern und denen von anderen Organisationen. Bei den eigenen Mitarbeitern wird zwischen normalen Mitarbeitern und dem IT-Personal entschieden. Angriffe durch das IT-Personal sind besonders kritisch, weil diese Mitarbeiter über mehr Rechte als der durchschnittliche Mitarbeiter verfügen und außerdem auch meist über höhere Sachkenntnis. Solche Angriffe können aus Unzufriedenheit mit der Arbeitsstelle durchgeführt werden oder um Wissen zu einem anderen Arbeitgeber mitzunehmen.

Gerade große Firmen arbeiten sehr eng mit anderen Firmen zusammen, die dafür auch einen begrenzten Zugriff erhalten müssen. Das kann ein realer Zugang zu den Gebäuden sein, wenn beispielsweise Reinigungspersonal oder Wachleute im Gebäude sind und unbeobachtet an die Hardware der Mitarbeiter herankönnen. Auch kann es sein, dass im Fehlerfall externe Unterstützung benötigt wird, wenn beispielsweise Computer nicht richtig funktionieren. Auch hier muss man bedenken, dass an diesen Stellen mit schadhaften Verhalten gerechnet werden muss. Es ist daher beispielsweise die Frage, ob man ein Notebook, auf dem wichtige Firmendaten gespeichert sind, zu einer Reparatur geben sollte.

1.1.3 Kommunikationsszenarien

Bei der Kommunikation zwischen zwei Teilnehmern kann man zwischen mehreren Szenarien unterscheiden, was insbesondere dann relevant ist, wenn die Kommunikation über ein nicht vertrauenswürdiges Netzwerk (typischerweise das Internet) erfolgt.

- **Lesen**: Ein Angreifer hat die Möglichkeit den Datenverkehr mitzulesen, was in den meisten Fällen auch eine Möglichkeit beinhaltet, den Datenverkehr dauerhaft zu speichern.
- **Verändern**: Ein Angreifer hat sich in die Kommunikation in der Art integriert, dass die Kommunikation zwischen dem Sender und Empfänger über ihn läuft. Damit kann er den Datenverkehr nicht nur mitlesen, sondern auch aktiv verändern (Teile weglassen, hinzufügen, verändern). Dieses Szenario wird Man-in-the-Middle (MitM) genannt.

- **Unterbrechen**: Der Datenverkehr zwischen Sender und Empfänger könnte unterbrochen werden, so dass die Daten den Empfänger nicht erreichen. In dieser Situation erhält aber auch kein Angreifer die Daten.
- **Entfernen**: Der Angreifer hat die Kommunikation so verändert, dass die Daten des Senders zu ihm gesendet werden. Er leitet die Daten nicht weiter, so dass der Empfänger gar nicht erfährt, dass er überhaupt Daten erhalten sollte. Dieses ist dann der Fall, wenn diese Datenumleitung schon zu Beginn der Kommunikation zwischen Sender und Empfänger besteht. Diese Art der Manipulation ist durch eine Adressfälschung möglich, bei der sich der Angreifer als der Empfänger ausgibt.
- **Erzeugen**: In dieser Situation sendet ein Angreifer Daten an den Empfänger, ohne dass der Sender überhaupt Daten geschickt hat. Der Angreifer gibt also gegenüber dem Empfänger eine falsche Identität, nämlich die des Senders, vor.

Bei der Fälschung von Adressen spricht man von Spoofing (Beispiele: ARP Spoofing, IP Spoofing).

1.2 Typische Angriffsarten der Schichten 1 und 2

Gliederung

Bei Angriffen in Zusammenhang mit der Bitübertragungsschicht geht es um Beschädigungen der Infrastruktur (z.B. durch das Entfernen eines Verbindungskabels), so dass ein Endgerät oder Netz nicht mehr erreichbar ist.

Außerdem ist möglich, die Kommunikation abzuhören. Dieses ist insbesondere bei der Übertragung über die Luft zu beachten, wobei auch kabelgebundene Übertragungen abgehört werden können. Dieses ist im allgemeinen bei Kupferkabeln deutlich einfacher als bei Glasfasern.

Die Angriffsmöglichkeiten auf der Sicherungsschicht erfordern eine genauere Betrachtung. Hierbei muss man unterscheiden zwischen:

- Lokalen Festnetzen (LANs, realisiert mit Ethernet)
- Drahtlosen Lokalen Netzen (WLANs)

- Mobilkommunikationsnetzen (GSM, UMTS, LTE)

Ein weiteres Thema, das zu dieser Schicht gehört, ist RFID, mit dem Risiken hinsichtlich der unbemerkten Abfrage von Daten bestehen. Dieses ist für die Privatsphäre sehr relevant (siehe RFID-Studie des BSI).

1.2.1 Angriffe auf lokale Netze

Bei lokalen Festnetzen werden heutzutage fast ausschließlich Ethernet-Netze eingesetzt, die sternförmig mit Switchen aufgebaut sind. Andere Technologien wie Token Ring oder Token Bus gibt es so gut wie nicht mehr, so dass sich die folgende Diskussion nur auf Ethernet bezieht.

In lokalen Festnetzen kann es vorkommen, dass die Kommunikation von anderen Teilnehmern mitgeschnitten wird. Dieses ist heutzutage nicht so einfach wie in der Vergangenheit als diese Netze mit Bustopologien aufgebaut wurden. Damals erhielt jeder Teilnehmer im lokalen Netz alle Rahmen und man verließ sich darauf, dass jeder nur die für ihn bestimmten Rahmen auswertete. Mit der Einführung von Switches erfolgt aber seit Jahren schon eine gezielte Weiterleitung nur an den Port, an den der Empfänger eines Rahmens angeschlossen ist. Daher ist aus der Sicht des Angreifers eine spezielle Manipulation auf Basis von ARP notwendig, um den Verkehr zu sich umzulenken.

Das Address Resolution Protocol (ARP) dient zum Auffinden eines Endgerätes in einem lokalen Netz, das eine bestimmte IP-Adresse hat. Für diese IP-Adressse wird die zugehörige MAC-Adresse gesucht, da die Switches in LANs die Weiterleitung von Rahmen nur anhand von MAC-Adressen durchführen. Bei ARP werden Broadcast-Rahmen verwendet, in denen die IP-Adresse steht. Ein Endgerät, das diese IP-Adresse hat, meldet sich dann und teilt seine MAC-Adresse mit. Das anfragende Endgerät speichert die Zuordnung von IP- zu MAC-Adresse in einer internen ARP-Tabelle und sendet zukünftig Dateneinheiten an diese MAC-Adresse. Die eigene ARP-Tabelle kann man sich unter Windows mit dem Kommanda "arp -a" ansehen.

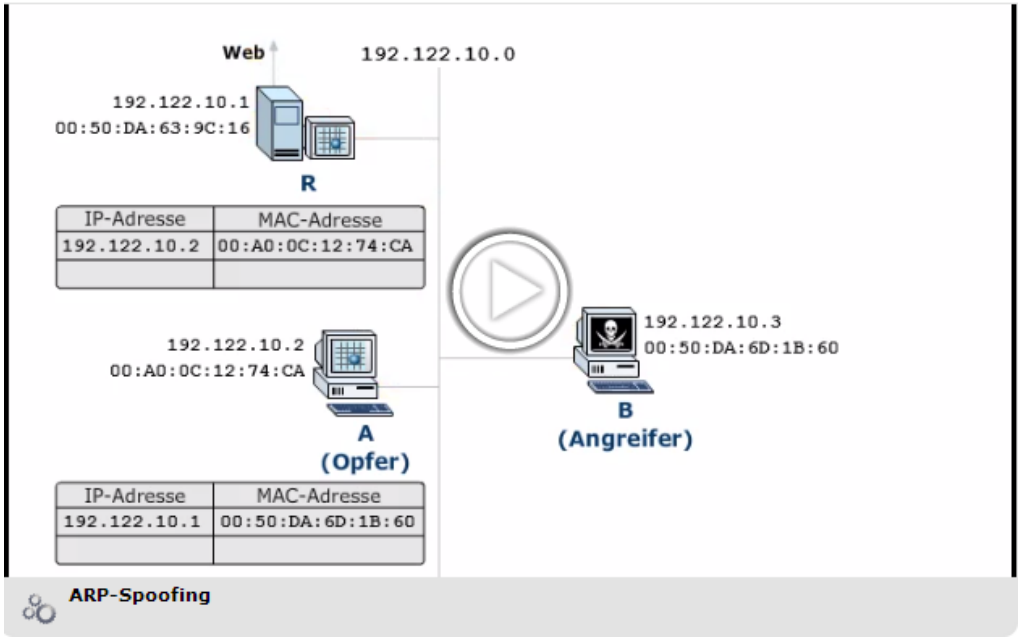
Dieser Vorgang wird beim **ARP Spoofing** (dt. Manipulation) genutzt, um Datenverkehr zu einem Angreifer umzuleiten. Die Rahmen können dann entweder nur ausgelesen oder auch verändert werden. Dabei sendet der Angreifer gefälschte ARP-Pakete an das Opfer. Eine ähnliche Technik – allerdings nicht mit gefälschten Angaben - wird auch beim freiwilligen ARP benutzt und ist daher nicht ungewöhnlich im lokalen Netz. In dem gefälschten ARP-Paket wird die IP-Adresse des Standard-Routers und die MAC-Adresse des Angreifers angegeben. Bei Erhalt dieses Paketes wird das Opfer diese Zuordnung in seine ARP-Tabelle übernehmen; alle weiteren Pakete werden dann an die MAC-Adresse

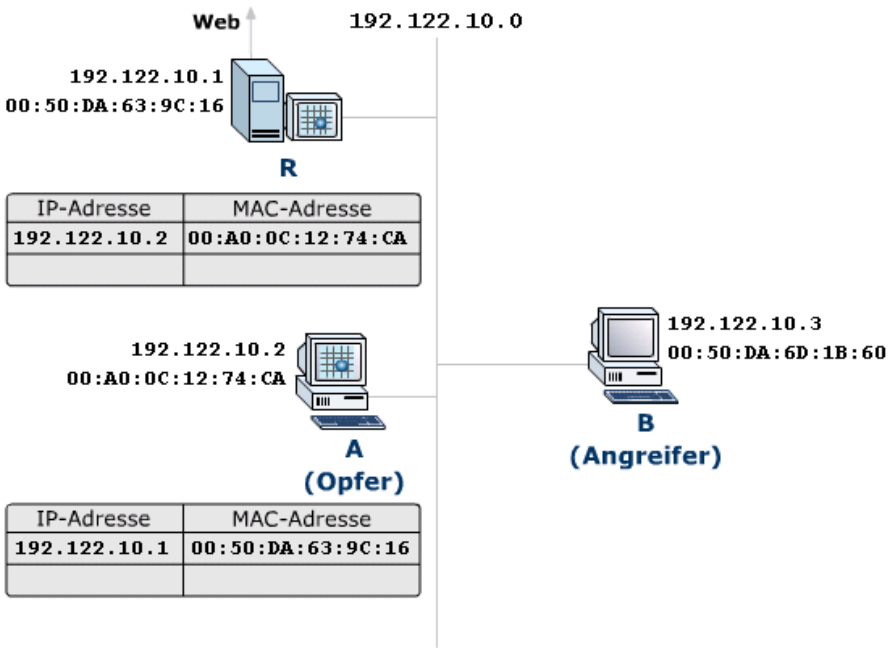
des Angreifers gesendet, der die Pakete manipulieren kann. Die manipulierten Pakete werden anschliessend vom Angreifer dem Standard-Router zugestellt.

In der Online-Version befindet sich an dieser Stelle eine Animation.

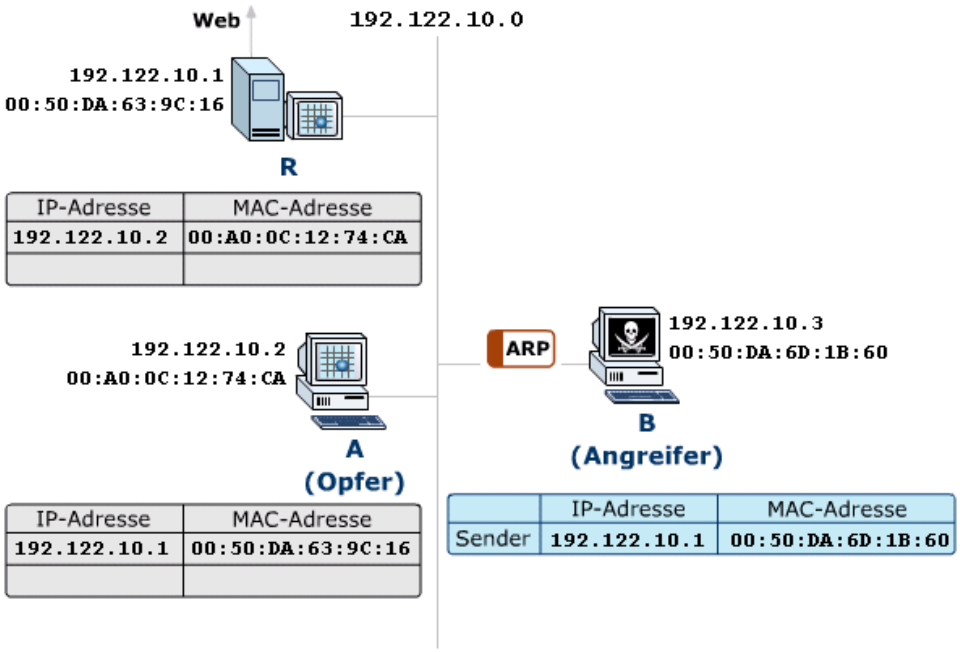
ARP-Spoofing

Anfang Druckversion

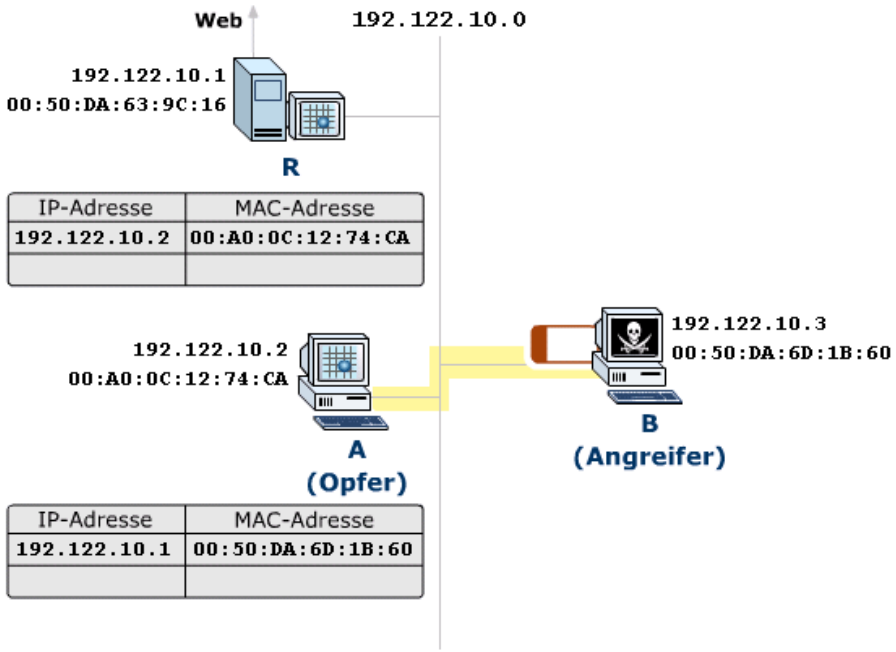




Host A kommuniziert über den Default Router R mit dem Internet. Die notwendigen Einträge sind in den ARP-Tabellen von Host A und dem Router eingetragen.



Der Angreifer B sendet ein ARP-Paket, in dem als IP-Adresse die Adresse des Default-Routers sowie die eigene MAC-Adresse eingetragen sind.



Host A überschreibt die MAC-Adresse des Routers mit der neuen MAC-Adresse und sendet anschliessend alle Pakete, die zum Default Router gehen sollen, an den Angreifer B.

Ende Druckversion

Die Manipulation muss sich nicht zwangsläufig auf den Standard-Router beziehen, sondern kann auch in analoger Weise für die Kommunikation zwischen zwei Rechnern im LAN angewendet werden.

Eine wenig praktikable Art den Angriff zu verhindern besteht darin, nur statische ARP-Tabelleneinträge zu verwenden. Dieses führt jedoch bei Umkonfigurationen zu einem manuellen Pflegeaufwand. Außerdem kann der Fehler schwierig zu finden sein, wenn den Nutzern diese statische Konfiguration nicht bekannt ist.

Zur Abwehr kann auch das Programm arpwatch eingesetzt werden, das Änderungen in der ARP-Tabelle erkennen und melden kann. Insbesondere kann es auffällig sein, wenn mehrere IP-Adressen derselben MAC-Adresse zugeordnet werden.

Für Angriffe dieser Art können Angreifer das im Internet verfügbare Ettercap (siehe Tools zum ARP Spoofing) nutzen.

1.2.2 Angriffe auf drahtlose lokale Netze

In Wireless LAN-Umgebungen ist die Situation prinzipiell so wie sie bei Festnetzen mit Bustopologien in der Vergangenheit war. Es kann jedes Endgerät die gesamte Kommunikation von Endgeräten in seiner Umgebung abhören. Ein Endgerät ist im normalen Betrieb so konfiguriert, dass es zunächst auf die Empfängeradresse von Dateneinheiten schaut, ob die Daten für es bestimmt sind. Dieses kann jedoch leicht umgestellt werden, um alle Dateneinheiten zu erhalten (diese Konfiguration nennt man *Promiscous Mode*).

Außerdem ist es bei ungeschützen WLANs möglich, dieses mitzunutzen und ggf. dort kriminelle Handlungen durchzuführen. Inzwischen ist diese Problematik auch in der Allgemeinheit bekannt, so dass man kaum noch ungeschützte WLANs findet. Laut der derzeitigen Rechtsprechung handelt ein Betreiber (auch eine Privatperson) fahrlässig, die ein WLAN schwach oder ungeschützt betreibt, so dass die sog. Störerhaftung gilt. Zu beachten ist, dass sich ein WLAN nicht leicht auf ein Gebäude beschränken lässt, so dass das WLAN auch außerhalb des Gebäudes abhörbar ist.

Es ist daher notwendig, die Kommunikation in WLANs mit geeigneten Verfahren zu verschlüsseln. Möglichkeiten, nur bestimmten MAC-Adressen die Teilnahme am WLAN zu erlauben sowie die Unterdrückung der SSID, bieten nur einen schwachen Schutz. Die Schutzmöglichkeiten werden insgesamt im Abschnitt "Schutz von drahtlosen lokalen Netzen" diskutiert.

1.2.3 Angriffe auf Mobilfunknetze

Bei Mobilfunknetzen muss man zunächst beachten, dass diese aus dem Funkzugangsbereich (d.h. der drahtlosen Übertragung zwischen der Basisstation und dem mobilen Teilnehmer) und einer festen Infrastruktur bestehen. Innerhalb der festen Instraktur des Netzes wird grundsätzlich nicht verschlüsselt. Die folgende Diskussion bezieht sich daher nur auf den Zugangsbereich via Funk. Ähnlich wie bei Festnetzen muss man technische Möglichkeiten auf höheren Schichten (z.B. VPNs) einrichten, um eine Ende-zu-Ende-Verschlüsselung zu erreichen.

Bei der Funkübertragung ist es notwendig, zwischen den verschiedenen Mobilfunkgenerationen zu unterscheiden. Die folgende Diskussion beschränkt sich auf die für Europa relevanten Technologien.

Bei der zweiten Mobilfunkgeneration, bei der in Europa nur die Technologie GSM und deren Weiterentwicklungen relevant sind, wurden aus heutiger Sicht wesentliche Fehler hinsichtlich der Sicherheit gemacht. Das BSI rät daher von der Verwendung bei sicherheitsrelvanter Kommunikation ab (siehe Sicherheitswarnung). Die Algorithmen, die zur Verschlüsselung implementiert wurden, wurden nicht offengelegt, so dass nicht wie z.B. bei der Standardisierung des Advanced Encryption Standards ein umfangreicher öffentlicher Test möglich war (ein solches Vorgehen wird "Security by Obscurity" genannt). Später wurden die Algorithmen jedoch allgemein bekannt und zeigten deutliche Schwächen. Außerdem erfolgt die Authentifizierung nur einseitig, so dass sich das mobile Endgerät gegenüber dem Netz authentifizieren muss, aber nicht das Netz gegenüber dem mobilen Endgerät. Damit sind gefälschte Basisstationen realisierbar, die das Abhören der Kommunikation ermöglichen (siehe beispielsweise Artikel von Heise.de). Diese Geräte werden IMSI-Catcher genannt, wobei IMSI die eindeutige Identifikation des Nutzers ist (nicht die Telefonnummer, sondern die IMSI ist das eindeutige Identifikationsmerkmal des Nutzers). Diese Identifikation kann also ermittelt werden, so dass die Zwischenschaltung einer falschen Basisstation nicht auffällt. Mittels der freien Software openBTS und geeigneter Hardware konnte ein solcher IMSI-Catcher schon für etwas mehr als 1000 Euro von mehreren Universitäten aufgebaut werden (zuletzt sogar nur für 200 Euro).

Die Verwendung von UMTS und LTE schützt nicht grundsätzlich vor den oben beschriebenen Gefahren. Da die UMTS- und LTE-Netze noch nicht so flächendeckend wie das GSM-Netz aufgebaut sind, ist in diesen Telefonen weiterhin auch eine Kommunikation per GSM vorgesehen, um nicht z.B. in einer ländlichen Gegend gar nicht erreichbar zu sein. Diese Möglichkeit heißt GSM Fallback und kann auch absichtlich herbeigeführt werden, um dann wiederum die genannten Schwachpunkte auszunutzen.

Aber nicht nur durch einen möglichen GSM Fallback kann es zum erfolgreichen Abhören können, sondern auch zu Schwächen bei UMTS an sich, wie eine gravierende Sicherheitslücke im Dez. 2014 zeigte (siehe Tagesschau.de-Meldung). Diese steht im Zusammenhang mit dem Signalisierungssystem im Netz (SS7), mit dem Gespräche aufgebaut werden, so dass die Nutzer hierauf keinen Einfluss haben (siehe Bericht vom 31C3).

Auf seiten der Endgeräte muss man zudem die Entwicklung hin zu Smartphones beachten, die inzwischen einen erheblichen Marktanteil gewonnen haben. Smartphones unterscheiden sich durch ihre Softwarearchitektur nur wenig von Notebooks oder Desktop Computern und benötigen daher einen ähnlichen Schutz mit Virenscannern und Firewalls. Solche Schutzmechanismen sind dort aber nicht etabliert.

1.3 Typische Angriffsarten der Schicht 3

Gliederung

Auf der Vermittlungsschicht sind IP und die dazu gehörigen Managementprotokolle ICMP, IGMP sowie die Routingprotokolle OSPF, IS-IS und BGP heutzutage von zentraler Bedeutung. Alle diese Protokolle wurden vor vielen Jahren für wissenschaftliche Netze entworfen, in denen man sich untereinander vertraut. Erst im Nachhinein wurde versucht, Sicherheitsaspekte zu berücksichtigen, was aber nur teilweise gelang.

Insbesondere kann der Echtheit von IP-Adressen nicht vertraut werden, da diese vom Absender beliebig eingestellt werden können (**IP Spoofing**). Im Netz könnten die Router Adressfälschungen erkennen, wenn Absendeadressen nicht aus einem passenden Adressbereich stammen, was jedoch in der Praxis kaum durchgeführt wird. Daher kann man bei Angriffen wie DDoS-Angriffen davon ausgehen, dass gefälschte IP-Adressen verwendet werden. Die einzige Schwierigkeit aus Angreifersicht ist dabei, dass man keine Antworten erhalten kann. Für Angriffe, wo dieses notwendig ist, müssen Angreifer andere Möglichkeiten finden (siehe Spoofed Scan im Abschnitt Port Scan).

1.3.1 ICMP-Pakete

ICMP lässt sich in vielfältiger Hinsicht missbrauchen, um Angriffe auszuführen.

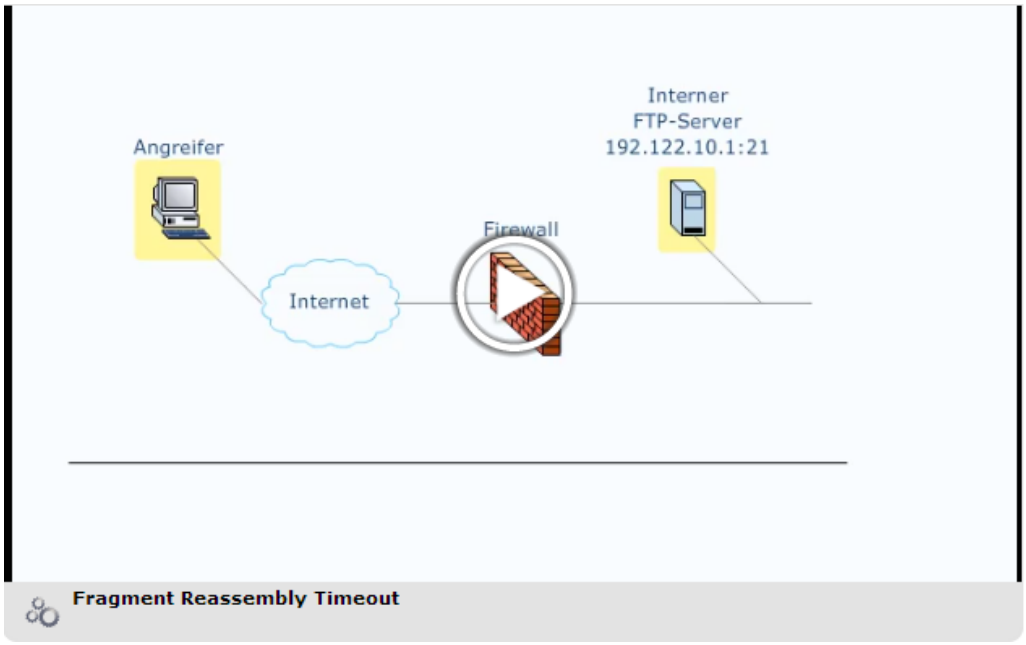
- Durch **ICMP Echo**-Nachrichten kann mit dem Programm ping die Verfügbarkeit eines Rechners festgestellt werden. Hiermit kann man feststellen, welche Rechner insgesamt in einem Netz vorhanden sind.
- Mit einer **ICMP Redirect**-Nachricht kann die Routing-Tabelle geändert werden, um so Pakete an den Angreifer umzulenken, der sie anschliessend weiterleitet, ohne dass der Angegriffene dies bemerken kann.
- Wenn Pakete nicht dem gewünschten Empfänger zugestellt werden können, wird eine **ICMP Destination Unreachable**-Nachricht an den Sender zurückgeschickt, der dann eine bestehende Verbindung abbricht. Falls diese Nachricht gefälscht ist, wird der Sender veranlasst bestehende Verbindungen zu beenden. Dadurch kann eine DoS-Attacke ausgeführt werden.
- Mit dem Senden einer **ICMP Source Quench**-Nachricht wird das Opfer veranlasst seine Übertragungsrate zu reduzieren, da hiermit eine Überlastung des Gegenseite signalisiert wird. Dadurch wird die Kommunikation behindert.
- **ICMP Tunneling** wird eine Angriffsart genannt, bei der die bei einem Angriff benötigten Daten in ICMP-Nachrichten verpackt werden. Wenn eine Firewall ICMP-Nachrichten passieren lässt, können diese Daten z.B. in ICMP Echo-Nachrichten transportiert werden. Da der Inhalt von Echo-Nachrichten für die Echo-Funktion belanglos ist und nicht weiter untersucht wird, eignet sich diese Nachricht als Transport-Medium, um beispielsweise Daten mit einem vorher beim Opfer installierten Server auszutauschen.
- Mit fragmentierten Paketen kann die Existenz eines Hosts festgestellt werden, der durch eine Firewall geschützt ist: Das erste Fragment wird in der Firewall auf Grund seiner Port-Nummer vernichtet; die folgenden Pakete werden von der Firewall durchgelassen, da sie keine Port-Informationen beinhalten. Das Opfer kann die Fragmente nicht reassemblieren, da das erste Fragment fehlt und sendet eine **ICMP Fragment Reassembly Time Exceeded**-Nachricht an den Angreifer zurück, der damit die Existenz des Opfers feststellt.

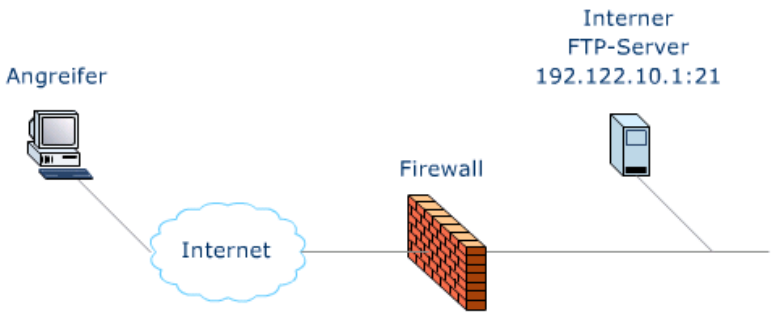
Die folgende Interaktion zeigt ein Beispiel eines Angriffs mit fragmentierten Paketen:

In der Online-Version befindet sich an dieser Stelle eine Animation.

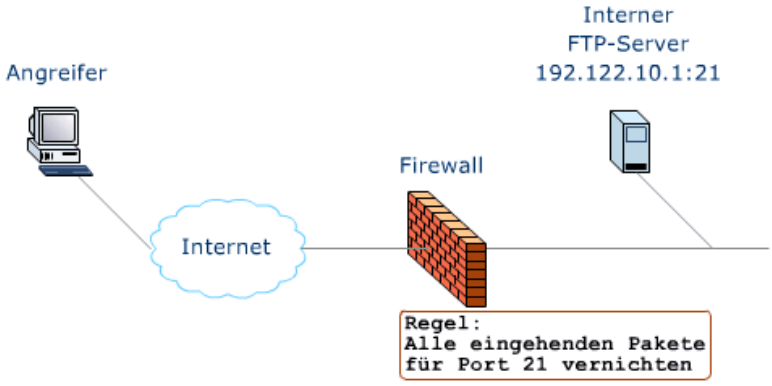
Fragment Reassembly Timeout

Anfang Druckversion

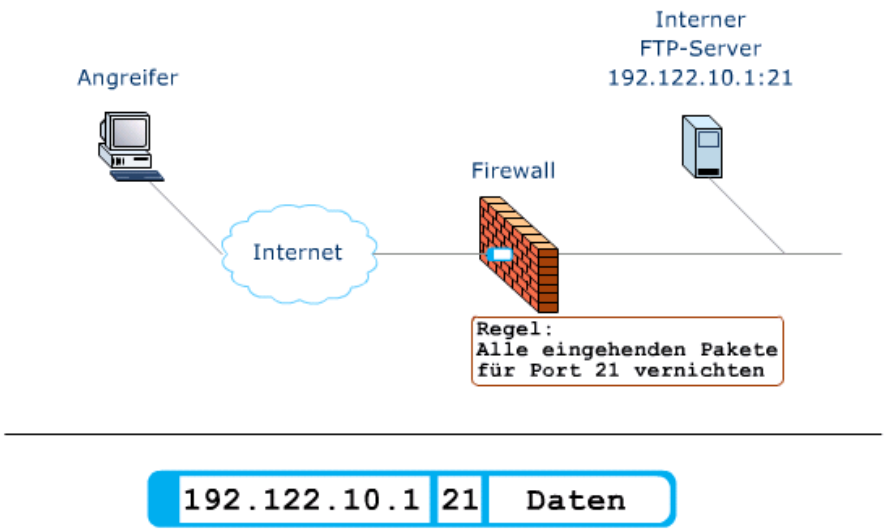




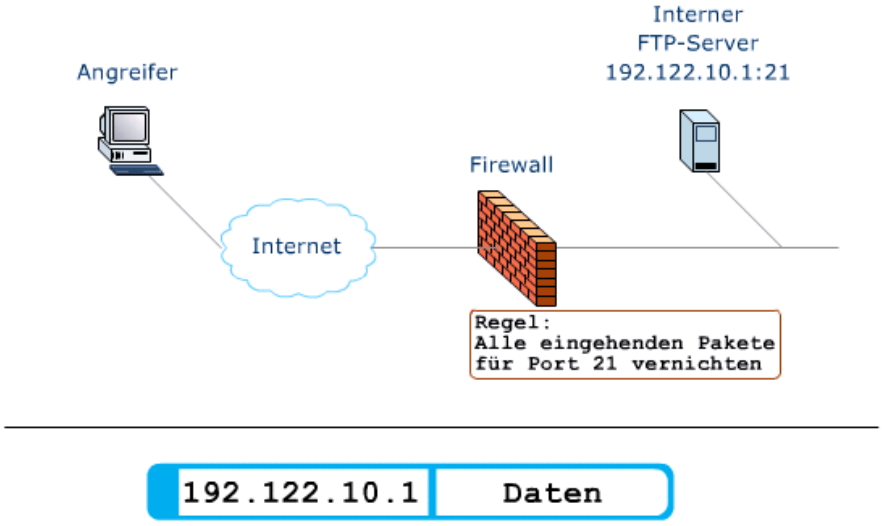
In einer Firma wird ein firmeninterner FTP Server betrieben, auf den vom Internet nicht zugegriffen werden soll.



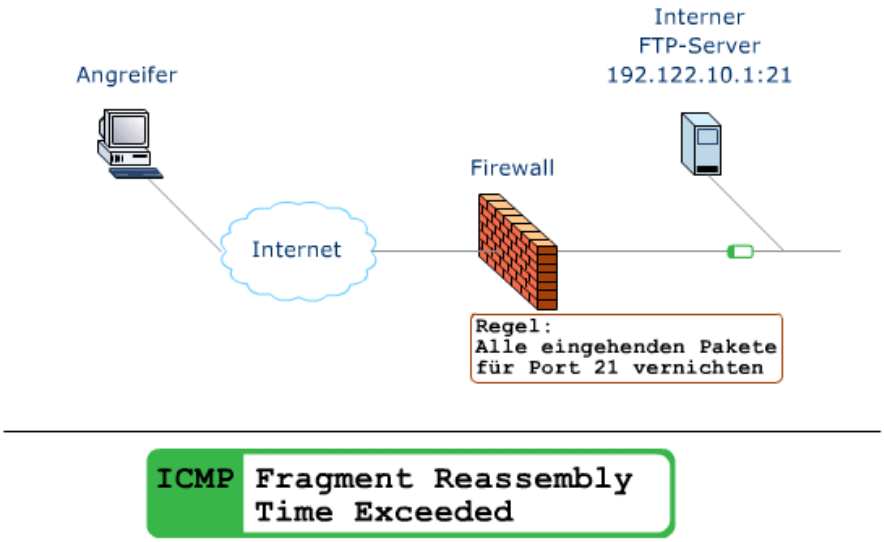
In der Firewall ist eine Regel definiert, die alle Pakete, die von aussen kommen und an Port 21 gerichtet sind, verwirft.



Der Angreifer erzeugt ein Paket für den FTP-Server, das fragmentiert ist. Im ersten Fragment sind der IP Header und der TCP Header mit der Port-Nummer 21 vorhanden. Dieses Paket wird von der Firewall verworfen.



Im nächsten Fragment sind die Portangaben des TCP Headers nicht mehr vorhanden. Dieses Paket wird von der Firewall durchgelassen und dem FTP Server zugestellt.



Da das erste Fragment fehlt, kann der FTP Server die Fragmente nicht zusammensetzen und sendet eine ICMP-Nachricht an den Absender zurück. So erfährt der Absender, dass der FTP Server existiert.
Ende Druckversion

1.3.2 Dynamisches Routing

Wenn es Angreifern gelingt, gefälschte Routing-Informationen an Router zu senden, können die Routing-Tabellen verändert und der Datenverkehr somit umgeleitet werden. Das kann zum Mitschneiden des Verkehr oder zur Durchführung von DoS-Angriffen genutzt werden. Hierbei muss unterschieden werden zwischen dem Routing innerhalb von Netzen eines Dienstanbieters (bezeichnet als *Autonomous System*) und zwischen den Netzen von Dienstanbietern.

Für das interne Routing in einem Netz werden häufig die Protokolle OSPF, IS-IS oder auch das Cisco-eigene Protokoll EIGRP genutzt. Beim OSPF-Protokoll können Passwörter zur Authentifikation benutzt werden. Diese Passwörter werden dann in der Praxis oftmals über lange Zeit nicht mehr verändert. Damit wird der Schutz, der durch das Passwort geboten wird, immer schwächer, da der Angreifer mehr Zeit und ggf. auf mehr aufgezeichneten Datenverkehr hat, das Passwort zu erraten.

Das bei ISPs häufig verwendete IS-IS Protokoll bietet in diesem Zusammenhang einen gewissen Schutz, da die Router untereinander mit einem komplett anderen Adressschema arbeiten. Dieses Protokoll ist nämlich eines der wenigen Protokolle aus der OSI-Welt, welches auch weiterhin Relevanz hat. Daher werden an dieser Stelle OSI-Adressen verwendet. Technisch funktioniert es ansonsten sehr ähnlich wie OSPF.

Für das Routing zwischen Autonomen Systemen wird in der Praxis BGP verwendet. Für dieses sind seit längerer Zeit Schwachpunkte bekannt, ohne dass Gegenmaßnahmen allgemein eingesetzt werden. Der wesentliche Schwachpunkt ist, dass die Routeninformatioen, die bekanntgegeben werden, nicht überprüft werden. Ein einzelner Anbieter, der dabei falsche Routeninformationen bekannt gibt, kann große Teile des Internets beeinflussen, wie ein Vorfall mit einem chinesischen Provider zeigte. Dass die Gefahren bzgl. BGP weiterhin bestehen, wird im einem Artikel von Zdnet.com dargestellt.

Im Jahr 2008 gab eine Situation, bei der die Regierung von Pakistan den Zugang zu Youtube im eigenen Land sperren wollte. Die technische Umsetzung durch die Pakistan Telecom hatte jedoch den Effekt, dass nicht nur der Zugang aus Pakistan nicht mehr möglich war, sondern auch weltweit. Eine wesentliche Rolle spielte in diesem Zusammenhang die Longest Prefix Matching-Regel von BGP, die besagt, dass spezifischere Routeneinträge gegenüber allgemeineren vorzuziehen sind. Pakistan Telecom hatte dabei Routeneinträge vorgegeben, die spezifischer waren als die von Youtube, so dass diese bevorzugt wurden. Youtube reagierte danach, indem man noch spezifischere bekannt gab, um den Verkehr wieder zu sich zu lenken. Erst später wurden die falschen Bekanntgaben zurückgenommen. Eine genaue Beschreibung der Entwicklung wird von RIPE angeboten.

Bei Privatpersonen oder kleinen Firmen, die nur über eine physikalische Leitung zu einem Provider an das Internet angebunden sind, ist diese Problematik nicht relevant. Hier wird das Routing statisch konfiguriert. Sobald die Internetkonnektivität für Organisationen aber sehr wichtig wird, verfügen diese oftmals über doppelte Netzanbindungen, so dass eine eigene Konfiguration von BGP notwendig wird, um den Datenverkehr lenken zu können.

1.4 Typische Angriffsarten der Schicht 4

Gliederung

In der Transportschicht kann durch verschiedenartige **Port Scans** festgestellt werden, welche Dienste auf einem Zielrechner aktiviert sind. Dieses ist aber nur eine Vorbereitung von Angreifern, um dann gezielt Schwachstellen der entdeckten Dienste auszunutzen. Zur Angriffsvorbereitung dient auch die **Betriebssystem-Erkennung**, bei der durch das Verhalten des Rechners, insbesondere als Reaktion auf fehlerhafte TCP-Pakete, die Betriebssystem-Version ermittelt wird.

Aufgefundene Dienste oder deren Netzverbindung können schliesslich durch einen **Denial of Service** (**DoS**) Angriff gezielt überlastet werden, so dass sie nicht mehr verfügbar sind. Solche Angriffe werden meist aus kriminellen Motiven heraus verübt und zielen auf einen wirtschaftlichen Schaden des Betroffenen ab, dessen Dienst dann während des Angriffs nicht mehr verfügbar sind. Oftmals wird Geld gefordert, damit solche Angriffe zukünftig unterbleiben. Eine andere Motivation stellt sog. Haktivism dar. Das sind Aktionen mit ähnlichen Methoden, aber politischen Zielen. So griffen Anhänger von WikiLeaks beispielsweise die Webseiten der Kreditkartenfirma Visa an (siehe Operation Payback).

1.4.1 Port Scan

Bevor Angriffe begonnen werden, wird versucht möglichst viele Informationen über das Opfer zu erlangen. Das Überprüfen offener Ports geht fast immer einem größeren Angriff voraus. Es gibt verschiedene Wege offene Ports zu erkennen:

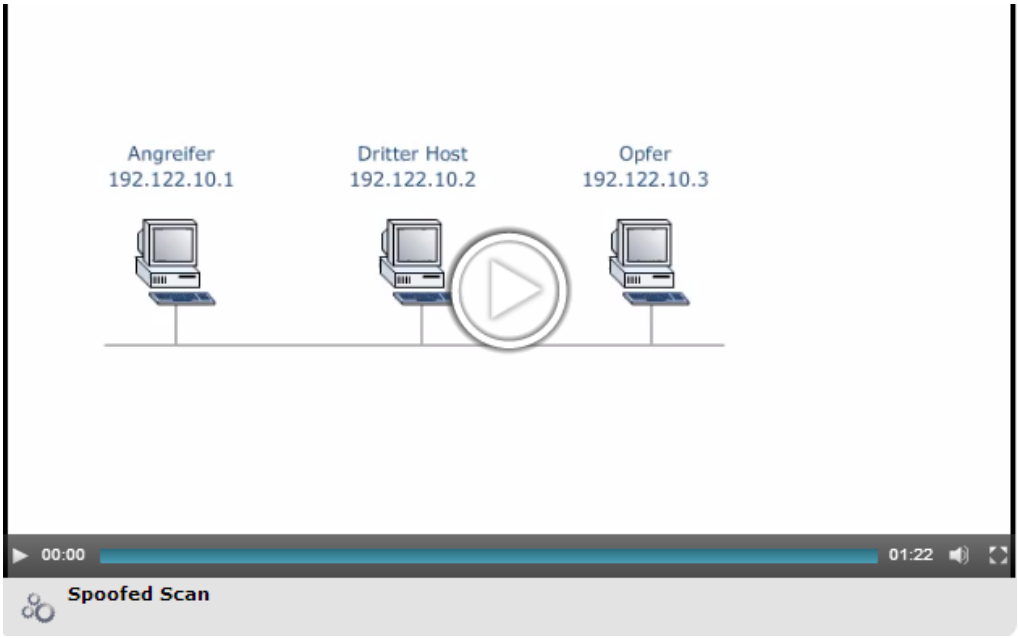
- Mit dem **TCP Connect Scan** wird eine vollständige TCP-Verbindung zum Opfer aufgebaut. Das kann das Opfer leicht erkennen, besonders, wenn in kurzen Abständen nacheinander Ports in aufsteigender Reihenfolge gescannt werden. Wenn Ports allerdings in zufälliger Reihenfolge in zufälligen Zeitabständen gescannt werden, ist dieser Angriff erheblich schwieriger festzustellen.
- Beim **TCP SYN Scan** wird nur ein SYN-Paket zum Opfer gesendet. Wenn ein SYN/ACK-Paket zurückgesendet wird, ist das ein Zeichen dafür, dass der gescannte Port im LISTEN-Zustand ist. Der Angreifer sendet nun ein RST-Paket an das Opfer, um keine vollständige Verbindung zustande kommen zu lassen. Diese Technik fällt viel weniger auf und wird u.U. vom Opfer nicht protokolliert.
- Mit einem **TCP SYN ACK Scan** kann eine statische Firewall durchdrungen werden, der bei einkommenden Paketen nur das ACK-Flag überprüft.
- Beim **TCP FIN Scan** wird nur ein FIN-Paket übertragen. Daraufhin sollte ein RST-Paket zurückgesendet werden, wenn der Port nicht geöffnet ist.

- Beim **TCP Xmas Tree Scan** werden im TCP-Header das FIN-, URG- und das PSH-Flag gesetzt. Daraufhin sollte ein RST-Paket zurückgesendet werden, wenn der Port nicht geöffnet ist.
- Beim **TCP Null Scan** werden dagegen alle Flags ausgeschaltet. Daraufhin sollte ein RST-Paket zurückgesendet werden, wenn der Port nicht geöffnet ist. Dieser Test liefert manchmal Ergebnisse, wo andere Scan-Techniken versagen.
- Mit einem **UDP Scan** wird ein UDP-Paket an einen Port gesendet. Wenn die ICMP-Nachricht "Port Unreachable" zurückgesendet wird, kann man davon ausgehen, dass der entsprechende Port nicht aktiv ist. Im Umkehrschluss kann man u.U. davon ausgehen, dass der Port aktiv ist, wenn keine ICMP-Nachricht zurückgesendet wird. diese Schlussfolgerung ist allerdings unzuverlässig, da UDP-Pakete aus vielen Gründen verloren gehen können.
- Normalerweise ist es für einen Angreifer bei einem Port Scan nicht möglich seine Identität durch Fälschen der IP Adresse zu verheimlichen, denn er würde dann keine Antwort des angegriffenen Systems erhalten. Es gibt Programme, die deshalb viele Scans mit gefälschten Adressen durchführen und nur einen Scan mit der echten Adresse, was zur Verwirrung des Zielsystems führen soll. Allerdings gibt es auch die Möglichkeit einen **gespooften Scan** durchzuführen, bei dem das Opfer nicht die Adresse des Angreifers erkennen kann. Dazu wird ein dritter Host benötigt, der keine aktiven Netzwerkverbindungen hat. Dieser Scan nutzt die Eigenart des IP-Protokolls aus, dass das Identifikations-Feld im IP-Header, das eigentlich nur bei der Fragmentierung benötigt wird, bei bestimmten Betriebssystemen bei jedem gesendeten IP-Paket um eins erhöht wird. Beim Scan laufen folgende Schritte ab: Der Angreifer sendet an den dritten Host in regelmässigen Abständen SYN-Pakete, die dieser mit SYN/ACK-Paketen beantwortet, wobei das Identifikations-Feld jeweils um eins inkrementiert wird. Nun werden vom Angreifer SYN-Pakete an das Opfer gesendet, in denen als Absender die Adresse des dritten Host eingetragen ist – als gespoofte IP-Adresse. Wenn der Port beim Opfer offen ist, schickt das Opfer ein SYN/ACK-Paket an den dritten Host, das dieser mit einem RST-Paket beantwortet und dabei das Identifikations-Feld inkrementiert. Wenn jetzt der Angreifer an den dritten Host ein SYN-Paket sendet, wird er ein SYN/ACK-Paket als Antwort erhalten, in dem das Identifikations-Feld um mehr als eins erhöht wurde. Dadurch erkennt der Angreifer einen offenen Port beim Opfer. Falls der gescannte Port beim Opfer nicht aktiv ist, wird das Opfer ein RST-Paket an den dritten Host senden, der wiederum das Paket nicht beantwortet und insbesondere das Identifikations-Feld dabei nicht erhöht.
- Es sind noch weitere Scan-Techniken möglich, die auch spezielle Eigenschaften der Implementationen ausnutzen.

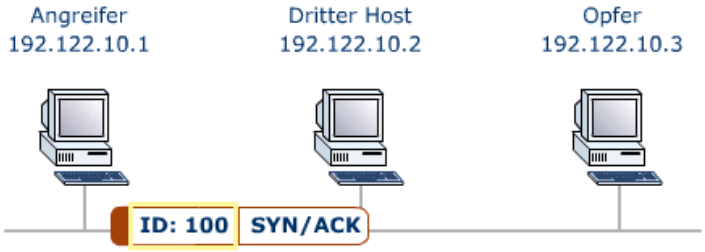
In der Online-Version befindet sich an dieser Stelle eine Animation.

Spoofed Scan

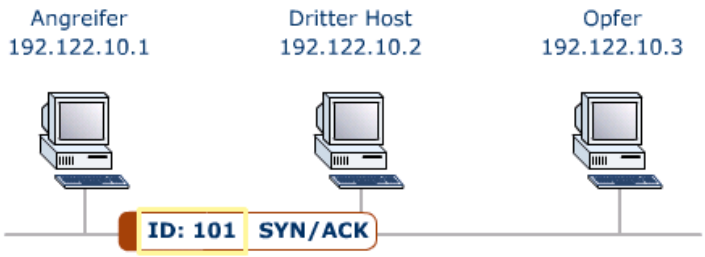
Anfang Druckversion



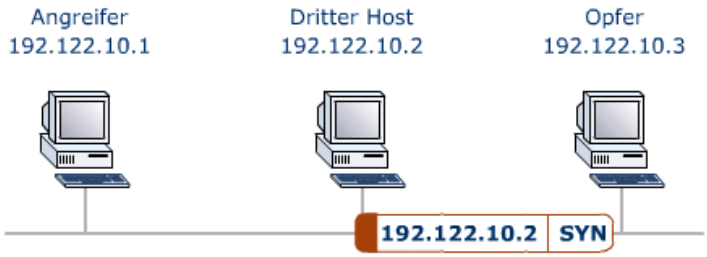
Der Angreifer will einen Port Scan beim Opfer durchführen, aber seine eigene IP-Adresse nicht bekanntgeben. Für die erfolgreiche Durchführung wird ein dritter Host benötigt.



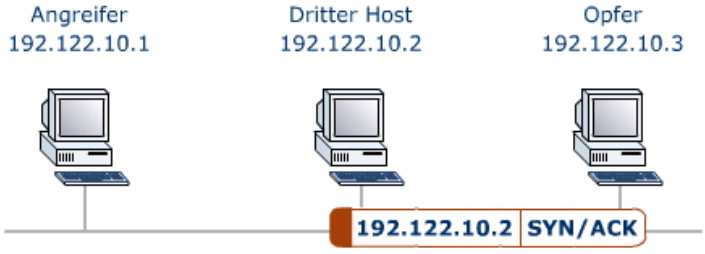
Der Angreifer sendet ein SYN-Paket an den dritten Host, das dieser mit einem SYN/ACK-Paket beantwortet, wobei die Identifikationsnummer im IP-Header gesetzt ist.



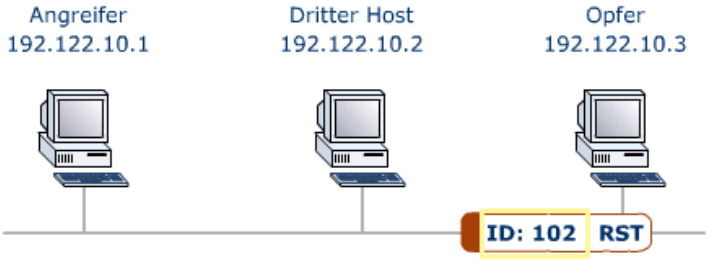
Der Angreifer sendet ein weiteres SYN-Paket an den dritten Host, das dieser wieder mit einem SYN/ACK-Paket beantwortet, wobei die Identifikationsnummer im IP-Header inkrementiert wird.



Jetzt sendet der Angreifer ein Paket an das Opfer, um festzustellen, ob der gewünschte Port aktiv ist. Dabei gibt er als Absender die IP-Adresse des dritten Host an.

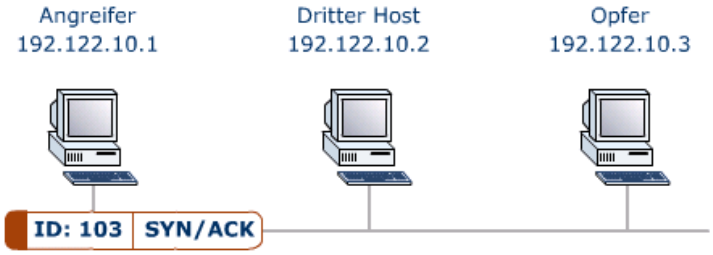


Wenn der Port aktiv ist, sendet das Opfer ein SYN/ACK-Paket an den dritten Host.



Der dritte Host kann mit diesem Paket nichts anfangen und sendet ein RST-Paket an das Opfer wobei er die Identifikationsnummer inkrementiert.

Wenn der Angreifer nun an den dritten Host ein SYN-Paket sendet, erhält er ein Paket, in dem die Identifikationsnummer um zwei erhöht wurde. Daraus schliesst der Angreifer, dass der untersuchte Port beim Opfer aktiv ist.



Ende Druckversion

Bei Port Scans ist es wichtig bemerken, dass es nicht nur die Situationen geben kann, in der ein Port entweder offen oder geschlossen ist. Es kann auch sein, dass eine Firewall zwischendrin das IP-Paket des Angreifers verwirft. Deshalb unterscheidet beispielsweise der Test von Heise.de, mit man seinen eigenen Netzwerkanschluss testen kann, zwischen den Resultaten "open", "closed" und "filtered".

Frage

Ist es Sicht des Angreifers unterscheidbar, ob ein Port geschlossen ist oder der Zugriff von einer Firewall verhindert wurde?

Lösung zeigen

Das kommt auf die Art des Port Scans an. Beim einfachen TCP Port Scan macht das einen Unterschied, weil einmal ein RST-Segment zurück kommt, das andere Mal aber gar keine Antwort. Beim Spoofed Scan kann man das nicht feststellen. Das Opfer antwortet nach Verwerfen des Segments durch die Firewall gar nicht, was aber denselben Effekt wie das RST des Opfers auf dem dritten Rechner hat, nämlich dass das Identifikationsfeld auf dem dritten Rechner nicht erhöht wird.

1.4.2 Betriebssystem-Erkennung

Ein wesentlicher Punkt zur Nutzung von Sicherheitslücken ist die **Betriebssystem-Erkennung** beim Opfer. Die Implementierung des TCP/IP Stacks weicht in den verschiedenen Betriebssystemen leicht voneinander ab. Das hat damit zu tun, dass bei der Spezifikation der Protokolle nicht für jeden Fehlerfall ein exaktes Verhalten festgelegt ist. Jedes System reagiert mit einem bestimmten Muster, das auch als „Fingerprint“ bezeichnet wird. An welchen Merkmalen lässt sich nun ein Betriebssystem erkennen?

Beispiel

Einige Beispiele sind:

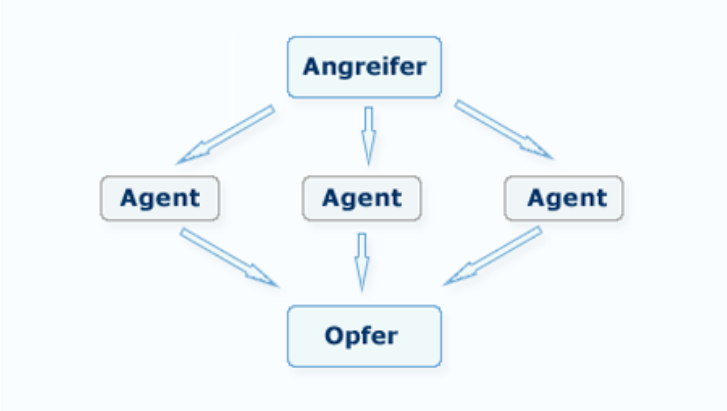
- Wenn nur ein **FIN-Paket** an einen aktiven Port gesendet wird, sollte es keine Antwort geben. Windows NT antwortete aber mit einem FIN/ACK-Paket.
- Die **Initial Sequence Number** wird durch eine einfach gehaltene Zufallsprozedur ausgewählt. Windows NT variierte die ISN um einen Wert von 16.
- Apple OS Version 7 setzte standardmäßig das **Don’t Fragment Flag** im IP-Header.
- Die Reaktion bei sich überlappenden **Fragmenten** ist verschieden: Manchmal überschreiben Fragmente mit höherem Offset Pakete mit kleinerem Offset, manchmal ist es andersherum.
- Viele Dienste senden nach dem Verbindungsaufbau einen **Banner**, der direkt die Anwendung benennt und auch auf das Betriebssystem schliessen lässt. FTP, Telnet, HTTP, SMTP und POP3 reagieren so. Aus diesem Gund wird die Übermittlung von Bannern häufig modifiziert oder ganz deaktiviert.
- Als weitere Merkmale können die Behandlung von ICMP-Nachrichten oder Standard-Einstellungen für das **Identifikations-Feld** und das **TTL-Feld** im IP-Header überprüft werden.
- Weitere Merkmale der Implementierung von TCP können benutzt werden, wie die Behandlung von **RST-Paketen**, die Unterstützung von **ECN** und Optionen oder die Größe des benutzten Fensters.

Eine Betriebssystemerkennung kann insbesondere mit nmap durchgeführt werden (siehe nmap Book, was diese Funktion noch genauer erklärt).

1.4.3 Denial of Service (DoS)

Gliederung

Als **Denial of Service** (**DoS**) werden Angriffe bezeichnet, deren Ziel es ist, einen Dienst außer Kraft zu setzen. So sind eine ganze Reihe von Angriffen auf WWW-Server großer Anbieter bekannt geworden. Es gibt verschiedene Möglichkeiten dazu. Die System-Ressourcen werden bei DoS-Angriffen wesentlich stärker beansprucht als im normalen Betrieb. Auch können Implementierungsschwächen ausgenutzt werden.



Verteilter DoS-Angriff

Bei einem verteilter DoS-Angriff (**Distributed DoS**, **DDoS**) greifen gleichzeitig verschiedene kompromittierte Systeme das Opfer an, wobei jedes einzelne System einen DoS-Angriff ausführt. Laut BSI-Lagebericht 2014 gab es in Deutschland 2104 mehr als 32.000 solcher Angriffe. Der Angreifer muss möglichst viele Systeme erobert haben, um Agenten installieren zu können, die den eigentlichen DoS-Angiff ausführen sollen. Dieses Systeme heißen dann **Bots**. Die Infizierung wird meist automatisch mittels Schadsoftware durchgeführt. Dabei wird nach fehlerhaft konfigurierten Systemen oder angreifbaren Softwarepaketen gesucht. Nach Installation der Agenten-Software auf diesen Systemen, z.B. durch Versenden von Trojanern in Emails, warten die Agenten auf Anweisungen, bevor sie gleichzeitig einen massiven Angriff auf das Opfer starten. Einige Arten erlauben sogar eine verschlüsselte Kommunikation zwischen den Angreifer und den Agenten.

Im Folgenden werden einige mögliche Angriffe beschrieben:

- Bei manchen Angriffen wird einfach eine große Flut von unsinnigen Daten erzeugt und diese in Richtung des Servers geschickt. Dieses ist beispielsweise mit dem LOIC Tool möglich und erreicht seine Wirkung, wenn das von vielen gleichzeitig gemacht wird. Bei diesem simpel zu bedienenden Tool kann man auch leicht das Kommando über den eigenen Rechner an einen Koordinator abgeben (über einen IRC-Kanal), der dann die Angriffe steuert.
- Beim **SYN Flooding-Angriff** werden SYN-Segmente an einen aktiven Port (z.B. Port 80, HTTP) gesendet. Der Server sendet ein SYN/ACK-Segment zurück, das aber nicht vom Angreifer beantwortet wird, sodass die Verbindung nicht vollständig aufgebaut wird. Der Server merkt sich diese halb-offene Verbindung in einer besonderen Warteschlange, die nicht sehr groß ist. Im normalen Betrieb wird sehr schnell das abschliessende ACK-Segment des Clients gesendet. Damit ist dann die Verbindung vollständig aufgebaut und kann aus der Warteschlange für halb-offene Verbindungen entfernt werden. Wenn das abschliessende ACK-Segment nicht eintrifft, bleibt die halb-offene Verbindung in der Warteschlange erhalten und wird erst nach einem Timeout, der im Minuten-Bereich liegen kann, entfernt. Außerdem wiederholt der Server mehrmals das SYN/ACK-Segment (z.B. fünf mal). Beim Angriff werden viele halb-offene Verbindungen erzeugt, sodass die Warteschlange schnell vollläuft und damit keine anderen Verbindungen mehr bedient werden können – damit ist der Dienst lahmgelegt. Der Angriff benötigt nur eine geringe Bitrate, da nur wenige Segmente an den Server gesendet werden müssen, um ihn zu überlasten. Da darüberhinaus die Absender-IP-Adressen bei diesem Angriff fast immer gefälscht werden, ist es schwierig den Angreifer zu identifizieren.
- Es gibt Gegenmaßnahmen, mit denen man die Auswirkungen von SYN Floods begrenzen kann. Dabei erfolgt die Reservierung von Ressourcen auf dem angegriffenen System erst nach erfolgreichem Three-Way-Handshake. Die Angreifer können den Angriff aber modifizieren und führen den TCP-Verbindungsaufbau zuende, aber senden dann auf aktiven Verbindungen nur wenig Daten. Wenn sie relativ viele dieser Verbindungen aufgebaut haben, wird der Server überlastet (siehe Slowloris Tools). Der modifizierte Angriff funktioniert jedoch nicht mit gefälschten IP-Adressen, sondern setzt viele Bots voraus.
- Bei einem **Smurf-Angriff** werden die Auswirkungen eines Angriffs verstärkt. Dazu wird eine ICMP-Echo-Anfrage an die Broadcast-Adresse des Netzes oder Sub-Netzes gesendet. Alle aktiven Hosts senden daraufhin eine ICMP-Echo-Antwort an den Absender zurück. Dieses Verfahren wird in der Praxis häufig von Netzwerk-Management Stationen eingesetzt, um festzustellen, welche Hosts im Netz aktiv sind. Beim Angriff wird die Absender-Adresse des Angreifers durch die Adresse des Opfers ersetzt, das dann alle Antworten erhält. Die Anzahl der Rechner,

die die Antworten senden, wird als **Verstärkungsrate** bezeichnet. Wenn die Verstärkungrate gross ist, können das Ziel-Netzwerk oder der Ziel-Rechner leicht überflutet werden. Es wird auch eine Variante dieser Angriffsart eingesetzt, da Router häufig ICMP-Nachrichten mit einer Broadcast-Adresse nicht weiterleiten. Bei einem **Fraggle-Angriff** werden deshalb UDP-Pakete an die Broadcast-Adresse des verstärkenden Netzwerkes gesendet, typischerweise an den Echo-Port 7. Jedes System, auf dem der Echo-Dienst aktiv ist, sendet dann das Paket an das Opfer weiter, wodurch eine große Datenmenge erzeugt wird. Wenn der Echo-Dienst nicht aktiv ist, wird immerhin noch eine ICMP-Nachricht „Port Unreachable“ erzeugt und an das Opfer gesendet.

Eine Sammlung von Informationen zu DDoS-Angriffen wird von Google Ideas und Arbor Networks angeboten.

1.4.3.1 DoS auf DNS-Basis

Das DNS dient bekanntlich zur Auflösung von symbolischen Namen in IP-Adressen. Hierbei gibt typischerweise ein Name Server in der jeweiligen Zone Auskunft über die Auflösung der zu dieser Zone gehörenden Namen. Man spricht hier von Authoritative Name Server. So kann man beispielsweise beim Server dns.fh-luebeck.de die IP-Adresse des WWW Servers der FH Lübeck erfragen. Während dieses beim Besuch der FH Lübeck-Webseite mit einem Browser automatisch im Hintergrund passiert, kann man das auch explizit mit dem Kommandozeilen-Tool *nslookup* durchführen, in dem man "nslookup www.fh-luebeck.de dns.fh-luebeck.de" eingibt.

Es gibt jedoch auch zahlreiche DNS Server im Internet, die so eingestellt sind, dass sie auch Anfragen beantworten, die nicht die eigene DNS Zone betreffen. Beispielsweise kann man auch den öffentlichen DNS Server von Google, der die IP-Adresse 8.8.8.8 hat, anfragen, welche Informationen dort über den WWW Server der FH Lübeck gespeichert sind ("nslookup www.fh-luebeck.de 8.8.8.8"). Die Antwort wird hier als "nicht autorisierende" Antwort gekennzeichnet. Während diese Art von Caching in vielen Fällen nützlich ist, bietet sie jedoch auch eine Möglichkeit einen DoS-Angriff zu begünstigen.

Diese Art Angriff wird als **DNS Amplification Attack** (oder auch **DNS Reflection Attack**) bezeichnet, also eine Verstärkung eines Angriffs mit Hilfe des DNS. Der wesentliche Punkt des Angriffs besteht darin, dass die Angreifer unter Verwendung von gefälschten IP-Adressen kleine Anfragen an diese öffentlichen DNS Server schicken, die mit großen Antworten beantwortet werden. Die falsch angegebene IP-Adresse ist diejenige des Ziels, was angegriffen werden soll. Als Voraussetzung für diesen

Angriff müssen den öffentlichen DNS Servern manchmal lange Einträge untergeschoben werden, falls diese nicht von sich aus schon solche Einträge erhalten. Ironischerweise eignen sich gerade die neu eingeführten Felder von DNSSEC sehr gut für diesen Zweck.

Am 19. März 2013 wurde eine solcher Angriff auf die Anti-Spam-Organisation Spamhaus.org durchgeführt, der zu dem bis dahin größten DDoS-Angriff führte. Konkret wurden aus 36 Bytes, die an die öffentlichen DNS Server geschickt wurden, 3000 Bytes große Antworten, was zu einen durchschnittlichen Datenvolumen von 75 Gbit/s beim Zielnetz führte (in der Spitze 300 Gbit/s). Seitdem konnten zwei Verdächtige verhaftet werden.

Eine Erklärung zu dieser Art von DDoS-Angriffen ist im Blog von Cloudflare, einer auf die Abwehr von solchen Angriffen spezialisierten Firma, zu finden.

1.4.3.2 DoS auf NTP-Basis

Das Network Time Protocol dient im Internet zum Austausch von Zeitinformationen. Ähnlich wie beim DNS stehen auch hier zahlreiche Server öffentlich zur Verfügung. Mit dem monlist-Kommando, das eine Liste von zuletzt durchgeführten Anfragen an den NTP Server herausgibt, können aus einer 234 Byte großen Anfrage Antworten mit einer Länge von bis zu 48 KByte generiert werden (siehe Artikel im CloudFlare Blog). Ein Blog-Eintrag von Symantec zeigt Angriffe mit dieser Methode, die Ende 2013 durchgeführt wurden. Das monlist-Kommando ist inzwischen aus NTP entfernt worden.

Laut BSI-Lagebericht 2014 sank die Zahl von NTP Servern in Deutschland, die sich für diese Art Angriff missbrauchen lassen zwischen Juni und August 2014 von 4000 auf 2500. Die Betreiber wurden gezielt vom BSI über die Problematik informiert.

1.4.3.3 DoS-Angriffe bei Persistent HTTP

Die Auslieferung von Webseiten erfolgt mit Hilfe von HTTP, wobei HTTP auf TCP basiert. Es gibt verschiedene Varianten von HTTP, die TCP-Verbindungen unterschiedlich nutzen. Aus der Sicht der Leistungsfähigkeit wäre die Verwendung von Persistent HTTP zu empfehlen, aber diese Möglichkeit kann von Angreifern zu DDoS-Angriffen genutzt werden.

Um dieses nachvollziehen zu können, werden an dieser Stelle, die drei HTTP-Varianten erklärt.

- Non-persistent HTTP: Die urspüngliche HTTP-Implementierung (HTTP 1.0) stammt noch aus einer Zeit (1996), in der Webseiten sehr textlastig waren und, wenn überhaupt, nur wenige Bilder oder andere Objekte enthielten. Es wird zunächst eine TCP-Verbindung verwendet, um den Text von der Seite zu laden. Die Seite wird vom Client ausgewertet und dann wird nacheinander für jedes Objekt in der Webseite eine TCP-Verbindung geöffnet, um es zu laden. Das ganze ist relativ ineffizient, zum einen wegen der häufigen TCP-Segmente zum Beginnen und Schließen von Verbindungen (Three-Way-Handshake und Four-Way-Close) und zum anderen wegen der geringen Datenrate am Anfang von TCP-Verbindungen (Slow Start).
- Multiple Simultaneous Connections: Vom damals führenden Browseranbieter Netscape wurde dann eine verbesserte Methode implementiert, mit der parallele TCP-Verbindungen genutzt werden. Der Text in der Webseite wird wie bisher in einer einzigen TCP-Verbindung geladen, die Objekte in der Seite jedoch mit einer Anzahl von parallelen Anfragen. Beispielsweise könnten immer sechs Objekte in parallel laufenden TCP-Verbindungen angefragt werden. Die Anzahl der insgesamt verwendeten TCP-Verbindungen bleibt jedoch gleich.
- Persistent HTTP: Mit HTTP 1.1 wurde als empfohlene Methode das Persistent HTTP eingeführt (auch als Keep Alive bezeichnet). Hiermit wird eine TCP-Verbindung nicht nach jedem Objekt geschlossen, sondern offen gehalten bis über die Verbindung alle Objekte transferiert wurden. Damit lässt sich das häufige Öffnen und Schließen von TCP-Verbindungen vermeiden. Außerdem kann innerhalb der TCP-Verbindung eine hohe Datenrate erreicht werden, sobald die Slow Start-Phase beendet ist. Das ganze lässt sich mit Request Pipelining noch verbessern, bei dem man auch innerhalb der Verbindung gleich mehrere Objekte kurz nacheinander anfragt, ohne das jeweils vorherige Objekt schon erhalten zu haben. Diese weitere Verbesserung ist aber nicht wesentlich und begünstigt die im folgenden dargestellte Schwachstelle hinsichtlich DDoS. An dieser Stelle ist aber zu bemerken, dass Persistent HTTP nur bei Objekten möglich ist, die vom selben Server geladen werden. Moderne Webseiten enthalten aber in vielen Fällen Objekte von einer Reihe von verschiedenen Servern, so dass diese Verbesserung nur teilweise anwendbar ist.

Insgesamt bleibt dennoch soweit der Eindruck, dass das Persistent HTTP nur Vorteile bietet, insbesondere da die Nutzer eine rasche Auslieferung von Webseiten erwarten. Diese Methode hat aber den Nachteil, dass sie DDoS-Angriffe begünstigt. Dieses liegt daran, wie die TCP-Verbindungen geschlossen werden. Bei den vorherigen Methoden ist klar, wann eine Verbindung nicht mehr benötigt wird. Sie wird zur Übertragung eines Objekts benötigt und so kann der Server die Verbindung nach Beendigung der

Übertragung schließen. Beim Persistent HTTP weiß der Server jedoch nicht, wieviele Objekte der Client in Zukunft noch über die Verbindung übertragen möchte. Er verlässt sich daher auf den Client, dass dieser die Verbindung schließt. Er selber hat eine relativ lange Wartezeit (z.B. 60 s), bis zu der er von sich aus die Verbindung beendet. Dieses bietet nun die Möglichkeit für DDoS-Angriffe, bei der Angreifer viele TCP-Verbindungen öffnen und diese nicht von sich aus schließen. Dadurch wird der Server, der irgendwann das Maximum der möglichen TCP-Verbindungen erreicht überlastet und kann keine weiteren TCP-Verbindungen mehr annehmen. Diese Problematik sollte man bei der Konfiguration eines Servers bedenken und entweder kein Keep Alive verwenden oder die Timeout-Zeit relativ kurz ansetzen.

Der Firefox-Browser bietet mit dem AddOn Firebug (Reiter Netzwerk) eine ausführliche Analysemöglichkeit für die TCP-Verbindungen bei der Auslieferung einer Webseite und deren zeitliche Reihenfolge. Mit dem auf Empfehlungen von Yahoo basierenden AddOn YSlow ("Warum langsam?") werden zudem Tipps gegeben, wie man als Betreiber des Servers die Auslieferung verbessern kann. YSlow wird als zusätzlicher Reiter in Firebug angezeigt. Eine vergleichbare Funktionalität wie Firebug ist im Google Chrome Browser bereits enthalten (Navigation auf der rechten Seite, weitere Tools, Entwicklertools).

1.4.3.4 Botnetze

Mit dem Begriff **Botnetz** sind Rechner (Bots) gemeint, in die Angreifer unbemerkt eingebrochen sind und die nun für Angriffe mißbraucht werden können. Der Nutzer eines Bots ahnt nicht, dass sein Rechner unterwandert wurde, da sich der Rechner unauffällig verhält. Das BSI schätzt im Lagebericht 2014, dass 1 Mio. internetfähige Geräte in Deutschland zu Botnetzen gehören. Neben dem Ausführen von DoS-Angriffen ist der Versand von Spam die typischte Verwendung von Botnetzen. Eine weitere Verwendung ist das Bitcoin Mining, bei der Währungseinheiten der Internetwährung Bitcoins von den Bots errechnet werden. Außerdem können angebliche Klicks auf Werbeanzeigen erzeugt werden (sog. *Click Fraud*). Im Bundestagswahlkampf 2013 wurde ein Unterstützer-Blog für Peer Steinbrück mit solchen Methoden lahmgelegt und daraufhin nicht weiter betrieben (siehe Meldung der Agentur).

Botnetze waren in der Vergangenheit hierarchisch strukturiert. Von Rechnern an der Spitze der Hierarchie (Command & Control Server) konnten Kommandos an die Bots versandt werden, die diese dann ausgeführt haben. Die Hierarchie konnte auch mehrstufig organisiert sein, so dass Bots die Kommandos an weitere Bots weiterleiteten. Um das Jahr 2011 konnte mehrere große hierarchische Botnetze zerschlagen werden.

Der signifikanteste Fall war dabei das Rustock Botnet, welches eine in die Millionen gehende Zahl von Microsoft Windows PCs befallen hatte. Die Beseitigung des Botnetzes im März 2011 hatte eine wesentliche Auswirkung auf den weltweiten Spam-Versand.

Aus der allgemeinen Netzwerkforschung ist bekannt, dass Peer-to-Peer-Netzwerke eine deutlich robustere Struktur aufweisen und auch dann noch funktionieren, wenn Teile des Netzwerkes beseitigt sind. Diese Erkenntnisse machten sich nach 2011 auch die Betreiber von Botnetzen zunutze, so dass schwer zu entfernende Netze mit Millionen von Bots gefunden wurden (siehe z.B. Artikel über versuchte Zerschlagungen des ZeroAccess Netzes oder Seite 4 und 5 im Sophos-Bericht 2014). Die typische Methode der Beseitigung des Botnetzes ist die Einschleusung von abgesicherten Rechnern in die Liste der Peers, die jeder Bot für sich verwaltet. Besteht diese Liste schließlich nur noch aus diesen abgesicherten Rechnern, so wurde der Bot erfolgreich vom Botnetz getrennt (die Technik nennt sich *Sinkholing*). Die Progammierer der Botnetze haben jedoch Methoden entwickelt, um dieses zu verhindern und immer weitere von ihnen kontrollierte Bots in den Peer-Listen zu halten. Außerdem werden sog. Domain Generator Algorithms eingesetzt, mit denen Kandidaten für Domains, unter den das Botnet zu erreichen ist, erzeugt und anschließend ausprobiert werden.

Die Größe von P2P Botnetzen kann zudem schwerer eingeschätzt werden als bei den hierarchischen Botnetzen (siehe Heise.de Meldung).

Im Bereich von der Botnetze hat sich eine organisierte Krimialität entwickelt, bei der Netze mit 10.000 Systemen über 200 Dollar für einen Tag "gemietet" werden können (laut BSI Lagebericht 2011).

Nicht nur Desktop Computer oder Notebooks können Teil eines Botnetzes werden. Viele Geräte, die heutzutage netzwerkfähig sind (Babyphones, Überwachungskameras), wurden auch schon über das Internet angeriffen und so zum Teil eines Botnetzes. Damit bringt das Internet of Things auch neue Gefahren mit sich. Im Jahr 2014 betraf dieses besonders Heim-Router des Herstellers AVM ("Fritzbox") (siehe beispielweise [http://www.heise.de/security/meldung/AVM-Router-Weitere-Luecke-in-der-FritzBox-Fernwartungsfunktion-2296040.html diesen Heise.de-Artikel), bei dem die Fernwartungsfunktion erhebliche Schwächen aufwies.

Im Jahr 2012 wurde ein aufsehenerregender Fall namens Carna Botnet bekannt, welches mit Hilfe von übernommenen fremden Geräten einen kompletten Scan aller IPv4-Adressen durchführte (Artikel bei Spiegel Online). Dieses Botnetz war an sich harmlos und wurde nur zu einer Art von Vermessung des Internets genutzt, bei der die Bots sämtliche IPv4-Adressen nach Geräten absuchten. Das Botnetz war sehr

erfolgreich darin unter Verwendung von schwachen Login/Passwort-Kombinationen (etwas "admin"/"admin") in netzwerkfähige Geräte wie DSL Router einzudringen.

1.5 Typische Angriffsarten der höheren Schichten

Gliederung

Mit den höheren Schichten sind die Schichten oberhalb der Transportschicht, also die Anwendungen gemeint. Auf dieser Ebene gibt es vielfältige Angriffsmöglichkeiten, die u.a. Schadsoftware, Manipulationen von Anwendungen, das Brechen von Passwörtern und Social Engineering umfassen.

Einen wesentlichen Einfluss auf dieses Gebiet hat die Tendenz zum Cloud Computing, bei dem viele Daten und Anwendungen in das Internet ausgelagert werden. Dies ist von der Kostenseite häufig eine attraktive Lösung, aber es entstehen zusätzliche Sicherheitsrisiken, insbesondere im Hinblick auf die Vertraulichkeit der Daten. Hierbei ist zu entscheiden, wie es bewertet, wenn sich das Rechenzentrum des Cloud-Anbieters garantiert in Deutschland befindet oder man keine Information darüber hat, wo die Daten am Ende verarbeitet werden.

1.5.1 Passwort- und Identitätsdiebstahl

Gliederung

Die Authentifizierung beim Zugriff auf Anwendungen wird in den meisten Fällen durch Kombinationen von Nutzerkennung (Login) und Passwort geregelt. Dabei haben viele Nutzer häufig mehrere dutzend solcher Login/Passwort-Kombinationen, um privat und beruflich verschiedenste Dienste nutzen zu können. Hierbei besteht die Schwierigkeit, wie man mit diesen Passwörtern umgeht. Schwer zu erratende Passwörter sind meistens auch schwer zu merken, so dass die Nutzer zwischen dem Verwenden von einfachen Passwörtern (z.B. Name des Familienhundes) oder dem Aufschreiben von Passwörtern wählen müssen. Alternativ werden Password Safes angeboten, die mit einem Master-Passwort geschützt sind und darin die weiteren Passwörter speichern. Sie können auch sichere Passwörter generieren. Der alternative Password Safe Master Password generiert dagegen die anwendungsspezifischen Passwörter bei Bedarf stets neu aus dem Master Password, Nutzernamen und Anwendungsnamen, so dass es keine Passwortdatei gibt, die kompromittiert werden könnte. Man vertraut dabei jedoch auf die Sicherheit der speziellen Hashfunktion PBKDF2. Mit Password Safes sind generell separate Programme und nicht die Passwortspeicherfunktionen in Webbrowsern gemeint, die als unsicher gelten.

Als Alternative zu Login/Passwort-Kombinationen kommen Fingerabdrucksensoren in Frage. Diese lassen jedoch teilweise mit nicht allzu hohem Aufwand überlisten, wie die Fälle des iPhone 5 und iPhone 6 zeigen.

Eng verwandt mit dem Thema Passwortdiebstahl ist das Thema Identitätsdiebstahl. Wenn man die Login/Passwort-Kombination eines anderen Nutzers erlangt hat, kann man mit dessen Identität Handlungen vornehmen. Ein Identitätsdiebstahl liegt aber auch schon vor, wenn Kreditkartendaten zusammen mit Adressdaten erbeutet wurden, ohne dass die Angreifer auch die PIN haben. Der Begriff Identitätsdiebstahl ist also allgemeiner zu sehen.

1.5.1.1 Passwörter im Klartext

Passwörter und Benutzerkennungen zur **Authentifizierung** von Anwendern werden von einigen älteren Protokollen im Klartext übertragen. Diese Protokolle, zu denen FTP, Telnet, SMTP, POP3/IMAP, HTTP, wenn eine Authentifizierung erforderlich ist, und SNMPv1/SNMPv2 gehören, sollten daher nicht mehr oder nicht mehr ungeschützt eingesetzt werden.

Telnet sollte generell verboten werden und stattdessen nur noch **SSH** (Secure Shell) eingesetzt werden. Bei anderen (SMTP, POP3, IMAP, HTTP) sollte eine Kombination mit SSL/TLS durchgeführt werden.

SNMP wird häufig benutzt, um Router und Switches im Netzwerk zu administrieren. Häufig wird dabei SNMPv1 oder SNMPv2 eingesetzt, das zwar einen sog. "Community String" als eine Art Passwort für alle kennt, der jedoch im Klartext übertragen wird. Häufig werden auch die Default-Einstellungen (typischerweise Community String "private" für Schreibzugriffe und Community String "public" für Lesezugriffe) beibehalten. Mit SNMPv3 wurde eine gutes Sicherheitskonzept eingeführt, welches jedoch verwaltet und auch von den Endgeräten unterstützt werden muss.

Neben der Übertragung von Passwörtern im Klartext stellt auch die Speicherung von Passwörtern im Klartext eine große Gefahr dar. Passwörter sollten daher nicht im Klartext, sondern als Hash-Werte abgelegt werden. Außerdem sollten "Salt" und "Pepper", bei der Speicherung von Passwörtern genutzt werden.

Aber auch bei Passwörtern, die als Hashes gespeichert werden, gibt es Angriffsmöglichkeiten, insbesondere wenn das Passwort im Klartext in einem Wörterbuch zu finden war. Hier können sog. Rainbow Tables genutzt werden, in den für viele mögliche Klartextpassworte die Hashes abgelegt sind. Solche Rainbow Tables findet man z.B. unter freerainbowtables.com und MD5 Passwort, Tools dazu heißen DistrRTgen oder Rainbow Crack.

1.5.1.2 Herausfinden von Passwörtern

Zum Erlangen von Passwörtern von anderen Benutzern gibt es verschiedene Möglichkeiten. Man kann annehmen, dass das Passwort relativ einfach ist, d.h. noch auf einer Default-Einstellung ist ("root"/"root") oder auf persönlichen Daten den Nutzers beruht (z.B. Geburtsdatum). Außerdem können Wörterbuchangriffe mit Listen von häufig verwendeten Wörtern genutzt werden. Ist das Passwort damit nicht zu finden, aber relativ kurz, kann man mit einer Brute Force-Methode alle möglichen Passwörter durchprobieren (siehe 1pw.de für Beispielrechnungen zur Suchdauer).

Man kann jedoch auch mit Methoden des Social Engineering versuchen, das Passwort zu erhalten. Schon lange bekannr ist das Phishing ("Password Fishing"), mit dem man Nutzer mit Hilfe einer E-Mail mit enthaltener URL auf eine nachgebaute Webseite lockt, um dort den Nutzer zur Eingabe des Passwortes zu bewegen. Eine Modifikation davon nennt sich Spear Phishing, wenn die E-Mail persönlich auf den Nutzer zugeschnitten wird und dadurch glaubwürdiger wirkt.

Die mit mancher Anwendungssoftware mitgelieferten Möglichkeiten zur Verschlüsselung sind unzureichend, wie beispielsweise bei der von Microsoft angebotenen Software zur Verschlüsselung von Office Dokumenten. Hierzu wird im Internet Software angeboten, mit der man leicht ein "vergessenes" Passwort wieder rekonstruieren kann. Die Software kann natürlich nicht unterscheiden, ob der legitime Benutzer diese verwendet oder ein Angreifer.

Genauso ist der Schutz durch das Passwort beim Login in manche Betriebssysteme nur schwach, weil die Hersteller legitime Nutzer, die tatsächlich ihr Passwort vergessen haben, nicht ausschließen möchten (siehe z.B. Artikel vom com-Magazin).

1.5.1.3 Identitätsdiebstahl

Der Diebstahl von digitalen Identitäten entwickelte sich in den vergangenen Jahren zu einem großen Problem, bei dem Millionen von Nutzern betroffen waren. Das Jahr 2013 war dabei das Jahr mit einem Rekord an Identitätsdiebstählen. Es gab 8 besonders große Fälle, bei den mehr als 10 Millionen Nutzerdaten pro Fall gestohlen wurden. Insgesamt wird die Zahl der gestohlenen Identitäten auf 552 Millionen geschätzt (siehe Symantec Security Threat Report 2014). Im September 2014 wurde bekannt, dass die Kreditkartendaten von 56 Millionen Kunden der amerikanischen Baumarktkette Home Depot gestohlen wurden, nachdem vorher schon 40 Millionen Datensätze bei der Supermarktkette Target entwendet wurden (siehe Heise.de-Artikel).

In die Kategorie des Identitätsdiebstahls, aber auch dem Eindringen in Netzwerke fällt ein Angriff auf Sony Pictures im Dezember 2014 (siehe Heise.de-Meldung). Deren Datennetz war tagelang nicht verwendbar, es wurden gefälschte Apps im Namen von Sony verbreitet und Gehaltslisten von Sony-Mitarbeitern wurden entwendet. Der Angriff hatte auch in den Wochen danach gravierende Folge für Sony (siehe Tagesschau.de-Artikel), u.a. wurde die Firma von Mitarbeitern wegen mangelhaften Sicherheitsvorkehrungen zum Schutz von persönlichen Daten verklagt.

Das soziale Netzwerk LinkedIn führte 2013 eine optionale Zwei-Faktor-Authentifizierung ein, um Missbrauch zu erschweren (siehe LinkedIn Blog). Dabei erhält der Nutzer eine Zahl der SMS zugeschickt, die zusätzlich zum Passwort eingegeben werden muss, wenn der Zugriff von einem bisher nicht für diesen Account verwendeten Computer erfolgt. Es wird jedoch nicht erklärt, wie der Computer wiedererkannt wird (z.B. per Cookie).

Sicherheitsrisiken bei Bankkarten mit Chips, die die unsicheren Karten mit Magnetstreifen ersetzt haben, wurden beim 31C3 gezeigt.

1.5.2 Schadprogramme

Gliederung

Unter Schadprogrammen versteht man Programme oder Programmteile, die absichtlich herbeigeführte unerwünschte Wirkungen haben. Diese Wirkungen können ganz unterschiedlich sein, z.B. das Löschen oder Verändern von Dateien, das Lahmlegen von Netzwerken durch Erzeugung einer hohen Netzlast oder das Ausspionieren des Nutzers durch Protokollierung der Tastatureingaben. Es sind außerdem verschiedene Verteilungsmöglichkeiten für Schadsoftware zu beachten.

Während sich manche Verbreitungswege wie E-Mail-Anhänge schon allgemein als Gefahrenquelle herumgesprochen haben, ist das sog. **Malvertising** noch nicht im allgemeinen Bewußtsein. Dieses bedeutet, dass eine Webseite Schadcode enthält, der nur das Aufrufen der Webseite mit einem anfälligen Browser erfordert, um den Nutzer zu infizieren. Diese Art der Infektion wird Drive-By-Exploit oder auch Drive-by-Download genannt (siehe "Tatort Internet" bei Heise.de für die Analyse einer betroffenen Seite).

Bei solchen Webseiten muss es sich nicht um wenig vertrauenswürdig wirkende Seiten handeln, sondern auch bekannte Webportale können davon betroffen sein (siehe Pressemitteilung des BSI von 2013). Bei der Vermietung von Werbeflächen auf Webseiten haben sich inzwischen ganze Verwertungsketten etabliert, so dass der eigentliche Webseitenbetreiber keinen Überblick darüber hat, wer die Werbeflächen schließlich anmietet. So kann schließlich entsprechender Schadcode auf den Seiten landen, was laut BSI (Fokus IT-Sicherheit 2013) bei jeder 35. deutschen Webseite der Fall ist. Laut BSI-Lagebericht 2014 gibt es in Deutschland monatlich mehr als 1 Mio. Infektionen mit Schadprogrammen.

Besonders unangenehm sind Situationen mit sog. **Zero-Day Exploits**. Hierbei wird eine Software-Schwachstelle bekannt und zeitgleich gibt es schon erste Angriffe, die diese erfolgreich ausnutzen. Der Hersteller der Software hat jedoch noch nicht mit einem Patch reagiert, so dass man den Angriffen ungeschützt ausgeliefert ist. Hier gibt es

kriminelle Strukturen, in denen die Informationen über diese Arten von Schwachstellen verkauft werden (siehe Artikel bzw. White Paper über die kriminelle Elderwood-Struktur bei Symantec).

1.5.2.1 Viren

Viren sind die älteste Schädlingsform der Computergeschichte (der Begriff geht auf die Doktorarbeit von Fred Cohen von 1984 zurück, wobei der erste Virus in freier Wildbahn 1982 geschrieben wurde). Dabei handelt es sich um Programmteile, die sich in andere Programme einbauen und massenweise kopieren. Im Gegensatz zum Wurm benötigen sie stets einen Wirt, in dem sie sich einnisten. Normalerweise bestehen sie aus einer Verbreitungs- und einer Schadfunktion. Schadfunktionen können z.B. Passworte ausspähen oder Datenbestände löschen. Die Schadfunktion kann an Bedingungen geknüpft werden, so dass sie z.B. nur an bestimmten Tagen ausgeführt wird.

Als Wirte für den Ansiedlung der Viren gibt es verschiedene Möglichkeiten. Meistens treten Viren als Dateiviren auf, bei denen sie in Dateien auf einem Rechner vorkommen. Viren können sich jedoch auch im Boot Sektor einer Festplatte oder in Makrofunktionen von Programmen (wie Microsoft Excel) befinden.

Bei Dateiviren sind weitere Unterscheidungen möglich.

- **Überschreiben eines Teils der Wirtsdatei**: Diese Art von Virus fällt relativ leicht auf, da dann das Programm nicht mehr wie bisher funktioniert. Allerdings ist dadurch auch eine Desinfektion nicht möglich, da der bisherige Code nicht mehr vorhanden ist.
- **Appender**: Hier wird der Code hinten an die Datei angefügt. Die Einsprungadresse in das Programm wird verändert, so dass erst der Virencode ausgeführt wird. Danach wird zur eigentlichen Einsprungadresse weitergeleitet, so dass auch der normale Code der Wirtsdatei ausgeführt wird. Aus der Sicht des Anwender scheint sich das Programm also normal zu verhalten, wenn die Schadfunktion des Virus keine auffälliger Wirkung hat.
- **Prepender**: Dieser Virus fügt sich am Anfang einer Datei ein. Nach der Ausführung wird der Originalzustand der Wirtsdatei im Arbeitsspeicher wieder hergestellt.
- **Cavity-Infektion**: Bei diesem relativ seltenen Virus werden leere Bereiche in der Wirtsdatei (am Ende von Sections, wo vorher Nullbytes staden) genutzt, um den Viruscode unterzubringen. Da hierzu genaue Kenntnisse der Wirtsdatei notwendig sind, ist die Programmierung aufwendig. Der Virus kann jedoch nicht an der Dateigröße erkannt werden, da diese unverändert bleibt.

- **EPO**: Bei dieser Virenart wird die Manipulation der Einsprungadresse verschleiert. Der Einsprung zum Virencode erfolgt durch eine versteckte Anweisung.

1.5.2.2 Würmer

Würmer sind Programme, die sich selber über Netzwerke verbreiten können. Oftmals beinhalten sie keine gefährlichen Funktionen, um nicht aufzufallen. Es ist möglich, dass sie große Mengen von **Spam-Mails** versenden und so Mailserver überlasten. Sie können allerdings auch Passwörter ausspähen. Früher wurden Würmer hauptsächlich in Mailanhängen versendet, die sich in das gesamte Adressbuch kopiert haben. Es gibt aber auch neuere Entwicklungen, die sich über Peer-to-Peer (**P2P**) Netzwerke oder **ICQ** verbreiten können.

Der erste Wurm der Computergeschichte war 1988 der nach seinem Programmierer benannte Morris-Wurm. Mit diesem Programm wollte sein Entwickler eigentlich nur feststellen, wieviele Rechner damals an das Internet angeschlossen waren. Er nutzte bekannte Schwachstellen von Anwendungen aus, um sich zu verbreiten und sollte jeden Rechner nur einmal zählen. Durch einen Programmierfehler wurden Computer jedoch teilweise mehrfach infiziert, so dass sich die Infektion immer weiter steigerte und zum Ausfall von Systemen und Netzen durch Überlast führte. Geschätzt wurden 6000 von damals 60000 mit dem Internet verbundenen Systemen infiziert. Als Folge dieses Vorfalls, der die Gefährdungen von Computernetzen der Öffentlichkeit deutlich machte, wurde das CERT an der CMU eingerichtet.

Ein Wurm, der sich sehr schnell ausbreitete, war der '''SQL-Slammer''' im Jahr 2003. Diese schnelle Verbreitung kam dadurch zustande, weil er nur wenig Code benötigt und in einem einzigen UDP-Paket gesendet werden kann. Dieses Paket wird an Port 1434 eines Microsoft SQL-Servers geschickt. Bei einem ungepatchten Server nutzt es Programmierfehler aus und erzeugt Buffer-Overflows, durch den das Systems infiziert wird. Nach der Infektion versucht der Wurm, sich in einer endlosen Schleife an zufällig ausgewählte IP-Adressen zu versenden. Damit kann er eine große Netzlast erzeugen, sodass Server nicht mehr erreicht werden können.

1.5.2.3 Trojaner

Als Trojanische Pferde oder Trojaner werden Programme bezeichnet, die scheinbar eine nützliche Applikation darstellen, deren eigentlicher Sinn jedoch darin besteht einem Angreifer Hintertüren zu installieren, über die er sich im System anmelden kann. Es gibt verschiedene Arten von Trojanern, doch die meisten bestehen aus einem Server,

der an einem vorgegebenen Port auf Anfragen eines Angreifers wartet. Durch das Warten auf Anfragen an einem bestimmten Port sind diese Server recht leicht mit einem Portscanner zu entdecken.

Trojanische Pferde kamen in der Praxis bei einem Spionagefall beim DLR im Frühjahr 2014 und im Zusammenhang mit dem DNS Changer-Fall im Jahr 2011 vor (siehe Angriffe auf das Domain Name System), der ca. 4 Mio. Rechner betraf. Ein schwierig abzuwehrender Trojaner ist der Zeus-Trojaner, der insbesondere zum Ausspionieren von Bankzugangsdaten und anderen Login/Passwortkombinationen genutzt wird. Trojaner werden zum Teil auch als Baukasten für relativ wenig Geld angeboten, so dass viele einen solchen einsetzen können (siehe Meldung über BlackShades Trojaner).

Das Botnetz ZeroAccess ist eine Bespiel für ein Botnetz, dass durch Trojanische Pferde gebildet wurde. Es umfasste zwischenzeitlich mehr als 2 Mio. Rechner, die zum *Click Fraud* eingesetzt wurden (das Errechnen von Bit Coins wurde zwischenzeitlich nicht mehr gemacht, siehe Seite 6 im Report von Sophos). Diese Art von Betrug bezieht sich auf Werbemodelle im Internet, bei den eine Firma Geld bezahlt, wenn ihr Werbebanner auf einer anderen Internetseite angeklickt wird. Bei diesem Betrug werden die angeblichen Nutzerklicks jedoch vom Botnetz ausgeführt.

Während die meiste Schadsoftware sich auf Windows-Betriebssysteme bezieht (laut BSI-Lagebericht 2014 95%), dürfen die Benutzer anderer Betriebssysteme auf keinen Fall davon ausgehen per se geschützt zu sein. Daher sei an dieser Stelle auf das Trojanische Pferd Flashback verwiesen, das laut Zdnet.com 600.000 Macs betraf und auf einer Java-Schwachstelle beruhte. Schwachstellen können aber genauso bei Linux vorkommen (siehe Wikipedia.de-Artikel über Shellshock).

Der typische Schadcode, der für Angriffe auf mobile Endgeräte verwendet wird, fällt unter die Trojaner-Kategorie (siehe Seite 16 im Symantec Internet Security Threat Report). Dabei tarnen sich Schadprogramme als nützliche Apps. Hierbei stellt sich die Situation bei iOS und Android, den beiden führenden Plattforme, unterschiedlich dar. Bei iOS sind zwar deutlich mehr Schwachstellen bekannt, die führen jedoch nicht zu mehr tatsächlichen Angriffen, weil Apple die Nutzer zur Verwendung des Firmen-eigenen Stores zwingt. Bei Android können die Nutzer jedoch direkt fremde Apps installieren und sich so eher mit Schadcode infizieren. Außerdem gilt Google als weniger restriktiv bei der Zulassung zu deren App Store. Laut BSI-Lagebericht 2014 ist 98% aller mobilen Schadsoftware für Android-Geräten geschrieben. Eine Schwierigkeit der Android besteht auch darin, dass bei vielen Smartphones schon nach kurzer Zeit keine Aktualisierungen mehr möglich sind. So sind ältere Smartphones wesentlichen Angriffsmöglichkeiten ausgesetzt, die bis Android-Version 4.1.2 in Kombination mit dem Standardbrowser möglich waren.

Nicht versteckt, sondern direkt mit eigener Webseite wird für den Trojaner FlexiSpy geworben, wobei die Anwendungsgebiete untreuer Ehepartner, Schutz von Kindern und Mitarbeiterüberwachung genannt werden. Gelingt es diese Software unerkannt auf dem Zielgerät zu installieren, ist es möglich, komplette Bewegungsprofile zu erstellen, unbemerkt Kamera und Mikrofon des Smartphones aus der Ferne zu bedienen, Gespräche mitzuhören und Passwörter zu knacken.

Anmerkung

Die Abkürzung "Trojaner" für "Trojanisches Pferd" verdreht die historische Analogie. Die Stadt Troja (an der Westküste der heutigen Türkei) wurde der Sage nach von den Griechen belagert, die scheinbar die Belagerung aufgaben und ein hölzernes Pferd zurückliessen. Dieses Pferd wurde von den Trojanern in die Stadt gezogen, so dass einige griechische Soldaten, die sich im Inneren des Pferdes befanden, mit in die Stadt gelangten. Diese konnten später unbemerkt die Stadttore öffnen und so den Griechen die Eroberung der Stadt ermöglichen. In einem trojanischen Pferd befinden sich also Griechen und keine Trojaner.

1.5.2.4 Ransomware

Unter **Ransomware** versteht man ein Schadprogramm, welches den Zugriff auf den eigenen Rechner sperrt. Oftmals wird dem Nutzer eine strafbare Handlung (z.B. der Besitz von Kinderpornographie) vorgeworfen, die angeblich von einer Behörde (Polizei, Verfassungsschutz) entdeckt wurde. Nach Bezahlung eines Geldbetrags (typischerweise in Form einer Internetwährung wie Bitcoins) werde der Rechner wieder entsperrt. Die Bezahlung des Geldbetrags führt jedoch in den meisten Fällen nicht zur Entsperrung des Rechners.

Eine Weiterentwicklung dieser Schadprogramme nennt sich Ransomcrypt oder Cryptolocker (siehe Seite 6 im Symantec Security Threat Report 2014). Hierbei verschlüsseln die Angreifer die Dateien auf der Festplatte des Opfers. Sollte der Opferrechner Festplatten über das Netzwerk einbinden, sind diese auch betroffen und damit weitere Nutzer. Das Video von Sophos zeigt wie eine erfolgreiche Infektion mit Cryptolocker aussieht. Die Angreifer verlangen dann eine Zahlung, mit der angeblich der Schlüssel bereitgestellt wird.

In naher Zukunft wird mit weiteren Varianten gerechnet, die neben der Verschlüsselung der Festplatte zusätzlich versuchen, auch Backups in der Cloud (z.B. bei Diensten wie Dropbox oder Google Drive) zu finden und diese ebenfalls zu verschlüsseln (siehe McAfee Report Q3 2014).

2013 wandten sich 8500 BürgerInnen an das BSI, deren Rechner von Ransomware befallen wurde (siehe BSI-Lagebericht 2014).

1.5.3 Buffer Overflows

Viele Einbrüche in Systeme basieren auf der Ausnutzung von Programmierfehlern, die Pufferüberläufe (engl. Buffer Overflows) ermöglichen. Hauptsächlich sind davon in C oder in C++ geschriebene Anwendungen betroffen, da diese Programmiersprachen durch manche Funktionen nicht überprüfen, ob die Eingaben so sind wie erwartet. Die Java hat diese Problematik wegen der automatischen Speicherverwaltung nicht.

Ein Beispiel ist für so eine Schwachstelle in der Programmierung kann die Verwendung des C-Befehls **strcpy-Befehl** (String Copy) sein. Dieser kopiert im Speicher Daten von einer Quelle zum Ziel, wobei nicht überprüft wird, ob die Quelldaten im Speicherbereich des Ziels Platz haben. Wenn die Quelldaten größer sind als der Platz im Zielspeicherbereich (z.B. ein String mit 50 Zeichen, wo nur max. 10 Zeichen vorgesehen sind), kommt es zu einem Buffer Overflow und es werden Daten im Speicher des Ziels überschrieben.

Durch Buffer Overflows wird typischerweise der bei Programmaufrufen benötigte Stack überschrieben, wobei die Rücksprungadresse des aufrufenden Programms verändert wird und nun auf einen kurzen Programmcode verweist, der ebenfalls mit auf dem Stack abgelegt wurde. Beim Aufruf des angegriffenen Programms wird der Code des Angreifers ausgeführt, mit dem normalerweise eine Shell gestartet wird, sodass der Angreifer damit Zugang zum System erhält. Die Rechte des angegriffenen Programms werden auch dem Angreifer zugeteilt. Dieser wird daher versuchen Programme mit Administratorrechten durche entsprechende Eingaben zu kompromittieren, damit er anschliessend ungehindert mit vollen Rechten auf dem System arbeiten kann. Das heißt, nach einem erfolgreichen Angriff dieser Art hat ein Angreifer den Rechner vollständig unter seiner Kontrolle.

1.5.4 Rootkits

Als Rootkit wird die Möglichkeit bezeichnet auf einem kompromittierten System unentdeckt zu bleiben und die durch einen Einbruch erlangten Privilegien später nach Belieben nutzen zu können. Das Ziel des Angreifers besteht darin, keine Spuren seiner Aktivitäten oder Modifikationen zu hinterlassen.

Wurden anfänglich veränderte Systemprogramme installiert, um Log-Files zu unterdrücken, werden inzwischen umfangreiche, schwer zu entdeckende Änderungen im Kernel durchgeführt, um dieses Ziel zu erreichen. Rootkits werden verstärkt unter Linux eingesetzt, da der Quellcode frei erhältlich und damit leicht zu modifizieren ist; es gibt aber auch Rootkits für Windows.

Die ersten Rootkits besaßen die Möglichkeit, aus den Log-Dateien bestimmte Einträge zu löschen, so dass es nicht mehr möglich war, durch die Auswertung der Log-Dateien einen Angreifer zu entdecken. Laufende Prozesse oder spezielle Dateien des Angreifers können jedoch während des Angriffes leicht entdeckt werden.

Eine fortgeschrittene Methode besteht aus dem **Austausch von Systemprogrammen** wie *ps*, *ls* oder *netstat*, die so modifiziert werden, dass sie die Aktivitäten des Angreifers nicht aufzeigen. Darüber hinaus kann noch eine ganze Anzahl anderer Systemprogramme ausgetauscht werden, wie *passwd*, *killall* oder *syslogd*. Dabei haben die ausgetauschten Programme die gleiche Länge wie die Originalprogramme. Werden allerdings Integritätssicherungsverfahren wie SHA-1 oder MD5 verwendet, um Hashes als Prüfsummen der Programme zu bilden, können die geänderten Programme erkannt werden. Eine solche Überprüfung ermöglicht z.B. das Windows-Programm HashCheck, das eine Erweiterung des Windows Explorers darstellt und die Prüfsummen der Dateien in einem zusätzlichen Reiter bei den Dateieigenschaften anzeigt.

Die wirkungsvolle Kontrolle durch Hash-Prüfsummen kann mit **Kernel Rootkits** umgangen werden. Dabei werden nicht mehr die Systemprogramme ausgetauscht, sondern es werden die von Systemprogrammen benutzten Systemaufrufe manipuliert. Entdeckt werden können die manipulierten Systemaufrufe z.B. durch Laufzeituntersuchungen, wobei die Anzahl der ausgeführten Befehle gezählt wird. Weicht diese signifikant von der Anzahl im nicht kompromittiertem System ab, ist dies ein deutlicher Hinweis auf einen manulierten Systemaufruf. Ein Programm wie '''chrootkit''' ist geeignet diese Manipulationen festzustellen.

Was ein Angreifer mit einem kompromittiertem System vorhat, ist nicht vorhersagbar. Häufig werden die Systeme als **FTP Server** (aber nicht auf dem Standard Port 20/21) betrieben, um unerlaubt lizensierte Software zu verteilen. Eine gute Möglichkeit, diese Art von Angriffen zu erkennen, ist eine Veränderung der Netzlast, die regelmäßig vom Administrator überprüft werden sollte.

Die Untersuchung eines fortgeschrittenen Windows 7 Rootkits ("TDL-Familie"), das ein eigenes verschlüsseltes Dateisystem angelegt, ist in der Serie "Tatort Internet" bei Heise.de dargestellt.

1.5.5 Schwachstellen von Web Anwendungen

Gliederung

Bei der Programmierung von Webanwendungen können sich vielfältige Schwachstellen ergeben, die später von Angreifern ausgenutzt werden können. Von den Schwachstellen werden auf den Unterseiten Injections und XSS erklärt.

Die folgenden Verweise ermöglichen es zudem, sich noch genauer mit dem Thema zu befassen.

- Mit der OWASP Top 10 steht eine Liste von typischen Schwachstellen von Webanwendungen im Internet bereit. Die Liste ist nach der Häufigkeit des Vorkommens der Schwachstellen geordnet und weist einige Schwachstellen aus, die seit Jahren zu den häufigsten gehören und wo sich die Situation in der Praxis nur wenig verbessert.
- Vom SANS-Institute wird eine Liste der 25 gefährlichsten Programmierfehler herausgegeben.
- Softwareschwachstellen werden von MITRE kategoriert, wobei sicherheitsrelevante Schwachstellen in einer speziellen Common Vulnerability and Exposures Datenbank verwaltet werden.
- Das BSI stellte 2013 zwei Dokumente zur Auftragsvergabe für die Entwicklung sicherer Webanwendungen bereit. Ein Dokument mit konkreteren technischen Anforderungen wurde bereits 2006 veröffentlicht.

Die Fa. Google bietet Personen, die Sicherheitslücken im Google Chrome Browser melden und auch einen Exploit liefern, eine Belohnung von bis zu 15.000 Dollar (siehe Nachricht über Erhöhung der Summe).

PlugIns, die zur Anzeige von Webseiten verwendet werden, weisen des öfteren gravierende Schwachstellen auf, die auch rasch aktiv ausgenutzt werden. In den letzten Jahren waren davon insbesondere die Java Virtual Machine und der Adobe Flash Player betroffen. Bei beiden PlugIns wurde zumindest eine zwischenzeitliche Deaktivierung empfohlen (siehe Heise.de-Artikel zu Java und Heise.de-Meldung zum Flash Player).

1.5.5.1 Injections

Unter Injection versteht man die Eingabe von Code durch böswillige Nutzer, wo eigentlich nur normale Zeichen als Eingabe erwartet werden.

Die meistgenannte Fall bei Injections ist die **SQL Injection**, die bei der Verwendung einer SQL-Datenbank möglich sein kann. Sehr viele Webseiten werden auf Basis einer Kombination eines Servers (meistens Apache Webserver) mit einer SQL-Datenbank (häufige Verwendung von MySQL und PostgreSQL) realisiert, bei der die ausgelieferte Webseite dynamisch unter Verwendung von Informationen aus der Datenbank aufgebaut wird. Falls nicht entsprechende Programmierrichtlinien eingehalten werden oder ein geeignetes Programmierrahmenwerk verwendet wird, kann es bei Formularen auf der Webseite sein, dass Angreifer diese zu direkten Zugriffen auf die Datenbank nutzen können.

Hierzu ein einfaches Beispiel: Auf einer Webseite kann man sich mit einer Login/ Passwort-Kombination einloggen. In ein Login-Feld soll der Benutzername und in ein Passwort-Feld das Passwort geschrieben werden. Die Eingaben in den beiden Feldern werden in Variablen gespeichert, die dann in einer SQL-Anfrage weiterverwendet werden. Ein Beispiel für eine solche Anfrage ist SELECT * FROM Benutzer WHERE login='$login' and password='$password', mit der der Benutzer mit dieser Login/ Passwort-Kombination in der Datenbank gefunden würde. Bei SQL bedeuten zwei Striche, dass der Rest als Kommentar zu verstehen ist. Der Angreifer kann sich damit unberechtigt Zugriff verschaffen, wenn er einen Benutzernamen kennt, die oftmals leicht zu erraten sind (z.B. Vorname.Nachname). Dann kann er beim Login-Feld einen Benutzernamen eingeben, den er aber um zwei Striche ergänzt (z.B. Vorname.Nachname --). Bei der SQL-Anweisung bedeutet dieses, dass der Rest der Anweisung zum Kommentar wird und damit die Bedingung ("and password='$password'") nicht mehr relevant ist. Die Authentifizierung erfolgt also lediglich dadurch, dass es den Nutzernamen in der Datenbanktabelle gibt.

Dieses ist aber nur eine Möglichkeit von vielen. Angreifer können zum Beispiel auch versuchen, zusätzliche Datenbankabfragen zu starten, indem sie hinter einem Eingabewert ein Semikolon und dahinter eine komplette Datenbankanfrage schreiben. Das Semikolon hat bei SQL die Bedeutung, dass es zwei Anweisungen voneinander trennt. Hier muss der Angreifer etwas raten, wie die Tabellen und Attribute benannt sind, aber dieses wird in Datenbankschemata oftmals mit üblichen Begriffen bezeichnet.

Diese Angriffe lassen sich durch Prepared Statements verhindern, wobei es sich um vorformulierte Anfragen an die Datenbank handelt. Die Eingaben des Angreifers können so nicht Teil des Codes der SQL-Anfrage werden.

Außerdem kann man bei der Programmierung beispielsweise nicht direkt in PHP programmieren, sondern unter Verwendung eines PHP-Rahmenwerks (z.B. Symfony2, Zend), bei dem bei der Umsetzung des Codes in PHP Code bereits auf die Schwachstellen geachtet wird.

1.5.5.2 Cross Site Scripting

Gliederung

Bei XSS wird versucht, eine Codeausführung beim Nutzer einer Webseite herbeizuführen, wobei dieser Code schadhaft für den Nutzer ist. Bei dem Code handelt es sich in den meisten Fällen um JavaScript, aber auch HTML, Flash, ActiveX und weiterer Code, der beim Nutzer ausgewertet wird, ist denkbar. Der Begriff bedeutet übrigens nicht, dass mehrere Websites involviert sind.

Im folgenden werden die drei XSS-Varianten (Persistent Attack, Reflected Attack, DOM-based Attack) genauer erklärt, ehe ein Praxisbeispiel dargestellt wird.

1.5.5.2.1 Persistent XSS

Dieser Angriff basiert auf einer Schwachstelle des Webservers, der die Eingaben von Nutzern nur unzureichend überprüft. Beispielsweise könnte auf einer Webseite ein Gästebuch angeboten werden, bei dem die Benutzer Grußbotschaften hinterlassen können. Der Betreiber der Webseite nimmt an, dass die Nutzer hier nur Texte hineinschreiben werden. Ein Angreifer könnte jedoch JavaScript Code (zusätzlich zum Text) eingeben, der auf der Serverseite in eine Datenbank gespeichert wird. Beispielsweise könnte die Eingabe so aussehen:

Schöne Webseite

Wird die Webseite danach von weiteren Benutzern aufgerufen, so erhalten diese eine Zusammenstellung der vorherigen Einträge, wobei auch der Eintrag des Angreifers ausgeliefert wird. Dieses führt zur Ausführung des Codes bei den weiteren Nutzern.

Als Gegenmaßnahme muss der Server Eingaben dahingegend überprüfen, ob es sich um Code handelt. Solche Eingaben müssen entweder abgelehnt oder so umcodiert werden, dass sie nicht mehr ausführbar sind. Bei JavaScript Code muss man beispielsweise auf das <-Zeichen achten.

1.5.5.2.2 Reflected XSS

Bei dieser Angriffsvariante bringt der Angreifer einen Benutzer dazu, auf einen präparierten Link zu klicken. Beispielsweise schickt der Angreifer eine E-Mail an den Nutzer, der der Administrator einer Webseite ist. In dieser E-Mail wird auf ein angebliches Problem mit der Benutzung der Webseite hingewiesen, wobei gleich ein Link mitgeschickt wird. Mit diesem soll sich der Benutzer bequem und schnell ansehen können, welches Schwierigkeiten es gibt. Dieser Link ist jedoch präpariert und enthält Code im Parameterbereich.

Beispielsweise könnte der Link so aussehen:

Ein Webserver, der dieses nicht herausfiltert, liefert dann den Code mit aus.

Im Unterschied zu der Persistent-Variante wird der Schadcode jedoch nicht permanent auf dem Server gespeichert. Dieses ist also ein Angriff auf einen ausgewählten Nutzer, während Persistent XSS alle zukünftigen Nutzer betrifft.

1.5.5.2.3 DOM-based XSS

Bei DOM handelt es sich um das Dokument Object Model, d.h. es geht um die Auswertung von Code beim Nutzer, während bei diesem eine Webseite angezeigt wird. Bei dieser Variante des Angriffs wird die Webseite über zusätzliche Parameter aufgerufen, die nachher mit verarbeitet werden. Wenn bei diesen Parametern nicht überprüft wird, ob diese JavaScript Code enthalten, wird ggf. JavaScript bei der Verarbeitung ausgeführt.

Das HTML-Dokument in einem Beispielszenario könnte so aussehen.

Es könnte aufgerufen werden mit:

1.5.5.2.4 XSS-Angriff auf Apache Issue Tracking System

Die gemeinnützige Apache Foundation (bekannt durch ihren gleichnamigen Webserver) verwendet zum Verwalten von Software-Problemen das Issue Tracking System JIRA von Atlassian. Im April 2010 wurde dieses System für einen XSS-Angriff missbraucht, der hier zusammengefasst dargestellt wird (genauere Beschreibung auf Apache.org).

Der Angreifer legte einen neuen Eintrag an, in dem auf eine URL verwiesen wird. Damit der Versuch Code einzuschleusen nicht gleich erkannt wurde, wurde hier zusätzlich ein Dienst zur Verkürzung von URLs (in diesem Fall tinyurl) verwendet, so dass nur diese verkürzte URL sichtbar war (Hinweis: Das Firefox AddOn Long URL Please löst verkürzte URLs standardmäßig auf, um deren wahren Zweck zu zeigen). Der JavaScript Code hatte den Zweck, die Cookies von Benutzern zu stehlen, wobei auch Administratoren des Apache-Projekts betroffen waren. Am selbem Tag unternahmen die Angreifer zudem einen Brute Force-Angriff, um das Passwort der Seite login.jsp zu erraten.

Eine dieser Angriffsmethoden war schließlich erfolgreich, so dass die Angreifer mit Hilfe der Administatorrechte nach einigen Schritten zahlreiche Login/Passwort-Kombinationen zur Verfügung hatten. Außerdem konnten sie in einen weiteren Server eindringen, bei dem ein Passwort ebenfalls funktionierte. Der Angriff wurde nach vier Tagen entdeckt, als viele Passwort-Rücksetzungsnachrichten generiert wurden, mit denen weitere Benutzer zu Logins angeregt werden sollten.

Bei Apache waren die Passwörter nicht im Klartext gespeichert, sondern (so wie es sein sollte) als Passwort-Hashes, so dass die Angreifer trotz des erfolgreichen Eindringens nicht die Passwörter im Klartext hatten.

Zwei Tage nach diesem Angriff wurde die Methode von den Angreifern auch erfolgreich bei Atlassian angewendet.

Es soll positiv erwähnt werden, dass die Situation von beiden Organisationen klar dargestellt wurde und auch die Schlußfolgerungen öffentlich gemacht wurden.

1.5.6 Angriffe auf das Domain Name System

Das DNS stellt den wichtigsten Infrastrukturdienst im Internet dar. Ohne die Übersetzung von Namen in IP-Adressen wäre das Internet so gut wie nicht mehr verwendbar, da man sich als Mensch viel besser symbolische Namen merken (bzw. durch eine Suchfunktion finden) kann als die Zahlenkombinationen in den IP-Adressen.

Eine Manipulation der DNS-Auflösung kann unbemerkt vom Nutzer erfolgen und so insbesondere zum Ausforschen von Login/Passwort-Kombinationen verwendet werden. In einem angenommen Fall sei die DNS-Auflösung manipuliert. Wenn der Nutzer dann eine Webseite aufruft, wird von der DNS-Auflösung eine falsche IP-Adresse zurückgeliefert. Unter dieser IP-Adresse könnten die Angreifer die Webseite, die der Nutzer eigentlichen aufrufen wollte, nachgebaut haben. Technisch stellt dieses im Bezug auf die Oberfläche keine große Schwierigkeit dar, da der Code zur Darstellung der Oberfäche geliefert wird, wenn man die richtige Webseite aufruft. Meldet sich der Nutzer nun mit Login und Passwort bei der nachgebauten Webseite an, erhalten die Angreifer die Login und Passwort-Kombination und können damit bei der richtigen Webseite die Identität des Nutzers annehmen.

Ein Mechanismus, der das ganze zumindest bei Seiten von Banken und anderen sehr kritischen Seiten verhindern soll, sind die Zertifikate der Internetseiten, hier die speziellen Extended Validation-Zertifikate. Diese werden nur an bestimmte Institutionen nach einem Prüfverfahren vergeben, so dass eine fehlende Zertifizierung in der Browserzeile angezeigt wird. Der Nutzer muss jedoch darauf achten, dass dann dieser grüne Balken in der Browserzeile fehlt.

Der DNSChanger Trojaner (entdeckt im November 2011) war ein Trojanisches Pferd, welches zu einer Manipulation der DNS-Einstellungen auf den betroffenen Rechnern führte. Die Angreifer lenkten die DNS-Anfragen der Rechner auf von ihnen betriebene DNS Server mit falschen Namensauflösungen um. Hierbei ging es den Angreifern darum, die Werbeanzeigen auf Webseiten zu manipulieren und eigene Werbung einzublenden. In der Spitze waren 4 Mio. Nutzer davon betroffen, wobei der erzielte Gewinn auf mindestens 14 Mio. Dollar geschätzt wird (die Kriminellen wurde jedoch in Estland verhaftet). Die Grafik der DNS Changer Working Group zeigt, dass es Monate lang dauerte, die Desinfektion durchzuführen. Das FBI sah sich gezwungen, die von den Kriminellen aufgesetzten Server noch einige Monate lang weiter zu betreiben, allerdings dann mit den richtigen Auflösungen. Man befürchtete, dass ansonsten viele Nutzer das Internet nicht vernünftig weiter nutzen könnten, da diese bei Schwierigkeiten nicht eine beseitigte Manipulation des DNS als Ursache vermuten würden.

1.5.7 Angriffe auf HTTPS

Bei der Übertragung von Webseiten wird HTTP oftmals mit SSL/TLS kombiniert, um die Verbindung abzusichern. Allerdings bestehen hierbei für Angreifer Manipulationsmöglichkeiten, die nur für einen aufmerksamen Benutzer zu entdecken sind.

Bei einem Szenario (siehe Präsentationen von Black Hat Security Konferenz 2009), das sich z.B. in einem Internet-Cafe ereignen könnte, hat ein Angreifer als Man-in-the-Middle (siehe Kommunikationsszenarien) die Möglichkeit, die Kommunikationsinhalte zu manipulieren. Der Nutzer ruft eine Webseite mit normalem HTTP ab, die dann Links auf einen nur per HTTPS zugänglichen Bereich enthält, der ein Login über ein Formular erfordert. Der Angreifer manipuliert diesen Link und ändert das HTTPS zu HTTP. Der Nutzer schickt dann das ausgefüllte Formular zum Angreifer, der nun mit diesen Daten eine HTTPS-Verbindung zum Webserver aufbaut. Der MitM kann somit in der Folge die eigentlich verschlüsselte Kommunikation mitlesen und auch manipulieren. Für den Benutzer ist die Manipulation nur dadurch erkennbar, dass im Browser nicht https, sondern nur http steht und auch das Schlosssymbol fehlt. Der Angreifer könnte ggf. sogar das FavIcon ändern, so dass hier ein Schloss dargestellt würde. Im Falle von Banken mit Extended Validation Certificates fällt die Manipulation jedoch mehr auf, da hier normalerweise dieses spezielle Zertifikat von den Browser deutlicher hervorgehoben wird.

Gegen diese Art von Angriffen kann auf der Server-Seite ein Schutz realisiert werden, wenn dort festgelegt wird, dass die Seite immer per HTTPS erreicht werden soll. Dieses kann mit HSTS Headern erreicht werden, was aber nur dann funktioniert, falls die Webseite beim ersten Aufruf nicht manipuliert ist und die Einstellung dann im Webbrowser gespeichert bleibt (siehe Seite 50 in *iX14*).

Mit einer speziellen Webseite können sich Domains registrieren, die nur per HTTPS erreichbar sein sollen. Diese Liste gilt für Chrome, Firefox und Safari.

Weitere Schwachpunkte bei HTTPS haben mit einer unzureichenden Validierung von Zertifikation zu tun (siehe weitere Präsentation).

Außerdem kann es Programmierfehler in Browsern geben, durch die gefälschte Zertifikate nicht erkannt werden (siehe Intel Security-Bericht über eine unzureichende Zertifikatvalidierung im Firefox Browser).

1.5.8 Abhören von E-Mails

Der E-Mail-Dienst wurde für ein Netz entworfen, in dem man sich gegenseitig vertraut. Dadurch wurden die Protokolle SMTP, POP und IMAP ohne eine Verschlüsselung der Nachrichten implementiert.

Im Gegensatz zum ebenfalls unverschlüsselten HTTP reicht in diesem Fall jedoch eine Kombination mit der SSL/TLS-Verschlüsselung auf keinen Fall aus, um eine Ende-zu-Ende-Verschlüsselung zu realisieren. Hierzu muss man sich die Übertragung von E-Mails und die Verwendung der Protokolle dabei vor Augen führen. Unter der Annahme, dass Nutzerin Alice an Nutzer Bob eine E-Mail senden möchte und Bob sei Kunde eines anderen Providers als Alice, dann erfolgen drei Schritte.

- Alice sendet die E-Mail unter Verwendung von SMTP an den Mail Server ihres Providers.
- Der Mail Server von Alices Provider sendet die E-Mail wiederum per SMTP an den Mail Server von Bobs Provider. Dort liegt die Nachricht dann abholbereit vor.
- Bob fragt seine E-Mails mit POP3 oder (heutzutag meistens) IMAP ab und erhält dabei die Nachricht von Alice.

Alice und Bob können dabei bei ihrem Mail Programm die Verwendung von SSL/TLS einstellen, die dann mit SMTP und POP3/IMAP kombiniert wird. Damit wird aber nur die Übertragung zum Mail Server des Providers und die Abholung vom Mail Server des Providers verschlüsselt. Die E-Mails liegen auf den Mail Servern der Provider wiederum unverschlüsselt vor und außerdem haben beide keinen Einfluss darauf, ob die Kommunikation zwischen den Providern verschlüsselt erfolgt. Wie im Rahmen der "E-Mail made in Germany"-Initiative deutlich wurde, wurden von großen E-Mail-Providern vor den Snowden-Enthüllungen die E-Mails zwischen den Providern unverschlüsselt ausgetauscht, was nun beseitigt werden soll (siehe Heise.de-Meldung). Google zeigt auf seinen Seiten eine Statistik, mit welchen E-Mail Providern Google mit seinem Gmail-Dienst verschlüsselt kommuniziert.

Um sich zu schützen kann man entweder auf verbesserte Dienste der Anbieter vertrauen oder selbst mit seinen Kommunikationspartnern eine Ende-zu-Ende-Verschlüsselung durchführen.

1.5.9 Social Engineering

Der Schwerpunkt in diesem Kapitel lag soweit auf technischen Angriffsmöglichen, bei denen die Einbeziehung von Menschen nur in wenigen Fällen explizit genannt wurde. Viele Angriffsversuche stellen heute aber eine Kombination aus dem Ausnutzen technischer und menschlicher Schwächen dar.

Ein Beispiel ist sog. **Keylogger Hardware**. Hierbei handelt es sich um eine kleine Hardware, die in den Tastaturanschluss am PC gesteckt wird. Damit geht alles, was der Nutzer eintippt durch diese Hardware, also insbesondere auch die Eingaben von Logins und Passwörtern. Diese relativ kleine Hardware wird in vielen Fällen unentdeckt bleiben, wenn die Desktop Rechner unter dem Schreibtisch stehen. Eine solche Keylogger Hardware kann legal erworben werden und ist leicht zu bekommen (wie die Eingabe von "Keylogger Hardware" in eine Suchmaschine zeigt). Ein Szenario wäre beispielsweise, dass sich jemand in das Reinigungspersonal bei einer Firma einschleicht und dabei die Hardware platziert. Nach einigen Tagen kann diese dann wieder unauffällig entfernt werden.

Präparierte **USB-Sticks** stellen ebenfalls ein großes Risiko dar, da diese mit automatischen Funktionen nur durch das Anstecken an einen Rechner viele Befehle absetzen können (siehe Artikel über BadUSB Sticks). Hier wäre ein Szenario denkbar, dass Angreifer scheinbar zufällig USB Sticks verlieren. Mitarbeiter einer Firma, die ausspioniert werden soll, könnten einen solche Stick in ihren Rechner einstecken, um den Besitzer festzustellen und den Stick zurückzugeben. Auf diese Weise infizieren sie sich jedoch mit Schadsoftware.

Die Funktionalität eines solchen BadUSB-Sticks kann sich auch in anderer Hardware verbergen, die mittels USB angeschlossen wird. Insbesondere Computer-Mäuse eignen sich für diesen Zweck, bei dem entweder eine Maus verschenkt wird (siehe Falldarstellung auf Heise.de) oder Angreifer bei einem Beusch heimlich die Maus austauschen. Das zusätzliche Bauteil kostet übrigens nur ca. 9 Dollar.

Eine andere Problematik besteht in der Möglichkeit zur Manipulation der Anzeige von Telefonnumern. Dieses wird '''Caller ID Spoofing''' genannt. Die Fälschung der Anzeige der eigenen Telefonnummer, die man bei einem Anruf verwendet, war in Deutschland schon immer illegal, in den USA bis zum Jahr 2010 jedoch nicht. Es gibt spezielle Apps, die die Fälschung ermöglichen, was insbesondere durch VoIP-Dienste ermöglicht wird (solche Angebote sind wiederum mit einer Suchmaschine nicht schwer zu finden). Durch die Fälschung der angezeigten Telefonnummer besteht die Möglichkeit eine interne Rufnummer vorzutäuschen, beispielsweise von der IT Support-Abteilung. Damit könnte

der Angreifer einen Nutzer auffordern, ausnahmeweise sein Passwort preiszugeben, da der Rechner erhebliche Auffälligkeiten zeige.

Oftmals führt auch die umständliche Bedienung oder, je nach Betrachtungsweise, die Nachlässigkeit der Nutzer zu Sicherheitsrisiken. Beispielsweise wurden für den NSA-Untersuchungsausschuss des Bundestages Handys mit einer kryptographischen Verschlüsselung (Hersteller Secusmart) angeschafft, die jedoch wegen komplizierter Bedienung von den Abgeordneten teilweise nicht genutzt werden (siehe Tagesschau.de-Artikel).

Die sozialen Netzwerke sind in diesem Zusammenhang ebenfalls sehr relevant. Hier sei beispielsweise auf den Fall "Robin Sage" verwiesen, bei dem ein falsches Nutzerprofil mit erfundenem Lebenslauf in sozialen Netzwerken angelegt wurde. Dieses war zwar nur ein Sicherheitstest, der jedoch zeigte, wie schnell mit dieser Methode das Vertrauen von anderen Nutzern erschlichen werden konnte.

1.6 Angriffswerkzeuge

Gliederung

Im folgenden werden ausgewählte Sicherheitswerkzeuge besprochen, die häufig verwendet werden. Viele dieser Tools sind in einer speziellen Linux Distribution namens Kali Linux enthalten, die als erstes vorgestellt wird.

Im Internet gibt es hilfreiche Übersichtsseiten, die Sicherheitswerkzeuge auflisten und kurze Beschreibungen enthalten.

- Eine Sammlung von 125 vielfach genutzten Security Tools wird auf der Seite sectools.org angeboten.
- Auch bei Heise.de wird eine Liste von Security Tools verwaltet.

1.6.1 Kali Linux

Von der Fa. Offensive Security wird eine spezielle Linux Distribution namens Kali Linux angeboten (eine Vorgängerversion war unter dem Namen BackTrack bekannt). Diese Linux Distribution, die auf Debian Linux basiert, enthält mehr als 300 Tools zum Testen der Netzwerksicherheit, wobei die meisten dieser Tools eher als Angriffs- und nicht als Abwehrwerkzeuge angesehen werden müssen. Sie dürfen daher nur zum Testen von eigenen Netzwerken oder mit explizitem Einverständnis von anderen Netzbetreibern für die Anwendung auf deren Netze eingesetzt werden. Bei Kali Linux erfolgt vier mal am Tag eine automatische Aktualisierung der Software, so dass die Tools stets aktuell sind.

In einem Artikel von heise.de wird Kali Linux und die Verwendung einiger mitgelieferter Tools beschrieben. Eine Anleitung wie man Kali Linux in eine VirtualBox-Umgebung installiert, ist im Kali Forum zu finden.

Die Tools openVAS, nmap, zenmap, macchanger, ettercap und wireshark, die auch in diesem Abschnitt vorgestellt werden, sind Teil der Kali Linux Distribution.

1.6.2 Nmap

'''Nmap''' (Network Mapper) ist ein freies Tool, um Netze zu erkunden und Sicherheitsschwächen aufzudecken. Es gibt Versionen für alle gängigen Betriebssysteme. Mit Nmap können ganze Netze überprüft werden, aber es kann auch für einzelne Hosts eingesetzt werden. Nmap stellt fest, welche Hosts im Netz vorhanden sind, welche Ports geöffnet sind (Port Scanner), welche Paket-Filter bzw. Firewalls benutzt werden und hat noch viele andere Eigenschaften. Nmap kann von OpenVAS als Port-Scanner benutzt werden.

Nmap wird häufig vor einem Angriff benutzt, um möglichst viele Informationen über das Opfer zu erhalten. Hierzu ist insbesondere eine Funktion interessant, mit dem das Betriebssystem des Opfers festgestellt und so gezielt Schwachstellen gefunden werden können (siehe Betriebssystem-Erkennung).

Die graphische Oberfläche von nmap heißt zenmap. Ein einfacher Versuch mit zenmap stellt fest, welche anderen Geräte sich noch im eigenen Netz befinden. Hat man beispielsweise die private IP-Adresse 192.168.2.12 dann kann man das Netz 192.168.2.0/24 absuchen und erhält eine graphische Anzeige der Nachbargeräte.

Mit dem Portscanner ZMap hat die Universität Michigan einen alternativen Portscanner entwickelt, der für sehr effiziente Scans eines Ports auf sehr vielen IP-Adressen ausgelegt ist. Falls eine 1 Gbit/s-Verbindung ins Internet bereit steht, kann damit in nur 45 Minuten ein Port auf sämtlichen öffentlichen IPv4-Adressen (das sind 3,7 Milliarden Adressen) getestet werden. Diese sehr viel bessere Effizienz als Nmap geht auf eine spezifische Verwendung von Threads und ein geschicktes Verteilen von Anfragen zurück (siehe Präsentation bei Usenix-Konferenz, Seite 43 in *iX14*). Mit der Seite Scans.io stellt die gleiche Forschungsgruppe die Rohdaten von durchgeführten Scans zur Verfügung. Die Administratoren von Servern müssen also damit rechnen, dass aktuell vorhandene Schwachstellen von Angreifern sehr wahrscheinlich entdeckt werden. Sie können sich keinesfalls darauf verlassen, in der Menge der vielen IPv4-Adressen nicht gescannt zu werden.

1.6.3 OpenVAS

Mit den Tool OpenVAS (Open Vulnerability Assessment System) steht ein freies Werkzeug zur Verfügung, mit dem verschiedenste Schwachstellen von Geräten im eigenen Netz untersucht werden können. Die Entwicklung des Tools wird vom DFN-CERT und dem BSI unterstützt.

OpenVAS ist eine Weiterentwicklung der letzten freien Version des Tools Nessus, für welches 2005 die Benutzung von neuen Versionen kostenpflichtig wurde.

Mit OpenVAS können Systeme auf ihre Verwundbarkeit überprüft werden. Ein auf einem UNIX-ähnlichen Betriebssystemen installierter OpenVAS-Dämon kann von OpenVAS-Clients, die auch unter Windows einsetzbar sind, über das Netz administriert werden und den Test auf Verwundbarkeit durchführen um zu erkennen, ob in ein Netzwerk eingebrochen oder ob es missbraucht werden kann.

Neben vielen anderen Tests werden auch Port Scans durchgeführt, wobei das zu verwendene Scan-Programm angegeben werden kann. Häufig wird hierzu Nmap benutzt. Innerhalb von OpenVAS wird zudem Arachni verwendet, wobei dieses Schwachstellen in Webanwendungen auffinden kann (siehe für eine Übersicht von Schwachstellenscannern für Webanwendungen). Arachni kann u.a. testen, ob Cross Site Scripting oder verschiendene Arten von Injections (z.B. SQL Injection) bei einer Webseite möglich sind. Arachni kann auch unabhängig von OpenVAS genutzt werden. Bei dem Test einer sich in der Entwicklung befindlichen Webanwendung an der FH Lübeck wurde hiermit beispielsweise entdeckt, dass die Eingaben in das Formular bei der Erstregistrierung im Klartext übertragen wurden.

Als Ergebnis zeigt OpenVAS einen umfangreichen Report, der auf verschiedene Arten u.a. auch grafisch ausgegeben werden kann. In den Reports werden die gefundenen Lücken im Klartext beschrieben. Die Größe des Risikos und Lösungsvorschläge werden angegeben.

Im Folgenden ist der Report (von Nessus) für eine gefundene Sicherheitslücke zu sehen:

Vulnerability ftp
(21/tcp) The remote FTP server seems to be vulnerable to an exhaustion
attack which may makes it consume all available memory on the
remote host when it receives the command :
NLST /../*/../*/../*/../*/../*/../*/../*/../*/../*/../
Solution : upgrade to ProFTPd 1.2.2 if the remote server is
Proftpd, or contact your vendor for a patch.
Reference : http://online.securityfocus.com/archive/1/169069
Risk factor : High
Nessus ID : 10634

Eine regelmäßige Überprüfung der eigenen Systeme mit OpenVAS ist ratsam. Für wissenschaftliche Einrichtungen in Deutschland bietet das DFN-CERT den Netzwerkprüfungsservice an (siehe auch Artikel in den DFN-Mitteilungen). Bei diesem Service wird unter anderem OpenVAS für die Untersuchung der Netzsicherheit genutzt.

Vom BSI gibt es eine Studie, wie Penetrationstests durchgeführt werden sollten.

1.6.4 Wireshark

Der freie Paket-Analysator '''Wireshark''' (früherer Name Ethereal) kann dazu verwendet werden, den Datenverkehr an den eigenen Netzwerkschnittstellen aufzuzeichen und auszuwerten. Es wird für Windows, Mac OS und als Quellcode bereitgestellt. Wireshark hat kommerzielle Netzwerkanalysatoren so gut wie bedeutungslos gemacht, da Wireshark alle gängigen Netzwerkprotokolle auswerten kann.

Auf der Wireshark-Homepage werden mehrere Videos angeboten, die dessen Verwendung erklären.

Bei der Aufzeichnung von WLAN-Daten unter Windows ist zu beachten, dass Wireshark diese nicht mit allen Details anzeigt. Wireshark stellt diese als Ethernet-Rahmen dar und entfernt so eine ganze Reihe von WLAN-spezifischen Informationen. Dieses kann auch bei der Analyse von VLANs vorkommen, so dass VLAN Tags nicht angezeigt werden.

1.6.5 Tools zum ARP Spoofing

Bei Ettercap handelt es sich um ein Tool, mit dem ARP Spoofing und weitere Funktionalitäten zum Auswerten der gesammelten Daten integriert sind. So können dann Benutzernamen und Passwörter herausgefiltert werden. Die ausgelesenen Daten können auch an Wireshark zur weiteren Auswertung weitergeleitet werden.

1.6.6 Tools für WLAN

Bei Kismet handelt es sich um einen Open Source WLAN Sniffer, der passiv arbeitet. Das bedeutet, dass von diesem Tool keine Daten in das WLAN gesendet werden. Kismet gibt es für Linux, MacOS und über Cygwin auch für Windows. Ein anderer WLAN-Sniffer ist NetStumbler.

Bei aircrack-ng handelt es sich um eine Sammlung von Open Source Software zum Analysieren von Schwachstellen in WLANs. Für das Angreifen der WEP-Verschlüsselung stehen verschiedene Möglichkeiten zur Verfügung, die eine schnelle Entschlüsselung erlauben. Zum Angriff auf WPA/WPA2-gesicherte Netzwerke sind Wörterbuchangriffe implementiert. Im Gegensatz zu Kismet ist Aircrack-ng auch dafür ausgelegt, aktiv Daten in das WLAN einzuschleusen.

1.6.7 Tools zur Herausfinden von Passwörtern

Das Tool John the Ripper dient zum Testen der Sicherheit von Passwörtern. Es steht als Open Source Software für viele Betriebssysteme zur Verfügung.

Mit John the Ripper können sowohl Brute Force- als auch Wörterbuchangriffe durchgeführt werden.

1.6.8 Schwachstellendatenbanken

Im Metasploit-Projekt werden Informationen über Schwachstellen gesammelt und entsprechende IDS-Signaturen erstellt. Mit dem Metasploit Framework können Tests durchgeführt werden, ob diese Schwachstellen tatsächlich vorhanden sind (siehe *Neug11*).

Mit der von der Fa. Offensive Security betriebenen Google Hacking Database können gezielt Webserver gefunden werden, die gewisse Schwachstellen aufweisen. Ist beispielsweise bekannt, dass z.B. eine bestimmte Version eines Webservers angreifbar ist, können damit Webseiten gesucht werden, die auf dieser Software basieren. Das Auffinden von Schwachstellen kann aber auch unabhängig von dieser Datenbank durch eine spezielle Verwendung der normalen Googlesuche durchgeführt werden (siehe Artikel von Ars Technica).

Eine Schwachstellendatenbank wird auch von der NIST unter nvd.nist.gov bereitgestellt.

1.7 Praktikum: Angriffe aus dem Internet

Aufgabe

- Stellen Sie fest, ob Ihr Rechner das Identifikations-Feld im IP-Header bei jedem Paket um eins erhöht.
- Versuchen Sie mit **nmap** Kenntnis über das Betriebssystem des Hosts scanme.nmap.org zu erlangen.

1.8 Zusammenfassung: Angriffe aus dem Internet

In diesem Kapitel wurden typische Angriffsarten, die im Internet vorkommen, vorgestellt, wobei die Gliederung nach dem Hybriden Modell erfolgte. Zusätzlich wurden Angriffswerkzeuge vorgestellt.

Sollten Sie den dem Studium der Angriffsmöglichkeiten der Ansicht sein, dass diese zu vielfältig sind und daher eine Rückkehr zur analogen Technik anzuraten sei, dann sollten Sie den Erwerb einer Schreibmaschine in Betracht ziehen. Diese erreichen inzwischen wieder unerwartete Verkaufszahlen, z.B. für das Verfassen von Angeboten.

Als Kunde der Bankfiliale in Gammesfeld kann man sich zudem noch unabhängig vom Internet machen, wobei aber nur Einwohner des Ortes als Kunden akzeptiert werden. Damit ist nicht nur gemeint, dass diese Bank kein Internetbanking anbietet. Sie ist auch selbst nicht mit dem Zentrale der Genossenschaftsbanken vernetzt. In der Filiale wurde allerdings 2009 schließlich doch ein Computer angeschafft.

Das investigative Online-Portal "der Postillon" hat in einer representative Umfrage herausgefunden, dass 98% aller Hacker keine Skimaske vor dem Computer tragen, auch wenn dieses fälschlicherweise oft so dargestellt wird.

Auf humorvolle Weise beschäftigt sich Comedy Hacker Tobias Schrödel mit IT-Sicherheit. Bei seinen Auftritten demonstriert er u.a. wie leicht es ist Telefonnnummern zu fälschen. Ralf Wildfang und Thomas Pusch von der Fa. ML Consulting zeigen ebenfalls Hacking Methoden, u.a. die Wirkung von Trojanern auf Smartphones sowie Cross Site Scripting (siehe Bericht zu Auftritt in Köln).

I Literaturverzeichnis

BFHR11 Michael Brenner, Nils Otto vor dem gentschen Felde, Wolfgang Hommel, Helmut Reiser und Thomas Schaaf: "Praxisbuch ISO/IEC 27001: Management der Informationssicherheit und Vorbereitung auf die Zertifizierung", Hanser Verlag, München, 2011.

Böhm02 Wolfgang Böhmer: "VPN - Virtual Private Networks - Die reale Welt der virtuellen Netze", Hanser Verlag, München, 2002.

Doyl06 Jeff Doyle: "OSPF and IS-IS: Choosing an IGP for Large-Scale Networks", Addison Wesley, Upper Saddle River, NJ, 2006.

Ecke13 Claudia Eckert: "IT-Sicherheit, Konzepte - Verfahren - Protokolle", 8. Auflage, Oldenburg Verlag, 2013.

iX14 iX Kompakt Security, 4/2014, Heise Zeitschriften Verlag, Hannover, 2014.

KRS13 Heinrich Kersten, Jürgen Reuter, Klaus-Werner Schröder: IT-Sicherheitsmanagement nach ISO27001 und Grundschutz - Der Weg zur Zertifizierung, 4. Auflage, Springer Vieweg, Wiesbaden, 2013.

KuRo14 James F. Kurose und Keith W. Ross: "Computernetzwerke - Der Top-Down-Ansatz", 6. Auflage, Pearson Studium, München, 2014.

Neug11 Frank Neugebauer: "Penetration Testing mit Metasploit", d.punkt Verlag, Heidelberg, 2011.

Rech12 Jörg Rech: "Wireless LANs", 4. Auflage, Heise Zeitschriften Verlag, 2012.

Schi03 Jochen Schiller: "Mobilkommunikation", 2. Auflage, Pearson Studium, München, 2003.

Schm13 Klaus Schmeh: "Kryptographie. Verfahren, Protokolle, Infrastrukturen", d.punkt Verlag, Heidelberg, 2013.

Stal14 William Stallings: "Network Security Essentials - Applications and Standards", Fifth Edition, Pearson, Harlow, England, 2014.

TaWe12 Andrew S. Tanenbaum und David J. Wetherall: "Computernetzwerke", 5. Auflage, Pearson Studium, München, 2012.

II Abbildungsverzeichnis

III Medienverzeichnis