Angriffsverfahren

Wie finden Angriffe statt und was bewirken sie.
AllgemeinIch zeige hier nur einige der unzÃ¤hligen MÃ¶glichkeiten, die Cracker oder Script-Kiddies nutzen kÃ¶nnen, um Daten zu manipulieren, abzuhÃ¶ren, umzuleiten oder sonstige Angriffe durchzufÃ¼hren. Den Begriff Hacker habe ich hier absichtlich nicht verwendet, da dieser eigentlich Computerprofis bezeichnet. Cracker sind zwar auch Computerprofis, allerdings im negativen Sinn. Eine Unterscheidung kann hier auch in White- und Black-Hat erfolgen.Es soll keine Anleitung fÃ¼r solche AktivitÃ¤ten sein, sondern nur als Sensibilisierung fÃ¼r den Internet-User dienen!Begriffe

Social-Engineering: Personen dazu bringen geheime Informationen preiszugeben.

Port Scanning: Welcher Dienst lÃ¤uft auf dem Rechner?

Eavesdropping/Sniffing: Netzwerkverkehr mitlauschen.

IP Spoofing: Absenderadresse fÃ¤lschen.

Hijacking: Netzwerkverkehr umleiten.

Replaying: Mitgelauschte Pakete (Passwort-Authentifizierung) an einen Server erneut senden um sich mit den fremden Login einzuloggen.

Man-in-the-middle-Attack: Netzwerkverkehr Ã¼ber den eigenen PC durchschleusen.

Dos/DDos: Ein NetzwerkgerÃ¤t/Server "in die Knie zwingen".DoS/DDoS (Denial of Service)

Der Zweck dieses Angriffes ist es eine GerÃ¤t (Server, Router,...) mit sinnlosen Daten zu Ã¼berschÃ¼tten damit er keine regulÃ¤ren Anfragen mehr beantworten kann.

Dies konnte man frÃ¼her leicht mit einem Syn-Flooding erreichen. Hier werden hunderte von Verbindungsanfragen (SynÂ´s) an einem Server gestellt die der Server zu beantworten versucht. Diese SynÂ´s sind zwar kleine Pakete allerdings cached der Server diese Anfragen fÃ¼r einige Zeit und fÃ¼llt somit kontinuierlich seinen Speicher an bis er crashed.

Bei einem DDoS werden viele Rechner mit einem Tool infiziert welche diese SynÂ´s zur gleichen Zeit an einen bestimmten Server senden.

Ein Dos kann aber auch mit nicht spezifizierten IP-Paketen durchgefÃ¼hrt werden. Man nutzt dabei Schwachstellen eines bestimmten Betriebssystems aus, welches zB. bei Ã¼bergroÃŸen oder unbekannten Paketen einen SpeicherÃ¼berlauf produziert und dabei abstÃ¼rzt.

Betriebsysteme mit aktuellen Patches sollten vor solchen Angriffen geschÃ¼tzt sein.Brute-Force / Dictionary-Attack

Mit Brute-Force ist JEDE VerschlÃ¼sselung "knackbar" (auch AES, SHA, MD5, ... , in denen bis dato keine VerschlÃ¼sselungsschwÃ¤che festgestellt wurde). Es ist nur ein Zeitfaktor bzw. eine Frage der Rechenleistung bis alle MÃ¶glichkeiten durchprobiert sind.

Diese Attacken werden auf PasswÃ¶rter angewandt die nicht entschlÃ¼sselbar sind, da sie in Form eines Hash (MD5, SHA,...) abgelegt werden.

Eine Brute-Force-Attacke zielt darauf ab, auf ein Kennwort-GeschÃ¼tztes GerÃ¤t oder eine Kennwort-GeschÃ¼tzte Datei, Zugriff zu erlangen.

Dabei werden tausende Buchstaben/Zahlenkombinationen pro Sekunde durchgefÃ¼hrt bis man eventuell auf das richtige Passwort stÃ¶ÃŸt. Ein Passwort wie "Anita", "Mercedes", "FichtenstraÃŸe", "Passwort", oder Ã¤hnliches ist in wenigen Millisekunden gefunden! Ein Passwort wie "Password4Roland" erraten bessere Tools auch in einigen Sekunden. Bei komplizierten Buchstaben/Zahlenkombinationen wie "diekp+dkkk" ist eine Brute-Force-Attacke meist sinnlos, da sie zu lange dauern wÃ¼rde. Die Ausrede eines Users, "Das kann ich mir nicht merken", kann mit folgender Hilfestellungen gekontert werden: das ist ein kompliziertes passwort , das keiner knacken kann (der "," wird gegen ein "+" getauscht)

Der Unterschied zur Dictionary-Attack besteht darin, das hier nicht (nur) Buchstaben/Zahlenkombinationen durchprobiert werden sondern ein "WÃ¶rterbuch" zu Hilfe genommen wird. Die EintrÃ¤ge im WÃ¶rterbuch werden der Reihe nach durchprobiert.

Ein typischer Fall ist das EntschlÃ¼sseln eines PC- oder Router-Passwortes.Kompromittierung

Hier versucht man zB. den SchlÃ¼ssel einer IPSec-Verbindung zu entschlÃ¼sseln um in ein Netz einzudringen oder den Verkehr mitzulauschen, oder in ein System einzudringen. Viele Leute glauben das eine VPN-Verbindung immer sicher ist. Dem ist nicht immer so, weil eine IPSec-Verbindung mit einem einfachen Preshared-Key in kÃ¼rzester Zeit kompromittiert werden kann.

Die Vorgehensweise ist folgende: Man versucht eine IPSec-Verbindung mit dem VPN-Router aufzubauen. Die Einstellungen fÃ¼r die VerschlÃ¼sselung (DES, 3DES, AES,..) und IKE-Parameter (DH-1, DH-1,...) kann man leicht von Hand durchprobieren. Es wird fÃ¼r den Verbindungsaufbau einfach ein beliebiger Preshared-Key verwendet und eine Verbindung initiiert. Der VPN-Gateway sendet nach der Initiierung eine Challenge die lokal am PC gespeichert wird. Nach der erfolglosen Einwahl wird die abgespeicherte Challenge des VPN-Gateways in Ruhe mit einer Brute-Force- & Dictionary-Attack bearbeitet und wartet auf das Ergebnis. Wenn es ein einfacher SchlÃ¼ssel ist, ist er in Sekundenbruchteilen entschlÃ¼sselt. Jetzt kann man mit den richtigen und vollstÃ¤ndigen VPN-Parametern eine Verbindung zum VPN-Gateway aufbauen.

Der WEP-Key eines WLAN, kann bei entsprechenden Traffic, ebenfalls in relativ kurzer Zeit (bei genÃ¼gend Traffic der Ã¼ber den AP lÃ¤uft) alleine durch mitlauschen kompromittiert werden. Diese Tools nÃ¼tzen eine SchwÃ¤che im RC4-Algorithmus des WEP.

Ein anderer Fall einer Kompromittierung ist das Einschleusen eines Trojaners um den Rechner fernsteuern zu kÃ¶nnen oder Tastatureingaben mitlesen zu kÃ¶nnen.Man-in-the-middle-Attack

Wird verwendet um einen verschlÃ¼sselten Datenverkehr mitzulauschen. Dabei wird eine Verbindung die ein Rechner initiiert auf den eigenen Rechner umgeleitet und anschlieÃŸend an die eigentliche Zieladresse weitergeleitet.

In einem geswitchten Netz braucht man nur den ARP-Cache (Defaul-Gateway) eines PC zu verÃ¤ndern und schon ist eine Umleitung des gesamten Netzwerkverkehrs mÃ¶glich. Dabei kÃ¶nnen auch Daten einer VerschlÃ¼sselten Verbindung (SSL, SSH1) mitgelesen, mitprotokolliert und natÃ¼rlich auch entschlÃ¼sselt werden.

In einem gerouteten Netz ist dies etwas schwieriger. Hier muss man den DNS-Eintrag am jeweiligen DNS-Server verÃ¤ndern oder die DNS-Cache-EintrÃ¤ge am PC modifizieren. Dies funktioniert nicht in jeder Netz-Konstellation, da Routing-Technische Eigenschaften dies verhindern kÃ¶nnen.