SEMINARARBEIT
SICHERHEIT IN RECHNERNETZEN II

ATTACKEN AUF COMPUTERSYSTEME

Firewallsysteme II

Fachbereich Automatisierung / Informatik
Hochschule Harz Wernigerode

Professor: Prof. Dr. H. Strack

Verfasser: Patrick Kosiol
u15691
6607
7. Semester Kommunikationsinformatik
Distributed Computing

Wernigerode, 9. Februar 2004

ABSTRACT

Firewalls schützen sensible Computernetzwerke vor dem Zugriff unbefugter Dritter. Diese offerieren jedoch auch Schwachstellen, die einem Angreifer die Möglichkeit geben vertrauliche Daten zu sehen, zu manipulieren oder gar zu löschen. Verschiedene dieser Angriffsmöglichkeiten werden in dieser Seminararbeit dargelegt und mögliche Lösungsansätze vorgestellt. Bezogen auf die Angriffsmöglichkeiten wird gezeigt wie ein derartiger Eindringling vorgeht um gezielt Zugang zu geheimen Datensätzen zu erlangen oder gar komplette Computersysteme zu übernehmen.

Patrick Kosiol

INHALTSVERZEICHNIS

Abbildungsverzeichnis iii
Abkürzungsverzeichnis iv
Kapitel 1 – Einleitung 1
Kapitel 2 – Motivation der Angreifer 2
1. Sicherheitsexperten 3
2. Script Kiddies 4
3. Nicht ausgelastete Erwachsene 4
4. Ideologische Hacker 4
5. Kriminelle Hacker 5
6. Unternehmensspione 5
7. Verärgerte Angestellte 5
Kapitel 3 – Abläufe der Angriffe 7
1. Das Vorgehen der Hacker 7
2. Die Wege der Hacker 8
Kapitel 4 – Angriffstechniken 9
1. Heimliches Zuhören und Mitschneiden 9
1.1. Passwörter mitschneiden 10
1.2. Analysieren des Netzwerkverkehrs 11
1.3. Scannen von Netzwerkadressen 11
1.4. Scannen von Ports 12
1.5. IP Half-Scan Attack (stealth – attack oder half – open – scan) 12
1.6. IP – Spoofing 12
1.7. ARP – Spoofing 12
1.8. MAC – Flooding 13
1.9. Switch – Monitoring 13
1.10. Finger, WOHIS, NSLookup und DNS 13
1.11. Mitschneiden von SNMP – Packten 14
1.12. Funktionweise von „Packet Sniffern“ 15
2. Denial of Service und Distributed Denial of Service 15
2.1. Ping of Death 16
2.2. SYN – Angriff & LAND – Angriff 16
2.3. Teardrop 17
2.4. Ping / ICMP Flood 17
2.5. Smurf – Attack 18
2.6. Service spezifischer DoS – Angriff 18
2.7. DNS Cache Verschmutzung 18
2.8. Routen umbiegen (RIP, BDP, ICMP) 19
2.9. SNMP Rekonfiguration 19
2.10. UDP Bomb / Flood 19
2.11. UDP Snork Angriff 19
2.12. Mail Bomb Angriff 19
3. Protocol Exploitation 20
3.1. Source – Routing – Attack 20
3.2. Pufferüberläufe 20
4. Imitationen 21
4.1. DHCP, WINS und DNS Imitationen 22
4.2. Passwort mitschneiden, wiederholen und Server imitieren 22
5. Man in the Middle 23

6. Hijacking 23
Kapitel 5 - Firewallkonzepte 24
1. Paketfilter 24
2. Stateful Inspection Packet Filters 24
3. Application Proxies 25
4. Verschiedene Firewalltopologien 26
4.1 Ein Webserver *vor* der Firewall 26
4.2 Ein Webserver *hinter* der Firewall 27
4.3 Ein DMZ Netzwerk....27
4.4 Die Zwei – Firewalllösung....28
Kapitel 6 - Fazit 29
Literaturverzeichnis 30

ABBILDUNGSVERZEICHNIS

Nummer	*Seite*
2.1 – Hackerarten	3
3.1 – Das Vorgehen der Hacker	7
4.1 – Die Angriffsmuster der Hacker	9
4.2 – NSLookup – Angriff	14
4.3 – 3 – Wege – Handshake bei TCP	16
4.4 – Teardrop – Angriff	17
4.5 – Pufferüberläufe	21
4.6 – verschlüsselter 3 – Wege – Handshake	22
4.7 – Man in the Middle	23
5.1 – Application Proxy	25
5.2 – Ein Webserver vor der Firewall	26
5.3 – Ein Webserver hinter der Firewall	27
5.4 – Ein DMZ – Netzwerk	28
5.5 – Ein zwei Firewall Netzwerk	28

Die Nummerierung richtet sich nach den Kapitelnummern. Innerhalb eines Kapitels werden die Bilder fortlaufend nummeriert.

ABKÜRZUNGSVERZEICHNIS

Abkürzung	
DNS	Domain Name Service
IP	Internet Protocol
TCP	Transfer Control Protocol
UDP	User Datagram Protocol
LAN	Local Area Network
MAC	Media Access Control
NetBIOS	Network Binary Input Output System
NAT	Network Adress Transaltion
FDDI	Fibre Distributed Data Interface
NFS	Network File System
SMB	System Management Bus
FTP	File Transfer Protocol
SSL	Secure Socket Layer
DMZ	Demilitarized Zone
TCP / IP	Transfer Control Protocol / Internet Protocol
IDS	Intrusion Detection System
ARP	Address Resolution Protocol
NSLookup	Name Service Lookup
SNMP	Simple Network Management Protocol
TDR	Time Domain Reflection
SQL	Structured Query Language
DoS	Denial of Service
DDoS	Distributed Denial of Service
ICMP	Internet Control Message Protocol
SYN	Synchronize
ACK	Acknowledge
RPC	Remote Procedure Call
WINS	Windows Internet Name Service
ID	Identification
RIP	Routing Internet Protocol
BGP	Border Gateway Protocol
MS	Microsoft
URL	Uniform Resource Locator
Enc(PW)	Encrypted Password
HTML	HyperText Markup Language

Kapitel 1

EINLEITUNG

Als Oberbegriff für diese Seminararbeit ist der Bereich Firewallsysteme zu nennen. Aber warum wird in einer modernen und zivilisierten Welt eigentlich ein Firewallsystem benötigt? Welche Gefahren gibt es, vor denen ein derartiges System schützen soll? Wie gehen potentielle Angreifer vor, was sind ihre Taktiken und wie kann man sie dabei aufspüren und unschädlich machen?

Alle diese Fragen werden hier behandelt und Anhand der verschiedensten Angriffsmethoden aufgezeigt und analysiert.

Diese Seminararbeit setzt einige wichtige Vorkenntnisse des Lesers voraus. Aufgrund dessen wird darauf verzichtet Begriffe wie X.25 oder TCP/IP zu erklären. Informations- und Netzwerktechnische Grundkenntnisse sind hierfür zwingend erforderlich.

K a p i t e l 2

MOTIVATION DER ANGREIFER

Um die Angriffsmethoden und –strategien eines Hackers nachvollziehen zu können muss geklärt sein, warum dieser Angreifer Arbeit und Gefahr in Kauf nimmt um Computersysteme anzugreifen. Nichtsdestotrotz gäbe es ohne die Hacker keine Firewallsysteme, sie wären völlig nutzlos, da nie jemand ein Computersystem angreifen würde. Ursprünglich wurde der Begriff **Hacker** für Menschen verwendet, die sich gut mit Computern und deren Technik auskennen. Durch die Medien wurde dieser Begriff allerdings immer mehr in das kriminelle Milieu abgeschoben und hat sich seit geraumer Zeit dort festgesetzt. Es wurde dann versucht den Begriff **Cracker** als kriminellen Hacker zu etablieren, allerdings gelang dies nicht und somit steht ein Hacker immer noch für das Synonym des Bösen der Computerbranche. Mittlerweile wird dieser Begriff für jede Person genutzt, die versucht in ein Computersystem unauthorisiert einzudringen.

Die Kunst des Hackens zu erlernen beziehungsweise später auch erfolgreich Hacks durchzuführen nimmt sehr viel Zeit in Anspruch. Demzufolge kann man, wie von angesehener Fachliteratur und auch vielen Experten in diesem Gebiet proklamiert, ein Hacker in eine der zwei folgenden Kategorien eingeteilt werden.

I. Freizeit – Hacker

II. Profitorientierte Hacker

Ferner gibt es noch weitgehendere Differenzierungen in diesem Bereich. Folgende Auflistung offeriert die verschieden Möglichkeiten der genaueren Kategorisierung wobei mit steigender Nummerierung auch die Gefahr steigt, die von diesem Hacker ausgeht.

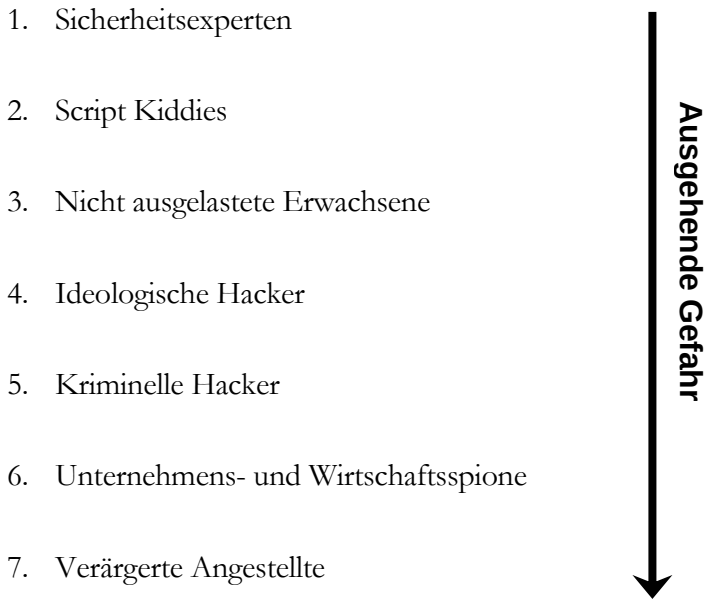

Abbildung 2.1

Dem zu folge geht von einem Sicherheitsexperten, wie soll es auch anders sein, die geringste Gefahr aus und von einem verärgerten Angestellten die potentiell höchste Gefahr aus. Dies zeigt auch wiederum wie wichtig es ist die Angestellten dementsprechend zu motivieren und geistig an das Unternehmen zu binden.

1. Sicherheitsexperten

Ihnen sind die diversen Hackingtechnicken vertraut und sie könnten Sie auch einsetzen wenn sie wollten. Dies wird allerdings nicht geschehen, da sie es aus moralischen und ethischen Gründen heraus ablehnen. Sie haben erkannt, dass sie mit der Prävention von Angriffen mehr Geld verdienen kann als mit den Angriffen selbst. Die meisten dieser so genannten Sicherheitsexperten waren früher selbst Hacker. Sie halten sich in Hacking – Communities und – Foren auf um immer auf dem aktuellsten Stand zu sein und die neusten Techniken zu kennen. Somit ist es ihnen möglich effektiver auf Angriffe reagieren und diese abwehren zu können.
Große Firmen engagieren derartige Experten um ihre eigenen Sicherheitssysteme oder die ihrer Kunden auf Brust und Nieren prüfen zu lassen. Diese Gruppe von Hackern (hier nicht im kriminellen Kontext) finden die meisten Sicherheitslöcher und Exploits in verschiedensten Softwarearchitekturen und schreiben Testprogramme dafür. Immer wieder werden diese Personen kritisiert, dass sie die auftauchenden Sicherheitsprobleme veröffentlichen. Es wird ihnen vorgeworfen, sie unterstützten das Hacking. Dies ist allerdings eine reine Unwahrheit, im Gegenteil. Durch diese Veröffentlichungen beugen Sie dem Hacken nur vor.

Was wäre, wenn niemand hacken würden und die ganze Computerwelt absolut in ‚Frieden' leben würde? Firwallsysteme sowie die diversen Verschlüsselungsalgorithmen wären absolut unnötig. Das Internet wäre ein ‚gleicher' Platz. Aber kommt nun der erste Hacker seiner Art daher, würde er uneingeschränkten Zugriff auf alle Daten der Welt haben. Es gäbe keine Grenzen.

2. Script Kiddies

Dieser Bereich wird hauptsächlich von Schülern und Studenten gefüllt. Diese haben für gewöhnlich ständig mit Computern zu tun, belegen derartige Kurse und studieren zu meist IT – lastige Studiengänge. Für Angriffsszenarien benutzen sie ihre eigenen Rechner oder für größere Aktionen die Computer in ihrer Schule / Computer Universität bzw. anderer öffentlicher Einrichtungen. Sie sind ständig auf der Suche nach potentiellen Zielen im weltweiten Netz und lieben den Kick. Diese Gruppe macht in etwa 90% aller Hacker im Internet aus. Sie wollen in der Regel keinen Schaden anrichten. Die größte Motivation für sie ist das beschaffen ‚freier' Dinge, sprich Software, Musik etc. Sie wollen, beim Eindringen in fremde Computersysteme, ihre eigenen Kräfte messen und etwas hinterlassen, was zeigt: „Ich war hier!" oder ähnliches. Allerdings gehört zu diesem Teilbereich auch die Sektion der Cybervandalen. Diese dringen in Systeme ein und versuchen alles zu zerstören was möglich ist. Mit diesem Akt fallen sie aber sofort in die Kategorie 5, der kriminellen Hacker.

3. Nicht ausgelastete Erwachsene

Diese unterbeschäftigen Erwachsenen waren früher Script Kiddies und sind mittlerweile aus dem jugendlichen Alter heraus. Ihre einzige Liebe gilt dem Hacken und sie sind ziemlich gut darin. Diese Menschen schreiben die Skripte, die von den Script Kiddies benutzt werden. Für sie gilt, wie auch für die vorangehende Gruppe: Sie wollen keinen Schaden anrichten und haben keine außerordentlich böswilligen Gedanken. Ein Großteil von ihnen sind Software- und Contentpiraten, die Cracks für bestehende kommerzielle Software schreiben. Außerdem stammen aus ihren Federn die meisten Software – Viren. Zu meist wollen sie zeigen wie gut sie sind und gegen die Regierung bzw. verschiedene Großkonzerne rebellieren. Das Hacking ist eine Art Wettbewerb für sie. Etwa ein zehntel aller Hacker unserer Erde kann in diese Kategorie eingeordnet werden.

4. Ideologische Hacker

Ihre politische Einstellung ist ihr Antrieb. Stehen etwa Wahlen oder wichtige politische Entscheidungen bevor, dann werden sie aktiv. Als Ziele kann man hier hauptsächlich Webseiten der ideologischen Gegner ausmachen. Aber auch Denial of Service Attacken werden gegen die

Gegner wie zum Beispiel Microsoft gefahren um diese außer Betrieb zu setzen. Es ist meist schwierig derartige Angreifer Dingfest zu machen. Oft kommen sie aus anderen Ländern, wo das Hacken nicht illegal ist, und werden somit in ihrer Regierung und ihrem Gesetz geschützt. Beispielsweise wurden Zeitungs- und Regierungsseiten von Palästinensern und Israelis verändert um ihre Ziele der Welt kund zu tun. Tausende von Internet – Information – Servern (Microsoft) wurden vom so genannten „Code Red" aus China befallen. Er veränderte auch die darauf gehosteten Seiten so dass Anti – USA – Parolen propagiert wurden. Derartige DoS – Angriffe nehmen immer mehr zu und treiben die Nutzung der Bandbreite enorm in die Höhe.

5. Kriminelle Hacker

Rache oder Geld sind die Ziele der kriminellen Hacker. Kredit – Karten – Daten stehlen, laufende Banktransaktionen hacken und vieles mehr gehört zu ihrem täglichen Leben um so schnell wie möglich an Geld zu kommen. Ihnen ist jedes Mittel recht und sie wollen alles haben woraus sie einen Nutzen ziehen können – auf Kosten Ihrer Opfer. Aufgrund der Tatsache, dass derartige Angriffe nicht sehr leicht benötigen diese Hacker einen hohen Grad an Intelligenz und sind demzufolge in einer verhältnismäßig geringen Zahl vertreten.

6. Unternehmensspione

Hacker dieser Kategorie sind auch ziemlich selten anzutreffen. In erster Linie liegt es daran, dass ihre Arbeit illegal ist und ihre Auftraggeber demzufolge auch illegal handeln würden. Außerdem sind sie sehr teuer. Nichtsdestotrotz werden sie oft gegen High – Tech – Firmen von fremden Regierungen engagiert um ihre ansässigen Unternehmen zu unterstützen.

7. Verärgerte Angestellte

Das größte Sicherheitsproblem stellen die verärgerten Angestellten dar, da ihre Angriffe schwer zu lokalisieren sind bevor sie geschehen. Hat eine Firma beispielsweise eine andere mit dem ausgliedern von Netzwerkdiensten beauftragt und nach geraumer entschieden, dass diese Firma nicht länger gebraucht wird, entsteht sehr schnell eine große Motivation für Angriffe. Aufgrund der guten Kenntnisse dieser Personen bezüglich der Netzwerkstrukturen kann man verhältnismäßig wenig gegen sie tun. Ein Angestellter, der einmal Administrator war kennt alle Sicherheitslöcher, Hintertüren, die Passwörter anderer und ‚administrative' Tools zum finden von möglichen Exploits. Kein Betriebssystem ist dem ‚Root – Level – Eploit' immun, nicht einmal das hochgelobte OpenBSD. Hat jemand einen Konsolen – Zugang und ist er motiviert ein System zusammenbrechen zu lassen, dann schafft er es auch, unabhängig von den Sicherheitsmaßnahmen.

Allerdings gibt es auch Vorteile. Diese Angreifer sind leicht zu finden und somit auch leicht zu verklagen. Das Gesetz ist in diesem Falle auf der Seite der Geschädigten Firma.

Aufbauend auf dem Wissen der Gefahr um die Motivationen der verschiedensten Angreifertypen kann man folgendes zusammenfassen. Firewallsysteme sind wichtig um derartige Eindringlinge abzuwehren, zurück zu verfolgen und letztendlich zu identifizieren.

K a p i t e l 3

ABLÄUFE DER ANGRIFFE

1. Das Vorgehen der Hacker

Prinzipiell geht ein Angreifer immer nach folgendem Schema vor.

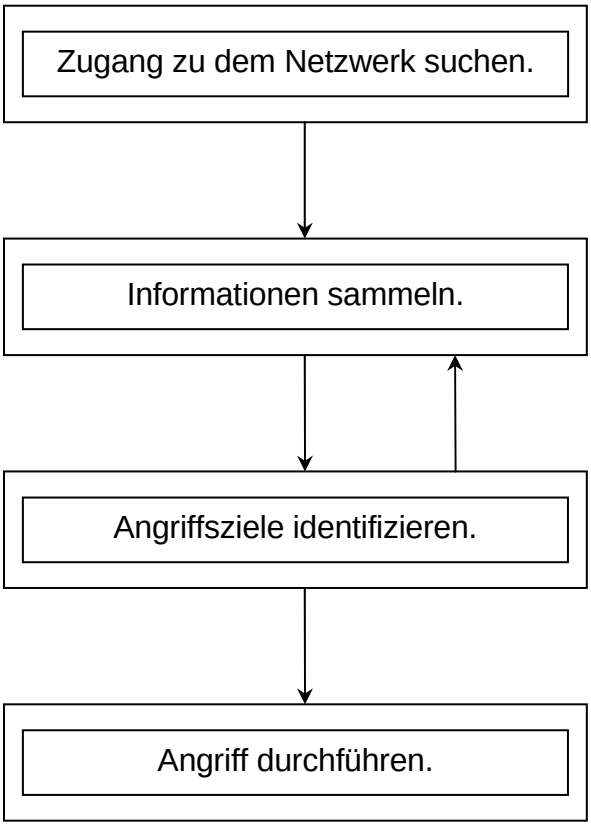

Abbildung 3.1

Demzufolge wird ein Angreifer immer zuerst einen Weg ins Netzwerk suchen (wenn er nicht schon drin wie z.B. bei den verärgerten Angestellten), danach wird er Informationen über das Netzwerk sammeln. Wie ist die IP Struktur, welche Server gibt es in dem Netzwerk, wie kann der DNS – Server erreicht werden? Diese, und viele mehr, sind Fragen die den Eindringling brennend interessieren. Aufgrund der gesammelten Informationen können dann die Angriffsziele ausgemacht und der Angriff vorbereitet und genau für diese Systeme zugeschnitten werden. Zu guter Letzt ist die Durchführung des Angriffs das Tüpfelchen auf dem i.

Um genau dies zu verhindern gibt es Firewallsysteme. Sie sollen den Angreifer daran hindern in ein Netzwerk einzudringen. Aber ist ihm dies leider einmal gelungen sollen ihn auch weitere interne Firewalls daran hindern essentielle Informationen sammeln zu können. Gelingt ihm auch dies besteht immer noch die Möglichkeit jeden einzelnen Rechner mit einer so genannten „Personal Firewall" (z.B. die freie „Kerio Personal Firewall" unter Windows oder die „iptables" unter Linux) vor unbefugten Zugriff auf offene Dienste zu schützen.

2. Die Wege der Hacker

Für alle Angreifer gibt es vier verschiedene Wege in verbotene bzw. geschützte Netzwerke. Diesbezüglich hat sich in den letzten Jahren sehr viel getan, die Internetanbindungen wurden immer preiswerter und öffneten somit mehr und mehr das weltweite Netz. Natürlich offerierte eine derartige Veränderung neuen potentiellen Hackern die Möglichkeit dem Mythos des Hackens nachzukommen. Durch den angesprochenen Zustrom neuer Nutzer und auch deren Computer sowie möglicherweise ganzer Netzwerke hinter diesen öffentlichen IP – Adressen, vergrößerte sich die Spielwiese der Hacker um einiges. Nichtsdestotrotz sind Unternehmensnetzwerke immer noch deren bevorzugte Ziele. Folgende vier Wege existieren für die Angreifer:

1. Über einen Computer in dem anzugreifenden Netzwerk direkt
2. per Remote Control (z.B.: DialUp o.ä.)
3. via Internet
4. durch direktes Verbinden zum Netzwerk (z.B.: per Wireless LAN)

Diese vier Möglichkeiten repräsentieren alle Möglichkeiten in ein Netzwerk einzudringen. Demzufolge zeigen sie auch alle Grenzen von Netzwerken auf, die geschützt werden müssen. Firewallsysteme lösen einen Großteil der angesprochenen Sicherheitsprobleme und können die Sicherheit in einem Computernetzwerk erhöhen.

Kapitel 4

ANGRIFFSTECHNIKEN

Hat ein Angreifer erst einmal einen Zugang zu einem Netzwerk bekommen, geht er nach folgendem Muster vor.

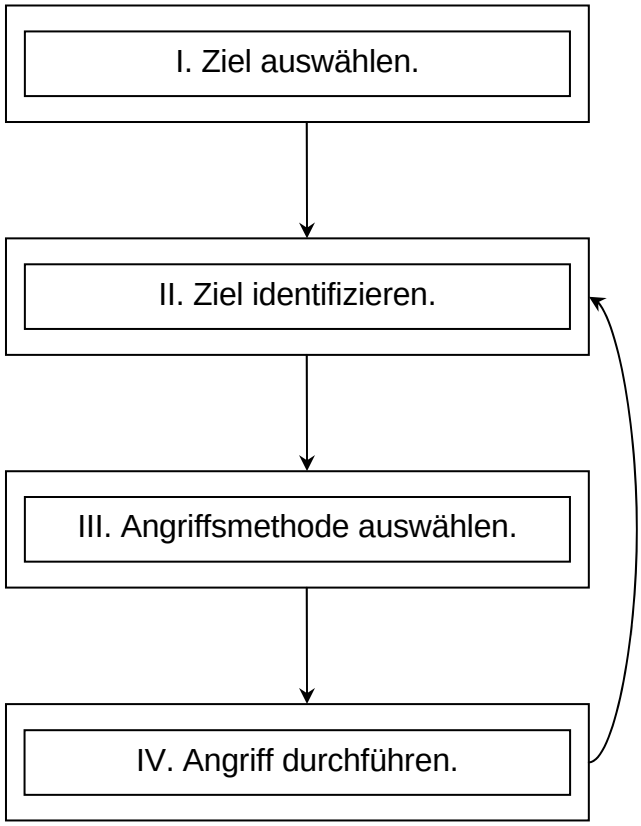

Abbildung 4.1

Ein Angriff läuft in der Regel immer in diesem Schema ab. Zwischen den Punkten II. bis IV. gibt es einen kreislaufähnlichen Ablauf. Mit jedem erfolgreichen Angriff sammelt ein Hacker immer mehr Informationen und bekommt somit oft die Möglichkeit noch weiter in verschiedene Systeme einzudringen.

1. Heimliches Zuhören und Mitschneiden

Unter diesem Oberbegriff ist das Lauschen eines Angreifers auf einer Netzwerkschnittstelle zusammengefasst. Beispielsweise liefert der Datenaustausch bei dem Domain – Name – Service eine große Anzahl an Informationen mit hohem Informationsgehalt. Hierzu gehören

Betriebssysteminformationen, Diensteinformationen, Netzwerkdaten, all dies sind Details die ein Hacker dringend benötigt.

Auch das Nutzen von Hubs statt Switches als Netzwerkgeräte erleichtern einem Eindringling das Mitschneiden von Informationen. Besitzt er einmal physischen Zugang zu einem Hub kann er sich dort verbinden und die Netzwerkkarte in einen so genannten „promiscous mode" versetzen, welcher ihm erlaubt alle vorbeikommenden Pakete mitzulesen.

1.1. Passwörter mitschneiden

Unter diesem Oberbegriff ist das Lauschen eines Angreifers auf einer Netzwerkschnittstelle zusammengefasst. Hierbei besteht für den Angreifer nahezu keine Gefahr erwischt zu werden. Das Mitschneiden des Netzwerkverkehrs ist technisch sehr einfach. Die meisten Protokolle übertragen ihre Daten unverschlüsselt, einige verschlüsseln jedoch wenigstens das Passwort. Werden alle Daten unverschlüsselt übertragen hat der Hacker leichtes Spiel. Aber auch ein verschlüsseltes Passwort wird ihn nicht abschrecken. Sollte der Verschlüsselungsalgorithmus schwach oder gar defekt sein, kann er das Passwort „offline" möglicherweise entschlüsseln oder aber eine Brut – Force – Attacke (ausprobieren aller Möglichkeiten) starten, da der Benutzername bekannt ist. Je mehr Datenverkehr an der Schnittstelle eines Hackers „vorbeikommt", desto mehr Informationen fließen ihm zu. Somit sollte der entstehende Netzwerkverkehr immer so gering wie möglich halten werden auch im Hinblick auf kostspielige Bandbreite. In diesem Kontext ist die Möglichkeit der MAC – Authentifizierung zu nennen. Dies würde bedeuten, dass eine Kommunikation nur zwischen authentifizierten MAC – Adressen statt findet. Allerdings steht dem die Tatsache entgegen, dass es einem Angreifer möglich ist „MAC – Adressen – Spoofing" zu betreiben. Hat ein Eindringling erstmal den Benutzernamen und das Passwort, kann er diesen Rechner ohne Probleme übernehmen. Um allerdings Daten per „Remote" mitschneiden zu können benötigt dieser z.B.: lediglich Zugriff auf den Netzwerkmonitor, der in jedem Microsoft Windows System integriert ist. Allerdings erscheinen für dieses Werkzeug immer wieder Sicherheitslücken, die es ihm ermöglichen den Netzwerkmonitor ferngesteuert zu bedienen. Aber auch der Microsoft Internet Explorer (mit 90% der weltweit meistgenutzte Browser) hat einen Dienst zum automatischen Authentifizieren im Intranet. Dieser sollte ursprünglich dazu dienen den leichten Aufbau eines Intranets realisieren zu können. Ein Server stellt beispielsweise eine Anfrage an den Client und dieser antwortet dann mit Benutzername und Passwort. Hierbei ist das Passwort mit einer Einweg – Hashfunktion verschlüsselt. Nun hat der Angreifer die Möglichkeit das Passwort per „Brut – Force" oder „List – Compare" (vergleichen des Passwortes mit einer Liste der

meistgenutzten Passwörter). Ist dies geschehen, hat dieser wiederum den Benutzernamen und das Passwort. Einen Nachteil gibt es aber auch bei dieser Möglichkeit. Der Benutzer des angesprochenen Clients muss vorher die Seite des Hackers besucht haben.

1.2. Analysieren des Netzwerkverkehrs

Nicht nur Passwörter sind wichtig, sondern insbesondere auch Informationen über die Netzwerkinfrastruktur spielen in dieser Beziehung eine wichtige Rolle. Zu diesen Informationen zählen:

- IP – Adressen der Quell- und Zielrechner
- Ortung der Router und Gateways
- Die Menge des Verkehrs zwischen einzelnen Rechnern
- Verschiedene Arten von Verkehr lassen auf die Funktionalitäten der Server schließen
- Dienstefähigkeit für Broadcasts (z.B.: für NetBIOS)
  → zeigt die Möglichkeit eines Sicherheitslochs und / oder mögliche Angriffsziele

→ ein Application – Proxy oder auch eine Firewall (mit NAT – Unterstützung) kann diese Probleme lösen. Das Abstellen von Broadcasts ist hier dringend erforderlich und bei jeder guten Firewall möglich.

1.3. Scannen von Netzwerkadressen

Diese Aktion ist der Anfang aller Angriffe und er wird in der Regel in Verbindung mit einem Port – Scan angewandt. Zu meist wird eine Range von IP – Adressen angegeben, die getestet werden. Kommt eine Antwort auf den Test ist ein potentielles Opfer gefunden. Hauptsächlich wird das Scannen von Netzwerkadressen innerhalb des TCP/IP – Protokolls vollzogen aber es ist auch möglich dies innerhalb von NWLink, X.25 und FDDI anzusiedeln. Die beste Möglichkeit das Scannen von Netzwerkadressen zu verhindern ist, darauf aufzupassen (als Netzwerkadministrator) ob dies geschieht und dann Schritte einzuleiten, die diese Aktionen stoppen. Gateways, Paketfilter und Router müssen so konfiguriert werden, dass Verbindungsanfragen zu Hosts geloggt werden, die nicht aus dem eigenen Netz kommen.

Diese Log – Dateien müssen natürlich regelmäßig überprüft werden. Eine andere Möglichkeit besteht darin die Software Alarm geben zu lassen wenn ein Scan läuft (wenn diese das unterstützt).

1.4. Scannen von Ports

Das Ziel dieser Aktion ist es Betriebssystemversionen, Dienste und offene Ports zu entdecken. Die Betriebssystemversion ist dahingehend wichtig, da verschiedene Betriebssysteme auch verschiedene Dienste per default zur Verfügung stellen. Es wird bei einem gefundenen offenen Port versucht so viele Informationen wie möglich von diesem Port auszulesen. Um einen Angreifer in dieser Aktion ausmachen zu können besteht die Möglichkeit einen „Honey Pot" aufzusetzen. Dieser Server dient lediglich dazu angegriffen zu werden. Es wird nicht veröffentlich, dass es diesen Server gibt, somit kann jeder Verbindungsversuch auf diesen Rechner als Angriff gewertet werden. Diese Verbindungsanfragen werden mitgeloggt und enttarnen somit den Eindringling.

1.5. IP Half-Scan Attack (stealth – attack oder half – open – scan)

Moderne Intrusion Detection Systeme (IDS) alarmieren den Benutzer eines Systems wenn er gescannt wird. Um dies zu verhindern gibt es dieses Prozedere. Es werden nur Start- bzw. Endpakete geschickt ohne eine richtige Verbindung aufzubauen. Viele IDS können dies nicht erkennen.

1.6. IP – Spoofing

Die Quell – IP wird hierbei im Paket ausgetauscht und somit wird dem Kommunikationspartner ein anderer Absender vorgetäuscht. Dies wird sehr oft in Verbindung mit anderen Attacken verwandt.

1.7. ARP – Spoofing

Dies ist eine leichte und effektive Möglichkeit so viel Verkehr wie möglich mitschneiden zu können. Hierbei wird den Clients vorgemacht, dass der Rechner des Angreifers der Router ist. Somit senden diese Clients ihre Daten an den Router, welcher unter der Kontrolle des Hackers ist. Die ARP – Pakete werden so abgeändert, dass die IP – Adresse des Routers auf die IP – Adresse des Angreifer – Rechners gemappt wird.

1.8. MAC – Flooding

Hierbei wird ein Switch mit einem kontinuierlichen Strom in dem eine Unmenge gefälschter zufälliger MAC – Adressen überflutet. Dies zwingt die meisten Switches in die Knie und sie wechseln somit von dem „bridging“ in den „repeating – mode“. Hierdurch wird der Switch veranlasst ein Hub – ähnliches Verhalten zu zeigen. Dies wiederum vereinfacht dem Angreifer das Mitschneiden von mehr Netzwerkverkehr.

1.9. Switch – Monitoring

Switches mit einem Monitoring – Port sind von diesem Angriff betroffen. Hat ein Angreifer den physischen Zugang zu einem solchen Switch kann er sich einfach an den Monitoring – Port anschließen und den gesamten Verkehr wiederum mitschneiden. Da hierfür allerdings der physische Zugang nötig ist müssen Netzwerkgeräte in verschlossenen Räumen gehalten werden.

1.10. Finger, WOHIS, NSLookup und DNS

Finger und WHOIS sind die Favoriten der Hacker in diesem Teilbereich da sie Zugangsnamen und persönliche Adressinformationen des Benutzers preisgeben. Somit besteht für den Eindringling schon die Möglichkeit des versuchten Zugriffs auf Computersysteme mit dem Zugangsnamen und gängiger Passwörter. Allerdings kann ein Netzwerkadministrator auf diese beiden Dienste leicht verzichten und sollte dies im Hinblick auf die Sicherheit auch. Sie sollten abgeschaltet werden. Allerdings ist der Domain – Name – Service von äußerster Wichtigkeit. Ein DNS – Server wird dann benötigt, wenn man hinter einer Firewall ein größeres Netz in Betrieb hat. Ein Angreifer kann durch den DNS die Struktur des Netzwerks herausfinden, da dieser die Zuordnung von IP – Adressen zu Namen speichert. Ein derartiger Server muss so konfiguriert werden, dass er nur Anfragen vom internen Netz entgegen nimmt und Anfragen von außen verwirft. Allerdings könnte ein Hacker ein Programm schreiben, dass auf der Basis von NSLookup einen DNS – Server simuliert.

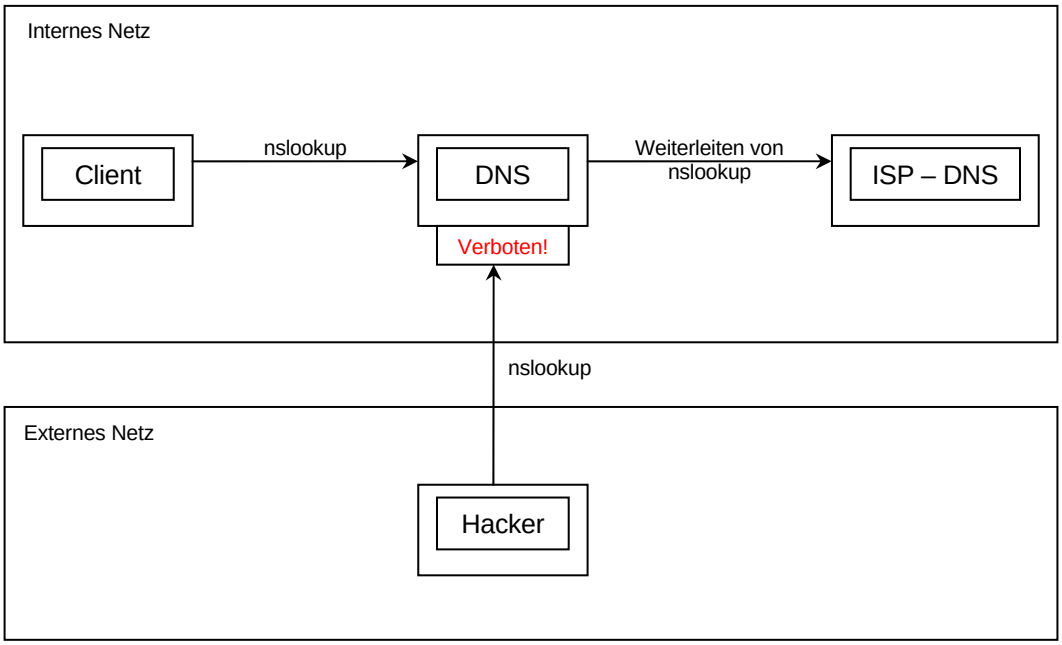

Abbildung 4.2

Das DNS – System ist hierarchisch aufgebaut. Kann ein DNS – Server eine Anfrage nicht auflösen reicht er diese an den nächsten weiter. Viele Internetseiten antworten nicht auf Anfragen, wenn ein so genanntes „reverse mapping“ nicht möglich ist. Somit müssen sie eine Anfrage an den lokalen DNS – Server stellen können. Daraus ergibt sich ein Problem, da potentielle Angreifer keine Anfrage von außen an den DNS – Server stellen dürfen. Dies wird durch eine Firewall gelöst indem sie auch Namensübersetzungen machen. Es werden alle Anfragen von außen geblockt außer von dem DNS – Server, der gerade vom Client eine Anfrage bekommen hat.

1.11. Mitschneiden von SNMP – Packten

Dieses Protokoll dient dem Management des Netzwerks sowie der Kontrolle und Überwachung von Netzwerkgeräten. Beispielsweise wird SNMP im Wohnheimnetz der Hochschule Harz zum kontrollieren des Verkehrs an den Switchports direkt benutzt. Ein deratiger Switch schickt regelmäßig SNMP – Pakete zum Administrator. Hierdurch kann ein Hacker auch eine Vielzahl an Informationen über das Netzwerk und deren Struktur in Erfahrung bringen. Um dieses Problem zu lösen sollte die Weiterleitung von SNMP – Paketen deaktiviert werden.

1.12. Funktionweise von „Packet Sniffern“

Grundsätzlich wurden solche Programme entwickelt um Netzwerkprobleme zu lösen und nicht um Daten zu „stehlen“. Es fängt alle vorbeikommenden Pakete ab und ermöglicht das Anzeigen sowie das Analysieren des Paketinhalts und auch deren Header. Diese Programme können auch gegen Hacker eingesetzt werden um sie zu identifizieren und zu verfolgen. Das Finden von „Sniffern“ kann mit Hilfe des Time Domain Reflectometers (TDR) erfolgen. Es sendet einen Impuls durch das Kabel und kreiert daraus einen Graph der Reflektionen, die zurückgegeben werden. Menschen, die einen derartigen Graph lesen können sind in der Lage ob und wo nicht authorisierte Geräte ans Kabel angeschlossen sind. Derartige Tools sind z.B.: Antisniff, neped oder Sentinel.

2. Denial of Service und Distributed Denial of Service

Dieser Abschnitt behandelt Angriffe die dem Lahmlegen von diensten eines bestimmten Servers gelten. In der Regel soll hierbei nicht das gesamte System beeinträchtigt werden, sondern nur einige oder ein ganz bestimmter Dienst. Auch die Übernahme des Systems steht hierbei nicht im Vordergrund. Beispielsweise konnte man vor geraumer Zeit noch einen (namentlich nicht genannten) SQL – Server mit nur einem einzigen UDP zum Absturz bringen. Dies wurde auf dem Kongress des Chaos Computer Club im Dezember 2003 demonstriert. Da dies mit nur einem speziell modifizierten UDP – Paket vollzogen werden kann ist eine wahre Großtat diese Sicherheitslücke zu entdecken.

Denial of Service Attacken sind die populärste Methode für Internethacker das Netz zu stören. Immer wieder bringen diese Angriffe große Internetserver zum Absturz. Ihr Ziel ist es bestimmte Netzwerke zu „deaktivieren“ und die Erreichbarkeit verschiedener Dienste zu verhindern. Die Software für derartige Angriffe ist fertig und steht der weiten Welt im Internet zur Verfügung. Praktisch jeder kann einen DoS – Angriff fahren ohne Ahnung davon zu haben wie er technisch funktioniert. Prinzipiell läuft es immer darauf hinaus Systemressourcen zu überreizen wie z.B.: die CPU oder den Arbeitsspeicher. Bei einem Distributed Denial of Service – Angriff wird das Prinzip des der Arbeitsteilung angewandt. Viele Rechner, über das Internet verteilt, führen gleichzeitig einen DoS – Angriff auf dasselbe Ziel aus. Beispielsweise ist es möglich, dass ein Hacker in der Vorbereitungsphase so genannte Trojaner auf vielen PCs im Internet installiert und diese als Zombie – Programme laufen lässt. Für einen Angriff werden diese Programme geweckt und führen dann zeitgleich den Angriff durch. Somit wird auch die wahre Herkunft des Angriffs verschleiert.

2.1. Ping of Death

Dieser Angriff ist weitestgehend veraltet und funktioniert bei Microsoft Windows ab der Version 95b nicht mehr. Aufgrund der hohen Popularität, des historischen Wertes und der Vollständigkeit wegen wurde er aber hier mit aufgenommen. Ein Angreifer schickt in diesem Fall einen Ping an das ausgewählte Opfer. Allerdings handelt es sich hier nicht um ein normales ICMP – Paket, sondern um ein so genanntes „killer IP packet" welches größer als 65535 bytes beträgt. Diese Größe entspricht genau dem Maximalwert der IP – Spezifikationen. Somit wird das System des Opfers hängen bleiben, neu starten, oder gar abstürzen.

2.2. SYN – Angriff & LAND – Angriff

Der auch „synchronized request attack" genannte Angriff bezieht sich auf den 3 – Wege – Handshake des TCP – Verbindungsaufbaus zwischen zwei Rechnern. Da TCP verbindungsorientiert ist muss eine Sitzung zum senden von Daten aufgebaut werden. Dies erfolgt folgender Maßen.

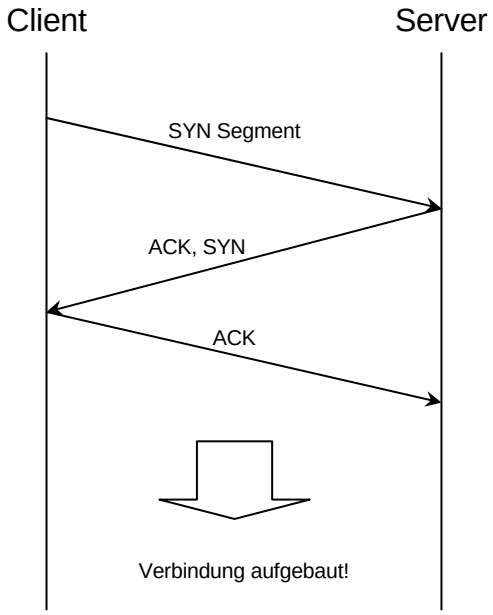

Abbildung 4.3

Ein Opfer des Angriffs wird mehreren SYN – Paketen gezielt beschossen in denen die IP – Quell – Adressen gefälscht sind. Das Angriffsziel antwortet auf diese Anfrage mit SYN / ACK – Paketen und wartet auf Antwort. Auf jedes verschickte ACK – Paket wird eine Antwort erwartet. Diese so genannten SYN/ACK – Waits sind in einer Warteschlange untergebracht, die irgendwann voll ist. Alle weiteren ankommenden SYN – Pakete werden daraufhin ignoriert.

Damit einer dieser SYN/ACK – Waits aus der Warteschlange gelöscht werden kann muss eine Antwort kommen oder der Timeout für das warten überschritten werden um den 3 – Way – Handshake zu terminieren. Da die Quell – IP – Adressen alle gefälscht sind wird nie eine Antwort vom verbindungsanfordernden Client kommen. Die Warteschlange bleibt voll und es besteht kein Platz mehr für richtige SYN – Anfragen. Somit ist der Dienst nicht mehr erreichbar und das Ziel des Hackers ist erreicht.

In der abgewandelten Form LAND sind die IP – Quell – Adressen immer gleich und zwar die des Opfer – Rechners. Dies verhindert das herausfiltern von nicht internen IP – Quell – Adressen.

2.3. Teardrop

Hierbei werden IP – Fragmente erstellt, die Teile eines IP – Pakets sind, in die originale IP – Pakete zerlegt werden können wie es beim Transfer durchs Internet geschieht. Das Problem besteht hierbei an den Offsetfeldern in den Fragmenten welche dafür da sind die Stelle (in bytes) im Originalpaket zu indizieren. Hier kann eine Überlappung stattfinden.

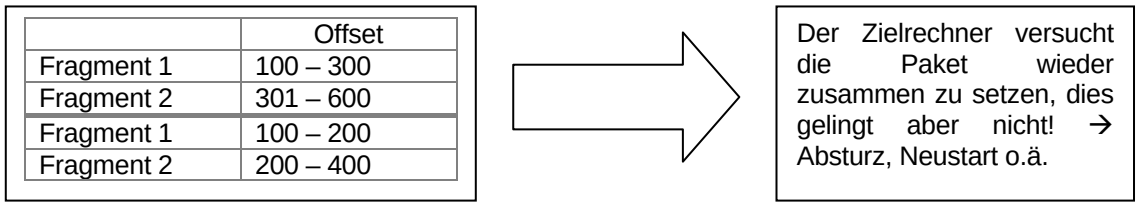

Abbildung 4.4

Variationen dieses Angriffs sind auch unter den Begriffen TearDrop2, NewTear, SynDrop oder auch Boink bekannt. Derartige Programme generieren Fragmentüberlappungen.

2.4. Ping / ICMP Flood

Ein spezieller Client wird hierbei angegriffen indem eine hohe Anazahl von ICMP – Paketen an WinSock oder Dialer – Software geschickt wird. Das verhindert, dass die Software auf Server – Ping – Aktivitäten antwortet, somit sollte der Server – Timeout auslaufen und die Verbindung geschlossen werden. Eine Variation hiervon ist auch unter Fraggle – Attack bekannt. Dabei wieder IP – Adresse des Opfers in das ICMP – Paket eingetragen und der Angreifer sendet diese Pakete an komplette Subnetze. Daraufhin wollen alle erreichbaren Rechner dieser

Anfrage antwortet und fluten den Client mit Echo – Reply – Nachrichten. Um dies zu verhindern können Firewalls so konfiguriert werden, dass sie ICMP – Pakete blocken.

2.5. Smurf – Attack

Hierbei handelt es sich um eine Art Brut – Force – Angriff. Im Grunde ist das Vorgehen hier das gleiche wie bei ICMP – Flood allerdings wird in diesem Fall der Datenstrom zu einem Netzwerk – Router geleitet. Das Ziel dieses Angriffs ist die Broadcast – Adresse des Netzes wodurch der Router diese Anfragen verteilt. Dadurch entsteht ein sehr hoher Verkehr im Netzwerk und es tritt ein DoS für die Benutzer ein um sich zu legitimieren. Zu meist wird in diesem Angriff IP – Quell – Adresse im Paket geändert. Daraus folgt, dass zwei Netze gleichzeitig angegriffen werden können und somit eine hohe Effizienz auftritt. Wodurch auch ab und zu ganze Internet Service Provider für einige Minuten außer Gefecht sind. Ein vergleichsweise langsames Modem kann ca. 40 – 50 ICMP – Pakete / Sekunde herausschicken. Dies multipliziert mit der Anzahl der Rechner bietet genug Angriffskraft um einen T-1 – Anschluss lahm zu legen. Als Gegenmaßnahme kann hier die Einschränkung des Broadcast – Traffics am Router nennen sowie die Firewall so zu konfigurieren, dass einkommende ICMP – Pakete herausgefiltert werden.

2.6. Service spezifischer DoS – Angriff

Genau ein Dienst nach einem derartigen Angriff nicht mehr erreichbar sein. RPC, NetBIOS, DNS und WINS sind in diesem Blickpunkt besonders attraktiv. Daten verschiedener Dienste sind auch unterschiedlich formatiert. Ein DNS wird somit keine WINS – Pakete verarbeiten können. Dadurch können die angegriffenen Rechner abstürzen wobei der Angreifer nur schwer auszumachen ist. Viele DNS – Versionen können mit derartigen Paketen umgehen aber einige stürzen noch ab wenn sie beispielsweise eine Antwort vor einer Anfrage bekommen haben. NetBIOS sollte von außen absolut nicht erreichbar sein. Dieser Dienst ist auch sehr anfällig.

2.7. DNS Cache Verschmutzung

Hierbei beobachtet der Hacker den Verkehr des DNS und stellt die Sequenz fest, die ein Rechner benutzt um Anfrage – IDs für rekursive DNS – Anfragen zu generieren. Somit kann er eigene Informationen diesen Anfragen hinzufügen. Zum Beispiel Daten, die den Vektor zu einem Rechner umleiten, der unter der Kontrolle des Hackers ist. Clients könnten möglicherweise auch nicht mehr Namen zu IP – Adressen auflösen können oder im schlimmsten Fall ihre kompletten Daten zu dem Rechner des Angreifers schicken.

2.8. Routen umbiegen (RIP, BGP, ICMP)

Wenn ein Eindringling einen Router kontrolliert kann er Bereiche des Netzwerks abtrennen oder den Verkehr in andere leiten. Routing erfolgt durch Protokolle wie beispielsweise RIP, OSPF und BGP. RIP nutzt keine Authentifizierung, somit kann er RIP – Pakete einfach manipulieren und dadurch die Routingtabellen nach seinen wünschen verändern. OSPF ist hier schon ein bisschen sicherer und BGP kann in diesem Bereich als ziemlich sicher bezeichnet werden.

2.9. SNMP Rekonfiguration

Bezug nehmend auf den Abschnitt des SNMP – Paket – Sniffens kann man diese Pakete auch verändern. Dies versetzt den Angreifer in die Lage Netzwerkgeräte umzukonfigurieren und Daten aus dem Netz zu leiten. Hierbei besteht jedoch eine Abhängigkeit zu den Fähigkeiten der angesprochenen Netzwerkgeräte

2.10. UDP Bomb / Flood

Ein Hacker kann sich UDP oder anderer Protokolle annehmen, die echo – Pakete benutzen, um eine Flut von UDP – Paketen zu generieren. Beispielsweise hat ein Rechner ein Programm, dass UDP – Pakete mit Buchstaben darin generiert und die an einen anderen Rechner schickt. Jedes geschickte Paket wird mit Echo – Paketen beantwortet. Es würde ein unendlicher UDP – Strom entstehen, auch als UDP – Storm bekannt. Die Ports 7 (echo), 13 (daytime), 17 (Zitat des Tages) und 19 (chargen) werden hierfür gern genutzt. Dementsprechend sollten Firewalls so konfiguriert sein, dass diese Ports nicht durchgelassen werden.

2.11. UDP Snork Angriff

Dies ist ähnlich dem UDP – Bomb – Angriff. Hierbei wird das UDP – Frame mit dem Quellport 7 (echo) oder 19 (chargen) und dem Zielport 137 (MS Location Service) erzeugt. Es entsteht eine Flut von UDP – Paketen und das angegriffene System wird langsamer und kann letztendlich abstürzen.

2.12. Mail Bomb Angriff

Das Ziel des Mail Bomb Angriffs ist es den Mailserver zu überwältigen und dessen Mailingdienst zu stoppen. Es wird eine hohe Anzahl an Mails an einen bestimmten Empfänger bzw. ein bestimmtes System geschickt. Mittlerweile existieren Programme im Internet wo

einfach nur die Angriffs Mail Adressen eingetragen braucht um einen derartigen Angriff zu starten. Nebenbei schützen diese Tools auch die Identität der Angreife sodass der Angriff nicht zurückverfolgt werden kann. Eine Variation genannt „List Linking“ gibt es auch. Dabei wird die Mail – Adresse des Opfers auf große Mailinglisten gesetzt. Beispiele für derartige Programme sind: UnaBomber, ExtremeMail, Avalaunche oder Kaboom. Firewallsysteme sollten regelmäßig überarbeitet und gewartet werden indem die Paketfilter so konfiguriert werden, dass Pakete aus Netzen von denen wiederholt Mailbomben kommen herausgefiltert werden. Dies funktioniert allerdings nicht mit Mailinglisten.

3. Protocol Exploitation

Diese Gruppe von Angriffen nutzt Fehler (so genannte Bugs) in verschiedenen Protokollen aus um mehr Zugriff zu bekommen als erlaubt ist.

3.1. Source – Routing – Attack

IP ermöglicht es dem Sender seinem Paket zu sagen über welche Router es gehen soll. In diesem Bereich kann man zwei Variationen unterscheiden:

3.1.1. Strict source routing: Der Sender kann die exakte Route festlegen (ist eher selten).

3.1.2. Loose source record route (LSSR): Der Sender kann Router angeben, die die Pakete passieren müssen.

Diese Option im IP Header überschreibt die Routingentscheidungen des passierenden Routers. Ursprünglich ist es dazu vorgesehen damit Administratoren Netzwerke kartographieren und Netzwerkprobleme lösen können. Indem sie Netzwerkverkehr auf einer bestimmten Route erzwingen. Ein Eindringling kann hierdurch an Informationen in Form von IP – Adressen des Local Area Networks kommen, die normalerweise nicht von außen erreichbar sind. Doch durch das Routen des Verkehrs durch eine Maschine die von beiden Seiten (Internet / Intranet) erreichbar sind. Source – Routing kann bei den meisten Routern und Firewalls deaktiviert werden und sollte es auch.

3.2. Pufferüberläufe

Dies sind die bekanntesten Möglichkeiten um Sicherheitsprobleme auszunutzen. In C / C++ wird Speicher allokiert, wenn eine Variable angelegt (1) wird und im Programmstack gespeichert. Wenn jetzt die nächste Funktion aufgerufen wird, dann wird der Rückgabewert

wiederum in dem Stack gespeichert (2). Wenn mehr Daten in die vorher allokierte Variable geschrieben werden als normalerweise reinpassen wird der Rückgabewert der Funktion überschrieben. Demzufolge enthält der Return – Pointer beim Ende der Funktion einen falschen Wert. Aber der Rechner macht trotzdem an dieser Stelle weiter und stürzt für gewöhnlich ab. Der jenige, der das Programm verfolgt hat kann an der angesprochenen Stelle Extra – Daten hinterlegen und somit beispielsweise an eine andere Stelle im Programm springen. Dadurch kann ausführbarer Programmcode (z.B.: per URL oder einer Internetseite) eingeschleust werden. Es müssen immer so viele Daten geschrieben werden damit der Return – Pointer an den Anfang des Stacks springt. Der Programmcode wird mit dem Rechteck des ursprünglichen Programms (bzw. dessen Benutzers) ausgeführt. Ist dies hier „root“ oder „Administrator“ dann steht dem Eindringling alles offen. Er kann ein weiteres Sicherheitsloch öffnen oder beispielsweise einen Trojaner einschleusen. Einige Programmiertechniken sind dermaßen anfällig, dass ein Hacker einfach danach scannen kann (z.B.: strcpy() → keine Puffergrenzen).

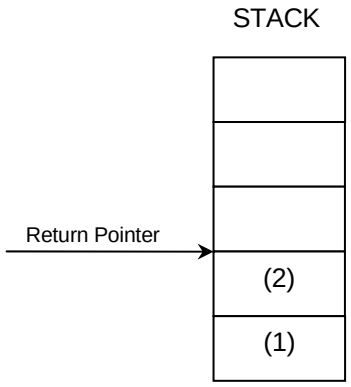

Abbildung 4.5

Ist ein derartiger Bug gefunden dann wird ein Exploit – Code geschrieben der darauf passt. Dieser Code, auch Skript genannt, wird auf einer Homepage veröffentlicht und von den Script Kiddies herunter geladen. Der Apache Webserver und der Internet Information Server machen zusammen ca. 90% aller Webserver im Internet aus. Sendmail ist der mit 80% am häufigsten verwendete Mailserver der Welt. Demzufolge diese Programme / Dienste ständig analysiert und es ist interessant wie selten wirklich neue Angriffe auftauchen. Somit kann man mit unbekannten Web- bzw. Mailservern das Risiko eines Sicherheitsproblems minimieren.

4. Imitationen

In diesem Bereich kann man auch das IP – Source – Routing ansiedeln.

4.1. DHCP, WINS und DNS Imitationen

Wurden die externen DHCP, WINS und DNS Server außer Funktion gesetzt, kann der Hacker diese Dienste anbieten und die ankommenden Anfragen befriedigen.

4.2. Passwort mitschneiden, wiederholen und Server imitieren

Verschlüsselte Daten werden gespeichert und später geschickt. Bei Chellange – Response wird dem Passwort ein Zeitstempel hinzugefügt.

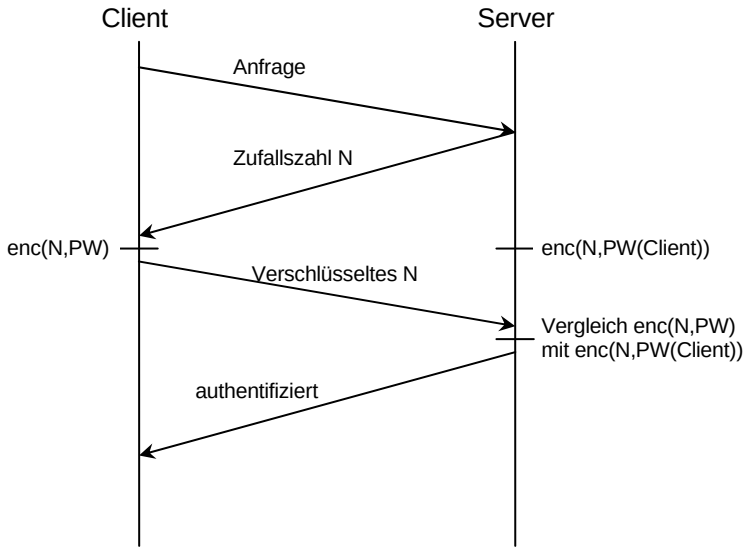

Abbildung 4.6

Sollte ein Hacker den Verkehr zwischen Client und Server stören kann es so weit kommen, dass dieser auf eine geringere Verschlüsselung umschaltet oder diese gar ganz abstellt. Dann kann ein Hacker einen Server errichten, der diesen Dienst übernimmt und die Passwörter aufsammelt. Es wird eine Zahl festgelegt, die immer als Pseudozufallszahl gesendet wird. Somit wird das entschlüsseln des Passworts erleichtert.

5. Man in the Middle

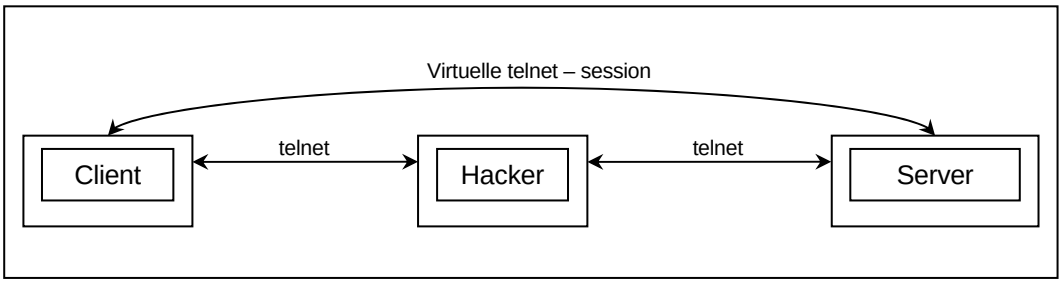

Abbildung 4.7

Bei dem Man in the Middle – Angriff befindet sich der Hacker zwischen den beiden Kommunikationspartnern. In dem gezeigten Beispiel stellt der Client eine Telnet – Verbindung zu einem Server auf und versucht eine HTML – Datei aufzubauen. Der Hacker fungiert als eine Art Gateway und leitet alle Daten weiter, somit wird eine virtuelle Point 2 Point Telnet – Verbindung simuliert. Allerdings loggt der Hacker alle die gesamten Daten mit. Als Lösung könnte man hier Verschlüsselungsalgorithmen einführen und das lokale Netz so absichern, dass kein Eindringling reinkommen kann.

6. Hijacking

Unter Hijacking versteht man das Übernehmen einer bereits bestehenden und authentifizierten Netzwerkverbindung. Es kann verschiedenen Schichten passieren: Erstens auf dem TCP – Layer und zweitens auf der SMB / NFS – Ebene, welche auf TCP aufsetzt. Hierzu muss ein Hacker in der Lage sein die TCP – Sequenznummern voraussagen zu können, dann kann er die TCP – Verbindung „umbiegen“ und einen DoS – Angriff auf den Client fahren. Für SMB benötigt man die richtige Frame ID, Tree ID und User ID. SMB – Hijacking ist theoretisch möglich aber es existieren noch keine Programme die dies bewerkstelligen, da keine SMB – Server nach außen hin offen sind. Dies ist auch zwingend notwendig.

K a p i t e l 5

FIREWALLKONZEPTE

Um derartige Gefahren abwehren zu können wurden Konzepte für Firewallsysteme entwickelt. Diese erlauben es den Datenverkehr zwischen zwei (oder mehr) Netzen zu filtern und ‚gefährliche' Daten nicht in das zu schützende Netz durch zu lassen. Im Folgenden werden verschiede auserwählte Schutzmechanismen und ~technologien vorgestellt.

1. Paketfilter

Diese Filtermethode im Bereich der Paketfilter einzuordnen. Paketfilter arbeiten im Allgemeinen nach dem Prinzip des Analysierens aller eingehenden Datenpakete. Dies kann auf den IP und / oder TCP / UDP Schichten passieren. Da derartige Paketfilter jedes Paket für sich betrachtet kann es keine komplette TCP – Session überwachen. Somit ist es schwer falsche Pakete (mit gespooften Adressen) zu erkennen die über eine Ein – bzw. Ausgangsschnittstelle in die Firewall gelangen. Sie geben vor zu einer Session zu gehören indem bei ihnen das ACK – Flag gesetzt ist. Paketfilter sind so konfiguriert, dass sie Netzwerkverkehr zu Quell- und Zieladressen, Quell- und Zielports sowie von verschiedenen Protokolltypen (z.B. ICMP) blockieren.

Warum sollte man also Paketfilter einsetzen wenn es so leicht ist sie zu täuschen?

Die Antwort lautet Geschwindigkeit. Wenn diese Filter keine Anwendungsdaten in den Paketen analysieren sind sie annähernd so schnell wie Router, die nur Paketrouting und ~Weiterleitung machen. Wie wir sehen werden haben sich die Konzepte der Paketfilter stark weiterentwickelt.

2. Stateful Inspection Packet Filters

Stateful Inspection Packet Filters steht für *Zustandsüberprüfende Paketfilter*.

Dieses Konzept hat als Ziel die Leistungsfähigkeit und Sicherheit ‚normaler' Paketfilter zu steigern wobei die Geschwindigkeit der Analysierung in etwa gleich bleiben soll. Ein Paketfilter mit Stateful Inspection ist in der Lage Netzwerk – Sitzungen zu verfolgen, so ist es möglich ein eingehendes ACK – Paket genau einer Verbindungstabelle zuzuordnen. Es wird ein neuer Eintrag in der Tabelle angelegt, wenn die Firewall ein SYN – Paket erreicht (welches den Anfang einer neuen TCP – Sitzung repräsentiert). Dieser Eintrag zeigt dann auf alle folgenden Pakete der erstellten Session.

Derartige Einträge werden wieder aus der Tabelle gelöscht wenn eine bestimmte (konfigurierbare) Zeit (Timeout) überschritten wurde.

Diese Zustandsbehaftung kann auch auf die UDP – Kommunikation in einer Pseudo – Art angewandt werden. In diesem Fall erzeugt die Firewall einen Eintrag in die Verbindungstabelle wenn das erste UDP – Paket übermittelt wurde. Ein UDP – Paket eines weniger sicheren Netzwerks (eine Antwort) wird nur akzeptiert wenn ein entsprechender Eintrag in der Tabelle zu finden ist. Wenn wir auf die Anwendungsschicht (Schicht 7) schauen finden wir einige Zustandsbehaftete Protokolle wie das File Transfer Protocol (FTP). FTP ist ein bisschen anders indem sich der Benutzer auf Port 21 (Befehle) verbindet und der Server eine Verbindung in Rückrichtung eine Verbindung auf Port 20 (Daten) aufbaut, wenn dieser eine Datei anfordert. Wenn die Firewall diese FTP – Kontrollverbindung nicht erkennt wird sie die Datenverbindung nicht erlauben. Dieses Konzept bezieht sich auch auf die neuen Multimediaprotokolle wie RealAudio und NetMeeting.

Stateful Inspection Packet filters sind die Geschwindigkeitskönige der Firewalls und am flexibelsten im Integrieren neu entwickelter Protokolle. Allerdings sind sie weniger sicher als Application Proxies. Check Point FireWall-1 (FW-1) und die Cisco PIX sind die führenden Firewalls in diesem Bereich.

3. Application Proxies

Wie der Name schon impliziert arbeiten die *Application Proxies* als Zwischenhändler in Netzwerksitzungen. Die Verbindung des Benutzers endet an dem Proxy und eine entsprechende separate Verbindung wird vom Proxy zum Zielhost aufgebaut. Die Verbindung wird bis hoch zu der Anwendungsschicht hin analysiert. Es ist charakteristisch, dass Proxies ein größeres Maß an Sicherheit bieten als Paketfilter, allerdings sind sie auch nicht so performant. Folgende Graphik zeigt der Paketprozess abgearbeitet wird bevor ein Paket geblockt oder zugelassen wird.

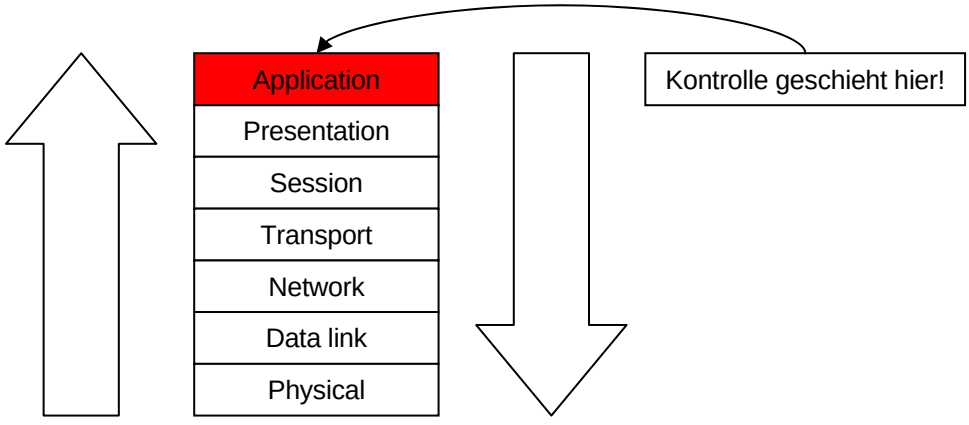

Abbildung 5.1

Eine potentiell wichtige Limitierung von *Application Proxies* ist die, dass neue Anwendungsprotokolle implementiert werden müssen damit der Proxy mit diesen Umgehen kann. Somit kann es passieren, dass es eine neue Multicasting – Video – Technik gibt und der Proxy diese nicht verarbeiten kann. Beispiele für Proxy – basierte Firewalls sond Gauntlet von Secure Computing (übernommen von Computer Associates) und Symantec Raptor (auch als Enterprise Firewall bekannt).

4. Verschiedene Firewalltopologien

Aufgrund der verschiedenen Anforderungen und Dienste die ein Unternehmen heutzutage benötigt gibt es eine Unzahl an Varianten wie eine Firewall im Unternehmensnetzwerk platziert werden kann. Im Folgenden werden einige wenige auserwählte Topologien vorgestellt.

4.1 Ein Webserver *vor* der Firewall

Als Unternehmen im Internetgeschäft benötigt man einen Webserver der die Firma nach außen hin repräsentiert und somit auch erreichbar sein muss, und ein Internes Netz welches vor dem Zugriff von Außerhalb geschützt sein muss.

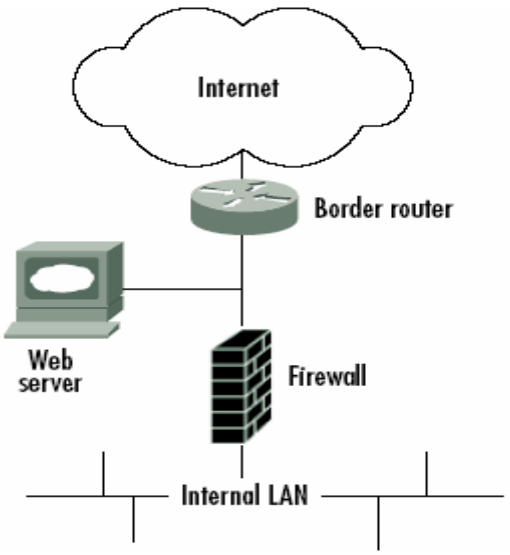

Abbildung 5.2

Somit hat die Firewall genau zwei Schnittstellen, die innere und die äußere. Hier kann ganz genau festgelegt werden, welche Daten in das Firmen interne Intranet dürfen und welche geblockt werden. Allerdings steht hier einem potentiellen Angreifer Tür und Angel offen um den Webserver anzugreifen. DoS – Attacken sind, wie in Kap. 4 – 2 beschrieben, ein bevorzugter Angriff auf derartige Server und könnten nicht abgewährt werden.

4.2 Ein Webserver *hinter* der Firewall

Hierbei würde der Webserver innerhalb des internen Firmennetzes platziert werden. Um von außerhalb auf ihn zugreifen zu können muss die Firewall so konfiguriert werden, dass sie Port 80 und möglicherweise auch noch 443 (SSL) durchlässt.

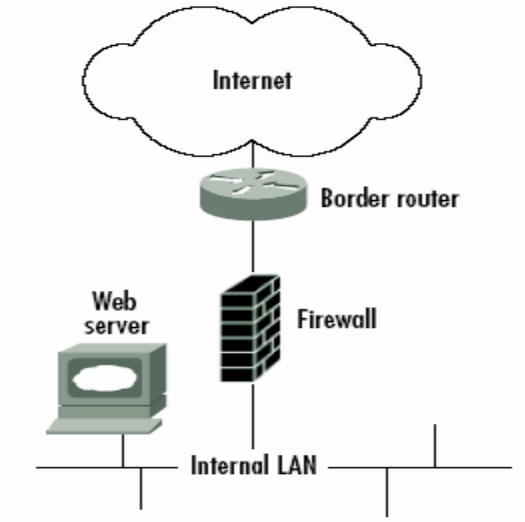

Abbildung 5.3

Dies schützt den Webserver und das interne Netz in gleichen maßen. Allerdings ist es einem Eindringling, der schon einmal Zugang zum internen Netz gefunden hat ein Leichtes den Webserver ohne Restriktionen anzugreifen.

4.3 Ein DMZ Netzwerk

Dieses Problem löst die Fähigkeit einiger Firewalls mit mehreren Netzwerkschnittstellen wie sie in den meisten kommerziellen Lösungen angewandt wird. Es werden bestimmte Zonen angelegt, die nicht als interne aber auch nicht als externe Zone angesehen werden. Derartige Zonen werden *DMZ* genannt, also ***de**militarisierte **Z**one*. Eine *DMZ* wird von der Firewall im selben Maße vor dem externen wie vor dem internen Netzwerk geschützt.

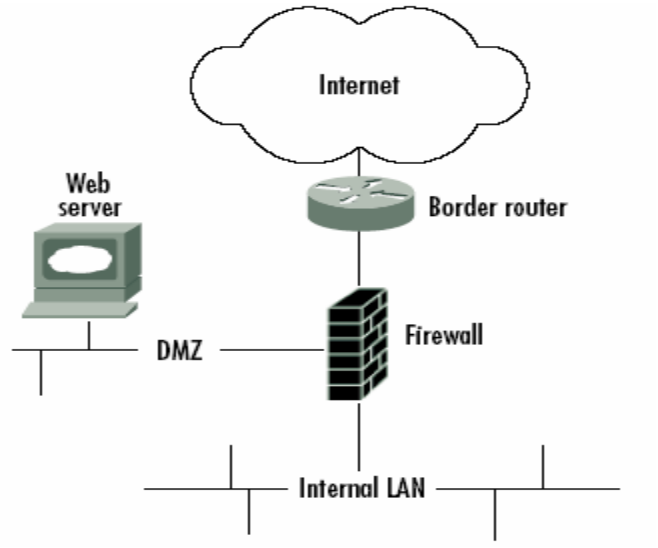

Abbildung 5.4

4.4 Die Zwei – Firewall - Lösung

Ein anderes Design, welches of Anwendung findet, ist der Einsatz von zwei Firewalls. Eine für das interne Netz und eine für das externe Netz mit der *DMZ* dazwischen. Manchmal werden Firewallsysteme von verschiedenen Herstellern benutzt mit dem Glauben, dass ein Sicherheitsloch in einem der Firewalls von der anderen geblockt wird. Aber die Erfahrung zeigt, dass fast alle ‚Firewalldurchbrüche' aufgrund schlecht konfigurierter Firewalls geschehen konnten und nicht durch Fehler in den Systemen selbst.

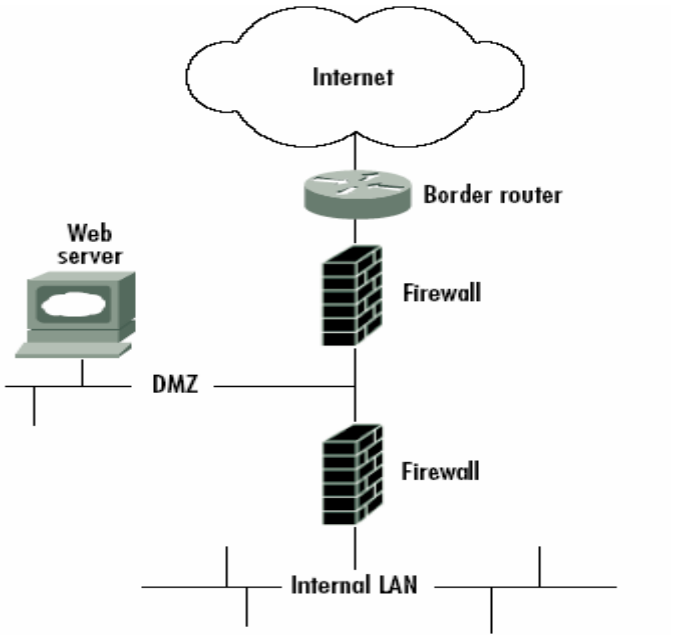

Abbildung 5.5

Ein derartiges Design erhöht nur die Kosten und den Managementaufwand ohne sehr viel mehr Sicherheit zur Verfügung zu stellen.

Kapitel 6

FAZIT

Die hier vorgestellten Angriffstechniken repräsentieren nur eine kleine Auswahl aller Möglichkeiten die ein Angreifer heutzutage hat. Nichtsdestotrotz sind die beliebtesten und somit auch meist angewendeten. Von derartigen Eindringlingen, seien sie gut- oder bösartig, geht eine Gefahr aus die unbedingt so weit wie möglich minimiert werden muss. Der Sicherheitsaspekt spielt in der heutigen Welt eine große Rolle und darf nicht unterschätzt werden. Auch wenn Firewallsysteme nicht das Allheilmittel hierfür sind, tragen Sie dennoch stark dazu bei die Sicherheit zu erhöhen und das Gefahrpotential in einem erträglichen Maß zu halten. Ein Administrator derartiger Systeme muss immer auf dem neusten Stand der Technik sein und darf die Wartung seiner Systeme nicht außer Acht gelassen werden. Die Konzeption eines zu sichernden Netzes sollte sehr gut überlegt sein und nicht ‚einfach mal schnell' implementiert werden. Firewalls, seien sie hardware- oder softwarebasiert, sind immer so gut zu konfigurieren, dass sie auf die Sicherheitsbedürfnisse des zu schützenden Netzes abgestimmt sind und ein Gleichgewicht mit den Diensteanforderungen innerhalb dieses Netzes bilden.

LITERATURVERZEICHNIS

- *Best Damn Firewall Book Period*
  Syngress Publishing
  ISBN: 1-931836-90-6
  Herausgegeben: 2003

- *Firewalls 24seven 2nd Edition*
  SYBEX Publishing
  ISBN: 0-7821-4054-8
  Herausgegeben: 2002
  Matthew Strebe, Charles Perkins

- *Load Balancing Servers, Firewalls, and Caches*
  Wiley Computer Publishing
  ISBN 0-471-41550-2
  Herausgegeben: 2002
  Chandra Kopparapu

- *Persoenliche Firewalls*
  Markt + Technik Verlag
  ISBN 3-8272-6289-5
  Herausgegeben: 2002
  Mick Tobor

- *Firewalls for Administrators and Remote Users*
  Prentice Hall
  ISBN 0-13-046222-5
  Herausgegeben: 2002
  Lisa Yeo