Thema der Ausgabe

Netzwerk-Verteidigung mit stationären und eventgesteuerten IP-Sinkholes

Victor Oppleman 

Schwierigkeitsgrad

Eine, bisher nicht sonderlich beachtete, Netzwerksicherheits-Technik hat sich als eine der effektivsten Möglichkeiten gegen Denial-of-Service-Attacken herausgestellt. Dieser Artikel wird erklären, wie man die Technik einsetzt, um wertvolle Informationen über die Gefahren zu erhalten.

Es wurde von Internet-Service-Provider hauptsächlich eingesetzt, um ihre Downstream-Kunden zu schützen. Dieser Artikel wird erklären, wie man die Technik namens Sinkholeing einsetzt, um wertvolle Informationen über die Gefahren zu erhalten, die das Netzwerk bedrohen. Durch die Implementierung von Sinkholes bekommt man neue Ansätze bei der Netzwerkverteidigung und des Sammelns von Informationen, sowohl bei Bedrohungen als auch bei Fehlkonfigurationen im Netzwerk.

Für Netzwerk-Erfahrene wird der Artikel folgendes bringen:

- Sinkhole: Hintergrund und Funktion – Eine kurze Einführung über IP-Sinkholes und wie eine Reihe von Firmen sie erfolgreich implementiert haben;
- Netzwerk-Köder-Fallen – Wie Sinkhole-Techniken, Darknets und Honeynets in Verbindung mit Netzwerk-Monitoring-Elementen dazu benutzt werden können um Scanning, Infiltrierungsversuche und andere Vorkomnisse zu vereiteln und zu analysieren;
- Schutz vor Denial-of-Service – Wie Firmen und ihre Upstream-ISPs eine Lösung für Denial-of-Service durch den Einbau von breitgefächerten, eventgesteuerten Sinkholes entwickelt haben;
- Backscatter und Tracebacks – Eine kleine Erklärung von Backscatter und darüber, wie Tracebacks eingesetzt werden können, um den Angriffspunkt eines Denial-of-Service in einem großen Netzwerk herauszufinden.

In diesem Artikel erfahren Sie...

- Sie werden lernen, wie man Sinkhole-Techniken einsetzt und wie man sich vor Denial-of-Service-Attacken schützt.

Was Sie vorher wissen/können sollten...

- Sie sollten ein Grundwissen über Denial-of-Service-Attacken besitzen;
- Sie sollten sich mit den Netzwerk-Verkehr-Belangen auf ISP-Seite auskennen.

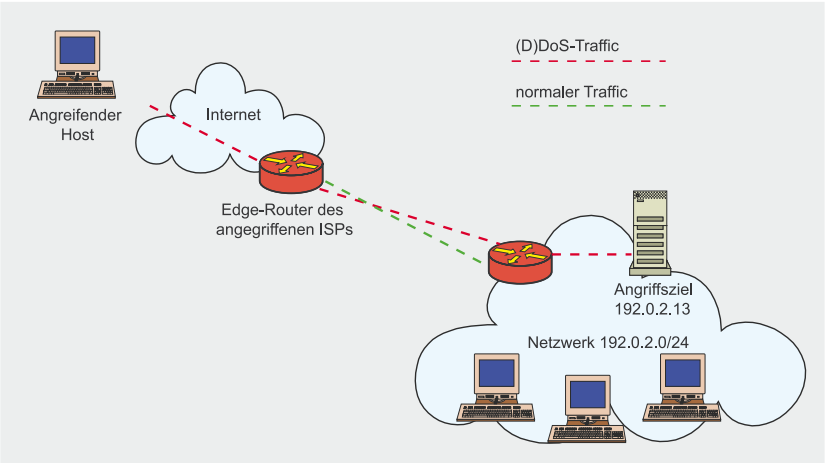

Abbildung 1. *Ein Angriff auf die IP-Addresse 192.0.2.13 (vor dem Sinkholing)*

Hintergrund und Funktion

In diesem Text könnte der Begriff Sinkhole allgemein als ein Mittel zum Umleiten spezifischen IP-Netzwerk-Verkehrs nach verschiedenen sicherheitsrelevanten Zwecken wie Analyse und Forensik, Ablenkung von Angriffen und das Erkennen von abnormalen Aktivitäten, definiert werden. Tier-1 ISPs habe diese Taktiken zuerst implementiert, meist um ihre Downstream-Kunden zu schützen. Seitdem wurde die Technik angepasst, um damit bedrohungsrelevante Informationen zur Sicherheitsanalyse zu sammeln. Wir wollen uns die einfachste Form eines Sinkholes einmal vorstellen. Wir nehmen folgendes an:

Bösartiger, zerstörender Traffic aus diversen Netzwerken zielt auf das Netzwerk 192.0.2.13; siehe Abbildung 1. Die Firma, die durch diesen Verkehr angegriffen wird, nutzt 192.0.2.0/24 als Netzwerk-Adressblock, welcher durch den Upstream-ISP geroutet wird. Der Angriff wird störend, unterbricht Geschäftsprozesse der Zielorganisation und erhöht womöglich die Kosten durch eine höhere Bandbreitennutzung. Dazu macht er eine Reaktion des ISPs nötig, da wegen des überdurchschnittlichen Verkehrswertes andere Kunden als Kollateralschaden betroffen sind.

Der ISP reagiert und initiiert temporär ein Sinkhole vom Typ Blackhole, mit dem sie eine spezifische Route für das Ziel (192.0.2.13/32) vorgeben, deren nächster Hop das Discard-Interface auf einem Edge-Router ist (auch als null0 oder *Bit-Bucket* bekannt); zu sehen in Abbildung 2.

Diese Strategie leitet den Verkehr in das Sinkhole des ISPs, anstatt es ihm zu gestatten downstream zum eigentlichen Ziel zu fließen. Der Nutzen besteht darin, dass anliegende ISP-Kunden nicht mehr von dem Verkehr betroffen sind – ein durchdachtes Sinkhole-Konzept des ISPs vorausgesetzt – und dass das Ziel des Angriffes seine Internetverbindung und den Zugriff auf das speziell angegriffene Ziel wieder erhalten hat. Leider kann die spezielle, angegriffene IP-Adresse, bzw. das dahinterliegende Gerät, nicht mehr mit anderen Systemen im Internet arbeiten, bis das Sinkhole wieder entfernt wird (sinnvollerweise nachdem der Angriff aufgehört hat). Natürlich hätte man auch die Services, die das Ziel zur Verfügung gestellt hat, auf eine andere Adresse migrieren können – hier hätte man allerdings viele andere Dinge beachten müssen, wie z.B. das Auslaufen der DNS TTL, usw.

Dieses Beispiel ist lediglich eine Art von Sinkhole, normalerweise bezeichnet als ISP-induzierte Blackhole-Route, die sie allerdings mit dem Konzept vertraut machen soll, damit wir weitere Einsatzmöglichkeiten von Sinkholes erklären können.

Netzwerk-Köder-Fallen durch Sinkholes

Eine eher neue Art, Sinkholes einzusetzen ist der Einsatz von Köder-Netzwerken, um Fallen einzubauen und für Aufdeckungs- und Datensammlungszwecke.

Zwei Typen von Köder-Netzwerken, die wir hier besprechen wollen, sind das Darknet und das Honeynet. Beide können genutzt werden, um Sicherheitsinformationen zu sammeln. Eines jedoch ist speziell im Bereich des sicheren Netzwerktechniken.

Darknets einbauen

Im Allgemeinen ist ein Darknet ein Teil gerouteter, zugeteilter IP-Raum, in dem keine wichtigen Services liegen. Diese Art von Netzwerken werden als *dark* bezeichnet, weil dort anscheinend nichts ist. Tatsächlich aber enthält das Darknet mindestens einen Server, der als Packet-Vakuum agiert. Dieser Server sammelt und organisiert

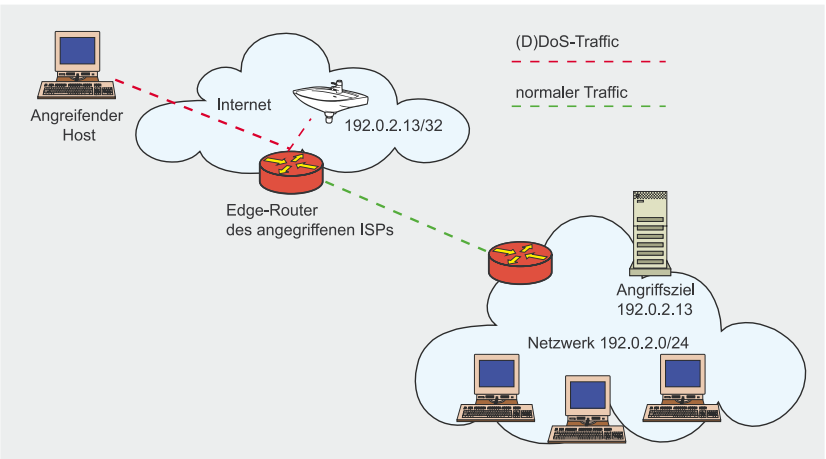

Abbildung 2. *Ein Angriff auf die IP-Adresse 192.0.2.13 (mit Sinkholing)*

Listing 1. *BGB Bespielkonfiguration*

```
router bgp XXX
redistribute static route-map static-to-bgp
# Route-map is a policy mechanism to
# allow modification of prefix attributes, or special
# filtering policies
route-map static-to-bgp permit 10
match tag 199
set ip next-hop 192.0.2.1
set local-preference 50
set community no-export
set origin igp
```

Listing 2. *Die Basiskonfiguration auf der ISP-Seite*

```
router bgp XXX
# Route-map is simply a policy mechanism
# to massage routing information such
# as setting the next hop
neighbor < customer-ip > route-map customer-in in
# prefix-list is a static list of customer prefixes and mask length that
# are allowed.  Customer should be allowed to
# announce down to a single host
# in their prefix(es) such as 172.16.0.1/32
neighbor < customer-ip > prefix-list 10 in
# ebgp-multihop is necessary to prevent
# continuous prefix announcement and
# withdrawal
neighbor < customer-ip > ebgp-multihop 2
# Now we define the route-map for policy match
# and setting the blackhole
# next hop
route-map in-customer permit 5
# the customer sets this community on their side,
# and the ISP matches on its
# side.  XXXX  would likely be the customer ASN,
# and NNNN is an arbitrary number agreed
# on by the ISP and the customer
match ip community XXXX:NNNN
set ip next-hop < blackhole-ip>
set community additive no-export
```

die Packete, die in das Darknet eintreten; nützlich für Echtzeit-Analyse oder Post-Event Netzwerk-Forensik.

Jedes Packet, dass das Darknet betritt, tut das unerwartet, denn kein legitimiertes Packet sollte je in einem Darknet auftauchen. Die Pakete, die also dort sind, sind entweder auf eine Fehlkonfiguration zurückzuführen, oder, das häufigere Szenario, sie wurden von Malware versendet. Diese Malware scannt nach verletzbaren Geräten und sendet dabei auch Packete in das Darknet, wobei sie sich dadurch preisgibt und nach einer genaueren Erforschung verlangt. Es ist eigentlich eine geniale Methode, um Würmer und andere sich verbreitende Malware zu finden. Ohne false-positives und ohne Signaturen oder komplizierte statistische Auswertungen kann der Sicherheitsadministrator mit einem sauber implementierten Darknet, Scanning (also Versuche von Malware, nebenliegende Hosts zu entdecken, die für eine Verbreitung geeignet sind) in jeder beliebigen Netzwerkgröße erkennen. Dieses ist ein machtvolles Security-Tool. Desweiteren zeigen Pakete im Darknet u.U. eine andauernde Fehlkonfiguration des Netzwerkes, von der der Netzwerk-Administrator gerne etwas erfahren möchte. Natürlich bieten Darknets noch viele weitere Anwendungsmöglichkeiten im Bereich der Sicherheit. Sie können genutzt werden, um Fließ-Kollektoren, Backscatter-Erkenner, Packet-Sniffer und Eindringerkennungs-Systeme zu hosten. Die Eleganz des Darknets kommt daher, dass es durch simple Verkehrsreduzierung die Benutzung von false-positives oft stattlich nach unten schraubt.

Die Implementierung eines Darknets ist relativ simpel. Hier sind fünf einfach Schritte:

Suchen Sie sich einen oder mehrere unbenutzte IP-Adressbereiche in Ihrem Netzwerk, die Sie in ihr Darknet routen möchten. Der Bereich könnte von einem /16-Bereich von Adressen, bis hin zu einer einzigen (/32) Adresse sein. Je höher die Anzahl der Adressen, desto genauer wird später die Erkennung von ungebetener Netzwerk-Aktivität. Ich empfehle, mehrere Adress-Segmente zu wählen, wie z.B. ein /29 aus jedem internen Netz und ein /25 von Ihrer externen Netzwerk-Belegung. Es gibt keinen Grund, warum man einen internen, privaten Adress-Bereich nicht zum Darknet machen könnte (wie bsp. RFC 1918 Bereich, 10.0.0.0/8). Tatsächlich können Sie durch das *Darkneten* von internen Regionen auch internes Scanning sehen, dass Sie möglicherweise verpassen würden, wenn Sie so nur externe (public) Netzwerk-Segmente behandeln. Eine andere Strategie, die bei Organisation eingesetzt werden könnte, die spezifische Routings für ihr internes Netzwerk haben, ist sich auf die Regel *Die spezifischste Route gewinnt* zu verlassen (meist durch ein internes Gateway-Protokoll verteilt). Soll heißen: Wenn ich die Netzwerke 10.1.1.0/24 und 10.2.1.0/24 intern benutze, dann kann ich mein komplettes 10.0.0.0/8-Netzwerk in mein Darknet routen. Ich weiß, dass mein Netzwerk gut konfiguriert ist und das Darknet jeden 10.0.0.0/8-Verkehr empfangen wird, bis auf den der zu den Netzwerken geht, die ich explizit benutze/route (diese haben meist statische Routeneinträge innerhalb meiner Netzwerk-Struktur).

Als nächstes werden Sie ihre physische Topologie konfigurieren. Sie benötigen einen Router oder (Layer-3) Switch, der den Verkehr in

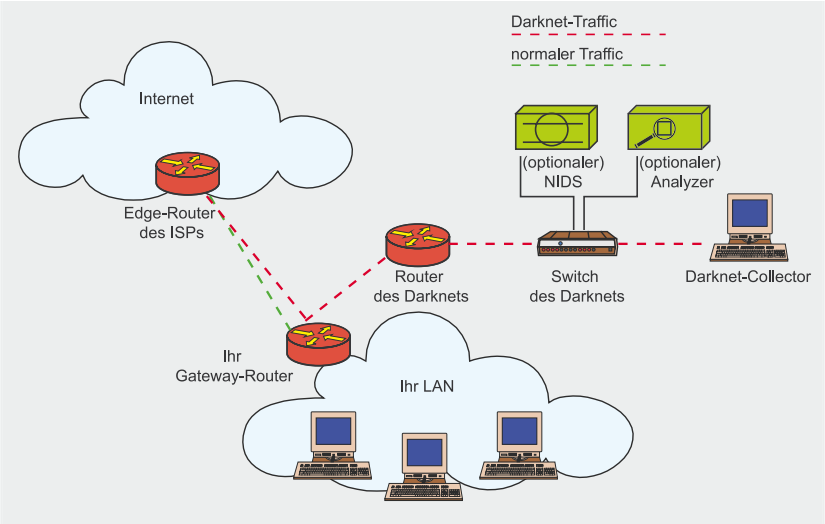

Abbildung 3. *Eine Referenz-Topologie für Darknets*

Ihr Darknet weiterleiten wird, einen Server mit genügend Speicher, der als Ihr Daten-Sammler agieren wird und einen Ethernet-Switch, der diese Komponenten und andere, die in Zukunft hinzukommen können (wie einen IDS-Sensor oder Protokoll-Analyzer), verbindet. Als Router können Sie ein existierendes, internes oder externes (oder beides, obwohl das nicht empfehlenswert ist) Gateway-Gerät verwenden – die meisten *Enterprise*-Darknets (im Gegensatz zu denen der Telecom-Carrier) sind im DMZ-Bereich der Oraginsation zu finden und vom Rest des Netzwerks getrennt. Deshalb könnten Sie überlegen, diese Job eine Firewall an Stelle eines Routers übernehmen zu lassen. Wir empfehlen, dass Sie für externe Darknets Ihren externen Gatway-Router nutzen, und für interne einen internen Layer-3-Switch. Egal für welchen Weg Sie sich auch entscheiden, wichtig ist, dass Sie das Routing-Gerät so konfigurieren, dass es den Traffic für das Darknet, den es von einem dedizierten Ethernet-Interface empfängt (durch den Switch), zum Sammler-Server senden, den Sie so einrichten müssen, dass er diese Pakete akzeptiert. Der Sammler-Server muss ebenfalls ein dediziertes Darknet-Interface besitzen, das diese Pakete empfängt. Für das Management braucht der Sammel-Server mindestens ein zusätzliches Ethernet-Interface (das auf einem separaten Management-LAN sitzen muss). Benutzen Sie ihre besten, eigenen Praktiken rund um die Netzwerkgerät-Sicherheut, denn Sie können sich sicher sein, dass bald alle Sorten von Verrückten durch dieses Netzwerk-Segment fließen werden. Kämpfen Sie gegen den Drang an, auf die Schnelle einen existierenden DMZ-Switch zu nutzen, um diese Komponenten zu verbinden, so lange sie kein korrekt eingerichtetes VLAN haben, dass keine Broadcast-Pakete ins Darknet lässt – erinnern Sie sich; das Darknet ist nur für unlegitimierten Verkehr gedacht – deshalb wollen wir hier keine legitimen Broadcast-Pakete aus den anderen LANs. Abbildung 3 zeigt ein Beispiel für diese Konfiguration. In unseren Beispielen verwenden wir einen Router oder Switch, der unter Cisco IOS mit einer Layer-3 Software-Lizenz läuft, einen FreeBSD-basierten Server und einen herkömmlichen, unmanaged Layer-2-Switch, um die Geräte zu verbinden.

Damit unser Sammel-Server nicht ARP (adress resolution protocol) für jede Adresse im Darknet-Bereich anwenden muss, werden wir den Router so konfigurieren, dass er jeglichen Verkehr für das Darknet auf einen einzelnen Endpunkt, nämlich das Darknet-Ethernet-Interface des Servers, leiten soll. Um das zu erreichen, ist unser Vorschlag, ein dediziertes /30-Netzwerk zwischen Router und Darknet-Interface einzurichten, wie bsp. 192.0.2.0/30. Das würde bedeuten, dass das Ethernet-Interface des Routers 192.0.2.1/30 bekäme und der Server könnte unter 192.0.2.2/30 erreicht werden. Die Interface-Konfiguration hängt stark von der im Einzelnen verwendeten Plattform ab, deshalb gehen wir davon aus, dass Sie selbst wissen, wie es bei Ihrer funktioniert. In unseren Beispielen verwenden wir einen Cisco IOS mit einer Layer-3 Software-Lizenz. Wenn das getan ist, geben Sie einfach die passenden Routing-Einträge in den Switch, um jeden Darknet-Verkehr nach 192,0,2,2 auf dem Sammel-Server zu routen:

```
router#conf t
router(config)# ip route 10.0.0.0 ←
255.0.0.0 192.0.2.2
router(config)# ^Z
router# wr
```

Jetzt sollten Sie Darknet-traffic erhalten. Ein Beispiel für eine logische Topologie ist in Abbildung 4 zu sehen.

Was mit dem Verkehr anzustellen ist, wenn er erst mal dort ist, ist eine ganz andere Geschichte. Der Server sollte so konfiguriert werden, dass er auf keine Daten antwortet, die er auf seinem Darknet-Interface empfängt. Natürlich wird er ARP für seine konfigurierte Adresse (nur 192.0.2.2/30) benutzen, um Kommunikation mit dem Router herzustellen; alle anderen Pakete sollten aber von einer Host-basierten Firewall verworfen werden. Wie bereits vorher erwähnt, sollte auf dem Darknet Interface kein Management stattfinden – dafür müssen Sie ein anderes Ethernet-Interface konfigurieren. Die Standard-Route für das System sollte das Gateway des Management-Interfaces sein. Betreffs der Firewall, wird die Wahl der Plattform des Servers, die der Firewall vorgeben; wir empfehlen aber ein BSD-basiertes System, sowie pf oder ipfw2 als Firewall zu nutzen. Ob Firewall-Logging aktiviert sein sollte oder nicht, hängt stark davon ab, was Sie damit machen möchten. Wir benutzen Logfile-Analyse-Tools, die ein aktiviertes Logging benötigen (damit die Logs geparsed und Alarme generiert werden können); allerdings, abhängig von diversen Hard- und Softwares, sowie der Größe Ihres Darknets,

Listing 3. *Die Kunden-Basiskonfiguration*

```
router bgp XXXX (customer's ASN)
# the customer will install a static route,
# which is redistributed into BGP
# hereredistribute static route-map static-to-bgp
# just like the ISP, use a route-map to set
# and match specific prefix
# attributes
route-map static-to-bgp permit 5
# match the arbitrary tag,
# agreed on by the customer and the ISP
match tag NNNN
set community additive XXX:NNNN
# NNNN is the tag, agreed on by the customer and the ISP
ip route 192.168.0.1 255.255.255.255 Null0 tag NNNN
```

kann Logging zu massiven Verlusten in der Darknet-Performance führen. Als zusätzliche Sicherheitsmaßnahme (Firewalls können abstürzen oder versehentlich ausgeschaltet werden), sollte der Darknet-Verkehr Null-geroutet werden, falls er ungefiltert bleibt. Ein Null-Route-Beispiel unter FreeBSD würde so aussehen:

```
route add -net 10.0.0.0/8 ←
127.0.0.1 -blackhole
```

Nun, da Ihr Darknet brummt und Ihr Sammel-Server geschützt ist, müssen Sie die Daten in ein Format setzen, dass nützlich für Analyse- und Forensik-Tools ist. Die offensichtlich am besten geeignete Wahl wären wohl pcap-formatiere Binärdateien, da sie praktisch allgegenwärtig sind und die meisten Netzwerk-Analyse-Tools mit ihnen arbeiten können. Der einfachste Weg, dies auf einer anhaltenden Basis zu erreichen, ist, das voreingebaute Rotation-Feature von tcpdump zu nutzen. Das Programm tcpdump wird von einer Netzwerk-Forschungs-Gruppe des Lawrence Berkeley National Laboratory zur Verfügung gestellt. Ein Beispiel-Eingabe, um mit tcpdump diese Log-Rotation zu erreichen, ist:

```
tcpdump -i en0 -n -w darknet_dump -C125
```

In diesem Beispiel wird tcpdump angewiesen auf dem Interface en0 zu horchen; Nummer-zu-Name (DNS) ist dabei deaktiviert und es wird alle 125 Millionen Bytes eine Datei namens *darknet_dumpN* angelegt, wobei *N* genutzt wird, um den Dateinamen einzigartig zu machen. Dies wird uns eine pcap-formatierte Binärdatei ausgeben, die den Netzwerk-Verkehr enthält. Diese Datei könnten Sie dann in Ihrem favorisierten Netzwerk-Analyse-Programm ausgeben lassen. Die Idee dahinter ist, eine Kopie der Daten zu behalten und sie mit einer Fülle an Programmen zu bearbeiten, um nach interessanten Merkmalen des Verkehrs zu suchen. In einem normalen Szenario, werden Sie ein Programm wie tcpdump mit einem spezifischen BPF (Berkeley packet filter)-Ausdruck benutzen, um nach Dingen in diesen Dateien zu suchen. Da dies nicht während der Laufzeit (Aufnahmezeit) getan werden kann, können wir verschiedene Tools benutzen, um uns später und ohne Risiko etwas zu verlieren, eine Aufnahme des kompletten Verkehrs anzuschauen.

Ein weiteres, hilfreiches Tool, dass es uns einfach macht, den Fluss des Verkehrs zu visualisieren ist Argus, das Audit Record Generation and Utilisation System entwickelt von QoSient. Obwohl die Konfiguration zu umfangreich ist, um sie hier im Detail zu beschreiben, nutzen wir Argus regelmäßig, um nach interessanten Flüssen in unseren Darknets zu suchen. Argus bietet die Möglichkeit eines flussbasierten Interface zur Zusammenfassung, dass helfen soll exakt zu verstehen, was bei den bösartigen Verkehrsflüssen vor sich geht.

Um die Größe des Verkehrs zu messen, der in das Darknet eintritt, könnten Tools wie MRTG (*http://www.mrtg.org/*) von Tobias Oetiker helfen. MRTG kann dabei helfen, wunderschöne Graphen aus Ihrem nicht-ganz-so-wundervollen Netzwerkverkehr zu erzeugen. Es gibt außerdem dutzende von Programmen, die Firewall-Logs parsen und eine schnelle und einfache Alternative zu den eher komplizierten pcap-basierten Analyse-Tools oder Argus sein können. Behalten Sie die Performance-Probleme im Kopf, die Sie mit textbasiertem Logging des Packetfilters und dem nachträglichen Parsen dieser Dateien haben.

Es gibt buchstäblich Dutzende von Tools, die in Ihren Darknet ver-

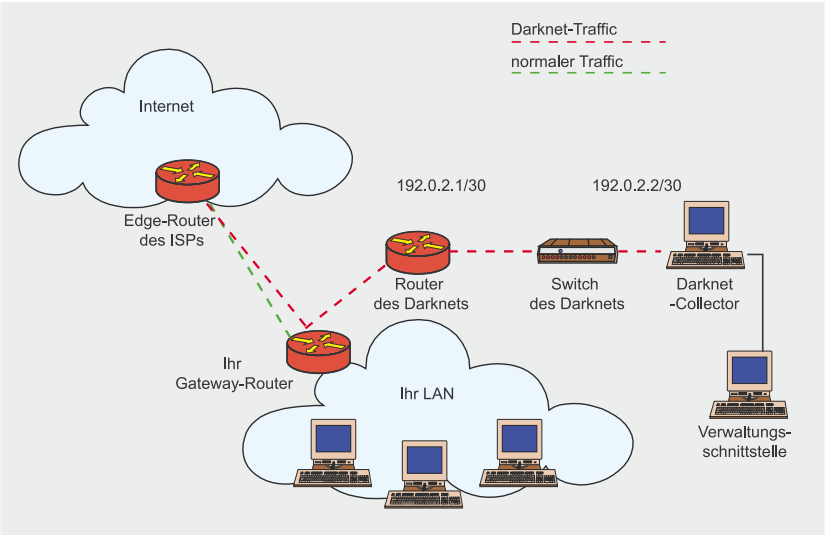

Abbildung 4. *Eine logische Topologie für Darknets*

wendet werden können. Um Sie an den Start zu bringen, hier ein paar, die Sie auch in unseren Netzen finden würden:

- Einen IDS-Sensor (Bro, Snort, et al.);
- Einen Paket-Sniffer (tcpdump wie vorher beschrieben);
- Einen Fluss-Analyzer (argus, netflow export from router, SiLK, flow-tools);
- Einen Firewall-Logfile-Parser, der RRD-Datenbanken für Graphen ausgibt;
- MRTG um Verkehrsmessungen grafisch aufzubereiten;
- p0f (von Michal Zalewski) um Plattformen von infizierten/scannenden Geräten zu kategorisieren.

Honeynets einbauen

Wie ein Darknet, ist ein Honeynet ein Teil gerouteter IP-Bereich. Statt aber eine Stelle vorzugeben, zu der Pakete geschickt werden, um zu sterben, gaukelt diese Stelle einen oder mehrere Services vor, während sie die Verbindung zulässt (Handshake) und einen kompletten Zwei-Wege-Dialog herstellt. Ein *Honeypot*, das System, das den Service vortäuscht, soll eine festgestellte und konstant gemonitorte Ressource sein, die Angreifer auffordern soll, sie zu untersuchen und/oder zu infiltrieren. Obwohl es ein paar verschiedene Arten von Honeypots gibt, haben Sie alle dasselbe Ziel: Die Taktiken zu lernen und so viele Information wie irgend möglich über den Angreifer zu sammeln.

Physikalische Honeypots

Physikalische Honeypots sind komplette Maschinen im Honeynet, mit eigenen IP-Adressen, Betriebssystemen und Service-vortäuschenden Tools.

Virtuelle Honeypots

Virtuelle Honeypots sind *Software-simulierte* komplette Honeypot-Systeme im Honeynet, die bestimmte Vorgaben, wie Betriebssystem, Netzwerk-Stack und Services simuliert, um als Köder zu fungieren. Ein einziger physikalischer Server könnte ein Netzwerk von tausenden von virtuellen Honeypots herstellen.

Low-Interaction Honeypots

Low-interaction honeypots (der gängigste Typ von Honeypots) sind ausgelegt, um einen Angreifer mit einer oder mehreren offensichtlich ausnutzbaren Schachstellen zu locken, Dialog herzustellen und die ersten Pakete der Kommunikation mit dem Angreifer zu fangen. Logischerweise wird der Angreifer oder die automatische Malware wohl erkennen, dass das Ziel nicht ausgenutzt werden kann. Bevor das geschieht, können aber wichtige Daten, wie die Taktik oder die Signatur der bösartigen Software ausgemacht werden. Solche low-interaction Honeypots werden heutzutage genutzt, um Spammer-Taktiken auszukundschaften (über den Versuch, Methoden herauszufinden, wie bsp. die Timing-Charakteristiken von SMTP-Transaktionen der Spammer).

Es gibt im Allgemeinen nur wenige kommerzielle Implementierungen von Honeynet-Technologie – die bekannteste ist das Open-Source-Projekt honeyd von Niels Provos. Weiterführende Informationen über das Setup von honeyd kann auf *http://www.honeyd.org* gefunden werden.

Tipp: honeyd ist als virtueller/s Honeypot/Honeynet ausgelegt, dass eine Anzahl verschiedener Betriebssysteme und Softwarekomponenten simulieren kann, um Angreifer anzulocken.

Eine weitere Form von low-interaction Honeypots, die erwähnenswert ist, ist ein neues Konzept von Tom Liston namens LaBrea. LaBrea (benannt nach der Teergrube) ist ein Software-Daemon (Service), der automatische Antworten auf Verbindungsanfragen in enormen IP-Adressbereichen generieren kann. Kurz gesagt kreiert es eine Umgebung, die interessant für Malware-Scans und -Verbreitung ist. Aber es hat einen verrückten Trick. Sobald die Malware versucht zu verbinden, verlangsamt LaBrea die Geschwindigkeit des Netzwerk-Stacks des Senders, oft signifikant. Es gibt also keine Interaktion auf der Applikationseben, aber viel davon auf Layer 4, wenn die (TCP) Verbindungs-Handshakes stattfinden. LaBrea beherrscht sogar ARP für alle virtellen IP-Adressen in seiner Konfiguration, was das Setup unglaublich einfach macht. Weitere Informationen über LaBrea auf: *http://labrea.sourceforge.net/labrea-info.html*.

Einige Forschungen haben ergeben, dass low-interaction Honeypots eine brauchbare Taktik

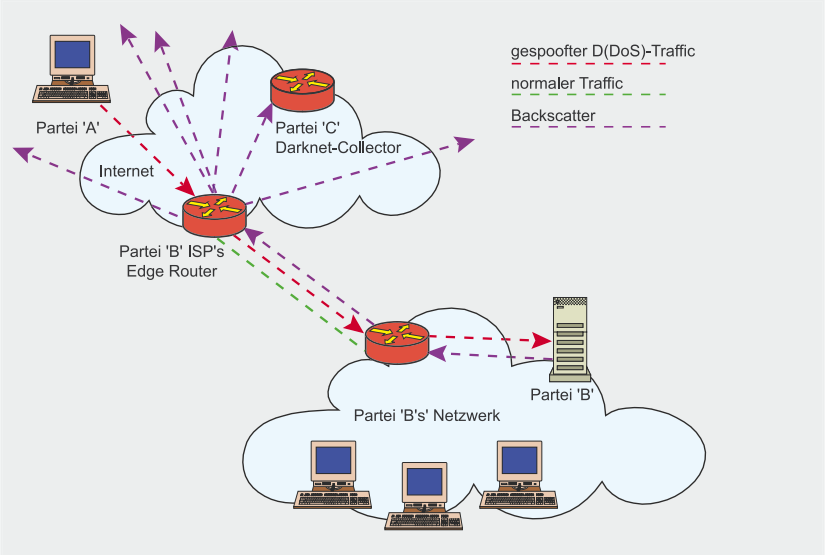

Abbildung 5. *Ein Beispiel für backscatter während eines DDoS-Angriffes*

gegen hochperformante Würmer ist, indem sie sie langsamer macht, um die Netzwerk-Infrastruktur zu schützen. Wir meinen, dass die Konfiguration, die nötig ist, um dieses zu realisieren sehr schwierig ist. Dennoch können LaBrea und honeyd konfiguriert werden, um so eine Wurm-unfreundliche Umgebung zu erzeugen.

High-Interaction Honeypots

High-interaction Honeypots werden eher selten genutzt, sind aber äußerst wertvoll. Statt nur die ersten Transaktionen eines Dialogs zwischen Angreifer und Honeypot aufzuzeichnen, lässt ein high-interaction Honeypot den Angriff das System komplett infiltrieren, auf dem es sitzt. In diesem Szenario kann man also nicht nur nützliche Informationen über Probing und die Explotation sammeln, sondern es erlaubt den Sicherheits-Administrator auch, den Angreifer zu beobachten, wenn er erst einmal in das System eingedrungen ist. Dabei deckt er unwissentlich selbst alle seine Tools und seine Intention auf.

Es gibt eine non-profit Organisation The Honeynet Project (*http://www.honeynet.org/*), die ein Programm herausgibt, um Usern die Möglichkeit zu geben, selbst high-interaction Honeypots einzusetzen. Sie stellen auch exzellente Forensik-Tools zu Verfügung, um die während der Infiltration gesammelten Daten auszuwerten.

Tipp: The Honeynet Project (*http://www.honeynet.org/*) verbreitet eine Reihe fantastischer Tools, um eigene Honeynets aufzubauen. Wir empfehlen Ihnen, Honeywall, Termlog und Sebek tools Ihre Aufmerksamkeit zu schenken. Außerdem hat das Projekt-Team ein Buch entwickelt, dass sich mit der Psychologie, den Taktiken und Tools der Angreifer beschäftigt. Das Buch, *Know Your Enemy,* aktuell in der zweiten Auflage, ist über honeynet.org erhältlich. Einkünfte durch den Verkauf werden zur Honeynet-Forschung eingesetzt.

Empfehlungen für den Gebrauch von Honeynets

Für Forschungsunternehmen, oder solche mit viel Geld und Zeit zum Wegwerfen (kennen Sie so eins?) können Honeybots von unschätzbarem Wert sein; die Nutzung für den alltäglichen Gebrauch im Unternehmen können wir aber nicht empfehlen. Natürlich kann, wenn ein harmloses Stück bösartiger Software seinen Kopf zeigt und kein Sniffer oder Forensik-Tools eine Lösung bringen, kann ein Honeynet implementiert werden, dass eine Kommunikation herstellen kann, indem es sich als einfaches Ziel darstellt und dabei genügend Informationen sammelt, um den Angreifer zu identifizieren. Ein weiterer Anwendungsbereich wäre einen Verdacht auf eine Infiltration zu verifizieren. Es sollte also ein weiterer Pfeil im Köcher des Sicherheits-Administrators sein.

Eine Implementierung, die es wert ist, erwähnt zu werden, wird bei einem der weltgrößten Chiphersteller verwendet. Diese haben, im ganzen Netzwerk verteilt, Linux-Server, die VMWare laufen lassen, die jeweils vier Maschinen erzeigen, eine für jede benutzte Windows-Version, die im Unternehmen genutzt wird – NT, 2000, 2003 und XP. Jede davon wird mit den normalen Patches auf dem neuesten Stand gehalten. Das Linux OS überwacht den Verkehr und Änderungen, um neue Würmer oder andere Bedrohungen auszumachen, die im Unternehmensnetz zirkulieren. Sie nutzen diese Umgebung in der Kombination Honeynet und IDS für Würmer. Weitere Details über diese Implementierung auf *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*

Implementierung von Sinkholes als Verteidigung gegen DDoS-Angiffe (Blackhole Routing)

Eine weitere neuartige Nutzung von Sinkhole-Technologie ist die der Verwendung zur Verteigung gegen (distributed) Denial-of-Service-Angriffe. Im Abschnitt *Hintergrund und Funktion* in diesem Artikel, haben wir bereits ein erstes simples Beispiel für die Backhole-Routing-Technik bekommen. Sobald das exakte Ziel des Angriffes identifiziert war, wurde die IP auf das Discard-Interface am Rand des Netzwerken umgelenkt. Das schützte das Netzwerk vor der totalen Stilllegung durch Link-Überausnutzung, wirkte sich aber immer noch auf die netzweite Performance aus, besonders auf angrenzende Kunden, die einige Teile der Topologie mit dem angegriffenen Netzwerk teilten. Heutzutage haben Telecom-Carrier ihre Netzwerk danach aufgebaut und verfeinerte Versionen dieser Verteidigungsmaßnahme in die komplette Netzwerk-Designphilosophie eingebaut. In vielen Fällen sind die Carrier nun in der Lage Traceback-Techniken anzuwenden, um die Eintrittspunkte des Angriffs zu lokalisieren und dort die bösartigen Pakete mit Blackhole abzufangen (Am Eintrittspunkt selbst), statt es ihnen zu erlauben den kompletten Downstream-Weg vom Backbone, bis zum Zielnetzwerk-Link zu verstopfen. Diese Traceback-Technik ist häufig unötig, da die Blackhole-Routen der Carrier situationsabhängig über Edge-Router durch das ganz Netzwerk gegeben werden, indem eine BGP-Community verwendet wird. Dadurch wird der bösartige Verkehr an jedem Eintrittspunkt in dem Moment, in dem er auftritt, mit Blackholes umgeleitet und in vielen Fällen kann dadurch ein Stau an Backbone und Edges vermieden werden. Einige haben Kontrolle und Automatisierung darüber sogar bis auf den Endkunden ausgeweitet, was als Kunden-gesteuerte Echtzeit-Blackholes bekannt ist.

Ausgelöstes Blackhole-Routing

Wie vorher erwähnt, haben viele ISPs ein verteiltes, automatisiertes System implementiert, um Blackhole-Routing auf IP-Adressen *auslösen* zu lassen. Der Auslöser kann vom ISP oder von Kunden gestellt werden, egal ob manuell oder automatisch. Ausgelöstes Blackhole-

Routing nutzt das sinple Sinkhole, wie eingehend im Abschnit *Hindergrund und Funktion* beschrieben. Das Sinkhole könnte auf allen Eintritts-(Edge-)Routern im ISP-Netzwerk konfiguriert werden, auf denen er mit anderen Providern oder Kunden Verkehr austauscht. Wenn ein Angriff auf ein Netzwerk-Ziel indentifiziert wurde, kann ISP oder Kunde den *attacked*-Präfix (oder einen genaueren) in die BGP-Routing-Tebelle eintragen. Der Präfix ist mit einem Next-Hop versehen, der statisch zum Discard-Interface routet und im ISP-Netzwerk über das interne BGP (iBGP) verteilt wird. Dann, sobald Pakete das Ziel mit dem *attacked*-Präfix haben, werden sie sofort zum Discard-Interface gesendet und zwar auf den Router, der am nächsten am Paket sitzt.

Die folgenden Schitte sind für den ISP nötig, um den verteilten Blackhole-Mechanismus zu implementieren:

- suchen Sie sich einen nicht-global gerouteten Präfix aus, wie Test-Net (RFC 3330) 192.0.2.0/24, der als nächster Hop genutzt wird, wenn etwas geblackholed werden muss. Ein Präfix mit einer Länge von 24 ermöglicht es viele verschiedene IP-Adressen für verschiedene Arten von Blackhole-Routing zu verwenden. Sie könnten z.B. zwischen Kunden-, internen und externen Blackhole-Routes unterscheiden wollen;
- konfigurieren Sie eine statische Route auf jedem Eintrittsrouter für 192.0.2.0/24, die auf das Discard-Interface zeigt. Z. B. `ip route 192.0.2.0 255.255.255.0 Null0`;
- konfigurieren Sie BGP und Policy Routee-Maps, um ein mit Blackhole zu behandelndes Präfix mitzuteilen, wie in Listing 1 zu sehen.

In der Beispielkonfiguration verteilen wir statische Routen ins BGP, die *tag 199* entsprechen, setzen den nächsten Hop auf eine IP-Adresse, die auf das Discard-Interface geroutet ist, setzen den lokalen Vorrang auf 50 (weniger vorrangig) und gehen sicher, dass diese Routen nicht auf einen externen peer laufen (no-export).

Tabelle 1. *ICMP-Pakete*

ICMP-Pakete	Beschreibung
3.0	Network unreachable
3.1	Host unreachable
3.3	Port unreachable
3.4	Fragmentation required
3.5	Source route failed
3.6	Destination network unknown error
3.7	Destination host unknown error
3.10	Host administratively prohibited
3.11	Type of service network unreachable
3.12	Type of service host unreachable
3.13	Communication administratively prohibited
11.0	TTL expired during transit
11.1	Fragment reassembly timeout

TCP-Pakete	Beschreibung
RST bit set	TCP Reset

Wenn diese Basiskonfiguration einmal vorgenommen wurde, kann der Auslöser vom ISP aktiviert werden, indem er eine statische Route für das angegriffene Präfix (oder den Host), der geblackholed werden soll. Z.B.:

```
ip route 172.16.0.1 255.255.255.255
192.0.2.1 Null0 tag 199
```

Die statische Route hier ist der Abzug, der den Blackhole-Routing-Prozess aktiviert. Der Router, auf dem diese Route konfiguriert ist, wird die Route über iBGP an alle internen Router, auch Edge-Router, weiterleiten. Jeder Router mit einer statischen Route zum Discard-Interface für 172.16.0.1/32 wird solchen Verkehr sofort lokal Blackholen.

Der ISP könnte auch einen automatischen Auslöser über BGP aufsetzen wollen, so dass ein BGP-Kunde auch ohne Eingriff des ISP eine Blackhole-Route auslösen könnte. Das ist der machtvollste Aspekt des ausgelösten Blackhole-Routings. Die Konfiguration auf ISP-Seite ist nur leicht unterschiedlich, und zwar darin, dass Community- und ebgp-multihop benutzt werden, um die Routen der Kunden, sauber erhalten und umgesetzt werden. Die Basiskonfiguration der ISP-Seite sieht aus wie in Listing 2 beschrieben.

Der ISP hat schon die < *blackhole-ip* > statisch zu den Discard-Interfaces im Netzwerk geroutet, so dass, sobald der Kunde einen Präfix durchgibt, der mit Blackholes behandelt werden soll, der ISP diese Route intern wiederverteilt und jeglicher Verkehr zu diesem Präfix am Rand des ISP-Netzwerks geblackholed wird.

Die Basiskonfiguration für den Kunden sieht man auf Listing 3.

Wenn die PBG-Konfiguration erst einmal steht, muss der Kunde nur eine statische Route für das Präfix # eingeben, das angegriffen wird. Mit einer sehr einfachen BGO-Konfiguration und ein wenig Hilfe von Ihrem ISP, haben Sie nun eine sehr schnelle Methode um auf Denial-of-Service-Angriffe gegen einen einzelnen Host, oder ein Präfix zu reagieren.

Anmerkung: Stellen Sie sicher, dass Sie sich mit dem technischen Kontakt Ihres ISP besprechen, bevor Sie eine solche Lösung implementieren, da die Lösungen auf der ISP leicht unterschiedlich sein können.

Tabelle 2. *Zusammenfassende Checkliste*

Schritt	Beschreibung
Untersuchen Sie, wie Ihnen Ihr ISP während eine DDoS-Attacke helfen kann.	Erstellen Sie einen Plan, mit DDoS-Angriffen umzugehen, der die Möglichkeiten Ihres ISPs im Echtzeit-Blackholing mit einbezieht. Ein offener Dialog zwischen Ihrem Unternehmen und Ihrem ISP über die Aktivierung von kunden-ausgelösten Echtzeit-Blackholes, damit Sie sich ohne Zeitverlust selbst schützen können.
Überlegen Sie sich ein eigenes, internes Darknet zu implementieren.	Erinnern Sie sich; ein internes Darknet gibt Ihnen die Möglichkeit, Würmer früher als Ihr Anti-Virus-Vendor zu fangen. Gleichermaßen deckt es Netzwerk-Fehlkonfigurationen auf, über deren Entdeckung Sie froh sein werden.
Überlegen Sie sich ein eigenes, externes Darknet zu implementieren.	Externe Darknets geben Ihnen einen Einsicht, was Ihr Netzwerk von außen trifft und die Tools, die Sie dabei benutzen, sind besser für die Augen als ein standard Firewall-Log. Der Backscatter, der in einem externen Darknet gesammelt wird, gibt Ihnen Kenntnisse darüber, ob Ihr Netzwerk in einen Angriff auf eine dritte Partei einbezogen wird.
Nutzen Sie Honeypots zur Forschung, wenn Sie die Zeit und das Geld haben.	Obwohl die meisten Unternehmen wohl keinen nennenswerten Nutzen in der Implementierung von Honeynets sehen werden, sind sie für Forscher der informationssicherheit unbezahlbar. Überlegen Sie sich, ein Honeynet in Ihr Unternehmen zu integrieren. Solche Überlegungen sollten eine Überprüfung der Landesgesetze einbeschließen, da diese die Entscheidnung stark beeinflussen können.

Backscatter und Tracebacks

In diesem Abschnitt werden wir die kreativen Benutzungen von Köder-Netzwerken erforschen, und wie man mit ihnen Angriffe entdeckt, Spoofing durchführt und den Schurken sogar jagt.

Backscatter

Nach all der Diskussion um Köder-Netzwerke DDoS-Angriffe scheint es passend, die Idee von Backscatter zu erwähnen. Während meines ersten Sementers am College, schrieb ich Briefe (ja, die mit Papier) an diverse Freunde, die viel durch die Gegend fuhren. Zerstreut, wie ich bin, habe ich beständig die falsche Rücksender-Adresse auf die Umschläge geschrieben. Ich hatte vergessen, meine Zimmernummer aufzuschreiben, oder sie war komplett unleserlich (damals hatte ich das Bier entdeckt). Gelegentlich kam es vor, dass einer meiner Freunde, an die ich schrieb, umgezogen ist und der von mir versandte Brief wurde am Postamt zurück geschickt, mit der Aufschrift *Zurück zum Absender.* Da aber die Absenderadresse nicht korrekt geschrieben war, ging der Brief nicht an mich zurück, sondern zum Bewohnerbüro, welches mich anrief und mich wissen lies (sie kannten ja meinen Namen), dass ich wieder einmal die Absenderadresse falsch geschrieben hatte und dass da ein Brief läge, denn ich nochmal senden müsste. Dieser *Zurück zum Absender* Rücklauf ist eine Form von Backscatter. Der Backscatter gab dem Bewohnerbüro die Information, dass ich einen Brief geschrieben hatte (und an wen er gehen sollte).

Wenn im Internet Partei A vorhat, einen Denial-of-Service-Angriff gegen Partei B durchzuführen, Party A aber seine Identität verschleiern möchte, versieht er die Pakete normalerweise mit einer falschen Quell-Adresse (die IP-Header sehen dann so aus, als ob sie von Parte A-Z kommen würden; beispielsweise ist nur A-Z in IPv4 2^{32} Permutationen). Während solcher Angriffe senden Router und andere Netzwerkgeräte im Weg unvermeidlich eine Reihe und Nachrichten zurück, die von Verbindungs-Resets, über Quench-Request, bis hin zu Unreachable-Notifications. Da diese Nachrichten *Zurück zum Absender* gehen, und da der Sender gefälscht ist, werden die Parteien A-Z diese Nachrichten erhalten und so Kenntnis vom Angriff gegen Partei B bekommen. Genau, wie das Bewohnerbüro wusste, dass ich einen Brief gesendet habe. Das ist in Abbildung 5 dargestellt.

In der heutigen Packetfilterung werden die meisten dieser Meldungen still von unseren Firewalls verworfen, weil sie als Antworten zu Nachrichten angesehen werden, die wir nie gesendet haben. Mit einem implementierten, externen Darknet aber, so wie wir es vorher erklärt haben, können wir nach diesen Backscatter-Paketen schauen und herausfinden, wenn unser Adressbereich in einen Angriff auf eine bestimmte Partei hereingezogen wird. Die folgenden Typen von Paketen,

Im Internet

- Extreme Exploits: Advanced Defenses against Hardcore Hacks, herausgegeben von McGraw-Hill/Osborne Copyright 2005 *http://www.amazon.com/gp/product/0072259558/*
- Internet RFCs 3330 (Special-use IPv4 Addresses) und 3882 (Configuring BGP to Block Denial of Service Attacks)
- The Team Cymru Darknet Project *http://www.cymru.com/Darknet/*
- Die Homepage von tcpdump and libpcap *http://www.tcpdump.org/*
- Die Homepage von ARGUS *http://www.qosient.com/argus/flow.htm*
- Die Homepage von Honeyd *http://www.honeyd.org*
- Die Homepage des HoneyNet Projekts *http://www.honeynet.org*
- Die Homepage von des pdf Tools *http://lcamtuf.coredump.cx/pdf.shtml*
- Chris Morrow und Brian Gemberlings Artikel über ISP-Blackholing und Backscatter-Anallyse *http://www.secsup.org/Tracking/*
- Dan Hawrylkiws Präsentation über Honeynets *http://phoenixinfragard.net/meetings/past/200407hawrylkiw.pdf*
- Ein FAQ über den OpenBSD Packetfilter *http://www.openbsd.org/faq/pf/*

Über den Autor

Victor Oppleman ist ausgebildeter Autor, Referent und Lehrer auf dem Feld der Netzwerk-Sicherheit und Consultant für einige der meistbewunderten Unternehmen der Welt. Opplemans Open-Source-Software ist auf hunderttausenden Computern weltweit zu finden und er hält Patente am geisitges Eigentum über verteilte, anpassungsfähige Routing- und Wireless-Kunden-Applikationen. Der meiste Inhalt dieses Artikels wurde Opplemans Buch, *Extreme Exploits: Advanced Defenses Against Hardcore Hacks*, herausgegeben von McGraw-Hill/Osborne (Copyright 2005) entnommen und ist bei Ihrem Fachbuchhändler erhältlich.

können, wenn sie in einem Darknet auftreten, als Backscatter klassifiziert werden und sagen aus, dass unser (Darknet-) Adressbereich in einen Angriff hineingezogen wird.

Traceback

Da wir nun einen Hebel an Backscatter haben, wie können wir es benutzen?In einem Netzwerk mit mehreren Internet-Transit-Gateways, kann es, während einer lähmenden Attacke, nützlich sein, den Eintrittspunkt der *bösen Pakete* zu lokalosieren. Diese Technik, genannt *Traceback*, kann uns helfen. Denn wenn wir den Eintrittspunkt in unserem (oder im ISP-)Netzwerk erst gefunden haben, können wir dafür sorgen unseren Verkehr dort nicht mehr laufen zu lassen, um unsere Links zu entlasten und potentiell *guten* Verkehr fließen zu lassen (über alternative Gateways), nicht so wie in der simpleren DdoS-Blackhole-Taktik, welche wir vorher besprochen haben. Traceback erlaubt es uns, den Backscatter, den wir in unseren Darknets sammeln zu nutzen, um den Punkt zu finden, an dem der Angriff das Netzwerk betritt. Unglücklicherweise ist das wirklich nur für ISPs richtig oder für weitreichende Datennetze mit vielen Internet-Gateways. Einige Anlehnungen an diese Beschreibung schließen den Nutzen von Blackhole-Verteidigung an *jedem* Internet-Gateway ein. Da das große ISPs und einige große Firmennetzwerke machen, scheint es angebracht, den Prozess wenigstens zu erklären.

Ausgehend von der Annahme, dass Sie Ihr Netzwerk wie oben beschrieben konfiguriert haben, können Sie einen Traceback mitten im Denial-of-Service-Angriff in drei einfachen Schritten ausführen:

- identifizieren Sie das Ziel und vergewissern Sie sich, dass der Angriffs-Verkehr gespoofed wird (falls er es nicht ist, wird die Traceback-Taktik keine Früchte tragen);
- blackholen Sie die Route für die spezifischen Hosts (voraussichtlich /32), die angegriffen werden an jedem Ihrer Gateways. Diese Blackhole-Anwendung wird den Gateway-Router dazu bringen ICMP-Unreachable Messages zu generieren, die zu den gespooften Quellen der Angriffspakete zurückgesendet werden;
- in Ihren Darknets benutzen Sie die Darknet-Tools, die Sie haben um nach dem Backscatter-Verkehr zu schauen (wahrscheinlich in der Form von ICMP-Unreachables) mit der IP Ihres Gateway-Routers darin. Wenn Sie die Adresse eines Ihrer Gateways als Quelladresse dieser Backscatter-Pakete sehen, zeigt Ihnen das, dass dieses Gateway aktuell der Eintrittspunkt für den Angriffs-Verkehr ist. *Voilá*, Sie haben herausgefunden, wo der Angriff das Netzwerk betritt. Wenn Sie keine hochentwickelten Darknet-Tools eingerichtet haben, kann Ihnen eine kleine Zugriffsliste am Router-Interface ihres Darknets die Arbeit für Sie machen:

```
access-list 105 permit icmp any any unreachables log; access-list 105 permit ip any any
```

Wenn sie dann den Terminal-Monitoring-Mode an dieser Zugriffsliste benutzen (oder einfach im Log nachlesen), bekommen Sie einen Backscatter-Report für den armen Mann, in dem Sie nach IP-Adressen Ihrer Gateways schauen können.

Die Traceback-Taktik und die Blackhole-Verteidigung gegen DDoS-Angriffe sind in Situationen nützlich, in denen Fluten von bösartigem Verkehr die Header gefälscht (gespooft) haben. Dies war bis vor kurzem noch der gebräuchliche Weg solche Angrife durchzuführen. Aber durch die starke Zunahme von Zombie-Maschinen und Botnetzen, haben viele Angreifer aufgehört, DDoS-Pakete zu spoofen – es gibt keinen Grund, Header zu fälschen, wenn die Armee aus attackierenden Systemen überall ist. Gleichfalls sind gespoofte DDoS-Angriffe wegen des breiteren Einsatzes von uRPF und Eintritt-Filterung zurückgegangen. ●